匯民聲

刷臉遍地開花 須保信息安全

人臉識別缺乏統一行業標準 個人信息亟需法律法規保護

「刷臉」正成為特色鮮明的一種智慧生活方式。坐車能「刷臉」，消費購物能「刷臉」，進出小區門禁能「刷臉」，甚至就連上個公廁也可以「刷臉」取廁紙。不過，隨着「刷臉」應用遍布各類生活場景，個人生物特徵被隨意錄取，信息安全因此面臨遭洩露的風險。多名行業人士及學者表示，「刷臉」時代的確存在亂象，亟需行業標準、法律法規為民眾的個人信息安全保駕護航。同時，人臉識別技術不應「因噎廢食」，創新和信息安全需做好平衡，堅守科技創新造福於民的初衷。

●香港文匯報記者 孔雯瓊、倪夢璟、夏微 上海報道

●雖然「刷臉」便利生活，但不少民眾擔心相關的個人信息安全隱患。圖為成都一名顧客早前通過「刷臉」支付系統自助結賬。 資料圖片

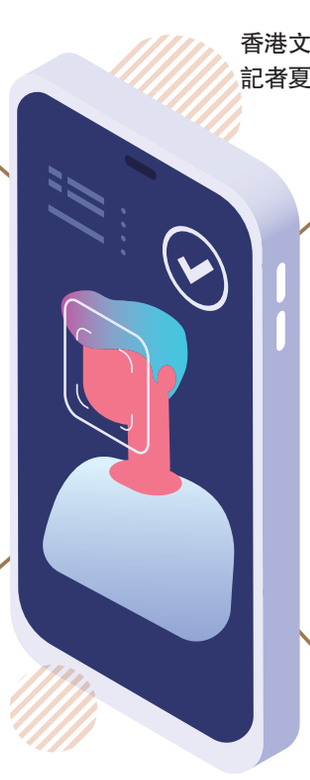
民眾反應

香港文匯報記者夏微 攝

王先生：體驗過「刷臉」進小區、進公司。感覺很好，一推出就馬上辦理人臉採集。不擔心侵犯個人隱私，因爲機場、高鐵站都會採集人臉信息，現在生活中哪裏會有不採集個人信息的地方呢？

張女士：坐飛機過安檢的時候有過「刷臉」的經歷。生活中不怎麼用，因爲不太清楚到底是什麼公司做的人臉識別系統，萬一做這個的公司不正規怎麼辦？只有政府部門提供的設備才敢信任。

受訪者供圖



香港文匯報記者夏微 攝

劉先生：小區實行「刷臉」解鎖門禁已經一年多，非常贊許。這樣可以把不是本社區的人員隔離在外，極大地提升了小區的安全性。

受訪者供圖

朱先生：去超市、便利店結賬用過「刷臉」支付，人臉識別應用到生活中還是很方便的。但是個人隱私和信息，應該受到法律法規的保護，防止個人信息的洩露帶來的風險。

「換臉」App恐含隱私漏洞

近期，在內地抖音平台上，通過一款名為Avatarify的App製作的趣味視頻風靡一時。不過，在內地登上下載排行榜不久，這款AI「換臉」App便悄然下架。

與此前紅極一時的「換臉」App——ZAO類似，Avatarify也是通過「一鍵轉換」，讓用戶僅需提供照片便可以得到想要的「換臉」動態圖片或視頻。

在普通大眾參與這項娛樂的同時，也有不少用戶開始意識到輕易上傳個人信息，有極大安全隱患。網友提醒，「最近很火的『螞蟻呀嘿』（抖音視頻）會不會對人臉識別技術有影響，往壞處想，類似這種技術會不會被拿去冒充別人進行人臉掃描？」

而即便上述軟件已下架，網上還有人提出可以付費幫忙製作動態視屏。雖然有少數網友表達了對視頻製作的興趣，但仍有網友說：「個人隱私一定要自己保護好。」還有網友笑稱，「付費把自己的Face ID（人臉識別）獻出去的操作也是滿分。」

