

國立臺灣大學法律學院法律學系



碩士論文

Department of Law

College of Law

National Taiwan University

Master Thesis

警察使用人臉辨識系統查證身分的合法性研究—以

M-Police 即時相片比對功能為中心

The Legality of Police Administration Using AFR

Identifying People: Focusing on M-Police Facial

Recognition System

甘佳加

CHIA-CHIA KAN



指導教授：李建良 博士

Advisor: Chien-Liang Lee, Dr.iur

中華民國 110 年 1 月

Jan 2021

國立臺灣大學碩士學位論文

口試委員會審定書

警察使用人臉辨識系統查證身分的合法性研究—以
M-Police 即時相片比對功能為中心

The Legality of Police Administration Using AFR
Identifying People: Focusing on M-Police Facial
Recognition System

本論文係甘佳加君（R07A21011）在國立臺灣大學法律學系
完成之碩士學位論文，於民國110年1月11日承下列考試委員審查
通過及口試及格，特此證明

指導教授：

李康良

口試委員：

李寧修

謝碩致

李康良



謝辭

本文的寫作由開始到結束，前前後後耗時近一年。前期蒐集資料的時候，便遭遇很大的困難，多次都想著是不是要換論文題目，從頭開始了，還好有滢仁、惠萱及惠萱爸爸及時的出手幫忙，才能夠順利地蒐集到足夠的資料開始寫作，若不是有你們的幫助，給予足夠的素材，本文怕是要胎死腹中了！開始撰寫以後，更大的困難迎面而來，邏輯的不一致及寫作上的盲點一一浮現，前後進行了數次大大小小的修正，但總感覺沒辦法修到重點，挫敗感不斷累積，多次讓人想打退堂鼓。感謝指導教授李建良老師耐心的指導，幫助學生調整論文架構及定名，穩住整篇文章的進行，討論時也具體的告訴學生修正的方向，讓論文的寫作能夠繼續進行，不致整篇文章亂了套，以致後續的論發及口試遙遙無期。感謝在天寒地凍的早晨中來參加論發的各位同學們以及對於本文所給予的修正上建議。感謝爽快答應擔任學生口試委員的謝碩駿老師及李寧修老師，兩位老師於口試時，給予了學生十分豐富的反饋，一步一步耐心的引導學生領會本文思考上的盲點，指出本文的不足之處，讓最後的修正能夠順利無礙的進行，也讓本篇文章能夠更加完整。

開始寫作的這一年來，畢業的壓力如影隨形，寫作上也時常遇到腦袋空空沒有靈感導致論文進度大幅落後，不知所措的時候，感謝亭宇這一路上的鼓勵，在我論文焦慮症發作的時候，陪我到處閒逛紓壓，穩定情緒，及協助論文的校對；感謝擔任論發及口試紀錄的韻帆，若不是有妳完整而細節的紀錄，後續的修正就無法如此順利的完成，更謝謝妳在論發及口試後為我加油打氣，讓我無論如何都要對自己有信心能夠把最後這一哩路走完，這一路有妳陪我，是我最幸運的事情；謝謝我親愛的姐姐，以一個過來人的身分，不斷叮囑我、鞭策我的論文寫作進度，更在口試當日到場陪伴，幫助緩解緊張情緒及及時處理突發狀況。更謝謝我的父母，這一路上的陪伴與支持，他們在台北及苗栗兩處來回奔波，只為了讓我能夠

心無旁騖專心於寫作上，協助我處理大大小小的事情，感謝我的父母讓我能夠向著畢業的目標勇往直前。



歷經無數個挑燈夜戰的夜晚，看過數次的日出，本文終於完成。心情放鬆之餘，碩士生涯也將進入尾聲而邁向人生的下一階段。感謝一路上提點我的老師們，及陪伴我、為我加油打氣的朋友、家人們。謹將本文獻給你們。

佳加 Jan, 2021.

中文摘要

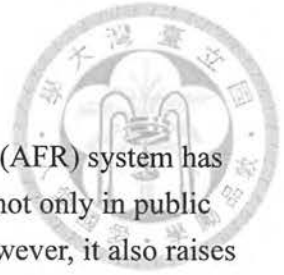


由於科技不斷進步，人臉辨識技術發展亦日趨成熟。現今，不論於公領域或是私領域，人臉辨識系統均被廣泛地運用，人臉辨識系統帶來生活上便利的同時亦對隱私權的保護造成衝擊。而自 2012 年起，我國警政署啟用 M-Police 人臉辨識系統（正式名稱為：即時相片比對功能）並應用於相關勤務之執行上。本文聚焦於警政署針對人臉辨識系統的應用，具體而言，於警察行政危害防止層面上的應用，探討警察於執行危害防止任務時，使用人臉辨識系統查證民眾身分的合法性。職是之故，本文首先將說明使用人臉辨識系統查證身分對於基本權所造成的影響及憲法第 23 條關於限制基本權之要件。由於目前警察使用該系統係以取得當事人同意為前提，探討該同意與法律保留原則間的關係。最後是關於警察職權行使法上的分析，究竟該法得否支撐警察使用此系統查證民眾身分。

除此之外，為有效使用人臉辨識系統進行身分識別，人臉資料庫的建立不可或缺。警政署所開發使用的 M-Police 人臉辨識系統背後亦建有龐大的資料庫，其中最具爭議者，在於使用內政部戶政司國民身分證相片資料庫之資料作為人臉資料庫之建檔基礎。此舉屬於機關間資料共享（流通）之情形，涉及諸多法律上爭議，例如：個資法及警職法上有關資料蒐集及利用規定的適用順序及個資法第 16 條但書第 2 款「增進公共利益」的解釋等，本文亦將著重於此進行分析。將警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫之行為，分為戶政機關傳遞相片資料、警政署取得相片資料及使用該資料建置人臉資料庫此三個行為，並分別探討所涉的法律爭議。

中文關鍵字：人臉辨識系統、隱私權、法律保留、當事人同意、警察職權行使法、個人資料保護、目的拘束原則、機關間資料共用

Abstract



Since technology improved so fast, Automatic Facial Recognition (AFR) system has become more and more mature. Nowadays, AFR is commonly used not only in public sector but also in private. Undoubtedly, AFR brings convenience, however, it also raises great privacy issue as well. In 2012, National Police Agency started to apply their own AFR system, the so-called M-Police Facial Recognition system, to several services. This thesis will focus on analyzing the legality of police administration using M-Police facial recognition system identifying people. To be more specific, focus on the legality of the use of the system in terms of preventing hazards.

The analysis will start with the impact it brought to the rights protected under the Constitution. According to Article 23 of the Constitution, all the freedoms and rights enumerated in the preceding Articles shall not be restricted by law except by such as may be necessary to prevent infringement upon the freedoms of other persons, to avert an imminent crisis, to maintain social order or to advance public welfare. Therefore, the thesis would first discuss whether the law is needed if police officers use AFR under the consent of the person. Analyze the relationship between consent and Legal Retention Principle and then discuss whether Police Power Exercise Act is enough to support the use of M-Police Automatic Facial Recognition system.

Nevertheless, in order to use AFR system properly, face database is necessary. In order to make the best use of M-Police facial recognition system, National Police Agency built the face database not only from their own database but also from National ID Card Photo Database kept in the Department of Household Registration, Ministry of The Interior. Such incorporation was the most controversial. It would raise serious personal data protection issue when the data was transformed from one agency to another. Yet the thesis would also analyze the legal problem involved in such behavior under Personal Data Protection Act.

Key words: Automatic Facial Recognition system, privacy, consent, Legal Retention Principle, Police Power Exercise Act, personal data protection, the principle of purpose-specification, data sharing between sectors,

簡目



第一章 緒論	1
第一節 研究動機與目的	1
第二節 研究範圍	3
第三節 問題意識與研究方法	5
第四節 本文架構	6
第二章 警政署人臉辨識系統的建置與應用	10
第一節 人臉辨識系統介紹	10
第二節 警政署 M-Police 人臉辨識系統介紹	13
第一項 M-Police 警用行動載具說明	14
第二項 系統運作	19
第三節 英國南威爾斯警局使用人臉辨識系統的情形	27
第四節 小結	31
第三章 警察使用人臉辨識系統查證身分對基本權之影響	34
第一節 警察臨檢對基本權之影響	35
第二節 人臉辨識系統的使用對隱私權之影響	40
第一項 我國隱私權之發展	40
第二項 資訊隱私權內涵	45
第三項 人臉辨識系統對資訊隱私權保障的衝擊	48
第三節 警察使用人臉辨識系統與憲法第 23 條限制基本權之要件	49
第四章 警察使用人臉辨識系統查證身分的合法性	53
第一節 警察使用人臉辨識系統與法律保留原則	53
第一項 法律保留原則詳要	53
第二項 當事人同意與法律保留原則間之關係	57
第二節 現行警察使用人臉辨識系統查證身分之法制	61
第一項 人臉辨識系統與警察職權行使法	62
第二項 警政署針對人臉辨識系統使用的內控規範	76
第三項 小結	85
第三節 警察使用人臉辨識系統與比例原則	88
第一項 警察使用人臉辨識系統的評估	90
第二項 警察使用人臉辨識系統的疑慮	94
第五章 警政署使用國民身分證相片資料建置人臉資料庫之爭議	97
第一節 國民身分證相片資料之蒐集及提供與資料庫的建置	98
第一項 國民身分證相片資料之蒐集與資料庫之建置	98
第二項 機關申請使用國民身分證相片資料庫的程序規範	100
第二節 警政署以國民身分證相片資料作為人臉資料庫建檔基礎之爭議	

第一項	個資法—目的拘束原則.....	111
第二項	戶政機關傳遞國民身分證相片資料予警政署.....	118
第三項	警政署取得及使用國民身分證相片影像檔建置人臉資料庫..	125
第三節	評析.....	133
第一項	警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫 133	
第二項	申請程序及警政署內部使用規範.....	136
第六章	結論.....	138
參考文獻		148

詳目



第一章 緒論	1
第一節 研究動機與目的	1
第二節 研究範圍	3
第三節 問題意識與研究方法	5
第四節 本文架構	6
第二章 警政署人臉辨識系統的建置與應用	10
第一節 人臉辨識系統介紹	10
第二節 警政署 M-Police 人臉辨識系統介紹	13
第一項 M-Police 警用行動載具說明	14
第一款 M-Police 的開發	15
第二款 M-Police 建置人臉辨識系統	17
第二項 系統運作	19
第一款 系統操作	19
第二款 使用情狀	20
第三款 M-Police 申請主體要件	22
第四款 辨識方法採用	25
第三節 英國南威爾斯警局使用人臉辨識系統的情形	27
第四節 小結	31
第三章 警察使用人臉辨識系統查證身分對基本權之影響	34
第一節 警察臨檢對基本權之影響	35
第二節 人臉辨識系統的使用對隱私權之影響	40
第一項 我國隱私權之發展	40
第二項 資訊隱私權內涵	45
第三項 人臉辨識系統對資訊隱私權保障的衝擊	48
第三節 警察使用人臉辨識系統與憲法第 23 條限制基本權之要件	49
第四章 警察使用人臉辨識系統查證身分的合法性	53
第一節 警察使用人臉辨識系統與法律保留原則	53
第一項 法律保留原則詳要	53
第一款 法律保留原則的內涵	53
第二款 法律保留原則之範圍	54
第二項 當事人同意與法律保留原則間之關係	57
第二節 現行警察使用人臉辨識系統查證身分之法制	61
第一項 人臉辨識系統與警察職權行使法	62
第一款 警察職權行使法的立法	62
第二款 警察職權行使法之定位	65
第三款 臨檢的內涵以及警職法身分查證規定之介紹	65

第二項 警政署針對人臉辨識系統使用的內控規範	76
第三項 小結	85
第一款 人臉辨識系統作為查證身分之手段與警職法規定間的扞格	85
第二款 警政署針對人臉辨識系統使用內控措施的缺失	87
第三節 警察使用人臉辨識系統與比例原則	88
第一項 警察使用人臉辨識系統的評估	90
第二項 警察使用人臉辨識系統的疑慮	94
第五章 警政署使用國民身分證相片資料建置人臉資料庫之爭議	97
第一節 國民身分證相片資料之蒐集及提供與資料庫的建置	98
第一項 國民身分證相片資料之蒐集與資料庫之建置	98
第二項 機關申請使用國民身分證相片資料庫的程序規範	100
第一款 警政署申請使用戶政機關國民身分證相片資料庫之程序規範	100
第二款 警政署使用國民身分證相片資料庫的使用規範	104
第二節 警政署以國民身分證相片資料作為人臉資料庫建檔基礎之爭議	108
第一項 個資法—目的拘束原則	111
第一款 目的拘束原則的內涵	112
第二款 目的拘束原則之例外	114
第二項 戶政機關傳遞國民身分證相片資料予警政署	118
第一款 戶政機關傳遞行為之性質	120
第二款 傳遞行為與個資法第 16 條但書第 2 款「增進公共利益所必要」	123
第三項 警政署取得及使用國民身分證相片影像檔建置人臉資料庫 ..	125
第一款 警職法與個資法間的關係	125
第二款 警政署取得及使用戶政機關國民身分證相片資料建置人臉資料庫 ..	129
第三節 評析	133
第一項 警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫 ..	133
第一款 有關「執行法定職務範圍之必要」之內涵	134
第二款 個資法第 16 條但書第 2 款「增進公共利益」過於抽象 ..	135
第三款 警察「危害防止」的職務內涵	136
第二項 申請程序及警政署內部使用規範	136
第六章 結論	138
參考文獻	148

圖目錄



圖 1、M-Police 新舊版示意圖，資料來源：Ithome， https://www.ithome.com.tw/article/117303 (最後瀏覽日：06/15/2020)。	14
圖 2、M-Police 設計架構圖，資料來源：內政部警政署 (2012)，〈內政部警政署「M-Police 行動警察建置案簡介」〉，《政府機關資訊通報》，第 291 期，頁 2。	14
圖 3、現今 M-Police 的功能示意圖，資料來源：內政部警政署 (2018)，〈內政部警政署「前瞻警政、科技警察」智慧聯網專案〉，《政府機關資訊通報》，第 352 期，頁 4。	16
圖 4、警政巨量資料平臺機關整合示意圖，資料來源：內政部警政署 (2018)，〈內政部警政署「前瞻警政、科技警察」智慧聯網專案〉，《政府機關資訊通報》，第 352 期，頁 3。	16
圖 5、警政雲運作架構，資料來源：內政部警政署資訊室 (2014)，〈政府機關資訊通報〉，第 317 期，頁 2，臺北：內政部警政署。	18
圖 6、M-Police 與警政雲端系統整合示意圖，資料來源：內政部警政署 (2018)，〈內政部警政署「前瞻警政、科技警察」智慧聯網專案〉，《政府機關資訊通報》，第 352 期，頁 2。	19
圖 7、警政相片比對系統架構，資料來源：張凱淳 (2012)，〈人臉辨識技術應用於警政治安之探討研究〉，《前瞻科技與管理》，2 卷 1 期，頁 87。	25
圖 8、多重比對臉部檢測法示意圖，資料來源：NEC 官網， https://tw.nec.com/zh_TW/solutions/security/neofacetec.html ? (最後瀏覽日：06/11/2020)。	26
圖 9、攝動空間法示意圖，資料來源：NEC 官網， https://tw.nec.com/zh_TW/solutions/security/neofacetec.html ? (最後瀏覽日：06/11/2020)。	26
圖 10、適應領域混合比對法，資料來源： https://tw.nec.com/zh_TW/solutions/security/neofacetec.html ? (最後瀏覽日：06/11/2020)。	27

表目錄

表 1、我國及英國南威爾斯警局使用人臉辨識系統的比較，資料來源：本文自製	33
--------------------------------------	----



第一章 緒論

第一節 研究動機與目的

人臉辨識系統係利用人臉特徵資料進行身分辨識，為生物識別技術之一，該技術自西元（下同）1970 年代發展迄今約莫 50 年，技術日趨成熟，如今人臉辨識技術已有高達 99.8% 的辨識率¹，因此近年來，不論是在公領域或是私領域，人臉辨識系統均被廣泛的應用，目前已知常見的使用方式包含：國家海關出入、犯罪偵查及預防、門禁系統、線上購物付款、偵測並鎖定廣告投放客戶、解鎖科技裝置、社群媒體的標記（tag）功能、搜尋引擎以圖找圖、學校的點名與學習系統、商家偵測特定族群或個人等²。其中，人臉辨識於犯罪偵查及預防的應用上主要有二方面，一為內政部警政署開發 M-Police 警用行動載具（本文以 M-Police 簡稱之），並內建人臉辨識功能，正式名稱為即時相片比對功能（本文的討論客體，為求寫作上之便利，以人臉辨識系統稱之），並用於緝捕通緝犯以及犯罪預防（或廣義而言，可稱危害防止）的勤務；而另一將人臉辨識系統用於犯罪偵查的機關為法務部調查局³。本文的研究重心則置於前者，即內政部警政署對於人臉辨識系統的應用上。

自 2012 年起，警政署啟用 M-Police 人臉辨識系統並應用於相關勤務上，此一系統對於查證身分、協助失智老人返家⁴以及打擊犯罪⁵有莫大助益，惟另一方面警

¹ Ithome, <https://www.ithome.com.tw/news/131691>（最後瀏覽日：06/16/2020）。

² 臺灣人權促進會, <https://www.tahr.org.tw/news/2288>（最後瀏覽日：06/16/2020）。

³ Ithome, <https://www.ithome.com.tw/news/131691>（最後瀏覽日：06/16/2020）。

⁴ 例如：臺灣即時報，

<https://1688safety.com/2019/05/07/%E5%B0%B1%E6%98%AF%E9%80%99%E6%A8%A3%E5%A5%BD%E7%94%A8-m-police%E4%BA%BA%E8%87%89%E8%BE%A8%E8%AD%98%E5%8A%A9%E5%A4%B1%E6%99%BA%E8%80%81%E4%BA%BA%E5%9B%9E%E5%AE%B6/>（最後瀏覽日：06/16/2020）；屏東時報, <https://pingtungtimes.com.tw/?p=18698>（最後瀏覽日：06/16/2020）；警光, <https://police.npa.gov.tw/NPAGip/wSite/ct?xItem=117003388&ctNode=11511&mp=1>（最後瀏覽日：06/16/2020）；公民新聞, <https://www.peopo.org/news/395467>（最後瀏覽日：06/16/2020）；桃園電子

察對於人臉辨識系統的使用亦遭立委質疑嚴重侵害個人資訊隱私權，且並無相關法律做為依據⁶，尤其該系統整合內政部戶政司國民身分證相片資料作為其人臉資料庫的建檔基礎之一，代表持有 M-Police 的警察等同握有全國 2,300 萬人民的個人資料，若資料不慎外洩，將對民眾造成難以想像的隱私權侵害。為了回應立委針對 M-Police 人臉辨識系統的質疑，亦為說明警政署使用該系統的法律依據。警政署發布針對人臉辨識系統的疑慮說明資料。據該資料所稱，警政署引進 M-Police 人臉辨識系統的使用，有警察職權行使法（本文簡稱警職法）第 6 條及第 7 條有關警察查證身分之規定可作為法律依據，同時警政署亦建有內部監督制度確保資料安全以及監督設備的使用情形。除此之外，於人臉資料庫方面，警政署基於警察行使職權、維護治安及危害防止之目的，取得內政部戶政司國民身分證相片資料並使用該資料建置人臉資料庫，均有依照戶籍法及個人資料保護法（本文簡稱個資法）之規定，且針對該相片資料的保護，機關亦訂有內政部警政署國民身分證相片影像資料使用管理要點，規範相關資安措施，避免資料外洩，因此合法無虞。警政署欲藉由此說明資料，除說明其使用人臉辨識的正當性基礎外，亦希望能夠消除民眾對於警政使用人臉辨識系統執法的疑義。

縱使根據上述警政署所發布的疑慮說明資料，警察使用人臉辨識系統似無任何爭議。惟本文仍然對於警察使用人臉辨識系統查證身分一事抱持懷疑態度，聚焦於警察將 M-Police 人臉辨識系統應用於危害防止之勤務上，作為蒐集資料的手段，尤其是用於查證身分的情形，而此處所指的查證身分，專指警察依警職法第 6 條及第 7 條所為的身分查證行為。鑒於人臉辨識系統對於資訊隱私權影響甚鉅，

報，<https://tyenews.com/2019/11/34951/>（最後瀏覽日：06/16/2020）。

⁵ 例如：三立新聞網，<https://www.setn.com/News.aspx?NewsID=400405>（最後瀏覽日：06/16/2020）；自由時報，<https://news.ltn.com.tw/news/society/breakingnews/1312869>（最後瀏覽日：06/16/2020）。

⁶ 立委質疑，太陽花學運期間警政署不斷地到處錄影蒐證，再藉由 M-police 連結戶政資料，蒐集參與學運人員之個資，並加以建檔，以「偵查犯罪」之藉口，行政治監控之實，同時便於秋後算帳，且並無相關法律支持該行政作為。

<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=12332&pid=156431>（最後瀏覽日：06/16/2020）。



人民對於此一系統本身便抱持著懷疑的態度，而警政署更進一步將此一系統應用於危害防止任務之執行，是否真如警政署所發布的說明資料所述，警察此一應用合法無虞？本文以為，實有細究的必要。警政署基於危害防止的目的，除導入人臉辨識系統的使用之外，更基於該目的，取得內政部戶政司國民身分證相片資料，並用於建置人臉資料庫。簡言之，該系統背後的人臉資料庫，除整合警政署自身的失蹤人口、前科犯、通緝犯及治安顧慮人口資料庫的資料外，亦整合內政部戶政司國民身分證相片資料作為人臉資料庫的比對來源之一，因此民眾只要持有國民身分證，警察便可有效利用該系統查證民眾身分，等於警察「一機在手。全國2,300萬人民的個資手到擒來」，此舉有效提升警察值勤效率的同時亦引發極大的爭議。

綜上，本文將探討警察使用人臉辨識系統查證身分的合法性。警察使用人臉辨識系統查證身分對於現行法制的衝擊，探討於現行法制下，為何警察使用人臉辨識系統極具爭議的原因。除此之外，該系統另一個引發爭議之處在於背後的人臉資料庫，除整合警政署自有的失蹤人口及通緝犯資料等外，亦使用戶政司國民身分證相片資料，此為該系統的特殊之處，本文亦將針對警政署使用戶政機關國民身分證相片資料建置人臉資料庫一事進行探討。

第二節 研究範圍

目前警政署所開發的 M-Police 人臉辨識系統，主要應用於危害防止及犯罪偵查兩方面。於犯罪偵查方面，此系統對於逮捕通緝犯有莫大的助益；而於為害防止方面，則係於警察臨檢的使用最為常見。為害防止屬於警察的行政作用，涉及警職法的相關規定，而犯罪偵查則涉及刑事訴訟法的規定。雖二種情況警政署均導入人臉辨識系統的使用，惟所涉及的法律問題實則完全不同，而本文礙於篇幅，無法將兩種使用人臉辨識系統的情況均加以分析，為求問題意識以及文章架構的

明確，本文研究範圍限於此系統於危害防止方面的應用，亦即限於警察執行危害防止任務而使用人臉辨識系統查證身分的情形，涉及警職法之規定。以下便以一件警察於查證身分時使用人臉辨識系統的實例更加具體說明本論文的研究範圍。

於 2020 年 7 月 20 日，桃園一名 84 歲廖姓老翁，因步伐較慢，半路與好友走散，沒想到老翁居然足足走了 5 公里，直到體力不支癱坐公園長凳，恰逢北勢派出所警員巡邏經過，由於老翁體力透支，說起話來有氣無力，面對員警詢問亦完全無法清楚表達，於是員警利用 M-Police 人臉辨識系統查出老翁身分，並聯繫上老翁心急如焚的親人，讓其平安回到家人身邊⁷。

上述的案例可更加具體的說明本論文的研究範圍，本論文的研究範圍，精確而言，著重於探討 M-Police 人臉辨識系統於危害防止任務應用的合法性。警察之職權依警察法第 2 條之規定：「警察任務為依法維持公共秩序，保護社會安全，防止一切危害，促進人民福利。」概念上，「危害防止」較能全面的說明警察行政任務⁸，犯罪預防屬於危害防止任務的一部分⁹，警察危害防止任務的範圍包括犯罪預防以及保護人民生命、身體免受危害等，因此警職法第 6 條中關於警察查證身分之情事不限於合理懷疑有犯罪之嫌疑或有犯罪之虞的情形，亦可因有防止本人或他人生命、身體之具體危害之必要下查證其身分。職是之故，於名稱上，本文使用「危害防止」而非「犯罪預防」來說明警察行政任務的內涵。惟不論犯罪預防或是危害防止，均是警察行政任務一環，而警職法作為警察行政的重要法律規範，本文於分析此應用之合法性時將聚焦在警職法的討論上。又因警察多將該系統作

⁷ 桃園電子報，<https://tyenews.com/2020/07/71210/>（最後瀏覽日：08/03/2020）。

⁸ 警察的作用可區別為行政及司法二種，後者為警察協助犯罪偵查方面的職權涉及刑事訴訟法的相關規定，前者為本文的研究範圍，危害防止便是警察行政作用的一環，而警職法即是規定警察行政作用的法規範之一。陳英淙（2017），〈論警察危害防止與刑事追訴的分與合〉，《政大法學評論》，第 151 期，頁 97。

⁹ 陳英淙（2019），〈從危害概念論警察法中的資訊式職權（informationelle Befugnisse）--以監視錄影為例探討之〉，《軍法專刊》，65 卷 5 期，頁 8-11。



為查證身分、資料蒐集之手段，尤以查證身分之情形最為普遍，因此將著重在本文第 6 條及第 7 條之討論。至於警察於犯罪偵查時使用此一系統則不在本文的研究範圍。本文所稱查證身分行為專指警察執行警職法第 6 條及第 7 條之行為而言。查警職法第 6 條及第 7 條有關查證身分之要件及手段之規定，係專為警察執行危害防止任務而欲查證身分時所訂定¹⁰。詳言之，本文之研究範圍限於警察執行危害防止勤務，依據警職法第 6 條及第 7 條之規定查證民眾身分時，使用人臉辨識系統的合法性，著重於警職法第 6 條及第 7 條第 2 款及第 3 款，即警察查證民眾身分的要件及手段之規定，尤其針對警職法第 7 條有關查證身分之手段，分析警職法作為警察使用人臉辨識系統查證身分法律依據的爭議之處。除此之外，由於人臉辨識系統亦是資料蒐集的手段之一，警職法第二章「身分查證及資料蒐集」中有關之規定本文亦將加入一同分析。

第三節 問題意識與研究方法

本文藉由整理及分析相關書面文獻作為主要研究方法來探討下述之問題，且由於 M-Police 人臉辨識功能的使用涉及實務，因此亦詢問相關人士，了解該系統於實務上的使用情形並取得警政署內部未公開之行政規則，讓本文可更加全面的分析現行警政使用人臉辨識系統查證身分之法制。

人臉辨識系統與警察查證身分的行為結合，將限制人民基本權的保護，尤其對於隱私權的影響更甚。而依憲法第 23 條之規定，限制基本權的保護須符合法律保留原則及比例原則。於法律保留的討論上，首先，由於警察使用此一系統查證身分係以取得當事人同意為前提，鑒於我國警察人臉辨識系統的使用情形係一對一之模式，當事人的同意極具重要性，若該系統之使用係以取得當事人同意為前提，是否仍須有明確法律依據？再者，若仍須法律依據，現行警職法第 6 條及第 7

¹⁰ 立法院第五屆第三會期第十五次會議議案關係文書，警察職權行使法草案審查報告，頁 200-201。

條之規定是否足以支撐此一應用？探討現行法制下，警察使用人臉辨識系統查證身分的困境以及可能的解決途徑。於比例原則方面，以經當事人同意使用該系統便無需法律依據為前提假設下，評估該系統是否有助於危害防止目的的達成。

除此之外，警察所使用的人臉辨識系統，其背後的人臉資料庫除使用機關自身的失蹤人口及通緝犯資料外，亦使用內政部戶政司國民身分證相片資料作為建檔基礎，此一行為涉及個人資料的蒐集及利用，第一層次涉及機關蒐集及利用該個資的依據，尤其是警政署可否基於犯罪預防之目的而取得此一個資；第二層次則涉及機關蒐集及利用該個資是否符合個資法之討論，涉及個資法目的拘束原則的原則及例外的適用，且於本文機關間資料共享之情形，於個資法的討論上，由於個資法並未針對機關間資料共享之情形有獨立規定，因此於此種情形，須分別針對戶政機關以及警政署適用個資法的規定。於警政署而言，其取得及使用該資料建置人臉資料庫，依個資法第 15 條及第 16 條之規定，需為執行法定職務之必要始可，因此爭議在於，警察可否基於犯罪預防之目的，取得及使用相片資料建置人臉資料庫？此一問題涉及警察犯罪預防任務的內涵。於戶政機關而言，其將相片資料傳遞予警政署之行為，係逾越蒐集目的利用個資之情形，須探討是否符合個資法第 16 條但書之規定，是否係基於增進公共利益且為「執行法定職務所必要」？此一問題亦與警察危害防止任務的內涵有關。

第四節 本文架構

本論文共計六個章節，探討警察使用人臉辨識系統查證身分之合法性，以及該系統使用內政部戶政司國民身分證相片資料作為人臉資料庫建檔基礎的爭議。本文章節安排如下：

第一章為緒論。介紹本文的研究動機及目的、並劃定研究範圍以及說明本文

的問題意識及研究方法。本文係研究警察執行危害防止任務時，使用人臉辨識系統的合法性，究竟警職法有關身分查證及資料蒐集之相關規定或本法第 28 條之規定可否作為警察使用人臉辨識系統的法律依據。除此之外，亦探討該系統使用內政部戶政司國民身分證相片資料建置人臉資料庫的合法性。

第二章則是介紹人臉辨識技術以及警察所使用 M-Police 人臉辨識系統，說明該系統於實務上的使用情形、使用程序以及申請的主體要件等，並藉由比較我國與英國南威爾斯警局的使用人臉辨識系統的情形，突顯我國警察使用人臉辨識系統的特殊之處。

第三章則是分析警察使用人臉辨識系統查證身分對於基本權之影響。由於警察將人臉辨識系統的使用與臨檢結合，作為查證身分的手段，因此臨檢對於基本權所造成之影響，自人臉辨識系統導入後仍會存在，且臨檢對於基本權之影響是影響我國臨檢法制的關鍵因素，因此本文認為針對此部分仍有加以說明的必要，以利後續法制上的探討。針對警察臨檢對於基本權之影響，已有釋字第 535 號解釋在案，可資參照。本章除再度說明警察臨檢對於基本權之影響外，亦會詳細分析人臉辨識系統對於隱私權之影響。人臉辨識系統係使用人臉特徵資料進行身分識別的科技。因此，於隱私權的討論上，包括人臉特徵資料之特性、該資料是否屬於資訊隱私權的保護客體、警政署蒐集利用該個資是否會限制資訊隱私權之保障等，均為本章所欲探討之問題。

第四章承接上一章之說明，由於人臉辨識系統與查證身分行為結合將限制人民基本權之保護，因此依據憲法第 23 條之規定，須符合法律保留原則及比例原則之要求。本章分為兩大部分，第一部分說明此一應用與法律保留原則間的關係，由於警察使用此一系統查證身分係以取得當事人同意為前提，則第一個爭議在於

倘此一應用係基於當事人之同意，是否還需法律保留？此涉及法律保留原則之範圍。而第二個爭議在於，倘此一應用仍需有明確的法律依據，則現行以警職法為中心的法制是否足夠支撐此一使用？探討現行法制下，警察使用人臉辨識系統的困境。其中，針對警察使用人臉辨識系統查證身分與警職法規範間的衝突，此一問題本文將由警察臨檢此一行為的內涵的角度出發進行說明。由於釋字第 535 號解釋中對於臨檢，該解釋使用警察勤務條例第 11 條第 3 款對於臨檢之定義¹¹，亦即定位於舉凡警察採取限制或干預人民的行動自由、財產權或隱私權的手段，如：檢查、路檢、取締或盤查等，不問名稱為何，均可稱之為臨檢，將臨檢採取較為廣義之解釋¹²。身分查證行為基於其權利侵害性，自屬臨檢。臨檢的性質係屬行政機關為達成行政目的所行使的蒐集資料之行為¹³，而不論是在對人或是對處所之臨檢，身分查證為臨檢不可或缺的程序，因此亦有學者直接將警職法中賦予警察身分查證之權限直接稱其路檢或臨檢¹⁴。無論如何，身分查證為警察臨檢的必要行為，而為說明警察使用人臉辨識系統查證身分與現行警職法有關身分查證規定有所衝突的理由，仍需由警察臨檢此一行為的內涵出發加以說明。第二部分則係此一應用與比例原則間的關係，假設於法制上允許警察使用人臉辨識系統查證身分，評估此一應用是否有助於危害防止目的之達成、是否為警察執行危害防止任務達成所必要，且為侵害最小之手段？

第五章則針對人臉資料庫之部分進行探討。由於警察所使用的人臉辨識系統其背後的人臉資料庫除使用機關自身的前科犯、失蹤人口、通緝犯及治安顧慮人口資料庫之資料外，其中，最具爭議者，在於使用內政部戶政司國民身分證相片

¹¹ 警察勤務條例第 11 條第 3 款：「臨檢：於公共場所或指定處所、路段，由服勤人員擔任臨場檢查或路檢，執行取締、盤查及有關法令賦予之勤務」

¹² 周燕輝（2003），《行政調查法制之研究：以警察臨檢法規範為核心》，頁 98，私立中國文化大學法律學研究所碩士論文。

¹³ 周燕輝，前揭註 12，頁 109。

¹⁴ 林明鏘（2010），〈警察行使職權與身分查證之問題〉，氏著，《警察法學研究》，二版，頁 390，臺北：新學林。



資料庫之資料作為建檔基礎。本章將分析警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫之合法性。針對此一問題的分析將分為兩個部分，首先第一部分為說明內政部取得國民身分證相片資料的法律依據及他機關請求提供該資料的程序規範。第二部分為探討警察使用內政部戶政司國民身分證相片資料建置人臉資料庫的爭議。此一行為屬於機關間資料共享（流通）之情形，本文依先後順序，分為戶政機關傳遞相片資料、警政署取得及使用相片資料建置人臉資料庫此三行為，並分別探討各行為所涉的爭議，同時藉由本文之情形，說明現行個資法的不足之處。

第六章為結論。總結前幾章之討論，分別對於警察使用人臉辨識系統查證身分的合法性及該系統使用內政部戶政司國民身分證相片資料建置人臉資料庫的爭議提出本文之看法。警察如欲合法無虞的於執行危害防止任務時使用人臉辨識系統查證身分，警職法應有明確的法律依據，且該系統的使用與達成警察危害防止任務有密切關聯，始可合法無虞，惟現今警職法並無明文准許警察可使用此一系統查證民眾身分，縱認在法無明文的情形下，得基於當事人的同意而使用此一系統，惟此一系統是否與達成危害防止任務間有密切關聯，在警政署並無相關統計數據佐證以及現今該系統係作為輔助工具的情形下，或有疑慮。而在警察使用內政部戶政司國民身分證相片資料建置人臉資料庫方面，警察危害防止職務可否正當化取得相片資料以及建置人臉資料庫，須視該任務之內涵為斷，警察犯罪預防任務的內涵，由於數位時代的來臨以及組織犯罪的猖獗等因素，或有漸漸擴張之趨勢，但基於為害防止之目的使用國民身分證相片資料建置人臉資料庫亦有將普羅大眾均當作犯罪嫌疑人之疑慮，需審慎評估。縱認答案為肯定，現行個資法對於逾越蒐集目的外使用個資之情形，有規範寬鬆之嫌，尤其是與本文有關的個資法第 16 條但書第 2 款之事由「增進公共利益」，過於抽象，不利於個人資料保護。除此之外，就申請提供相片資料之程序也有未竟之處，將於結論中總結。

第二章 警政署人臉辨識系統的建置與應用



本章將介紹人臉辨識系統、警政署所使用的 M-Police 人臉辨識系統以及該系統實務上使用情形與申請主體要件等。

第一節 人臉辨識系統介紹

人臉辨識(Automatic Facial Recognition, 簡稱 AFR), 屬於生物識別(Biometric)的一種。生物識別是指透過人體指紋、臉部、聲音或虹膜等身體器官組織的獨特性來辨識身分的一項技術, 使用人體身上的特徵作為識別的密碼, 因此在技術的開發上必須選擇準確度高、容易使用的辨識特徵以利使用, 主要可分為生理上的(如臉形、指紋、虹膜), 或是獨特的行為模式(如聲音、簽名、密碼)。以準確度來說, 「生理特徵」在唯一性及安全性上明顯優於「行為特徵」。生物識別技術是利用每個人獨一無二的生理或行為特徵來辨識使用者的身分, 易言之, 在生物識別技術的運用下, 你的身體就是密碼, 不需要額外記住一長串不易記住的數字, 也不怕遺失, 複製不易, 更不用擔心遭人盜用, 因為你是獨一無二且「隨身攜帶」¹⁵。而人臉辨識系統就是透過個人的臉孔, 識別某特定個人之身分的生物識別技術之一。

人臉辨識技術既是利用人臉進行身分辨識, 因此該技術的前提為「人臉偵測」(Face Detection), 找出可供比對的人臉影像。人臉偵測有 4 種常見的方式¹⁶, 分別為: 條列式規則區分法(Knowledge-Based method)¹⁷、樣板比對法(Template-Based

¹⁵ 曾婉菁(2014),〈人臉偵測及辨識方法探究〉,《印刷科技》,30 卷 2 期,頁 21。

¹⁶ 賴昭嘉(2012),《基於行動裝置與安控系統之人臉辨識系統》,頁 21-22,國立臺灣科技大學資訊工程學系碩士論文。

¹⁷ 條列式規則區分法主要是將一般主要人臉的成像知識來進行影像編碼,簡言之,以建立規則的方式偵測人臉。這樣的好處是,所取得的人臉在局部化時可以將特徵作人臉影像區域標定,利用人

method)¹⁸、基於表像的方法 (Appearance-Based method)¹⁹及基於特徵的方法 (Feature-Based method)²⁰。不論是上述哪種方式，均是以讓系統找出可供比對的人臉為其主要目的，藉由告知系統「何謂人臉」，讓其自動找出可供比對之樣本。

一般來說，偵測到人臉後，「人臉辨識」便會透過電腦演算法，將所抽取出的特定人的臉部特徵資料（例如：兩眼距離、顴骨形狀、下巴形狀、或其他獨特的臉部特徵），與人臉資料庫中的其他臉孔資料加以比對，以識別出其身分。人臉辨識技術需要的只是人臉特徵資料，而系統所揀選出並用於比對的臉部資料，通常係具一定程度可識別性，可辨識出這張臉並進而確認身分即可。人臉辨識系統演算法主要任務為擷取具識別性的人臉特徵並進行身分辨識工作。進行人臉辨識時人臉特徵擷取係十分重要的工作，如何在高維的資料群中做分類並擷取特徵，並進行辨識工作是一個重要的課題²¹，技術上有主要元素分析 (Principal Component Analysis, 簡稱 PCA)、離散小波轉換 (Discrete Wavelet Transform, 簡稱 DWT)、線性鑑別式分析 (Linear Discriminant Analysis, 簡稱 LDA) 等線性分析方式及獨立

臉圖形之幾何性質來進行最後人臉區域之標定，因為標定之人臉區域假設均具有固定區域的範圍，所以在區域標定上可以用橢圓長短軸之比例來標定人臉，但是這樣的方式將耗費大量時間。賴昭嘉，前揭註 16，頁 21。

¹⁸ 樣板比對法為先建立人臉模型的範本，當範本建立好之後，並將成品用於描繪整個人臉的臉部特徵，同時計算人臉影像與範本圖案間之相互關聯性，以進行人臉偵測，此方法亦可同時用來進行人臉特徵之局部化。由於樣板配對需要耗費大量的計算成本與記憶體容量，往往在實際做法上並不實用。賴昭嘉，前揭註 16，頁 21。

¹⁹ 基於表像的方法和樣板配對的方法，在做法上是相類似的，只是基於表像方法之模型必須透過擷取大量訓練影像之臉部外觀變化來進行學習，此種學習的模型常被用來做為人臉偵測的方法。此種演算法比樣板配對法具有較高的人臉偵測率，但這種演算法需要耗費比較大量的計算時間以及記憶體空間，尤其若要將其方法建立在可攜式行動平台上，可能會造成執行時間大增或是硬體資源不足等現象。賴昭嘉，前揭註 16，頁 22。

