誰能擁有你的臉？全球首宗人臉辨識技術執法應用之司法案例簡析──個人權利保護與執法機關無差別監視之直面對決

吳維雅*

壹、前言

人臉辨識科技（Facial Recognition Technology，以下簡稱FRT）在公私部門廣泛被運用，已與個人生活領域產生密切連結。於私領域，FRT普遍用於解鎖手機；又如旅客搭乘航空器，使用航空公司提供之FRT系統，辦理入出境手續、進行報到、托運行李、實際登機等程序，優點在於可以迅速完成相關手續，節省時間與勞力[1]；再者，提供居家安全防護的門禁管制設施業者，也有將FRT系統融入產品及服務進行銷售[2]；另外，在職場之領域，若干公司也開始採行FRT作為落實員工出缺勤考核、門禁入出管制之工具[3]，甚或在招聘新進員工或遴選職務升遷人選時，使用FRT所提供、蒐集之由各競爭者的表情、動作、語音及選詞等特徵所萃取出來的數據，加以分析評估，作為用人決策之

*本文作者係前台灣高等法院法官，現美國華盛頓大學博士生

註1：Delta航空公司於2018年起率先與美國邊境關務局（US Customs and Border Protection, CBP）及運輸安全局（Transportation Security Administration, TSA）展開一項生物特徵辨識合作計畫（Biometric Program）。先後在美國境內各國際機場採行FRT措施，提供搭乘國際航班旅客自由選擇是否運用該系統接受運送服務。據該公司內部統計，多數旅客對於此項服務並無太大疑慮，進而選擇使用，研究顯示此套系統可以有效節省旅客因登機所需耗費的時間。參 https://reurl.cc/NXRdV5（造訪日期：2021年1月5日）；而我國長榮航空公司也於2020年12月1日加入此項CBP計畫，在舊金山國際機場提供FRT的登機服務。參 https://www.evaair.com/zh-tw/about-eva-air/news/news-releases/2020-12-01-pr-news.html（造訪日期：2021年1月5日）。

註2：藉由FRT及演算法之應用，造訪者被設置於大門外的攝影裝置攝下臉部影像，可用以辨別該人與家庭各主要成員的面孔是否具有相似性，如不相似，會連結到通報系統。系統同時具備解除或啟動警報之功能，用以預防非法侵入他人住宅的侵害行為。參Anne Dennon, What You need to Know About Facial Recognition Home Security Cameras, (Oct. 28, 2020) available at https://www.reviews.com/home/security-systems/facial-recognition-cameras/（造訪日期：2021年1月12日）。

註3：MuthuKalyani.K & VeeraMuthu.A, Smart application for AMS using facing recognition, Computer Science & Engineering: An International Journal (CSEIJ), Vol. 3, No. 5, (Oct. 2013), available at https://arxiv.org/pdf/1401.6130.pdf（造訪日期：2020年12月27日）。

參考。諸如上述有關FRT的科技產品或工具，多半廣為供應商宣稱能夠加快作業流程，有助於企業降低成本並提高效率[4]，也因此而獲得許多消費者的青睞。

至於FRT於公部門的執法應用，一項典型便是為刑事偵查目的而作用。例如，針對過去的犯罪，用以查找辨識嫌犯或確認犯人之同一性；對於未來潛在的犯行，期能有效偵測並作出事前預防。而執法部門使用FRT進行即時監視，從事與犯罪有關的調查，並鎖定特定對象，加以FRT及演算法之運用，配合政府部門掌有的大型人臉資料庫的建制，進行大規模查找搜尋比對匹配嫌犯的工作，這些用途在各國一般都很少受到規範監督。例如，在英國倫敦大都會區[5]、萊斯特郡[6]和南威爾斯[7]，時聞警察以大量部署於街頭的公開攝影機從事即時的FRT監視。然而，為偵查目的而使用即時FRT，亦不侷限於公共場所，服務於倫敦大都會之警方即曾承認使用過由私人在住宅錄製的FRT掃描圖像進行辦案[8]。而由南威爾斯警方試點部署的FRT使用，首先成為全球目光焦點，是目前世界上第一起個人起訴挑戰警方，主張使用FRT執法為違法的司法案例[9]。本文擬就上開案例歷審裁判進行分析探討，透過一、二審法院分別對個人權利保護與警方執法利益兩種不同面向的價值判斷及利益衡量的說明，了解該案就人民自由權利與公眾安全需求的考量，或可作為日後我國在構築FRT執法運用的法律框架的一項參考。

貳、英國南威爾斯警方使用人臉辨識科技執法之司法案例（Edward Bridges v. Chief Constable of South Wales Police）[10]

註4：參Dave Zielinski, Facial analysis technology in the workplace brings risks, Society for Human Resource Management (SHRM), (Jul. 9th, 2020), available at https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/facial-analysis-technology-workplace-brings-risks.aspx（造訪日期：2021年1月13日）。

註5：Live Facial Recognition, METROPOLITAN POLICE, available at https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/（造訪日期：2021年2月5日）。

註6：Justin Lee, Leicenstershire Police expand use of face recognition technology, BIOMETRIC UPDATE, (Sep. 8th, 2015), available at https://www.biometricupdate.com/201509/leicestershire-police-expand-use-of-face-recognition-technology（造訪日期：2020年12日19日）。

註7：South Wales Police allows facial recognition challenge, BBC NEWS, (Jul.12 , 2018), available at https://www.bbc.com/news/uk-wales-44802080（造訪日期：2020年12月5日）。

註8：Leo Kelion, Met Police gave images for King's Cross facial recognition scans, BBC NEWS, (Sep, 6th, 2019), available at https://www.bbc.com/news/technology-49586582（造訪日期：2021年1月20日）。

註9：Jenny Rees, South Wales Police use of facial recognition ruled lawful, BBC NEWS, (Sep. 4th, 2019), available at https://www.bbc.com/news/uk-wales-49565287（造訪日期：2020年12月30日）。

註10：以下有關一審判決內容說明均見UK, High Court of Justice (Queens'Bench Division－Divisional Court Cardiff), *Edward Bridges v. Chief Constable of South Wales Police* [2019] EWHC 2341, 4th

