撰文 鄧詠筠、劉修迄
插圖 Aslan Hon

天羅

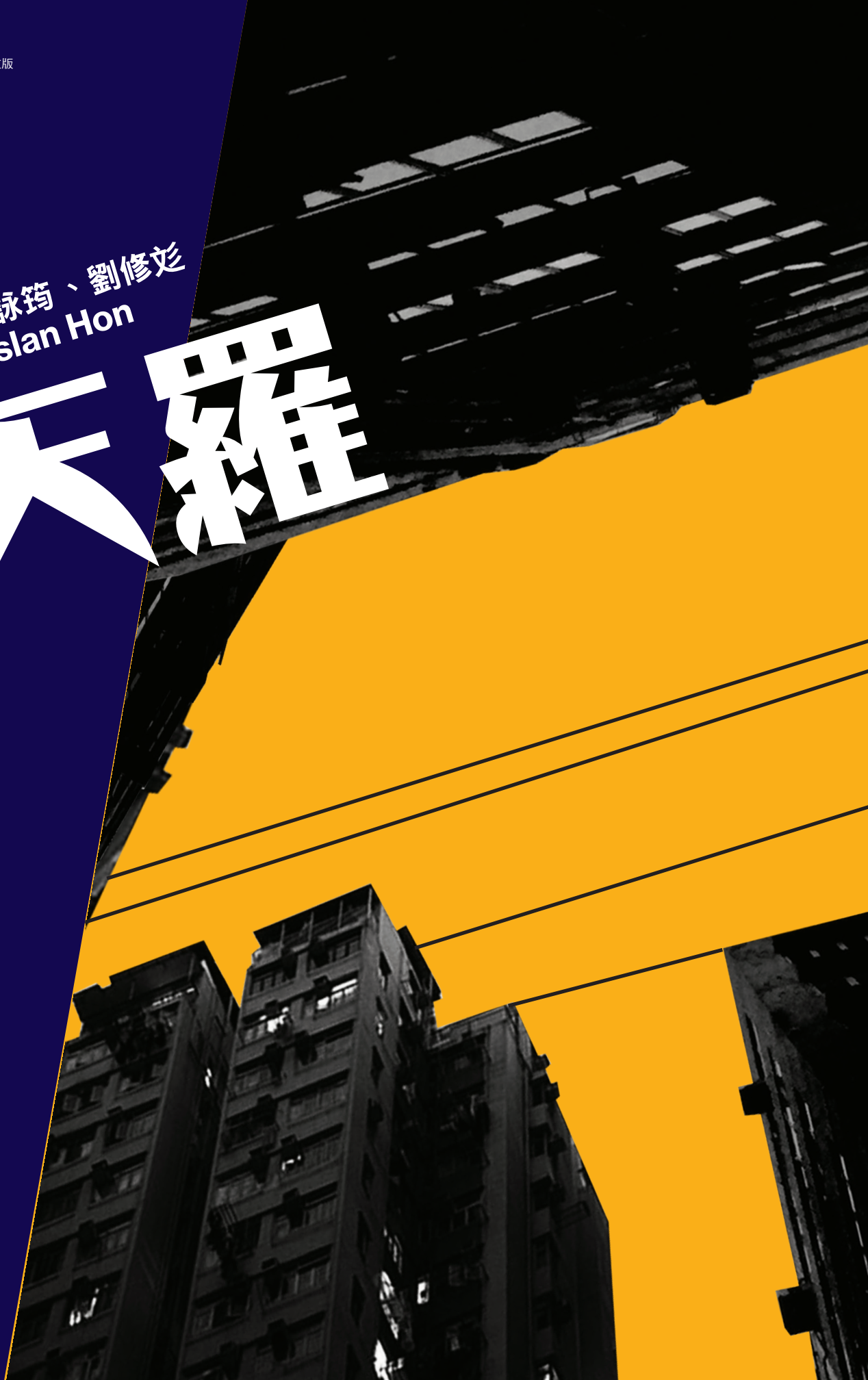
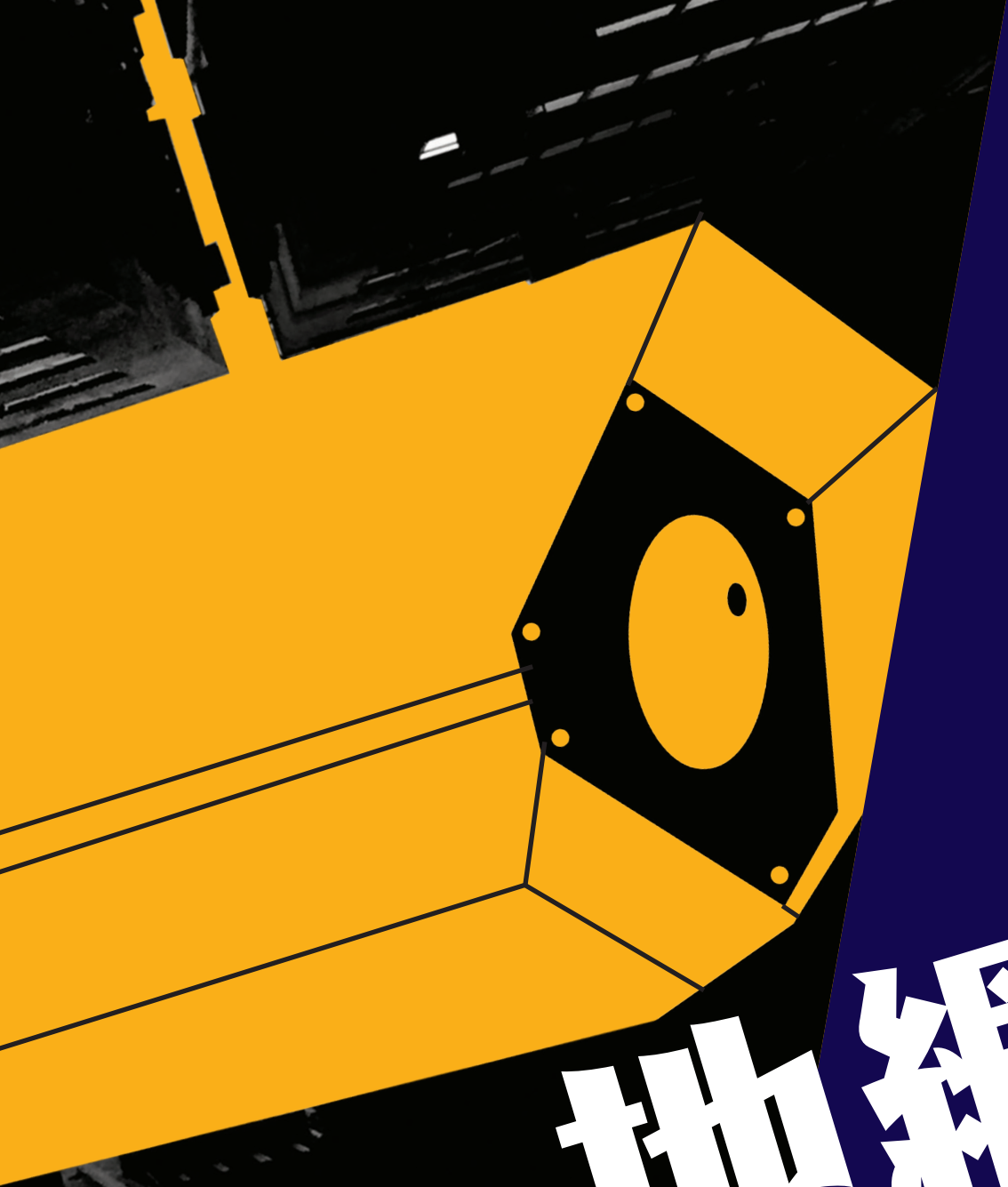


PHOTO ILLUSTRATION: GWEN CHAN



地網

世界各地都在探索智慧城市的可能運用。智慧燈柱、人臉辨識過關等項目，或能令市民的生活更加便利。然而，政府也正在掙扎著找出新興科技與數據監控之間的界線。在商業領域，我們的數碼足跡也正被以各種不同方式收集、販賣，變成私人企業的商品。新時代裡，誰擁有數據，誰便控制了人。你的個人資料存在哪裡？被用來做什麼？