²⁰ 基於特徵的方法是一種以人臉特徵不變的特性來進行人臉偵測之偵測法，其目的在於找出人臉存在的特徵，像是人的膚色，五官等進行比對分析。舉例來說，利用人臉膚色在色彩空間中的群聚特色，並利用這樣的群聚建立起人臉分布模型，即使當人臉姿勢、視角產生變化時，依然能夠運用基於特徵的方法來找出人臉確定的位置。而利用人臉五官的相對固定位置，或是臉部的橢圓特色等人臉幾何進行臉部定位，則可運用來進行人臉區域之局部化，並且適當地解決光線強弱對影像色彩之影響，並且在偵測正確率上準確性相當的高。賴昭嘉，前揭註 16，頁 22。

²¹ 梁皓雲 (2006)，《利用區塊人臉特徵為基礎之混合式人臉辨識系統》，頁 31，國立中央大學資訊工程研究所碩士論文。

要素分析 (Independent Component Analysis, 簡稱 ICA) 等非線性分析的方式²², 除此之外, 尚有類神經網路 (Neural Network)、支援向量機 (Support Vector Machine, 簡稱 SVM) 等方法²³。



而在比對的技術上, 目前使用的技術主要有 2D 與 3D 兩種。2D 的人臉辨識由於取像容易, 是過往最常被使用的人臉辨識技術, 但其準確率容易受環境光照、拍攝角度的干擾; 而 3D 技術的引入, 主要即是為了解決前述 2D 影像所遭遇的干擾。儘管 3D 的人臉辨識可改善 2D 的辨識問題, 卻因為 3D 的臉部模型提供了更多個人的臉部資料, 因此準確率受臉部表情的干擾也比 2D 要來得大²⁴。目前我國警政署在人臉辨識的比對技術上, 由其正式名稱 (M-Police 即時相片比對功能) 可推知, 仍是以 2D 的比對方式為主。

人臉辨識系統的好處在於, 由於其非接觸式的辨識、因此並無衛生上的疑慮, 且該系統操作簡便、速度快。再者, 人臉辨識系統無法以照片作假, 亦不會受帽子或其他外物所影響且不須受辨識者的配合即可擷取影像, 但缺點就如同前述, 該系統可能受環境外部光線所影響²⁵。

再者, 欲使用人臉辨識系統查證民眾身分, 必須建置人臉資料庫作為身分比對的基礎及來源。而警政署所使用的 M-Police 人臉辨識系統, 該系統背後的人臉資料庫, 以國民身分證相片資料、前科犯、治安顧慮人口、失蹤人口以及通緝犯資料庫之資料作為建檔基礎。其中, 除國民身分證相片資料庫為內政部戶政司所有外, 其餘 4 個資料庫均為警政署固有的資料庫。正因國民身分證相片資料庫非

²² 張凱淳 (2012), 〈人臉辨識技術應用於警政治安之探討研究〉, 《前瞻科技與管理》, 2 卷 1 期, 頁 82。

²³ 賴昭嘉, 前揭註 16, 頁 23。

²⁴ 台灣人權促進會, <https://www.tahr.org.tw/news/2288> (最後瀏覽日: 04/03/2020)。

²⁵ 曾婉菁, 前揭註 15, 頁 23。

屬警政署固有之資料庫，M-Police 人臉辨識系統整合此資料庫極具爭議性，此機關間資料共享之情形，涉及諸多法律爭議，包括警職法與個資法間的適用關係、個資法上目的拘束原則的原則及例外的適用等。有關警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫之爭議，本文將於本文第五章中詳細說明。

第二節 警政署 M-Police 人臉辨識系統介紹

前一節中，首先介紹何謂人臉辨識技術，簡言之，人臉辨識系統係生物識別技術的一種，由人臉偵測、系統演算法以及人臉資料庫所構成。藉由人臉偵測技術偵測到人臉後，系統演算法便會擷取人臉特徵資訊並與人臉資料庫中的資料進行比對來識別身分。而警政署對於人臉辨識系統的使用其實並不陌生，早於 M-Police 人臉辨識系統之前，警政署已於內部建置警政相片比對系統，該系統使用道路監視器的影像，進行人臉辨識的工作。以往欲使用該系統比對身分，僅能於機關內的專用電腦且由專責人員負責，又因技術並不純熟，加上影像品質不佳等因素影響，比對工作往往十分耗時。現今，由於科技進步，雲端技術的發達，警政署便著手開發 M-Police 警用行動載具並內建人臉辨識的功能加上其背後龐大的資料庫，使在外執勤的員警，只要手持 M-Police 便可使用人臉辨識系統查詢民眾身分，加上影像技術的提升及技術的進步，辨識工作不到 30 秒便可以完成，且準確率高。再者，M-Police 的外觀與一般智慧型手機無異，機型輕巧、便於攜帶，正由於 M-Police 便於攜帶的優點，加上影像技術的提升，能有效查證民眾身分，且使用者眾多，人臉辨識系統的使用因此於警察機關漸漸普及。本節將介紹警政署 M-Police 警用行動載具，並藉由警政署針對人臉辨識系統疑慮說明資料以及筆者的訪談，說明 M-Police 人臉辨識系統申請主體要件與使用程序、使用情狀、目的以及該系統的運作方式等，以利後續的法制探討。



圖 1、M-Police 新舊版示意圖，資料來源：Ithome，<https://www.ithome.com.tw/article/117303>（最後瀏覽日：06/15/2020）。

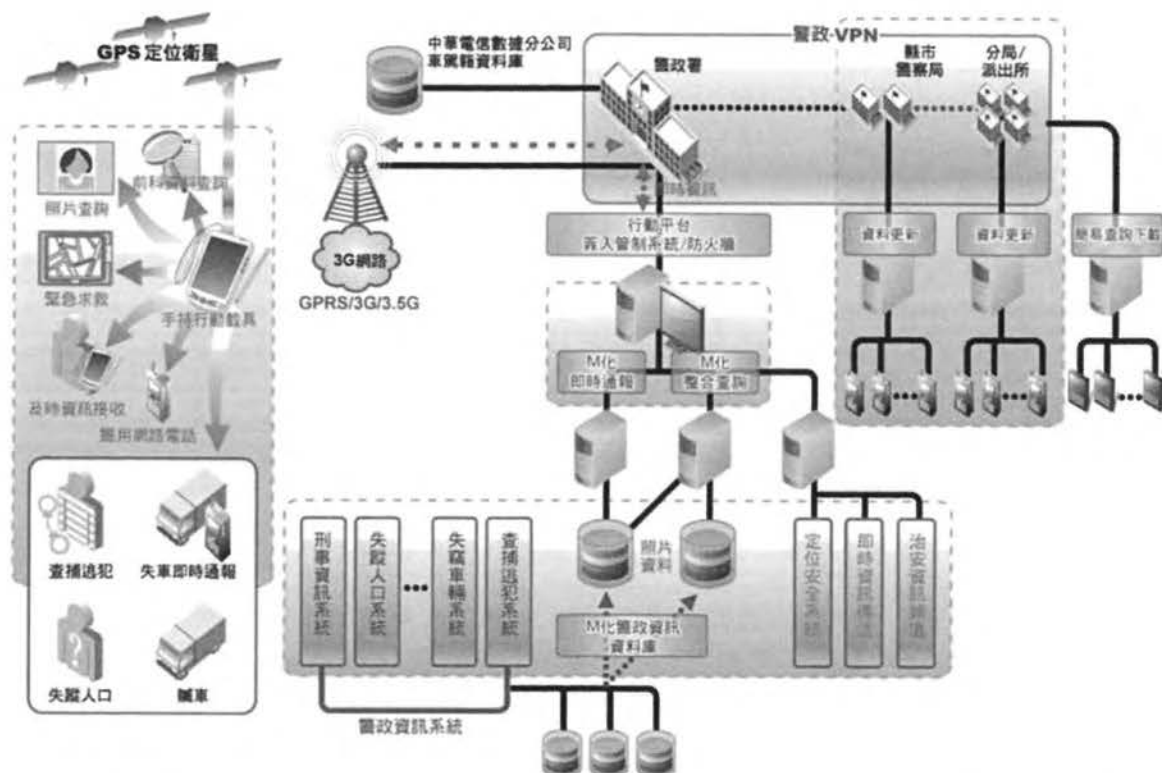


圖 2、M-Police 設計架構圖，資料來源：內政部警政署（2012），〈內政部警政署「M-Police 行動警察建置案簡介」〉，《政府機關資訊通報》，第 291 期，頁 2。

第一項 M-Police 警用行動載具說明

警察所使用的人臉辨識系統係建置於 M-Police 的功能之一，正式名稱為即時相片比對功能。簡言之，該系統係藉由所拍下的民眾臉部特寫照片，與資料庫中

的照片進行比對，進而確認民眾身分。以下將先介紹 M-Police 的開發過程及其主要功能。



第一款 M-Police 的開發

「M-Police 行動警察建置案」係行政院愛臺十二建設「智慧臺灣 (i-Taiwan)」子計畫之一，自 2007 年至 2011 年為期 5 年執行，為擴展警政資訊行動化之應用，建構 M-Police 平臺及開發新型載具。至今，M-Police 整合了全國至少 9 個機關超過 30 個資料庫（例如：刑案系統、通訊監察系統、車籍資料、戶政資料、手機通聯資料以及 CCTC 等²⁶），供基層員警在執勤查詢各式資料使用²⁷，藉由結合後端資料庫提供第一線執勤員警更多資訊，M-Police 可提供查詢之項目（會因網路連線狀態略有不同），於具連線狀態下有「查捕逃犯、失蹤人口、應受尿液採驗人、遺失身分證、逃逸外勞、中輟學生、治安顧慮人口、失竊汽機車、戶籍、車、駕籍、統號變更、典當紀錄、前科、國人相片、治安顧慮人口相片、大陸人士行方不明相片、逃逸外勞相片、脫離兒少、緊急求救、治安資訊頻道、刑案紀錄、失蹤人口影像」，而「全國廣播即時訊息及人車協尋」具備向全國 M-Police 使用者發布即時性訊息之功能，如全國性重要治安、交通資訊獲通報涉案人、車之資訊，以集合全國警察力量投入犯罪查緝工作，有效提升治安維護效能²⁸。而現在的 M-Police 具有八大功能（即時相片比對、家戶訪查系統、即時車牌辨識、警察 SOP、警察法規查詢、雲端勤務派遣系統、現場影音傳送系統、以及 M-Police 整合查詢）²⁹，其中本文所稱的人臉辨識系統便是八大功能之一的即時相片比對功能。

²⁶ 海岸巡防署（2018），《海巡雙月刊》，頁 38，臺北：海洋委員會海巡署。

²⁷ 王正嘉（2019），〈AI 與人臉辨識技術運用於犯罪偵防之問題分析〉，溫祖德（等著），《刑事政策與犯罪研究論文集（22）》，頁 243，臺北：法務部司法官學院。

²⁸ 臺中市政府警察局清水分局，

https://www.police.taichung.gov.tw/qingshui/home.jsp?id=61&parentpath=0,5&mcustomize=faq_view.jsp&dataserno=201712050094&t=FAQ&msermo=201712050010（最後瀏覽日：04/04/2020）。

²⁹ Yahoo 新聞，

<https://tw.news.yahoo.com/%E8%AD%A6%E6%94%BF%E8%88%87%E6%99%82%E4%BF%B1%E9%80%B2-m-police%E5%8D%94%E5%8A%A9%E6%89%93%E9%80%A0%E7%A7%91%E6%8A%80%E6%88%B0%E8%AD%A6-185902832.html>（最後瀏覽日：05/26/2020）。

行動服務-M-Police



圖 3、現今 M-Police 的功能示意圖，資料來源：內政部警政署（2018），〈內政部警政署「前瞻警政、科技警察」智慧聯網專案〉，《政府機關資訊通報》，第 352 期，頁 4。



圖 4、警政巨量資料平臺機關整合示意圖，資料來源：內政部警政署（2018），〈內政部警政署「前瞻警政、科技警察」智慧聯網專案〉，《政府機關資訊通報》，第 352 期，頁 3。



第二款 M-Police 建置人臉辨識系統

M-Police 的人臉辨識系統為內政部警政署於「警政雲端運算發展計畫」期間所建置。「警政雲端運算發展計畫³⁰」係行政院於 2011 年 12 月 27 日核定，期程自 2012 年至 2015 年為期 4 年，依該計畫並於 2013 年建置自動人臉偵測暨比對系統³¹，也就是「即時相片比對」功能，發展使用 M-Police 進行即時相片擷取及查詢的程式，即「即時相片比對系統」，也就是本文所稱的人臉辨識系統。藉由將相片畫面上傳，與「國民身分證相片資料庫」中的相片進行人臉特徵值比對，由於當初該系統於建置人臉資料庫時，整合內政部戶政司國民身分證相片資料³²，因此可以介接內政部戶政司所儲存國民身分證相片資料的個人照片，作為身分辨識的依據³³，並可彈性設定依年齡、戶籍地、身分類型（失蹤人口、通緝犯、治安顧慮人口及中輟生等）條件進行逐案查詢，縮小過濾清查範圍，有效縮短查證民眾身分之時間。為擴大應用警政署所建置之警政相片比對系統，員警持 M-Police 執勤時，遇到可疑嫌犯或是昏迷、失智民眾，可啟動相片比對系統，並使用載具拍下民眾相片，立即與國民身分證相片資料庫進行比對，系統可於 30 秒內完成身分辨識的任務，並將資料庫中將該民眾之基本資料傳給員警，以提高執勤的效率及為民服務之品質³⁴。

³⁰ 依據該計畫，內政部警政署著手打造警政雲，將雲端技術適度與警政工作整合，依據勤業務需求規劃多項雲端運用。包括：建置雲端運算資訊基礎與平臺，為提升雲端基礎與平台服務的穩定度及可用性，透過虛擬化技術將 CPU、記憶體、儲存空間等硬體資源加以分割利用，規劃出各種等級之虛擬化資源，建置雲端運算基礎環境，提供警政系統所需之龐大運算與儲存資源，以及安全的管理機制。同時亦可依據各系統之服務需求量的變化進行動態調整與擴充，確保警政雲上各警政資訊服務之穩定度與效能。且虛擬化環境可提供伺服器負載平衡，自動根據後端虛擬化主機的狀態，適時調整負載平衡，隨時維持快速反應，並減少管理營運的複雜度。透過自動化控管與維運，讓警政資訊系統的服務品質大幅提升，以提供員警最佳的服務，同時可以有效提升警政資訊中心內伺服器的運作效能，降低系統維運成本。有效運用雲端運算技術解決 M-Police 系統運算及查詢負荷超載問題。內政部警政署資訊室（2014），《政府機關資訊通報》，第 317 期，頁 2&4，臺北：內政部警政署。

³¹ 內政部警政署（2013），《警政工作年報》，頁 1-434，臺北：內政部警政署。

³² 王正嘉，前揭註 27，頁 243。

³³ ihome，<https://www.ihome.com.tw/article/117303>（最後瀏覽日：04/04/2020）。

³⁴ 內政部警政署資訊室，前揭註 30，頁 1-7。

而如前述，由於 M-Police 整合超過 30 個資料庫的資料，因此得作為人臉資料庫建檔基礎者，除國民身分證相片資料外，亦包括前科犯、通緝犯、失蹤人口資料庫之資料等。而警察於比對身分時，實際上可針對現場情形及需求選取身分比對的資料庫類別（例如：國民身分證、前科犯、治安顧慮人口、失蹤人口以及通緝犯），但由於本文係探討警察執行危害防止勤務時使用 M-Police 人臉辨識系統查證身分的合法性，而基於危害防止的目的以及臨檢查證身分之客體多為一般民眾的考量下，為有效確認民眾身分，警察或多選擇以國民身分證資料庫作為身分的比對來源。而該系統使用內政部戶政司國民身分證相片資料庫之資料作為人臉資料庫的建檔基礎亦是爭議所在。本文除探討警察使用人臉辨識系統查證身分之合法性外，亦將探討警政署使用內政部戶政司國民身分證相片資料作為人臉資料庫建檔基礎之爭議。

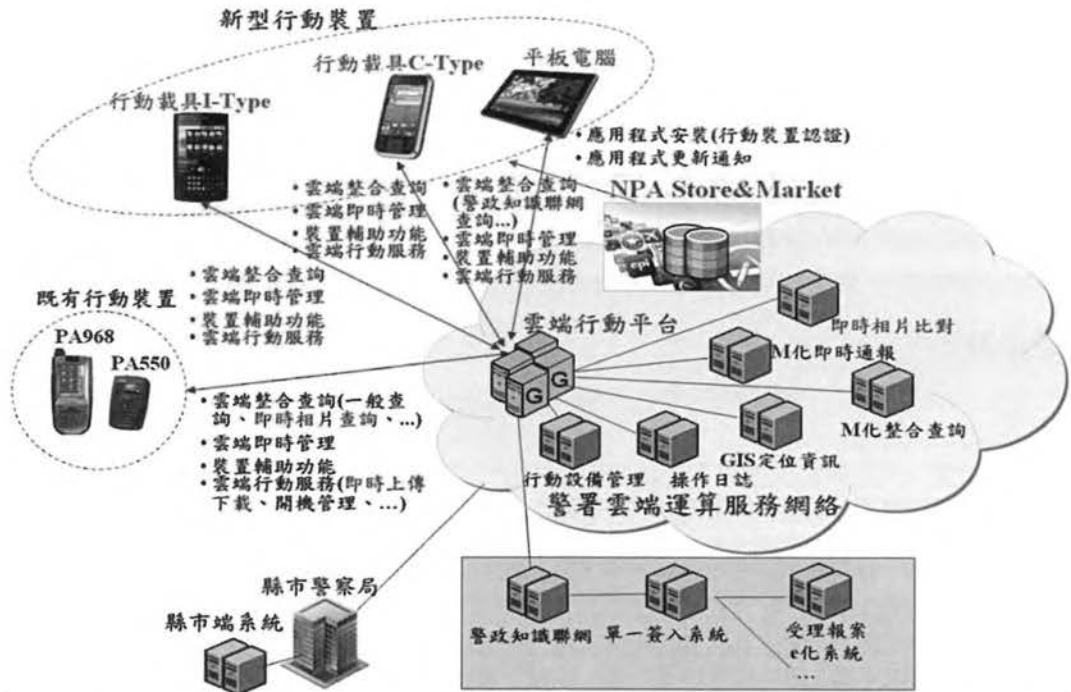


圖 5、警政雲運作架構，資料來源：內政部警政署資訊室（2014），《政府機關資訊通報》，第 317 期，頁 2，臺北：內政部警政署。



圖 6、M-Police 與警政雲端系統整合示意圖，資料來源：內政部警政署（2018），〈內政部警政署「前瞻警政、科技警察」智慧聯網專案〉，《政府機關資訊通報》，第 352 期，頁 2。

第二項 系統運作

於前段中，本文介紹 M-Police 的基本架構及其內建的人臉辨識系統，以下將詳細介紹該系統的操作及其於實務上的使用情形，包含何時會使用該系統以及誰可申請使用此一系統。

第一款 系統操作

欲使用 M-Police 人臉辨識系統查證民眾之身分，使用者首先須使用專屬之帳號密碼登入系統。登入成功後，選取即時相片比對功能，並拍攝受檢人的臉部照片，拍攝完成後，將該臉部照片上傳。上傳後於進行比對前，操作者可設定條件並縮小比對來源，提高比對的準確率，並可選擇比對之資料庫類別（例如：國民身分證、前科犯、治安顧慮人口、失蹤人口以及通緝犯資料庫等），及設定年齡範圍、性別、亦可選擇候選人名額。設定完成後，系統會將所拍攝之圖片，與操作

者所選定的資料庫中的相片進行比對，比對的動作會於警政雲端系統中快速進行，若出現比對吻合之結果，系統會自動將此人之姓名、身分證統一編號、生日及戶籍地址等個資提供給操作者，由操作者進行後續之判斷及確認³⁵。



第二款 使用情狀

針對警察何時會使用 M-Police 人臉辨識系統確認民眾身分此一問題，根據內政部警政署針對人臉辨識系統疑慮說明資料第 4 點，在警察勤務中使用 M-Police 人臉辨識系統常見的情形有：遇個案執行為民服務（如協助迷途老人返家）、查證民眾身分及協助犯罪偵查等法定職務³⁶。由於本文的研究範圍限於探討 M-Police 人臉辨識系統於危害防止任務方面應用的合法性，其中協助迷途老人返家及查證身分便屬於危害防止任務的範疇，屬於本文的研究範圍。細觀之，所稱協助迷途老人返家及查證身分，係指警察執行警職法第 6 條身分查證之勤務而言。警職法第 6 條第 1 項規定：「警察於公共場所或合法進入之場所，得對於下列各款之人查證其身分：一、合理懷疑其有犯罪之嫌疑或有犯罪之虞者。二、有事實足認其對已發生之犯罪或即將發生之犯罪知情者。三、有事實足認為防止其本人或他人生命、身體之具體危害，有查證其身分之必要者。四、滯留於有事實足認有陰謀、預備、著手實施重大犯罪或有人犯藏匿之處所者。五、滯留於應有停（居）留許可之處所，而無停（居）留許可者。六、行經指定公共場所、路段及管制站者。」據此，警察查證身分亦包括協助迷途老人返家的情形，不限於合理懷疑有犯罪之嫌疑或有犯罪之虞之人，故協助迷途老人返家及查證民眾身分兩種情形實則得以「執行警職法第 6 條查證民眾身分之勤務」代替。而根據筆者訪談，執行警職法第 6 條查證民眾身分之勤務為實務上最常使用該系統的情形，尤其是協助迷途老人返家，新聞報導中亦經常出現有關 M-Police 人臉辨識系統協助迷途老人成功返

³⁵ 關於 M-Police 人臉辨識系統的操作，可參照 Youtube 之影片，<https://www.youtube.com/watch?v=B9t23Ck8UPI>（最後瀏覽日：12/02/2020）。

³⁶ 內政部警政署針對人臉辨識系統疑慮說明資料，載於：<http://www.moex.com.tw/pdf/m-police%20topic.pdf>（最後瀏覽日：05/25/2020）。

家之實例。正由於此系統常見於查證身分時使用，本文便著重於此探討警察使用 M-Police 人臉辨識系統查證民眾身分的合法性。



依據警政署針對人臉辨識系統疑慮說明資料第四點，實務上，警察於執行臨檢勤務需查證民眾身分時，並不會於第一時間使用人臉辨識系統查證民眾身分，反之，仍會先循傳統臨檢程序，詢問受檢人之身分及令其出示身分證明文件，由其證明自己的身分，若受檢人無法證明自己之身分，或是所出示之身分證件經警察懷疑並非其本人時，於取得受檢人同意的前提下，便會使用該系統拍下受檢人臉部照片與資料庫（於本文中，專指國民身分證相片資料庫）中的照片進行身分識別，以此查證民眾身分。而警察欲使用該系統查證民眾身分，前提須符合警職法第 6 條有關查證身分之要件實屬當然。惟於執行臨檢勤務而欲使用該系統查詢民眾身分時，由於涉及新興科技的使用，與傳統臨檢相較，不但侵害基本權程度有別，程序上亦不盡相同。過往警察執行臨檢勤務而須查證民眾身分時，須一一詢問民眾身分資訊，並要求民眾出示身分證件以供核對及證明身分，同時還須提防民眾假冒他人身分的情形；一旦於臨檢時使用人臉辨識系統查證民眾身分，前階段的程序雖不變，仍須先要求民眾出示身分證件證明身分，但當民眾無法或提供的身分證件警察合理懷疑非本人時，自此時點後，程序便與過往有所不同，警察會詢問民眾是否同意使用人臉辨識系統查證身分，得到同意後，便會使用該系統查證身分，反之，倘受檢人不同意，警察便不會使用此一系統，但會回到傳統模式，將其帶往勤務處所續行查證行為（警職法第 7 條第 2 項）。警察使用人臉辨識系統查證民眾身分與傳統臨檢行為除程序上有所不同外，使用人臉辨識系統識別身分，警察便無須向人民詢問任何有關身分資訊，只要警察拍下民眾臉部拍攝相片，待比對成功後，便可直接取得身分資料（包括：姓名、性別、身分證統一編號等），人民無法隱瞞任何身分資訊亦無法拒絕提供，但同時人臉辨識系統的使用亦減少民眾假冒身分的可能。

綜上，依現行警察使用人臉辨識系統查證身分的程序，人臉辨識系統一定程度改變臨檢程序，加上整合了內政部戶政司國民身分證相片資料庫，又使用了人臉特徵資料此一敏感個資進行身分辨識，對於基本權之侵害與傳統身分查證行為相較，程度輕重有別。除此之外，此系統的使用係以取得受檢人同意為前提，亦產生若干疑問。當事人同意的內涵為何？是否係避免被帶往勤務處所而出於不得已之同意？若是在取得受檢人同意的情形下始使用此一系統查證身分，此一系統的使用是否還須有明確的法律依據？換言之，倘當事人同意警察使用此一系統查證身分，是否仍有「侵害」基本權之情事，而須符合憲法第 23 條限制基本權之要件？關於此一爭議，將於後一章節中說明。

第三款 M-Police 申請主體要件

由於 M-Police 人臉辨識系統整合眾多資料庫，牽涉多筆個資，為避免個資外洩，以及方便內部監督，並非所有警察均有權使用 M-Police。根據內政部警政署針對人臉辨識系統疑慮說明資料第四點，M-Police 即時相片比對系統之使用，員警須有本系統使用權限。而承前段，由於 M-Police 多係於臨檢時使用，因此有權使用該系統之人，據筆者的訪談，係實際在外執行勤務且具有警職人員（包含派出所，刑事警察人員）始有權提出申請以使用 M-Police。所稱在外執行勤務且具有警職的人員係指組織意義警察機關³⁷中，依法得行使警察職權之人員，主要指的是經警察特考及格任用，具有警察官身分之警察人員³⁸，且從事外勤³⁹者而言。簡

³⁷ 組織意義警察機關係相對於功能意義警察機關而言，組織意義的警察機關，係指依警察組織法令分別設置之警察機關，包括中央內政部所屬警政署（及其所直隸機關）、中央警察大學，以及地方直轄市、各縣市警察局及其分局等。功能意義的警察機關，則不以警察組織法令所設之機關為限，而係以機關之職能具警察功能為認定標準，例如釋字第 588 號解釋中，將法務部所屬行政執行處列為警察機關：「憲法第 8 條第 1 項所稱『非經司法或警察機關依法定程序，不得逮捕、拘禁』之『警察機關』，並非僅指組織法上之形式『警察』之意，凡法律規定，以維持社會秩序或增進公共利益為目的，賦予其機關或人員得使用干預、取締之手段者均屬之，是以行政執行法第 19 條第 1 項關於拘提、管收交由行政執行處派執行員執行之規定，核與憲法前開規定之意旨尚無違背。」李震山（2006），〈警察法：第一講警察作用法通論〉，《月旦法學教室》，第 41 期，頁 74-75。

³⁸ 李震山，前揭註 37，頁 74-75。

³⁹ 有關警政內部組織編制，詳參內政部警政署之網站介紹

<https://www.npa.gov.tw/NPAGip/wSite/ct?xItem=68012&ctNode=12575>（最後瀏覽日：10/27/2020）。

言之，以所從事的勤務決定員警是否有使用 M-Police 的權限。而有使用需求的員警，需向所屬單位的資訊室（科）申請專責的帳號密碼，經受理申請後，該科室的所屬人員除審核是否核准申請給予專責帳密外，尚會根據申請人的勤務需求，調整該組帳密的使用權限，意即可能並非每組帳密均有使用人臉辨識系統的權限，而經申請核准取得專責帳號及密碼後，嗣後始可於執行法定職務（勤務中）時，登入 M-Police 介面，輸入帳號密碼，倘該組帳密有使用人臉辨識系統的權限，始得使用人臉辨識系統查證民眾身分，使用時，警政署的資訊室資料庫，會記下每筆該警員查詢的檔案，稱之為 log 檔。一旦員警有私下非法使用，警政署就可透過該警員的帳號，回溯追查其究竟查過哪些人的資料⁴⁰。

而內政部警政署針對人臉辨識系統疑慮說明資料第五點，『M-Police「即時相片比對」使用權限，比照本署「警政相片比對系統」之授權程序，派出所層級使用權限亦須依規定程序申請核准，以杜絕員警恣意性查詢他人相片之情形發生。』此係指 M-Police 人臉辨識系統其內部的使用權限申請流程將比照舊有「警政相片比對」系統，進行統一規定，避免濫用之情事。而之所以內部的使用權限申請流程將比照舊有「警政相片比對」系統，係因此二系統具一定程度的相似性，均是藉由臉部相片來確認身分。而警政相片比對系統的建置較 M-Police 人臉辨識系統為早，且只能於警政機關的桌上型電腦上使用，使用該系統時，員警須將待比對樣本相片進行裁剪、比例調整等基本影像處理前置作業後，即可登入將待比對影像上傳系統。影像如符合比對最低基本需求，即可自動啟動人臉偵測功能取出人臉區塊，並擷取人臉區塊之特徵值，與人臉資料庫特徵值進行相似度比對排序，最後再輸出結果。該系統提供「1：N 比對」及「1：1 比對」兩種功能，各警察機關專責查詢人員可點選「1：N 比對」功能，設定比對資料庫、性別、年齡區間及候選者結果數（至多 200 名）等條件，即可依序輸出與待比對樣本相片特徵值相

⁴⁰ 自由時報，<https://news.ltn.com.tw/news/society/paper/1091656>（最後瀏覽日：05/26/2020）。

似的人臉（至多 200 名），協助員警縮小偵查範圍，加速破案。另點選「1:1 比對」功能，並輸入身分證號，即可驗證待比對樣本相片身分，系統會依據計算出的相片相似度，協助承辦人員判斷兩者是否為同一人。而該系統所使用的影像來源，主要為比對由金融機構提款機、便利商店、村（鄰）里、交通要道及各地政府所建置的監視錄影器所拍攝到的影像畫面，然而由於攝影機品質、鏡頭角度之差異，或拍攝地點光源限制等因素，大部分的原始影像均無法達到最佳比對的基本需求，在運用上有所限制⁴¹。

此二系統均是利用臉部相片進而確認身分，但警政相片比對系統所使用的影像來源較多，包括監視錄影器及金融機構的提款機，但該系統於使用上較不方便須先對影像進行處理使其清晰化到一定程度始可進行比對，且比對的效率遠不及 M-Police 人臉辨識系統。相較之下，M-Police 人臉辨識系統所使用的影像來源係員警直接對民眾臉部所拍攝的照片，由於現今影像技術的提昇，可直接使用該照片與人臉資料庫進行比對，且並無樣本數的限制，減少確認身分所需的時間。M-Police 人臉辨識系統與警政相片比對系統有一定程度的相似性，但前者卻比後者，於效能上要提昇許多，且該系統與智慧型手機結合，有利於該系統的普及。本文認為，正因兩系統間有一定程度的相似性，M-Police 人臉辨識系統的使用權限，係比照「警政相片比對系統」之授權程序辦理。

⁴¹ 張凱淳，前揭註 22，頁 87-88。

行檢測⁴⁴。



圖 8、多重比對臉部檢測法示意圖，資料來源：NEC 官網，
https://tw.nec.com/zh_TW/solutions/security/neofacetec.html? (最後瀏覽日：06/11/2020)。

(二) 攝動空間法 (Perturbation Space Method)

此檢測法係為應對隨時變更的環境條件，而事先登錄各種預測角度，因此該檢測法不易受到臉部角度變化及光線明暗變化而影響比對精確度⁴⁵。

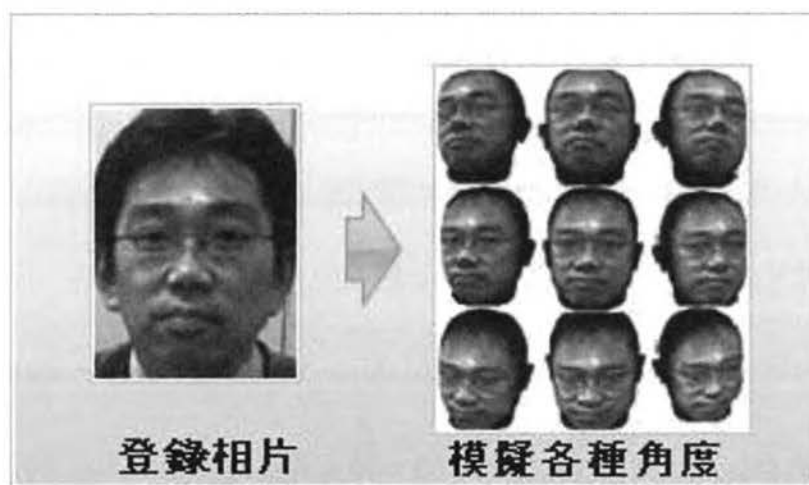


圖 9、攝動空間法示意圖，資料來源：NEC 官網，

⁴⁴ NEC 官網，https://tw.nec.com/zh_TW/solutions/security/neofacetec.html? (最後瀏覽日：04/04/2020)。

⁴⁵ NEC 官網，https://tw.nec.com/zh_TW/solutions/security/neofacetec.html? (最後瀏覽日：04/04/2020)。

https://tw.nec.com/zh_TW/solutions/security/neofacetec.html? (最後瀏覽日：06/11/2020)。



(三) 適應領域混合比對法 (Adaptive Regional Blend Matching)

此比對法是將照片切割成好幾個小方塊，由小方塊之間進行特徵比對，主要比對重點放在相似度較高的區塊，因此遮蓋住的部分臉部也可順利進行比對，減少因改變服裝、表情及環境變化帶來的影響⁴⁶。



圖 10、適應領域混合比對法，資料來源：https://tw.nec.com/zh_TW/solutions/security/neofacetec.html? (最後瀏覽日：06/11/2020)。

第三節 英國南威爾斯警局使用人臉辨識系統的情形

除我國將人臉辨識系統應用於警察勤務上外，其他國家亦有將人臉辨識系統應用於警察勤務之實例，英國南威爾斯警局便是其中之一，且其將人臉辨識系統應用於警察勤務上之行為已於 2019 年 4 月 9 日於 *Bridges v. CCSWP and SSHD* 一案中，經英國高等法院王座分庭 (High Court of Justice Queen's Bench Division) 判決以南威爾斯警局使用人臉辨識系統 (該人臉辨識系統名稱為 AFR Locate) 的行

⁴⁶ NEC 官網，https://tw.nec.com/zh_TW/solutions/security/neofacetec.html? (最後瀏覽日：04/04/2020)。

為既符合歐洲人權法案有關限制隱私權的要件規定，亦符合個人資料保護的相關規範，且英國現行法律制度已足支撐非恣意使用人臉辨識系統的情形為由，認定英國南威爾斯警局使用人臉辨識系統執法的行為合法無虞⁴⁷。



針對人臉辨識系統於協助警察勤務上的使用情形，英國南威爾斯警局與我國有極大的差異，二者間的使用差異與本文後續的法制探討息息相關。英國南威爾斯警局所使用的人臉辨識系統亦係由 NEC 公司所開發並將該系統應用於兩方面，一為將不明嫌犯及有前科的利害關係人與該警局所建置的通緝犯資料庫進行身分的比對，此稱為 AFR Identity⁴⁸，就此一應用本文不加以著墨，因與本文的主題不相關；另一就是用於犯罪偵查與預防，在某一定點對於路過的民眾進行大規模自動化的人臉偵測與辨識，一次性辨識出多數人之身分，目的為緝捕通緝犯或預防犯罪、維護社會秩序，此一應用稱為 AFR Locate，亦是與本文最為相似之應用，以下將介紹英國南威爾斯警局使用 AFR Locate 的情形。

英國南威爾斯警局自 2017 年 7 月開始首次於親王國球場啟用 AFR Locate，而當時該場地正舉辦歐洲冠軍聯賽的總決賽。AFR Locate 結合監視錄影機 (surveillance camera)，包括固定式閉路監視錄影機 (closed-circuit television cameras，以下簡稱 CCTV)、在警車上裝設或由警察人員隨身攜帶之的行動式錄影機，以取得各種場所進出的每一個人的即時影像。接著，透過 AFR 技術，將監視錄影機所蒐集的臉部影像 (Face Image) 與目標人物資料庫 (Image Database) 進行比對，而此所指的目標人物資料庫係以通緝犯資料庫為建檔基礎，當系統判斷

⁴⁷ 原文「We are satisfied both that the current legal regime is adequate to ensure the appropriate and non-arbitrary use of AFR Locate, and that SWP's use to date of AFR Locate has been consistent with the requirements of the Human Rights Act, and the data protection legislation.」R (Bridges) v CCSWP and SSHD [2019] EWHC 2341.

⁴⁸ 原文「SWP uses AFR in two ways. The first is known as AFR Identity under which images of unknown suspects and persons of interest related to past crimes or incidents, are compared against images in the SWP custody database.」R (Bridges) v CCSWP and SSHD [2019] EWHC 2341.

臉部特徵有吻合的比對結果時，還會再交由系統操作員進行作進一步的人工確認，確認結果的正確性。經操作員確認結果無虞後，將立即示警執法人員，讓執法人員判斷該人物是否為調查對象⁴⁹。易言之，執法人員會自行評估是否要有進一步的動作，也只有在確定為通緝犯的前提下才會有進一步的動作，針對執法人員的應對，南威爾斯警局開發了一套交通號誌系統（traffic light system），以顏色區別緊急程度及對應的應對措施。紅色代表需要立即回應；黃色則是代表需要進行逮捕行為；綠色則是僅是需要確認訊息即可⁵⁰。而英國市區使用監視錄影機的情況十分普遍，據統計 2016 年英國 CCTV 便高達 600 萬台，平均每一台蒐集 10 個民眾的資料，雖然部分監視錄影機的效用有限，但仍形成不可忽視的監視體系⁵¹。對於傳統監視錄影機之應用，英國大倫敦地區警察總局下設有 CCTV 中心，用以監控大倫敦地區的監視錄影系統，在該中心的監控室內警察人員緊盯著螢幕工作，其主要任務為監控恐怖份子、跟蹤車輛盜竊犯和交通違規者；同時，在監視錄影機裝設的周圍會設立警告標牌，讓民眾知悉附近有監視錄影機在進行監視⁵²。

根據英國內政部文件顯示，現階段 AFR 技術主要用於提升監視錄影系統的功能，其依賴監視錄影系統所取得的即時影像資料，以進行辨認作業⁵³。也就是說，AFR 技術的發展，讓監視錄影系統的功能不再是單純地記錄、保留影像的犯罪偵查工具（crime detection），而是可以即時且針對性地找出可疑人士，達到「預防犯

⁴⁹ 吳采薇（2019），〈英國警察機關使用自動化臉部辨識技術與相關監督機制之研究〉，《科技法律透析》，31 卷 2 期，頁 29。

⁵⁰ 原文「SWP has developed a traffic light system with colours (red, amber and green) to delineate the urgency and type of intervention required. Red indicates the need for an immediate response because e.g. of a counter-terrorist threat, amber indicates the need for an arrest intervention, and green indicates the need for an identification for intelligence development purposes only.」R (Bridges) v CCSWP and SSHD [2019] EWHC 2341.

⁵¹ Mail Online，

<https://www.dailymail.co.uk/news/article-3872818/One-CCTV-camera-10-people-Report-says-six-million-UK-useless.html>（最後瀏覽日：06/20/2020）。

⁵² 新竹市警察局（2009），〈赴英國考察警察制度、治安、交通及預防犯罪報告書〉，頁 16，載於：http://www.hccg.gov.tw/uploaddown/doc?file=abroad_report/53.pdf&filedisplay=53.pdf&flag=doc

⁵³ UK Home Office，Biometrics Strategy，頁 11-12，載於：

<https://www.gov.uk/government/publications/home-office-biometrics-strategy>

罪」(crime prevention)的功能⁵⁴。其次，政府能監視的範圍除了 CCTV 的拍攝範圍，尚能透過行動式監視錄影機的應用，讓監視範圍更為擴大且不受區域限制。南威爾斯警方在大型活動辦理期間，例如足球賽、嘉年華會等，利用專用警車上設置的監視錄影機所拍攝的影像，與警方掌握的嫌疑犯、可疑人士名單（例如：紅色警戒名單（由涉犯重罪之人所組成）、紫色警戒名單（名單中每人至少都涉嫌於南威爾斯地區有過一次犯罪）等）進行即時比對，而英國警方用於建立人臉資料庫的建檔基礎，係使用機關自有的 Niche Record Management System 中的通緝犯照片，並根據使用人臉辨識設置場所的不同，以嫌犯是否會經過該處為判準，將該系統中的照片進行排列組合建立各種名單，例如前所述紅色警戒以及紫色警戒名單，人臉資料庫便是由各種名單所組成，資料庫中通常計有 400 至 800 人不等，但最多不會超過 2,000 人，並在極短時間內辨認出名單上的人物⁵⁵，將人臉辨識系統正式運用於警察執法。而當警方於特定場所設置人臉辨識系統後，會有一系列事前公開的告知行為，告知民眾此處將進行大規模自動化人臉偵測以及辨識，其告知行為包括：於設置人臉辨識系統前，利用臉書以及推特告知安裝的地點及安裝事實並邀請設置人員一同參與⁵⁶；於裝載 AFR 功能的警用汽車上以及於加裝 AFR 功能的監視錄影機方圓半徑約 100 哩處張貼 A2 大小的「公平處理聲明（Fair Processing Notices）」告示⁵⁷以及針對所有鄰近部署 AFR 區域的民眾以及告知將受 AFR 干預的民眾發放明信片大小的通知⁵⁸，但即便英國警方於事前有進行上述公開告知的行為，多數民眾仍然對於警方使用人臉辨識一事渾然不知。除此之外，值

⁵⁴ Michael Bromby, 'Computerised Facial Recognition Systems: The Surrounding Legal Problems', 頁 3, 載於: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1551840

⁵⁵ INSIDE, <https://www.inside.com.tw/article/10123-nec-face-recognition> (最後瀏覽日: 06/20/2020)。

⁵⁶ 原文「prior to each AFR deployment, utilizing Facebook and Twitter to advertise the deployment and its location and invite engagement with officers who are deploying the technology」R (Bridges) v CCSWP and SSHD [2019] EWHC 2341.

