



No. 194
APR, 2023

政風電子報



§主題故事

臺灣如何應對抖音的潛在威脅。

§廉政案例

國會史上最大宗立委集體貪瀆案！
構成貪污重罪將褫奪公權。

§資安宣導

資安不設防...從公部門到民間 駭
客駭一輪。

§公務機密

調查官外洩偵查筆錄！ 學長行賄、
學弟洩密均起訴。

§消費宣導

家用監控鏡頭存私隱外洩風險
9成不符歐洲網絡安全標準促生
產商改善和加強監管。

§廉政小劇場

企業誠信成功經營。

§獎勵廉能

臺灣如何應對 抖音的潛在威脅？



◆ 中正大學傳播系教授、台灣媒體觀察教育基金會董事長、台灣事實查核教育基金會董事長 — 羅世宏

不只臺灣，全球正面臨抖音帶來的潛在威脅。

TikTok is China's next big weapon

早在 2019 年，美國網路媒體《Axios》即曾報導指出，「TikTok 將會是中國的下一個絕佳武器！」¹ 抖音的演算法專為吸

睛內容而設計，具有錄製影音的便捷功能與病毒式大量擴散的魔力，有可能讓沒沒無名的普通人在一夕間爆紅。這些特質，

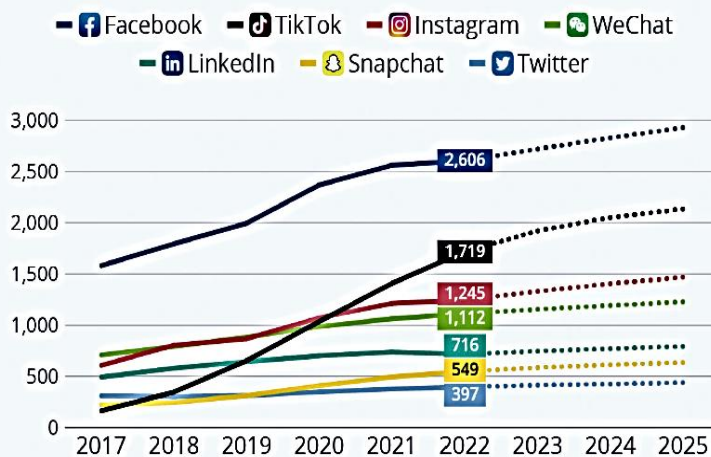
¹ Shane Savitsky, "TikTok is China's next big weapon", *Axios*, July 20, 2019, <https://www.axios.com/2019/07/20/tiktok-china-online-privacy-personal-data>.



抖音的演算法專為吸睛內容而設計，具有錄製影音的便捷功能與病毒式大量擴散的魔力，吸引許多民眾下載使用。（Photo Credit: HS You, <https://fic.kr/pi/2e7Zx7B>）

The Rapid Rise of TikTok

Number of active users of selected social networks worldwide (in millions)



Estimations as of June 2022. Projections from 2023 until 2025.
Source: Statista Advertising & Media Outlook



statista

根據數據統計，抖音自 2017 年開始逐漸崛起，目前已進入超過 150 個國家，是全球僅次於 Facebook 在最短時間內達到 10 億用戶的社交媒體。（Source: Statista, <https://www.statista.com/chart/28412/social-media-users-by-network-amo>）

不只讓全球各地的知名人物、網紅趨之若鶩，也讓青少年及其他年齡層使用者流連忘返。表面上它是輕薄短小的娛樂社交工具，但卻也常被用於散播假訊息與色情內容，並且是監控全球用戶隱私、蒐集個資的利器。由於大數據已成為 21 世紀最重要的戰略資源，抖音成功走向全球不只讓它在商業上具有競爭與廣告投放優勢，也可能被用於地緣政治、科技與軍事競爭，特別是它無法不受控於愈來愈獨裁的中國大陸政府，這一點特別令人憂慮。

在技術和商業操作上，抖音無疑是非常成功的數位產品與服務。目前，抖音已進入超過 150 個國家，用戶數量超過旗下擁有 Facebook、Instagram、Messenger、