一、案件事實

全球首宗針對警務運用FRT為偵查目的進行司法審查的案例，發生於英國南威爾斯。案件起源於主人翁即代表自由黨起訴、其本身也是自由及民權倡議者的Edward Bridges，於2018年針對南威爾斯警方（South Wales Police）部署的一項自動人臉辨識科技裝置（Automated Facial Recognition Technology Locate[11]，運作原理類同於FRT，為求與該案判決用語一致，以下針對本案之說明概以AFR稱之），分別2次捕獲他在公開場合出現的人臉影像：一次是在2017年12月間，在人流往來頻繁的Cardiff街道上逛聖誕市集時；另一次是在2018年3月間，他參加一場和平示威抗議活動時被攝錄。Bridges主張警方就AFR之部署使用為不合法，提起訴訟主張應交付司法審查。

南威爾斯警方從2017年起即在某些事件發生地點或可能發生犯罪的公共場所進行試點性質的AFR系統部署。該系統每秒鐘可以捕捉50張人臉，再以生物特徵分析法，將捕捉到的人臉影像與警方職務上掌有的臉部影像資料庫內的數據資料進行比對，而資料庫內也建制有警方的監視列表（Watchlists），也就是將警方較為感興趣的人特定出來，例如某些對治安具有危害性的人的相關信息等。AFR使用即時攝影機捕捉公眾的數位影像，其中運用的軟體可以將個別的人臉獨立出來，並且萃取出該人臉部的特徵點，用以創建生物識別模版。AFR系統將模版與政府掌有的大型巨量數位資料庫的數據作比對，以生成與監視列表中列出的臉孔之間彼此的相似度得分。如果比對結果是匹配，該系統會發出警報，警方將檢查這些影像，確認這項匹配，並決定是否對匹配影像所指涉的個人，進行下一步的干預作為；但如果這些被

September 2019. 判決全文參
https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf.（造訪日期：2020年7月12日）。

註11：依據南威爾斯警方針對AFR的公開說明網頁：AFR是一套可以自動偵測到影像或錄影畫面中的人臉，進而與已經建制的（人臉）數據庫作比對。實務上通常的運作程序為：將由街頭臨時設置的CCTV（參見下列註16有關CCTV之說明）取得的「即時」影像，與警方於監視列表（Watchlist）中所列出感興趣的人進行比對，看是否能構產生匹配之結果。如果偵測出匹配結果，系統就會發出警示。另外，也有將犯罪現場的影像（例如CCTV所攝到的靜止影像）與大型影像數據庫（例如由受監禁人的圖組影像匯集而成的數據庫）進行比對。AFR功能有兩種，一為識別，亦即可將未知的嫌疑人或警方所感興趣的人的靜止圖像，與大約由50萬受監護人的數據庫進行比對，可能可以得到約200條結果。在未採用AFR前，通常要花2週時間，才能識別出特定的嫌疑人；但採用AFR系統後，識別結果通常可以同日達成。該過程結合最先進的技術與有豐富經驗的識別官員進行匹配的工作，就整個南威爾斯，該系統已經識別出數百名嫌疑人。AFR是實現人臉辨識技術的「即時」部署，為了定位出警方有興趣的人究竟係屬何人，所在何處，AFR系統將「即時」臉部攝影與預先決定好的監視列表進行比對後，然後生成可得匹配的結果，再由操作者進行審核。未能與監視列表匹配的人臉影像，則不會被記憶或保留。監視列表是一項獨特的部署，不屬監視列表中所列的人民，是不會被識別的。參
https://afr.south-wales.police.uk/（造訪日期：2020年11月2日）。

捕獲的人臉與警方監視列表中的數據比對後未發現足以匹配的對象，則AFR會即刻自動將街頭捕捉到的人臉影像自系統刪除。然而，被AFR系統捕捉到影像的原告Bridges，原本並不列名於警方的監視列表，因此他依據歐洲人權公約（European Convention on Human Rights, ECHR，以下簡稱「人權公約」）第8條[12]（尊重私人和家庭生活的權利）以及英國1998及2018年修訂的數據保護法（Data Protection Act 1998《1998年DPA》；Data Protection Act 2018《2018年DPA》）[13]，起訴主張警方使用AFR為不合法，侵害上開法律賦予他的權利。

二、高等法院Cardiff分區法院（High Court of Justice-Divisional Court Cardiff）之一審認定[14]

一審法院發現使用AFR確實干預到個人依人權公約第8條所享有的權利，也指出本件雖涉及人臉生物特徵，本質上具有隱私性質，就好像DNA能夠析出獨特且具個人識別性的數據信息，且具有普遍且精準識別的功能；然而本件AFR事後發現原告並非監視列表中羅列的注意對象後，隨即將捕捉到的影像刪除，影像存取時間僅為瞬間，整個干預及數據處理的過程都極為短暫，原告的生物特徵數據，瞬間以演算法處理後，即刪除丟棄；本案警方的干預作為雖屬明確，然有規範AFR何時及如何使用之充分的法律授權，加上警察本即享有預防及偵測犯罪之權力，是本件AFR的使用合於比例性，也符合運用科技執法應採公開、透明且涉公眾參與（public engagement）重要性的現行標準；又不違反僅能為特定有限的目的、在有限的時間內、涵蓋於有限的區域內之相關限制，並未過分干預人權公約第8條之權利；且在使用FRT前，也有進行公開宣傳（於社群媒體如臉書、推特上宣傳），通過AFR措施，已成功識別出想要鎖定的個人，有高達37起案件的嫌犯因此被逮捕或遭遇處置，而這些成果在未運用此項科技之前，是無法達成的，也就未能將嫌疑人定位出來，足見警方使用AFR在個人權利與社區利益間存在著公平及衡平，應屬合於人權公約第8條第1項、第2項但書之合法干預。

另外，關於數據保護法（Data Protection Act,《DPA》）的判斷，一審法院認為所捕捉到的個人影像，雖構成個人數據，但因AFR

註12：《歐洲人權公約》第8條規定（第1項）人人享有使自己的私人和家庭生活、家庭和通信得到尊重的權利。（第2項）公部門不得侵犯上述權利。但依照法律規定之干預，及基於民主社會的國家安全、公共安全或國家經濟福祉目的的利益考量，為防止混亂或犯罪，保護健康或道德，保護他人的權利與自由所進行的必要干預，不在此限。European Convention on Human Rights, available at https://www.echr.coe.int/documents/convention_eng.pdf（造訪日期：2020年12月1日）。

註13：原告Bridges主張南威爾斯警方使用AFR違反《1998年DPA》第4條第4項要求使用數據必須遵守數據保護準則之規定，其並主張針對未來潛在使用AFR的情形，另違反《2018年DPA》第35條要求為執法目的而處理個人數據必須合法且公平。並指出員警有未依據《2018年DPA》第64條第1項落實適足的數據保護影響評估（Adequate Data Protection Impact Assessment, DPIA）之違法。