前往觀塘參加遊行之前，V.S.（化名，受訪者不願透露姓名）再三確認自己在鏡頭底下是隱形的。他用墨綠色的頭套遮住整張臉，穿長袖長褲、戴護目鏡、防曬冰袖、工地手套，甚至連背包和鞋子都用銀色強力膠布纏了起來。

沒有臉孔，隱藏身上所有標記，他指指護目鏡上貼著的玻璃紙說：「你看不到我的眼睛對吧，但我看得到外面。這是我用來保護自己的方法。」V.S. 的聲音從頭套底下傳出來。

隨著香港的抗議活動越來越頻繁，不少市民開始擔心智慧燈柱上的監視鏡頭、藍牙探測器和無線射頻識別（RFID）等智能裝置會涉及侵犯個人私隱，甚至有人質疑智慧燈柱收集的資料會被政府用作監控用途，或連結人臉辨識系統，在香港建立社會信用體系。

因此那天，遊行隊伍抵達終點後，V.S. 與一群示威者將九龍灣常悅道上的智慧燈柱一一解剖研究。

與舊式燈柱不同，這些平均造價68萬港元的高科技設備裝有攝影機、藍牙探測器與無線射頻識別等裝置，可以用來收集實時交通和天氣數據、監控非法傾倒垃圾、提供定位服務和改善Wi-Fi與5G網絡功能。截至今年6月底，九龍灣常悅道、啟德承啟道和觀塘市中心已有50支智慧燈柱投入服務。

負責多功能智慧燈柱試驗計劃的香港創新及科技局政府資訊科技總監辦公室表示，智慧燈柱能「協助相關部門收集各類實時城市數據，加強城市和交通管理」，未來將會分階段在中環和金鐘、銅鑼灣和灣仔、尖沙咀安裝350支智慧燈柱。整體試驗計劃預計於2021至2022年度完成。

但一些示威者認為智慧燈柱是政府監控的象徵。

今年29歲的V.S. 說，智慧燈柱倒塌的背後，反映的是信任問題。「科技的本質可以是好的，可以讓生活更方便。但現在的問題是我們不相信這個政府。」

7月底上傳YouTube的一段關於智慧燈柱的短片，或許正說中了香港人內心的憂慮。該影片的拍攝者白兵是一個時事與科技評論YouTuber，3月設立的帳號，現在已經近8萬人訂閱。白兵在片中解釋智慧燈柱的功能。他表示，智慧燈柱最令人擔憂、且可能會對資訊安全及私隱造成威脅的，是燈柱配有的「監控三寶」——高清鏡頭、無線射頻識別裝置和未來可擴充的5G服務。該影片目前已錄得超過52萬次點擊率。

根據香港創新及科技局政府資訊科技總監辦公室公布的資料，每支智慧燈柱上最多可以安裝12個全景攝影機及1個交通監察攝影機，可用以監察實時交通情況，配合人工智能收集非法棄置廢物相關數據等。香港創新及科技局局長楊偉雄表示，燈柱上的鏡頭並不會儲存影像，亦無人臉辨識功能，某些智能裝置也因為爭議所以暫不啟用，但似乎仍無法平息擔憂。

白兵指出，早前無綫電視在拍攝燈柱示範畫面時，便意外拍攝到燈柱能偵測人臉，且「就算燈柱上的鏡頭真的沒有人臉辨識功能，只要後台有人臉辨識的系統，一樣可以達到人臉辨識的效果。」他解釋，人臉辨識之外，也有其他方法能透過影像識別並追蹤市民，例如衣著、髮型、步姿，或者如耳廓等能辨認的生物特徵。若影像回傳，或經由第三方存取，可能用來做更複雜的分析。

白兵也質疑，智慧燈柱中的無線射頻識別技術或可用來追蹤市民位置。當市民經過智慧燈柱時，燈柱設有的定位技術或能讀取新智能身份證上的位置資訊，讓智慧燈柱成為一個大型無線射頻採集器，只要你身處燈柱數十米內即可被偵測到。在適當的距離下，即使沒有物理接觸亦能讀取卡中的資料。

另外，根據香港政府新聞公報，為了配合香港未來發展5G服務，智慧燈柱中將會預留空間供流動網絡營辦商安裝5G

頭套、安全帽、口罩、貼有玻璃紙的護目鏡、防曬冰袖、工地手套等，已成為前線示威者保護個人身份的基本裝備（示意圖，照片非受訪者）

PHOTO: KYLE LAM/BLOOMBERG

部份智慧燈柱設有攝錄鏡頭

服務小型基站，亦可提供免費Wi-Fi服務。「未來如果完成5G最終極的網速，便可以完成很多更快速的運算，」白兵接受訪問時說，「且5G基站本應每幾百米才需要一個，但現時燈柱的安裝密度只相距數十米，反而符合了無線射頻識別技術定位所需距離。」

不信任的氛圍已經漸漸從街頭，蔓延到商業層面。燈柱倒塌的那天晚上，為智慧燈柱供應藍牙傳送器的訊科系統（TickTack Technology Limited）在公司網頁發出公告稱，由於公司員工及家人受到人身安全威脅及公眾對公司提供的服務有疑慮，決定完成現時已安裝的50支燈柱相關工作後，停止供應智慧燈柱項目的其他智能裝置。早前，有網民發現訊科系統的公司網站連結到中國內地「天網」工程承辦商之一的上海三思公司（Sansi）管理介面，質疑燈柱內的數據安全性。訊科系統回覆指他們與上海三思無任何股權及從屬關係，並就衍生之誤會向社會各界致歉。

位於香港九龍灣常悅道的智慧燈柱

PHOTO: ASLAN HON (2)

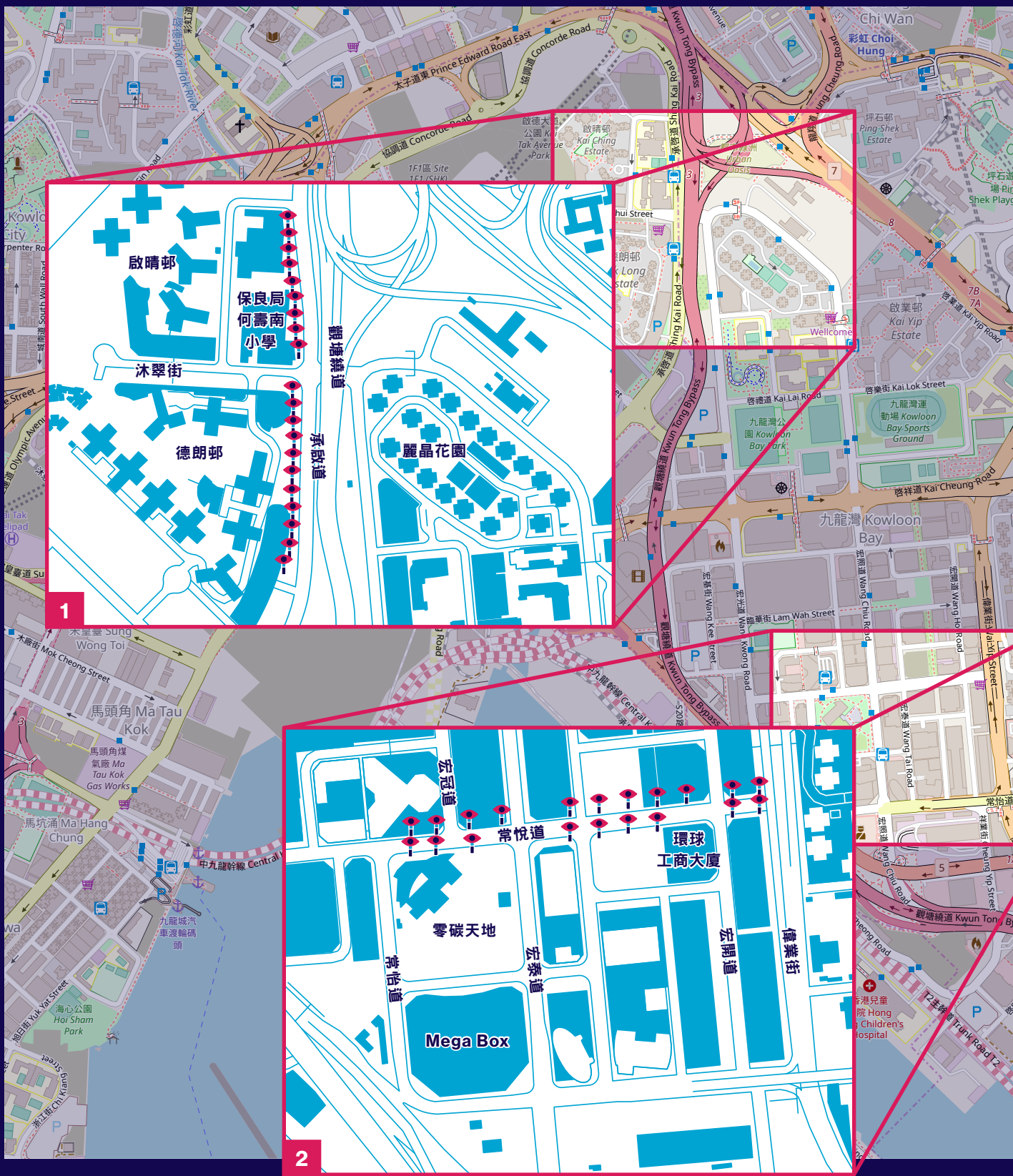
「8月24日是香港創科最黑暗的一天，」香港創新及科技局局長楊偉雄說。雖然他極力解釋，指智慧燈柱不是收集個人數據，收集到的數據如空氣質素、氣象、交通情況等，會在政府「資料一線通」網站公開，又指政府重視私隱，燈柱系統無人臉辨識功能，但市民似乎不買賬。