Whatsapp 的 Meta 集團的一半以上，也是全球僅次於 Facebook 在最短時間內達到 10 億用戶的社交媒體。毫無疑問的，抖音已成為首款「征服全球」的中國大陸社群媒體，其全球觸達率和影響力遠超過其他中國大陸社群媒體或數位平臺服務（如微博、微信）。抖音背後的母公司是中國大陸網路巨頭「字節跳動」（ByteDance）集團，該集團尚未上市，但市值估計高達 3 千億美元，其中抖音即占半數，市值估計達到 1 千 5 百億美元。

印尼、印度、美國等案例

面對抖音這個始終不能令人放心、但在全球各地又廣受歡迎的中國大陸數位網



2020年「中」印爆發邊境衝突，印度以國家安全和隱私疑慮為由，禁止民眾使用抖音等59種中國大陸開發的應用程式；2021年，印度政府宣布永久禁止抖音。（Source: SCMP Clips, <https://youtu.be/b-e9cf7m9Kl>）

路巨頭，不少國家亟思反制之道，包括尋求全面封殺或是予以立法納管的可能性。

曾經最早對抖音採取封殺手段的國家是印尼。2018年，印尼以抖音「存在大量不良內容，非常不利於兒少的健康成長」為由，全面封禁抖音。後來印尼解除禁令，因為抖音有積極回應印尼官方關切，建立印尼在地的內容審查團隊，過濾刪除色情暴力內容。

另一個曾經封殺抖音的國家是印度。2019年，印度馬德拉斯高等法院以抖音涉嫌傳播色情內容為由，要求印度政府禁止國民下載抖音。抖音母公司「字節跳動」遂向印度最高法院提出上訴，印度政府後來撤銷對抖音海外版TikTok的禁令，並且在當地的Google Play和App Store恢復上架。

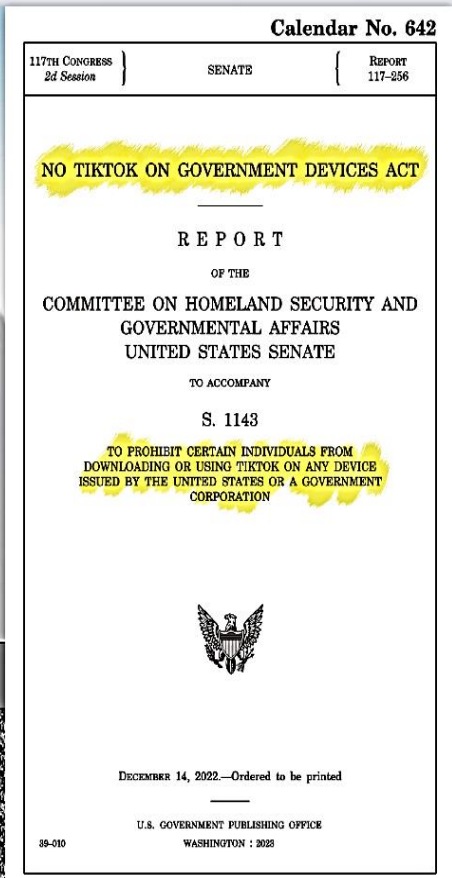
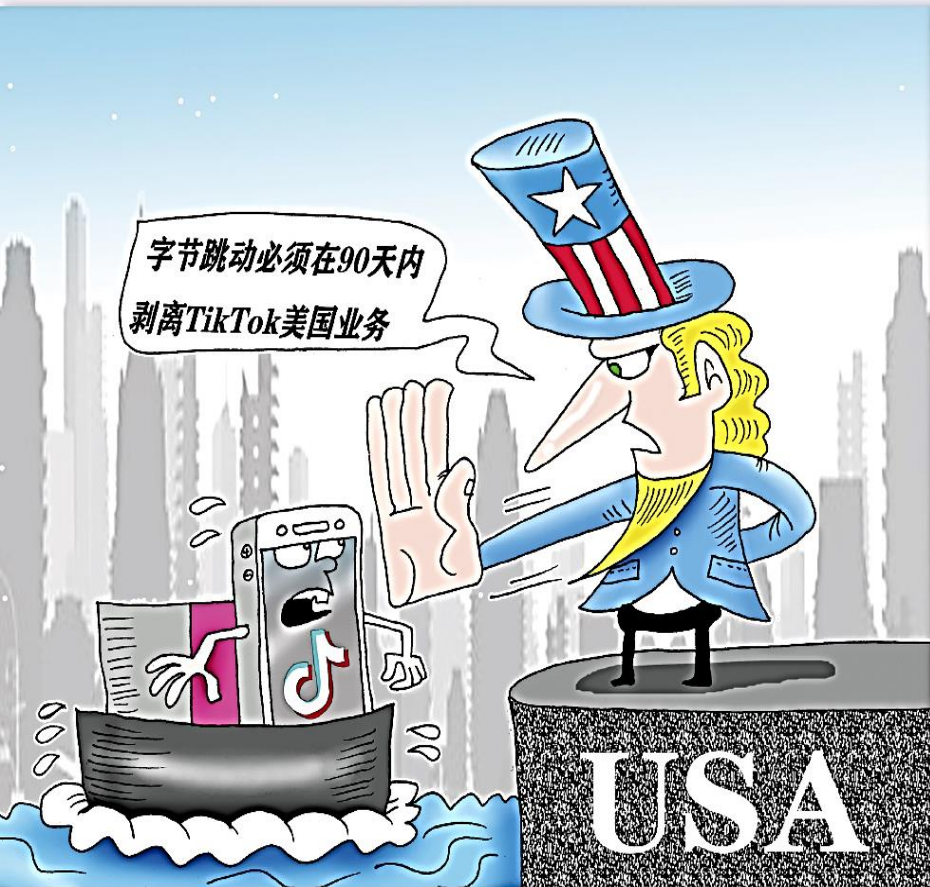
然而，2020年「中」印兩國爆發邊境衝突，印度旋即又再度以國家安全和隱私疑慮為由，禁止印度民眾使用抖音等59種

