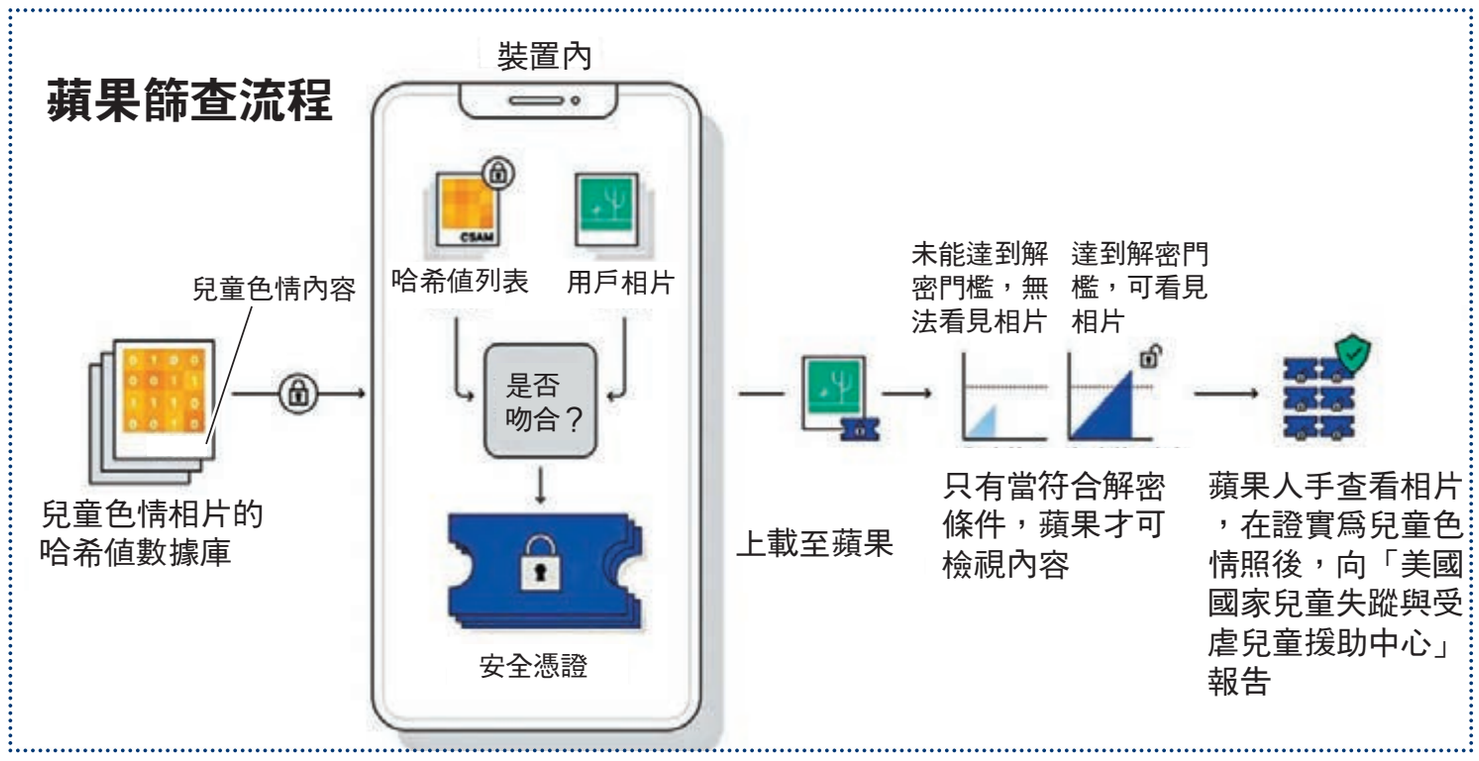
未上傳至伺服器已檢查 如客戶端設監測系統

掃描iPhone封殺猥褻兒童照 蘋果恐變美監控工具

美國蘋果公司前日宣布，計劃推出新程式以打擊兒童色情罪行，美國用戶從iPhone等裝置上載相片至雲端iCloud時會進行掃描，檢查是否屬兒童色情相片，一旦發現有問題便會向執法部門舉報。不過由於蘋果使用的程式，是在照片到達蘋果的伺服器前已進行掃描，多個民權組織均認爲蘋果此舉等同製造「後門」，可能成爲美國政府監控國民的工具。 ●香港文匯報記者 林文佑