「市民出門只要路過監控燈柱，就可能會被收集數據，而數據亦不知道將保留多久，」由一群香港市民組成的監控燈柱關注組在一封公開信中表示。「除此之外，智慧城市規劃還有更多可以收集數據的途徑，例如醫療系統、稅務、銀行服務、機場，甚至上網、消費、聊天、用手機程式都會無聲無息地暴露你的個人資料。這些大數據全部都可被收集、分析、比對及監控。香港政府從無對市民交代、亦無進行諮詢，剝奪市民的知情權利。」

監控燈柱關注組認為，政府倘若希望挽回大眾信心，可以公開所有技術文件以及收集到的資料與數據；清楚表示各政府部門的數據閱覽權及使用權，釐清警方查閱數據的界限；採取立法及行政措施，確保市民個人私隱及資訊安全，保障人權等。 ▶

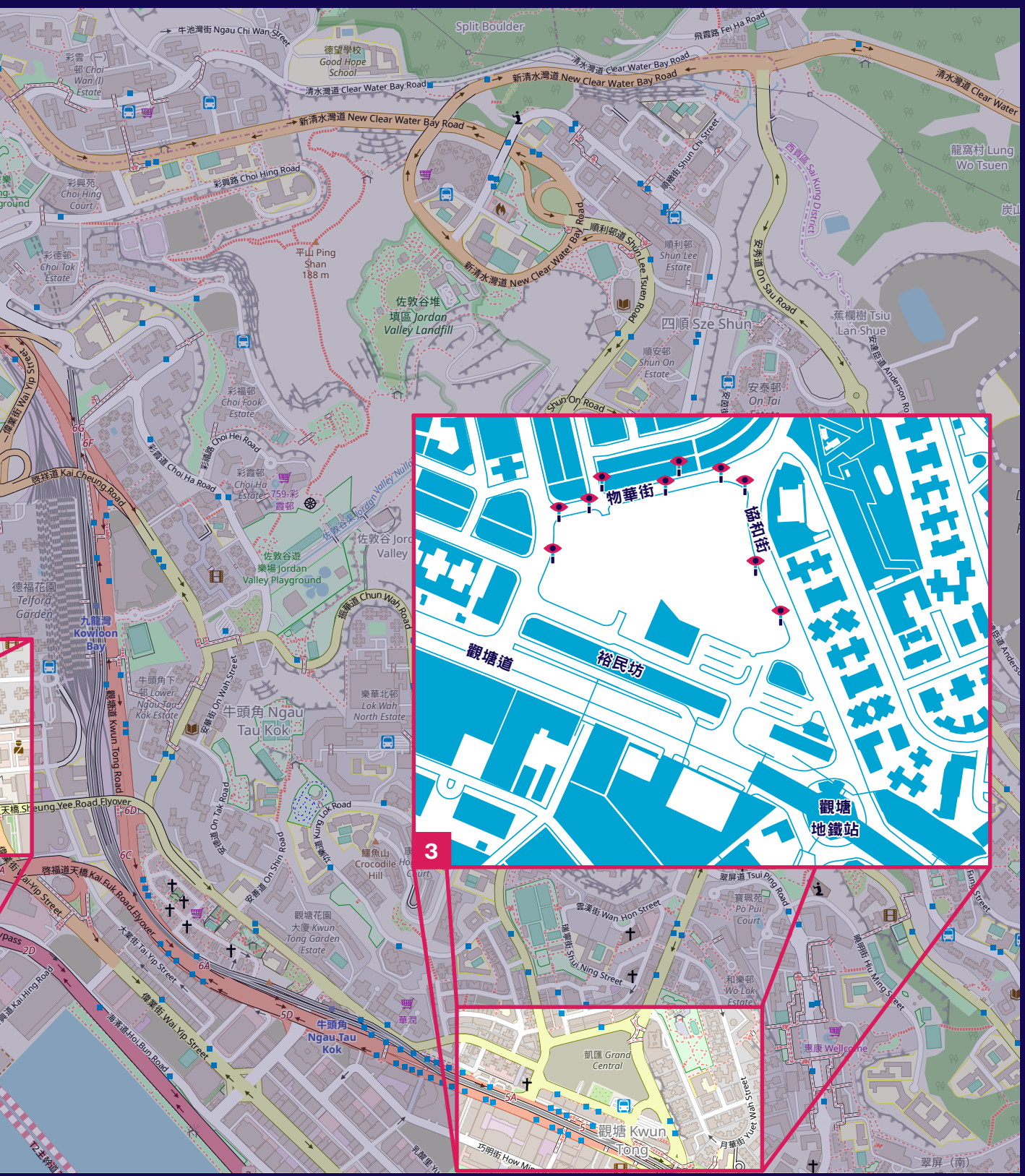
觀塘及啟德發展區智慧燈柱位置圖

智慧燈柱



觀塘及啟德發展區總共有50支智慧燈柱，分布位於：

地區1，啟德承啟道： 20支
地區2，九龍灣常悅道： 20支
地區3，觀塘物華街至協和街： 10支



資料來源：測繪處；地圖：OPEN STREET MAP

近年來，世界各地的都市都在探索智慧城市的可能運用——通過監測道路，確保公共交通工具準時運行及改善壅塞；依照感測器錄得的行人數量調節街燈光暗度，以減少能源消耗；在公共區域安裝攝影機，配合影像識別技術以管理城市治安。智慧城市透過資訊及通訊科技加強城市功能，但是，新興科技與數據監控之間常常只有一線之隔。有多少個人資料被政府收集，而收集來的資訊又如何被運用，市民大多並不知情。

這個擔憂並不只發生在香港。新加坡政府宣布將在超過10萬支智慧燈柱上安裝攝影機，結合人臉辨識以進行人群分析時，便引發了安全專家和人權組織的憂慮。與其他城市相比，新加坡並沒有高犯罪率或高恐怖威脅級別來證明安裝人臉辨識攝影機的必要性。

但香港與中國內地的關係讓它所處的情勢更加特別。中國內地在人臉辨識等監控技術上投入鉅資。天網工程，其最著名的項目之一，被稱為「保護中國的眼睛」，這些攝影機背後多擁有人臉辨識算法，能用來做大規模監視。

根據英國科技研究網站Comparitech的數據，按人均閉路電視鏡頭數量計算，全球10個最受監視城市便有8個在中國內地。排名首位的重慶有超過258萬個監視鏡頭，平均每1000個人，便有168.03個鏡頭望著自己。香港北邊的深圳排名第二，1000個人有159.09個鏡頭監控。

