



香港文匯報訊(記者張帥北京報道)備受消費者關注的央視「3·15」晚會,今年將第一彈瞄向了網絡和數據安全。爆料指,基於人工智能和大數據的人臉識別技術正在深度融入民生服務、城市治理、安防保障等各個領域,但不少商戶在消費者不知情的情況下,違規利用人臉識別技術,記錄消費者信息。針對人臉識別亂象,中國工信部在16日發布的《2021年工業和信息化標準工作要點》指出,將研究與制定網絡和數據安全標準,並編制相關指南。

# 商戶違規收集 刷臉遭「偷臉」

## 非知情下兩分鐘即拍三張 工信部：擬研制網絡和數據安全標準

當前,各式的監控攝像頭在民眾生活中幾乎已經無所不在,這些攝像頭大都是以保障公共安全為目的,但是部分商家所安裝的攝像頭看似普通,實則暗藏玄機。曝光信息稱,不少科勒衛浴門店安裝有具有人臉識別功能的攝像頭,在顧客不知情的情況下,抓取人臉數據,生成人臉ID。

### 有平台擁上億人臉數據量

除了科勒衛浴、無錫寶馬汽車4S店,港匯恒隆MaxMara專賣店,也被發現安裝有人臉識別功能的攝像頭。相關「捕捉」記錄顯示,不到兩分鐘,消費者便被攝像頭的人臉識別功能抓拍了三次,角度雖然不同,但人臉編號卻都相同,消費者人臉信息被商家精準掌握。

目前,提供這種人臉識別攝像頭的企業至少有四家,分別是萬店掌、悠絡客、雅量科技、瑞為信息等。悠絡客公司有經理透露,其一家就已經安裝了「上百萬」個人臉識別功能攝像頭。萬店掌公司薛經理更是表示,他們平台目前擁有人臉數據量已經「上億」。

### 去年60人涉竊賣「人臉」被捕

商家獲取消費者人臉信息有何用?調查顯示,在後台,商家可以對搜集的人臉數據進行編號、備註信息等,並且還可以獲取客戶在不同門店出入、消費記錄,以後顧客再去哪家店,去過幾次,商家便都會知道,然後再有針對性地進行營銷。令人更為擔心的是,人臉識別正在成為違法犯罪新手段。2020年,60名犯罪嫌疑人在竊取、販賣人臉數據被公安部抓獲。

### 洩露將威脅財產隱私安全

信息行業專家指,人臉信息屬於個人獨有的生物識別信息,目前已經成為很多用戶的賬號密碼、支付密碼等,但由於用戶無法更改自己的人臉信息,一旦洩露,將嚴重威脅用戶的財產安全和隱私安全。日常生活中,人臉識別具有無意識性與非接觸性,個人很可能被長時間大規模地積累數據而不被察覺,具有很強的侵入性。

目前,雖然中國國家市場監管總局在《個人信息安全規範》中明確規定,收集個人信息時應獲得個人信息主體的授權同意,但是目前在大多數應用場景,被搜集信息的個體幾乎都被「蒙在鼓裏」。

今年政府工作報告中,明確將「加強網絡安全、數據安全和個人信息保護」作為一項重點工作。香港文匯報注意到,作為維護信息安全的主管部門,工信部在16日最新發布的《2021年工業和信息化標準工作要點》中,將維護網絡和數據安全列為一項重點工作,並透露今年將大力開展5G及下一代移動通信、網絡和數據安全等標準的研究與制定,編制網絡和數據安全強制性國家標準體系建設指南。

### 人臉識別隱患：

- 人臉信息屬於個人獨有生物識別信息,被盜後無法進行「重置」
- 人臉識別無法辨別人臉照片、人臉視頻以及三維人臉面具
- 數據收集者存儲的大量的面臉信息,是黑客侵入的主要對象
- 人臉信息洩露,容易威脅個人隱私以及財務等多方面安全