新程式只會在美國使用，預料在9月或10月推出iOS 15系統時啟用。據蘋果前日在官網解釋，公司會採用名為「NeuralHash」的技術，日後用戶上傳相片至iCloud時，系統會將照片與執法部門的兒童色情資料庫（CSAM）作對比，如果內容吻合，便會經人手作進一步覆核，一旦確認為違法內容，蘋果便會關閉涉事賬戶，並通知一直與警方合作的國家兒童失蹤與受虐兒童援助中心（NCMEC）。

模糊iMessage猥褻內容 可通知家長

此外，為保障未成年人士接觸到有問題內容，系統亦會掃描透過iMessage向未成年人傳送的訊息和相片，若發現有猥褻內容，會將其模糊，並彈出通知，稱若用戶點閱便會通知家長。

facebook（fb）等科企亦有同類檢驗系統，分別在於掃描的時機，其他科企的系統是在用戶相片抵達公司伺服器後，才進行篩查，蘋果的系統則在上載前進行比對，等同在客戶端設立監測系統；蘋果則強調，會採用「加密圖像技術」進行比對，直至電腦發現有問題才會解密，同時若用戶不上載照片至iCloud，系統亦不會進行比對。

關注兒童權益組織大多歡迎有關做法，NCMEC行政總裁克拉克便指出，蘋果產品的用戶非常多，新措施對受害兒童而言可起救命作用，並指出「現實就是私隱和保護兒童可以並存」。

加密用戶訊息承諾淪空談

民權組織則對監測客戶端的做法感到不安，「電子前線基金會」指出蘋果的出發點良好，但要打造一個只限於監管兒童色情物品的客戶端監測系統是「不可能」，先例一開，蘋果加密用戶訊息的承諾便淪為空談，亦會打開大門作更廣泛用途，形容無論如何狹窄的電腦後門都是後門。

約翰霍普金斯大學資訊安全研究所電腦科學系副教授格林則在Twitter形容，蘋果如同向各地政府發出明確訊息，如果是為了找出禁制內容，設立系統掃描用戶手機並無不妥。

斯諾登批蘋果如全球大監控 產品變「電子告密者」

● 斯諾登（右）形容，蘋果的最新規定如同在全球進行大規模監控計劃。圖為他2014年受訪。 資料圖片

蘋果公司為打擊兒童色情罪行，決定在用戶電子裝置設置相片掃描系統，但不少網絡安全專家均認為此舉立下危險先例，擔心蘋果日後受到各地政府壓力，將內容審查範圍擴展至兒童色情以外。曾揭露美國政府監控計劃的中央情報局（CIA）前僱員斯諾登形容，蘋果的最新規定如同在全球進行大規模監控計劃。

斯諾登表示，即使蘋果用意如何良好，人們亦需明白蘋果現時可以針對兒童色情內容，難保將來不會涉及其他範疇，形容蘋果在未有徵得用家同意下，便將旗下所有產品變成「電子告密者」。他亦指出，蘋果一直被認為是致力保護用家私隱的科企，例如在2015年加州一宗槍擊案後，即使收到聯邦調查局（FBI）要求和聯邦法官命令後，仍拒絕解鎖槍手法魯克的iPhone，但蘋果作風現時已明顯改變。