目前，香港有約5萬個由政府及公營機構安裝的保安鏡頭，人均鏡頭數量為全球排名第26位。香港政制及內地事務局局長聶德權在6月答覆立法會議員莫乃光的提問表示，所有政府部門目前都沒有採購或研發具錄影及自動化人臉辨識功能的閉路電視系統，或在閉路電視系統使用自動化人臉辨識技術，但是這仍然引起人們對私隱及個人資料使用的擔憂——特別是當數據集中在政府內部的時候。

為了解人臉辨識目前在香港的應用，我們根據《公開資料守則》，向政府物流服務署索取各部門招標文件。翻查2014年8月至今的招標資料後，記錄顯示香港政府目前至少在四個範疇使用了人臉辨識技術——入境事務處底下的新一代智能身份證、電子護照系統、出入境管制系統，與資訊科技總監辦公室負責的數碼個人身份系統（eID）。

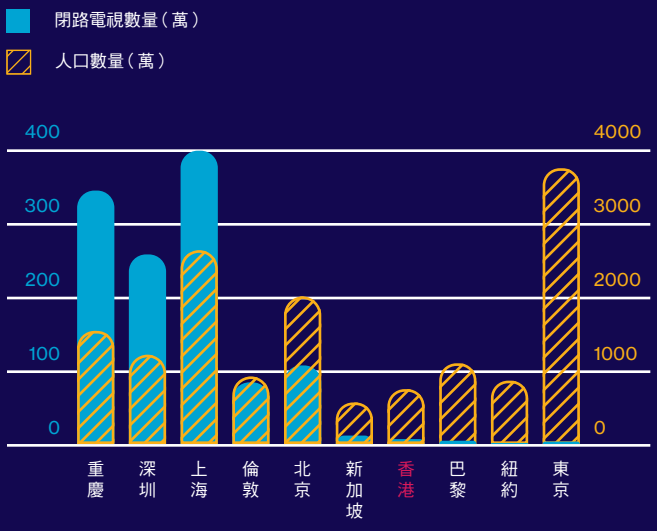
這些文件並不涵蓋所有政府採購案件。政府物流服務署負責批審超過1000萬港元的政府採購，金額較小的案子則由各個部門分別處理。

2016年9月，入境事務處開始為新一代智能身份證系統公開招標。根據招標文件，身份證上的照片應該具有足夠高的質素，以令不同的人臉識別軟件運作，其中細節必須能夠識別包括痣與疤痕等細小特徵，以便身份驗證。另外，供應商提供的人臉辨識軟件也需「支持一對一的人臉驗證，且能識別來自相機、實時影片等不同影像來源中的人臉。」除了臉部特徵之外，新一代智能身份證也存有持卡人指紋，以作身份辨認。

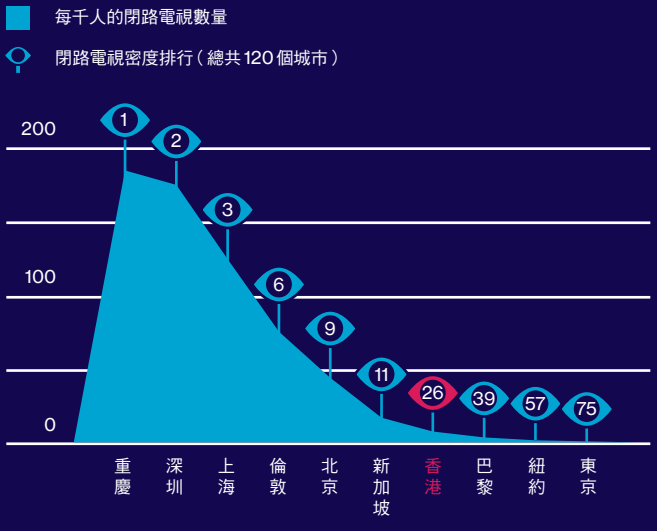
入境事務處於2017年12月招標的電子護照系統對照片與指紋的細節要求均與新一代智能身份證相似。入境事務處回覆指，透過所收集的個人資料儲存於入境處的伺服器內，在傳輸和儲存個人資料時，會以國際認可和通行的高級別加密標準進行加密，並進行定期保安風險評估，以確保系統持續符合所需的保安要求。

各地閉路電視密度

閉路電視數量

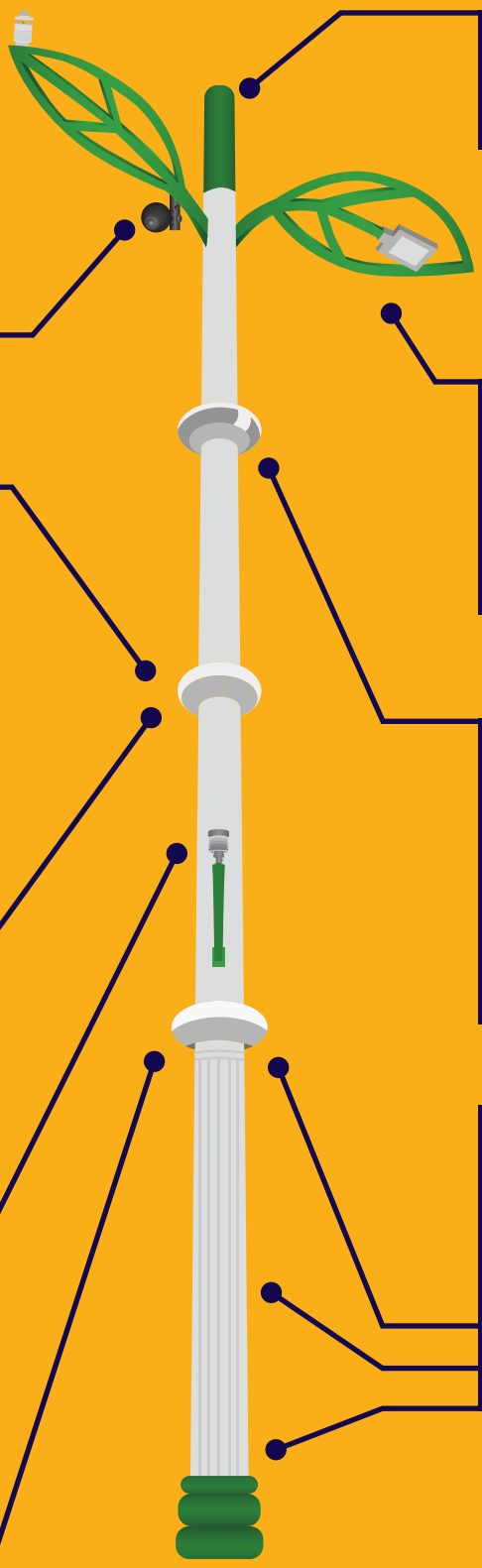


世界排名



資料來源：COMPARITECH

拆解智慧燈柱



熱能交通採測器及監察攝影機

功能及應用：
▶ 收集實時交通數據，包括車速、車輛類型、交通流量、交通狀況等

相關部門：
運輸署

4G / 5G 小型基站

功能及應用：
▶ 提供流動網絡營辦商安裝小型基站

LED 燈

功能及應用：
▶ 採用省電燈具以及智能化管理，以節省能源

相關部門：
路政署

Wi-Fi 熱點

功能及應用：
▶ 免費 Wi-Fi 服務

相關部門：
資訊科技總監辦公室

AI 全景攝影機

功能及應用：
▶ 降低解像度，拍攝交通快照
▶ 拍攝車牌號碼以計算不同類別的車流量*
▶ 以錄像收集數據，打擊非法傾倒建築廢料*

相關部門：
路政署、環保署

藍牙交通探測器

功能及應用：
▶ 檢測車輛駕駛狀況及平均車速*

相關部門：
運輸署

氣象感應器

功能及應用：
▶ 收集地區氣象數據，包括氣溫、濕度、風速及風向、降雨量、紫外線指數等

相關部門：
天文台

藍牙傳送器、無線射頻識別標籤（RFID）、地理位置二維碼

功能及應用：
▶ 提供準確定位服務，支援政府服務及業界開發相關應用，例如提供附近公共設施資訊

相關部門：
地政署

空氣質素感應器

功能及應用：
▶ 收集地區性空氣質素

相關部門：
環保署

資料來源：資訊科技總監辦公室；插圖：GWEN CHAN

* 暫緩啟用

人臉辨識流程

具有15年經營保安及智能系統經驗的傑成系統有限公司營運總監孫加成分享，人面辨識科技於過去兩年急速發展，目前的準確度已可高達97%。

人臉辨識軟件主要計算眼距、眼的大小、鼻的位置、嘴，以及臉部輪廓，並運算成數字符號，成為人面「數碼地圖」。電腦會透過演算法將這組資料及數字與數據庫內的資料比較，然後找出配對度最高的組合。而擁有人工智能的電腦會透過在過程中不斷學習，提高配對的準確度。「建立系統的過程中，會有很多人『教導』人工智能學習，在不同的動作或臉部輪廓上透過『畫點』的方式，讓系統更準確地辨識人的動作及臉部表情。」