中國大陸開發的手機應用程式。2021年1月，印度政府宣布永久禁止抖音。

美國與其他西方國家也逐漸正視抖音帶來的潛在威脅。繼美國前總統川普2020年封殺抖音的行政命令被法院推翻以來，美國各界持續不斷有封殺或嚴加監管抖音的呼聲。去（2022）年12月23日，美國眾議院終於通過政府預算法案，限制美國聯邦政府使用字節跳動旗下各類軟件或服務，包括短影音軟體抖音。在此之前，美國國會曾多次嘗試限制美國聯邦政府部門使用抖音，這次終於成功達陣。

美國民主黨籍聯邦參議院情報委員會成員班奈特近日更呼籲蘋果和谷歌應用程式商店下架抖音，因為這個短影音平臺構成美國國安風險。

除了美國之外，其他民主國家如英國和澳洲也有類似呼聲。例如，在英國禁止華為參與5G工程建設後，英國保守

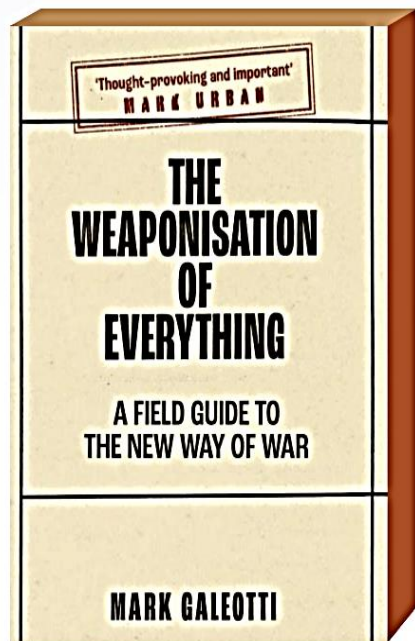


美國參議員提案禁止在聯邦政府內部使用抖音應用程式，該條款列入政府預算法案後，已經由參眾兩議院表決通過。（圖片來源：中新社／達志影像；Congress.gov, <https://www.congress.gov/bill/117th-congress/senate-bill/1143>）

黨前黨魁 Sir Iain Duncan Smith 也要求應該禁止抖音。同樣的，澳洲前總理 Scott Morrison 曾公開提醒澳洲公民謹慎考慮使用抖音的數據安全問題，而其他的澳洲國會議員亦公開質疑抖音暗地裡為中國大陸政府蒐集外國公民的隱私個資。

萬物皆可被武器化

《武器化的萬物論》（The Weaponisation of Everything，耶魯大學出版社，2022年）一書的作者馬克·加列歐提（Mark Galeotti）指出，資訊絕對是下一場戰爭的致命武器。在中國大陸對外軍事擴張意圖明顯、不斷繞臺軍演恫嚇的當下，