註14：見前揭註10一審判決。

挑中這些影像，使之與其他影像區隔分別開來，使得AFR比單純的CCTV[15]更為複雜。因AFR的原理是利用數位信息來特定各個面孔圖像，並從這些圖像中擷取出有關臉部特徵的信息數據，再與資料庫內有關監視列表中受到關注的人，與其臉部信息數據進行相互比對，進而查明CCTV錄製到之人臉影像信息，與監視列表中受關注的人的臉部信息，是否產生匹配的結果[16]。基於上述性質，為使AFR捕捉到的人臉影像能與監視列表中的信息相匹配，AFR必須使捕捉到的所有影像各自與其他個別影像之間彼此能夠被區隔分辨出來，因此即便警察無意去識別這些未出現在監視列表上的個人，但事實上這項判定，將各個捕捉到的影像之間相互進行區辨識別的處理過程，已經該當《2018年DPA》所規範有關個人敏感數據的處理[17]。

然而，法院進一步認為使用AFR構成的數據處理，並未違反《1998年DPA》規範下的相關原則──認為使用AFR該項處理，已滿足合法及公平的要求。且根據普通法規定，警察有義務預防並偵查犯罪，屬於必要的合法利益，亦符合《2018年DPA》第35條第5項所要求之各款規定[18]，包括須嚴守為執法目的所必要，也

註15：Closed-Circuit Television（CCTV），是指在特定的區域進行視訊傳輸，並只在固定迴路設備裡播放的電視系統，因攝影機通過專用同軸電纜線路或無線通信鏈路與監視器和/或錄像機進行通信，採點對點連接模式，但信號非公開傳輸，因此稱之為「閉路電視」，特色在於對於攝錄內容的訪問觸及，係受設計者的限制。主要用於監視以及安全維護目的，例如錄影機、大樓內部的監視錄影器等。參https://en.wikipedia.org/wiki/Closed-circuit_television（造訪日期：2021年1月10日）。

註16：見前揭註10一審判決。

註17：《2018年DPA》第35條第8項b款，條文內容文字：「本條所稱敏感處理，是指為唯一地識別出個人之目的而處理基因數據或生物特徵數據。」條文原文如下：

(3)In this section, "sensitive processing" means──

(b)the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual.見https://www.legislation.gov.uk/ukpga/2018/12/section/35（造訪日期：2021年1月8日）。

註18：《2018年DPA》第35條第3項至第5項，上述條文內容意旨略為：處理如為為執法目的之敏感處理，該處理必須在第4項、第5項所指的兩種情形才能准許。即──(4)(a)取得數據主體同意，且──(4)(b)處理時，控制方備有適當的政策文件（見第42條）；以及──(5)(a)該處理需嚴格審查為執法目的所必要，且──(5)(b)該處理需至少符合Schedule 8其中一項條件，且──(5)(c)進行處理時，控制方應備有適當的政策文件（見第42條）。

條文原文如下：

(3)In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4)The first case is where──

(a)the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5)The second case is where──

(a)the processing is strictly necessary for the law enforcement purpose,

就是在導入AFR數據處理時，必須為執行警察職務所必要。另外，依據《2018年DPA》第35條第5項c款之規定，要求進行數據處理時，數據控制方（Controller，即掌有數據、進行控制的一方，本案數據控制方為警方）必須有適當的政策文件以為執行依據。雖然一審法院認為本案相關的政策文件內容太過簡要，未盡詳實，但法院拒絕作出認定這些現存文件是否充分的判斷，反而指出這項判斷應留待由個別執行的警察，依據個案、遵循信息委員會辦公室（Information Commissioner's Office, ICO）[19]所訂定的指南（Guidance）來處理，始為妥適。此外，一審法院認為本件警方依據《2018年DPA》第64條而製作的數據保護影響評估，已足認符合該條文的要求[20]。

法院也認為本件警方並未怠於依據2010年平等法（《2010年Equality Act》）第149條[21]之要求履行有關消除歧視的義務，也沒有任

(b)the processing meets at least one of the conditions in Schedule 8, and
(c)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42). 見
https://www.legislation.gov.uk/ukpga/2018/12/section/35（造訪日期：2021年1月18日）。

註19：UK Information Commissioner's Office (ICO)，為英國政府組織中專責資訊安全與隱私權維護的獨立機關，負責執行相關法律、受理隱私權爭議申訴，並作出判斷，也被賦予制定行政規則之立法權限。參https://ico.org.uk/about-the-ico/what-we-do/（造訪日期：2021年1月15日）。ICO於本案一審期間，針對警方試點使用AFR之爭議，曾作出一份調查報告，報告中強調司法應謹慎審查，認為“如不採取適當的隱私保護措施，這項新的侵入性技術可能帶來的會是破壞，而非強化對警察的信心…任何使用這套系統的警察部隊或私人組織都應意識到現存的數據保護法律及相關行政指南仍然適用”。ICO同時表示，日後該機關在制定有關即時人臉辨識系統立法建議與執法指南時，會把本案判決的內容納入考量。參
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/09/statement-high-court-judgement-frt-south-wales-police/（造訪日期：2021年1月7日）；而本案二審判決後，ICO再次針對判決發表意見，認為上訴法院判決釐清了警察在公共場使用即時人臉辨識技術的情況，“臉部識別依賴於敏感的個人數據，然而要在人們的隱私權，與警察必須有效執行其功能角色而施用監視技術的行為間，取得平衡，具有相當的挑戰性。但要使公眾對警察及其行動產生信任與信心，就必須具備清楚的法律框架，本件（上訴法院）的判斷，恰為此跨出了有效的一步。”參
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/08/ico-statement-on-the-court-of-appeal-judgment/（造訪日期：2021年1月7日）。

註20：《2018年DPA》第64條主要在要求當處理可能對個人自由權利產生高風險結果的個人數據時，數據控制方（Controller）必須在處理前進行數據保護影響評估，即預期該處理操作對於個人數據保護影響的評估。評估內容必須包括數據主體之自由權利遭受的風險、如未解決該風險所預設之措施、審酌數據主體跟其他人的權利及合法利益，以確保個人數據保護的維護及安全機制。為確定某種處理方式可能導致對個人自由權利產生的風險，以及數據控制方必須考慮到該項處理的本質、範圍、背景及目的。本條文見
https://www.legislation.gov.uk/ukpga/2018/12/section/64/2018-05-25#:~:text=64Data%20protection%20impact%20assessment&text=(1)Where%20a%20type%20of,a%20data%20protection%20impact%20assessment.（造訪日期：2021年1月15日）。