❶ 人臉偵測

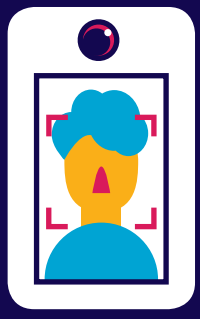
系統從圖像中抓取圖案，並將它們與臉部模型進行比較，若圖案與模型相似，系統會標記出臉部位置，並發出信號

閉路電視

系統可以通過臉部、步姿、衣服顏色等細節區隔與追蹤個體

安檢系統

海關、邊境、安全檢查站與保安系統紀錄並儲存人臉，目前港珠澳大橋高鐵西九龍總站及香港機場的邊境檢查站有使用相關技術



個人裝置

智能手機的應用程式和安全性功能會使用人臉偵測，如解鎖手機等。數碼個人身份系統便是使用個人流動裝置提供的生物辨識功能進行綁定及認證

其他來源

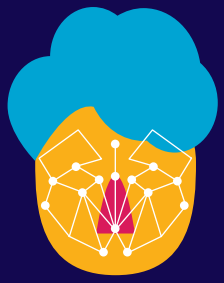
圖片、影片、電腦、熱像儀等其他可以捕捉圖像的來源

❷ 特徵擷取

將照片角度等調整至較為一致的基準，運用五官關鍵點、幾何特徵、熱度、樣板等數據，透過演算法將臉部圖像轉換為含有精確信息的數值，並建立臉部樣板

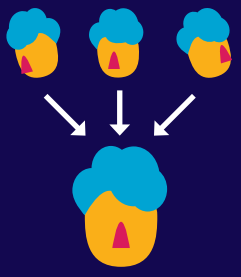
幾何

計算臉部特徵，如眼睛、鼻尖、耳朵之間的空間關係



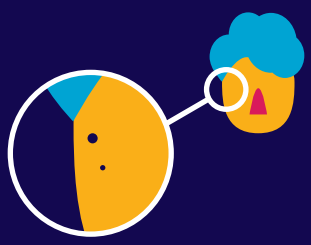
光度

有些演算法在燈光條件或角度扭曲的情況下也能重建臉部



膚質

定位並分析毛孔、疤痕、皺紋與色斑等，香港新一代身份證儲存的臉部圖像便要求須精細至能顯示痣與疤痕等小特徵



熱度

使用熱度建立臉部樣板能為以化妝、偽裝或是帽子、口罩等衣物遮擋的臉孔提供更多信息

現時，全球多個國家及不同企業都廣泛使用人臉辨識系統。英國南威爾斯警察正在使用由日本企業NEC生產的「NeoFace Watch」，NEC指出，與其他生物辨別技術如指紋、瞳孔等相比，人臉辨識無須觸碰的特點擁有很突出的優勢，因為可以在不觸碰當事人、毋須互動的情況下遠距離獲得個人資料。

❸ 人臉辨識

臉部樣板建設完成後，它可以與數據庫進行特徵比對，識別一個人的身份、年齡或性別等

至於目前市民普遍的擔憂——是否會與警務處分享儲存在身份證與護照中的個人資料，用於與警方拍攝的照片或影像比對，入境事務處指，他們「十分重視個人資料私隱及紀錄管理，只有按實際的工作需要和獲授權的職員才可登入個別的電腦系統」，政府部門之間並不會共享數據庫；警務處則以「披露訊息會妨礙犯罪、違法行為、逮捕或起訴罪犯的預防與調查，及會危害拘留設施與監獄安全」為由，拒絕提供任何有關使用影像或生物特徵辨識目標的細節。

熟悉資訊科技、知識產權與私隱相關法律的法政匯思前召集人蔡騏解釋，在香港，個人資料受到《個人資料（私隱）條例》的保護，這當中也包括政府部門，如入境處所收集的資料。「私隱條例的第一原則是不收集過多的資料。收集資料的目的是什麼，收集了什麼樣的資料需要寫清楚，同時也要通知事主。事主是有知情權的。」法政匯思是一個由香港大律師、事務律師、法律系學生及擁有法律學位的人士所組成的專業團體，成立宗旨為捍衛法治、司法獨立，並為民主、人權、自由、公義等核心價值發聲。

但是，如果要將資料用於打擊、偵辦或起訴案件，則可以免除條例中的一些原則——執法機構能取得豁免權，令他們能在事主的同意之下取得個人資料；若第三方擁有關於個人的數據，他們也可以分享給警察，而不必擔心違反法律。

「然而擁有豁免權並不代表他們『必須』分享數據給警察，」蔡騏說，「擁有數據的第三方如入境處或是電訊公司，有責任不提供過多的資料。如果他們認為警察要求的資料與案件無直接關係，可以拒絕要求，這時警察便須獲得法庭手令，才能令他們移交訊息。」

除了個人訊息會不會被用來作執法用途外，社會信用體系會不會經由智慧城市包裝，橫跨邊界、擴展至香港，或是個人數據是否會回傳至中國內地，也成為香港人的擔憂。

翻查得標通知及公司登記資料，我們發現近年多次投得香港政府部門智慧城市相關專案的公司——包括含有人臉識別技術的新一代智能身份證、電子護照系統，與出入境管制系統——其實具有中國央企背景。

根據2018年3月23日的得標通知，一間名為香港愛信諾（國際）有限公司的企業投得一份近2350萬港元的合同，成為入境處新一代智能身份證系統硬件和軟件供應商之一。同年2月，愛信諾亦投得入境事務處的廣深港高速鐵路香港段西九龍總站出入境管制系統合約，價格約39萬港元。

根據「公司註冊處」資料，愛信諾為總部位於北京的航天信息公司在港成立的全資子公司。航天信息於2000年成立，2003年在上海證券交易所掛牌，由中國航太科工集團直接控股。航太科工是由中國中央直接管理的航太軍事央企，前身為國防部第五研究院。

航天信息過去五年曾多次標得香港政府項目，如建立蓮塘/香園圍口岸、廣深港高鐵香港段西九龍站口岸、港珠澳大橋香港段口岸的出入境管制系統，以及為入境事務處提供新的出入境管制系統等，得標總額近16.3億港元。其中，航天信息得標的入境事務處出入境管制系統標書中便寫道，得標公司的系統須負責「創建、更新、刪除和儲存包括但不限於臉部圖像與模板的數據。」

研究私隱的香港中文大學法律學院助理教授Stuart Hargreaves表示，目前沒有證據顯示中國能存取這些資料，香港人對於智慧燈柱與人臉辨識系統的擔憂，都可以歸結為信任問題。

「智慧城市可以滿足安全性、便利性和環境改善的需求，但是，同樣的▶

資料來源：U.S. GOVERNMENT ACCOUNTABILITY OFFICE、蔡騏系統有限公司及其他綜合資訊

◀ 技術如果運用在不正確地方，便會令人頭痛——例如不僅僅是用來偵辦案件，而是打壓合法的抗議，甚至壓制日常的創意，」Stuart Hargreaves說。

「如果人們不信任他們的政府，那麼他們也不會相信有關智慧城市和數據使用的法律可以保證他們的安全，無論其設計得多好——我們已經在香港看到了這一點。人們根本不相信政府告訴他們有關智慧燈柱或閉路電視的使用訊息，這不是因為他們有證據，而是因為普遍缺乏信任。」