加密技術專家麥菲特表示，當用戶購買一部手機，便期望可控制手機上的資料，蘋果卻拒絕賦予客戶這項權利，甚至自以為由蘋果篩查手機內容是毫無問題，形容蘋果在保障個人私隱範疇倒退一大步。

擷取「數碼指紋」 設雙重加密減誤判

蘋果公司為確保新的相片掃描功能可保障用戶私隱，只會擷取相片內獨有的哈希值（hash value），不會直接看到相片內容，在與非牟利組織「美國國家兒童失蹤與受虐兒童援助中心」（NCMEC）兒童色情資料庫內的相片哈希值對比，在結果吻合後才會經人手檢視。蘋果亦設立雙重加密機制，減少系統誤判機會，避免無辜用戶被誤作管有兒童色情照。

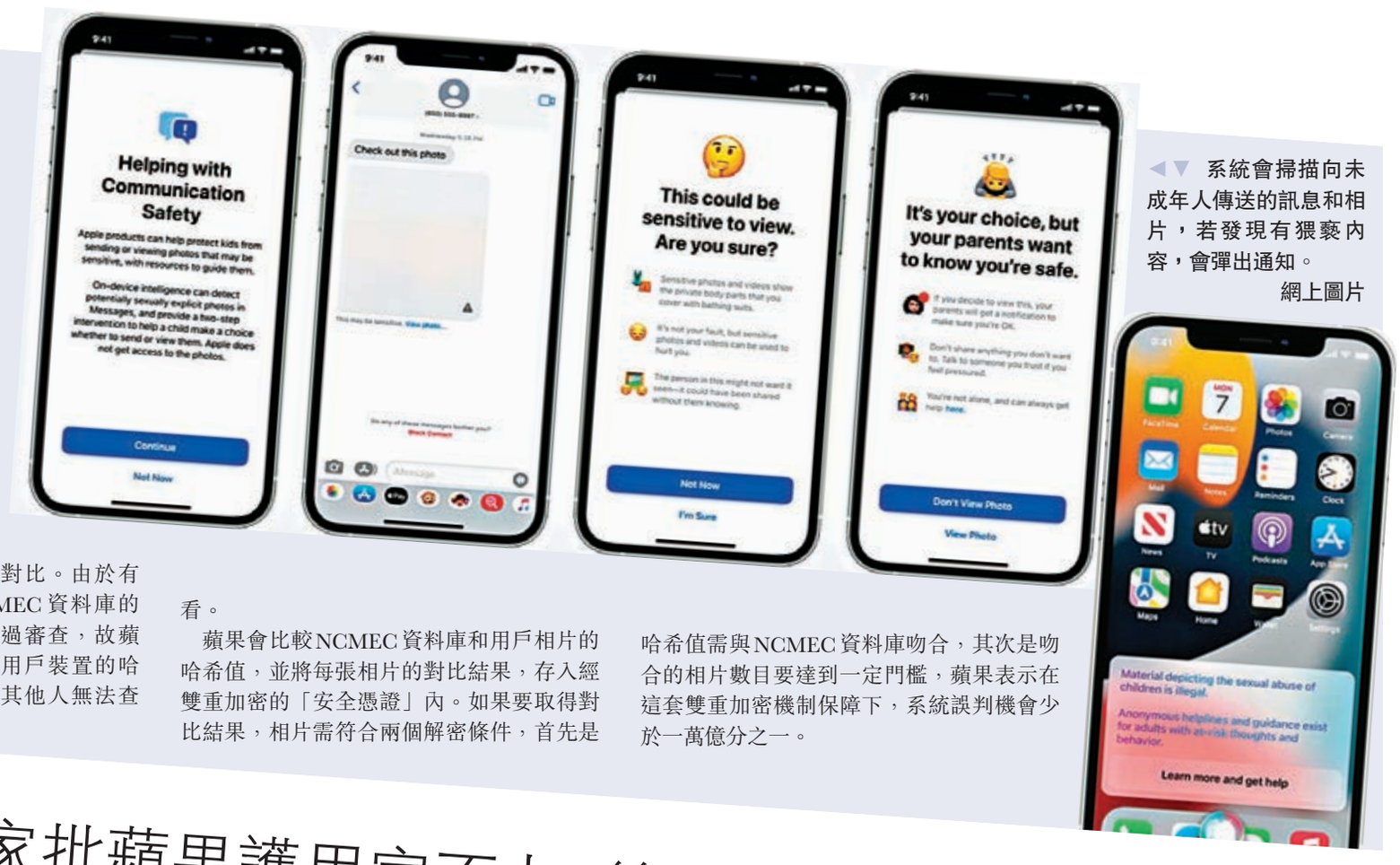
裁剪上色仍可還原

所有相片均可透過演算法取得其獨特的哈希值，相片的複製檔案和原相均有相同哈希值，等同照片的「數碼指紋」，科企現時偵測兒童色情內容的系統，亦是透過對比哈希值運作。蘋果今次將應用新的哈希值處理技術，令相片即使經過裁剪和上色，亦可還原原相的哈希值，令不法之徒無法透過修改相片以逃避篩查。

誤判機會 少於一萬億分之一

在新流程下，用戶上傳相片至iCloud前，蘋果會將NCMEC資料庫的哈希值下載至用戶裝置，並掃描裝置內等候上載的照片作對比。由於有人可能乘機讀取裝置內NCMEC資料庫的哈希值，並利用相關資料避過審查，故蘋果透過加密技術，將下載至用戶裝置的哈希值數據庫「亂碼化」，令其他人無法查看。

蘋果會比較NCMEC資料庫和用戶相片的哈希值，並將每張相片的對比結果，存入經雙重加密的「安全憑證」內。如果要取得對比結果，相片需符合兩個解密條件，首先是哈希值需與NCMEC資料庫吻合，其次是吻合的相片數目要達到一定門檻，蘋果表示在這套雙重加密機制保障下，系統誤判機會少於一萬億分之一。