註21：平等法第149條要求公部門在行使其職能時，必須善盡充分考慮消除歧視、騷擾、受害及任何其他本法禁止行為的需求；要考慮增進對具相關保護特徵之人與或不具相關保護特徵之人，彼此間機會

何建議案指示警方何時開始試驗AFR，或指示警方承認或應承認AFR系統下的軟體，也許以某種間接歧視的方式在運作。一審法院認為：即便AFR的使用處理違反了人權公約第8條，但符合《1998年DPA》、《2018年DPA》之規定，且未違反2010年平等法《2010年Equality Act》，滿足了合法及公平的要求，又警方採取之手段也合於比例原則及數據保護原則，因此認為本件AFR的使用為合法，而於2019年9月4日判決駁回原告所有的請求。

三、上訴法院（Court of Appeal of England and Wales）之二審認定[22]

Bridges不服原判決，提起上訴，主張一審法院判決有如下謬誤：(1)將警方使用AFR誤為合於人權公約第8條第2項屬對原告合法的干預。(2)將使用AFR侵害原告權利，誤為合於人權公約第8條第2項符合比例原則之干預。(3)誤認本案已依《2018年DPA》第64條規定落實充足的數據保護影響評估（DPIA）。(4)將警方以AFR處理臉部敏感個人數據誤為已依《2018年DPA》第42條規定提出適當的政策文件。(5)警方未依2010年平等法《2010年Equality Act》第149條規定，履行公部門應盡的平等義務（Public Sector Equality Duty，PSED），因為警方實施的平等影響評估明顯不足，未能意識到基於性別或種族的間接歧視。上訴法院同意前揭上訴理由所持論點(1)、(3)及(5)，另駁斥論點(2)及(4)。茲分述如下：

（一）有關人權公約之判斷

1.原告方上訴理由

上訴法院認為本案警方使用AFR，顯然存在法律依據上的根本缺陷；亦即，警方並無針對防止恣意使用提出足夠的法律保護，尤其是關於使用AFR的政策文件更是不足，這使得警方在依現有政策文件執行時，個別執法員警可以決定究竟何人會被列名於監視列表，也可決定究竟AFR要配置何處。如此一來，個別員警的裁量空間極大。實則，政策文件必須清楚表明賦予警方自由裁量的範圍及其行使的方式為何，上訴法院檢視警方最近版本的政策文件，認為並未明確表明員警得以行使裁量權的具體內容，這將使得AFR不只可以用於警方有合理事由相信某個處所會出現監視列表

平等的需求；要考慮促進具相關保護特徵之人與或不具相關保護特徵之人保持良好關係的需求。在善盡促成具相關保護特徵之人與或不具相關保護特徵之人間機會平等需求的充分考慮下，尤要充分考慮消除具相關保護特徵之人遭受不利影響的需求，就與在不具相關受保護特徵需求不同的情況下，要採取滿足具相關受保護特徵之人的需求，並鼓勵具相關受保護特徵之人參加公眾生活。另外，在充分考慮具相關保護特徵之人與或不具相關保護特徵之人之間建立良好關係時，要特別考慮到解決偏見及增進了解的需求。本條文見
https://www.legislation.gov.uk/ukpga/2010/15/section/149（造訪日期：2021年1月15日）。

註22：以下有關二審判決內容說明詳見*Edward Bridges v. Chief Constable of South Wales Police* [2020] EWCA Civ 1058. 判決全文參
https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf（造訪日期：2021年1月18日）。

上所列的個人，尚可擴及其他人，上訴法院指出這樣的裁量行使屬於“不可容許的寬泛”（Impermissible wide）。此種形式下之法律架構，欠缺滿足人權公約第8條第2項但書必要的品質，因此認為警方的政策文件未能滿足法律平等的精神。上訴法院同時指出，通常情況應以**警方是否有理由相信是否某處所有監視列表中的個人出現，以作為決定是否在該處部署AFR的重要判斷因素**。

2.原告方上訴理由

原告方主張警方執法未依比例原則，認為個人的權利及社區的利益都是構成比例原則分析的一部分，不能只考量對原告個人的影響，亦須考量AFR在其他相關場合被用來處理其他所有人的生物特徵數據的情形下所造成的影響。惟此項主張遭到上訴法院駁斥。法院認為AFR既已被認定為不合法如前述，則無庸再考慮於部署時，是否合於比例原則之問題；且原告最初的申訴只詳述AFR對自己的影響，並非針對廣大公眾，然而發生在其他每一個相關人身上的影響，與對於原告的影響一樣，都是微不足道的，不應作累積性的認定，因為所發生每個個別、微小且不重要的影響，並不會僅僅因其他人也受到類似影響，就會變得重要。法院認為，比例原則所要求的均衡執法並非單純的數學習題，也不是簡單的乘法問題，而是一項必須進行實質審查進而作出判斷的課題。

（二）有關數據保護之判斷

1.原告方上訴理由

原告主張本件警方作出的數據保護影響評估存在三個缺陷。第一、該評估未能辨識出所捕捉到的特定人，其個人數據並未列於監視列表上，本應即刻自動刪除，但警方仍對這些個人數據進行數據保護法規意義下的「處理」行為。第二、該評估並未認識到在人權公約第8條下的個人權利，是藉由對個人數據的「處理」行為而被包含進來。第三、該評估對於AFR所引發的其他風險，例如可能危及表現自由或集會自由，也都隻字未提。原告因而主張警方未能執行充分適足的數據保護影響評估。此外，ICO經由訴訟參加，也在該案進行中針對警方的數據保護影響評估提出批評，認為該評估並未包含對隱私、個人數據及保護措施的評估，且未能認識到AFR所牽涉的個人數據蒐集是一整個無差別的蒐集，如果發生錯誤結果，可能會發生個人數據被長期性的保存，未被立即刪除的風險。此外，認該評估未能解決使用AFR可能引起潛在的性別及種族偏見的疑慮。因此，ICO認為該評估未依照《2018年DPA》第64條規定進行適當的風險評估並減緩風險。

據此，上訴法院雖未完全同意原告方的上述各項主張，但也點出這份評估報告與人權公約第8條的關聯性。認為依據該評估報告，法院承認使用AFR確實侵犯了個人依人權公約第8條第1項的權利，故本案警方部署AFR為不合法，從而警方在該評估報告中聲稱未違反人權公約第8條也是錯誤的，儘管該評估報告試圖解決人權公約第8條的問題，但上訴法院也點出，上述警方執法的缺