「這不是法律設計不佳的問題，而是政府與公民之間的關係問題。也是在這裡，我們看到了一國兩制中的基本矛盾——當兩個系統以完全不同的方式回答問題時，『一個國家』會做什麼？『一個國家』可以接受差異嗎？還是試圖使一個系統與另一個系統保持一致？在示威活動中，人們對技術和私隱的恐懼，其實是對這兩種系統的差異逐漸消失的憂慮。」

正當大家擔心人臉識別對於個人私隱的影響時，其實每一日人們大大小小的個人資料正以不同方式被收集，然後變成生財工具。

擁有電腦科學學位，曾修習人工智能，被稱為「科技律師」的翰宇國際律師事務所（Squire Patton Boggs）合夥人陳曉峰指出：「其實智慧燈柱為我們帶來的私穩風險，並不會高於我們日常自願交出個人資料所帶來的風險。」他解釋：「當人工智能、大數據，應用在流動物聯網裝置，我們身處的世界便讓企業如劍橋分析（Cambridge Analytica）可以坐擁多達5000個有關個人行為傾向的數據點（data point，泛指一則資訊或一項事實）。」

劍橋分析是一家進行資料探勘及數據分析的私人控股公司。美國總統特朗普於2016年競選總統期間曾聘用劍橋分析，利用演算法，分析Facebook用戶的人格，令團隊可針對性的投放競選廣告；該公司前總裁說，正是這樣的技術幫助特朗普打敗了希拉莉（Hillary Clinton）。

「同時，我們每日都透過手機留下很多數碼足跡，甚至樂於在社交媒體及通訊軟件留下生活點滴，又『盲目』地接受應用程式的各種條款，容許我們的訊息、簡訊服務（SMS）、地理位置數據、上網瀏覽紀錄、鍵盤資料、聲音、臉部影像等資訊被收集，」陳曉峰說。

幾乎所有有關日常的資料都可能被收集。在美國科技企業Pegasystems擔任高級企業架構建設師的Praveen Kumar，專為企業提供電子轉型方案，並利用大數據撰寫預測消費者行為程式，他分享：「數據分為兩大種類，分別是歷史數據以及不斷變動的數據。」歷史數據是一些不會經常變動的基本資料，而變動的數據是指我們平日在使用電腦或手機時，進行瀏覽或購物的數據。「例如，我在亞馬遜網頁上的每一個點擊，都會留下一個數據點，如果我將一些貨物放入購物籃，就會得到約9個數據點。然後，有關你的編程模組便會因應由你身上獲得的數據點，發生著變化，然後根據你的喜好，向你推薦不同廣告及產品。」

這是科技界經常說的適應性預測編碼（adaptive and predictive coding）。模組（modeling）會因應你的瀏覽數據進行調整及行為預測，而你瀏覽得越多，有關網站所獲得的數據量就會越大，對瀏覽者的行為預測亦會越準確。另外，編碼亦會結合你的個人資料，如性別、地區、年齡，進行資料歸納及分類（profiling），並根據不同的分類「族群」，發放針對性的宣傳。

在天羅地網之下，我們在網上留下的個人資料正經過不同渠道被大幅收集，除了由網站用作了解客戶的個人偏好，更會被出售，用作市場推廣。根據網上市場推廣公司WebFX統計，現時全球約有4000家專門買賣個人資料的數據仲介公司（data broker），而其中一家規模最大的數據仲介公司Acxiom，擁有2.3萬個伺服器，用作收集及分析全球多達5億名消費者數據，而其擁有每名消費者的數據點多達1500個。而這只是一家公司擁有的數據量。

事實上，我們的個人資料亦可算價值不菲，根據行業研究機構Arance 副總裁Kannan Sivasubramanian估算，全球數據中介商行業全年收入多達2000億美元，當中市場推廣工具帶來達50%收入。學術論文《The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement》指出，美國超市沃爾碼（Walmart）每個小時內從客戶中便收集到超過2.5PB（petabytes，1PB等於100萬GB數據量），其規模相等

香港智慧城市藍圖重點計劃

2017年12月，香港政府公布《香港智慧城市藍圖》，提出六個智慧範疇與超過70項措施，以下是《彭博商業周刊／中文版》擷取的幾項重點：

- 由2021年開始試行在路口設置感應行人及車輛的智能交通燈系統
- 探索使用臉部生物辨識技術在包括於登記櫃檯、登機證檢查站和登機，提供無縫的機場行程體驗
- 在2020年為所有居民提供免費數碼個人身份，可使用單一的數碼身份認證進行政府和商業的網上交易
- 在2019年開始推行「多功能智慧燈柱」試點計劃，收集實時城市數據，加強城市管理及其他公共服務
- 於2018年在香港國際機場、廣深港高速鐵路西九龍站及港珠澳大橋香港口岸使用智能科技，提供便利旅客的服務
- 通過智能機場、Wi-Fi連通城市計劃及智慧燈柱提升旅客體驗

近期獲批中資科企的智慧城市相關項目

得標日期	項目	得標公司	合約費用（港元）
2019年7月	新一代政府雲端基礎設施	中國電信國際	2.13億
2019年2月	構建、支援及維護「數碼個人身份」系統	平安科技（深圳）有限公司	4403萬
		深圳市雄帝科技股份有限公司	350萬
2018年7月	蓮塘／香園圍口岸出入境管制系統	航天信息股份有限公司	1421萬
2018年3月	新一代智能身份證系統所需的硬件和軟件	香港愛信諾（國際）有限公司	235萬
2018年2月	西九龍總站出入境管制系統	香港愛信諾（國際）有限公司	39萬
2018年1月	西九龍總站出入境管制系統	航天信息股份有限公司	1327萬
2017年8月	港珠澳大橋香港口岸出入境管制系統	航天信息股份有限公司	3336萬
2014年11月	入境事務處的新出入境管制系統	航天信息股份有限公司	10.88億

資料來源：物流及服務署招標公告

於裝滿5000萬個4層資料櫃的資料。另外，根據國際廣告公司AdAge指出，在2015年，全球的手機用戶數據市場規模達240億美元，估計將於2020年上升至790億美元。

現時，全球各地對於企業正大量收集數據，已有不少爭議。最經典的例子要算是Facebook與劍橋分析透過心理分析應用程式，取得用戶資料，在選戰期間針對性發送廣告，左右選情，最終Facebook被罰款50億美元。

撰寫有關科技如何監控整個經濟的書籍《Dragon Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance》的作者Julia Angwin指出：「我們正生活在一個無差別地進行追蹤的世界，在那裡，企業以前所未見的速度不斷累積個人數據。」就個人私隱進行監察的全球私隱論壇估計，每個人被收集的資料多達4000個數據點。每一次人們使用電腦、感測器、智能電話、信用卡、電子儀器及不同工具時，就會留下與自己有關的線索，陌生人只要沿著這些線索，慢慢地沿藤摸瓜，便可找到當事人。

當可以收集數據的移動互聯網裝置越來越多，人們日常生活的更多細節，便更容易轉化成數據。根據Persistence Market Research於今年初發展的市場報告「Cellular IoT Market–Global Industry Analysis」，2017年移動物聯網市場價值為11億4520萬美元，預計從2018年到2026年的複合年增長率為26.7%。而這些移動物聯網的感測器及家居智能，結合人功智能的應用，亦變得越來越「貼心」。人們較熟悉的包括由Apple開發的HomePod、亞馬遜的Alexa等智能家居裝置外，來自美國的Emoshape甚至研發出可以感測人類情緒的晶片，能夠探測情緒，並作出不同反應。當科技一直發展，未來將可以對你體貼入微，最後，我們或許真的會如電影《觸不到的她》（Her）內的主角一樣，願意向一個移動裝置傾心吐意、推心置腹，甚至墮入愛河，直到不能自拔之時，才突然驚醒只是夢一場。

我們願意奉上數據後，持有龐大數據的企業一旦出現保安漏動、受到攻擊，個人數據便曝露於世，令我們平白承受不同程度的風險。不法之徒對於幾乎唾手可得的數據金礦虎視眈眈，用盡不同方式獲取個人資訊，並變現成金錢。