⁵⁷ 原文「displaying large A2-size Fair Processing Notice on the AFR-equipped police vehicles on site and at approximately a 100 metre radius of the AFR cameras」R (Bridges) v CCSWP and SSHD [2019] EWHC 2341.

⁵⁸ 原文「handing out of postcard-sized notices to members of the public in the vicinity of each AFR deployment and to every person that is spoken to as a result of an AFR intervention」R (Bridges) v CCSWP and SSHD [2019] EWHC 2341.

得一提的是，英國的人臉辨識系統，並非會全天候 24 小時開啟，為了進行資料的重整以及刪除，會關閉最長半天左右的時間。但現行 AFR 技術準確率不如預期，也使得民眾擔心可能會被系統誤認為罪犯。根據獨立報（Independent）的揭露，自 2017 年 6 月起，南威爾斯警方的 AFR 系統將 2,685 名民眾辨認為名單上的人物，其中僅有 234 人為成功辨認，系統準確率僅有 10%⁵⁹，準確率極低亦是該系統為人所詬病的其中原因之一。

第四節 小結

相對於英國南威爾斯警局將人臉辨識系統與監視錄影器結合，於某一定點針對不特定多數人進行大規模自動化人臉偵測與辨識，我國 M-Police 人臉辨識系統的使用，由於未與監視錄影器結合，無法如英國南威爾斯警局般進行大規模自動進行人臉偵測及辨識，僅在警察執行臨檢勤務時，若無法確認民眾身分，在取得民眾同意的前提下，才會使用 M-Police 人臉辨識系統查證民眾身分，且一次僅能比對一人，為一對一使用，於此種使用的情形下，當事人的同意更顯重要，係判斷此一應用是否具備合法性的決定因素之一。具體而言，我國 M-Police 人臉辨識系統的使用須由員警拍攝民眾臉部相片，並可彈性設定年齡、性別等要件，除縮小比對範圍，同時也提升系統的準確度。簡言之，我國人臉辨識系統的使用，須警察選定特定目標客體，拍攝臉部特寫照片，非如英國南威爾斯警局只要於某一地點啟用人臉辨識系統，系統便會直接針對不特定多數人進行自動的人臉偵測及辨識，因此就使用情形而言，我國警察現今對於人臉辨識系統的使用僅可作為一對一臨檢查證身分之手段，該系統還未與任何監視器結合，形成類似「天眼」的監視網絡。

⁵⁹ INDEPENDENT，

<https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html>（最後瀏覽日：06/20/2020）。

正因為我國警察人臉辨識系統的使用為此種一對一的模式，一次僅能針對特定一人進行身分識別，而非如英國南威爾斯警局般可一次性針對不特定多數人進行身分識別。在我國警察人臉辨識系統的使用係一對一的模式下，而警察於臨檢時如欲使用該系統查證民眾身分係以取得當事人同意為前提，該同意為判斷此一應用合法性的關鍵性因素，尤其是在分析人臉辨識系統作為臨檢查證身分之手段是否應有法律依據此一爭議時，當事人的同意為此一爭議的核心，而關於該爭議將於第四章中詳細說明。

就人臉資料庫的建檔基礎而言，英國南威爾斯警局所使用的人臉辨識系統其人臉資料庫係以機關自有的 Niche Record Management System 中的通緝犯照片作為建檔基礎且資料庫的容量至多 2,000 人；相較之下，我國警政署的人臉辨識系統其人臉資料庫卻是使用內政部戶政司國民身分證相片資料作為建檔基礎，換言之，使用他機關的資料庫作為建檔基礎，其資料量之龐大，幾乎涵蓋全國 2,300 萬民眾的個資，惟此舉有優點亦有缺點。資料量的龐大代表比對來源的豐富，配合事前條件的設定，有效提高人臉辨識的準確率；惟另一方面，由於人臉資料庫幾乎涵蓋全國 2,300 萬民眾的個資，因此亦衍生出相關爭議，包括是否有使用該資料庫的必要、個資法中對於此種機關間資料共享之規定是否完善等，有關警政署使用內政部戶政司國民身分證相片資料庫的相關爭議將於第五章中討論。本文茲以下表說明我國與英國南威爾斯警局使用人臉辨識系統的差異：

	我國	英國
使用目的	危害防止及逮捕通緝犯，但本文僅討論以危害防止為目的的使用。	犯罪預防及緝捕通緝犯
人臉辨識系統的使用情況	M-Police 警用行動載具內建人臉辨識功能，警察須選定目標客體，拍攝臉部特寫照，始可進行身分辨識。(靜態)	設置於某一定點，與各種監視錄影器結合，針對不特定多數人於同一時間，進行自動人臉偵測以及人臉辨識。(動態)
人臉辨識系統使用的事前程序	使用前會取得當事人同意。	事前會進行一系列公開告知行為。
使用期間	使用時間不連續亦不固定，且無關機進行資料重整時間。	使用時間連續，但會關閉一段時間進行資料重整。
人臉資料庫建檔基礎	失蹤人口資料庫、通緝犯資料庫、治安顧慮人口資料庫、前科犯資料庫、國民身分證相片資料庫。 (除國民身分證相片資料庫外，其餘均為警政署固有的資料庫)	機關自有 Niche Record Management System 中的通緝犯照片，並根據使用人臉辨識系統場所的不同，以嫌疑人是否會經過該處為判斷基準，建立各式名單。
人臉資料庫資料量	資料量龐大幾乎涵蓋全國 2,300 萬人民的個人資料	資料量較小，至多不超過 2,000 張比對照片
使用情形評估	一次僅能比對一人，須選定特定目標客體。整合國民身分證相片資料，有效提高警察臨檢查證身分的效率，作為臨檢查證身分的手段。資料量較龐大，且比對前可設定條件縮小比對來源，因此系統準確率較高。	一次性可比對多數人，系統會自動化針對不特定多數人進行人臉偵測及身分比對。人臉資料庫僅以通緝犯照片為比對來源，因此主要用於緝捕通緝犯，資料量小，系統準確率較低，須有中間人員進行結果之判別。

表 1、我國及英國南威爾斯警局使用人臉辨識系統的比較，資料來源：本文自製

第三章 警察使用人臉辨識系統查證身分對基本權之影響



於前一章中，本文介紹了警政署所開發的 M-Police 警用行動載具及其內建的人臉辨識系統，包含該系統於實務上的使用情形、申請主體要件及申請程序，亦比較我國與英國南威爾斯警局使用人臉辨識系統的情形，藉此舉突顯我國警察使用該系統的特殊之處。總而言之，人臉辨識系統本身除涉及人臉特徵資料此一新興個人資料的使用外，更由於我國警察將此一系統與臨檢結合，加上使用了內政部戶政司國民身分證相片資料作為人臉資料庫的建檔基礎，致使此事更添爭議。本章節將對警察使用人臉辨識系統查證身分對於基本權之影響進行說明，尤其是對於隱私權的影響。其中，針對警察臨檢以及公共場所的隱私權保障已有相關大法官解釋在案（釋字第 535 號及釋字第 689 號解釋參照），本章將較為詳細說明該系統對於隱私權，尤其是資訊隱私權的衝擊。

由於隱私權並非我國憲法明文所列舉的基本權利之一，因此將首先對我國隱私權的發展以大法官釋字為中心，介紹該基本權的發展及內涵，並針對人臉辨識系統的使用對資訊隱私權之影響進行分析，為避免模糊焦點，本文不論述有關資訊隱私權、資訊自決權與資訊自主權的相關爭議。而該系統的使用如會限制基本權的保護，則須符合憲法第 23 條之規定：「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。」

第一節 警察臨檢對基本權之影響



由前一章的討論可知，依目前警察使用 M-Police 人臉辨識系統的情形，該系統係單純作為查證身分的手段，成為臨檢程序的一部分，以警職法為法律依據，與現行臨檢法制結合。本文所稱的查證身分係指警察依據警職法第 6 條及第 7 條之規定所執行者而言，以危害防止為目的，且依釋字第 535 號解釋對於臨檢之定義，該行為自屬警察臨檢的一環。目前警察所使用的人臉辨識系統尚無法針對不特定多數人進行大規模自動偵測人臉及識別，而該系統既與警察臨檢結合，實有必要說明臨檢對於基本權之限制，釐清大法官對於警察臨檢的態度，以及我國警察臨檢的法律框架，以利後續探討有關人臉辨識系統使用與現行警職法間的衝突。具體而言，針對警察臨檢對於基本權之影響已有釋字第 535 號解釋在案，該號解釋理由書中載道：「依警察勤務條例第 11 條第 3 款：『臨檢：於公共場所或指定處所、路段，由服勤人員擔任臨場檢查或路檢，執行取締、盤查及有關法令賦予之勤務』，臨檢自屬警察執行勤務方式之一種。惟臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，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。」本號解釋中提及臨檢將對人民的行動自由、財產權及隱私權等基本權影響甚鉅，但卻未說明理由，具體而言，臨檢將如何限制人民的基本權，由於本號解釋催生了警職法的立法，可由警職法的規定中窺知一二。

由釋字第 535 號解釋中可知，對於臨檢，該解釋使用警察勤務條例第 11 條第 3 款對於臨檢之定義⁶⁰，亦即定位於舉凡警察採取限制或干預人民的行動自由、財產權或隱私權的手段，如：檢查、路檢、取締或盤查等，不問名稱為何，均可稱之為臨檢，將臨檢採取較為廣義之解釋⁶¹，而身分查證行為，作為臨檢的必要行為，

⁶⁰ 警察勤務條例第 11 條第 3 款：「臨檢：於公共場所或指定處所、路段，由服勤人員擔任臨場檢查或路檢，執行取締、盤查及有關法令賦予之勤務」

⁶¹ 周燕輝，前揭註 12，頁 98。



亦將限制人民的行動自由、財產權或隱私權，自屬臨檢。具體而言，身分查證將如何影響人民的居住自由、行動自由以及隱私權等基本權，可由警職法之規定中窺知。依警職法第 6 條第 1 項之規定：「警察於公共場所或合法進入之場所，得對於下列各款之人查證其身分：一、合理懷疑其有犯罪之嫌疑或有犯罪之虞者。二、有事實足認其對已發生之犯罪或即將發生之犯罪知情者。三、有事實足認為防止其本人或他人生命、身體之具體危害，有查證其身分之必要者。四、滯留於有事實足認有陰謀、預備、著手實施重大犯罪或有人犯藏匿之處所者。五、滯留於應有停（居）留許可之處所，而無停（居）留許可者。六、行經指定公共場所、路段及管制站者。」再者，依同法第 7 條規定：「警察依前條規定，為查證人民身分，得採取下列之必要措施：一、攔停人、車、船及其他交通工具。二、詢問姓名、出生年月日、出生地、國籍、住居所及身分證統一編號等。三、令出示身分證明文件。四、若有明顯事實足認其有攜帶足以自殺、自傷或傷害他人生命或身體之物者，得檢查其身體及所攜帶之物。依前項第二款、第三款之方法顯然無法查證身分時，警察得將該人民帶往勤務處所查證；帶往時非遇抗拒不得使用強制力，且其時間自攔停起，不得逾三小時，並應即向該管警察勤務指揮中心報告及通知其指定之親友或律師。」

由上開規定可知，警察實施臨檢查證身分之行為，首先，將影響人民的居住自由，因依警職法第 6 條之規定，警察對於合法進入的場所可實施查證身分的行為，此所稱得合法進入的場所，以營業處所為典型。依憲法第 10 條之規定：「人民有居住及遷徙之自由。」而居住自由的意涵可參酌釋字第 443 號解釋理由書中所載：「憲法第 10 條規定人民有居住及遷徙之自由，係指人民有選擇其居住處所，營私人生活不受干預之自由，且有得依個人意願自由遷徙或旅居各地之權利。」居住自由以「住宅」之保護為核心，釋字第 460 號解釋理由書中亦言及：「依一般觀念，所謂住宅係指供人日常居住生活、作息之用，固定於土地上之建築物，外

觀上具備基本生活功能設施，屬於居住者支配管理之空間，具有高度私密性。」

惟居住自由之保護，雖以住宅為中心，但不限於住宅，尚應包括住宅及其附屬空間、工作房、營業處所及其四周圍定之土地。憲法保障之居住自由權，就其整體而言，是要保障空間上的私人領域（隱私），而營業處所固然為「居住」概念所涵蓋，但基於其向外公開的特性，且具有與外部社會接觸往來之目的，並對外產生影響，營業處所受憲法居住自由保護的密度實涉及從業人員、消費者或一般大眾之利益，無形中將營業處所從私人領域中釋放出來。故營業處所受居住自由保障之必要性，自然依其所欲追求之業務目的而有所減輕，不似個人生活居住處所（住宅）完全受到憲法居住自由權之保障⁶²。營業處所雖受居住自由的保護密度將因其場所性質，而與住居所有所不同，但無礙營業處所本身係受居住自由所保障。既營業處所受憲法居住自由所保障，警察進入該場所實施查證身分的行為，將限制人民居住自由的保護。

除此之外，警察實施臨檢查證身分之行為，由於涉及將人民留置於某處，更甚者，依警職法第 7 條第 2 項之規定，若是詢問姓名、出生年月或是出示身分證等方法均無法查明身分的前提下，警察得將該人民帶往勤務處所查證，且帶往時如遇抵抗可使用強制力，且其時間自攔停起，不得逾三小時，並應即向該管警察勤務指揮中心報告及通知其指定之親友或律師。據此，縱使時間不若刑事羈押長，但警察查證身分的行為，亦將影響人民的行動自由，限制身體的自主性。每個人的身體自主性不受非法的侵犯，該自主性主要有兩種表現型式：首先是身體行動之自由，分別規定在憲法第 8 條之人身自由及第 10 條之遷徙自由。其次是身體不受傷害權，分別規定在憲法增修條文第 10 條第 5、7、8、9、12 項之健康權，以及規定在憲法增修條文第 10 條第 6 項的人身安全。而警察臨檢所侵害屬前者，憲法第 8 條身體行動之自由。憲法第 8 條所謂「人民身體之自由」，即是身體行動之

⁶² 李震山（2006），〈警察法：第四講 警察作用與基本權利保障（二）〉，《月旦法學教室》，第 47 期，頁 58-59。



自由，簡稱為「人身自由」。人身自由的侵害，係指違反當事人意願或在其無法表達意願時，而將其在一定時間內留置於某一特定處所⁶³。

我國憲法第 8 條第 1 項規定：「人民身體之自由應予保障。除現行犯之逮捕由法律另定外，非經司法或警察機關依法定程序，不得逮捕拘禁。非由法院依法定程序，不得審問處罰。非依法定程序之逮捕、拘禁、審問、處罰，得拒絕之。」而本條拘禁的意義可參酌釋字第 392 號解釋理由書中所載：「所謂『逮捕』，係指以強制力將人之身體自由予以拘束之意；而『拘禁』則指拘束人身之自由使其難於脫離一定空間之謂，均屬剝奪人身自由態樣之一種。至於刑事訴訟法上所規定之『拘提』云者，乃於一定期間內拘束被告（犯罪嫌疑人）之自由，強制其到場之處分；而『羈押』則係以確保訴訟程序順利進行為目的之一種保全措置，即拘束被告（犯罪嫌疑人）身體自由之強制處分，並將之收押於一定之處所（看守所）。故就剝奪人身之自由言，拘提與逮捕無殊，羈押與拘禁無異；且拘提與羈押亦僅目的、方法、時間之久暫有所不同而已，其他所謂『拘留』、『收容』、『留置』、『管收』等亦無礙於其為『拘禁』之一種，當應就其實際剝奪人身（行動）自由之如何予以觀察，未可以辭害意。」據此，警察於執行臨檢而須查證受檢人之身分時，須將受檢人留置於某處直至查明其身分，而受檢人無法拒絕符合法定程序的臨檢，若拒不配合，警察可強制將其帶離到勤務處所續行查證身分的行為。故此處之留置，依釋字第 392 號解釋之意旨，涉及將人民拘束於某一空間使其難以脫離，亦符合拘禁之意義。再者，就主體而言，由於警察臨檢查證身分行為實施之對象並非刑事被告，但縱非刑事被告亦同受憲法第 8 條人身自由之保護，參釋字第 384 號解釋理由書的說明：「人民身體自由享有充分保障，乃行使其憲法上所保障其他自由權利之前提，為重要之基本人權。故憲法第八條對人民身體自由之保障，特詳加規定。該條第一項規定：「人民身體之自由應予保障。除現行犯之逮捕由法律

⁶³ 李震山（2006），〈警察法：第三講 警察作用與基本權利保障（一）〉，《月旦法學教室》，第 45 期，頁 77-78。

另定外，非經司法或警察機關依法定程序，不得逮捕拘禁。非由法院依法定程序，不得審問處罰。非依法定程序之逮捕、拘禁、審問、處罰，得拒絕之。」係指凡限制人民身體自由之處置，在一定程度內為憲法保留之範圍，不問是否屬於刑事被告身分，均受上開規定之保障。除現行犯之逮捕，由法律另定外，其他事項所定之程序，亦須以法律定之，且立法機關於制定法律時，其內容更須合於實質正當，並應符合憲法第二十三條所定之條件，此乃屬人身自由之制度性保障。」故警察實施查證人民身分之行為，將限制憲法第 8 條所保障的人身自由，而依憲法第 8 條之規定限制人身自由須依法定程序否則不得實施，而非刑事被告與刑事被告間於限制人身自由上所應遵行之法定程序並不相同，再者，雖均涉及限制人身自由，但將因該程序屬行政或司法程序，法律保留的規範密度亦不相同，此與基本權之限制有關之內容，將於限制基本權之討論中一同說明。

臨檢亦會限制隱私權的保護，依警職法之規定，警察在滿足警職法第 6 條第 1 項之要件下，可於合法進入之場所以及公共場合以訊問或是令出示身分證明文件的方式查證民眾身分。首先，警察為查證身分需取得與受檢人身分有關之資料包括：姓名、國民身分證統一編號及出生年月等足資證明個人身分的資料，而在臨檢符合法定程序之前提下，受檢人須加以配合，不得拒絕，亦即強制其提供與身分有關之資料。而此種與身分有關之資料，本文認為，由於可直接連接到個人，具有一定的「私密性」，通常不會隨意提供予任何人，屬於個人隱私，為資訊隱私權的保護客體，而警察執行臨檢勤務，強制要求提供該種個資，將限制隱私權之保護。再者，依釋字第 689 號解釋，縱於公共空間，倘有「合理」的隱私期待，仍可主張隱私權的保護，因此警察於公共空間查證身分，亦可能會限制隱私權的保障。



警察實施查證身分的行為，除會限制憲法所保障的居住自由及人身自由等基本權外，亦會限制隱私權之保護。而在人臉辨識系統導入警察查證身分之勤務後，針對隱私權之影響，尤其是資訊隱私權的影響更甚。鑒於本文係探討人臉辨識系統此一新興科技作為警察查證身分的手段之合法性，而人臉辨識系統最為人詬病者便是其對隱私權之侵害，因此本文特針對隱私權之部分詳加說明。

第二節 人臉辨識系統的使用對隱私權之影響

由前述，警察臨檢由於涉及於公共場所強制蒐集與個人身分有關的資料，此一行為本身便會限制人民隱私權之保障。依警職法第 7 條之規定，警察為確認身分，得向受檢人詢問與其身分有關之資料並令其出示相關身分證明文件，以證明所言為真。所稱與其身分有關之資料包括：姓名、國民身分證統一編號及出生年月等足資證明身分的資料，且在臨檢符合法定程序之前提下，受檢人須加以配合，不得拒絕提供。而此種與身分有關之資料，本文認為屬於資訊隱私權的保護客體，而警察執行臨檢勤務，為查證人民身分，強制要求提供該種個資，將限制人民資訊隱私權之保護。由於臨檢與隱私權保護間之衝突，已有釋字第 535 號解釋可供參照，本節將著重探討人臉辨識系統的使用對於資訊隱私權的衝擊。

第一項 我國隱私權之發展

隱私權的概念最初在 19 世紀末被提出，當時 Samuel D. Warren 與 Louis D. Brandeis 於 Harvard Law Review 上共同發表了「隱私權」(The Right to Privacy)一文，並將隱私權界定為一種個人得「掌控及經營私人生活」(right to life)及「不受他人侵擾」(right to be alone)之權利⁶⁴，嗣後隱私權在學界及實務上逐漸被確立其地位與內涵。而我國則是於司法院釋字第 293 號解釋中首次提及隱私權一詞，

⁶⁴ 林建中(1997)，〈隱私權概念初探－從美國法之觀點切入〉，《憲政時代》，23 卷 1 期，頁 64。

但直到釋字第 585 號解釋始於理由書中明確表示，隱私權雖非憲法明文列舉之基本權利，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料之自主控制，其應為憲法第 22 條所保障⁶⁵屬於概括基本權之一。以下將藉由與隱私權相關的大法官解釋，依時間先後條列式說明我國隱私權的發展。

（一）「隱私權」一詞提出：釋字第 293 號（1992 年 3 月 13 日）

我國司法院大法官於釋字第 293 號中，首次提及隱私權一詞，該解釋的爭點為議會得否要求銀行提供放款資料，大法官於解釋文中提到「銀行法第四十八條第二項規定「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密」，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。惟公營銀行之預算、決算依法應受議會之審議，議會因審議上之必要，就公營銀行依規定已屬逾期放款中，除收回無望或已報呆帳部分，仍依現行規定處理外，其餘部分，有相當理由足認其放款顯有不當者，經議會之決議，在銀行不透露個別客戶姓名及議會不公開有關資料之條件下，要求銀行提供該項資料時，為兼顧議會對公營銀行之監督，仍應予以提供。」此號解釋首度提及人民有隱私權的保障，但並未針對隱私權本身的內涵有詳細的說明。

（二）承認隱私權的基本權地位：釋字第 585 號（2004 年 12 月 15 日）

爾後於釋字第 585 號解釋，該號解釋的爭點為 319 槍擊事件真相調查特別委員會條例違憲與否，該號解釋除針對國會調查權做出闡釋外，亦針對隱私權的部

⁶⁵ 李誠偉（2015），《巨量資料產生的刑事爭議－以資訊隱私權為核心》，頁 10-11，私立東吳大學法律學系碩士論文。

分作出較釋字第 293 號解釋更為細部的說明，解釋理由書中載到：「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料之自主控制，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。」該號解釋以人性尊嚴為基礎，承認隱私權具有憲法基本權的地位，且其權利內涵為個人生活秘密空間免於他人侵擾以及個人資料的自主控制。

（三）資訊隱私權的概念：釋字第 603 號（2005 年 9 月 28 日）

針對釋字第 585 號，隱私權「個人資料自主控制」的權利面向，釋字第 603 號大法官做出更為細緻的說明，本號解釋係針對戶籍法第 8 條第 2、3 項強制捺指紋之規定是否違憲，於解釋文中提及資訊隱私權一詞，並對其內涵做出闡釋：「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，其中包含個人自主控制其個人資料之資訊隱私權，保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」除此之外，該號解釋更進一步說明政府應如何正當地限制人民的資訊隱私權，理由書中載道：「隱私權雖係基於維護人性尊嚴與尊重人格自由發展而形成，惟其限制並非當然侵犯人性尊嚴。憲法對個人資訊隱私權之保護亦非絕對，國家基於公益之必要，自得於不違反憲法第二十三條之範圍內，以法律明確規定強制取得所必要之個人資料。至該法律是否符合憲法第二十三條之規定，則應就國家蒐集、利用、揭露個人資料所能獲得之公益與對資訊隱私之主體所構成之侵害，通盤衡酌考量。並就所蒐集個人資料之性質是否涉及私密敏感事項、或雖非私密敏感但易與其他資料結合為詳細之個人檔案，於具體個案中，採取不同密度之審查。而為確保個人主體性及人格發展之完整，保障人民之資訊隱私權，國家就其正當取得之個人資料，亦應確保其合



於目的之正當使用及維護資訊安全，故國家蒐集資訊之目的，尤須明確以法律制定之。蓋惟有如此，方能使人民事先知悉其個人資料所以被蒐集之目的，及國家將如何使用所得資訊，並進而確認主管機關係以合乎法定蒐集目的之方式，正當使用人民之個人資料。」據此，資訊隱私權屬於隱私權保障範圍之一⁶⁶，有別於傳統隱私權著重於實體的個人生活及身體空間，資訊隱私權著重於個人資料的自主控制，因此該權利所保障之客體為個人資料，且依據該號解釋資訊隱私權的具體的權利內涵為個人對其資料得決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，且人民對於其個人資料的使用有知悉、控制以及更正之權利，不同於傳統隱私權追求不受他人侵擾而傾向消極被動。該號解釋更進一步指出，資訊隱私權的保障並非絕對，國家基於公益之必要，自得於不違反憲法第 23 條之範圍內，限制人民資訊隱私權的保障。至於該法律是否符合憲法第 23 條之規定，則應考量系爭資料的敏感程度、國家蒐集、利用、揭露個人資料所能獲得之公益與對資訊隱私之主體所構成之侵害等因素，通盤分析而定。除此之外，亦提及為確保個人主體性及人格發展之完整，保障人民之資訊隱私權，國家就其正當取得之個人資料，亦應確保其合於目的之正當使用及維護資訊安全，國家蒐集資訊之目的，尤須明確以法律制定之。而此處所指「合於正當目的使用」該「目的」應是指蒐集資料的目的，因此國家對於已取得的個人資料，應於合於蒐集資料的目的範圍內使用，以保護人民資訊隱私權。

（四）公共空間有條件承認隱私權的保障：釋字第 689 號（2011 年 7 月 29 日）

釋字 689 號解釋更進一步針對人民於公共空間的隱私權保障作出闡釋，本號解釋係判斷社會秩序維護法第 89 條第 2 款使新聞採訪者之跟追行為受到限制之規定是否違憲，解釋理由書中對於人民於公共空間的隱私權保障有詳細的說明，理

⁶⁶ 黃天偉(2017)·《銀行保密義務與稅捐調查之衝突與調和—從資訊隱私權之觀點省思—》，頁 27，國立清華大學科技法律研究所碩士論文。



由書中載到：「生活私密領域不受侵擾之自由及個人資料之自主權，屬憲法所保障之權利，迭經本院解釋在案。對個人前述自由權利之保護，並不因其身處公共場域，而失其必要性。在公共場域中，人人皆有受憲法保障之行動自由。惟在參與社會生活時，個人之行動自由，難免受他人行動自由之干擾，於合理範圍內，須相互容忍，乃屬當然。如行使行動自由，逾越合理範圍侵擾他人行動自由時，自得依法予以限制。在身體權或行動自由受到侵害之情形，該侵害行為固應受限制，即他人之私密領域及個人資料自主，在公共場域亦有可能受到干擾，而超出可容忍之範圍，該干擾行為亦有加以限制之必要。蓋個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響其人格之自由發展。尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通念認為合理者。系爭規定符合憲法課予國家對上開自由權利應予保護之要求。」本號解釋說明了公共場所是否受到隱私權保護的爭議。由本號解釋中可知，個人縱使在公共場域中，仍然可主張隱私權的保護，資訊隱私權亦同，但基於公共場所地域的特殊性，個人在公共場域中隱私權的保護以得合理期待於他人者為限。所稱合理期待係指其不受侵擾之期待已表現於外，且該期待須依社會通念認為合理者始可。

經由大法官多號解釋，確立隱私權的基本權地位，該權利屬於憲法第 22 條的概括基本權之一，受憲法所保障，且即便於公共場所亦得受該權利所保護。而在經過一系列有關隱私權的解釋後，對於該基本權的權利內涵，亦有一個較為具體

的輪廓。人臉辨識系統涉及人臉特徵資料此種具高度人別識別性個資的蒐集及利用，尤其對於以保護個人資料為中心的資訊隱私權影響甚鉅，本文下段將介紹資訊隱私權的權利內涵。



第二項 資訊隱私權內涵

（一）資訊隱私權定義

個人資料具有私密性，本質上與隱私權的保障密不可分，因此，隱私權中有關個人資料部分，往往被稱為資訊隱私權⁶⁷。所謂「資訊隱私權」，係指個人具有自主控制其個人資料之權利，而其保障範圍包含揭露與否、範圍、時間、方式及對象、知悉與控制自身個人資料之使用情形、更正資料記載錯誤等，釋字第 603 號解釋文可資參照。舉例而言，個人資料保護法第 3 條及第 10 條明文保障當事人對於保有其個人資料之公務機關或非公務機關，有查詢、請求閱覽或製給複製本之權利，即係具體展現司法院釋字第 603 號解釋所揭示人民對其個人資料之使用有知悉與控制權⁶⁸。再者，在公共場域中的個人資料保護，可參酌釋字第 689 號解釋，此號解釋之理由書認為，基於科技發展迅速及侵擾私人活動設備的容易取得性，人民免於公開揭露之需要提升，因此個人於公共場域中亦能主張資訊隱私權的保護。

資訊隱私權雖然是以個人資訊之保護為其權利之外顯態樣，但關切的卻是特定個人資訊與個人之人格（personhood）或主體性（subjectivity）之間的緊密關聯性。尤其是在當事人無法自行保有並控制資訊時，有能力或有責任管理資訊之人，即應確保資訊在蒐集、儲存、處理、使用、傳輸等過程中，受到完善的管理，不會發生毀損、滅失、外洩、或遭竊取等導致個人人格圖像暴露之情況，以保護個

⁶⁷ 李震山（2007），《多元、寬容與人權保障——以憲法未列舉權之保障為中心》，2 版，頁 196，臺北：元照。

⁶⁸ 黃天偉，前揭註 66，頁 24。

人內在人格形成之彈性空間⁶⁹。綜上所述，資訊隱私權之概念可分析如下：



1.資訊蒐集：特定人、團體或機關，必須在合法與必要的情況下，始得蒐集個人資料，而且在使用個人資料時，必須受到一定之規範。

2.資料正確性：個人擁有存取檔案資料，以及更正錯誤資料的權利。

3.資料私密性：任何人、團體或組織，針對自身之資料，得以自己決定何時、何地以及如何、在何種程度之內，將個人資料傳達給他人之權利⁷⁰。

（二）資訊隱私權的保護客體

資訊隱私權的保護客體，自以「個人資料」為中心。惟個人資料的範圍極廣，性質亦各不相同。舉凡從證明個人生存於社會具有人別性之屬性資料，到個人在社會活動之所有紀錄，均屬個人資料，且性質差異極大，而並非所有個人資料均受資訊隱私權所保護；如姓名、聯絡方式、工作地點等，常為個人經營社會生活，建立人際關係上被預定必須公開之公共性高、私密性低之資料，可能將因無合理隱私期待或因自己主動公開而不受資訊隱私權所保護；然如 DNA、病歷、前科等，則為公共性低、私密性高之資料，且此類資料多屬個人不欲為人所知之私生活領域資料，如他人得濫行蒐集或利用，將造成該當個人精神不安或被貼標籤而致人格受損，本質上屬於個人隱私，為隱私權所涵攝保護之範圍⁷¹。而資訊隱私權與個資法二者均以保護個人資料為中心，則二者間之關係為何？簡言之，於隱私權所保護之隱私與個資法所保護之個人資料，二者間的重疊競合處便是資訊隱私權，

⁶⁹ 李誠偉，前揭註 65，頁 23-24。

⁷⁰ 任文瑗，范錚強，許通安（2006），〈資訊隱私侵害行為意圖之研究〉，《資訊、科技與社會》，6 卷 2 期，頁 77-100。

⁷¹ 范姜真嫻（2013），〈個人資料保護法關於「個人資料」保護範圍之檢討〉，《東海大學法學研究》，第 41 期，頁 100。

亦即資訊隱私權所保護者係具備「隱私」特徵的個人資料。由於個資法所保護的個人資料之範圍與隱私權保護隱私之範圍，有重疊競合處，亦有各自不同之部分。換言之，個人對自己私事決定權，及私生活領域單純不被干擾或窺伺（例如僅為尾隨、偷窺），若不涉及資料之蒐集、處理即非個資法所規範者；另一方面個人出入公共場所、或公開活動之活動資料，如容顏、特徵舉止，因無法合理期待不被同一場所或參加活動之他人知悉，並共有該資料，故本質上不具私密性，實難認定為隱私而納入隱私權保護之範圍。但個人私生活領域具有高私密性或稱高度敏感之資料，如前科、病歷、基因等，則為個資法所保護個資之同時亦屬隱私權所涵攝之隱私，此部分應得稱為資訊隱私權⁷²。職是之故，資訊隱私權的保護範圍實則狹小，但無論如何，若是屬於高敏感個資，則會受資訊隱私權所保護。而此處所指的高度敏感的個人資料除前述所指前科、病歷、基因等外，參酌釋字第 603 號解釋文及理由書中對指紋此種個人資料的敘述，其謂：「指紋係個人身體之生物特徵，因其具有人各不同、終身不變之特質，故一旦與個人身分連結，即屬具備高度人別辨識功能之一種個人資訊。由於指紋觸碰留痕之特質，故經由建檔指紋之比對，將使指紋居於開啟完整個人檔案鎖鑰之地位。因指紋具上述諸種特性，故國家藉由身分確認而蒐集個人指紋並建檔管理者，足使指紋形成得以監控個人之敏感性資訊。國家如以強制之方法大規模蒐集國民之指紋資料，則其資訊蒐集應屬與重大公益之目的之達成，具備密切關聯之侵害較小手段，並以法律明確規定之，以符合憲法第 22 條、第 23 條之意旨。」故指紋亦屬高敏感的個人資訊之一。釋字第 603 號解釋亦提出「高敏感個資」之標準，只要係具有人各不同、終身不變之特質，一旦與個人身分連結，即具備高度人別辨識功能者，即屬於高度敏感個資而同時受資訊隱私權及個資法所保護。國家如欲蒐集或使用該種類型的個資，便會限制人民資訊隱私權的保護，而須符合憲法第 23 條之規定始可為之。

⁷² 范姜真燄，前揭註 71，頁 100。

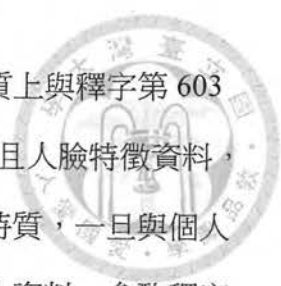
再者，資訊隱私權有確保個人主體性及完整人格發展之保護利益，因此應將蒐集個人資料之目的明確制定於法律中，讓人民透過事先知悉蒐集目的及使用方式，並確保國家之使用係屬合於目的且正當及維護資訊安全，釋字第 603 號解釋理由書可資參照⁷³。故資訊隱私權之保障範圍，亦應包含法律中應有蒐集個人資料之明確目的，且於公共場域中亦受有保護⁷⁴。簡言之，國家對於蒐集資料之目的應明確規範於法律中，以符合法律明確性原則。而法律應如何規定始符合法律明確性原則的要求？可否選擇不確定法律概念的立法模式？關於法律明確性的要求，可參酌釋字第 432 號解釋文的標準「法律明確性之要求，非僅指法律文義具體詳盡之體例而言，立法者於立法定制時，仍得衡酌法律所規範生活事實之複雜性及適用於個案之妥當性，從立法上適當運用不確定法律概念或概括條款而為相應之規定。苟其意義非難以理解，且為受規範者所得預見，並可經由司法審查加以確認，即不得謂與前揭原則相違。」據此，只要其意義非難以理解、且具可預見性，並可經由司法審查加以確認，即符合法律明確性原則。

第三項 人臉辨識系統對資訊隱私權保障的衝擊

人臉辨識系統為使用人臉特徵資料進行身分辨識的生物識別技術之一，對於資訊隱私權保障之衝擊便由此而生。人臉特徵資料係指關於一個人臉部的資料的集合（例如：臉形、眼距、眉形、鼻形、或是臉的比例等），將此等資料結合，可描繪出某一特定人的長相，進而連結至某一特定人士，足以辨識出一個人的身分，人臉辨識系統便是利用此種資料進行身分辨識。雖一個人的容貌可能因參與社會活動等，而暴露於公共視野，導致此種個資公開的公共性高、私密性低，可能不受資訊隱私權所保護。惟人臉辨識系統所使用的人臉特徵資料，不僅僅是關於一個人的容貌長相，此系統用於辨識身分的人臉特徵資料能夠更加細節性的描繪出臉部容貌，進而與特定人連結，而該種資料甚至可能將精細到連本人都不甚清楚

⁷³ 黃天偉，前揭註 66，頁 27-28。

⁷⁴ 黃天偉，前揭註 66，頁 28。



的地步。換言之，此系統所使用的人臉特徵資料，本文以為性質上與釋字第 603 號的指紋有一定程度的相似性，二者均屬個人身體的生物特徵，且人臉特徵資料，若無外力介入，經電腦參數化後，具有人各不同，終身不變之特質，一旦與個人身分連結，屬具有高度人別辨識性的個人資訊，屬於高敏感個人資料。參酌釋字第 603 號中關於指紋的敘述，解釋文及理由書中載道：「指紋乃重要之個人資訊，個人對其指紋資訊之自主控制，受資訊隱私權之保障。因指紋係個人身體之生物特徵，因其具有人各不同、終身不變之特質，故一旦與個人身分連結，即屬具備高度人別辨識功能之一種個人資訊。」人臉特徵資料與指紋相同，均為具備高度人別辨識功能的一種個人資訊，應受資訊隱私權所保護。個人人臉特徵資料既受資訊隱私權所保護，人臉辨識系統蒐集且利用此一個資將限制人民資訊隱私權的保護。

第三節 警察使用人臉辨識系統與憲法第 23 條限制基本權之要件

綜觀前二節之討論，我國警政署將人臉辨識系統與警察臨檢查證身分之行為結合，除將限制人民憲法第 8 條人身自由、第 10 條的居住自由等基本權外，亦將加重第 22 條的隱私權的限制。然基本權之保障並非絕對，憲法第 23 條規定：「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。」而司法院大法官解釋亦有諸多肯認得限制基本權之案例，其中與本文較為相關者，例如：釋字第 443 號解釋理由書中指出：「憲法所定人民之自由及權利範圍甚廣，凡不妨害社會秩序公共利益者，均受保障。惟並非一切自由及權利均無分軒輊受憲法毫無差別之保障：關於人民身體之自由，憲法第八條規定即較為詳盡，其中內容屬於憲法保留之事項者，縱令立法機關，亦不得制定法律加以限制（參照本院釋字第三九二號解釋理由書），而憲法第七條、第九條至第十八條、第二十一條及第二十二條之各種自由