陷，使得該評估報告無可避免地被認為未依《2018年DPA》第64條所要求對於數據主體享有的自由、權利所面臨的風險作適當的評估，也未能就解決這些缺陷所帶來風險採取對應之措施。

2.原告方上訴理由

原告主張針對《2018年DPA》第42條有關提出適當政策文件的要求，不應根據ICO的指南而把該等文件是否具備充分性的評估任務交給警方判斷，而是應由法院來認定。但此項論點遭到上訴法院的駁斥，認為：在AFR部署時，《2018年DPA》還沒有生效，因此當時沒有所謂未遵循法律的問題；另外針對AFR的未來使用以及適當的政策文件要求，《2018年DPA》第42條所指的文件是項持續發展中的文件，會隨著時間推進，以不斷進行檢視與更新的方式，來保存該份政策文件；由於在一審法院審理時，ICO尚未針對此類政策文件頒布指南，然鑑於警方已經根據事後頒布的ICO指南進行政策文件的更新，因此認為一審法院此部份的認定應屬適當。上訴法院並提到：即便最好的理想狀態是政策文件能夠包含更多的細節，但ICO事實上已經反覆表達出警方提出的文件原始版本合於第42條要求的立場，因此上訴法院認為原告持未有適當政策文件作為上訴理由的部分，並不成立。

（三）有關公部門應盡之平等義務之判斷

1.針對原告方上訴理由

關於原告方主張本案警方未依2010年平等法《2010年Equality Act》第149條履行公部門應盡的平等義務，因平等法賦予公部門此項義務的目的在於確保公部門執法時不致無意間忽略應獲取的信息。關於此點，上訴法院認為，本案警方未提出足夠的證據，證明AFR系統使用前，是否存在著可能基於種族和性別的固有偏見，因此認為警方違反政府應盡的平等義務。法院之所以認為警方在事前或使用AFR時均未遵循平等法第149條善盡平等義務，是因為發現警方未能提出足夠證據，證明AFR科技於使用前是否存在間接歧視的風險，作出這樣的認定原因有二：第一、因這些被捕捉的影像所得出的個人數據，經過比對，如發現未與監視列表中的人有所匹配，那麼這些經捕獲的個人數據就應被自動刪除，而被刪除的數據也就無法成為評估分析偏見存在與否的依據。第二、本案警方並不知道這套AFR的數據組是經過機器學習[23]（Machine learning）訓練過的，因此警方也未能

註23：機器學習是人工智慧發展的一部分，是透過讓機器自主學習並自我增強的演算法，透過迴歸分析，機器能從一堆數據中找出規律並做出預測，當輸入的數據越多，演算法也會隨著持續調整，並做出更精準的分析。參 https://reurl.cc/E2RLYK（造訪日期：2021年1月10日）。應用在人臉辨識科技的情況，則機器學習可以透過輸入越多的人臉數據，讓系統的演算法持續不斷被大量的數據訓練演算，進而逐步作出調整，達到更多更精確的人臉比對匹配的結果。

證明在訓練數據中是否存在人口失衡[24]（Demographic imbalance）即帶有偏見的訓練數據[25]（Training data）。上訴法院並未直接指摘AFR的運作一定會產生偏見，而是反面指出本案警方從未試圖以直接或獨立的確認方式，針對本案的辨識軟體不會產生無可接受的種族或性別上偏見進行瞭解與確認；再者，法院判決中表更示，雖然AFR是一項新穎且充滿爭議的技術，但寄望警方在未來如有意使用此項技術時，要能夠針對一切情形自我要求竭盡合理之能事，以確保所使用的軟體無從生成種族或性別之偏見。

上訴法院推翻原審判決認定之結果，認本件警方AFR的使用欠缺法律基礎，且未具備充足的政策文件指引執行，再加上對監視列表及AFR部署地點的選擇，警察被賦予過大的裁量權，AFR之使用不合法且不符合比例原則，違反人權公約第8條。另外，認為警方未進行適當的風險評估並減緩風險，未依平等法履行其平等義務，未確認AFR未存在不可接受的偏見。基本理由，法院於2020年8月11日撤銷原判，改判警方AFR之部署為不合法，原告在上訴審終於贏得本件訴訟。

四、對上訴法院判決的幾點迴響

本案上訴法院並非完全否定警方本於預防犯罪、偵測犯罪職能而部署AFR之必要，而是強調必須解決使用AFR的法律授權及其他根本性問題。本件裁判為全球首宗針對人臉辨識科技運用於執法目的所進行的司法審查，若能夠通過本判決所提出的一些論述要點，驅使出針對未來使用科技偵查、新形態執法合法性議題的廣泛且全面性的辯論，對於人臉辨識的未來法律定位與政策走向，應有幫助。據此，本文針對本案判決提出以下幾點迴響。

第一、上訴法院特別點出AFR（屬於一種警方試點移動式的部署）與僅為定點式的CCTV[26]不同，因前者涉及新穎複雜的技術，包含能夠自動處理大量具有個人識別性的數位信息，例如AFR技術涵蓋了機器學習（Machine learning）[27]能力，能夠增益演算法

註24：人口統計學（Demography）是社會科學中針對關於人口的規模、結構、發展及變化的研究，研究內容涵蓋許多實質性領域，包括在性別、年齡、種族、家庭出身以及歷史或文化背景如何塑造個人的生活和機會等面向。參 https://reurl.cc/WE1MM7（造訪日期：2021年1月30日）。而人口失衡，即指針對人口統計學在上述實質研究領域中發展與變化與呈現出來的不均衡現象。

註25：訓練數據是一組初始的數據，用來幫助在機器學習（Machine learning）的計畫中，去學習如何應用諸如神經網絡的技術來加以學習，並產生精密的結果。它可以藉由驗證及測試集的後續數據集進行補充。訓練數據也稱為訓練集、訓練數據集或學習集。數據集是計算機學習如何處理信息的材料。機器學習也使用演算法，去模仿人腦接受各種輸入，並權衡它們的能力，以便在單個神經元的大腦中產生活化的過程。參 https://www.techopedia.com/definition/33181/training-data（造訪日期：2021年1月25日）

註26：參前揭註15。

註27：參前揭註23。

促進自我調整、訓練學習，進而演算出更為精準的計算結果；然而，AFR所進行的這些大量比對人臉影像數據是否匹配於警方的監視列表對象的工作，所處理的大多數都非警方所感興趣的人，也就是大多數其生物數據被處理的人，都非監視列表中所列的個人，而AFR所處理的數據（人臉影像數據），均屬數據保護法《DPA》的敏感個人數據，也因此上訴法院在本案中有認知到：AFR係有別於單純由CCTV擷取影像之系統，有必要採取即更為精確、更加嚴密的法律保護措施，以保護數據主體。