《武器化的萬物論》為馬克·加列歐提所著，其指出資訊絕對是下一場戰爭的致命武器。（Photo Credit: Yale University Press）

抖音帶來的國家安全、資訊安全與個資監控隱患，值得我國政府正視並積極應對。

研究機構 NewsGuard 去年 3 月的一項研究發現，² 如果你剛剛註冊抖音新帳號，就算你沒做什麼特別的事，只是一路往下隨意刷著「為您推薦」頁面，那麼你可能最快在 40 分鐘之內就會被導向有關烏克蘭的假訊息。隨著抖音越來越受歡迎，人們對它可能成為假訊息擴散溫床的憂慮也在升高當中。例如，《紐約時報》報導，³ 假訊息和深度造假影片曾經大量透過抖音散播，證實有心人企圖利用抖音影響 2022 年美國期中選舉。

回應外界關切，抖音透過官網宣稱，⁴ 它將「持續透過多元方式打擊假訊息」。包括「持續移除具誤導性或藉 TikTok 欺騙公眾、引導輿論的帳號」，以機器學習技術偵測，並輔以人工審核方式「評估、確認並移除違反假訊息政策的內容」。

臺灣觀點

我國從 2019 年行政院公布實施「各機關對危害國家資通安全產品限制使用原則」後，已經限制公部門資通設備及所屬場域使用抖音。數位發展部 2022 年特別發出一則公告澄清：⁵ 雖然該部認定「抖音或



《紐約時報》報導，假訊息和深度造假影片曾經大量透過抖音散播，證實有心人企圖利用抖音影響 2022 年美國期中選舉。（Source: TIKTOK）

TikTok（國際版）是危害國家資通安全產品，我國政府並未禁止一般民眾使用抖音。吸取先進民主國家經驗，建議我國政府積極採取因應手段，除了應該落實公部門資通設備與所屬場所不得下載與使用抖音的規定外，也應該主動調查抖音的內容審查、廣告投放、演算法操作等，是否有違反市場公平競爭與消費者保護等情事，並且採取相應的平臺問責措施，公開要求抖音回應相關疑慮。

另外，我國也應該學習歐盟《數位服務法》立法，正式將包括抖音在內的跨國數位平臺納管，以便同時兼顧國家安全、資訊安全、個資隱私與言論自由的多重目標。

（資料來源：清流雙月刊112年3月號）

² Alex Hern, "TikTok algorithm directs users to fake news about Ukraine war, study says," *The Guardian Weekly*, March 21, 2022, <https://www.theguardian.com/technology/2022/mar/21/tiktok-algorithm-directs-users-to-fake-news-about-ukraine-war-study-says>.

³ Tiffany Hsu, "Worries Grow That TikTok Is New Home for Manipulated Video and Photos," *The New York Times*, November 4, 2022, <https://www.nytimes.com/2022/11/04/technology/tiktok-deepfakes-disinformation.html?searchResultPosition=1>.

⁴ TikTok, 《TikTok 持續透過多元方式打擊假訊息》，2022 年 10 月 3 日，<https://newsroom.tiktok.com/zh-tw/an-update-on-our-work-to-counter-misinformation-tw>。

⁵ 數位發展部，《數位部禁止一般民眾用抖音？》，2022 年 12 月 27 日，<https://moda.gov.tw/press/clarification/3473>。

國會史上最大宗立委集體貪瀆案！ 構成貪污重罪將褫奪公權

國會史上最大宗立委集體貪瀆案，一審判決11人有罪，目前上訴二審中，依最高法院刑事大法庭的裁定，只要這些立委收了錢，召開協調會邀請行政機關說明，或對官員施壓關說，都構成貪污重罪並遭宣告褫奪公權。

議員或立委等民代在議場外的活動五花八門，但如果基於民代身分及職務，只是為民服務、關切，不構成貪污罪，但收了錢打電話向人施壓或關說、對其他有同意權限的民代請託施壓、聯繫代為提案或代為質詢，都恐觸犯收賄、圖利等貪污罪。

目前高院二審中的立委集體貪瀆案，太流公司董事長李恒隆，涉嫌透過白手套郭克銘等人行賄立委蘇震清、陳超明、廖國棟、徐永明等，以《公司法》修法或舉辦公聽會，施壓經濟部撤銷太流增資登記，企圖奪回SOGO百貨經營權，李在2012年找蘇向經濟部施壓。