相關法規（部分）

民法典

第一千零三十二條

自然人享有隱私權。任何組織或者個人不得以刺探、侵擾、洩露、公開等方式侵害他人的隱私權。

信息安全技術個人信息安全規範

5.4（c）

收集個人生物識別信息前，應單獨向個人信息主體告知收集、使用個人生物識別信息的目的、方式和範圍，以及存儲時間等規則，並徵得個人信息主體的明示同意。

網絡安全法

第四十條

網絡運營者應當對其收集的用戶信息嚴格保密，並建立健全用戶信息保護制度。

第四十一條

網絡運營者收集、使用個人信息，應當遵循合法、正當、必要的原則，公開收集、使用規則，明示收集、使用信息的目的、方式和範圍，並經被收集者同意。

●袁海說，人臉識別技術在可預見的未來會有一波技術升級。圖為早前一名戴口罩的村民在北京大興區禮賢鎮東安村入口成功進行人臉識別。 資料圖片

本月的一個中午，白領陳小姐在上海人民廣場來福士的大食代吃午餐。在這裏，所有的餐飲檔口都配備了「刷臉」設備，陳小姐對着設備上的攝像頭，「嘀」一下，不到一秒就完成了支付。

上海肇觀電子科技有限公司市場總監袁海表示，人臉識別技術不僅僅會局限在金融和安防領域，而且會向百姓的出行和居家各個行業進行延展。交通行業方面，去年起，多個城市已經落地地鐵、城市公交等的「刷臉」乘車業務。在日常居家行業，越來越多的品牌開始推廣帶人臉識別功能的民用電鎖。

「AI識別人臉的速度是非常快的，金融支付領域的『刷臉』整體速度會在1秒左右，安防領域的門禁、考勤甚至在0.3至0.5秒即可識別。」袁海說，「刷臉」技術特有的便捷性，甚至可以改變未來生活方式。

強制「刷臉」入小區 業主質疑

然而，「刷臉」也引發了一系列關於個人信息安全的探討。家住上海松江一處高檔小區的劉先生表示，「去年1月小區就通知，小區門禁卡不再使用，以後只能通過人臉識別進入。」劉先生稱，為了辦理，需要帶着身份證、戶口本去物業進行人臉信息錄入。當時就有不少居民質疑，身份證、戶口本信息，物業有權獲取嗎？需要強制只能「刷臉」進入嗎？後期信息洩露怎麼辦？

業者：隱私保護法律框架初步建立

對於上述疑惑，袁海表示，「『刷臉』場景確實存在一些亂象，原因在於各路廠商平台湧入市場，又缺乏統一的管理。這就會帶來一些數據洩露的隱患，包括註冊數據、行動軌跡數據甚至個人財務數據等，這些洩露會帶來非常嚴重的後果。」

就算部分「刷臉」設備上會註明「個人信息不作保留」，但袁海說，這更像是「安慰劑」。「誰也不知道信息是否被收集，廠家和平台全憑良心做事，因為目前沒有一個統一的行業標準出台。」

規範的腳步已經在跟進。羅蘭貝格執行總監李冰表示，目前中國的隱私保護立法和標準制定都在逐步完善，從2016年的網絡安全法到2020年的個人信息安全規範，已基本建立起了隱私保護的基本框架。預計未來一至兩年中，數據安全法和個人信息保護法大概率也會陸續通過，屆時市場運行的法律基礎將進一步夯實。

袁海亦稱，「據我所知，內地一些城市已經開始試點規範化信息採集，比如由政府部門錄入人臉數據，再對應下發到前端設備。而且人臉圖像亦會做保護 ，能看到的僅僅是抽象之後的人臉特徵。」

未來市場發展由應用場景拓展驅動

多名受訪者均提及，有必要在確保安全的前提下繼續發展人臉識別技術。李冰指出，人臉識別其實是人工智能技術的一個應用場景，中國在應用技術層面競爭力較強，未來「刷臉」市場的發展主要由應用場景的拓展驅動，他強調，要鋪好底層的隱私保護法律基礎，把市場的功能交給市場去做，讓產業在不損害消費者利益的情況下自然發展。