第二、上訴法院已認定本案警方使用AFR，係已侵犯到個人之隱私權及數據保護權，認為現時足以規範AFR的法律架構明顯有嚴重欠缺，法院也發現《DPA》及警方政策文件並未提供關於在何處使用AFR的明確指南，包括是否應僅限於必須有情報顯示，有監視列表列明或被認為應列入該列表的某個人，其可能會出現的某個地點，才能在該地點部署AFR等內容。在政策文件不足的情況下，這些部署AFR的決定原本是委由個別執行任務的警察自行行使裁量權，而非以現時有效的法律作為支撐，也就是與上訴法院在本案中所發現的一樣，在這種賦予警察過大的裁量權的情形下，執行AFR之部署，是明顯欠缺干預個人數據及隱私權的適當法律基礎。

第三、針對未來AFR的使用，當執法機關對於執法所需的信息，如處於無法取得的情況下（此處的信息，是指當AFR所用的基礎軟體或演算法可能存在著種族或性別偏見的相關信息，而這些信息可能只有軟體的製造商知悉，警方無從得知這些信息），然而出於商業利益及商業敏感性的考量，通常不可期待軟體製造商能夠主動提供經訓練的演算法所需的必要數據集，而這些數據集正可用來評估這些演算法軟體是否存在著不可接受的性別或種族偏見所必要。上訴法院發現，如果沒有這些可供評估偏見存否的數據集信息，警方將難以履行其作為公部門的平等義務，也正因為此等義務是一種警方必須親自履行、無法委託轉嫁他人的義務，因此也無法仰賴軟體製造商或其他機構來代替警方履行評估其所使用的AFR軟體是否不存在偏見之義務。在這種情況下，警方未能適當履行平等義務，也因此未能向公眾保證不論其種族或性別，在制訂或實施政策之前，警方都已經適當的考量了他們的利益。然而，本件上訴法院並未表明使用AFR不可避免是不合法的，因此，在適當的法律架構推出前，以及AFR對個人權利及平等的影響評估作出後，AFR使用才有可能邁向合法的境地，即便僅僅是像南威爾斯警方所從事的是試驗性質的AFR，仍然有完善法律架構的必要。在這個脈絡分析下，除非短期內有更好的法律規範及保障措施可以一舉到位，否則現實上，使用AFR都可能難以成為合法，而這也意味在妥適充分的法制規範推出前，暫時停用AFR，以度爭議，未嘗不可成為一種選項。

第四、至於原告主張法院在評估人權宣言第8條對權利的干預比例時，不應僅考量該技術實際使用效果所及的對象，亦應考慮可能因AFR而被侵犯其自由、權利的潛在對象。原告這項論點雖遭法院駁斥，表示法院不考慮可能發生於未來的“假想情況”（Hypothetical

scenario）[28]。然而，對於一個人隱私權的侵犯程度可能相對較小，但真正的問題在於對大的群體甚或整個人群的隱私權普遍性的干預，這可能會出現在未來發生的案例中，成為需要面對思考並解決的問題。而為了衡量AFR技術在實際使用下所產生的利益，以及其潛在對個人的影響，要解決這個問題，首要之務必須確保一個強大且徹底的數據保護影響評估（DPIA）能夠被執行且落實，並且要要求公部門在使用該項技術，必須維持透明性與具問責性為前提。同時必須確保數據保護影響評估（DPIA）必須與AFR一起搭配使用，警方必須提供一個有詳盡說明的政策文件作為執行之輔助，而該政策文件也必須具體確定如何使用該項技術，而非賦予執法員警過大的裁量權。

五、本案之效應──對司法的肯認尊重，對立法的迫切需求

全球首宗由個人為挑戰公部門為執法目的所為的AFR部署，提起之司法審查案例，原告個人為抵抗警方所為無差別人臉辨識部署而起訴，雖不獲一審法院支持，但上訴法院作出翻轉性判決，使得代表著無以計數個人的原告方，取得這場法律防衛戰中的重大突破性勝利。此可由參與整個程序甚深的自由黨將此判決的獲勝描述為“在反對歧視性及壓迫性人臉辨識的抗爭中，取得重大的勝利”[29]可得明證。

而本件上訴法院判決一作成，南威爾約警方即表示無意提起上訴[30]，其首席警官Matt Jukes亦公開聲明：上訴法院的判決點出了社會必須關注、但政府仍著墨甚少的政策領域。警方的首要任務是保護公眾，惟有能確保警方承諾以負責任的態度及公正的方式來使用新技術，才能獲得公眾的信任；目前警方已與內政部、警察學院、國家警察局長委員會及負責監管全國監視攝影機的獨立委員會長官（Surveillance Camera Commissioner，SCC）[31]熱切討論如何順應判決結果，作進一步調整；機關之間相互合作非常重要，期能盡快將上訴法院作成決定的事項，納入警方

註28：參前揭註22二審判決。

註29：Liberty wins grounded-breaking victory against facial recognition tech, l.lBERTY, (Nov. 11th, 2020), available at https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/（造訪日期：2020年10月8日）。

註30：見South Wales Police use of facial recognition technology was proportionate rules Court of Appeal, (Aug. 11th, 2020), available at https://www.scl.org/news/12026-south-wales-police-use-of-facial-recognition-technology-was-proportionate-rules-court-of-appeal（造訪日期：2021年2月3日）。

註31：監視攝影機委員長（Surveillance Camera Commissioner, SCC）係由英國內政大臣依據保護自由法（Protections of Freedoms Act, 2012）所任命的獨立委員會官員，負責監管監視攝影機系統（如CCTV）及與這些系統連接的任何事物（如自動人臉辨識演算法）有關之運作，為監管全英國警察部隊在公開場所使用監視攝影機的獨立監管者。參 https://www.gov.uk/government/organisations/surveillance-camera-commissioner（造訪日期：2020年12月20日）。