其中靠著「太陽花運動」在政壇竄起的前時代力量黨主席徐永明，被檢方起訴指控，因李恒隆為了SOGO百貨經營權，請託他協助辦理公聽會，徐開口要錢，一審遭重判7年4月徒刑。

至於立委陳超明遭檢方指控收賄幫李恒隆辦公聽會，他應對方要求向經濟部施壓，指名要時任經濟部次長的王美花出席，但最後次長沒出席，且因陳的收費太高、效果不好，賄款遭李恒隆對半砍價，陳超明一審被判刑7年8月。

一審依貪污治罪條例的收賄罪重判涉案立委，由於刑事大法庭已對立委涉貪行為勾勒出違法態樣，二審如果採用此法律見解判刑，再上訴到最高法院後，涉案立委等人未來恐將遭重判定讞，因須宣告褫奪公權，就失去參選及從政機會。

民代收錢後構成貪汙行為態樣	
犯罪行為	觸犯法條
議場內施壓關說	貪汙治罪條例之收賄罪 
議場外開議前的拜會	
議場外要求相關人到其辦公室說明	
議場外出具便條或函件轉交承辦人	
議場外召開協調會邀請行政機關說明	
議場外向其他民代勸誘、請託或施壓，使其連署、代為提案或代為質詢	
違反利益衝突迴避	貪汙治罪條例之圖利罪

製表：《中國時報》林偉信

資安不設防...從公部門到民間 駭客駭一輪

故宮數千件國寶的數位圖檔遭駭，政府竟冷處理長達九個月，蔡英文總統高喊「資安即國安」，但層出不窮的個資外洩、駭客攻擊案件，證實闇黑部隊如入無人之境，已成無聲的國安危機。

繼華航、微風個資外洩後，臺灣資安破洞衝擊，連消基會高層都難倖免。消基會副董事長徐則鈺近日接到詐騙電話，對方精準說出姓名、電郵、下單誠品所購商品內容和日期，讓他差點上當，他義憤填膺地說，政府無積極作為，個資法賠償金額低，「所以沒有企業會怕！」

每月約新增三千人受害

目前，臺灣每月約新增三千至五千名民眾「受駭」，暴露在遭詐騙與認知戰風險中，有七成二企業供應鏈曾遭遇勒索病毒襲擊、陷入勒索病毒入侵風險。

臺灣在中美台局勢中，網路攻擊更頻繁。本報調查盤點發現，臺灣關鍵基礎設施舉凡石油、航空，到民營企業如華航、微風、iRent，再到半導體供應鏈如台積、廣達等科技廠商，早已全面被駭客「測試一輪」，無論國家級網攻或勒索軟體、駭客攻擊，臺灣毫無資安抵抗力。

根據來電辨識軟體Whoscall統計，二〇二二年，Whoscall攔阻高達四十六萬通短碼形式詐騙電話，數據較前一年暴增三倍。Whoscall的統計數據與刑事警察局不謀而合；根據刑事警察局出具的統計資料顯示，二〇二二年前五大高風險賣場分別是博客來網路書店、旋轉拍賣、蝦皮拍賣、誠品書局、迪卡儂。

據刑事局統計，全般詐欺（包含一般詐欺、網路詐欺）在二〇二二年的財損數高達近七十億元，創近五年來新高。其中又以網路詐騙增長最為迅速，去年全年通報的網路詐騙案將近七千件，財損金額逾廿億元，較五年前大幅升高四倍，上萬人受害。

逾千萬支手機資訊遭駭

除臺灣二千三百萬戶政個資遭駭外流，據Whoscall調查統計顯示，臺灣百分之六十五手機資料也外洩，若以我國廿至六十五歲人口共一千六百萬推估，全台一千〇四十萬人的手機號碼資訊落入駭客手中，平日恐遭詐騙、戰時將遇認知和假訊息戰。

雖然數位部積極幫助政府機關導入T-Road資料傳輸機制，但公部門人員未改變習慣，還是老採用傳統U S B、燒光碟傳輸資料，導致有心人士從中攔截資料甚至外洩；政府在完善政府機制、立法、資安人才培養、要求企業當責上，皆未採取積極行動。