整理：香港文匯報記者張帥



不少商家在消費者不知情下,通過人臉識別技術違規收集消費者信息。圖為顧客用刷臉支付系統結賬。資料圖片

## 中央強調健全數字規則 「十四五」推進數據安全立法

香港文匯報訊(記者張帥北京報道)伴隨智能科技發展,刷臉購物、考勤、解鎖、倒垃圾等各類智能場景應用逐漸普及及常見,日常中可以通過「刷臉」解決的事情越來越多。人臉識別無處不在,中央近年來也格外重視個人信息保護,強調健全數字規則。

人臉識別被廣泛應用,主要得益於方便、快捷、高效的特點。據了解,人臉識別的效率高於人工3倍-5倍,其採用的無接觸識別技術,能大大解放雙手。目前,在公安領域的出入境邊檢、刑偵,交通領域的機場、火車站、汽車站等場景,以及教育、醫療、行政等各個方面都已有深入應用。

在帶來方便的同時,人臉識別也引起社會對數據隱私保護的擔憂,一旦收集主體未能善加保護,便會導致大規模洩露。去年底召開的中央經濟工作會議明確強調,要依法規範發展,健全數字規則,完善有關數據收集使用管理、消費者權益保護等方面的法律規範。今年全國兩會期間,國務院總理李克強作政府工作報告提出,要加強網絡安全、數據安全和個人信息保護。

個人信息保護也將是未來很長時間政府工作關注的一大重點。中央近日最新發布的「十四五」規劃和2035年遠景目標綱要提及,要加強涉及國家利益、商業秘密、個人隱私的數據保護,加快推進數據安全、個人信息保護等領域基礎性立法,強化數據資源全生命周期安全保護,加強數據安全評估。並且,中國將推進網絡空間國際交流與合作,積極參與數據安全國際規則和數字技術標準制定。

## 沒制約易踩過界 加強立法劃底線



很多網民可能不了解的是,自己平時在社交朋友圈晒出的各類生活信息,包括本人、好友以及家人的照片,都有可能成為人臉數據違規採集與數據洩露的途徑。而加強信息保護,不能僅指望採集者自律,政府也應加強相關立法,劃定好採集的準則和底線。

對於人臉識別採集個人信息,只要源頭不保存便能避免洩露。實際上,在「信息即價值」的時代,商家很難抗拒保存採集信息的誘惑。央視「3·15」晚會曝光後,科勒回應稱已安排連夜拆

除人臉識別攝像設備,或者做斷電下線處理,同時督促供應商積極配合監管部門妥善處理。但是網友似乎並不買賬,沒有制約,很難相信企業所作出的「僅作到店人數統計」、「對設備所採集的信息不作保存、分析及轉移」的口頭承諾。

曝光一個科勒,市場上可能還有無數個「科勒」在未獲得授權同意的情况下,「悄然」收集客戶的個人信息。目前,有關個人信息安全尚只有一些行政部門的「規範」,在法律不完善的情況下,一旦受到利益驅使,人臉識別就很容易滑過隱私侵犯的邊界。因此,需要進一步立法立規、制

定標準,對人臉識別技術的應用安全加以引導。

值得一提的是,《個人信息保護法(草案)》去年10月已正式向全社會公開徵求意見,今年兩會期間,傳出草案已提請全國人大常委會審議的消息。草案內容明確提出,在公共場所安裝圖像採集、個人身份識別設備,應當為維護公共安全所必需,遵守國家有關規定,設置顯著的提示標識,草案並對個人權利以及處罰規則作了更加明確的界定,一旦審議通過頒布實施,將對保護個人信息安全發揮重要作用。