及權利，則於符合憲法第二十三條之條件下，得以法律限制之。」釋字第 523 號解釋理由書中載到：「凡限制人民身體自由之處置，不問其是否屬於刑事被告之身分，國家機關所依據之程序，須依法律規定，其內容更須實質正當，並符合憲法第二十三條所定相關之條件，方符憲法第八條保障人身自由之意旨，業經本院釋字第三八四號、第四七一號解釋等釋示在案。」釋字第 588 號解釋理由書中所載：「人身自由乃人民行使其憲法上各項自由權利所不可或缺之前提，憲法第八條第一項規定所稱「法定程序」，係指凡限制人民身體自由之處置，不問其是否屬於刑事被告之身分，除須有法律之依據外，尚須分別踐行必要之司法程序或其他正當法律程序，始得為之（本院釋字第三八四號解釋參照）。此項程序固屬憲法保留之範疇，縱係立法機關亦不得制定法律而遽予剝奪；惟刑事被告與非刑事被告之人身自由限制，畢竟有其本質上之差異，是其必須踐行之司法程序或其他正當法律程序，自非均須同一不可。」以及釋字第 603 號解釋理由書中亦載：「隱私權雖係基於維護人性尊嚴與尊重人格自由發展而形成，惟其限制並非當然侵犯人性尊嚴。憲法對個人資訊隱私權之保護亦非絕對，國家基於公益之必要，自得於不違反憲法第 23 條之範圍內，以法律明確規定強制取得所必要之個人資訊。至該法律是否符合憲法第 23 條之規定，則應就國家蒐集、利用、揭露個人資訊所能獲得之公益與對資訊隱私之主體所構成之侵害，通盤衡酌考量。並就所蒐集個人資訊之性質是否涉及私密敏感事項、或雖非私密敏感但易與其他資料結合為詳細之個人檔案，於具體個案中，採取不同密度之審查。而為確保個人主體性及人格發展之完整，保障人民之資訊隱私權，國家就其正當取得之個人資料，亦應確保其合於目的之正當使用及維護資訊安全，故國家蒐集資訊之目的，尤須明確以法律制定之。蓋惟有如此，方能使人民事先知悉其個人資料所以被蒐集之目的，及國家將如何使用所得資訊，並進而確認主管機關係以合乎法定蒐集目的之方式，正當使用人民之個人資訊。」



警察使用人臉辨識系統查證身分，此一應用與警察臨檢結合，將限制人身自由、居住自由、隱私權等基本權之保護。由上述的大法官解釋中可知，此一應用所涉的基本權均能限制，但須符合憲法第 23 條之規定，以防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益為目的，且符合比例原則的前提下，始得以法律限制基本權的保障，亦即須遵守法律保留原則、比例原則等限制基本權之要件。而法律保留之密度及比例原則的審查標準，將因所涉的基本權、事務的性質及其對基本權的影響程度而有不同的密度及審查標準。於本文的情形，警察使用人臉辨識系統查證身分，與警察臨檢結合，涉及於行政程序上對非刑事被告人身自由之拘束、人臉特徵資料的蒐集利用，由上述的大法官解釋中可知，此二者將是決定法律保留的密度及比例原則審查標準的關鍵。本文將於下章中，針對警察使用人臉辨識系統作為查證身分手段一事，分別針對法律保留原則以及比例原則進行分析。先說明法律保留原則，爾後說明比例原則，因法律保留原則係針對警察此一應用的「可否」進行討論，而比例原則係針對警察此一應用作得「如何」進行評價，邏輯上，倘無法作此一應用，當然並無後續評估的問題，因此本文首先說明法律保留原則。

惟須注意的是，將人臉辨識系統與臨檢查證身分之行為結合涉及人身自由的限制，而憲法第 8 條中內容上屬於憲法保留者，不得以法律加以變動，因此，須先將憲法第 8 條中屬於憲法保留之內容加以釐清。憲法第 8 條中屬於憲法保留之事項為該條第 2 項及第 3 項之規定：「人民因犯罪嫌疑被逮捕拘禁時，其逮捕拘禁機關應將逮捕拘禁原因，以書面告知本人及其本人指定之親友，並至遲於二十四小時內移送該管法院審問。本人或他人亦得聲請該管法院，於二十四小時內向逮捕之機關提審。法院對於前項聲請，不得拒絕，並不得先令逮捕拘禁之機關查覆。逮捕拘禁之機關，對於法院之提審，不得拒絕或遲延。」此二項所規定之程序，包括告知義務、二十四小時限制以及提審此三大項，僅適用於刑事被告，且大部

分均已落實於刑事訴訟法中⁷⁵。而臨檢查證身分的行為，縱涉及人身自由的限制，受拘束者非屬刑事被告且該程序屬行政程序，誠如釋字第 588 號解釋所言：「刑事被告與非刑事被告之人身自由限制，畢竟有其本質上之差異，是其必須踐行之司法程序或其他正當法律程序，自非均須同一不可。」職是之故，臨檢查證身分之程序，非屬憲法第 8 條憲法保留的範圍，而係屬於立法者得以立法決定之事項，屬於法律保留原則之範圍。

⁷⁵ 李震山，前揭註 63，頁 81。

第四章 警察使用人臉辨識系統查證身分的合法性



第一節 警察使用人臉辨識系統與法律保留原則

第一項 法律保留原則詳要

第一款 法律保留原則的內涵

法律保留原則又稱積極的依法行政原則，在法律保留的範圍內，行政機關僅在法律授權下，始得行為⁷⁶。法律保留原則積極要求行政應有法律依據，但以法律保留範圍內的事項為限，因此法律保留範圍內的事項為何，為重要課題，而此亦是本文所聚焦之處。法律保留原則的理論依據係源自民主原則、法治國家原則以及基本權之法律保留。基於民主原則，關於公共團體之重要事項，尤其是與人民有關之規定應由人民所選出的代表所組成、具有民主正當性之國會，經由公開透明之程序予以決定，關於法律保留的事項，應有法律依據；而基於法治國家原則，國家與人民之間的關係應由明確，有預見可能及穩定的法律予以規定；再者，人民之基本權應受保障，非依據法律或法律授權，不得加以限制，且如有限制基本權之必要，基於上開民主及法治國原則，法律應規定限制基本權之方式、要件及界線，以保障各個基本權⁷⁷。法律保留，在基本權限制的關聯上，又稱干預保留，指的是若欲限制人民基本權的保護，應保留由立法者以法律規定，沒有法律的依據，行政權不能擅自為之。干預保留的產生係由於 19 世紀歐陸的自由憲法運動，

⁷⁶ 林錫堯（2005），〈法律保留原則之理論與實踐〉，《法學叢刊》，50 卷 4 期，頁 1。

⁷⁷ 林錫堯，前揭註 76，頁 2-3。



為保護人民自由與財產權利，免於遭受傳統上由君主所控制的行政權力（國家）之恣意侵犯，因此要求行政若欲干預上開權利，須事先經代表人民一方的議會（社會）以法律方式表示同意，始得為之⁷⁸。

第二款 法律保留原則之範圍

關於法律保留原則之範圍，學說上有干涉保留說（又稱侵害保留說）、全部保留說、權力保留說、社會保留說以及重要事項說等。干涉保留說主張法律保留原則之範圍僅限干涉行政，且限於對自由權及財產權之干涉，始有適用。全部保留說則認為所有的行政行為均應適用法律保留原則，在國民主權主義與國會民主制度下，不承認「無法律之自由行政」。權力保留說則主張凡能左右國民權利義務之權力行政，均須有法律依據。社會保留說則認為現代國家之行政職務，並非僅限於公權力保障國民的自由與財產，更以確保國民的社會權為其重要職務，因此給付行政領域中以確保社會權為目的的社會保障型正義須有法律依據。重要事項說（又稱重要性理論）所謂「重要事項」其標準並非依照「事物之本質」，而係視規範內容對公益或人民是否具有意義、重要、根本、影響強烈等性質而定，其並非固定概念，而是因變公式。事物之性質對公益或人民越重要，則對立法的要求越高；對人民基本權的干涉愈有脅迫性、對公益影響越重大或問題愈複雜，則越需詳細、嚴密的法律規範⁷⁹。

我國自釋字第 443 號解釋後，針對法律保留原則之範圍，採取層級化法律保留以及重要性理論之見解，在採取干預保留的同時，對於給付行政部分也納入重要性理論的考量⁸⁰。釋字第 443 號解釋理由書中言及：「憲法所定人民之自由及權

⁷⁸ 許宗力（2003），〈基本權利：第六講—基本權的保障與限制（上）〉，《月旦法學教室》，第 11 期，頁 75。

⁷⁹ 林錫堯，前揭註 76，頁 3-4。

⁸⁰ 陳仲嶙（2020），〈從防疫出國禁令爭議再訪法律保留的疆界〉，《法律與生命科學》，9 卷 1 期，頁 25。



利範圍甚廣，凡不妨害社會秩序公共利益者，均受保障。惟並非一切自由及權利均無分軒輊受憲法毫無差別之保障：關於人民身體之自由，憲法第八條規定即較為詳盡，其中內容屬於憲法保留之事項者，縱令立法機關，亦不得制定法律加以限制（參照本院釋字第三九二號解釋理由書），而憲法第七條、第九條至第十八條、第二十一條及第二十二條之各種自由及權利，則於符合憲法第二十三條之條件下，得以法律限制之。至何種事項應以法律直接規範或得委由命令予以規定，與所謂規範密度有關，應視規範對象、內容或法益本身及其所受限制之輕重而容許合理之差異：諸如剝奪人民生命或限制人民身體自由者，必須遵守罪刑法定主義，以制定法律之方式為之；涉及人民其他自由權利之限制者，亦應由法律加以規定，如以法律授權主管機關發布命令為補充規定時，其授權應符合具體明確之原則；若僅屬與執行法律之細節性、技術性次要事項，則得由主管機關發布命令為必要之規範，雖因而對人民產生不便或輕微影響，尚非憲法所不許。又關於給付行政措施，其受法律規範之密度，自較限制人民權益者寬鬆，倘涉及公共利益之重大事項者，應有法律或法律授權之命令為依據之必要，乃屬當然。」

據此，由該號釋字出發，針對法律保留原則之範圍，於干預行政及給付行政領域，一般性判準為「視規範對象、內容或法益本身及其所受限制之輕重」，區分不同法律規範密度。而法律保留原則的適用，本文區別干預行政與給付行政領域，整理如下：

（一）干預行政

首先區別憲法保留以及法律保留兩個層次，憲法保留，如前述，涉及憲法第8條人身自由的規定，不能以法律加以變動。法律保留所涉及者，係人身自由以外



的其他基本權利。釋字第 443 號解釋將法律保留分為以下三個層次⁸¹：

1.絕對法律保留（國會保留）：涉及剝奪人民生命或限制人民身體自由，須由立法者親自以制定法律之方式規定之，不得由行政機關以訂定命令的方式加以補充。

例如：應由法院裁定之罰鍰的處理程序（釋字第 289 號）、對公務員所為免職處分的構成要件（釋字第 491 號）以及刑罰事項（釋字第 443 號）。

2.相對法律保留：涉及人民除人身自由外之其他自由權利之限制，應有法律依據，但亦可在符合授權明確性之前提下，將部分事項委由行政機關訂定命令補充之⁸²。例如：行政罰事項（釋字第 394 號、第 638 號）或租稅事項（釋字第 657 號）等均屬相對法律保留，允許部分事項得由行政機關以訂定命令之方式加以補充，惟授權明確性之標準將因事物之性質而有所差異。非屬絕對法律保留適用範圍內之事項，立法者固能以法律授權行政機關以命令的方式來決定，但該授權仍須符合授權明確性的要求，不能為空泛而無確定範圍的空白授權。授權時仍須就授權的目的、內容與範圍自為明確規定，絕不能不稍作指示即放任被授權的行政機關海闊天空行事，否則所謂法律的授權，將徒具形式，不具任何實質意義，將導致於行政領域中，須經法律授權、規制，從而行政自由決定空間相對狹窄的「法律從屬行政」，與不在法律保留範圍內，因此毋庸法律授權、引導，從而行政自由決定空間相對廣的「法律外行政」，兩者間的分界將趨於模糊⁸³。而法律只要足以令人從其授權條款與其他相關規定，依一般法律解釋方法推論得出其所要求行政機關以命令追求的目標與範圍，即可視為符合授權明確性的要求（釋字第 394 號）⁸⁴。

⁸¹ 莊國榮（2012），〈層級化法律保留原則的適用〉，《臺灣法學雜誌》，第 208 期，頁 1-12。

⁸² 廖元豪（2004），〈走自己的路——大法官「法律保留本土化」之路〉，《臺灣本土法學雜誌》，第 58 期，頁 31。

⁸³ 許宗力，前揭註 78，頁 74。

⁸⁴ 許宗力，前揭註 78，頁 75。

3.不適用法律保留：細節性技術性事項。該種事項由於僅對人民產生不便或輕微影響，故為憲法所許。判斷重點在於內容是否僅「對人民產生不便或輕微影響」，而不在執行特定法律，且為避免引發滑坡效應，應審慎評估，避免濫用。

（二）給付行政

給付行政由於並未限制人民之自由權利，因此爭議在於給付行政是否適用法律保留原則？針對此一問題，釋字第 443 號解釋理由書指出，給付行政雖未限制人民之自由權利，雖難謂與憲法第 23 條規定之限制人民之基本權利之法律保留原則有違，但於涉及公共利益或與實現人民基本權利之保障等重大事項，原則上仍應有法律或法律明確之授權為依據⁸⁵。肯認給付行政亦應有法律保留之適用，但於給付行政之領域，受法律規範之密度，較限制人民權益者為寬鬆，若涉及公共利益重大事項或是於實現人民基本權利具有重大意義，則屬相對法律保留之範圍，反之，則為不適用法律保留之給付行政⁸⁶。

第二項 當事人同意與法律保留原則間之關係

由前段可知，我國對於法律保留原則之適用範圍，從對基本權造成侵害之事項，擴展至關於基本權實現之重要事項，乃至更廣泛的涉及公共利益，攸關全民福祉甚鉅的給付行政領域均有適用⁸⁷。而不論係於干預行政或是給付行政之領域均深受重要性理論的影響，於干預行政之領域便是以「規範對象、內容或法益本身及其所受限制之輕重」之標準，區分不同法律保留規範之密度；於給付行政領域，更是以「是否涉及公共利益或是基本權實現之重大事項」決定是否須法律保留，均可見重要性理論的影響。

⁸⁵ 謝榮堂（2014），〈法律保留原則於給付行政之適用與例外〉，《警察法學》，第 13 期，頁 140。

⁸⁶ 莊國榮，前揭註 81，頁 12-13。

⁸⁷ 陳慈陽、王毓正（2003），〈論司法院大法官解釋對於基本權保障之理論發展〉，《月旦法學雜誌》，第 98 期，頁 26。

而本文所欲探討者，係當事人同意與法律保留原則之關係，涉及法律保留原則的適用範圍。具體而言，於第二章中本文提及警察如欲使用人臉辨識系統查證民眾身分時，程序上，須以取得人民同意為前提，始可啟用此一系統，且由於我國警察人臉辨識系統之使用目前仍為一對一之模式，此一同意更顯重要，如係在當事人之同意下始使用此一系統，則此一系統的使用是否仍須有明確的法律依據為本段欲討論之問題，此一問題涉及法律保留原則之適用範圍、當事人同意的內涵以及基本權之捨棄等爭議。

針對此一問題，有認為任何干涉人民基本權利之公權力行為，均應有法律依據，且由於基本權利不得拋棄，故公權力之干涉，若無法律明文規定，不得僅以業經人民同意為由，任意為之⁸⁸。縱使部分基本權之性質得由人民加以支配及拋棄，仍不得以人民之拋棄取代法律保留原則所要求之干涉授權⁸⁹。據此，縱使警察使用人臉辨識系統查證民眾身分事前已取得同意，惟由於該系統將限制人民基本權之保障，警察使用該系統仍須有法律依據始可。另有認為，於行政契約之領域中，人民原得自由支配運用為其利益所設定之法律地位，除有不當連結之情形，否則應允許人民透過與行政機關訂定行政契約之方式，合意拋棄法律地位⁹⁰。行政法院71年判字第212號判決即指出：「人民之自由權利，固不得任意加以限制，但其限制如係基於本人之承諾，而又無悖於公序良俗，則非法所禁止。」據此，警察使用該系統查證民眾身分，若已取得同意，由於警察此一限制基本權之行為係基於當事人之承諾，縱使無法律依據即可使用該系統。除前述兩種見解外，亦有採取折衷看法者，認為法律保留之提倡，本係為保障人民基本權利，限制行政機關從事行政行為時，如有涉及人民權利義務之不利地位形成者，應有法律之依據，此一原則係用於限制行政機關而非約制人民，如人民係在自由意願下出於自我意志

⁸⁸ 陳敏（2013），《行政法總論》，8版，頁591，臺北：自版。

⁸⁹ 陳敏，前揭註88，頁170。

⁹⁰ 陳敏，前揭註88，頁594。

所從事之拋棄權利，應尊重人民之選擇，無須有法律依據，除非該權利係受嚴密甚至完全之保障，不得逕自拋棄⁹¹。倘採此一看法，則除非人臉辨識於臨檢查證身分之應用所涉及之基本權利係受最高密度之保障者，而不得任由人民逕自拋棄者外，警察使用此一系統查證身分若已取得人民同意，縱無法律依據，亦無礙其合法性。

回到本文，針對警察係於取得當事人之同意的前提下，始使用人臉辨識系統查證身分，此一情形是否仍須法律保留，可由重要性理論之角度切入加以回答。由於我國針對法律保留原則之適用範圍深受重要性理論之影響，只要是屬於「重要事項」則應適用法律保留原則，而重要性的程度將影響法律規範之密度。所稱「重要事項」，可由功能最適⁹²觀點出發，法律保留範圍之決定標準，包括基本權之重要性、公共事務重要性等積極衡量標準以及緊急事故與規範不能之事務等消極衡量標準。於積極衡量標準方面，所謂基本權之重要性，以對基本權之實現是否重要作為判別準據；公共事務重要性，則可由受規範人範圍之大小、影響作用之久暫、財政影響之大小、公共爭議性之強弱、現狀變革幅度之大小、與現行法之比較等參考因素來協助劃定⁹³。

於本文之情形，於當事人同意警察使用人臉辨識系統查證身分的情形下，針對此一應用是否仍須有法律保留？當事人同意涉及拋棄基本權之保護，而本文傾向採取前述折衷說之看法，除非該權利係受嚴密甚至完全之保障而不允許拋棄者外，倘人民係在自由意願下出於自我意志所從事之拋棄權利，應尊重人民之選擇，

⁹¹ 許宏達（2015），〈擺盪在法律保留與契約自由間之行政契約合法性探討--以法定山坡地劃出之切結書為例〉，《軍法專刊》，61 卷 5 期，頁 51。

⁹² 所謂功能最適係要求考察國家機關之內部結構、組成方式；功能與決定程序等各面向之特徵，而將國家事務分配由具備最佳條件之國家機關來擔當做成。法律保留原則之適用範圍，簡言之，便是要劃定立法與行政之界線，因此本文選擇由功能最適的角度出發，說明法律保留原則之範圍。許宗力（2009），〈論法律保留原則〉，氏著，《法與國家權力》，頁 139，臺北：元照。

⁹³ 許宗力，前揭註 92，頁 183-192。



因基本權利的作用係用在於保護人民免於政府之干預，倘人民自願捨棄保護傘，原則上應無不許之理。於本文之情形，當事人同意警察使用人臉辨識系統所拋棄之基本權保護主要為隱私權，隱私權依釋字第 603 號解釋之見解，係得以法律限制之基本權利，固該基本權應非前述所稱受嚴密甚至完全之保障，當事人拋棄此一權利，應無不許之理，但本文認為前提是該同意係出於自由意志且在當事人瞭解拋棄權利的後果下所為。而由於下列之理由，本文仍認為此一應用仍須法律保留。

首先，縱使警察使用人臉辨識系統係基於當事人的同意，而本文亦認為除該基本權之性質係受最嚴密之保護而不允許拋棄者外，當事人拋棄基本權之保護並無不許之理，但該同意須出於自由意志，且在瞭解拋棄權利之後果下所為。惟於本文之情形中，該同意是否出於自由意志，不無疑問。由於警察將人臉辨識系統與警察臨檢結合，而臨檢如前述，涉及人身自由的限制，依警職法第 7 條第 2 項之規定，當警察無法依詢問或令出示身分證明文件的方式查證身分時，警察得將該人民帶往勤務處所，時間自攔停起，不得逾三小時，並應即向該管警察勤務指揮中心報告及通知其指定之親友或律師。職是之故，此同意是否係當事人為避免後續行政程序的拘束而出於不得已而為之，具半強迫性，不無疑問。再者，雖然我國警察使用人臉辨識系統仍限於一對一之情形，惟實際上人臉辨識系統的使用，不僅影響當事人，所有存在於人臉資料庫中的潛在候選人均會受到影響，系統為找出匹配之對象，將會逐一與資料庫中的資料進行比對。而我國人臉資料庫有以內政部戶政司國民身分證相片資料作為建檔基礎者，因此，實質上，警察使用人臉辨識系統查證身分所受影響之人將不計其數，而僅有當事人一人的同意或許並不足以正當化此一廣泛的影響。除此之外，人臉辨識系統與警察臨檢結合，亦一定程度改變臨檢程序，又涉及新興科技的使用，更使用高度人別識別個資進行身分識別，且此一系統與警察臨檢結合更涉及人身自由、居住自由等基本權之限制，



基於前述重要事項之判準，此一應用基於其對於公共事務重要性、所造成的社會爭議性之強度及對於現狀變革幅度，警察使用人臉辨識系統查證身分應為重要事項，而屬法律保留之範圍。職是之故，基於本文當事人同意背後動機的不確定性及人臉辨識系統對於社會爭議性及重要性，警察使用該系統查證身分須有法律依據，如此，警察將其作為查證身分之手段始具合法性。

第二節 現行警察使用人臉辨識系統查證身分之法制

於前一節中，本文認為縱使警察於臨檢時使用人臉辨識系統查證民眾身分，係以取得當事人之同意為前提，惟基於該同意背後的不確定性、人臉辨識系統的廣泛影響、及此一應用對於基本權之重要性，加上民眾對於人臉辨識系統的質疑，使該系統社會爭議性極高，警察使用人臉辨識系統查證民眾身分，仍須有明確法律依據始可。據警政署所發布人臉辨識系統疑慮說明資料第三點⁹⁴，此一應用的法律依據為警職法第 6 條與第 7 條第 2 款及第 3 款有關臨檢查證身分的要件及手段。而除警職法之規定外，此一應用亦涉及諸多內部行政規則，針對該系統的內部監管以及資料維護上，涉及警政署內部自訂的警用行動電腦使用管理要點、警察機關資訊安全實施規定以及警政日誌管理系統作業規定此三個行政規則。以下將分析，以警職法第 6 條及第 7 條為中心的法制是否足以支撐警察使用 M-Police 人臉辨識系統作為臨檢查證身分的手段。而由於警察係變相將該系統作為資料蒐集之手段，因此本文除分析警職法第 6 條及第 7 條外，亦將一同探討有關資料蒐集的相關規定（警職法第二章身分查證及資料蒐集的規範，及第三章即時強制章的第 28 條）。易言之，警職法的相關規定是否滿足憲法第 23 條法律保留原則之要求？本文將由警職法之定位出發，分析該法是否足夠作為警察使用 M-Police 人臉辨識

⁹⁴ 內政部警政署疑慮說明資料第三點：「依據警察職權行使法第 6 條、第 7 條查詢人民身分規定及個人資料保護法第 15、16 條公務機關執行法定職務必要範圍內等規定，故 M-Police 即時相片比對系統使用無適法性問題。」

系統的法律依據。



第一項 人臉辨識系統與警察職權行使法

第一款 警察職權行使法的立法

警職法尚未立法前，警察臨檢的法律依據為警察勤務條例，而經大法官釋字第 535 號解釋，此號解釋雖宣告警察勤務條例合憲，但認定本條例之內容不夠具體明確，要求相關機關應重新檢討制訂出一部適合警察人員的職權行使的法律，因此催生了現今的警察職權行使法。於本號解釋中，大法官於解釋理由書中載到：「警察勤務條例第三條至第十條乃就警察執行勤務之編組、責任劃分、指揮系統加以規範，第十一條則對執行勤務得採取之方式予以列舉，除有組織法之性質外，實兼具行為法之功能。查行政機關行使職權，固不應僅以組織法有無相關職掌規定為準，更應以行為法（作用法）之授權為依據，始符合依法行政之原則，警察勤務條例既有行為法之功能，得作為警察執行勤務之行為規範。依該條例第十一條第三款：「臨檢：於公共場所或指定處所、路段，由服勤人員擔任臨場檢查或路檢，執行取締、盤查及有關法令賦予之勤務」，臨檢自屬警察執行勤務方式之一種。惟臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，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。人民之有犯罪嫌疑而須以搜索為蒐集犯罪證據之手段者，依法尚須經該管法院審核為原則（參照刑事訴訟法第一百二十八條、第一百二十八條之一），其僅屬維持公共秩序、防止危害發生為目的之臨檢，立法者當無授權警察人員得任意實施之本意。是執行各種臨檢應恪遵法治國家警察執勤之原則，實施臨檢之要件、程序及對違法臨檢行為之救濟，均應有法律之明確規範，方符憲法保障人民自由權利之意旨。上開條例有關臨檢之規定，既無授權警察人員得不顧時間、地點及對象任意臨檢、取締或隨機檢查、盤查之立法本意。除法律另有規定（諸如刑事訴訟法、行政執行法、



社會秩序維護法等)外，警察人員執行場所之臨檢勤務，應限於已發生危害或依客觀、合理判斷易生危害之處所、交通工具或公共場所為之，其中處所為私人居住之空間者，並應受住宅相同之保障；對人實施之臨檢則須以有相當理由足認其行為已構成或即將發生危害者為限，且均應遵守比例原則，不得逾越必要程度，儘量避免造成財物損失、干擾正當營業及生活作息。至於因預防將來可能之危害，則應採其他適當方式，諸如：設置警告標誌、隔離活動空間、建立戒備措施及加強可能遭受侵害客體之保護等，尚不能逕予檢查、盤查。臨檢進行前應對受臨檢人、公共場所、交通工具或處所之所有人、使用人等在場者告以實施之事由，並出示證件表明其為執行人員之身分。臨檢應於現場實施，非經受臨檢人同意或無從確定其身分或現場為之對該受臨檢人將有不利影響或妨礙交通、安寧者，不得要求其同行至警察局、所進行盤查。其因發現違法事實，應依法定程序處理者外，身分一經查明，即應任其離去，不得稽延。前述條例第十一條第三款於符合上開解釋意旨範圍內，予以適用，始無悖於維護人權之憲法意旨。又對違法、逾越權限或濫用權力之臨檢行為，應於現行法律救濟機制內，提供訴訟救濟（包括賠償損害）之途徑：在法律未為完備之設計前，應許受臨檢人、利害關係人對執行臨檢之命令、方法、應遵守之程序或其他侵害利益情事，於臨檢程序終結前，向執行人員提出異議，認異議有理由者，在場執行人員中職位最高者應即為停止臨檢之決定，認其無理由者，得續行臨檢，經受臨檢人請求時，並應給予載明臨檢過程之書面。上開書面具有行政處分之性質，異議人得依法提起行政爭訟。現行警察執行職務法規有欠完備，有關機關應於本解釋公布之日起二年內依解釋意旨，且參酌社會實際狀況，賦予警察人員執行勤務時應付突發事故之權限，俾對人民自由與警察自身安全之維護兼籌並顧，通盤檢討訂定。」

本號解釋，重點有三，一為提出行為法及組織法的區別標準並認定由於警察勤務條例第 11 條中對於警察執行勤務得採取之方式予以列舉，因此本條例並非單



純的組織法而是兼具有行為法的性質，得作為警察執行勤務之行為規範，而由該號解釋對於警察勤務條例性質之說明可知，法律得兼具行為法及組織法的性質。

二為說明臨檢的目的、要件及方式，由本號解釋說明臨檢概念時引用警察勤務條例中關於臨檢的定義可知，針對臨檢定義採取廣義之見解。本文所著重身分查證行為，學說上有以對人的臨檢稱之，當然亦屬臨檢的方式之一，手段上，包含路檢、身分查證等均屬於臨檢的方式，而本文所著重的身分查證行為，學說上有以對人的臨檢稱之者，但無論臨檢的方式為何，其目的為維持公共秩序、防止危害發生，以犯罪預防為主要目的，而非犯罪的偵查，更由於臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，均影響人民行動自由、財產權及隱私權等甚鉅，立法者並無授權警察人員得任意實施之本意，因此實施臨檢之要件、程序及對違法臨檢行為之救濟，均應有法律之明確規範。再者，對人實施之臨檢則須以有相當理由足認其行為已構成或即將發生危害者為限，且均應遵守比例原則，不得逾越必要程度，儘量避免造成財物損失、干擾正當營業及生活作息以及要求臨檢應有救濟機制。三為認定本條例雖有違法律明確性原則，且規範欠缺完備，仍為合憲宣告，但要求有關機關應於本號解釋公布之日起二年內依解釋意旨通盤檢討訂定，催生了現今的警察職權行使法。

釋字第 535 號解釋係 2001 年 12 月 14 日所公布，而警察職權行使法係 2003 年 6 月 25 日經總統公布，並於同年 12 月 1 日施行，雖警察職權行使法施行後警察勤務條例並無因此廢止，至今仍為有效的法律，但該條例自釋字第 535 號解釋公布之後，至遲於 2007 年始有修正，且所修正之部分亦非該號解釋所指有關臨檢之部分，易言之，該條例中有關臨檢的規定，自釋字第 535 號公布後直至今日均無修正，反之，警察職權行使法對於臨檢身分查證行為，配合釋字第 535 號解釋之意旨，不但做出較為具體明確的規定，且為本號解釋明令二年內修正期間所新增定的法律，顯然係立法院針對釋字第 535 號解釋之意旨，對於警察行使職權新

訂的法律，因此警察臨檢應以警職法為法律依據。。



第二款 警察職權行使法之定位

警察職權行使法應屬於警察權限的一般法律而非特別法，雖於立法之初有意賦予本法特別法的地位，但最後並未予以採納⁹⁵。而本法的規範內容實無可能涵蓋警察為完成所負犯罪（危害）預防任務，所應具有之權限手段，因此除該法之規定外，尚待其他個別法之授權，始能建立完善的、整體的警察權限法制。綜觀警職法之規定，本法中對於警察執行勤務所得採取之方式及要件均予以規範（例如：查證身分、車輛攔停、即時強制以及治安顧慮人口的查訪等），除此之外，亦將救濟之方式加以明確化。由此觀之，警職法屬於警察行為法，規範警察行使職權的活動，與規範警察組織的組織法有所區別。警察組織法，相對於警察行為法，係規範警察機關內部的組織與權限，我國的警察法即屬於警察組織法⁹⁶。警職法既屬行為法，便可作為警察行使職權的法律依據，因此警察使用人臉辨識系統作為查證身分手段，有一行為法作為法律依據，但問題在於本法中有關身分查證行為的規定，具體而言，本法第 6 條及第 7 條第 1 項第 2 款及第 3 款之規定是否可支撐此一應用。本文將由臨檢的本質出發並檢視此二條之規定來回答此一問題。

第三款 臨檢的內涵以及警職法身分查證規定之介紹

（一）臨檢的內涵

釋字第 535 號解釋中對於臨檢，採取警察勤務條例第 11 條第 3 款對於臨檢之定義，係指警察於公共場所或指定處所、路段，臨場檢查或路檢，執行取締、盤查及有關法令賦予之勤務。定位於舉凡警察採取限制或干預人民的行動自由、財

⁹⁵ 當初行政院以及陳委員其邁等立法委員所提的警察職權行使法草案中，對於本法的適用範圍均有如是規定：「警察行使職權，依本法之規定；本法未規定者，適用其他法律之規定。」賦予本法特別法之地位，但爾後立法院三讀通過的版本將此規定刪除，因此本法不具特別法的優勢地位，為一普通法。

⁹⁶ 蔡震榮（2016），《警察職權行使法概論》，三版，頁 81，臺北：五南。

產權或隱私權的手段，如：檢查、路檢、取締或盤查等，不問名稱為何，均可稱之為臨檢，對臨檢採取較為廣義之解釋，身分查證自屬臨檢範圍。立法者之所以賦予警察臨檢權限，係因警察有積極預防犯罪之職責，有必要讓警察在遇到疑似犯罪之人事，情況卻尚不足以發動刑事訴訟法之強制處分之前，有權對現場人員進行初步調查。此外，讓警察對在場者進行身分查驗，尚有嚇阻犯罪的效果。犯罪者可能因為警察的存在與自身身分的曝光，放棄後續的犯罪計畫⁹⁷。

由臨檢的目的亦可更加說明臨檢的本質，警察臨檢，係警察行政任務其中之一，以危害防止為主要目的，並非針對犯罪行為所為的檢查，因此除特別法另有規定外，一般適用警察職權行使法，不適用刑事訴訟法的規定，亦無事前令狀原則的規定⁹⁸。再者，警察實施臨檢，相對刑事犯罪偵查係針對「特定被告」、「特定犯嫌」，警察臨檢則未針對特定對象或鎖定特定案情進行調查。警察實施臨檢乃積極、主動探求犯罪發生可能事跡，並以預防犯罪發生，維護社會秩序為其主要目的⁹⁹。

（二）臨檢與行政調查

臨檢的性質係屬行政機關為達成行政目的所行使的蒐集資料之行為，因此有論者認為臨檢本質屬行政調查。對於行政調查之定義，雖然國內迄今尚未有一致的看法，並經常與行政檢查或行政資料蒐集互相使用¹⁰⁰，但原則上，凡法規上有如調查、檢查、稽查、臨檢、查核、查證、詢問或備詢等用語，具有行政機關基於特定目的為蒐集資料之意涵，本質上即屬行政調查¹⁰¹。行政調查之定義，廣義

⁹⁷ 李佳玟（2014），〈青春專案〉，《月旦法學教室》，第144期，頁33。

⁹⁸ 吳景欽（2004），〈警察職權行使法中關於臨檢規定之正當性探討〉，《軍法專刊》，50卷6期，頁23。

⁹⁹ 林裕順（2015），〈臨檢盤查「半推半就」〉，《月旦法學教室》，第148期，頁25。

¹⁰⁰ 李震山（2007），《行政法導論》，7版，頁489，臺北：三民。

¹⁰¹ 洪家殷（2010），〈論行政調查中職權調查之概念及範圍——以行政程序法相關規定為中心〉，《東

而言，係指行政機關為達成特定之行政目的，所從事之資料蒐集活動。而此種蒐集活動，包含機關內部所實施之各種調查行為，亦包括行政機關對私人所實施者；其手段上得為任意性或強制性；對象上，不論對人、對事、對處所等，皆屬之；且得為一般性調查或個別性調查。而警職法第 6 條及第 7 條有關臨檢查證身分的行為即係警察機關基於維護社會秩序及預防犯罪的目的而對民眾強制蒐集與其身分有關之個資的行為，符合行政調查的定義，自屬廣義行政調查的一種。而臨檢本質既屬行政調查，以危害防止為其主要目的，為警察行政任務的一環，除警職法另有規定外，行政程序法中有關行政調查的規定原則上亦得適用於警察臨檢。雖依行政程序法第 3 條第 3 項第 3 款之規定，刑事案件犯罪偵查程序排除行政程序法的適用，但警察臨檢並非以犯罪偵查為目的，不屬於犯罪偵查程序一部分，反之，臨檢為警察行政的一環，以犯罪預防為其目的，因此並無不適用行政程序法的特權¹⁰²。

（三）臨檢為強制或是任意手段？

由前述可之，臨檢係以犯罪預防為主要目的，屬於警察行政的一環，而其本質應為行政調查。行政程序法中有關行政調查之規定，除警職法另有規定外，並無不適用之理。觀行政程序法之規定，於行政調查程序中，行政機關對於調查方法的選擇，享有極大的裁量空間，雖本法第 39 條至第 42 條列舉出 4 種行政機關得使用的調查方法，分別為：通知陳述意見¹⁰³、要求提供文書¹⁰⁴、送請鑑定¹⁰⁵及

吳法律學報》，21 卷 3 期，頁 5-6。

¹⁰² 李震山（2002），〈從釋字第五三五號解釋談警察臨檢的法制與實務〉，《台灣本土法學雜誌》，第 33 期，頁 76。

¹⁰³ 行政程序法第 39 條規定：「行政機關基於調查事實及證據之必要，得以書面通知相關之人陳述意見。通知書中應記載詢問目的、時間、地點、得否委託他人到場及不到場所生之效果。」

¹⁰⁴ 行政程序法第 40 條規定：「行政機關基於調查事實及證據之必要，得要求當事人或第三人提供必要之文書、資料或物品。」

¹⁰⁵ 行政程序法第 41 條規定：「行政機關得選定適當之人為鑑定。以書面為鑑定者，必要時，得通知鑑定人到場說明。」

進行勘驗¹⁰⁶，但實際上行政機關得採用的調查方法並不限於此，由於行政程序係採「自由證據原則」¹⁰⁷，依據該原則，行政機關可採用一切其認為是正確或是適當的調查方法，只要是合法且必要即可。惟此是否代表警察臨檢的手段將不受限制？可採取一切其認為是正確且適當的手段，只要合法且必要即可？此一爭議便涉及臨檢究屬強制或是任意手段的爭議。

針對臨檢為強制抑或是任意手段此一問題，釋字第 535 號解釋理由書中有謂：「臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，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。立法者當無授權警察人員得任意實施之本意。是執行各種臨檢應恪遵法治國家警察執勤之原則，實施臨檢之要件、程序及對違法臨檢行為之救濟，均應有法律之明確規範，方符憲法保障人民自由權利之意旨。」該號解釋認為由於警察臨檢將影響人民行動自由、財產權及隱私權甚鉅，因此基於該行為的權利侵害性，警察不得任意實施臨檢，因此臨檢的要件、程序及手段均須有明確的法律規定，換言之，基於臨檢權利侵害性，本號解釋將臨檢行為定性為強制手段而非任意手段。究其理由，針對強制手段及任意手段的區分，學界上有大致三種說法，分別為有形力行使說、實力說以及權利侵害說三種。有形力行使說係以是否有直接的、有形的實力行使來區別強制及任意手段；而實力說則是以社會通念上的妥當性限度來區別強制及任意手段；權利侵害說則是以「是否招致個人權利及法益之侵害」為判斷強制以及任意手段的標準¹⁰⁸。本文認為，釋字第 535 號解釋應係採權利侵害說的觀點，而將警察的臨檢行為定性為強制手段。本文亦認為權利侵害說之觀點較為可採，因近年來，科技的迅速發展，各種行政手段或是蒐證手段，層出不窮，例如照相、監聽、

¹⁰⁶ 行政程序法第 42 條規定：「行政機關為瞭解事實真相，得實施勘驗。勘驗時應通知當事人到場。但不能通知者，不在此限。」

¹⁰⁷ 洪家殷（2011），〈論行政調查之證據及調查方法－以行政程序法相關規定為中心〉，《東海大學法學研究》，第 35 期，頁 12。

¹⁰⁸ 鄭羽軒（2018），《警察職權行使法諸問題之研究》，頁 71，中央警察大學警察政策研究所博士論文。

測謊、檢查等，其雖非有形力之行使，但所造成的影響實質上與有形力之行使，並無二致，極易對隱私權等新興基本權利造成威脅。在此種情況下，若仍採取傳統「有形力行使說」的觀點判斷強制及任意手段，極易產生漏洞，亦不合時宜，而實力說的判準又有極大的不確定性，相較之下，以「是否招致個人權利及法益之侵害」為判斷依據區分任意與強制手段，除較能因應科技迅速的發展外，亦可避免過度擴張警察的權力，保障人權。按照權利侵害說，有形力不再是決定性的要素，於某些場合，雖非有形力之行使，亦有可能係強制處分；相反地，即使是任意處分，亦可能容許行使有形力。總而言之，於採取權利侵害說之場合，警察於實施臨檢時，倘欲施用有形力，重點在於「在何種情形下，容許何種程度之有形力」。

由於本文認為臨檢屬於強制手段而非任意手段，因此實施臨檢之要件、程序及手段均應有法律之明確規範，同釋字第 535 號解釋之意旨。此一觀點，亦落實於警職法第 7 條的立法中，本條將警察查證身分得使用的必要手段以法律予以列舉。因此行政程序法中有關行政調查程序的自由證據原則，於警察臨檢，該原則將受到限制。警察於臨檢時，並無廣泛調查方法裁量權，反而僅能依據警職法第 7 條所規定之方式查證民眾身分，且容許有形力的實施。警職法第 7 條第 2 項規定：「如依前項第二款（詢問姓名、出生年月日、出生地、國籍、住居所及身分證統一編號等）、第三款（令出示身分證明文件）之方法顯然無法查證身分時，警察得將該人民帶往勤務處所查證；帶往時，非遇抗拒不得使用強制力，且其時間自攔停起，不得逾三小時，並應即向該管警察勤務指揮中心報告及通知其指定之親友或律師。」據此，在無從確定身分之前提，而需將受檢人帶離原處時，倘遇抗拒時，容許施用有形力。由此可知，臨檢雖緊急必要之情況下重視行政目的效率，但其強制力作爲仍侷限在「任意處分」的範疇，高度尊重相對人配合警職勤務與否之「決定可能」。如同釋字第 535 號解釋所言：「臨檢應於現場實施，非經受檢