企業資安預算不到千萬

臺灣企業也未將防駭視為己任，據IThome統計，臺灣大型企業去年資安投資，平均每家企業預算僅新臺幣七百一十五萬元。民營企業輕忽己責已讓台積創辦人張忠謀、副總統賴清德、內政部長林右昌、台塑董事長林健男等台灣重要人士個資外洩。

未來戰爭主打「混合戰」（融合傳統、政治、網路和不對稱作戰），當美、歐、中國大陸在拚「資安軍備競賽」，臺灣資安還得補破網，個資外洩後的一連串惡性循環與外溢衝擊正要發酵。



調查官外洩偵查筆錄！ 學長行賄、學弟洩密均起訴

〔記者錢利忠 / 台北報導〕調查局驚傳偵查筆錄外洩案！時任桃園市調查處周姓調查官，涉嫌接受已從調查局退休並轉任光寶科技稽核室處長的曹男委託，私自將沈姓同事承辦台灣達爾科技併購光寶科子公司敦南科技所涉內線交易等兩起案件的移送書，外洩給曹男，調查局發現偵查筆錄外洩後移送桃園地檢署偵辦，周、曹2男昨被起訴。調查局長王俊力得知竟有調查官外洩同仁的偵查筆錄，對此深感痛心，並指示絕不姑息護短。

調查局指出，偵辦某違反證券交易法案期間，主動發掘有周姓同仁疑涉洩密不法情事，經蒐證後，報請桃檢指揮偵辦，並立即將周員調離現職，全力配合檢方偵辦；周員被依涉嫌洩漏國防以外秘密罪起訴，將依檢方偵查結果，召開考績委員會從嚴議處。據了解，周男已被調職至總務處，至少將面臨大過1支懲處。

調查局要求全體調查人員「正人必先正己」，執行案件偵辦工作，必須嚴守紀律，恪遵法令，若有違犯法紀情事，即查辦到底，嚴予究責，以符合國人期待。

全案起源於2021年5月，曹男從周男那得知其老闆所牽連的相關案件，是由沈姓調查官負責，便私下約沈男到超商碰面，除暗示沈男不要移送該內線交易案之外，還給沈男2台iPad平板電腦，沈男隨即將曹男行賄一事，向上陳報至調查局督察處，調查局隨即指示北部地區機動工作站介入調查，經報請桃檢指揮偵辦後，桃檢於昨日偵結起訴。



家用監控鏡頭存私隱外洩風險 9成不符歐洲網絡安全標準促生產商改善 和加強監管

「智能家居」近年愈趨普及，不少家庭都會安裝家用監控鏡頭，用家既可隨時隨地透過智能裝置觀看家庭成員起居活動，亦可直接與家人隔空對話，並且能夠將攝錄影像儲存，被視為保障家居安全的重要智能裝置。監控鏡頭透過連接網絡得以運作，故此網絡安全尤為重要，否則影像及個人敏感資料便有可能外洩，構成私隱甚至其他安全風險。消費者委員會測試了市面上10款家用監控鏡頭的網絡安全，結果發現只有1款樣本符合歐洲的網絡安全標準，其餘9款均有不同的網絡安全隱患，包括沒有以加密方式傳送影像和資料、未能防禦駭客以「暴力攻擊」方式破解密碼等。另外，監控鏡頭的應用程式在儲存用戶資料方面安全度不足，當中半數樣本可透過Android版本應用程式存取用戶於智能裝置中的檔案，而部分應用程式存取的權限亦過多。消委會促請生產商改善產品的網絡安全，例如加入防禦暴力攻擊的設計及為影片及資料進行數據加密。消費者為監控鏡頭設定密碼時亦要有足夠強度並且定期更改，以及善用防火牆及網絡監察等功能。

測試的10款家居監控鏡頭樣本，售價介乎\$269至\$1,888，全部樣本均提供雙向語音對話、移動偵測、夜視、Amazon Alexa 及 Google Assistant語音控制等功能。消委會委託獨立實驗室參考歐洲標準ETSI EN 303 645及工業標準OWASP MASVS測試此10款樣本的網絡安全，含防攻擊能力、資料傳送及應用程式安全性、儲存資料保密性，以及硬件設計。