律師行Norton Rose Fulbright全球數據保護、私隱及網絡保安聯席主席Chris Cwalina觀察到，網絡攻擊的方式不斷演化，而且越來越成熟。「我們看到很多網絡上的攻擊，最常見的是電郵帳戶被盜。10年前的攻擊主要是『smash and grab』（大規模擊毀然後迅速搶奪資料），先進行攻擊，然後快速拿取大量數據。現在，攻擊者的手法更加成熟，他們很有系統、財力豐厚，而且非常快速。他們會鎖定目標，而且更願意花時間在下手攻擊前，在網絡上潛伏，潛伏時間平均長達200日。」

犯罪方式正不斷演化。「傳統的重要資料如信用卡等，仍然受到歡迎。但現在，他們積極於收集個人資料，並且找到方法將這些資料變成金錢。他們得到數據後，會進行歸納及▶

數據仲介公司如何收集消費者數據

❶ 數據收集

大型數據仲介公司從各種來源收集個人數據

公開數據如法庭記錄、選民記錄、車輛購買紀錄

姓名和地址變更歷史、婚姻註冊、離婚紀錄、出生與死亡登記

問卷、商品保顧卡、抽獎券上填寫的個人資料

報刊雜誌訂閱紀錄、預訂旅行的資料

零售商、藥房、俱樂部等會員計劃

個人信用歷史與來自銀行、保險公司、醫院及僱主的數據

網絡上的公開數據

網站訪問歷史、搜索歷史

社交媒體、平台帳戶

智能手機和應用程式的使用

網購紀錄

智能電視、遊戲機、電子閱讀器、汽車等設備

❷ 數據收集

數據仲介公司從各種來源收集個人數據後，會找出能用來識別個人的重要標記（Unique ID），讓收集到的數據能與個人做連結。電子郵件地址和電話號碼是非常重要的標記，郵遞區號也是用來辨識個人的關鍵點。大型平台上的用戶名稱在連結跨平台的帳號時也有關鍵的作用。數據仲介公司還可以通過數碼足跡計來識別人員。

*註：Cookie 即網站為了辨別用戶身份而儲存在用戶端上的資料（通常經過加密）

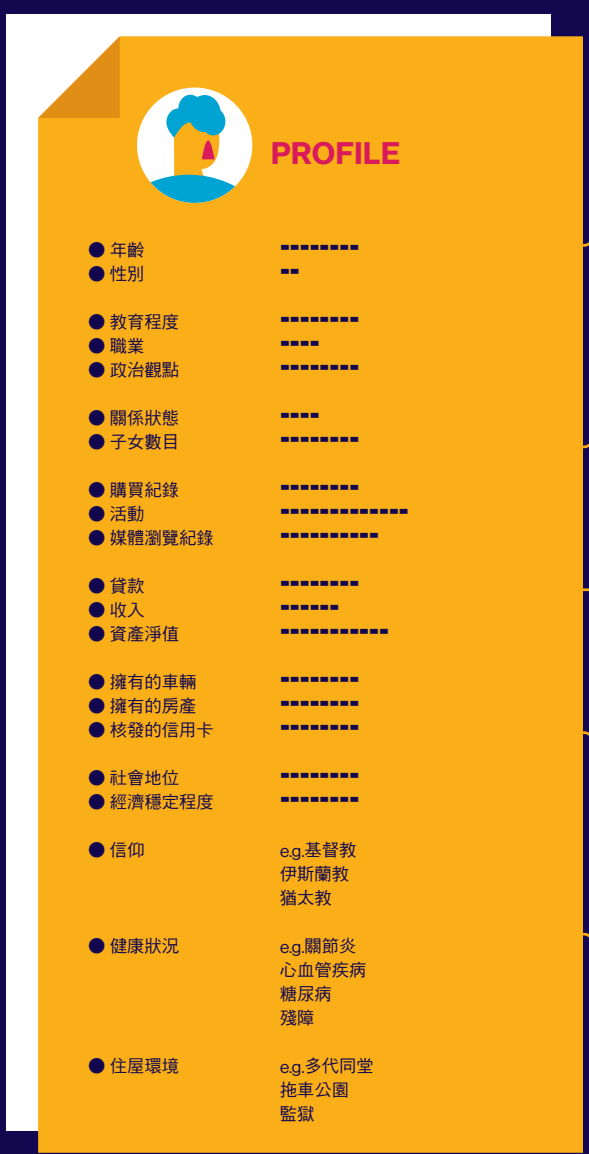
通過收集數千個數據點，數據仲介公司可以建立涵蓋廣泛的個人檔案，將人分類為多種類別，並商品化這個服務

❸ 建立個人檔案

大型數據仲介公司如Acxiom擁有7億用戶的多達3000個屬性和分數

❹ 商品化

客戶可以將其收集的用戶數據與數據仲介公司提供的個人資料數據相結合，然後在其平台上改善數據的使用



將用戶分類

尋找並確定目標

提供個人化內容

觀察人們的行為特徵

販賣數據

資料來源：CRACKED LABS

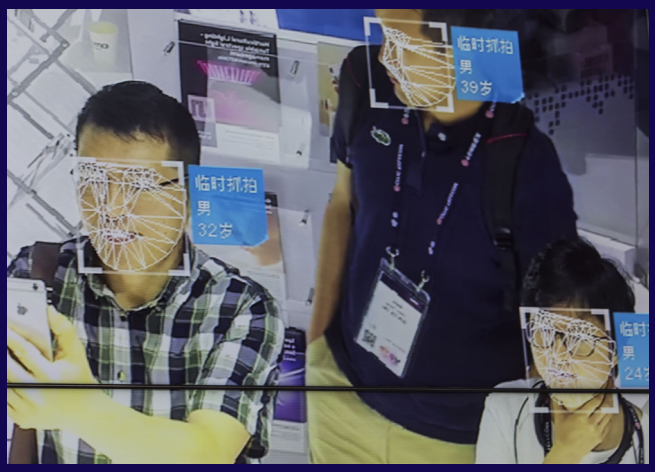
◀ 分類，然後出售，這是我們看到的趨勢。」Chris Cwalina解釋：「當然，由於金融機構更著重於保護資料，故此，不法之徒會將目標鎖定於數碼保安功夫做得較差的行業及公司。以醫療行業為例，他們可以將由醫療企業得來的資料，建立有關醫療健康的分類，並將資料出售，或偽造保險索償申請，從保險公司手中獲得賠償金。」Chris Cwalina又指：「透過要脅獲得金錢仍然非常普遍，他們會拿取任何可以獲得的內部資料，並進行勒索，要求資料持有人繳付贖金。」

即使沒有惡意攻擊的不法之徒，散落在各地的細碎個人資料，一旦被拼湊起來，就會如拼圖般將你整個生活呈現出來，找到你的真實身份。「這就是大數據經常引起憂慮的『data reidentification』（數據重新識別），在十多年前有一個很經典的例子，就是美國網絡供應商AOL在2006年以數字代替用戶姓名，公開所有網上搜尋紀錄後，有人從搜尋紀錄中，認出某一個特定的人，當時引起廣泛的關注，」香港中文大學數據科學與政策研究課程主任黃偉豪說，個案中被別人認出的62歲太太，在網上搜尋了「手指麻痺」、「60歲單身男士」、「到處小便的狗」、「佐治亞州Lilburn的地形」，以及「佐治亞州格威內特縣湖邊出售的住屋」，而住在當區又有飼養狗隻的單身女性，就只有Thelma Arnold，令認識她的人輕易地將線索串連起來，將她認出來。事件爆出後，AOL立即移除了有關資料。

到了十多年後的今日，有關我們的零碎資料更多、更廣泛，而且更易於被串連起來，一直關注網絡安全的互聯網協會（Internet Society）指出：「如果網絡供應商擁有你的帳戶資料，例如你的電郵地址、付款資料、購買紀錄或其他個人資料，網站內的cookie會將你在網上做的所有舉動與這些資料連結起來。這個『連結性』的概念在了解及分析網絡私隱時非常重要，因為比起任何在單一場合下收集的個人資料，『連結性』對於侵犯個人私隱的威脅更大。」而在香港是全世界擁有最高智能電話滲透率的地方，根據通訊事務管理局辦公室的數據，到2017年6月為止，香港的智能手機滲透率已高達237%，對於電訊供應商來說，是一個非常吸引的個人數據收集市場。