人同意或無從確定其身分或現場為之對該受臨檢人將有不利影響或妨礙交通、安寧者，不得要求其同行至警察局、所進行盤查。」強調臨檢之實施，須經相對人「同意」或配合「同行」（非該當「逮補」）為前提¹⁰⁹。警察實施臨檢高度仰賴受檢人的同意或配合，臨檢始可順行。警察實施臨檢，行使強制力非可「強制貫徹」，或雖相對人「不甘不願」，但仍止於「半推半就」限度。除此之外，臨檢的程序係由攔停、詢問、核對身分、檢查至放行所組成，而臨檢盤查的重點在於「詢問」，攔停乃達到詢問效果的前提手段。故合法的有形力行使，應注意並未造成強制答辯的情形。亦即，攔停限度於「輕度」、「一時性」、「過渡性」的手段，並注意警察比例原則的適用，考量涉案嫌疑重大、具體情況的緊迫、有形力行使的必要¹¹⁰。

（四）警職法有關身分查證手段之規定

目前警職法中對於警察於臨檢時，如欲查證受檢人之身分其得使用之手段，規定於本法第 7 條：「警察依前條規定，為查證人民身分，得採取下列之必要措施：一、攔停人、車、船及其他交通工具。二、詢問姓名、出生年月日、出生地、國籍、住居所及身分證統一編號等。三、令出示身分證明文件。四、若有明顯事實足認其有攜帶足以自殺、自傷或傷害他人生命或身體之物者，得檢查其身體及所攜帶之物。依前項第二款、第三款之方法顯然無法查證身分時，警察得將該人民帶往勤務處所查證；帶往時非遇抗拒不得使用強制力，且其時間自攔停起，不得逾三小時，並應即向該管警察勤務指揮中心報告及通知其指定之親友或律師。」據此，警察僅得以詢問及令出示身分證件之方式來查證身分。

詢問係指以口頭發問。詢問在身分查證程序中相當重要，若詢問得體，不僅可有效的快速確認受檢人身分，亦可於短時間內發現即將發生的危害或犯罪。詢

¹⁰⁹ 林裕順，前揭註 99，頁 25。

¹¹⁰ 林裕順，前揭註 99，頁 25-26。

問過程中，為確認受檢人陳述內容的正確性，必要時得令受檢人出示得證明身分之文件，但這並不表示詢問程序必然伴隨著令出示證明文件之程序，相反，此二程序係兩個獨立之程序，非必然緊接進行¹¹¹。若警察於詢問程序中已消除對受檢人的合理懷疑時，可不要求其出示證明文件¹¹²。而令出示身分證明文件，是指令受檢人提出其身分證明文件。所稱「身分證明文件」，並不以「官方證件」為限，但若證件之可信度低，或無照片等其他資料供臨檢警察核對時，即非適宜之證明文件¹¹³。

詢問及令出示證明文件，此二種查證身分之方式，共通點為行為時，警察係立於主動地位，要求相對人提供所需的資料。此舉使警察與受檢人雙方均會知悉提供了何種資料，而受檢人亦得控制其所提供的資料內容與種類，並拒絕提供無關之資料，但警察若是使用人臉辨識系統查證身分，則與本條所稱以詢問及令出示身分證件的方式查證身分，有所出入，概念上無法包括人臉辨識系統的使用。

（五）警職法其他與資料蒐集相關規定

由於警察係將人臉辨識系統用作查證身分的手段，換言之，亦是作為一種資料蒐集的手段。因此，除了前述警職法第 6 條及第 7 條外，於本法第二章有關身分查證及資料蒐集之相關規範（第 6 條至第 18 條）及第三章有關即時強制的規範（第 28 條），亦有可能作為警察使用人臉辨識系統的法律依據，以下將逐一說明可能與此應用有關之條文，例如：第 8 條、第 9 條、第 10 條、第 11 條及第 28 條。

1. 警職法第 8 條第 1 項第 1 款：針對交通工具之檢查

¹¹¹ 蔡震榮，前揭註 96，頁 130。

¹¹² 林明鏞（2011），《警察法學研究》，頁 152 以下，臺北：新學林。

¹¹³ 蔡震榮，前揭註 96，頁 130。

警職法第 8 條規定：「警察對於已發生危害或依客觀合理判斷易生危害之交通工具，得予以攔停並採行下列措施：一、要求駕駛人或乘客出示相關證件或查證其身分。二、檢查引擎、車身號碼或其他足資識別之特徵。三、要求駕駛人接受酒精濃度測試之檢定。警察因前項交通工具之駕駛人或乘客有異常舉動而合理懷疑其將有危害行為時，得強制其離車；有事實足認其有犯罪之虞者，並得檢查交通工具。」其中，與人臉辨識系統的使用有關者，為本條第 1 項第 1 款「要求駕駛人或乘客出示相關證件或查證其身分」，究竟本款所稱查證身分之手段可否包括人臉辨識系統的使用？

首先，本條與第 6 條及第 7 條有別，本條係專門針對「交通工具」的檢查，而第 6 條及第 7 條則是有關「人」的查證身分。但實際上，交通工具也是由「人」所駕駛，因此，本條主要也是針對車上之人加以查證，結果上與第 6 條及第 7 條並無不同¹¹⁴。惟本條畢竟係針對交通工具的檢查，為與第 6 條及第 7 條之情形加以區別，亦有特殊規定，針對交通工具之檢查限於「已發生危害或依客觀合理判斷易生危害之交通工具」始可。所稱「客觀、合理判斷易生危害」係指警察依據客觀事實及專業經驗合理判斷，認為該交通工具有易生危害之情事¹¹⁵。

由此可知，本條與第 6 條及第 7 條不同之情形在於加入交通工具，而針對交通工具的檢查有特別規定，與第 6 條及第 7 條對人之檢查加以區別。惟實際上，該特別規定係針對「交通工具」而非針對人，實際上針對交通工具的檢查主要也是對車上之人加以查證身分，既然特別規定係因交通工具的加入而訂定，而非針對人，因此，本文認為本條第 1 項第 1 款查證身分得使用的手段，應與第 7 條對人檢查得使用的手段相同。而如前述，本文認為第 7 條查證身分得使用的手段並不包括人臉辨識系統的使用，則本條第 1 項第 1 款亦無法作為警察使用人臉辨識

¹¹⁴ 蔡震榮，前揭註 96，頁 138。

¹¹⁵ 蔡震榮，前揭註 96，頁 138。

系統的法律依據。



2.警職法第 9 條至第 11 條：以「科技工具」蒐集資料

警職法第 9 條係針對警察於集會遊行或其他公共活動時蒐集資料的規定，本條第 1 項規定：「警察依事實足認集會遊行或其他公共活動參與者之行為，對公共安全或秩序有危害之虞時，於該活動期間，得予攝影、錄音或以其他科技工具，蒐集參與者現場活動資料。資料蒐集無法避免涉及第三人者，得及於第三人。」；第 10 條則是裝設監控設備之要件，本條第 1 項規定：「警察對於經常發生或經合理判斷可能發生犯罪案件之公共場所或公眾得出入之場所，為維護治安之必要時，得協調相關機關（構）裝設監視器，或以現有之攝影或其他科技工具蒐集資料。」；第 11 條則是針對警察犯罪情報之蒐集，本條第 1 項及第 2 項規定：「警察對於下列情形之一者，為防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動：一、有事實足認其有觸犯最輕本刑五年以上有期徒刑之罪之虞者。二、有事實足認其有參與職業性、習慣性、集團性或組織性犯罪之虞者。前項之期間每次不得逾一年，如有必要得延長之，並以一次為限。已無蒐集必要者，應即停止之。」

警職法第 9 條至第 11 條，授權警察在滿足各規範之前提要件下，得用「科技工具」蒐集所需之資料，且蒐集期間及資料之銷毀均有規範。則此處所指的「科技工具」是否包括人臉辨識系統的使用？由法條文字觀之，「科技工具」當然包括人臉辨識系統的使用，並無排除之理；惟若以立法背景而論，警職法係於 2003 年立法，而彼時人臉辨識系統的使用尚未普及，技術尚未純熟，警察或沒想到將人臉辨識系統作為資料蒐集之手段，因此，「科技工具」或未包括人臉辨識系統的使

用。本文以為，人臉辨識系統係用於身分識別的技術，主要用來辨識及查證身分，而如前述，警職法第 7 條查證身分的手段並未包括人臉辨識系統的使用，若此處的「科技工具」包括人臉辨識系統的使用，將間接承認警察得使用人臉辨識系統查證民眾身分，而與前述的法規範不一致，因此本文認為，此處「科技工具」應不包括人臉辨識系統的使用。

3. 警職法第 28 條：概括授權規範？

警職法第 28 條規定：「警察為制止或排除現行危害公共安全、公共秩序或個人生命、身體、自由、名譽或財產之行為或事實狀況，得行使本法規定之職權或採取其他必要之措施。警察依前項規定，行使職權或採取措施，以其他機關就該危害無法或不能即時制止或排除者為限。」本條的立法理由有三：一為個別法律賦予職權，乃依法行政之表現。惟社會政經文化等之變遷快速，法律一時自難以因應，若出現新興危害而不予處理，即無從維護公共安全與秩序，個人生命、身體、自由、名譽與財產，亦無法受到應有之保障，自非人民之福。此時若要求警察出面處理，自亦應賦予其相應之職權。爰參考德國警察法標準草案第 8 條第 1 項規定，於第 1 項予以明定。再者，危害之發生，可能係人之行為所肇致，亦有可能係物之狀況引起。第一項所稱行為，係指前者；所稱事實狀況，係指後者而言。最後，新興之危害，非必屬警察任務範圍。此時本應由各該任務機關自行處理。但實務上，一般民眾遇有危害，多求助警察。抑且各該任務機關，非如警察接近民眾且二十四小時服勤，遇有危害必俟其到場處理，殆屬不可能，且有些危害之制止或排除，間不容髮，各該任務機關勢難克竟全功。為維持行政之一致性。並填補人權保障之闕漏，由警察適時補充介入，有其必要。爰參考德國警察法標準草案第 1 條之規定，爰於第 2 項予以明定。

本條有認係警察的概括條款者，植基於立法理由第一點及第二點。本條列於「即時強制」章中，實為條文位置規定不當，本條為針對警察職權「具體措施」，或稱警察「類型化措施」的補充性條款，而警職法第 2 條已對警察職權「具體措施」加以規定，本條作為補充性的概括條款，應規定於其後較為恰當¹¹⁶。惟亦有採不同之見解者，認為本條係屬於即時強制的「概括條款」，適用範圍僅限於即時強制。基於體系解釋，本條既規定於「即時強制」章中，而非「總則」章中，應認為此規定並非權限的一般授權條款，而是即時強制的「其他補充條款」，藉以因應急迫性授權措施的不足，否則應移列「總則」章中。再者，由於新興的危害不斷發生，於事態緊急時，為使警察得採取一切必要的手段以茲因應，於即時強制章中，針對警察即時強制權限，為破除執行方法列舉原則，而訂定一般概括授權條款¹¹⁷。本文亦認為本條之規定，並非是警察一般權限的概括授權規範。除基於體系解釋，既本條係規範於即時強制章而非總則章中，本條的適用僅限於即時強制之情形。即時強制由於事態緊急或是事出突然，為使警察能夠有效因應此一緊急且急迫性之情形，手段上須有一定的彈性空間，因此訂定概括授權條款，讓警察得使用一切必要的手段以茲因應。再者，雖由於經濟文化快速變遷若不給予警察概括性之權限，以制止或排除人民之危害，或將增添警察勤務執行上之困難，惟若在警察缺乏對於概括條款的「補充性」與「承接性」之認識且救濟管道未暢通的情況下，實施概括授權條款，將導致本條款濫用之可能，進而產生衝擊¹¹⁸。因此，本文認為，本條並非警察權限的一般授權條款，而係即時強制的「概括授權條款」，換言之，本條的適用範圍僅限即時強制之情形，為使警察於緊急且急迫的情形下能夠適當的因應，因此賦予警察得使用一切必要手段因應。

¹¹⁶ 蔡震榮，前揭註 96，頁 242。

¹¹⁷ 林明鏘（2006），〈論警職法第 28 條之權限概括條款與補充性原則〉，《警察法學》，第 5 期，頁 19。

¹¹⁸ 李震山（1998），《警察任務法論》，四版，頁 160-163，高雄：登文書局。

綜上，警職法第 28 條並非警察一般權限的概括授權條款，反之，本條的適用範圍僅限於即時強制。職是之故，若符合即時強制的前提下，警察或得依本條之規定使用人臉辨識系統查證身分，惟依我國目前警察人臉辨識系統的使用情形，實則難以想像該系統作為制止或排除現行危害公共安全的工具。

第二項 警政署針對人臉辨識系統使用的內控規範

人臉辨識系統為 M-Police 警用行動載具的功能之一，而 M-Police 整合數機關數個資料庫，此一設備具龐大的後端資料庫，可提供查詢項目有：查捕逃犯、失蹤人口、應受尿液採驗人、遺失身分證、逃逸外勞、中輟學生、治安顧慮人口、失竊汽機車、戶籍、車籍、身分證統一編號變更、典當紀錄、前科、國人相片、治安顧慮人口相片、大陸行方不明人士相片、逃逸外勞相片、脫離兒少、緊急求救、治安資訊頻道、刑案紀錄、失蹤人口影像等。由於 M-Police 內建龐大的資訊，因此警政署為監督該設備的使用情形，亦訂有警用行動電腦使用管理要點、警察機關資訊安全實施規定及警政日誌管理系統作業規定等技術性行政規則，確保資訊安全及監督和管理人員使用 M-Police。以下將介紹上述的內部行政規則。

一、警用行動電腦使用管理要點

警用行動電腦使用管理要點（下稱管理要點）係於 2009 年 4 月 16 日由警政署以警署資字第 0980084670 號函發布全文共 9 點，迄今經 3 次修正，最近一次修正為 2012 年 5 月 8 日，以警署資字 101081198 號函修正該管理要點，本文則介紹後者，2012 年版本的管理要點。

該管理要點係警政署為律定各級警察機關警用行動電腦的使用及管理權責以及確保人民資訊隱私權及維護機關資訊安全所訂定的內部行政規則，不具對外性，

且該管理要點，如前述，主要係針對 M-Police 的使用、管理權限以及設備的維護，屬於警政署內部的技術性行政規則，而不具對外性。而此處所指的警用行動電腦，不僅包含本文的 M-Police 警用行動載具，尚包括手持行動電腦以及智慧型手機等警用電子配備。該管理要點簡介如下：

（一）安全管制方面：

各設備使用單位應律定專責保管人，負責該單位之設備保管、註冊、資料更新、列印日誌及使用人員管理等工作。而各設備使用單位專責保管人應於每月十日前下載前一個月之警用行動載具及智慧型手機查詢紀錄電子檔，下載線上查詢部分即可，並儲存於個人電腦或其他資料儲存媒體內，以供使用人員查閱，並由單位主管稽核管考，做成稽核書面紀錄備查，且相關查詢紀錄電子檔應妥善保存五年供資安稽核。且未經本署同意，不得擅自拆裝硬體配備、安裝軟體、或任意變更系統環境設定，亦不得擅自連接非警察機關之電腦設備。

（二）使用管制方面：

設備之使用限於警察機關所屬人員執行勤務或維護治安之目的，不得做目的以外之運用；警用行動電腦應建立登錄碼、帳號或密碼等身分鑑別機制，使用者應善盡保管個人鑑別資訊的責任，並依相關規定使用，以明責任，且不得有使用他人登錄碼、帳號或密碼之情事，使用者於使用完畢後，應登出系統。執勤領用及退勤繳還警用行動電腦時，均應於員警出入及領用槍彈、無線電、行動電腦登記簿上記錄。而執勤領用警用行動電腦，應持領機證向保管或值班人員領取，保管或值班人員應清點及管理領取情形，及彙齊保管領機證列入交接管理；退勤應立即繳還警用行動電腦並取回領機證。警用行動電腦原則僅限公務使用，倘欲於

勤餘時領用以辦理公務，應填具申請表單，並經單位主管核准。



(三) 資料保護方面，警用行動電腦內之資料列為一般公務機密；在資產管理方面，設備使用單位對警用行動電腦應予列冊管理。

(四) 罰則：

未定期下載查詢紀錄電子檔供使用人員查閱、查詢紀錄電子檔未妥善保存五年、單位主管未管制前述作為或未依規定辦理稽核工作、服勤攜出使用或退勤繳回未於登記簿登錄或置放領機證，半年累計達三次、使用他人登錄碼、帳號或密碼登入系統、擅自將設備借予非警察機關所屬人員使用、遺失警用行動電腦或勤畢未依規定繳回或非因公務攜出者，使用者有上述違反情事者，核予申誡處分；而非法複製或洩漏警用行動電腦資料者，核予記過處分；違反本管理要點，致生洩(失)密事件或使資訊系統遭受破壞者，將追究疏失人員之行政及刑事責任。

二、警察機關資訊安全實施規定

警察機關資訊安全實施規定（下稱實施規定）係警政署於 2008 年 3 月 6 日以警署資字 0970039156 號函發布，全文共 25 點。警政署為促進各警察機關制訂資訊安全政策，建立資訊管理制度，採行適當必要之資訊安全政策，確保資訊蒐集、處理、傳送、儲存及流通之安全而訂定的內部行政規則。該實施規定係針對 M-Police 系統的維護以及內建資料的管理等技術性事項，亦屬警政署內部的行政規則。由於該實施規定係發布於個人資料保護法修正施行前，而於個人資料保護法施行後未再行修正，因此實施規定仍使用個資法舊時的稱呼電腦處理個人資料保護法，該實施規定簡介如下：



（一）資訊安全措施的建立及相關法規的參酌

警察機關資訊安全維護，應依據電腦處理個人資料保護法（現今個人資料保護法前身）、國家機密保護法與行政院及所屬各機關資訊安全管理要點等有關法令，衡酌機關業務需求，參考本實施規定訂定資訊安全政策，研訂資訊作業之安全水準，並以書面、電子或其他方式通知所屬員工及有關機關（構）；具體資安措施包括：實施資訊資產安全分級管理措施，而該管理措施需訂定資訊安全等級分類標準，並建立資訊資產目錄包括資訊資產項目、保管者及安全等級分類等以及需將資訊及系統之輸出資料，標示適當安全等級及保護措施，以利使用者遵循。（實施規定第 3 點及第 5 點）

（二）資訊安全防護措施

資訊系統應具 5 項安全保護功能，分別為：密碼保護、檔案管理系統保護、系統使用權限管理、資料庫管理系統保護、各項應用作業系統之電腦主機，應全日二十四小時自動記錄每一帳號查詢及更新資料之時間、種類、內容及結果，並保留五年，以資查考。於軟體程式方面，作業軟體應建立使用權限，避免非業務權責人員閱覽、擷取或破壞；軟體程式之儲存應由系統人員規劃及配置，並建立檔案識別辨證，限制非該系統之軟體程式擷取或破壞，再者，為能迅速處理故障，並恢復正常使用，作業軟體應訂定故障復原程序。於資料的建置上，各機關建置資料時，應依業務需要建立使用權限，避免非業務權責人員閱覽、擷取或破壞。（實施規定第 6 點、第 7 點及第 8 點）

（三）安全管制措施



本署每六個月應配賦專屬電腦系統線上作業密碼，由各機關依工作需要分配使用，不得浮濫，並嚴禁多人使用同一密碼；各機關應將密碼使用名冊或電子檔（磁片、光碟）保留五年，於每半年配賦新密碼時，舊密碼使用名冊或電子檔（磁片、光碟）應併同配賦新密碼之公文送檔案室歸檔備查；專屬電腦系統線上作業密碼，如有洩密之虞，使用者應立即申請撤銷該密碼，密碼使用者因業務調整、調職、停（離）職時，管理者亦應立即依規定申請撤銷該密碼。針對網路的安全管制措施則有：對外開放資訊系統如涉及私人資料檔案，應以加密方式處理；系統管理者應隨時注意警示訊息，檢測安全防護措施，即時修補各項系統漏洞；各機關不得開放與外界連線作業，如有連線需求，應做安全評估，並訂定資訊安全管制規定，報經本署核准後實施；提供給內部人員使用之網路服務，與開放有關人員從遠端登入內部網路系統之網路服務，應嚴格執行身分辨識作業，進行安全控管；使用者因業務調整、調職、停（離）職時，管理者應立即申請撤銷其使用者帳號，並依機關資訊安全規定及程序，取消其存取網路之權限。於網站的安全管制上，網站首頁須具備即時自動復原機制；網站資料應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料不得上網公布；網站管理者應定期檢核相關日誌檔，遇有異常時，應立即採取有效因應措施。（實施規定第 9 點、第 10 點及第 11 點）

（四）警察機關資料維護、輸出之規定

1. 資料維護方面，資料應依電腦處理個人資料保護法（現今個人資料保護法前身）規定維護正確，於發現資料錯誤時，應依各作業之規定，檢附正確資料，送相關單位辦理更正，且具機密性及敏感性資料或文件，不得存放在對外開放資訊系統中。（實施規定第 8 點第 8 款及第 11 款）

2.資料輸出安全管制方面，經由電腦設備查得之資料，不得擅自拷貝或外洩。(實施規定第 9 點第 1 款)



(五) 網路使用者之管理規定

不得以任何方法竊取他人之登入帳號與密碼；使用者應確實遵守安全規定，如有違反網路安全情事，將限制或撤銷其網路資源存取權利。(實施規定第 14 點)

(六) 罰則

違反本實施規定者，將追究其行政疏失責任；如致生洩密或資訊系統遭受破壞，致觸犯刑事法令者，並依各該法令查究處理。(實施規定第 25 點)

三、警政日誌管理系統作業規定

警政日誌管理系統作業規定(下簡稱作業規定)係警政署為強化員警正確使用警政資訊系統查詢資料作業，並推動警政日誌管理系統(以下簡稱本系統)，督促機關及所屬人員確實依法行政，防止濫用或侵害個人資料隱私，確保民眾個人資料安全，維護警察整體形象而訂，全規定共計 15 條。該作業規定係為監督各設備的使用情形，並將各項查詢紀錄加以建檔，以供日後稽核。以下將簡介該作業規定：

(一) 日誌電子檔之內容

日誌電子檔的內容包括：警察機關單位名稱、使用日期、使用者、IP、查詢作

業、委託查詢者、委託單位、用途及查詢內容（作業規定第 3 條）



（二）警政日誌管理系統的維運管理及使用權限單位及各單位所職掌之權限

1.中央層級為本署資訊室及本署各系統業務單位（以下稱稽核單位）：職掌權限應區分資訊室及稽核單位有所不同。資訊室負責指定專責人員管理本系統之查詢及資料運用情形；系統維運、使用權限管理、資料庫維護、系統監控等整體管理及教育訓練工作；各警察機關資訊單位查詢權限申請、審核與使用權限核發及管理；提供警察機關政風、督察單位、各級法院及檢察署來文調閱跨轄日誌資料及定期針對異常查詢稽核、不定期抽查稽核。而稽核單位則負責運用日誌管理系統之調閱查詢紀錄功能進行業管系統即時稽核；每月應依查詢紀錄電子檔，定期針對統計分析表異常之查詢數量、時間及對象之所屬人員進行稽核，有明顯不當情形時，應責成第一層單位進一步查處深入稽核。（作業規定第 4 條及第 5 條）

2.第一層（局級）為直轄市、縣（市）政府警察局及專業警察機關之資訊單位：負責所屬單位查詢權限申請、審核與使用權限核發及管理；檢核各警政資訊系統使用者之查詢權限，確認使用者對資訊查詢或存取是否合宜；人員離職或調整至與業務無關之職務時，應依規定撤銷相關查詢權限；運用日誌管理系統之調閱查詢紀錄及統計分析功能，落實執行各系統資料稽核；運用 e 網通日誌管理系統之異常查詢/查詢排名、線上調閱查詢/單位查詢作業種類功能，落實執行各系統資料稽核；提供各級法院及檢察署來文調閱日誌資料；需指定專責人員負責下載轄區內查詢紀錄電子檔，供資安稽核：e 網通日誌管理系統須在每月十日前下載前一個月查詢紀錄電子檔，並配發所屬；而日誌管理系統則須定期下載每月或特定期間查詢紀錄電子檔；每月應依查詢紀錄電子檔，抽檢警察局內勤及所屬外勤分局（含大隊及隊）各五分之一以上單位，且查核量達單位查詢紀錄總數之百分之二。稽

核結果應提報各機關局務會議檢討，並保存相關紀錄備檢。(作業規定第 4 條及第 6 條)



3.第二層(分局級)為分局之資訊單位：負責檢核各警政資訊系統使用者之查詢權限，確認使用者對資訊查詢或存取是否合宜，人員離職或調整至與業務無關之職務時，應依規定提出撤銷相關查詢權限；運用日誌管理系統之調閱查詢紀錄及統計分析功能，落實執行資料稽核；指定專責人員應定期下載每月或特定期間轄區內查詢紀錄電子檔，供資安稽核；每月應依查詢紀錄電子檔，抽檢分局內勤與所屬外勤分駐所、派出所及隊各五分之一以上單位，且查核量達單位查詢紀錄總數之百分之二。(作業規定第 4 條及第 7 條)

4.第三層(所級)為分駐所及派出所：負責運用日誌管理系統之調閱查詢紀錄功能，進行即時稽核；每月應依查詢紀錄電子檔，定期針對統計分析表異常之查詢數量、時間及對象之所屬人員進行稽核，員警人數二十人以下者，應稽核至少一人；二十一人以上未滿四十人者，應稽核至少二人，依此類推，有明顯不當情形時，應陳報分局進行複查，並深入稽核。(作業規定第 4 條及第 8 條)

(三) 稽核措施

1.警政署資訊室得定期或不定期辦理督考各警察機關執行情形；直轄市、縣(市)政府警察局及專業警察機關應依本署維護個人資料安全專案稽核計畫配合辦理稽核；發現有異常查詢時，得調閱相關查詢紀錄，進行調查。(作業規定第 11 條)

2.警政署每年上半年及下半年針對特定機關各實施定期書面稽核一次，並不定時實施實地機動稽核，受檢單位之整備資料，應以電子檔陳報本署受檢。而受檢資料依層級不同，有所區別。若為受檢單位為第一層(局級)，每月依查詢紀錄電子檔，



抽檢警察局內勤及所屬外勤分局（含大隊及隊）各五分之一以上單位，且查核量應達單位查詢紀錄總數之百分之二，稽核結果應提報局務會議檢討，並保存相關紀錄備查。若為第二層（分局級），每月應依查詢紀錄電子檔，抽檢分局內勤與所屬外勤分駐所、派出所及隊各五分之一以上單位，且查核量應達單位查詢紀錄總數之百分之二，稽核結果應提報分局主管會報檢討，並保存相關紀錄備查。第三層（所級）則每月應依查詢紀錄電子檔，定期針對統計分析表中異常之查詢數量、時間及對象之所屬人員進行稽核，員警人數二十人以下者，應稽核至少一人；二十一人以上未滿四十人者，應稽核至少二人，依此類推，有明顯不當情形時，應陳報分局進一步查處深入稽核。除此之外，將實施不定期實地機動稽核，除年度定期實施稽核外，針對發生較多案件之特定機關，本署資訊室及政風室應組成特定機關日誌稽核小組，實施現地機動稽核。例外情形，如各系統另有稽核規定，且稽核頻率及內容較本規定嚴謹者，則該系統毋需重複執行本規定稽核事宜。（作業規定第 13 條）

3.特定機關經警政署函發通知後，應於文到一個月內（遇假日順延之），將前半年度辦理情形填報警察機關加強警政日誌管理系統稽核工作自評表（以下簡稱自評表），連同相關佐證資料陳報本署，俾利本署資訊室及政風室實施審核作業及考核評定執行成效。無正當理由未依規定於期限內陳報自評表及受檢資料者，將追究相關人員行政責任，業務主管申誡二次；承辦人員記過一次。（作業規定第 14 條）

（四）罰則

未依本規定方式作業，資訊業務主管及資訊業務承辦人員，各申誡二次；對於上級機關交查其機關內發生之洩密案件，未盡調查或處理之責，或事後未盡防護之責者，資訊業務主管及資訊業務承辦人員，各申誡一次。（作業規定第 15 條）



第三項 小結

第一款 人臉辨識系統作為查證身分之手段與警職法規定間的

扞格

(一) 當事人同意無法取代法律明文規範

縱使警察使用人臉辨識系統係以取得當事人同意為前提，惟該同意可能係當事人為避免被帶往勤務處所，為避免其人身自由受限而不得已為之，具辦強迫性色彩，且由於 M-Police 人臉辨識系統使用內政部戶政司國民身分證相片資料建置人臉資料庫，以致該系統一經使用，潛在影響者將不計其數，加上該系統所引發的重大社會爭議性、以及其對基本權所造成之影響，本文認為在我國法律保留原則之範圍深受重要性理論之影響下，此一原則的適用範圍已擴張至給付行政之領域，不以干預行政為限，此一應用仍應有法律明文規定始可。因此警察使用人臉辨識系統仍應有法律明文規定始可，而本文著重警察基於危害防止的目的使用人臉辨識系統，而警察執行危害防止任務（臨檢）的法律依據為警職法，因此該應用可能的法律依據為警職法的相關規定。

(二) 臨檢基於其權利侵害性，因此屬於強制手段，實施要件須有法律明確規定

據釋字第 535 號的解釋意旨，警察臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，均屬對人或物之查驗、干預，將影響人民行動自由、財產權及隱私權等基本權利甚鉅，因此立法者無授權警察人員得任意實施之本意，執行各種臨檢應恪遵法治國家警察執勤之原則，實施臨檢之要件及程序應有法律之明確規範。職是之故，臨檢基於其權利侵害性，屬於強制手段，實施臨檢的要件



及手段均須有明確的法律規定，查證身為臨檢的一環，亦同。警職法第 6 條及第 7 條明確規定警察實施查證身分的要件及手段，尤其是針對手段，警職法第 7 條第 1 項第 2 款及第 3 款明定，警察為查證人民身分得詢問姓名、出生年月日、出生地、國籍、住居所及身分證統一編號等及令出示身分證明文件。而詢問及令出示身分證件此二種方式，與警察使用人臉辨識系統查證受檢人身分並不相同，使用此一系統無須詢問亦無須受檢人出示身分證件，只要出現比對結果，系統會直接顯示受檢人的身分資訊，受檢人對於警察所取得的個資種類將失去控制權。再者，就權利侵害程度而言，詢問姓名抑或出示身分證件，對於受檢人的隱私侵害程度不及人臉辨識系統，依舉輕以明重之法理，既隱私侵害程度較輕微的手段都須法律明文始可為之，則隱私侵害程度較重者，亦須法律明文始可。

（三）警察如欲合法使用人臉辨識系統查證身分，應有法律明文准許警察使用人臉辨識系統之依據

綜上可知，現行警職法第 6 條及第 7 條有關身分查證之要件及手段之規定，尤其針對查證身分之手段，概念上無法涵括將人臉辨識系統作為查證身分之手段，除此之外，警職法第 8 條、第 9 條至第 11 條有關資料蒐集的規範以及第 28 條即時強制的概括授權條款亦無法支撐此一應用，因此現今警察使用人臉辨識系統查證身分，實則背後並無任何明文規範以為支撐。本文認為，正因現行法律並無明文准許警察使用人臉辨識系統之規範，但鑒於人臉辨識系統所產生的龐大優勢仍促使警察採取折衷之方式，以取得當事人同意為前提，強行導入人臉辨識系統的使用，才會引發若在當事人同意下使用人臉辨識系統查證身分是否需要法律依據之爭議。因此，為杜絕爭議及基於人臉辨識系統所導致的社會爭議性，本文認為，此一應用仍應有明確法律依據始可。

第二款 警政署針對人臉辨識系統使用內控措施的缺失



綜合前揭第一項及第二項之討論，於法制上，目前警察使用人臉辨識系統查證身分，係以警職法為中心，並搭配警用行動電腦使用管理要點、警察機關資訊安全實施規定及警政日誌管理系統作業規定此三個警政署內部行政規則建立內部監督制度，針對 M-Police 的系統及使用者訂定相關資訊安全維護及使用規範，亦針對違反內部規定的使用者及監督者訂定相應之罰則，以確保資訊安全及保障民眾資訊隱私權。惟本文認為警政署之內部規定雖就使用者及系統的資訊安全及管理措施均有相應之規定，例如：相關查詢及設備使用資料均需建檔，並搭配定期及不定期的稽核制度。使用者須遵守設備之使用規定，若有所違背輕則申誡，重則小過，均訂有相應之罰則。針對資訊安全部分，亦參考個資法、國家機密保護法等法律，建立系統加密、強化系統身分辨識功能等。

綜觀我國警政署針對人臉辨識系統使用的內控措施，可歸納為兩種方式：使用（或查詢）紀錄的保存以及針對使用（或查詢）紀錄指定專責人員定期稽核。本文認為，針對警政署的內控措施，首先，缺少資料保存的規範，亦即，內部規定僅提及使用者的查詢及設備使用紀錄將予以建檔並保留 5 年，但漏未規定，對於電子設備的資料以及人臉辨識系統所蒐集的人臉特徵資料的資料保存情形。以英國南威爾斯警局為例，其人臉辨識系統的資料保存時限依其 2018 年所公布 SWP's Standard Operating Procedures 及 Data Protection Impact Assessment 之規定，若為搭載人臉辨識功能的固定式閉路監視錄影機（CCTV）其電磁紀錄將保存 31 天，爾後系統將自動刪除；未比對成功的臉部影像資料則是立即刪除；生物特徵資料（此指臉部特徵資料），無論有無比對成功，立即刪除；比對成功的臉部影像資料，則於人臉辨識系統使用完畢後立即或於其後 24 小時內刪除；比對成功後所發布關於個人資料的警示，將保留 31 天；人臉資料庫中的相片影像以及生物特徵

資料，將於人臉辨識系統使用完畢後立即或於其後 24 小時內刪除。反觀我國並未有相關之規範，因此無從得知，系統的資料保存情形，最嚴重的情況，便是系統的資料永不刪除，因此警政署將永久保存所取得關於民眾的人臉特徵資料。再者，上述的行政規則，亦非全部均是公開可於網路上查找，警政日誌管理系統作業規定即非公開之內部行政規則，因此，民眾並非能夠全然了解警政署內部如何維護 M-Police 人臉辨識系統。資訊的不透明亦非僅體現於行政規則上，針對人臉辨識系統使用的稽核結果及相關文件，若警政署不主動公開，此內部文件，民眾亦難以知悉，因此將造成對於警政署使用人臉辨識系統的情形一無所知的窘境，不利於建立民眾對於該系統的信心。

第三節 警察使用人臉辨識系統與比例原則

退步言之，即使採取基於警察使用人臉辨識系統查證身分係以取得當事人同意為前提，由於當事人係出於自由意志而拋棄基本權保護，因此縱無法律依據，警察亦可使用人臉辨識系統查證民眾身分的立場。此一應用尚須符合比例原則之要求，法律保留係探討此一應用是否應以有法律依據為前提，而比例原則係評估此一應用的實效性，二者所關注的重點並不相同。

憲法第 23 條規定：「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。」據此，欲限制基本權之保護，除法律保留原則外，亦須滿足比例原則之要求。比例原則在運用上首先必需確定所欲追求的目的或結果是合於法律規定始可；此外尚有三個子原則，分別為手段的適合性，即手段要有助於結果的達成；手段的必要性，即已經沒有其他對於國民權利影響最小的手段時，始能適用；手段的妥當

性（狹義比例原則），即手段與結果間要合乎比例¹¹⁹。



警察使用人臉辨識系統查證身分，於比例原則的檢驗上，須探討人臉辨識系統的使用與犯罪預防目的達成間的關係。而人臉辨識系統又涉及人臉特徵資料此一高度人別識別性個資的蒐集利用，參酌釋字第 603 號理由書中對於戶政機關如欲蒐集高敏感個人資料與比例原則間的關係，其指出：「隱私權雖係基於維護人性尊嚴與尊重人格自由發展而形成，惟其限制並非當然侵犯人性尊嚴。憲法對個人資訊隱私權之保護亦非絕對，國家基於公益之必要，自得於不違反憲法第 23 條之範圍內，以法律明確規定強制取得所必要之個人資訊。至該法律是否符合憲法第 23 條之規定，則應就國家蒐集、利用、揭露個人資訊所能獲得之公益與對資訊隱私之主體所構成之侵害，通盤衡酌考量。而指紋係個人身體之生物特徵，因其具有人各不同、終身不變之特質，故一旦與個人身分連結，即屬具備高度人別辨識功能之一種個人資訊。由於指紋觸碰留痕之特質，故經由建檔指紋之比對，將使指紋居於開啟完整個人檔案鎖鑰之地位。因指紋具上述諸種特性，故國家藉由身分確認而蒐集個人指紋並建檔管理者，足使指紋形成得以監控個人之敏感性資訊。國家如以強制之方法大規模蒐集國民之指紋資料，則其資訊蒐集應屬與重大公益之目的之達成，具備密切關聯之侵害較小手段，並以法律明確規定之，以符合憲法第 22 條、第 23 條之意旨。」據此，公務機關如蒐集利用高敏感個資，於比例原則的檢驗上，係採取中度審查標準。職是之故，警察使用人臉辨識系統查證身分，如欲符合比例原則之要求，須該系統之使用有助於重大公益目的的達成，二者間具備密切關聯，且使用上不得逾越必要之程度，警察此一應用始可滿足比例原則之要求。

¹¹⁹ 馬興平（2008），《論資訊隱私權的保護-從釋字第 603 號解釋出發》，頁 96，國立中正大學法律所碩士論文。



第一項 警察使用人臉辨識系統的評估

針對比例原則的分析，實為警察使用人臉辨識系統查證身分的總體評估，包含該系統的使用效率、優勢及缺失等。該系統啟用自今已逾五年，本文將由效益面及技術面兩方面切入分析。

（一）效益面

1.人臉辨識系統的普及化

人臉辨識技術自 1970 年發展至今，迄今已逾 50 年，技術日趨成熟，現今人臉辨識技術的甚至已可有高達 99.8% 的辨識率。根據 CB Insights 的 AI 發展趨勢報告，人臉辨識在 2019 年已經成為人工智慧（Artificial Intelligence，下簡稱 AI）發展最具規模且普及度高的科技；同時，調研機構 Variant Market Research 數據顯示，人臉辨識市場規模預計將在 2024 年達到 154 億美元¹²⁰。而我國不論公領域亦或是私領域，對於人臉辨識系統的使用並不陌生，於公領域，例如：內政部移民署於 2012 年 1 月 1 日開始啟用「自動查驗通關系統」，以採集臉部特徵的方式，加速國人或有居留權的外籍人士的通關作業，而自動查驗通關系統並非強制使用，在使用該系統前，使用者須先自願向移民署登記後，方能啟用¹²¹；於私領域上，例如：蘋果手機 iPhone X 推出 Face ID 臉部辨識功能、校園或職場的自動門禁或是打卡系統以及中國信託商業銀行的「智能 ATM」等均可見到人臉辨識系統的身影。人臉辨識系統於近年來，開始漸漸普及，走入大眾的視野。人臉辨識系統不論是對人民或是對公務機關而言，並不陌生。

¹²⁰ 聯合新聞網，<https://udn.com/news/story/6868/4145079>（最後瀏覽日：06/17/2020）。

¹²¹ 台灣人權促進會，<https://www.tahr.org.tw/news/2288>（最後瀏覽日：06/17/2020）。

2.M-Police 人臉辨識系統的使用，對於警察於臨檢時查證民眾身分大有助益



警政所使用的 M-Police 人臉辨識系統，配合人臉辨識技術的提升，加上於比對前可縮小條件限縮比對範圍，有效提高系統準確率。該系統對於協助走失年長者返家有莫大助益，新聞中亦不乏成功之實例（例如：協助一名略有失智的 63 歲羅姓老翁返家¹²²、協助一名輕微精神障礙婦女¹²³以及協助身體不適年長者¹²⁴），縱使是長相極為相似的雙胞胎該系統亦可成功辨識出二者身分¹²⁵。除此之外，基於臨檢客體及其犯罪預防目的之考量，該系統整合了戶政司國民身分證相片資料庫之資料作為人臉資料庫的建檔基礎，此舉有效提升警察的執勤效率以及節省確認民眾身分的時間成本，有助於犯罪預防目的的達成，能夠第一時間使用該系統掌握民眾身分。以往警察執行臨檢勤務欲查證民眾身分時，程序上須詢問受檢人之身分並要求其出示身分證明文件供核對，一來一往較為耗時，且還須慎防冒名之情形。導入人臉辨識系統之使用後，系統可於 30 秒內辨識出身分，並自動提供相關身分資料，且經由系統層層篩選以及前置的條件設定，可有效防止冒名之情形，提升警察的執勤效率，此一系統對於警察臨檢查證身分大有助益。