5款鏡頭傳送影像或資料沒加密 駭客易竊探

監控鏡頭的應用程式會直接將鏡頭拍攝所得的實時動態影像，串流至流動裝置，方便用戶透過應用程式實時監察情況。測試發現，其中4款樣本在傳輸影像時，沒有使用可提供數據加密和訊息認證的「安全即時傳輸協定」（SRTP），只採用安全性較低的「即時傳輸協定」（RTP），過程中沒有將影片數據加密，傳送途中有機會受到駭客攻擊，能輕易窺探影片內容。另外1款樣本連接用家的Wi-Fi無線網絡時，使用「超文本傳輸協定」（HTTP）傳送資料，沒有把敏感資料加密，駭客可以從普通文字檔找到路由器的帳戶資料。若生產商改用安全性較高的「超文本傳輸安全協定」（HTTPS），可為用戶提供更大的私隱保障。

若有駭客試圖入侵，密碼愈長且愈複雜，所需的破解時間便會愈長。測試發現，有3款樣本在進行實時動態影像串流時，駭客可透過自動化工具和程式展開「暴力攻擊」，透過反覆試驗所有可能的密碼組合，試圖破解密碼，當中有2款的預設密碼只有6位數字或字母，強度非常低，較容易讓駭客破解，繼而竊取影片。另1款監控鏡頭則在使用手機應用程式登入帳戶時，駭客可不斷地重複嘗試以竊取帳戶資料。

消委會建議生產商進行實時動態影像串流或登入帳戶時加入防禦暴力攻擊的設計，例如採用多重認證及限制嘗試密碼的次數，當發現短時間內由同一IP地址多次登入失敗後，便自動將帳戶封鎖一段時間，防止駭客繼續攻擊，同時應加強預設密碼的長度及複雜性，藉此提高安全性。

3款鏡頭重新登入帳戶時 舊有對話金鑰仍有效

用戶每次登入連接鏡頭時均會使用相當於臨時密碼的對話金鑰，用以將傳送的資料和數據加密及解密。對話金鑰會在中斷連接後失效，當用戶再次登入時，會使用一個新的對話金鑰。不過，測試結果發現其中3款樣本在重新登入連接鏡頭時，用於上一次連接的對話金鑰仍然有效，假如駭客成功偷取舊的對話金鑰，即可連接鏡頭，偷窺室內影像。而該3款樣本中，有1款更可於同一手機內的應用程式登出帳戶或登入另一個帳戶後，仍然可以看到監控鏡頭拍攝所得的實時影像，存在安全漏洞。

應用程式儲存資料安全度不足 敏感資料有外洩風險

測試結果亦顯示，全部10款樣本在應用程式內儲存資料時，安全性均不足夠，例如將電郵地址、帳戶名稱或密碼等敏感資料，儲存於普通文字檔，卻沒有使用加密技術保護，相關資料要相隔一段時間後才會移除，令駭客有機可乘。

另外，部分監控鏡頭的應用程式內嵌瀏覽器，讓用戶可直接瀏覽網頁，但其中5款樣本Android版本的內嵌瀏覽器沒有封鎖存取檔案的權限，駭客可透過植入程式碼存取裝置內的檔案。此外，有5款樣本的手機應用程式存取過多權限，部分樣本存取的資料較為敏感，例如會讀取裝置上的行事曆、帳戶資料、用戶正在使用的應用程式等，裝置內的資料有機會外洩。消委會提醒消費者在安裝及使用監控鏡頭的應用程式前，需留意當中要求存取用戶資料的權限，因為當下載及完成安裝程式後，有關權限就會容許程式在毋須再經用戶同意下，自動存取相關資料，用戶亦無法知悉程式會如何及何時使用有關資料。

使用監控鏡頭 應告知家傭及訪客

根據個人資料私隱專員公署的《閉路電視監察及使用航拍機指引》，消費者若在家中安裝監控鏡頭，應知會包括家庭傭工在內的家中所有成員及訪客，亦須考慮監察的範圍和程度，並且應該充分理解公署發出的《僱主監察僱員工作活動須知：家傭僱主應注意的事項》中的內容，包括評估進行監察的需要、有否其他較不侵犯私隱的替代方法、考慮攝錄監察方式的合理性、告知僱員有關監察活動的公開性、以及妥善處理攝錄紀錄的方法等。