執法之實務指南[32]。

南威爾斯警方及犯罪委員長（South Wales Police & Crime Commissioner）Alun Michael判決後也隨即公開發表聲明，堅持預防犯罪、維護安全、自信且具有韌性的社區環境是警方的首要職責，也點出使用創新及擁抱人臉辨識技術至關重要，因為唯有這樣，才能讓警察在整個南威爾斯社區中提供最好的服務與運作；他認為上訴法院的判決對於形塑未來人臉辨識科技的運用有絕對的幫助，也期許著日後社會能在維護人民安全與確保公民自由兩者之間，進行明智均衡的公眾辯論，警方將會採取公開透明的方式繼續保持執法均衡[33]。本件上訴法院裁判認定警方就AFR的部署違反隱私權、數據保護法及平等法之情事，這也意味著過往英國警方長期習於在街頭大量使用AFR的作法[34]，可能會有所改變；而南威爾斯警方及英國其他地方警察部隊是否會順應此判決結果，重新評估AFR之部署，以及將會採取何種保護措施，容待日後進一步觀察。

此外，監視攝影機委員長（SCC）[35]Tony Porter於二審裁判後也立即提出公開呼籲，指出國家相關機構不應消極應對，如果希望能夠以合於道德與法律規範來使用AFR，那麼無論是技術本身、法律架構以及執法之人，都要能夠得到公眾的信任。法院已論知AFR的使用有明顯的法律缺陷，內政部跟國務卿都不應睡著，應該反思法院的意見，聽取獨立任命之監管者的意見，並提出建議；也要進行組織改革整合，重新檢視並更新法規；他也認為，本判決並沒有對技術產生致命影

註32：見Response to the Court of Appeal judgement on the use of facial recognition technology, South Wales Police, (Aug. 11th, 2020), available at https://www.south-wales.police.uk/news/south-wales/news/featured/2020/response-to-the-court-of-appeal-judgment-on-the-use-of-facial-recognition-technology/（造訪日期：2021年2月5日）。

註33：South Wales Police & Crime Commissioner Rt Hon Alun Michael ‘s statement, (Nov. 11th, 2020), available at https://commissioner.south-wales.police.uk/en/news/commissioner-statement-following-the-court-of-appeal-judgement-on-use-of-facial-recognition/（造訪日期：2021年2月1日）。

註34：一份由European Union Agency for Fundamental Rights於2019年11月27日作成的研究報告指出，英國在當時是唯一積極使用真實的監視列表（Watchlist）進行即時人臉辨識科技試驗的歐盟成員國。而第一個在英國使用人臉辨識科技的便是南威爾斯警方，該警局初始時係將AFR系統大量部署於大型運動賽事，用於偵查刑事案件偵測及預防犯罪。見Facial recognition technology: fundamental rights considerations in the context of law enforcement, Report of European Union Agency for Fundamental Rights (FRA), 11-12 (Nov. 27th, 2019), available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf（造訪日期：2021年1月13日）。本案上訴法院在判決後的新聞摘要也指出，南威爾斯警方於2017年5月至2019年4月間，在各種公共活動中大約部署了50餘次的AFR，AFR能夠每秒掃描50張面孔，前述期間及數量的AFR部署，估計未經數據主體同意而取得個人臉部生物特徵此敏感個人數據的數目，可能已多達50多萬人，而這些面孔絕大多數不在監視列表之中。參 https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Press-Summary.pdf（造訪日期：2021年1月10日）。

註35：見前揭註31。

響的意圖，如採用最新穎的先進技術，同時也要確保公民安全，那勢必就要訂出針對技術使用、監督具有明確標準的規範準則[36]。發表上述言論後，Porter即刻於2020年11月頒布一份內容完整的報告，目的在使日後警察於英格蘭及威爾斯的公開場所使用結合人臉辨識技術的公開監視攝影機系統時，能夠有一套完善的實務作法及指南可以遵循，也據此能夠精準定位出列於監視列表上的對象。Porter這份報告非常重要，因為它代表了Bridges案作成以來，政府機構主動頒布的第一份指南。該份報告主要目的並非指摘AFR為違法，而是在建立良好的實踐措施，協助英國警察部隊順應應用科技執法時所面臨的艱鉅廣泛的挑戰，特別是在使用AFR時要能履行法定義務，以確保未來使用即時人臉辨識技術的合法性[37]。

在*Bridges*案於2020年8月11日作成的同月間，主管的監視攝影機委員長馬上推出這部內容詳盡、因應法律要求的實務指南報告[38]，足見藉由司法審查機制對於導正AFR的合法使用有著立即且明顯的功能，這也是三權分立制度下，行政、立法、司法權之間相互制衡調和的極佳典範之一。監視攝影機委員長作為政府部門內一個組織的獨立官員，同時兼具政策執行及行政規則制定權能，其所屬機關對於建立AFR相關規範指南勇於承擔責任，積極任事，足為其他政府機關之表率。即便實務指南在法位階上，尚無絕對的拘束力，但仍提供英國警方一套健全而完整用於AFR執法的規範架構，也可堪執為英國甚至其他地域主權未來在立法規範AFR時得參考的素材。

參、代結語：未竟的法源——兼評我國科技偵查法草案相關條文

大法官釋字第603號解釋明確指出：指紋屬於人的生物特徵，具有獨特性與個人識別性，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，國家如欲以強制方法大規模蒐集國民之指紋資料，其資訊之蒐集必須與重大公益目的之達成具有密切關聯；如有多種手段可資達成目的，必須採取侵害較小之手段

註36：Tony Porter, Surveillance Camera Commissioner's statement: Court of Appeal judgment (R) Bridges v South Wales Police - Automated Facial Recognition, (Aug. 11th, 2020), available at https://www.gov.uk/government/speeches/surveillance-camera-commissioners-statement-court-of-appeal-judgment-r-bridges-v-south-wales-police-automated-facial-recognition（造訪日期：2021年2月2日）。

註37：Facing the Camera, Report of Surveillance Camera Commissioner, (Nov. 2020), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf（造訪日期：2021年1月10日）。

註38：此份實務操作指南內容涵蓋六個具體面向，包括：生物特徵識別、平等與道德；人權、依法與法律框架；治理、核准、監視列表、受保護特徵及人為決策者；完整性、使用素材作為證據及處理素材；公眾參與、信息提供、績效；問責與認證。參前揭註報告（該份報告內容龐雜，宥於篇幅，容或日後如有餘裕另為專文評析）。

為之；並應以法律明確規定之[39]。準以此解，人臉辨識亦屬獨具個人識別性的生物特徵之一，因此，國家機關如為刑事偵查目的，欲進行大規模蒐集人臉數據，並進行分析比對與匹配，勢必要受到憲法第22條、第23條比例原則、法律保留原則之拘束。然而，即便現今FRT於我國在警務及刑事偵查實務上的使用已經堪稱普遍[40]，然迄無現時有效的法律規範可為授權依據或賦予監督制衡機制。