3.我國警察使用人臉辨識系統的情況對於人民資訊隱私權的限制程度較小

M-Police 人臉辨識功能自 2012 年啟用至今，已逾 5 年，依警政署的統計資料，該功能已累積逾 84 萬的查詢次數，且署內已有逾 1,5000 台 M-Police 供基層員警於執法時使用¹²⁶。相對於英國南威爾斯警局將人臉辨識系統與道路監視錄影器結

¹²² 桃園電子報，<https://tyenews.com/2020/05/63241/>（最後瀏覽日：06/21/2020）。

¹²³ 中國時報，<https://www.chinatimes.com/realtimenews/20200604005808-260402?chdtv>（最後瀏覽日：06/21/2020）。

¹²⁴ 桃園電子報，<https://tyenews.com/2020/03/53664/>（最後瀏覽日：06/21/2020）。

¹²⁵ 三立新聞網，<https://www.setn.com/News.aspx?NewsID=400405>（最後瀏覽日：06/21/2020）。

¹²⁶ 財團法人臺灣網路資訊中心，

https://blog.twinc.net.tw/2019/09/11/4957/?fbclid=IwAR0G9eOmShU4pwx4PFvV3p4tKPm8N9DCyd_JiTMv9_n6lvm04LPsDeoM20M（最後瀏覽日：06/20/2020）。

合，進行大規模自動人臉偵測辨識，我國 M-Police 人臉辨識系統的使用，並未與任何監視錄影器結合，且一次僅可針對特定一人進行人臉辨識。除此之外，警察如欲使用 M-Police 人臉辨識系統查證身分，程序上須先依傳統模式仍無法查知其身分且在其同意的前提下始可使用該系統，該系統係立於輔助地位。簡言之，我國 M-Police 人臉辨識系統的使用，需警察特定目標客體，拍攝臉部特寫照片，且使用前尚會經受檢人的同意，非如英國警察機關般進行大規模自動針對不特定多數人的人臉偵測及辨識，因此就針對隱私侵害之程度而言，我國警察使用人臉辨識系統的情形對於隱私權侵害程度較輕微。

（二）技術面

人臉辨識系統於技術面上，除了準確率高低的疑慮外，由於該技術屬 AI 自動化決策的技術之一，因此尚有一個更為棘手的問題——演算法歧視 (Algorithm Bias)。演算法的歧視是近年來發展或是使用人臉辨識系統所遭遇的一大難題。

人臉辨識技術潛藏著所謂演算法歧視 (Algorithm Bias) 的問題。美國國家標準暨技術研究院 (NIST) 研究近兩百種臉部演算法後，發現人臉辨識系統在辨別非白人時會產生較大的誤差，因應人臉辨識被普及用在執法與身分辨識驗證，這項發現很有可能引發應用上的疑慮。根據《華盛頓郵報》報導指出，目前的人臉辨識系統，對亞裔、非裔美國人的誤判機率比白人高出 100 倍左右，NIST 驗證了目前的演算法中存在種族與性別偏見¹²⁷。而由於人臉辨識系統演算法歧視的問題，美國亞馬遜 (Amazon) 於 2020 年 6 月 20 日宣布將暫停警方使用人臉辨識系

¹²⁷ Yahoo 新聞，

<https://tw.news.yahoo.com/%E4%BA%BA%E8%87%89%E8%BE%A8%E8%AD%98%E7%B3%BB%E7%B5%B1%E4%B9%9F%E5%AD%98%E5%9C%A8-%E7%A8%AE%E6%97%8F%E6%AD%A7%E8%A6%96-%E7%A0%94%E7%A9%B6%E6%A9%9F%E9%97%9C%E8%A8%BC%E5%AF%A6-%E9%80%99%E9%A1%9E%E4%BA%BA-%E6%9C%80%E5%AE%B9%E6%98%93%E8%A2%AB%E8%AA%A4%E5%88%A4-100132805.html> (最後瀏覽日：07/07/2020)。



統執法，為期一年。除了亞馬遜之外，IBM 公司亦已於 2020 年 6 月 9 日宣布，將停止臉部辨識技術業務，擔憂這項技術可能會被用於大規模監視和種族歸納(racial profiling)¹²⁸。而 AI 的演算法歧視究竟如何發生？麻省理工學院媒體研究室的研究員 Joy Buolamwini 認為，由於人臉辨識背後的演算法，多由白人男性工程師寫的，而演算法要做出好的決策，就必須仰賴過往的資料所累積的經驗，而工程師也許無意識的讓自身的偏見、判斷影響演算法的運作，總而言之，若系統背後的科學家缺乏多元組成，某種程度上勢必也會影響演算法的運作¹²⁹。因此，從事 AI 的開發人員、研究人員和科學家之間需要更豐富的多樣性，要選擇與熟悉不平等、以及關注文化和社會領域的工程師或專家合作¹³⁰，才有可能降低 AI 演算法歧視的現象，但能否完全去除 AI 演算法歧視的現象則未可知。而針對人臉辨識系統演算法歧視的問題，英國高等法院王座分庭（High Court of Justice Queen's Bench Division）於 Bridges v. CCSWP and SSHD 一案中，其回應可總結為幾點：首先，雖經專家於庭上表示演算法歧視屬所有人臉辨識系統的共同特徵，亦經南威爾斯警局資訊科人員證實人臉辨識的結果確實女性辨識的錯誤率要較男性為高，但該科室的人員隨後亦證明此一結果的產生，並非肇因於演算法歧視，而是由於人臉比對資料庫中擁有相同臉部特徵的女性較男性為多，因此發生此一結果，與性別歧視無關。因此，僅靠不同性別辨識失誤率的高低，不足以證明英國警方所使用的人臉辨識系統有演算法歧視現象，仍有待更多的研究去證實。再者，由於警方所使用的人臉辨識系統確實存在女性辨識的錯誤率較男性為高的事實，亦經所屬資訊科人員的證實，因此英國警方或許會有進一步調查評估人臉辨識系統使用情形的必要，但針對此一問題更為妥適的回應，係設置一個中間審查機制，除非經系統操作員判定人臉辨識比對吻合的結果屬合理，否則不得對民眾採取進一步的

¹²⁸ 上報，https://www.upmedia.mg/news_info.php?SerialNo=89462（最後瀏覽日：07/08/2020）。

¹²⁹ 數位時代，

<https://www.bnext.com.tw/article/47297/researchers-combat-gender-and-racial-bias-in-artificial-intelligence>（最後瀏覽日：07/08/2020）。

¹³⁰ 台灣醒報，<https://anntw.com/articles/20191226-CKAu>（最後瀏覽日：07/08/2020）。

行為¹³¹。



縱然人臉辨識系統存有演算法歧視的疑慮，本文認為人臉辨識系統仍是一項具有莫大助益的科技，原因有以下：首先，演算法歧視的產生，其根源係來自人類社會的偏見以及歧視，因此只要人類社會存有歧視以及偏見，演算法歧視的現象幾乎是完全不可能消除，縱使加入具組成多樣化的設計團隊或是將人臉辨識的設計公開透明，亦無法保證能夠完全消除演算法歧視的現象。再者，不同人種或是性別之間辨識錯誤率的高低，不能排除係因人臉比對資料庫中有多筆共享相同臉部特徵的人或是其他因素（例如：臉部特徵不明顯等）所致，有時與歧視並無任何關係，因此機關所使用的人臉辨識系統是否確有演算法歧視的現象，僅靠錯誤率的高低並不足以證明，仍需有更多的資料加以佐證。即便該系統存在演算法歧視的問題，較為妥適的回應方式並非全然禁止該系統的使用，而係建立防護機制，由於演算法歧視之問題目前並無解決的方式，要求解決此一問題，無異於要求一項「完美」的科技，而其實防護機制便可有效緩和演算法歧視所造成的影響。英國南威爾斯警方便是採用此一機制，回應人臉辨識系統演算法歧視的問題，當人臉辨識系統出現比對吻合的結果時，系統操作人員（亦為警察）會再一次判定該比對結果的合理性¹³²。

第二項 警察使用人臉辨識系統的疑慮

由前節中可知，警察使用人臉辨識系統查證身分對於危害防止目的的達成確

¹³¹ 原文為「it will be appropriate for SWP to take account that whenever AFR Locate is used there is an important failsafe: no step is taken against any member of the public unless an officer (the systems operator) has reviewed the potential matched generated by the software and reached his own opinion that there is a match between the member of the public and the watchlist face.」R (Bridges) v CCSWP and SSHD [2019] EWHC 2341.

¹³² 原文為「if during a deployment of AFR Locate the software identifies a possible match between a face captured on the CCTV and an image on the watchlist, the two images are reviewed by an AFR operator (the system operator, who is a police officer) to establish whether he believes that a match has in fact been made. In our view, the fact that human eye is used to ensure that an intervention is justified, is an important safeguard.」R (Bridges) v CCSWP and SSHD [2019] EWHC 2341.



有實質上的助益，惟在採行中度審查基準的情形下，能否通過比例原則的檢驗則有疑慮。參酌釋字第 603 號解釋中，對於戶政機關蒐集指紋資料於比例原則上之檢驗，略以：「戶籍法第八條規定強制人民按捺指紋並予以錄存之目的，係為加強新版國民身分證之防偽功能、防止冒領及冒用國民身分證及辨識迷途失智者、路倒病人、精神病患與無名屍體之身分等，固不失為合憲之重要公益目的，惟強制全民按捺指紋並予錄存否則不發給國民身分證，仍不符合憲法第二十三條比例原則之限制。蓋就「加強國民身分證之防偽」及「防止冒用國民身分證」之目的而言，如欲發揮即時辨識之防止偽造或防止冒用功能，除須以顯性或隱性方式將指紋錄存於國民身分證上外，尚須有普遍之辨識設備或其他配套措施始可。惟為發揮此種功能，必須投入大量成本，且因缺乏適當之防護措施，可能造成資訊保護之高度風險。況主管機關已於新式國民身分證上設置多項防偽措施，如其均能發揮預期功能，配合目前既有顯性資料，已足以達成上揭之目的。次就「防止冒領國民身分證」之目的言，主管機關未曾提出冒領身分證之確切統計數據，是無從評估因此防範冒領所獲得之潛在公共利益與實際效果。末就有關「迷途失智者、路倒病人、精神病患與無名屍體之辨認」之目的而言，此類有特殊辨識身分需要的國民個案雖少，但辨識其身分之利益仍屬重要之公益目的。然而就目前已身分不明、辨識困難的國民而言，於換發國民身分證時一併強制按捺並錄存指紋資料對其身分辨識並無助益，而須著眼於解決未來身分辨識之需求。惟縱未來可能需要，並認此一手段有助前開目的之達成，然因此一需求，而強制年滿十四歲之全部國民均事先錄存個人之指紋資料，並使全民承擔授權不明確及資訊外洩所可能導致之風險，實屬損益失衡、手段過當，難以符合比例原則之要求。」由此觀之，對於戶政機關強制蒐集指紋資料於比例原則上之檢驗，大法官於該號釋字中考量數項關鍵因素，包括行政機關配套措施是否完善、是否有提出相應數據支撐蒐集目的、行政機關現有制度是否已足達成目的等均是重要的判斷事項。據此，警察若基於危害防止目的使用人臉辨識系統，欲通過比例原則之檢驗，須加以考量該

系統之內控措施是否完善，可否完善保護個人資料，避免資料外洩的風險且必須充分證明該系統對於危害防止的目的達成為必要且密切關聯，得以彌補現有手段的不足。



惟關於警政署對於該系統內控措施規範的不足已如前述，對於資料保存的規範上有未竟之處，加上有關該系統的稽核文件亦無公開，因此無法得知該內控措施對於個人資料的保護是否完善，實施的具體情形及成效，以及相關人員的使用情形。除此之外，人臉辨識系統的使用對於危害防止目的達成的實質上的成效，並無任何相關的統計資料以資佐證。再者，依現行該系統係立於輔助地位，輔助臨檢查證身分的執行而言，換言之，畢竟人臉辨識系統係近年始啟用之科技，縱使無此一系統，警察亦有他種方式可查出受檢者之身分，進而達成危害防止之目的，且無須蒐集人民的高敏感個資，人臉辨識系統充其量僅僅是一個「好用」的工具，而非與危害防止的執行緊密相聯。縱使現今警察危害防止之任務，由於資訊時代的來臨，人民安全需求提升等原因而有所擴張，亦無相關數據得以充分說明人臉辨識系統的使用為警察執行危害防止所必要且為密切關聯之手段。總而言之，欲通過比例原則的檢驗，須人臉辨識系統的使用對於危害防止而言，有具體的成效，且有關鍵性的作用，為其他方式所無法代替，且該系統的內控措施已足完善，並無個資外洩之風險，惟現階段，警政署並無任何有關數據，說明人臉辨識系統的使用對於危害防止的達成不可或缺，且內控措施又未足完善，本文認為，現行警察使用人臉辨識系統查證身分或難以符合比例原則之要求。

第五章 警政署使用國民身分證相片資料建置人臉資料庫之爭議



為使用人臉辨識系統，背後必須建有人臉資料庫作為身分比對來源。換言之，人臉辨識系統的使用，與人臉資料庫的建立密不可分。而警察為使用人臉辨識系統，背後亦須建有人臉資料庫作為身分比對的來源，否則該系統將無用武之地。警察所使用的人臉辨識系統其背後的人臉資料庫，除使用機關自有的通緝犯、治安顧慮人口、前科犯及失蹤人口資料庫之資料等作為建檔基礎外，其中最具爭議之處，在於使用內政部戶政司國民身分證相片資料作為人臉資料庫之建檔基礎。本章便探討警政署使用內政部戶政司國民身分證相片資料作為人臉資料庫建檔基礎之合法性。

本章於探討警政署使用國民身分證相片資料建置人臉資料庫之爭議，將分為兩部分進行分析，第一部分首先說明國民身分證相片資料之蒐集及資料庫之建置與機關申請使用相片資料之程序規範；第二部分則針對警政署使用國民身分證相片資料建置人臉資料庫一事，分別由戶政機關及警政署角度出發，戶政機關傳遞資料及警政署取得並使用該相片資料此二行為是否符合個資法第 15 條與第 16 條之規定及警職法第 16 條及第 17 條與個資法間的適用關係。

第一節 國民身分證相片資料之蒐集及提 供與資料庫的建置



第一項 國民身分證相片資料之蒐集與資料庫之建置

國民身分證相片資料的蒐集及建置成資料庫之依據係戶籍法第 52 條以及本條所授權訂定之國民身分證及戶口名簿製發相片影像檔建置管理辦法（下稱管理辦法）。戶籍法第 52 條規定：「國民身分證及戶口名簿之格式、內容、繳交之相片規格，由中央主管機關定之。國民身分證及戶口名簿之製發、相片影像檔建置之內容、保管、利用、查驗及其他應遵行事項之辦法，由中央主管機關定之。」而依據本條所授權訂定管理辦法第 32 條之規定，戶政事務所應將相片影像檔彙集後，儲存於中央主管機關（此指內政部）建置之資料庫，中央主管機關應指定專人（內政部戶政司所屬員工）依相關法令辦理安全維護事項，防止資料被竊取、竄改、毀損、滅失或洩漏。而相片影像檔的內容，依據該管理辦法第 31 條，包括：統一編號、相片影像、建檔之戶政事務所代碼、建檔之人員及日期以及其他應記載事項。

由此可知，國民身分證相片資料庫中個人相片影像檔內容包含身分證統一編號以及相片影像，而蒐集國民相片及建置該資料庫之目的，可由內政部戶政司的職務執掌¹³³加以推論，應是作為戶籍統計、各項人口普查，以及其他相關戶政業務的輔助，亦即基於戶政目的而蒐集國民相片並建置成國民身分證相片資料庫。

¹³³ 戶政司職掌業務有：戶政機關組織編制業務；出生、死亡、認領、收養、終止收養、監護、結婚、離婚等登記案件疑義解釋業務；涉及親子、收養、婚姻關係之父母、養父母、配偶姓名更正及補填案件；遷徙登記業務；初設戶籍登記業務；重複戶籍登記業務；國民身分證、戶口名簿業務（不包括現行空白證印製業務）；印鑑業務；戶籍謄本業務；戶籍資料提供業務；規費業務；罰鍰業務；戶籍統計業務；姓名使用及更改業務；原住民身分及姓名業務；戶警聯繫業務；配合選舉、役政業務等事項。內政部戶政司全球資訊網，<https://www.ris.gov.tw/app/portal/232>（最後瀏覽日：04/24/2020）

而內政部基於戶政目的蒐集國民相片並建置成國民身分證相片資料庫，針對此一行為本文認為應屬合法。首先，戶籍法係戶政機關為辦理戶籍登記而訂定之法律¹³⁴，該法共計 83 條，規範辦理戶籍登記業務應注意之事項及程序，包括戶籍登記之變更、更正、撤銷及廢止及戶籍資料之申請及提供，並訂有相關之罰則。簡言之，戶籍法係作為內政部辦理戶籍登記業務之行為規範，應屬行為法，因此內政部依戶籍法第 52 條之規定蒐集國民相片有行為法之授權。餘下的問題為，內政部蒐集相片資料是否符合比例原則之規定。釋字第 603 號解釋理由書中指出：「憲法對個人資訊隱私權之保護亦非絕對，國家基於公益之必要，自得於不違反憲法第二十三條之範圍內，以法律明確規定強制取得所必要之個人資訊。至該法律是否符合憲法第二十三條之規定，則應就國家蒐集、利用、揭露個人資訊所能獲得之公益與對資訊隱私之主體所構成之侵害，通盤衡酌考量。並就所蒐集個人資訊之性質是否涉及私密敏感事項、或雖非私密敏感但易與其他資料結合為詳細之個人檔案，於具體個案中，採取不同密度之審查。」據此，比例原則的審查標準將因機關所蒐集之個資性質，而採取不同密度之審查。戶政機關所蒐集之國民相片，其規格為最近 2 年內所攝彩色，脫帽、未戴有色眼鏡，眼、鼻、口、臉、兩耳輪廓及特殊痣、胎記、疤痕等清晰、不遮蓋，相片不修改，足資辨識人貌，直 4.5 公分，橫 3.5 公分，人像自頭頂至下顎之長度不得小於 3.2 公分及超過 3.6 公分，白色背景之正面半身薄光面紙相片 1 張，不得使用合成相片¹³⁵。由此可知，對於相片的要求極為重視須足以辨識容貌，臉部輪廓須十分清晰。此種相片的性質為何？是否屬於私密敏感之個資？

內政部所要求的臉部相片於人臉辨識系統使用前後性質上將有所差異。於我國警察使用人臉辨識系統使用前，此種臉部相片對於個人而言應非私密敏感之個資，因不論是於私領域或是公領域上，此種相片的繳交屬於常態。但於人臉辨識

¹³⁴ 戶籍法第 1 條規定：「中華民國人民戶籍之登記，依本法之規定。」

¹³⁵ 內政部戶政司全球資訊網，<https://www.ris.gov.tw/app/portal/187>（最後瀏覽日：12/27/2020）。



系統使用後，該相片卻成為人臉辨識系統用於身分識別的人臉特徵資料的來源，而人臉特徵資料係具有高度人別識別性的生物特徵資料，依釋字第 603 號解釋之意旨，人臉特徵資料應屬高敏感個資。而作為此種資料來源的臉部相片，是否亦一定程度上「質變」，成為私密敏感個資？本文以為，縱使臉部相片於人臉辨識系統的使用後成為抽取人臉特徵資料的媒介，相片資料仍非屬敏感個資，因相片資料若無搭配人臉辨識系統的使用，係日常生活中常見且由於社群網路之發達，個人亦會於網路上分享此種照片，因此，相片資料與釋字第 603 號解釋中的大法官所承認的私密敏感個資—指紋資料，本質上有所不同，亦與個資法第 6 條所列舉的特種個資，例如：基因、病歷、健康資料等性質上不相似。爾後倘人臉辨識系統的使用越發普及，個資法是否應對於此種媒介個資有所回應，此為日後人臉辨識系統使用漸趨普及所需面對的課題之一。由於相片資料非屬私密敏感個資，但相片資料對於內政部而言，卻是人口調查所不可或缺，對於辦理戶籍登記以及避免幽靈人口有關鍵作用，倘無相片便無法加以核實，將導致戶政業務執行上的困難。植基於此，內政部基於戶政目的蒐集國民相片並建置國民身分證相片資料庫應屬合法。

第二項 機關申請使用國民身分證相片資料庫的程序規

範

本段將介紹現行戶政機關提供國民身分證相片資料予他機關使用的程序規範以及他機關申請及使用該資料的相關規定。

第一款 警政署申請使用戶政機關國民身分證相片資料庫之程

序規範

(一) 戶籍法及國民身分證及戶口名簿製發相片影像檔建置管理辦法



依戶籍法第 52 條第 2 項之規定：「國民身分證及戶口名簿之製發、相片影像檔建置之內容、保管、利用、查驗及其他應遵行事項之辦法，由中央主管機關定之。」基於本條之授權，內政部訂定國民身分證及戶口名簿製發相片影像檔建置管理辦法。而依本辦法第 37 條之規定：「公務機關如需用國民身分證請領資料及相片影像檔，應依相關法令規定申請。」

依上開之規定，警政署若需使用戶政機關國民身分證相片資料庫的資料，需依相關法令提出申請。而此所謂「相關法令」，具體而言，係指依內政部所訂定各機關應用戶役政資訊連結作業及管理要點之規定提出申請。

（二）各機關應用戶役政資訊連結作業及管理要點

各機關應用戶役政資訊連結作業及管理要點（下簡稱管理要點），該管理要點係為提供各機關應用戶役政資訊，發揮資訊資源共享效益，提高行政效能，確保資訊安全所訂定，本要點共計 21 點。其中該管理要點第 5 點規定：「為維護國家安全及公共秩序，公務機關得申請應用國民身分證相片影像資料，其管理除另有規定外，準用本要點規定。」職是之故，警政署向戶政機關申請使用國民身分證相片資料細部之程序性、技術性事項均依照該管理要點之規定。而依該管理要點之規定，戶政機關係透過資訊連結系統，並以線上資料查詢、檔案傳輸或磁性媒體交換等三種方式之其中一種，將國民身分證相片資料提供予警政署（本要點所稱的連結機關）加以利用。以下將簡介該管理要點：

1. 資料之提供及申請機關

戶役政資料提供機關（以下簡稱提供機關）為內政部；而所申請的資料屬全

國性或跨直轄市、縣（市）者，向內政部提出申請。連結機關，指向提供機關申請，並經審核通過應用戶役政資訊之機關。（管理要點第 6 點）



2.提供資料之方式

本要點所稱連結作業，指內政部開發之連結介面、電子閘門及資訊中介服務等應用軟體及作業程序。連結作業資料提供方式為線上資料查詢、檔案傳輸及磁性媒體交換。而連結作業以各公務機關為連結對象。（管理要點第 2 點及第 3 點）。

3.資訊連結之申請及審核

申請成為連結機關須填具申請表、需求資料項目表，及提出使用戶役政資訊管理規定，供提供機關審核。提供機關應依本要點規定審核申請機關提交之申請表、資料項目表及使用戶役政資料之管理規定，並設定經審核通過之連結機關權限。（管理要點第 11 點及第 12 點）

4.連結機關訂定管理規定之義務

申請連結機關訂定使用戶役政資訊管理規定，規範內容應包括左列 13 項內容：使用戶役政資料之目的及資料安全管制作業、定期督考查核及配合提供機關實施稽核作業之具體程序、使用者查詢資料之具體作業程序、處理個人資料之保密措施、對於取得資料之處理及利用，違反電腦處理個人資料保護法（現個人資料保護法）規定致當事人權益受損時應負之責任、使用者違反規定時應負之責任、使用完成後資料之處理、申請連結案之承辦人及單位主管異動時，應函知提供機關。（管理要點第 13 點）



5.申請資料之取回

連結機關應於規定期限內，取回其所需資料，期限屆滿時，提供機關將刪除該資料，遇特殊事故時，應於到期日前通知提供機關，延長資料保留期限。各類資料保留期限依下列規定：若為線上資料查詢類：保留期限為一日；檔案傳輸類：保留期限為七日；磁性媒體交換類：保留期限為七日。(管理要點第 17 點)

6.資訊連結系統異常時的處理機制

連結作業發生網路通訊異常時，連結機關應先向電信機構查明原因，如為提供機關之網路線路異常時，應與其連繫解決之。常連結機關傳送查詢需求後，如查詢結果顯示提供機關電腦系統異常時，應與其連繫，俟提供機關修復後，再通知連結機關重新傳送查詢需求。(管理要點第 15 點)

7.相關稽核措施

連結機關應保存連結取得資料日誌，並定期稽核。提供機關應保存連結機關連結紀錄及所提供資訊日誌，並定期稽核。實施稽核作業時，連結機關與提供機關應密切配合。而提供機關查知連結機關違反本要點情事者，應當日通知連結機關限期改善，並得即暫停其連結作業及暫停其檔案應用。連結機關於改善違反事項，經提供機關審查符合本要點規定後，回復原連結作業。連結機關逾半年未改善者，應重新申請。(管理要點第 18 點及第 19 點)

8.連結作業的停止或終止：連結機關欲終止連結作業時，應於終止日前一個月內以書面通知提供機關。(管理要點第 20 點)

第二款 警政署使用國民身分證相片資料庫的使用規範



由前述可知，警政署為向內政部申請提供國民身分證相片資料，依各機關應用戶役政資訊連結作業及管理要點第 13 點之規定，須訂定資料使用管理規定，因此警政署訂有內政部警政署國民身分證相片影像資料使用管理要點（下簡稱使用要點），此為警政署內部行政規則，並未對外公開，因此無法於網站上查找，該管理要點全文共 16 點。以下將簡介該管理要點：

（一）資料管理相關規定參酌

警政署應依個人資料保護法、警察機關資訊安全實施規定及本要點規定管理國民身分證相片影像資料。（管理要點第 2 點）

（二）影像資料之內容

警政署及警察機關使用國民身分證相片影像資料時，僅得呈現個人基本資料（姓名、國民身分證統一編號），且非經本部同意，不得提供其他單位。（管理要點第 3 點）

（三）影像資料的查詢

員警為偵查犯罪及維護治安，於執行法定職務內，遇有下列情形者，得利用網路查詢國民身分證相片影像資料，其中與本文相關者為，對於警職法第 6 條規定之人，經詢問或令出示身分證明文件不能查證身分，須查詢國民身分證相片影像資料予以查證身分。（管理要點第 4 點第 2 款）



(四) 資訊安全措施

警政署及警察機關透過網路連線，進行國民身分證相片影像資料之提供或查詢時，應依左列規定辦理：一為須加強傳輸過程資料加密、身分鑑別及防火牆等資訊安全措施，確保資料庫安全管理。二為應自動加註識別碼，顯示查詢人單位、姓名及查詢日期等保全資訊。三為應自動記錄查詢人之登入帳號、IP 位址、查詢時間及查詢條件等日誌資料。四為協助查詢時，應於系統上方鍵入請求協助者之職別、姓名及事由；其未鍵入者，視為帳號使用者查詢使用。協助查詢資料之傳送，應轉為可攜式文件格式（Portable Document Format-PDF），並進行資料保全，設定密碼及唯讀功能。最後所查詢之國民身分證相片影像資料，不得另行傳送。使用目的未完成時，應妥善保管；完成任務後，應予刪除或銷毀。（管理要點第 5 點）

(五) 系統管理及使用權限

國民身分證相片影像資料系統權限區分如下：權限管理者（以下簡稱管理者）有權限授予及稽核之權。上一層管理者，得授與下一層具有管理者身分；各管理者應保留授權申請資料備查。而使用者則僅有查詢使用權。直轄市、縣（市）政府警察局管理者以防治（戶口）科人員為主，資訊人員為輔，各設專責人員，並由管理者負責授權、審核及稽核工作。而本部警政署所屬機關則應指定專責人員，負責授權、審核及稽核工作，層級比照直轄市、縣（市）政府警察局、分局及分駐（派出）所方式辦理。（管理要點第 6 點、第 10 點及第 11 點）

管理者之授權、管控及稽核規定如左：本部警政署為總管理者，負責直轄市、縣（市）政府警察局第一層管理者之授權及定期稽核。除此之外，採三層授權方

式管理；第一層（局級）：為直轄市、縣（市）政府警察局管理者，每機關以一人為原則，負責分局、直屬隊等第二層管理者之授權及定期稽核。第二層（分局級）：為分局之管理者，每分局以二人為原則，負責分局偵查隊、警備隊、交通分隊及分駐（派出）所等第三層單位管理者之授權及定期稽核。第三層（所級）：管理者由分駐（派出）所所長，或相當單位主管擔任為原則，僅授予員警使用權。（管理要點第 7 點）

管理者得授權使用者之對象規定如左：第一層管理者，以局本部人員為主。第二層管理者，以分局人員為主。第三層管理者，以分局偵查隊、警備隊、交通分隊及分駐（派出）所人員為主。而員警因勤務、業務需要使用國民身分證相片影像資料時，應登入警政知識聯網，點選電子化表單、電子化表單線上申辦、權限申請表、線上審核表單，選取國民身分證相片影像資料系統使用權限申請表並填寫申請項目，循行政程序，經所屬單位主管同意後，再由各層級管理者辦理權限設定。（管理要點第 8 點及第 9 點）

（六）使用規範

因執行職務或業務所知悉之國民身分證相片影像資料，除法律另有規定外，應予保密；處理及使用該資料時，應採取必要之保密措施。違反保密義務者，依相關法律規定處理；違反本要點查詢使用規定者，依警察機關加強戶役政資訊稽核實施計畫之規定懲處。（管理要點第 12 點）

（七）稽核措施

警察機關防治（戶口）單位應指定專人執行管理與稽核，包括系統內各項查

詢（含由系統自動保存日誌紀錄等）；本部警政署資訊室對於各項日誌紀錄，應定期備份。警察機關資訊單位應定期於每月五日前列印查詢報表送防治（戶口）單位查核。且警察機關政風或保防單位，應依本部警政署維護個人資料安全專案稽核計畫辦理稽核，發現有異常查詢時，應調取相關查詢紀錄，依法調查。（管理要點第 14 點及第 15 點）

第二節 警政署以國民身分證相片資料作為人臉資料庫建檔基礎之爭議



警政署使用內政部戶政司國民身分證相片資料作為人臉資料庫之建檔基礎，涉及個人資料之蒐集及利用行為。而個人資料的法律保護機制，觀念上須區分「得否」與「如何」蒐集、處理或利用個人資料。公務機關須先依法得以蒐集、處理或利用個人資料，而後才可討論蒐集、處理或利用個人資料之方式是否具合法性¹³⁶。而個資法所規範者係後者，亦即當公務機關可以蒐集、處理或利用個資時，須符合個資法之相關規定。公務機關可不可以蒐集、處理或利用個資需要獲得另一個法律之授權，換言之，個資法本身並無法作為公務機關蒐集、處理或利用個資之法律依據，個資法係規範機關如何蒐集、處理及利用個人資料，而至於機關可不可以蒐集、處理及利用個人資料，須另有法律授權¹³⁷。而就此授權究為組織法即足或是須為行為法始可？此一問題亦會涉及個資法第 15 條及第 16 條「執行法定職務必要範圍」要件中「法定」之解釋。

針對個人資料的蒐集、處理及利用，依釋字第 603 號解釋理由書中所載：「隱私權雖係基於維護人性尊嚴與尊重人格自由發展而形成，惟其限制並非當然侵犯人性尊嚴。憲法對個人資訊隱私權之保護亦非絕對，國家基於公益之必要，自得於不違反憲法第二十三條之範圍內，以法律明確規定強制取得所必要之個人資訊。」據此，公務機關蒐集個人資料，不論係直接蒐集（向當事人蒐集個資）或是間接蒐集（蒐集非由當事人提供之個資）、處理及利用個人資料，均屬對人民基本權之干預，除經當事人同意外，須有法律授權始可。而蒐集個資所涉及的基本權係除

¹³⁶ 李建良（2018），〈資料流向與管控環節--個資保護 ABC〉，《月旦法學雜誌》，第 272 期，頁 28。

¹³⁷ 林子儀、張陳弘、顏厥安、范姜真嫻、陳鈺雄、李建良、吳全峰、陳昭如（2018），〈最高法院一〇六年度判字第五四號判決（健保資料庫案）會議紀錄〉，《月旦法學雜誌》，第 272 期，頁 67。

人身自由外之其他基本權利，因此法律保留之密度，依釋字第 443 號「層級化法律保留」之見解，應屬相對法律保留之事項¹³⁸。而此所謂「法律」，須具行為法之性質，若僅是組織法則有所不足¹³⁹，因組織法並非基本權利干預行為的法律授權依據，組織法為一種任務規範，在於界定各行政機關的行政任務範圍，釐清管轄權；行為法則是一種職權規範，規定各行政機關為了履行各自之行政任務，得在符合何等條件下採取何種行政手段，從而與人民發生法律關係¹⁴⁰。職是之故，由組織法及行為法之功能及其規範目的可知，組織法主要係用於劃定各行政機關間的行政任務，無關行政行為之手段及要件，而行為法的目的在於規範行政行為之要件，行政機關之行為若將對基本權造成限制，必須要有針對該行為明確的法律規範，包括要件及限制等，而組織法並不會有相關規定。釋字第 535 號解釋理由書中亦明確指出：「行政機關行使職權，固不應僅以組織法有無相關職掌規定為準，更應以行為法（作用法）之授權為依據，始符合依法行政之原則。」故不論係警政署或戶政機關其蒐集、處理或利用國民身分證相片資料不得僅以組織法為依據，仍須有行為法之授權，始符合法律保留原則。

綜上，依釋字第 535 號解釋及第 603 號解釋之意旨，機關蒐集、處理及利用個資須有行為法之授權始可。而由於本文亦認為個資法不足以作為機關蒐集、處理及利用個資之依據，換言之，個資法第 15 條及第 16 條之規定不足以作為機關蒐集、處理及利用個資的法律依據，並無行為法的授權性質，職是之故，於解釋個資法第 15 條及第 16 條有關「執行『法定』職務必要範圍」之要件時，「法定」的「法」須為行為法僅有組織法並不足夠作為機關可以蒐集、處理及利用個資之依據。於健保資料庫（最高行政法院 106 年判字第 54 號判決）一案中，有論者認為最高行政法院之所以認為個資法第 16 條但書第 5 款關於「執行法定職務」之要

¹³⁸ 謝碩駿（2019），〈行政機關蒐集個資之法律依據〉，《月旦法學教室》，第 198 期，頁 14-15。

¹³⁹ 李建良，前揭註 136，頁 14。

¹⁴⁰ 謝碩駿，前揭註 138，頁 15。

求，僅以健保署組織法的法定職權規定即足，應係認為個資法第 16 條乃公務機關對於蒐集而來的個資為目的內及目的外利用行為的合法性要求規定，故本條本身即具有行為法授權性質，因此關於「執行法定職務」自然會理解為「公務機關在組織法上的職掌規範」，只要組織法之授權即可，無須再有行為法之依據¹⁴¹。

除此之外，警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫之行為，與健保資料庫案中的事實相似，均為不同公務機關間資料共享（或稱流通）之情形。於健保資料庫案中，健保署將資料交付予衛福部建立健康資料庫，由於健保署及衛福部均有自己獨立的組織法及人事、預算，因此二者均屬於行政機關而非內部單位，因此健保署將資料交付予衛福部之行為，屬於不同公務機關間資料共享之情形，且細部而言係所屬機關交付資料予上級機關。回到本文，警政署有自己獨立的組織法（內政部警政署組織法）及人事預算，故屬行政機關無虞，惟戶政司則不然，戶政司係依內政部組織法第 4 條所設立¹⁴²，換言之，戶政司並無自己獨立的組織法及人事預算，而是隸屬於內政部的內部單位，警政署亦隸屬於內政部¹⁴³，故警政署使用內政部戶政司國民身分證相片資料之行為，廣泛而言，係於內政部內資料共享（流通）之情形，惟實際上仍係警政署及內政部間不同公務機關間的資料共享情形，但本文之情形係上級機關交付資料予下級機關之情形，與健保資料庫案中的事實相似但有些微差異。於本文之情形，由於係上級機關交付資料予下級機關之情形，因此是否為個資內部傳送之行為，須加以討論，將於第二項有關「戶政機關傳遞國民身分證相片資料」的討論中加以說明。

關於不同公務機關間資料共享之情形，應如何適用個資法之規定，關於此一

¹⁴¹ 林子儀、張陳弘、顏厥安、范姜真嫻、陳鈺雄、李建良、吳全峰、陳昭如，前揭註 137，頁 66-67。

¹⁴² 內政部組織法第 4 條：「內政部設左列各司、室：一、民政司。二、戶政司。三、社會司。四、地政司。五、總務司。六、秘書室。」

¹⁴³ 內政部組織法第 5 條：「內政部設警政署，掌理全國警察行政事務，統一指揮、監督全國警察機關，執行警察任務；其組織以法律定之。」

問題依最高行政法院之見解（106 年判字第 54 號判決），其認為不同公務機關間資料傳遞之行為本質上屬於個人資料的「檔案格式的轉換」，應屬於個人資料的處理而非利用行為，但因個資法對於不同公務機關間的資料共享或稱流通（處理），並未有特別規定，形成法律漏洞，因此於此種機關間共享資料（處理）的行為應類推適用個資法第 16 條有關「資料利用」之規定¹⁴⁴。職是之故，依最高行政法院之見解，不同公務機關相互間個人資料之傳遞，應「類推適用」個資法第 16 條之規定。惟有對最高行政法院此一見解表示不同看法者，蓋個資法若未對此種機關間資料共享之情形有特別規範，則應視各機關的個資使用行為性質，適用對應的個資法規定即可，機關間資料共享（或稱流通）應就傳遞機關的傳遞行為及接受機關的資料蒐集行為的面向，分別適用相應的個資法規定，因此並未有法律漏洞之情事¹⁴⁵，本文亦採相同之見解，既個資法就資料蒐集、處理及利用已有相應的規範，於機關間資料共享之行為，應就不同行為分別適用相應的個資法規定即可，並無法律漏洞之情形。於本文中，警政署使用國民身分證相片資料建置人臉資料庫，依時間先後順序，分別為傳遞、取得及建置人臉資料庫三種行為，針對不同行為分別適用個資法第 15 條及第 16 條之規定即可，以下將依時間順序分別探討上述三種行為之合法性。

第一項 個資法—目的拘束原則

警政署使用國民身分證相片資料建置人臉資料庫，此一行為分別由戶政機關及警政署之角度出發，將涉及不同的爭議，但均與個資法目的拘束原則的原則與例外的適用有關，涉及個資法第 15 條及第 16 條之規定，為使後續之探討得直接切入核心，本節將首先對目的拘束原則以及所涉的例外事由，亦即個資法第 16 條但書第 2 款「為維護國家安全或增進公共利益所必要」的內涵進行說明。

¹⁴⁴ 吳全峰、許慧瑩（2018），〈健保資料庫行政訴訟案：個資保護與健保資料之跨機關流動及二次利用〉，《月旦醫事法報告》，第 19 期，頁 62-63。

¹⁴⁵ 林子儀、張陳弘、顏厥安、范姜真燊、陳鉅雄、李建良、吳全峰、陳昭如，前揭註 137，頁 66。



第一款 目的拘束原則的內涵

在個人資料保護上，「目的拘束原則」具有相當重要之地位，並有稱之為個資法上之「帝王條款」者¹⁴⁶。目的拘束原則係指特定目的所蒐集之個人資料不得為恣意利用¹⁴⁷，亦即原則上不得超出蒐集目的外利用個資。本於此原則，政府機關蒐集人民的訊息，必須在「法定執掌範圍內」的「必要範圍」基於「明確目的」才可以蒐集、處理及利用。據此，有認為在個人資料之處理上，目的拘束原則具有三個要素，即必須在公務機關之「法定職務內」、法定職務內之「必要性」及必須具有「明確性」¹⁴⁸。由此，目的拘束原則之內涵實際上係由「目的明確原則」及「限制利用原則」共同構築而成。