●香港文匯報記者張帥



## 被植詐騙軟件 長者手機淪「幫兇」

手機清理軟件入侵老年人手機,讀取老年人隱私信息的問題近日被媒體進行了曝光。然而,老年手機裏的陷阱遠不止這些。日前,記者探訪深圳華強北電子市場發現,針對老年群體設計的智能手機正逐步替代功能機,走進更多老年人的生活。許多商家瞄準這一市場,在老年手機裏植入各種商業軟件或監測軟件,收集老年人的數據或直接控制老年手機進行詐騙。在智能手機出廠環節植入軟件的手段更為直接,這些軟件植入手機以後刪不掉,其潛在的風險也更大,可以說一個針對老年智能手機的灰色地帶正在形成。

### 「用戶想刪都刪不掉」

深圳華強北電子批發市場可以按照要求進行定製手機,不僅有大量老年人為主要消費群體的功能機,一些商家還推出了適合老年人使用的智能手機。一些商家公開表示,企業可以定製這些手機,作為商業促

銷活動中的贈送禮品,廠家可以在所有手機裏幫忙植入企業產品有關的App,並留管理「後門」。包括品牌手機,他們也可以幫忙破解系統,預先將軟件裝進機子,「用戶想刪都刪不掉」。

一位店家老闆展示了兩款定製手機,裏面都按照客戶要求植入了和保健有關的軟件。這位老闆說,對這些企業來說,最重要的是獲取後台數據。

一位通訊行業從業人員稱,「破解系統」、植入App,這實際上就是一個「管理提級」的技術,並不難,只要是正規操作,合法使用,並不算違法。但這種技術又的確可以被犯罪分子所利用,關鍵在於定製者的真正目的。「即使正規系統軟件,獲得授權之後,都可以進行實時監聽,並收集後台數據。」他說。目前符合老年人要求的智能手機,基本都是造價低廉,品牌眾多,這無疑給一些不法分子提供了機會。

### 打印電話清單才知被控制

四川省攀枝花市最近破獲了一起通過在老年手機裏

植入木馬程式進行詐騙的案件,犯罪團伙註冊的「科技公司」就在深圳華強北。據警方介紹,2020年3月,成都一位市民收到一條短信後被詐騙資金6,400餘元人民幣。詐騙短信來自一個攀枝花地區的手機號。攀枝花市公安局東區分局接到線索之後,經調查確認:號主是一位使用功能手機的75歲退休老人,但老人根本不會發短信,發送這些短信的另有他人。

警方調查發現,這位老人的手機被植入了木馬程式,有人利用外部服務器控制手機向外發送詐騙短信。三個多月時間裏,老人的手機已經向200多個手機號發送短信380餘條,還有大量2G上網流量記錄。但老人對此一無所知。

辦案民警介紹,犯罪團夥用於詐騙錢財的木馬程式,其實就是一個手機銷售統計軟件「變種」,是一款手機生產商為統計真實銷售數據開發的軟件,能夠在手機被插入啟用時向手機生產商發送反饋信息。犯罪團夥將該軟件進行改寫升級,增加了發短信、刪短信、訂閱App等功能之後用於詐騙活動。主要方式是同SP商(手機內

容服務商)暗中勾結,通過在境外的服務器控制功能機,群發短信、獲取驗證碼暗中扣費獲利。被控制手機如果不打印電話清單根本發現不了。

### App上架安卓華為市場需具安全資質

長期致力於網絡安全的專業人士曲子龍說,目前,常規工具類的App審查都是平台自己定的審核規則,但是一些特殊行業的App如金融、社交,一些平台在上架安卓市場時,平台要求提供相關的資質認證。比如社交類的軟件,如果上架華為應用市場,應該要提供App開發者所在地區網監的「網絡安全評估報告」,通過這種方式倒逼用戶走合規的流程。在反向監管方面,工信部也一直對App的隱私、權限合規問題,做周期性的審查,對不合規的應用市場下架,或限期整改。

中國最高人民法院副院長賀小榮近日也曾對媒體表示,App運營商在提供某App下載服務時,依法不得收集與該應用軟件無關的個人信息,否則便構成違法。 ●澎湃新聞