電訊商手上擁有龐大的資料，無論是基本的個人資料，抑或是我們每一日的定位數據、通話紀錄，電訊商都瞭如指掌。研究個人數據私隱的香港中文大學新聞與傳播學院助理教授徐洛文，就電訊商擁有的個人資料進行研究及統計，並於2016年建立「誰手可得」網站，讓市民可以透過網站向電訊商索取有關自己的資料。「電訊商擁有我們非常之多的個人資料及數據，但我們一直不知道他們擁有我們的什麼數據，所以我利用條例賦予給我們的權利，要求查詢，」徐洛文

上海流動通訊大會中展示的人臉辨識裝置



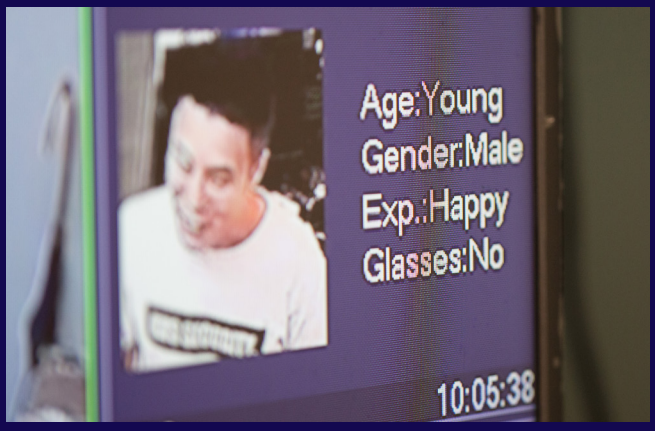
分享。根據在1996年成立的香港《個人資料（私隱）條例》，個人資料「是關乎一名在世人士，並可識別該人士身份的資料，存在的形式令資料可讓人切實可行地查閱或處理」，包括個人姓名、電話號碼、地址、身份證號碼、相片、病歷和受僱紀錄等。而我們可以要求查閱有關自己的「個人資料」，根據私隱條例的六項保障資料原則內第六項：「資料當事人有權要求查閱其個人資料」，換言之，每個人都「可以查問機構擁有什麼資料」。

然而，對於「個人資料」的定義，似乎仍然存在極大的爭議性，我們甚至無法擁有定義個人資料的權利。徐洛文向香港7大電訊商發出要求，但最後全部皆只願提供有關姓名、住址、電話、地址、身份證號碼等傳統的個人資料，然而，手機的網絡位址（IP Address）、地理位置（GPS location）及瀏覽紀錄，則被電訊商界定為「非個人資料」，故此不用向外披露。徐洛文解釋：「在法律上，資料分為『個人資料』及『非個人資料』，一旦電訊商界定為『非個人資料』，便毋須向當事人交代，甚至可將有關資料出售予數據仲介公司牟利。」他認為，這些資料應該被列為個人資料，要重新定義的話，則需要與電訊商對簿公堂，就如何定義個人資料提出訴訟。換言之，現時法律上，對於個人資料的定義，仍然存在非常大的爭議及漏洞，屬於一個可讓收集資料的企業任意「搬龍門」的領域，令持有龐大用戶資料的大型企業幾乎擁有絕對的優勢。

但現時科技鋪天蓋地，「是否交出個人資料」已成為一個兩難的處境，當中最主要涉及的問題，在於對數據使用者以及對網絡安全的信任。立法會資訊科技界議員莫乃光說：「以現在社會對政府的信任程度來說，恐怕並不足夠。另一個平衡及補救的方式是，市民可以保障自己的權利有多大？」他認為，現時保障私隱的法例很落後，以懲罰的標準為例，國泰於2018年洩漏940萬名乘客資料，並沒有強制通知（mandatory notification），於7個月後才公報有關事件。「我們仍停留在20

PHOTO: QILAI SHEN/BLOOMBERG

傑成系統有限公司展示的保安系統中，目標人物的年齡、表情均能清楚辨識



年前的做法與現時歐盟《通用數據保障條例》（GDPR）的做法相差很遠，」莫乃光說。歐盟於2016年推出的GDPR，被稱為最嚴厲的私隱條例，「企業如何處理整體數據，甚至演算法的控制及利用、透明度，你如何運算以及整個運算過程是否適合原則？市民有沒有權反對？用戶需要「主動要求加入」（Opt in），還是「主動要求退出」（Opt out）？

陳曉峰指出：「不遵守GDPR的成本可以很高，違反者可被罰款2000萬歐元，甚至是高達4%的全球收入，罰款令企業的生意增長及發展實驗性科技受阻。」因此，具有一定的阻嚇性。另外，他又指：「一些地區會將某一些數據歸類於較嚴格的管治及保護，例如生物辨別數據、病人的健康資料以及財務資料。現時，個人資料條例在香港保護一些可以辨別到在世人士的資料。我們應否擴闊這個定義？私隱專員一直提倡『提升』個人資料（私隱）條例，由於這個倡議會帶來健康的平衡，受到業界的歡迎及支持。」

另一方面，網絡裝置上的保安亦引起不少疑慮。網絡保安專家UDomain行政總裁范健文指出，「隨著物聯網裝置越來越多，社交媒體更盛行，外洩的風險便更高。在很多國家，很多物聯網裝置出現被入侵的情況。最近五年，才開始更多人真正著重資訊保安，因為多了大型的私隱數據洩漏，所有事都越來約貼身，訂機票、電訊公司、旅行社等。」

他又指出，現時市場上欠缺為移動物聯網裝置設定保安系統的意識及人才，「本身為物聯網裝置編寫程式的人，未必是編程人員，而是電子工程師，負責焊接底板，安裝攝影機，令攝影像素更高，但如果你問他在影片由這個攝影機傳送到雲端時如何進行加密時，這並非他們的專業。但是，不論是黑客抑或保安調查員，他們很多時候已在短時間內看到漏洞。」根據他的觀察，很多保安資訊洩漏的事件，就發生在這個位置，「通常他們以功能性為本，不知道甚麼是保安。而且很多人都認為保安、加密等都是在很後期才考慮的事，所有功能齊全後才會考慮。」范健文說，他曾幫助10間學校做保安核實（security audit），「學校是被遺忘的一塊，卻擁有非常龐大的個人資料，我們用了少於100個小時，已經接觸到兩萬多筆私人資料，這是很震撼的。」

為了對抗鋪天蓋地的監視，市場上已出現了不少對抗方式。例如由德國公司HyperFace設計的人臉迷彩圍巾，驟眼看上去只是一塊紫色的迷彩毛巾，但對於人臉辨識系統來說，卻會出現1200張人臉，直接令系統當機。另外，又有由日本國立情報學院研究所開發、名為蒼蠅眼鏡（Privacy Visor）。Privacy Visor鏡片上有網狀花紋薄膜，透過薄膜反射光線到監視鏡頭，令被拍攝者的眼睛變暗，而鼻樑到顴骨的位置會過於光亮，影響系統的辨識能力。

「面對科技的急速進步，大數據應用得宜的話，可以令我們整個城市更有效率地運行。例如在強烈颱風如山竹來襲之後，可以透過城市內的感應器，立即知道哪個地方有嚴重的樹木倒塌及山泥傾瀉，直接派員處理，」香港中文大學數據科學與政策研究課程主任黃偉豪說，為了令數據更公開透明，現時有些地方政府，會開設公開數據網站，讓個人及企業可自由地獲取政府在城市中收集的數據，包括美國、英國、加拿大、台灣以及香港等。未來，我們可能無可避免地，需要交出越來越多資料，有關於私隱的討論亦將會一直持續，但討論的過程中，需要不斷完善保障個人私隱，並在便利與保障私隱之間進行取捨。

當我們幾乎每日都為最新科技的面世而嘖嘖稱奇時，它們如何被掌握科技的人所運用，卻是一念天堂一念地獄。無可否認地，當下每個人內心最大的隱憂，會如著名政治哲學家鄂蘭（Hannah Arendt）所指，當權者會透過大規模的監視，令私穩與公共的界線變得模糊，令每個人都在自我審查，成為一個牢不可破的圓形監獄。當我們被拉進鋪天蓋地充滿新科技的未來時，會否迎來如作家赫胥黎（Aldous Huxley）在反烏托邦作品《美麗新世界》（Brave New World）中剝奪人性的高科技未來，抑或是一個真正的美麗新世界？ B

PHOTO：李運發（2）