目的明確原則，亦有學者稱為目的特定原則，係指個人資料於蒐集時目的即應明確化，其後之利用亦應與蒐集目的相符，於目的變更後亦應明確化。據此，於蒐集個資的當下，便須具備具體、明確且正當之目的¹⁴⁹。至於所謂的「特定目的」，涉及到如何確定其目的問題，此處的「特定目的」行政機關不可任意定之，基於行政機關蒐集、處理個資，由於將干預人民資訊隱私權之保護，應有法律保留原則之適用，依法始可為之，此特定目的須屬該當行政機關執行其法定職務被預定達成之任務¹⁵⁰。由於目的拘束原則明顯地取決於，在個案中如何使其目的獲得具體化之確認。而目的確定越具體，越可避免發生目的外之蒐集或利用等情形。因此，與明確性原則有密切之關係。本於明確性原則之要求，使人民對於行政機關進行各種個人資料之蒐集、處理或利用行為時，得以預見該行為之目的等，因

¹⁴⁶ 李惠宗（2013），〈個人資料保護法上的帝王條款—目的拘束原則〉，《法令月刊》，第 64 卷第 1 期，頁 38。

¹⁴⁷ 林玫君（2018），〈大數據時代的個人資料保護〉，《興大法學》，第 24 卷，頁 11。

¹⁴⁸ 李惠宗，前揭註 146，頁 49。

¹⁴⁹ 洪宛伶（2019），〈公務機關共用個人資料法制研究〉，頁 31，國立臺灣大學法律學研究所碩士論文。

¹⁵⁰ 范姜真嫻（2019），〈自實務判決檢視行政機關蒐集、處理或利用個人資料之問題〉，《警察法學》，第 18 期，頁 96。

此得以有所調適，並防止公權力之濫用。如何達到目的確認所必要之明確性，無法有一致性之答案，也只能取決於個案之情形，不過一般而言，若對人民之負擔越重，目的明確性之要求越高¹⁵¹。而為使公務機關以及非公務機關能夠對於個資法所稱之「特定目的」有所掌握，個資法第 53 條規定：「法務部應會同中央目的事業主管機關訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用」，因此法務部於 2012 年 10 月 1 日以法令字第 10103107600 號修正發布「個人資料法之特定目的及個人資料之類別」，以協助各機關確定其目的。其中，與本文較為相關的戶政以及犯罪預防分屬該規範第 1 條所列編號○一五及○二五的特定目的，亦即戶政及犯罪預防為個資法所承認可以作為資料蒐集、處理及利用的特定目的。限制利用原則係指個人資料之利用，除法律另有規定或經當事人同意者外，不得為特定目的以外之利用，因此，原則上個資之蒐集、處理及利用均不得逾越原特定目的的必要範圍¹⁵²。

目的拘束原則為個人資料保護中之重要基本原則，我國將該原則落實於個資法第 5 條、第 15 條以及第 16 條。個資法第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」本條為總則性之規定，適用於所有與個人資料保護之事項。又本條涵蓋甚多原則，除目的拘束原則之外，並有尊重原則、誠信原則、必要原則及禁止不當聯結原則等；而第 15 條及第 16 條則針對資料蒐集、處理及利用行為分別適用目的拘束原則所為的個別規定。

¹⁵¹ 洪家殷（2018），〈公務機關資料之蒐集與個人資料之保護〉，《東吳法律學報》，30 卷 4 期，頁 46。

¹⁵² 洪宛伶，前揭註 149，頁 31。



第二款 目的拘束原則之例外

為了避免該原則過於嚴苛以致行政窒礙難行，因此個資法第 16 條針對資料利用行為，明文准許倘有本條但書的例外事由，公務機關可超出蒐集目的外利用個資，此為目的拘束原則之例外。惟應注意的是「目的外利用個資」，本質為「限制利用原則」及「目的限制原則」的例外，基於例外規定從嚴解釋之原則，個資法相關規定及其要件，均應明確且做嚴格解釋，避免濫用情事，而破壞個資法重要的立法本旨¹⁵³。經查，該條於 1995 年電腦處理個人資料保護法（個人資料保護法的前身）便已有明文規定，並非近期所新增定之規定，而是立法已久，以下將簡介本條的立法歷程。

（一）1995~2010 年 5 月 26 日：電腦處理個人資料保護法（個人資料保護法之舊稱）時期

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

立法理由共計五點，一為公務機關對於個人資訊之利用應依本條規定為之，明定不得逾越執行職務之必要範圍，且應受目的明確化原則之限制。二為目的明

¹⁵³ 范姜真嫻，前揭註 150，頁 99。

確化原則如嚴格執行，難免會因過於嚴苛以致窒礙難行，爰以列舉方式為例外規定，以資調和。惟各公務機關得否為目的外之利用，仍須依法令裁量，爰為第一款之規定。三係基於公益與私益之平衡，如有正當理由僅供內部使用、維護國家安全與增進公共利益或為學術研究而有必要者，公務機關應得為目的外之利用，爰為第 2 款、第 3 款、第 4 款及第 7 款之規定。四為目的外利用係為免除當事人之急迫危險、有利於當事人權益或經當事人書面同意者，應予准許。又目的外之利用，係為防止他人權益之重大危害而有必要者，亦應准許，爰為第 5 款、第 6 款、第 8 款及第 9 款之規定。第五點係有關外國立法例之參考，參考日本法第 9 條及德國法第 14 條第 2 項之立法例而訂定。據此，並非僅我國針對目的拘束原則有例外之立法例，日本及德國為避免該原則過苛，進而導致行政窒礙難行，亦有例外的規定，於公益及私益的保障間取得平衡。

(二) 2010 年 5 月 26 日~2015 年 12 月 30 日：改稱個人資料保護法，並將目的拘束原則的例外移列至第 16 條

2010 年電腦處理個人資料保護法名稱修正為個人資料保護法，原第 8 條之規定移列至第 16 條，條文內容修正成：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為維護國家安全或增進公共利益。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、有利於當事人權益。七、經當事人書面同意。」

本條的修正理由共計十點，除款次變更、文字的修正及刪除不明確或是贅述

之款次等形式之變更外，修正理由僅對於第 5 款「公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人」有較為細節之說明¹⁵⁴。而對照新舊法之規定，雖然例外事由 9 款事由縮減成 7 款，但細觀其內容實質上並無太大之區別，僅刪除「有正當理由而僅供內部使用」及將「維護國家安全」、「增進公共利益」合併成一款事由，並酌做文字之修正。而與本文相關的第 2 款「為維護國家安全或增進公共利益」此一事由則無任何細節之說明，包括定義或是具體的事例均無。

（三）2015 年 12 月 30 日~迄今：修正本條第 2 款及第 7 款事由

2015 年 12 月 30 日本法再度進行修正，本條修正為現行之規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為維護國家安全或增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、有利於當事人權益。七、經當事人同意。」將本條第 2 款事由修正為「為維護國家安全或增進公共利益所必要」加上必要性之要件，並將第 7 款之書面要件刪除，修正為「經當事人同意」，放寬同意方式，不以書面為限。

由上述本條的立法過程中可知，從目的拘束原則的例外明文化起，與本文最

¹⁵⁴ 針對第 5 款事由之修正，本條修正理由第 9 點稱係為促進資料合理利用，以統計或學術研究目的，應得准許特定目的外利用個人資料，惟為避免寬濫，爰限制公務機關或學術研究機構基於公共利益且有必要，始得為之。另該用於統計或學術研究之個人資料，經提供者處理後或蒐集者依其揭露方式，應無從再識別特定當事人，始足保護當事人之權益，爰將現行條文第 7 款予以修正，款次移列至第 5 款。法務部法律事務司（2016），《個人資料保護法規及參考資料彙編》，二版，頁 59，臺北：法務部。

為相關的「為維護國家安全或增進公共利益所必要」此款事由，自本條立法至今，未曾改變，一直都是目的外利用原則的例外事由。惟針對該款事由之定義或是具體內涵，即便本條歷經三次的修法，不論是條文或是修法理由中，均未有任何細節性的說明。而細觀之，「為維護國家安全或增進公共利益所必要」實可區分為 2 個部分，包含維護國家安全及增進公共利益，並輔以必要性為判斷標準，本文著重係前者「增進公共利益」。然無論是舊法或是新法均僅規定「增進公共利益」此一不確定法律概念，而未有具體說明。

針對本款「增進公共利益」的定義，可參酌法務部法律字第 1000004930 號函，於該行政函釋中，法務部對於本款的內涵有較為具體的說明，略以：「三、按（舊）電腦處理個人資料保護法（簡稱個資法）第 8 條規定：「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用：一、法令明文規定者。…四、為增進公共利益者。」是以，公務機關如有上開各款事由之一，得就其保有之個人資料為特定目的外之利用。至於上開第 4 款所稱「增進公共利益」，依實務見解，係指社會不特定之多數人可以分享之利益而言（臺灣新竹地方法院 95 年度訴字第 762 號判決及前司法行政部（68）台函民字第 03294 號函參照），例如對國家財政而言，有助於控制稅收、健全稅制（司法院釋字第 655 號解釋許玉秀大法官不同意見書參照）、防止逃漏關稅、維持課稅公平（司法院釋字第 281 號解釋文參照）及防止走私，避免損害之繼續發生或擴大（司法院釋字第 324 號解釋理由書參照）等皆屬之。惟上開（舊）個資法第 8 條第 4 款「為增進公共利益者」之規定，乃屬抽象之概念，尚難遽定其範圍及認定標準，宜依具體個案分別認定之。」據此，增進公共利益係指社會不特定之多數人可以分享之利益而言，但此實屬抽象之概念，是否符合本款事由，需個案認定。



回到本文。警政署使用內政部戶政司相片資料建置人臉資料庫的行為，此一行為屬於機關間資料共享（或稱傳遞）之情形，且係由內政部（資料傳遞機關）將相片資料傳遞於警政署（資料接收機關），此一行為於內政部及警政署均涉及不同的問題。此種機關間資料共享之情形，原蒐集、處理個資之行政機關（本文的內政部）提供（利用）個資，及請求提供（蒐集）個資的行政機關（本文的警政署），雙方機關均須符合個資法所規定之要件，始得稱合法，或有稱此為雙重評價制或是個人資料傳遞行為的行為評價雙元性¹⁵⁵。於警政署，涉及個資法第 15 條及第 16 條本文之適用；於內政部，倘其傳遞個資的行為屬資料利用行為，屬於目的外利用，涉及個資法第 16 條但書第 2 款「增進公共利益」此一目的拘束原則例外事由的適用。警政使用內政部戶政司國民身分證相片資料建置人臉資料庫係由 3 個行為所組成，順序由先至後分別為，內政部傳遞國民身分證相片資料、警政取得相片資料及利用相片資料建置人臉資料庫。以下將分別針對此三個行為，適用個資法之情形進行分析。

第二項 戶政機關傳遞國民身分證相片資料予警政署

本段於討論內政部傳遞相片資料予警政署行為的合法性時，將使用「戶政機關」此一名稱代替「內政部」，先予敘明使用此一名稱的理由。實際上，戶政司並無自己獨立的組織法與人事預算，僅屬於內政部的內部單位，故無法冠以「機關」之名。惟由內政部組織法第 10 條至第 17 條可知，內政部各單位間所職掌的業務大不相同，以本文之戶政司為例，依內政部組織法第 11 條¹⁵⁶之規定，戶政司掌管所有與戶政有關之事項，與同為內政部內部單位的民政司所職掌的業務便完全不

¹⁵⁵ 詹鎮榮（2015），〈公務機關間個人資料之傳遞—以台灣桃園地方法院行政訴訟 102 年度簡字第 2 號判決出發〉，《法學叢刊》，60 卷 1 期，頁 10。

¹⁵⁶ 內政部組織法第 11 條：「戶政司掌理下列事項：一、關於人口查記計畫及章則擬訂事項。二、關於人口查記機構設置及人口查記人員訓練事項。三、關於戶口普查之規劃事項。四、關於戶口調查及僑民調查事項。五、關於人口統計資料之整理、分析事項。六、關於戶籍登記事項。七、關於國籍行政事項。八、關於國民身分證及姓名使用事項。九、關於人口政策事項。十、關於其他戶政事項。」

相干，與警政署的職務範圍差異更是極大。內政部戶政司主掌戶政相關業務，蒐集並建置國民身分證相片資料庫及該資料庫之相關維護均屬其業務範圍¹⁵⁷，而相關戶政法規的訂定及申請書的格式（例如：各機關應用戶役政資訊連結作業及管理要點、戶政機關資料交換安全約定、各式申請表及資料項目清單等）亦然¹⁵⁸，因此雖然名義上決定是否提供資料及提供警政署相片資料者為內政部（戶政司之上級），但實質上由於戶政業務屬於戶政司的職掌範圍，因此本文認為，此些決策難以想像並無戶政司的參與，甚至戶政司才是實質上的決策及提供者亦不無可能，畢竟戶政資料是儲存在戶政司處，由其進行管理及維護，而實際上傳遞資料者亦為戶政司¹⁵⁹，內政部或僅是行政內部程序上主管簽核之角色。

警政署時任資訊室主任於接受採訪介紹 M-Police 時亦說到：「M-Police 後端必須串接許多個人資料，才能讓一線員警迅速查詢。於串接資料上，技術面問題並不難解決，反而是溝通協調比較多困難，例如：行照、駕照資料是由交通部所管轄。戶政資料則是儲存在內政部戶政司。警政署使用、介接這些不同單位的資料庫時，需要不斷溝通，說明 M-Police 的應用情境、使用方法，以及警察執勤相關的法規、管轄範圍，在符合法規之下，讓該單位授權警政署可以介接使用這些資料¹⁶⁰。」據此，警政署為使用國民身分證相片資料與戶政司來回溝通數次，戶政司於相關決策中佔有重要角色。職是之故，本文為寫作上考量與強調戶政司於資料傳遞的重要角色，更為強調內政部原蒐集國民身分證相片資料的目的與其傳遞相片資料予警政署係逾越蒐集目的外利用個資之情形，因此使用「戶政機關」此一名稱。由於本文本就屬於不同公務機關間資料共享（內政部與警政署）之情形，縱使用「戶政機關」此一名稱代替「內政部」於本文之討論並無太大的影響，使

¹⁵⁷ 內政部戶政司全球資訊網，<https://www.ris.gov.tw/app/portal/232>（最後瀏覽日：01/19/2021）。

¹⁵⁸ 內政部戶政司全球資訊網，<https://www.ris.gov.tw/app/portal/232>（最後瀏覽日：01/19/2021）。

¹⁵⁹ 國民身分證相關業務及戶籍資料提供業務均為戶政司的職掌。參內政部戶政司全球資訊網，<https://www.ris.gov.tw/app/portal/232>（最後瀏覽日：01/19/2021）。

¹⁶⁰ iThome，<https://www.ithome.com.tw/article/117303>（最後瀏覽日：01/19/2021）。

用「戶政機關」此一名稱除能突顯內政部原蒐集國民身分證相片資料的特定目的，更能強調傳遞行為的爭議所在，故本段將使用「戶政機關」此一名稱。



第一款 戶政機關傳遞行為之性質

首先，戶政機關傳遞相片與警政署之行為究屬資料的處理或利用須先加以釐清，涉及此一行為究竟應適用個資法第 15 條或第 16 條之規定。若屬資料處理行為，則依個資法第 15 條之規定，該行為不可逾越蒐集目的；反之，若為資料利用行為，在滿足一定條件下（存在個資法第 16 條但書的事由），例外允許機關超出蒐集目的外利用個資。

資料處理的定義，依個資法第 2 條之規定，係指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。而資料利用則是指將蒐集之個人資料為處理以外之使用，亦即除資料處理以外之行為，均屬資料利用，適用個資法有關資料利用之規定。回到本文，戶政機關傳遞相片資料予警政署，是否屬於個資法第 2 條資料處理中的內部傳送行為？內部傳送依個資法施行細則第 6 條第 2 項之規定，係指公務機關或非公務機關本身內部之資料傳送。而由於本文實際係上級機關（內政部）將資料傳送給下級機關（警政署）之情形，亦即於有上下隸屬關係的行政機關間傳遞個資，究竟此種情形是否屬於個資法所稱的內部傳送情形，為本段欲探究之問題。若依個資法施行細則對於內部傳送之定義，實則與本文之情形十分相似。法務部函釋對於內部傳送行為作出進一步的說明，法務部法律字第 10303513050 號函有謂：「按個資法第 2 條第 4 款：『處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、…或內部傳送。』復依本法施行細則第 6 條第 2 項：『…內部傳送，指公務機關或非公務機關本身內部之資料傳送。』上開『內部之資料傳送』目的係為建立個人資料檔案所為，故非本法第 16 條規範之『利用』之行為，自無第 16

條之適用。惟公務機關或非公務機關內部亦可能為利用個人資料而為個人資料之傳遞，如係為利用個人資料所為之個人資料傳遞，則該資料傳遞行為非屬本法第 2 條第 4 款之『處理』行為，應屬個人資料之「利用」而適用本法第 16 條規定。」簡言之，法務部的函釋係以資料傳遞目的判斷該行為究是利用或係處理行為，如係為利用個人資料而傳遞個人資料，就算在機關內部傳送，仍認定為利用而非處理行為。

除此之外，戶政機關將相片資料傳遞予警政署之行為，與經最高行政法院 106 年判字第 54 號判決確定的健保資料庫案事實相似，於該案中，健保署將資料交付予衛福部建立健康資料庫，該行為經最高行政法院認為雖傳遞行為本質上屬於個人資料的「檔案格式的轉換」，故應屬於個人資料的處理而非利用行為，但因個資法對於不同公務機關間的資料共享（流通），並未有特別規定，形成法律漏洞，因此於此種機關間共享資料（處理）的行為應類推適用個資法第 16 條有關「資料利用」之規定¹⁶¹，職是之故，依最高行政法院之見解，不同公務機關相互間個人資料之傳遞，雖本質上屬於資料處理行為，但由於「機關間傳遞」此一情況的特殊性，因此應「類推適用」個資法第 16 條之規定。惟有對最高行政法院此一見解表示不同看法者，縱使個資法未對此種機關間資料共享之情形有特別規範，則應視各機關的個資使用行為性質，適用對應的個資法規定即可，機關間個資傳遞應就傳遞機關的傳遞行為及接受機關的資料蒐集行為的面向，分別適用相應的個資法規定，因此並未有法律漏洞之情事¹⁶²。職是之故，機關間個人資料之傳遞行為，縱使依最高行政法院之見解僅屬於「個人資料檔案格式的轉換」，惟既然檔案格式的轉換不屬於個人資料的處理，依個資法第 2 條對於利用之定義，便屬於個人資料的利用行為，應直接適用本法第 16 條，而非類推適用¹⁶³。

¹⁶¹ 吳全峰、許慧瑩，前揭註 136，頁 62-63。

¹⁶² 林子儀、張陳弘、顏厥安、范姜真嫩、陳鈺雄、李建良、吳全峰、陳昭如，前揭註 137，頁 66。

¹⁶³ 邱文聰（2018），〈被掏空的法律保留與變質的資訊隱私權憲法保障—評最高行政法院 106 年度判字第 54 號判決與相關個資法條文〉，《月旦法學雜誌》，第 272 期，頁 34。

綜上，本文認為戶政機關將相片資料傳遞予警政署之行為，應屬資料利用行為，適用個資法有關資料利用之相關規定。首先，由法條文字出發，內部傳送的定義依個資法施行細則第 6 條第 2 項係指公務機關或非公務機關本身內部之資料傳送，且由於個資法第 15 條將資料的蒐集及處理並列，故兩者應連結看待¹⁶⁴，換言之，資料的蒐集與處理行為此二行為緊密相連。職是之故，內部傳送所稱公務機關本身內部資料的傳送，應係指將蒐集而來的個資於機關「內部單位」傳送之情形，將所蒐集而來的個人資料，依各單位的業務職掌，傳送予相應的單位進行後續的處理。因此，若傳送予「外部」機關，縱使該傳遞行為係於有上下隸屬間的行政機關發生，仍非屬資料處理的「內部」傳送，反之，應認定為資料利用行為。亦有論者主張相似之見解，由最高行政法院的見解出發，其認為於健保資料庫一案中，法院不當擴張個資「處理」行為的內涵。最高行政法院未考慮公務機關於「內部」進行檔案格式轉換，與交付「外部」機關進行前述行為，二者間本質上的不同之處。個資處理行為的範圍僅及於「內部傳送」，不能進一步擴張解釋認為包括「不同公務機關間資料傳遞（流通）」之情形，若將所蒐集之個資交付「外部」機關進行格式轉換，建置資料庫並儲存，難認為可與機關內部個資處理行為等同視之，故不同公務機關間資料傳遞（流通）應認定為資料利用行為¹⁶⁵。再者，依法務部函釋之見解，由於戶政機關傳遞相片資料予警政署係基於資料利用目的而傳遞個人資料，為使警政署利用該資料建置人臉資料庫而交付相片資料，故應屬利用行為。除此之外，實際上於健保資料庫案中，健保署將資料交付予衛福部，亦屬於在有上下隸屬關係間的行政機關傳遞資料之情況¹⁶⁶，但最高行政法院仍認定此一行為屬於在不同公務機關間傳遞資料之情形。而縱使依最高行政法院之見解該傳遞行為本質上屬於檔案格式的轉換，但檔案格式的轉換不屬於個人資料的處理，依個資法第 2 條對於利用之定義，便屬於個人資料的利用行為，應直接適

¹⁶⁴ 吳全峰、許慧瑩，前揭註 136，頁 63。

¹⁶⁵ 吳全峰、許慧瑩，前揭註 136，頁 69-70。

¹⁶⁶ 依衛生福利部組織法第 5 條第 1 項第 3 款規定：「本部之次級機關及其業務如下：三、中央健康保險署：規劃及執行全民健康保險事項。」

用本法第 16 條之規定。



由於戶政機關當初係基於戶政之目的而蒐集國民身分證相片資料，如今卻基於危害防止之目的而將資料傳遞予警政署，此利用行為涉及於蒐集目的外利用個資，具體而言，涉及個資法第 16 條之但書第 2 款之規定，以下將分析此依傳遞行為是否符合個資法第 16 條但書第 2 款「增進公共利益所必要」之情事。

第二款 傳遞行為與個資法第 16 條但書第 2 款「增進公共利益所必要」

個資法第 16 條規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為維護國家安全或增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、有利於當事人權益。七、經當事人同意。」首先，戶政機關此一資料傳遞行為，所面臨的第一個問題為戶政機關作為資料傳遞機關，其目的外利用行為是否也須符合第 16 條本文規定之「執行法定職務必要範圍內」？若採肯定之見解，學者稱之為「並立模式」，須雙方機關都為了執行各自之法定職務而不得不利用該資料，如此將大幅限縮目的外利用之情形¹⁶⁷。反之，若採否定之見解，學者稱之為「擇一模式」，僅須傳遞機關或接收機關其中一方為「執行法定職務必要範圍內」即可合法進行利用¹⁶⁸，而我國法務部之函釋亦採否定之見解¹⁶⁹。回到本文，不論係採擇一說或並立說之見解影響並不大。於前述，本文

¹⁶⁷ 洪宛伶，前揭註 149，頁 53。

¹⁶⁸ 洪宛伶，前揭註 149，頁 54。

¹⁶⁹ 法務部法律字第 10403508020 號函：「三、單純釐清個資法之條文文義或規範意旨者（二）：按

實際上資料傳遞之軌跡係由內政部將資料交付予警政署，而警政署與內政部間係具有上下隸屬關的行政機關¹⁷⁰。內政部的法定職務範圍，依內政部組織法第 1 條規定：「內政部掌理全國內務行政事務。」職是之故，與警察有關之事務亦屬於內政部的法定職務範圍，且有關警察勤務之執行，亦有警職法此行為法的授權，因此不論採取擇一說或並立說之見解，均會符合個資法第 16 條本文「執行法定職務範圍」的規定。

戶政機關傳遞資料之行為，若要符合個資法第 16 條但書第 2 款之規定，尚須滿足必要性以及增進公共利益之情事。增進公共利益為不確定法律概念，其內涵十分抽象，係指不特定多數人得分享的利益，而是否有「增進公共利益之情事」須個案判斷。於本文之情形中，警察執行危害防止任務維持社會秩序的同時，亦會增進公共福祉，因此滿足增進公共利益的要求。因此戶政機關傳遞相片資料予警政署，該傳遞行為的合法性，重點在於「必要性」之判斷，究竟傳遞行為是否為警政署執行危害防止任務所必要？而為滿足必要性之要求，須戶政機關傳遞相片資料的行為為警察執行危害防止任務所必須始可。因此問題的核心在於警察危害防止任務之內涵。以往警察危害防止任務的核心係阻止有高度蓋然率即將對警察所保護的法益發生損害之行為，進而達到為害防止之目的，同時降低犯罪率。若由此觀點出發，戶政機關似無傳遞國民身分證相片資料予警政署的必要，因危害防止針對的是有高度發生危害蓋然率之行為，使用警政署自有的資料庫（例如：

個資法第 16 條規定：「公務機關對個人資料之利用，除第 6 條第 1 項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：…」是以，如符合該條但書所列各款情形之一，即得排除本文「應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符」之規定，而得將個人資料為特定目的外之利用。換言之，該條但書所列各款情形乃是立法者衡酌人格權之保護及促進資料之合理利用後所作出之價值判斷，允許公務機關得在符合所列各款情形之一時，就個人資料為特定目的外之利用，且無須受限於其法定職務必要範圍內（例如：甲機關為執行其法定職務所必要，向乙機關請求提供資料，如乙機關依「法律明文規定」有配合提供資料之義務，此時乙機關配合提供資料雖係協助甲機關執行其法定職務，而非執行乙機關自身之法定職務，仍可認其符合資法第 16 條但書第 1 款之規定）。

¹⁷⁰ 依內政部組織法第 5 條規定：「內政部設警政署，掌理全國警察行政事務，統一指揮、監督全國警察機關，執行警察任務；其組織以法律定之。」

通緝犯資料庫、前科犯資料庫、治安顧慮人口資料庫）來建置人臉資料庫便可達到危害防止之目的，畢竟於身分上，通緝犯才是預防犯罪的根本，而非針對一般國民。惟如今，由於資訊時代的來臨，警察危害防止任務範圍有逐漸擴張的傾向，加入積極探求危害的面向，如此一來，戶政機關國民身分證相片資料的傳遞，以及後節警察使用該相片資料建置人臉資料庫，或都將因警察危害防止任務的擴張而有其必要性

第三項 警政署取得及使用國民身分證相片影像檔建置

人臉資料庫

第一款 警職法與個資法間的關係

於本文中，警政署作為資料接收機關，其取得戶政機關國民身分證相片資料及使用該資料建置人臉資料庫，原則上應分別適用個資法第 15 條及第 16 條本文之規定。資料蒐集係指以任何方式取得個人資料之行為，例如：警政署依法向衛生福利部中央健康保險署蒐集失蹤人口之就醫時間及地點等個人資料此種自其他機關取得資料之行為亦屬蒐集行為¹⁷¹。因此警政署取得國民身分證相片影像檔之行為，亦屬資料蒐集行為，原則上應適用個資法第 15 條之規定。而針對警政署使用相片資料建置人臉資料庫的行為，此屬資料利用行為，應適用個資法第 16 條之規定，且由於警政署資料蒐集及利用均是基於犯罪預防的目的，因此此一資料利用行為並無逾越蒐集目的，因此無涉個資法第 16 條但書之規定，適用本文之規定即可。惟同時警職法亦針對警察蒐集及利用個資，於本法第 16 條及第 17 條，訂定相應之規定。因此，於警政署取得及使用國民身分證相片資料建置人臉資料庫一事，應適用個資法或係警職法之規定，此一問題涉及個資法與警職法間的關係，

¹⁷¹ 法務部法律事務司，前揭註 154，頁 237。

須先加以釐清。



查個資法於法律適用上，是屬於普通法位階，而警職法則屬於特別法之位階，可參原電腦處理個人資料保護法第 2 條的刪除理由：「中央法規標準法第 16 條：『法規對其他法規所規定之同一事項而為特別之規定者，應優先適用之。』本法的性質應為普通法，其他特別法有關個人資料蒐集或利用之規定，不論較本法規定更為嚴格或寬鬆，依特別法優於普通法之法理，自應優先適用各該特別法之規定。¹⁷²」職是之故，個資法之規定，與警職法相較，屬於普通法之規定，但二者規範目的並不相同。個資法係以「保護個人資料」為目的，而警職法則以「防止或預防危害」為目的。若在個資法無特別保護之規定，而警職法有規定時，則適用警職法，兩者係屬於補充適用之關係，故警察行使職權有關蒐集資料並加以運用、傳遞等，應依警職法之規定為之，警職法未規定，才適用個資法¹⁷³。因此，於本文之情形，由於警職法對於個人資料之蒐集及利用，於本法第 16 條及第 17 條均有規範，故原則上應優先適用警職法之規定。惟細觀之，警職法有關第 16 條及第 17 條之規定，自 2003 年警職法立法以來，迄今並未有任何修正，反觀個資法於 2010 年經過大修，使個人資料的保護越趨完善。將警職法第 16 條及第 17 條與個資法第 15 條及第 16 條進行比較，不難發現其實後者對於個人資料的保護較為完善。

首先，警職法第 16 條規定：「警察於其行使職權之目的範圍內，必要時，得依其他機關之請求，傳遞與個人有關之資料。其他機關亦得依警察之請求，傳遞其保存與個人有關之資料。前項機關對其傳遞個人資料之正確性，應負責任。」為避免機關重複蒐集及節省人力、物力等，因此於本條第 1 項中明訂警察與其他機關間，得依對方之請求，互為傳遞相關之個人資料。而本條的要件有三，一為

¹⁷² 許義寶（2020），〈警察蒐集與利用個人資料職權之研究--以警察職權行使法第十七條為中心〉，《警察法學》，第 19 期，頁 143。

¹⁷³ 蔡震榮，前揭註 96，頁 201。

目的拘束原則，警察在履行警察任務之必要範圍內，有權儲存、利用或變更資料。若取得目的與儲存目的合於警察之目的，即可為之。若儲存目的與當時蒐集目的不一樣時，為目的之改變，資料傳遞原則上受目的拘束，任何目的改變之傳遞係不被允許。二為履行警察任務所必要。所謂警察任務係指警職法所規定警察行使職權之範圍。三為尚未逾越儲存期限¹⁷⁴。由本條的立法理由中可知，本條的本質為機關間的職務協助，為了提高行政效率，避免重複蒐集及節省人力、物力特訂定本條之規範，使機關間得互相傳遞個人資料。換言之，本條允許警察只要是在行使職權的目的範圍內且滿足必要性的要求下，即可向內政部請求傳遞相片資料並依法取得，惟如此戶政機關傳遞相片資料之行為有規避個資法第 16 條規定之虞。再者，本條對於機關間的職務協助並未規範要件，因此相關要件應回歸行政程序法之規定。關於機關間的職務協助，係規範於行政程序法第 19 條中¹⁷⁵。而內政部與警政署係有上下隸屬關係的行政機關，因此依本條之規定，內政部為發揮共同一體之行政機能，應於其權限範圍內互相協助，除協助之行為，非其權限範圍或依法不得為之者；或是如提供協助，將嚴重妨害其自身職務之執行者；抑或有正當理由而不能協助之情形者外，內政部應協助警政署業務之執行。據此，倘警政署依警職法第 16 條之規定要求戶政機關傳遞相片資料及取得該相片資料，由於機關間職務協助的要件，依警職法及行政程序法之規定，實則十分寬鬆，如此，將等同變相架空個資法所建立的諸多有關個人資料保護的保護框架，為個人資料的

¹⁷⁴ 蔡震榮，前揭註 96，頁 197-198。

¹⁷⁵ 行政程序法第 19 條規定：「行政機關為發揮共同一體之行政機能，應於其權限範圍內互相協助。行政機關執行職務時，有下列情形之一者，得向無隸屬關係之其他機關請求協助：一、因法律上之原因，不能獨自執行職務者。二、因人員、設備不足等事實上之原因，不能獨自執行職務者。三、執行職務所必要認定之事實，不能獨自調查者。四、執行職務所必要之文書或其他資料，為被請求機關所持有者。五、由被請求機關協助執行，顯較經濟者。六、其他職務上有正當理由須請求協助者。前項請求，除緊急情形外，應以書面為之。被請求機關於有下列情形之一者，應拒絕之：一、協助之行為，非其權限範圍或依法不得為之者。二、如提供協助，將嚴重妨害其自身職務之執行者。被請求機關認有正當理由不能協助者，得拒絕之。被請求機關認為無提供行政協助之義務或有拒絕之事由時，應將其理由通知請求協助機關。請求協助機關對此有異議時，由其共同上級機關決定之，無共同上級機關時，由被請求機關之上級機關決定之。被請求機關得向請求協助機關要求負擔行政協助所需費用。其負擔金額及支付方式，由請求協助機關及被請求機關以協議定之；協議不成時，由其共同上級機關定之。」

保護留下一個破口。



再者，警職法第 17 條規定：「警察對於依本法規定所蒐集資料之利用，應於法令職掌之必要範圍內為之，並須與蒐集之特定目的相符。但法律有特別規定者，不在此限。」本條與個資法第 16 條相同之處在於針對資料利用行為，均要求原則上資料利用行為不得逾越蒐集目的使用。惟細觀之，個資法第 16 條係要求資料的利用須於「執行法定職務必要範圍內」，但警職法第 17 條卻僅要求「法令職掌之必要範圍內」即可。換言之，個資法要求資料利用行為必須要有「法」定的職掌依據，且依釋字第 535 號解釋之意旨，該「法」須為行為法始可，較警職法第 17 條「法令」之要件嚴格，對於個人資料的保護較為周全。

綜上，本文認為，由立法時間而言，警職法第 16 條及第 17 條之規定，自 2003 年警職法立法以來，迄今並未有任何修正，縱使在個人資料保護法於 2010 年大修後，亦無相應的調整。反觀個資法自 2010 修法以來，對於個人資料的保護日趨完善，再者，若是允許機關得依職務協助為由，請求他機關傳遞所持有的個資及藉此取得他機關所蒐集的個資，對於個人資料的保護將產生衝擊，等同變相架空個資法關於資料蒐集及利用的相關規範。再者，由於行政程序法中對於職務協助，尤其是針對有上下隸屬關係間機關的職務協助，例如本文內政部與警政署的情形，要件十分寬鬆，如此，對於個人資料的保護將產生不利的影響。職是之故，由於警政署使用戶政機關國民身分證相片資料建置人臉資料庫一事，涉及個人資料的蒐集及利用，基於個資法係以個人資料之保護為立法目的，因此本文針對該行為將適用個資法第 15 條及第 16 條之規定加以分析。

第二款 警政署取得及使用戶政機關國民身分證相片資料建置

人臉資料庫



警政署作為資料接收機關，其取得國民身分證相片資料及使用該資料建置人臉資料庫，應分別適用個資法第 15 條及第 16 條本文之規定。警政署取得國民身分證相片影像檔之行為，屬資料蒐集行為，應適用個資法第 15 條之規定。而針對警政署使用相片資料建置人臉資料庫的行為，此屬資料利用行為，應適用個資法第 16 條之規定，且由於警政署資料蒐集及利用均是基於為害防止的目的，故該資料利用並無逾越蒐集目的，因此無涉個資法第 16 條但書之規定，適用本文之規定即可。而不論是針對警政署取得相片資料的資料蒐集行為或是使用該資料建置人臉資料庫的利用行為，依據個資法第 15 條及第 16 條之規定，均要求需為「執行法定職務『必要』範圍內」。因此，不論是警政署取得相片資料或是使用該資料建置人臉資料庫，除需基於特定目的外，此一蒐集及利用行為亦需為執行法定職務所必要始可，以下將說明「執行法定職務必要範圍」此一要件。

「執行法定職務必要範圍」內容上實則包含兩個子要件，一為「法定職務」，另則是「必要性」。其中，所稱法定職務，此「法」需為行為法始可，雖健保資料庫案中，最高行政法院於 106 年判字第 54 號判決中認為僅需有組織法之依據即可，不必另有行為法的特別規定，惟依釋字第 535 號¹⁷⁶及第 603 號¹⁷⁷解釋之意旨以及組織法及行為法的規範內容差異，國家蒐集及利用個人資料，將限制資訊隱私權

¹⁷⁶ 釋字第 535 號解釋理由書略以：「行政機關行使職權，固不應僅以組織法有無相關職掌規定為準，更應以行為法（作用法）之授權為依據，始符合依法行政之原則。」

¹⁷⁷ 釋字第 603 號解釋文略以：「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。」

之保護，不得僅以組織法為依據，亦應有行為法之依據始可¹⁷⁸。回到本文，警政署係為執行臨檢犯罪預防之勤務而取得相片資料並使用該資料建置人臉資料庫，警察執行臨檢勤務有警職法作為職務依據，且警職法為行為法，因此符合法定職務之要求。問題在於，警政署取得相片資料及使用該資料建置人臉資料庫，是否為執行犯罪預防職務所必要？涉及必要性的闡釋。於健保資料庫案中，由最高法院適用的情況觀之，其將該要件視為比例原則，且在案件涉及個資法第 6 條敏感個資的前提下，以「合理性審查標準」操作，此舉有悖於釋字第 603 號解釋中，針對國家大規模蒐集敏感個資且建置資料庫之資訊作為採取中度審查標準的態度¹⁷⁹。若以合理性審查標準判斷警政署取得相片資料並建置資料庫是否為執行危害防止任務所必要，於此標準下，警察取得及建置人臉資料庫之行為有高度可能將通過必要性的要求。或有主張由於只要符合必要性之要求，個資便有被蒐集及利用的可能，進而限制資訊隱私權的保護，因此針對必要性應採取嚴格的標準，係指若不採取該行為，則公務機關的特定任務將不能履行、不能完整履行或不能合法履行的地步¹⁸⁰。本文則是認為針對必要性之標準，依據釋字第 603 號解釋之意旨，由於涉及大規模蒐集以及建置資料庫之資料作為，雖相片資料並非高敏感之個人資料，但人臉資料庫的建置與人臉辨識系統的使用密不可分，加上此一系統對於社會的爭議性，於本文之情形中，針對必要性至少應採取中度審查標準。惟針對必要性不論採取何種標準，問題核心在於警察危害防止任務的內涵。

回到本文，警政署係為執行警職法中危害防止任務而向戶政機關請求傳遞相片資料，由於警職法係針對警察執行危害防止勤務所訂的法律，該法並規範警察行使職權之要件，故為行為法而非組織法，因此警政署取得國民身分證相片資料之爭議並非在於警政署取得該資料有無行為法之授權依據，而在於警政署為執行

¹⁷⁸ 邱文聰，前揭註 163，頁 35。范姜真嫩，前揭註 150，頁 96-97。

¹⁷⁹ 邱文聰，前揭註 163，頁 42。

¹⁸⁰ 謝碩駿(2014)，〈全民健康保險資料庫：一個不可想像其不存在的網羅/北高行 102 訴 36 判決〉，《台灣法學雜誌》，260 期，頁 215-216。

危害防止任務是否有必要取得國民身分證相片資料？



查釋字第 603 號解釋理由書中，針對戶政機關倘係基於犯罪預防之目的而強制蒐集人民指紋，明確否定戶政機關基於該目的而蒐集指紋之合法性，理由書中略以：「有以戶籍法第八條修正增列第二項與第三項規定之修法動機與修法過程為據，而謂強制蒐集全體國民之指紋資料並建庫儲存，亦有為達成防範犯罪之目的云云，惟動員戡亂時期終止後，回復戶警分立制度（本院釋字第五七五號解釋參照），防範犯罪明顯不在戶籍法立法目的所涵蓋範圍內。況關係機關行政院於本件言詞辯論程序亦否認取得全民指紋目的在防範犯罪，故防範犯罪不足以為系爭法律規定之立法目的。」理由有二，一為犯罪預防並不在戶政機關之法定職權範圍之內；二為關係機關自身便否認此一蒐集目的。據此，該號解釋理由書中並沒有否定基於犯罪預防之目的而蒐集個資之情形。而警政署可否基於犯罪預防之目的取得國民身分證相片影像檔之資料？

首先，從目的、機能上來說，警察的作用可區別為「犯罪（危害）預防活動」與「犯罪偵查活動」兩者。而犯罪預防權限乃是警察日常活動的主要範疇，通常是基於國家一般的統治權，直接以維持公共秩序及除去障害為目的，對於國民以命令、強制之手段，限制其自然自由之作用，而此限制之作用便是於犯罪發生的前階段作為¹⁸¹。警察將因所從事者係犯罪預防活動或為犯罪偵察活動而受不同法律規範。相對刑事犯罪偵查活動而言，警察犯罪預防活動係以維護公共秩序為目的，警察職權行使法即是針對警察，於實施犯罪（危害）預防活動時，所得採取措施之法律¹⁸²。針對犯罪預防活動，手段之採取不以犯罪事實的發生為前提¹⁸³，因此權限之發動，亦無令狀原則等刑事程序原理之適用。