另外，法務部於2020年9月8日公告預告制定「科技偵查法」，提出草案供公眾審閱並表示意見[41]。該草案版本對於以刑事目的之科技偵查手段，依照公部門所需不同的調查方式，涉及不同程度之干預型態，採層級化處理，亦即干預程度越大，規範要件越嚴格，審查密度就越嚴密；反之，則較寬鬆。通觀該草案條文，有關在公共場所部署FRT，進行即時性蒐集辨識特定人臉的監視作為，或有可能落入該草案第3條第1項所稱的干預標的與受其指定方式之限制；亦即，對於位於**非隱私空間之人**或物，**秘密實施監看**、與聞、測量、**辨識、拍照**、錄音、錄影之調查屬之；於偵查中檢察官認有必要，或檢察事務官、司法警察（官）於調查犯罪情形及蒐集證據之必要下，始得為之[42]；另審諸該條項的草案說明，有關本條所稱非隱私空間之定義，依草案第2條，係屬隱私空間以外之空間[43]。然而，部署FRT相機攝錄鏡頭的地點，通常為公共場所，例如街頭、路口、重要的交通樞紐如轉運站、火車站、地鐵站、商業區、住宅區或學校周邊等公眾可及之處所，顯非草案第2條第2款所指的隱私空間，而屬第2條第3款的非隱私空間。如順此邏輯，自應落入該草案第3條所指的標的範圍，無庸再就受干預之人或空間場所是否具有合理之隱私期待進行判斷[44]，即得由檢察官、檢察事務官或司法警察（官）依職權判斷執行之必要性，自行從事干預即可，也無需進行法官保留或令狀審查之程序。然而，

註39：見釋字第603號解釋，司法院，2005年9月28日，參 https://reurl.cc/6y0OmO（造訪日期：2021年1月10日）

註40：參見吳維雅，〈公共場所運用人臉辨識科技執法適足性之研析──以美國憲法第四修正案為框架〉，《檢察新論》，2020年8月，28期，第143-144頁。人臉辨識科技的運作原理，亦參前揭吳維雅文，143頁暨注釋3。

註41：見法務部2020年98法檢字第10904527940號「科技偵查法」草案公告及附件草案總說明、草案條文。草案內容參 https://join.gov.tw/policies/detail/d1fb429e-a4a9-40f9-8a26-a592f7e73e9f（造訪日期：2021年1月8日）。

註42：見前揭註草案第3條第1項。

註43：按該草案第2條第2款定義隱私空間為：住宅、建築物、交通工具或其他具有隱蔽設施之地上物之內部空間，且具有隱私或秘密之合理期待。同條第3款則定義非隱私空間為前款以外之空間。參前揭註42草案第2條。

註44：草案第3條之說明欄第2點亦指出：就非隱私空間進行科技偵查，除非隱蔽空間之要件外，尚需符合無合理隱私期待之要件，在此前提下，不需過度限制執法機關以科技設備或技術計行調查，但仍以必要情形為限，且調查方式受法定限制。參前揭註42草案第3條說明。

如該草案片面以「隱私空間」與「非隱私空間」二分為斷，即認定在公共場所運用FRT執法不需嚴密監督，而在未實質探究FRT的運用脈絡和原理，未考量可能發生的風險疑慮的情況下，逕採寬鬆之立法，難認對FRT有妥適充足的規範；再者，公共場所中，如經部署密度極高的CCTV，滴水不漏地捕捉任何可能經過的人臉影像，大量普遍性地存取公眾的生物特徵數據，再用以與監視列表上的對象進行無差別式的辨識比對與匹配，實難認無過度執法之虞；此種情形，就好比在海中撒下綿密的流刺網進行漁撈，連僅僅瞬間路過的人們都難以倖免，對於個人如意欲享有「被孤立的權利」（Right “to be let alone”[45]），或想保有不受干預的自由，都將構成重大侵擾與威脅，並不因身處公共場所而有不同；是以，個人遭受此種干預，是否仍保有隱私的合理期待，容有商議空間[46]，未可一概而論。從而，針對FRT應用於偵查執法之目的，上開草案對於個人權利保護是否已為合理周詳之考慮，仍非無疑。而該草案經公眾辯論過程後，因普遍意見認為爭議過大，是以在預告期屆滿後，草案由法務部自行取回繼續進行研議修正，迄今尚未定案送交行政院為後續之審議[47]。

綜上，復衡酌依據我國個人資料保護法，生物特徵辨識數據亦未劃入敏感性個資之範疇[48]，致使目前我國針對FRT的執法應用，在法律基礎上可謂付之闕如，更遑論提供同上開Bridges案中，由上訴法院諭知的隱私權、數據保護權、公部門平等義務的保護。然而，對應於FRT的執法應用目前已如火如荼開展之現況，以及數據主體的權利保護高度需求，二者間的折衝協調與利害權衡，亟須社會上的公民，協力凝聚問題意識，積極參與審議討論；更需要立法者對此議題持續保持關注與熱情，積極介入，勇於倡議，以保障個人權利為首務，同時又能兼顧鼓勵創新執法，增進警方效率，維護社會安全的利益，為充滿爭議的FRT執法，打造出一套雙贏可行的方案。

註45：“Right to be let alone”為美國前最高法院大法官Louis Brandies在加入最高法院的26年前，作為一名年輕律師，針對當時社會上不斷有名流人士遭小報記者侵入私領域、尾隨跟拍而流出的隱私照片之事件，公開發表言論，認為必須採取對人的保護，確保個人享有被孤立的權利（Rright to be let alone），這句話成為日後隱私保護研究中的經典語句。Brandies大法官嗣後於1890年與Samuel Warren共同於《哈佛法律評論》發表名為“The Right to Privacy”（4 Harvard L.R. 193 (Dec. 15, 1890)）的文章，是後世人研究隱私權必讀之文獻，足為經典。參Leah Burrows, To be let alone: Brandeis foresaw privacy problems, BrandeisNow, (Jul. 24th, 2013), available at https://www.brandeis.edu/now/2013/july/privacy.html（造訪日期：2021年2月5日）。

註46：見前揭註40吳維雅文。該文對在公共場所運用人臉辨識科技執法是否保有隱私合理期待有較為深入的分析探討。

註47：參周志豪、王聖藜，〈科技偵查法草案惹議，法部研議修正〉，聯合新聞網，2020年9月17日，https://udn.com/news/story/7321/4866245（造訪日期：2021年2月5日）。

註48：依據我國個人資料保護法第6條，敏感性個資僅含有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，未包括生物特徵辨識數據（Biometric data）。