◀▼ 系統會掃描向未成年人傳送的訊息和相片，若發現有猥褻內容，會彈出通知。 網上圖片

● Pegasus透過「零點擊」攻擊手法入侵包括iPhone在內的手機。 網上圖片

專家批蘋果護用家不力 籲開放系統增防護力

蘋果公司一直標榜旗下裝置的安全性，但以色列科技公司NSO開發的間諜軟件「Pegasus」，早前被揭發協助多國政府監控記者和政界人物的手機，當中包括iPhone，反映蘋果產品存在安全漏洞。部分資訊安全專家認為，蘋果有能力採取更多措施，保護用戶免受Peagsus入侵，例如加強開放iOS作業系統，讓研究人員進一步了解系統特性，有助預防黑客攻擊。

Pegasus透過「零點擊」攻擊手法入侵目標人物手機，即是對方沒有點擊黑客發出的訊息或連結亦會「中招」。

預防「零點擊」攻擊不理想

雖然蘋果今年較早時於iOS 14加入「BlastDoor」功能，試圖預防「零點擊」攻擊，但效果未如理想，故蘋果推出iOS更新版本，應對Pegasus揭露的漏洞。資訊安全研究人員歐文斯表示，iOS受到Pegasus入侵，反映即使蘋果旗下產品的保安功能嚴密，只要黑客擁有一定資源，仍可成功入侵，「蘋果確實嘗試提高安全性，但所付出的努力不符合外界期望。」

不少網絡安全人員一直提出，蘋果應加強作業系統的「可觀察性」，令其他研究員更了解iOS，不但有助抵擋黑客攻擊，亦可解構攻擊是如何發動。iOS安全研究員斯特拉法赫表示，雖然提高「可觀察性」可能構成黑客更易入侵的風險，但蘋果能採取更安全的方式應對，他對於蘋果未有這樣做感到費解。