¹⁸¹ 梁添盛（2006），《警察法專題研究（2）》，2 版，頁 23，桃園：自版。

¹⁸² 鄭羽軒，前揭註 108，頁 53-54。

¹⁸³ 蔡震榮，前揭註 96，頁 81。

犯罪預防，或廣泛而言，可稱危害防止。所謂「危害」，一般而言，係指一事實狀態或是一行為，若不及時加以阻止，足以對公共安全或公共秩序產生危害之虞者稱之¹⁸⁴。危害的判斷現已轉向採主客觀混和說，倘狀態或行為以可期待的發生進程，具足夠的蓋然性，足以損害警察所保護之法益者，即屬危害¹⁸⁵。因此，危害為損害蓋然性之逼近，損害乃警察法所保護的個人和公共利益遭到波及，此為社會安全和公共秩序的內涵，並具體落實於警職法中（參照警職法第 1 條¹⁸⁶），為警察任務之一，申言之，警察根據警職法行使職權時，即取得授權基礎，當警職法所保護的法益遭受威脅時，表示危害存在，警察有權採取防止措施，也因為危害尚未發生，還未與犯罪產生交集，才須要防止，透過行政手段加以防範，具有向未來形成之性質¹⁸⁷。然自 1980 年代起，資訊時代來臨後，通訊及電腦等科技設備不斷推陳出新，所產生的各種技術屢屢強化更新，而警察為了找出危害的源頭或是防止危害發生，大幅度以資料或是訊息的蒐集為重點，因此資料蒐集的重要性與日俱增，同時「危害」亦被賦予新的面向，跨越已發生危害和即將發生危害之界線，來到尚未露出端倪，但卻值得懷疑的區域，發展出危害防止的新面貌¹⁸⁸。現今，警察危害防止之任務，由於社會環境中危害的成因增多與激進主義之興起，人民的安全需求強度上升，漸漸有將警察任務擴張至得預先發動職權釐清風險的情狀，並採行必要措施之趨勢，由「危害防止」漸漸導向「危險預防」，使得預防國家隨著風險社會的來臨逐漸形成¹⁸⁹。

綜上，警察危害防止之任務，由於資訊時代之來臨加上社會安全需求強度的上升，而被賦予新的面貌，警察危害防止的任務範圍也隨之擴張，由過往針對已

¹⁸⁴ 蔡震榮，前揭註 96，頁 145。

¹⁸⁵ 陳正根（2009），〈警察與秩序法上扣留措施之探討〉，《國境警察學報》，第 12 期，頁 152-153。

¹⁸⁶ 警職法第 1 條規定：「為規範警察依法行使職權，以保障人民權益，維持公共秩序，保護社會安全，特制定本法。」

¹⁸⁷ 陳英淙，前揭註 8，頁 94。

¹⁸⁸ 陳英淙，前揭註 9，頁 5。

¹⁸⁹ 李寧修（2019），〈警察存取預防性資料之職權與個人資料保護：以監視器之運作模式為例〉，《臺大法學論叢》，48 卷 2 期，頁 394。

發生危害或即將發生危害，現今漸漸加入針對有危害疑慮之區域積極探查是否有危害的面向。職是之故，為配合警察犯罪預防任務之擴張，資料之取得更具重要性，背後須有更加完整的資料支持，倘僅有警政署自有之資料（如通緝犯及失蹤人口），恐怕無法因應現今危害防止的任務需求。植基於此，警政署或有基於犯罪預防（危害防止）之目的而取得國民身分證相片影像檔之需要並利用該資料建置人臉資料庫之必要。

第三節 評析

第一項 警政署使用內政部戶政司國民身分證相片資料

建置人臉資料庫

值得注意的是，於機關間共享資料之情形，人民或無法知悉其個資已提供予他機關以及他機關後續利用的情形。依個資法第 9 條之規定：「公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。有下列情形之一者，得免為前項之告知：一、有前條第二項所列各款情形之一。二、當事人自行公開或其他已合法公開之個人資料。三、不能向當事人或其法定代理人為告知。四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。第一項之告知，得於首次對當事人為利用時併同為之。」其中，本條第 2 項第 1 款所稱「有前條第二項所列各款情形之一」的免為告知事由有 6 款，分別為：依法律規定得免告知、個人資料之蒐集係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、告知將妨害公務機關執行法定職務、告知將妨害公共利益、當事人明知應告知之內容、個人

資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。據此，若警政署向內政部取得國民身分證相片資料，係因其執行法定職務所必要時，其處理及利用可免除告知義務。因此警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫，個資法第 15 條及第 16 條有關「執行法定職務必要範圍」此一要件，極具重要性，為個資保護的第一扇門。

第一款 有關「執行法定職務範圍之必要」之內涵

（一）「法」定「職務範圍」：組織法或作用法？並立說或擇一說？

最高行政法院於健保資料庫案中，認定個資法第 15 條及第 16 條所稱「法定職務範圍」，該「法」僅需有機關組織法之依據即可，不必另有行為法之特別規定。惟此一見解，與釋字第 535 號及第 603 號解釋之意旨，有所出入，蓋組織法係規範行政機關間事務的劃分，而行為法則是行政機關對外行使職權的依據，因此僅以組織法為依據便可限制人民資訊隱私權之保障，並不符法律保留原則之要求，尤其健保資料庫案涉及敏感個資大規模的蒐集及資料庫之建置。而本文亦涉及資料大規模的蒐集及資料庫之建置，雖本文認為國民身分證相片資料並非敏感個資，惟此舉亦將限制人民資訊隱私權之保護，因此亦須有行為法為依據。

除此之外，由於本文涉及個資法第 16 條但書第 2 款目的外利用事由的適用，則目的外利用行為是否仍須符合個資法第 16 條本文「執行法定職務範圍之必要」之要件，此涉及並立說及擇一說的爭議。法務部函釋採取擇一說之見解，認定於目的外利用個資之情形，可排除本文「執行法定職務範圍」之規定，但最高行政法院則採取相反之看法，將第 16 條主文「執行法定職務範圍」認定為資料利用的一般性要件，故於目的外利用之情形亦須視符合本文「執行法定職務範圍」的要求，一定程度限制目的外利用行為。針對目的外利用個資的情形是否要符合本文「執行法定職務範圍」，法務部及最高行政法院有不同之見解，若基於個人資料保

護之觀點，肯定說似乎較為可採，惟行政機關間職務範圍並不相同，採取肯定說往後僅有在雙方機關間職務重疊之部分始可傳遞資料，不利於機關間資料的流通，將導致行政成本的增加、行政效率的降低。回到本文，實則不論採擇一說或是並立說之見解，於本文影響不大，由於內政部與警政署間具上下隸屬關係，因此警政署之職務範圍亦為內政部所涵括，故於本文內政部傳遞相片資料予警政署之情形，不論採擇一說或是並立說影響不大，重點在於該傳遞行為是否為執行危害防止任務所必要，警察危害防止任務的內涵為何。

（二）執行法定職務之「必要」：標準？合理審查標準？

於健保資料庫一案中，最高行政法院將該必要性之要件，視為比例原則進行適用，且其標準十分寬鬆，看似採取合理審查標準，亦與釋字第 603 號解釋，針對大規模蒐集敏感個資並建置資料庫之行為，應採取中度審查標準之見解，對於個人資料之保護應審慎對待。或有認為，針對該必要性，應採取嚴格的標準，係指若不採取該行為，則公務機關的特定任務將不能履行、不能完整履行或不能合法履行的地步¹⁹⁰。此一見解較中度審查標準更為嚴格，本文認為，針對必要性之檢驗，至少應採取中度審查標準，始符合個資法保護人民個人資料之規範意旨。

第二款 個資法第 16 條但書第 2 款「增進公共利益」過於抽象

個資法第 16 條但書第 2 款「增進公共利益所必要」此一容許於蒐集目的外使用個資之事由過於抽象，法務部函釋雖嘗試解釋其內涵，亦僅稱以不特定多數人得分享之利益，概念仍十分抽象，且該函釋亦承認此款事由係依抽象概念須個案判斷。惟行政的特徵本來就是公益取向，殊難想像有行政行為不符合增進公益之要件，且考量到我國行政實務向來慣於將公益做廣義解釋，此款事由等同大開行

¹⁹⁰ 謝碩駿，前揭註 163，頁 215-216。

政後門，使機關可透過此一事由無所不能在蒐集目的外利用或提供資料，架空本條目的拘束原則之保護，反致實務上例外成原則之窘境，不利於個人資料之保護。因此有謂基於比例原則之考量，應將此款事由限縮解釋為「重大」公共利益始可¹⁹¹。

第三款 警察「危害防止」的職務內涵

回到本文。警察係為執行危害防止之職務而取得內政部戶政司國民身分證相片資料並使用該資料建置人臉資料庫。不論係在討論戶政機關是否有傳遞相片資料予警政署之必要或是警政署有無取得及使用該資料建置人臉資料庫之必要，均與警察危害防止任務之內涵息息相關。過往警察危害防止任務之內涵，著眼於防止具有高度蓋然性將對警察所保護之法益產生損害之行為，時點上警察危害防止係於犯罪行為未發生前，施以行政手段介入進而達到預防危害的效果，警察危害防止任務著眼於即將發生危害或是已發生危害但未達犯罪，植基於此，警察是否有取得國民身分證相片資料的必要？本文認為仍有待觀察。由此一任務之內涵觀之，警察自有的通緝犯資料庫便可達到犯罪預防之效果，基於通緝犯身分上的特殊性，警察危害防止之任務應著重於此，而非針對一般人民進行犯罪預防。惟現今，由於資訊時代的來臨，社會安全需求提高，警察危害防止任務有漸漸擴張之傾向，轉向警察可積極探求危害之面貌，倘此一轉變為實槌，警察或有取得國民身分證相片資料並使用該資料建置人臉資料庫之必要。

第二項 申請程序及警政署內部使用規範

由內政部所訂定各機關申請使用國民身分證相片資料之的細部程序性及技術性規定可知，內政部係透過資訊連結系統，並以線上資料查詢、檔案傳輸或磁性媒體交換等三種方式之其中一種，將國民身分證相片資料提供予警政署進行利用。

¹⁹¹ 洪宛伶，前揭註 149，頁 56。



而依據管理要點之規定，警政署於申請作為連結機關時須檢具申請書以及其對於該個資的使用管理規範交由內政部進行審核，待審核通過後，才會提供國民身分證相片資料予警政署進行利用。其中，警政署於申請成為連結機關時，申請書中需載明使用個資之目的，且使用管理規定上亦須規範資訊安全措施及監督辦法，因此內政部於審核時，理論上可得知連結機關使用個資之目的及其資安措施，並加以評估資安措施是否完善，個資使用目的是否有利於公益目的，進行實質上的審核。換言之，基於資訊隱私權及個人資料保護之考量，將個資提供（傳遞）予他機關時，傳遞機關同時考量了其他細緻的變因，包括資訊內容、可能的侵害以及資訊安全保護等，惟由於個資法規寬鬆之故，此一審核或將流於形式，且審核之標準為何亦未見於程序規範之中。前階段審核寬鬆，倘後階段的稽核措施又未確實執行，對於人民個人資料的保護將造成十分不利的影響。

第六章 結論



人臉辨識系統自 1970 年發展至今，由於技術發展純熟，此一科技日漸普及，不論係於公領域或是私領域均可見到該技術的身影，而警察亦將此一技術應用於危害防止任務查證身分之行為上，爾後發布針對人臉辨識系統疑慮說明資料，稱此一應用合法無虞，本文聚焦於此一應用的合法性進行分析。人臉辨識系統的使用與臨檢查證身分行為結合將限制基本權，因此依憲法第 23 條之規定，此一應用須符合法律保留原則及比例原則。於法律保留原則方面，此一系統在取得當事人同意之前提下使用，是否仍須法律依據？若仍須法律依據，作為臨檢查證身分及資料蒐集之手段，此一應用可能的法律依據為警職法的相關規定，本文由警察臨檢此一行為的內涵出發，說明為何警職法第 6 條及第 7 條不足作為此一應用之理由及相關資料蒐集條文為何亦不足支撐此一應用。於比例原則方面，倘警察使用此一系統符合法律保留原則，評估此一系統與危害防止目的達成間之關係。除此之外，警察所使用的人臉辨識系統其背後的人臉資料庫除使用機關自有的通緝犯、前科犯、治安顧慮人口及失蹤人口資料庫作為建檔基礎外，最具爭議之處在於整合內政部戶政司國民身分證相片資料，本文亦聚焦於此進行探討。此屬機關間資料共享之情形，涉及個資法上目的拘束原則的原則及例外之規定。結合前幾章之討論，本文將結論總結如下：

一、警察使用人臉辨識系統查證身分之情形

本文首先回顧警察使用人臉辨識系統查證身分之情形，此處之查證身分專指警察依據警職法第 6 條及第 7 條所為，以危害防止為目的，屬臨檢的一環。警察所使用的人臉辨識系統其正式名稱為 M-Police 即時相片比對功能，係內建於 M-Police 警用行動電腦的功能之一，於 2012 年開始啟用，在外執行勤務之警察，

因勤務所需可向所屬機關的資訊科（室）申請專屬的帳號密碼，以便於臨檢時使用此一系統查證民眾身分。警察於臨檢時如遇有使用此一系統的需求，操作上需先登入事前申請之帳密，並點選即時相片比對功能，拍下受檢人的臉部特寫照片並上傳，在進行比對前，更可彈性選定比對的資料庫類別、性別、年齡範圍、以及候選人名單等條件縮小比對來源，爾後，於警政雲端系統進行比對，若系統出現比對吻合之結果，系統將自動將有關之身分資料提供予執勤之員警。

目前，由於該系統的使用未與任何監視器結合，因此無法如英國南威爾斯警局般一次性對不特定多數人進行大規模自動化的人臉偵測與身分辨識行為，我國警察對於人臉辨識系統的使用侷限於一對一的身分查證，且由於該系統整合了內政部戶政司國民身分證相片資料庫做為人臉資料庫的建檔基礎之一，因此該系統最常見於臨檢時使用，作為查證身分的手段之一，本文的研究範圍亦限於此處。此系統提高警察臨檢的效率同時亦減少民眾冒用他人身分之可能。警察於臨檢時，如須查證民眾身分，程序上，仍會先循傳統模式，攔停後，以詢問及令出示身分證明文件的方式獲得身分資料，若無果或懷疑其係冒用他人身分而欲使用此一系統時，會詢問是否同意使用該系統查證身分，在取得其同意的前提下，才會使用人臉辨識系統進行身分識別。

綜上，我國警察對於人臉辨識系統之使用，由於尚未與道路監視器結合，無法一次性針對不特定多數人進行大規模自動化的人臉偵測及辨識，目前的應用停留於一對一的身分識別，須選定特定目標客體拍下臉部照片，且系統不會偵測到人臉後隨即自動進行身分辨識之工作，是否針對特定人進行身分識別由人工操作。此一模式作為警察臨檢查證身分之手段，不僅對於現行法制的衝擊較輕微，亦符合警察臨檢針對特定人的特性。



二、警察使用人臉辨識系統查證身分與現行法制的衝突

(一) 人臉辨識系統的使用與查證身分行為結合將侵害基本權

首先，由於我國將人臉辨識系統的使用與臨檢查證身分行為結合，成為臨檢的一環，作為查證身分的手段之一。因此，警察臨檢對基本權所造成的影響作為影響我國警察臨檢法制的關鍵因素，仍有加以說明的必要。關於警察臨檢對於基本權之影響，已有釋字第 535 號解釋在案，可資參照。警察臨檢涉及進入營業處所、對人民暫時留置以及蒐集身分資料等行為，將對人民居住自由、身體行動自由及隱私權等基本權造成影響。而人臉辨識系統加入警察臨檢時使用，對於人民隱私權影響更甚。人臉辨識系統係使用人臉特徵資料此一個資進行身分識別，而人臉特徵資料具備高度人別識別性，若無外力的影響，具終身不變的性質，此種個資依釋字第 603 號之解釋意旨，屬高敏感個資，為資訊隱私權的保護客體，警察蒐集並利用此種資料，將限制人民資訊隱私權之保護。綜上，人臉辨識系統的使用與警察臨檢結合將限制人身自由、居住自由及隱私權等基本權，而依憲法第 23 條之規定，限制基本權須符合比例原則及法律保留原則。

(二) 現行警察使用人臉辨識系統查證身分並無法律依據

警察使用人臉辨識系統查證身分須符合法律保留及比例原則之要求。於法律保留之討論上，第一層次的問題便是警察若是基於當事人的同意下使用人臉辨識系統查證身分，是否仍須有明確法律依據始可？本文採取肯定之見解，認為縱使基於當事人同意下使用此一系統，仍須有法律依據。查法律保留原則係限制基本權之要件，若在當事人出於自由意志拋棄基本權之保護下，仍要求法律保留，固與本原則之內涵有所不符。惟針對法律保留原則之範圍，我國深受重要性理論之

影響，但凡為「重要事項」均為法律保留原則之範圍，而須適用此原則。因此法律保留原則之範圍，漸漸由干預行政之領域，擴及於給付行政之領域。回到本文，警察使用人臉辨識系統查證身分，鑒於該系統所引發的社會爭議性，加上由於該系統使用內政部戶政司國民身分證相片資料建置人臉資料庫，因此該系統一經使用將有不計其數的潛在受影響者，本文認為警察使用人臉辨識系統查證身分仍須法律保留。

職是之故，警察使用人臉辨識系統查證身分仍須有明確法律依據。第二層次之問題，便是現行警職法是否有明文准許警察使用人臉辨識系統查證身分。而人臉辨識系統作為查證身分之手段，此一應用可能的法律依據為警職法第 6 條及第 7 條，尤其是第 7 條關於查證身分之手段規定。臨檢依釋字第 535 號解釋之意旨，該解釋以：「臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，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。人民之有犯罪嫌疑而須以搜索為蒐集犯罪證據之手段者，依法尚須經該管法院審核為原則（參照刑事訴訟法第一百二十八條、第一百二十八條之一），其僅屬維持公共秩序、防止危害發生為目的之臨檢，立法者當無授權警察人員得任意實施之本意。是執行各種臨檢應恪遵法治國家警察執勤之原則，實施臨檢之要件、程序及對違法臨檢行為之救濟，均應有法律之明確規範，方符憲法保障人民自由權利之意旨。」該解釋以臨檢將侵害基本權利為由將臨檢定性為強制手段，實施臨檢的程序、要件及手段均須有法律明確規定。因此，人臉辨識系統作為查證身分之手段亦同，須有法律明確規定，警察使用此一系統始可符合法律保留原則。惟警職法第 7 條規定有關查證身分得使用之手段，僅限詢問及令出示身分證明文件此二種，而不論是詢問或是令出示身分證明文件，意義上均無法包括人臉辨識系統的使用，概念相距甚遠。再者，依警職法當初立法背景考量，或許亦未設想到此一新興科技可作為查證身分之手段，因此警職法第 8 條、第 9 條至第 11 條有關資料蒐集的規

範以及第 28 條即時強制的概括授權條款亦無法支撐此一應用。換言之，目前警察使用人臉辨識系統查證身分背後實無法律依據支撐此一應用。



於比例原則之討論上，假設警察得基於當事人同意在無法律依據下使用此一系統查證民眾身分或是警職法已明文人臉辨識系統得作為查證身分之手段，警察此一應用仍須符合比例原則，始可確保其合法性。由於人臉辨識系統的使用，涉及高敏感個資的蒐集及利用，加上與警察臨檢結合，依釋字第 535 號及第 603 號解釋之意旨，須該系統之使用有助於危害防止目的的達成，二者間具備密切關聯，且使用上不得逾越必要之程度，警察此一應用始可滿足比例原則之要求，應採中度審查標準。惟目前人臉辨識系統是作為查證身分的輔助工具使用，加上警政署並無任何統計資料說明人臉辨識系統的使用有助於危害防止目的的達成，二者間是否具備密切關聯，在相關資料均不透明的情況下，實在難以判斷，現今使用情形僅能說明人臉辨識系統是一項「好用」的工具，能通過合理審查的標準，但是否為危害防止的「必要」工具，而通過中度審查標準，仍有待觀察。

三、警察使用戶政司國民身分證相片資料作為人臉資料庫的建檔基礎

我國警察所使用的人臉辨識系統特殊之處在於該系統背後的人臉資料庫除使用機關自有的通緝犯、前科犯、治安顧慮人口及失蹤人口資料外，最具爭議之處在於使用內政部戶政司國民身分證相片資料庫之資料建置人臉資料庫，此為機關間資料共享之情形。再者，為使用人臉辨識系統進行身分辨識，人臉資料庫之資料不可能進行去識別化之動作，否則該系統將無用武之地。因此，警政署使用內政部戶政司國民身分證相片資料庫之資料作為人臉資料庫之建檔基礎時，該相片資料並不會進行去識別化，反而會精確地進行個人資料檔案的建置，清楚連接到某一特定人。本文之情形，具體而言，涉及個資法上目的拘束原則的原則及例外

的適用。關於警政署使用戶政機關國民身分證相片資料作為人臉資料庫的爭議，分為兩部分進行說明，第一部分為國民身分證相片資料之蒐集及資料庫之建置與機關申請提供相片資料之程序規範。第二部分為警政署使用相片資料建置人臉資料庫之行為，分為傳遞、取得及使用該資料建置人臉資料庫三個行為分別探討所涉及的法律爭議。

針對第一層次的問題，國民身分證相片資料的蒐集及資料庫之建置與機關申請提供該資料的程序規範。內政部係依戶籍法第 52 條之規定蒐集國民身分證相片資料並建置成國民身分證相片資料庫，而戶籍法為行為法，規定有關戶籍登記的相關要件，故內政部此蒐集相片資料之行為係以行為法為依據。而對於機關申請提供相片資料的相關程序規範，由於警政署申請提供者為國民身分證相片資料，並非戶籍資料，因此相關程序係適用各機關應用戶役政資訊連結作業及管理要點之規定而非適用各機關申請提供戶籍資料及親等關聯資料辦法之規定，此二者之申請程序差異在於若係申請提供戶籍資料，依據各機關申請提供戶籍資料及親等關聯資料辦法第 9 條之規定，須出具資料交換安全協議書（戶政司網站上文件名為戶政機關資料交換安全約定）；惟若係申請提供國民身分證相片資料則無須出具此一協議書，此一差異的理由為何不得而知。此一安全協議書中將載明使用個資之特定目的，檔案傳送之方式，甚至會有相關保密責任及稽核措施之要求，此一文件的效力與行政契約相同，且對於個人資料之保護將有實質上之效果。惟為何僅於申請提供國民身分證相片資料無須出具？此一差異的理由各機關應用戶役政資訊連結作業及管理要點並未說明。除此之外，縱使警政署於申請提供相片資料時，申請書中需載明使用個資之目的，且使用管理規定上亦須規範資訊安全措施及監督辦法，因此內政部於審核時，理論上可得知連結機關使用個資之目的及其資安措施，並加以評估資安措施是否完善，個資使用目的是否有利於公益目的，進行實質上的審核。惟由於個資法規範寬鬆之故，此一審核或將流於形式，且審



核之標準為何亦未見於程序規範之中。

針對第二層次之問題，警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫，此屬機關間資料共享的情形，於個資法的討論上，戶政機關及警政署，就其資料上的行為，應分別適用個資法之規定，且雙方均須符合個資法所規定之要件，始得稱合法，此為雙重評價制或稱為個人資料傳遞之行為評價雙元性。本文涉及個資法第 15 條及第 16 條目的拘束原則的原則及例外的適用，分為戶政機關傳遞相片資料、警政署取得及使用該資料建置人臉資料庫，此三行為分別探討所涉法律爭議。個資法並無完全禁止行政機關間相互提供執行法定職務而蒐集、保有之個資，做目的外利用，倘完全禁止，則各機關於執行各自之法定職務時，均須自己蒐集個資，不得向其他保有該個資之行政機關請求提供，將影響行政效率、增加行政成本，亦可能造成人民之負擔。故在提升行政效率、行政品質、合理利用個資、甚至是為保護當事人權利等考量下，於例外事由所定要件下，應得適度允許行政機關將個資提供給他機關，亦符合個資法第 1 條促進個人資料合理利用之規範意旨，先予敘明¹⁹²。

首先，就戶政機關而言，其將相片資料傳遞予警政署，此資料傳遞行為屬於資料利用行為。由於戶政機關蒐集該相片資料係基於戶政目的，如今卻基於危害防止之目的而將相片資料傳遞予警政署，有於蒐集目的外利用個資之情形，涉及個資法第 16 條但書目的拘束原則例外的適用，具體而言，涉及該條但書第 2 款「增進公共利益所必要」之情事。此一資料傳遞行為涉及兩個問題，一為於個資法第 16 條但書目的外利用之情形是否要符合本文「執行法定職務必要範圍」之要求？此涉及並立說及擇一說之爭議。二為個資法第 16 條但書第 2 款「增進公共利益」之解釋。

¹⁹² 范姜真燊，前揭註 150，頁 99。



首先，個資法但書第 16 條第 2 款「增進公共利益」之解釋，此屬不確定法律概念，法務部函釋亦僅稱社會不特定之多數人可以分享之利益而言，定義十分抽象，而就行政行為的公益導向之特性而言，殊難想像有無法增進公共利益的情形，無疑為機關於目的外利用個資的情形開一後門。本款目的外利用之事由不符合例外應從嚴解釋之法理，不利於個人資料的保護。再者，於目的外利用之情形，是否仍須符合個資法第 16 條本文「執行法定職務必要範圍」的要件？法務部與最高行政法院採取不同之觀點，最高行政法院認為縱於目的外利用之情形，仍須符合本文「執行法定職務必要範圍」之要件。惟法務部則採相反之見解，認為目的外利用之情形無須符合本文「執行法定職務必要範圍」之要求。惟於本文，不論採何種見解，影響不大，因內政部與警政署間係具上下隸屬關係的行政機關，因此凡屬警政署之職務範圍，亦屬內政部之職務範圍。因此內政部基於危害防止之目的而傳遞相片資料予警政署，核心的問題在於戶政機關傳遞國民身分證相片資料是否為危害防止所必要？此涉及警察危害防止任務之內涵。

就警政署而言，其基於犯罪預防之目的取得國民身分證相片資料及使用該資料建置人臉資料庫，由於分別屬於資料蒐集及利用行為，應分別適用個資法第 15 條及第 16 條本文之規定，且並無目的外利用個資之情形。惟在進入個資法之討論之前，由於警職法第 16 條及第 17 條，亦針對警察資料蒐集及利用加以特別規範，因此需先釐清警職法與個資法間的適用順序。個資法的定位屬於個人資料保護的普通法，因此警職法有關資料蒐集及利用之相關規定原則上理應優先適用。惟細觀之，警職法第 16 條及第 17 條之規定，自警職法於 2003 年立法以來並未經過任何修正，反觀個資法於 2010 經過大修，使個人資料保護越趨完善，加上警職法第 16 條本質上為機關間職務協助，職務協助的要件於警職法或是行政程序法均十分寬鬆，因此倘認機關得以職務協助為由，恣意取得他機關所儲存的個人資料，等同變相架空個人資料保護的框架，且個資法才是以個人資料保護為其立法目的。

職是之故，針對警政署取得及使用相片資料建置人臉資料庫一事，本文認為於警職法相關規定未調整前，仍應適用個資法為宜。警政署取得及使用相片資料建置人臉資料庫於個資法之討論上，核心問題在於警政署是否有基於執行危害防止任務之必要而取得國民身分證相片資料，此涉及警察危害防止任務之內涵。

由此觀之，於警政署使用內政部戶政司國民身分證相片資料建置人臉資料庫一事上，不論是戶政機關傳遞相片資料的必要性或是警政署取得及使用該資料建置人臉資料庫的必要性爭議，均與警察危害防止任務內涵息息相關。警察危害防止任務係在於防止警察法所保護的個人和公共利益受損，警察有權採取防止措施，也因為危害尚未發生，還未予犯罪產生交集，才須要防止，透過行政手段加以防範，具有向未來形成之性質。過往警察的危害防止任務著重於已發生危害和即將發生危害的情形。然自 1980 年代起，資訊時代來臨後，由於社會安全需求的上升加上組織犯罪的猖獗，警察危害防止的任務有逐漸擴展之趨勢，來到尚未露出端倪，但卻值得懷疑的區域，發展出危害防止的新面貌，倘此一轉變為實槌，則僅依靠警察自有失蹤人口、前科犯、通緝犯及治安顧慮人口資料建置人臉資料庫，或許不足以應付警察危害防止之任務，而有取得並使用國民身分證相片資料建置人臉資料庫之必要。

四、展望未來

總結而言，為杜絕爭議以及建立民眾對於人臉辨識系統的信心，警察使用人臉辨識系統查證身分應有相關法律依據明文准許警察使用此一系統，且此一系統的使用須公開透明，相關文件及統計數據應公開。再者，針對使用國民身分證相片資料庫建置人臉資料庫一事上，由於資訊時代的來臨，社會日趨多元及複雜，倘未來警察危害防止任務擴展新面貌，使用國民身分證相片資料建置人臉資料庫

或有其必要性，惟為兼顧個人資料的保護，現行個資法或有加以檢討之必要，尤其是個資法第 16 條但書第 2 款「增進公共利益」之解釋及適用，本款事由過於抽象，要件過於寬鬆。於今資訊爆炸之時代，未來機關間共享資料之機會勢必會增加，適用此款之機會也會隨之上升，若該要件之解釋仍如此寬鬆，對於個人資料之保護勢將形成巨大威脅，亦不符目的外利用例外解釋應從嚴之法理。

未來根據警政署於 2019 年回復立法院的文件，在「108 年度警政雲端運算建置案」此計畫中的說明，警政署目前似乎有意再另外建置一個人臉辨識系統，稱為「影像特徵比對系統」，這個新系統與原有的「相片比對系統」的差異目前尚不清楚，但新系統在建置完成後，警政署內部預計將可同時儲存 5,000 萬張以上的照片，並可同時提供最多 1,000 張可能人選的照片（FBI 最多為 50 張可能人選），而針對此一應用立法院亦質詢警政署是否可能使用路口監視器的影像進行人臉辨識，警政署則回以目前道路或監視器由於目的為監看道路人車通行狀況，所攝錄的人臉影像未達可供相片比對系統的基本要求，此一回答的模糊之處在於，不能保證當未來設備更新、架設位置改變後，不會使用路口的監視器對往來的人民進行靜態甚至即時的人臉辨識¹⁹³。因此，未來或許警政署有意讓人臉辨識系統與道路監視器結合，進行大規模的自動化的人臉偵測及辨識。現今僅僅是將人臉辨識系統作為臨檢查證身分的輔助工具便有諸多個資法及警職法上的疑慮，亦突顯我國個資法規範未竟之處。倘將來若將人臉辨識系統與道路監視器結合，進行大規模自動化即時人臉偵測及辨識，法制上如何規範，亦會是一大課題。

¹⁹³ 財團法人台灣網路資訊中心，<https://blog.twinc.tw/2019/09/11/4957/>（最後瀏覽日：12/07/2020）。



參考文獻

(一) 專書

李震山 (1998), 《警察任務法論》, 四版, 高雄: 登文書局。

李震山 (2007), 《多元、寬容與人權保障—以憲法未列舉權之保障為中心》, 2 版, 臺北: 元照。

李震山 (2007), 《行政法導論》, 7 版, 臺北: 三民。

法務部法律事務司 (2016), 《個人資料保護法規及參考資料彙編》, 二版, 臺北: 法務部。

林明鏘 (2011), 《警察法學研究》, 臺北: 新學林。

林明鏘 (2002), 〈警察臨檢〉, 《月旦法學教室 (3) 公法學篇》, 臺北: 元照。

陳敏 (2013), 《行政法總論》, 8 版, 臺北: 自版。

梁添盛 (2006), 《警察法專題研究 (2)》, 2 版, 桃園: 自版。

許文義 (2001), 《個人資料保護法論》, 臺北: 三民。

蔡震榮 (2016), 《警察職權行使法概論》, 三版, 臺北: 五南。

(二) 期刊

王正嘉 (2019), 〈AI 與人臉辨識技術運用於犯罪偵防之問題分析〉, 溫祖德 (等著), 《刑事政策與犯罪研究論文集 (22)》, 頁 235-253, 臺北: 法務部司法官學院。

內政部警政署資訊室 (2014), 《政府機關資訊通報》, 第 317 期, 臺北: 內政部警政署。

內政部警政署 (2013), 《警政工作年報》, 頁 1-434, 臺北: 內政部警政署。



吳采薇(2019),〈英國警察機關使用自動化臉部辨識技術與相關監督機制之研究〉,《科技法律透析》,31卷2期,頁28-39。

李寧修(2019),〈警察存取預防性資料之職權與個人資料保護:以監視器之運作模式為例〉,《臺大法學論叢》,48卷2期,頁393-435。

李建良(2018),〈資料流向與管控環節--個資保護ABC〉,《月旦法學雜誌》,第272期,頁25-31。

李惠宗(2013),〈個人資料保護法上的帝王條款一目的拘束原則〉,《法令月刊》,第64卷第1期,頁37-61。

李佳玟(2014),〈青春專案〉,《月旦法學教室》,第144期,頁33-35。

李震山(2006),〈警察法:第一講警察作用法通論〉,《月旦法學教室》,第41期,頁74-84。

李震山(2006),〈警察法:第三講 警察作用與基本權利保障(一)〉,《月旦法學教室》,第45期,頁77-88。

李震山(2006),〈警察法:第四講 警察作用與基本權利保障(二)〉,《月旦法學教室》,第47期,頁52-62。

吳景欽(2004),〈警察職權行使法中關於臨檢規定之正當性探討〉,《軍法專刊》,50卷6期,頁14-31。

李震山(2002),〈從釋字第五三五號解釋談警察臨檢的法制與實務〉,《台灣本土法學雜誌》,第33期,頁69-78。

林玟君(2018),〈大數據時代的個人資料保護〉,《興大法學》,第24卷,頁1-45。

邱文聰(2018),〈被掏空的法律保留與變質的資訊隱私權憲法保障一評最高行政法院106年度判字第54號判決與相關個資法條文〉,《月旦法學雜誌》,第272期,頁33-43。

林裕順(2015),〈臨檢盤查「半推半就」〉,《月旦法學教室》,第148期,頁24-26。



- 林明鏘 (2010),〈警察行使職權與身分查證之問題〉,氏著,《警察法學研究》,二版,頁 390-408,臺北:新學林。
- 林明鏘(2006),〈論警職法第 28 條之權限概括條款與補充性原則〉,《警察法學》,第 5 期,頁 11-34。
- 林錫堯(2005),〈法律保留原則之理論與實踐〉,《法學叢刊》,50 卷 4 期,頁 1-21。
- 林明鏘(2002),〈警察臨檢與行政程序〉,氏著,《警察法學研究》,二版,頁 378-379,臺北:新學林。
- 林建中 (1997),〈隱私權概念初探—從美國法之觀點切入〉,《憲政時代》,第 23 卷第 1 期,頁 53-78。
- 范姜真嫻(2019),〈自實務判決檢視行政機關蒐集、處理或利用個人資料之問題〉,《警察法學》,第 18 期,頁 91-128。
- 洪家殷 (2018),〈公務機關資料之蒐集與個人資料之保護〉,《東吳法律學報》,30 卷 4 期,頁 29-68。
- 范姜真嫻 (2013),〈個人資料保護法關於「個人資料」保護範圍之檢討〉,《東海大學法學研究》,第 41 期,頁 91-123。
- 洪家殷(2011),〈論行政調查之證據及調查方法—以行政程序法相關規定為中心〉,《東海大學法學研究》,第 35 期,頁 1-43。
- 洪家殷 (2010),〈論行政調查中職權調查之概念及範圍—以行政程序法相關規定為中心〉,《東吳法律學報》,21 卷 3 期,頁 1-52。
- 海岸巡防署 (2018),《海巡雙月刊》,臺北:海洋委員會海巡署。
- 許義寶 (2020),〈警察蒐集與利用個人資料職權之研究--以警察職權行使法第十七條為中心〉,《警察法學》,第 19 期,頁 103-150。
- 陳仲嶙(2020),〈從防疫出國禁令爭議再訪法律保留的疆界〉,《法律與生命科學》,9 卷 1 期,頁 1-37。



陳英淙(2017),〈論警察危害防止與刑事追訴的分與合〉,《政大法學評論》,第 151 期,頁 91-150。

陳英淙(2019),〈從危害概念論警察法中的資訊式職權(informationelle Befugnisse)--以監視錄影為例探討之〉,《軍法專刊》,65 卷 5 期,頁 1-38。

許宏達(2015),〈擺盪在法律保留與契約自由間之行政契約合法性探討--以法定山坡地劃出之切結書為例〉,《軍法專刊》,61 卷 5 期,頁 38-57。

莊國榮(2012),〈層級化法律保留原則的適用〉,《臺灣法學雜誌》,第 208 期,頁 1-15。

張凱淳(2012),〈人臉辨識技術應用於警政治安之探討研究〉,《前瞻科技與管理》,2 卷 1 期,頁 81-92。

陳正根(2009),〈警察與秩序法上扣留措施之探討〉,《國境警察學報》,第 12 期,頁 143-175。

許宗力(2009),〈論法律保留原則〉,頁 117-213,氏著,《法與國家權力》,臺北:元照。

許宗力(2003),〈基本權利:第六講—基本權的保障與限制(上)〉,《月旦法學教室》,第 11 期,頁 64-75。

曾婉菁(2014),〈人臉偵測及辨識方法探究〉,《印刷科技》,30 卷 2 期,頁 21-40。

詹鎮榮(2015),〈公務機關間個人資料之傳遞—以台灣桃園地方法院行政訴訟 102 年度簡字第 2 號判決出發〉,《法學叢刊》,60 卷 1 期,頁 1-27。

廖元豪(2004),〈走自己的路—大法官「法律保留本土化」之路〉,《臺灣本土法學雜誌》,第 58 期,頁 21-40。

謝碩駿(2019),〈行政機關蒐集個資之法律依據〉,《月旦法學教室》,第 198 期,頁 14-16。

謝碩駿(2014),〈全民健康保險資料庫:一個不可想像其不存在的網羅/北高行 102 訴 36 判決〉,《台灣法學雜誌》,260 期,頁 209-217。



謝榮堂（2014），〈法律保留原則於給付行政之適用與例外〉，《警察法學》，第 13 期，頁 123-158。

吳全峰、許慧瑩（2018），〈健保資料庫行政訴訟案：個資保護與健保資料之跨機關流動及二次利用〉，《月旦醫事法報告》，第 19 期，頁 61-87。

林子儀、張陳弘、顏厥安、范姜真嫻、陳鈺雄、李建良、吳全峰、陳昭如（2018），〈最高行政法院一〇六年度判字第五四號判決（健保資料庫案）會議紀錄〉，《月旦法學雜誌》，第 272 期，頁 63-84。

任文瑗，范錚強，許通安（2006），〈資訊隱私侵害行為意圖之研究〉，《資訊、科技與社會》，第 6 卷第 2 期，頁 77-100。

陳慈陽、王毓正（2003），〈論司法院大法官解釋對於基本權保障之理論發展〉，《月旦法學雜誌》，第 98 期，頁 14-30。

（三）學位論文

李誠偉（2015），《巨量資料產生的刑事爭議—以資訊隱私權為核心巨量資料產生的刑事爭議—以資訊隱私權為核心》，私立東吳大學法律學系碩士論文。

官峰任（2018），《臺灣警政單位導入即時影像人臉辨識系統關鍵成功因素之研究》，國防大學管理學院資訊管理學系碩士論文。

周燕輝（2003），《行政調查法制之研究：以警察臨檢法規範為核心》，私立中國文化大學法律學研究所碩士論文。

洪宛伶（2019），《公務機關共用個人資料法制研究》，國立臺灣大學法律學研究所碩士論文。

梁皓雲（2006），《利用區塊人臉特徵為基礎之混合式人臉辨識系統》，國立中央大學資訊工程研究所碩士論文。

馬興平（2008），《論資訊隱私權的保護-從釋字第 603 號解釋出發》，國立中正大學法律所碩士論文。

黃天偉（2017），《銀行保密義務與稅捐調查之衝突與調和—從資訊隱私權之觀點省思—》，國立清華大學科技法律研究所碩士論文。

賴昭嘉（2012），《基於行動裝置與安控系統之人臉辨識系統》，國立台灣科技大學資訊工程學系碩士論文。

薛傑仁（2010），《生物辨識之人臉辨識的方法》，私立亞洲大學生物及醫學資訊系碩士論文。

鄭羽軒（2018），《警察職權行使法諸問題之研究》，中央警察大學警察政策研究所博士論文。