新加坡、德國、芬蘭及美國等國家已推出物聯網裝置的網絡安全標籤認證計劃，歐盟亦已將網路及通訊安全的要求加入無線電設備指令，並於2024年8月強制生效，英國亦正研究立法規管。消委會建議香港政府可參考不同國家的做法，推出適合本港的相關計劃或標準，從而推動本地物聯網裝置的網絡安全。

消委會提醒消費者選購和使用家居監控鏡頭時，應注意以下事項：

- 一. 不應購買沒有品牌或來歷不明的產品，不但品質沒有保證，網絡安全亦未必完善。
- 二. 建立帳戶時密碼應有足夠強度，例如長度不應少於8位，並混合大小楷字母、數字及特殊符號來提高密碼強度，以及定期更改，防止被輕易破解。若監控鏡頭由專人上門安裝及設置，切記在安裝後立即更改密碼。
- 三. 建議在有需要進行監控時才開啟應用程式及啟動鏡頭，完成後建議把應用程式及鏡頭關掉。此外消費者應使用個人智能裝置登入鏡頭觀看畫面，不應以任何公用及沒有管理權限的裝置登入帳戶，亦應避免使用公共無線網絡Wi-Fi進行監控，以免帳戶資料被記錄及盜取。
- 四. 應善用防火牆、網絡監察及活動紀錄等功能，經常查看紀錄以偵測可疑活動。此外亦應不時檢查及更新韌體（firmware），以保持產品良好運作及修補安全漏洞。
- 五. 假如懷疑鏡頭內部系統曾被入侵或植入程式，建議修復一次官方韌體及將產品還原至出廠狀態，並可在重新安裝時建立全新帳戶及設定新密碼。

(資料來源:消費者委員會)



嘩破，就只差那麼一點點... 你幹嘛這麼固執嘛？

哎喲，又吃不出來！如果公司無法如期交貨，以後怎麼再接大財團的生意啦？

我跟你說，只要是我們公司出貨的產品，就一定要「檢驗合格」，差一點點都不行，那是魚目混珠！

小風啊，嘩破對於企業誠信的堅持是有道理的，這些年來，不都是這樣腳踏實地、勻勻仔行(臺語)、撐過難關、走到了今天！

1 2
3 4

我知道大家都很打拼、很辛苦，再堅持一下，我們把產品的品質顧好，一定要檢驗合格的產品才能夠出貨，勻勻仔行(臺語)，沒問題的啦！

廉政溫馨小叮嚀

企業誠信，是成功經營最踏實的路！廉政工作的推動，需要民間社會力量共同參與，結合私部門共同反貪，人人堅持不做違法的事，一起為誠信經營的企業提供公平的競爭環境。



內政部移民署政風室
關心您



獎勵廉能

本署北區事務大隊桃園市專勤隊屬員 拒收餽贈，廉潔表現，特予表揚

本(112)年1月30日北區事務大隊桃園市專勤隊屬員執行陳女申請大陸地區人民來臺團聚案之訪談勤務，面談結束後陳女在等待整理列印「電話訪談紀錄表」予渠審閱簽名時，試圖塞紅包至屬員口袋，經屬員斷然拒絕，屬員於第一時間報告該隊隊長，並向政風人員通報。



本署北區事務大隊新北市專勤隊屬員 拒收餽贈，廉潔表現，特予表揚

本(112)年2月8日下午4時許，北區事務大隊新北市專勤隊屬員執行大陸地區人民劉女申請在臺長期居留審核前查察勤務，屬員於勤務結束欲離開時，劉女突取出1捲新臺幣千元鈔強塞給屬員，屬員見狀旋即制止劉女並返還該捲新臺幣，返隊後屬員立即報告該隊隊長，並通報政風室。



政風電子報

刊名 / 政風電子報

出版機關 / 內政部移民署政風室

地址 / 10066臺北市中正區廣州街15號7F

出版年時間 / 中華民國112年4月

頻率 / 月刊

編輯總召 / 康明旺

主編 / 簡國樑

本室編輯小組 / 張文山、陳安莉、陳怡安、蔡雅雯

為落實新世代反毒政策，衛生福利部食品藥物管理署與插畫家「怪奇事務所」合製6款插圖建置於該署「睡睡平安」粉絲團，網址：
<https://www.facebook.com/sleepverywell>
請多支持喔~~~



HAPPY CHILDREN'S DAY