掃碼看片

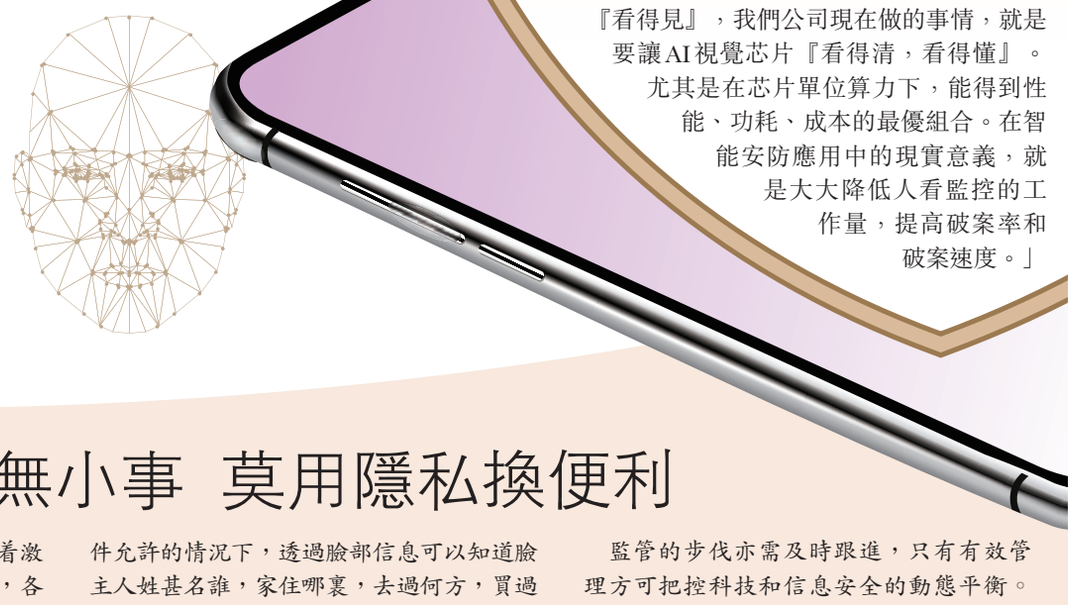
一旦破解 風險極高

據內地媒體報道，一家內地的科技公司瑞萊智慧Real AI團隊宣布，通過AI算法生成特殊花紋，攻破了19款手機的面部解鎖系統。從技術層面來說，人臉識別到底是否安全？

杭州電子科技大學副教授徐偉棟說，「刷臉」支付存在着不少的安全問題，「其中最大的風險當屬人臉等生物特徵的不可重置性。」他舉例表示，以密碼為代表的傳統支付手段也有可能被竊取或洩漏，但客戶只要重置密碼，就能讓攻擊者獲得的舊密碼失去價值，這意味着風險的上限是發現密碼洩漏之前的財產損失。但由於人臉識別這一種生物特徵無法重置，一旦洩漏，「就會意味着在互聯網的某個角落裏，永遠留着你的個人（信息）『鑰匙』，風險的上限是非常高的。」

技術升級有望保障安全

不過，亦有行業人士持樂觀態度。袁海說，人臉識別技術在可預見的未來會有一波技術升級的行業需求，會加築起一道又一道的防線來保障安全。相對應的，更高AI算法複雜度帶來的對AI芯片的算力提升要求，後續市場對芯片算力的需求會進一步提高。他舉例，「比如說傳統監控只是讓機器『看得見』，我們公司現在做的事情，就是要讓AI視覺芯片『看得清，看得懂』。尤其是在芯片單位算力下，能得到性能、功耗、成本的最優組合。在智能安防應用中的現實意義，就是大大降低人看監控的工作量，提高破案率和破案速度。」



微觀點 「人臉」無小事 莫用隱私換便利

當下社會正經歷着激動人心的科技變革，各類人臉識別場景鋪天蓋地冒出，很多人「靠着一張臉」開始在生活中暢行無阻。但是，那些一味追求便捷的人們，對自己的「人臉價值」認知迷茫，這就不可避免身陷隱私遭洩露的危險地帶。

在信息時代，人臉等同於數據，在技術條件允許的情況下，透過臉部信息可以知道臉主人姓甚名誰，家住哪裏，去過何方，買過什麼，資產多少。這些對個人而言至關重要的信息，甚至可以在一秒內就完全讀出。

隱私大過天，個人信息安全無論何種情況下，都不應作爲交換便利的代價。用戶在「刷臉」時，需要有知情權，並可以有選擇權。有權力知道自己的生物特徵信息是否有保障，更有權自行選擇是否開啓「刷臉」功能。

監管的步伐亦需及時跟進，只有有效管理方可把控科技和信息安全的動態平衡。可喜的是目前內地已有地方在試點由當地政府部門牽頭人臉數據統一管理和應用，法律法規中開始新增或提及對個人隱私的保護。

相信在不久的未來，規範管理會一步一步做到位，創新科技只有在有效的法規和規範的基礎上，才可以做大做強。