小心私隱被竊！9成家用鏡頭存安全漏洞

外出工作的家人想時刻關心小孩、長者或寵物，又或擔心家居發生意外，家用監控鏡頭可隨時隨地透過智能裝置觀看家人的起居活動，儲存攝錄的影像，甚至可直接與家人隔空對話。但萬一監控鏡頭存有網絡安全的漏洞，影像便有機會外洩構成私隱風險，所以網絡安全十分重要。本會首次測試市面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，餘下9款均存有不同的網絡安全問題，例如未能防禦駭客的「暴力攻擊」、傳送資料時沒有加密等。此外監控鏡頭的應用程式亦有待改善，全部樣本儲存用戶資料均不夠安全，當中6款更可透過應用程式存取智能裝置的檔案，用戶私隱有外洩風險。

梧天男

我當年喺澳洲同而家屋企都有用監控 cam。

當時喺澳洲用監控 cam，係因為屋企生意上有需要。不過當有劫案發生，發現原本部 cam 攝錄得唔夠清楚，之後屋企就再 upgrade 另一部。

至於香港屋企，我會用 cam 睇住狗狗 Arthur。見佢平日習慣留喺邊個位置，我就會喺嗰度加張氈放杯水。不過有時 Arthur 都會同我作對，故意搞亂檔！

物聯網裝置的網絡安全不容忽視！

隨着科技發展，不少智能裝置已備有通訊功能，可透過互聯網互相傳送資料及發出指令，形成物聯網（Internet of Things，簡稱IoT）。而智能家居亦愈趨普及，家用物聯網裝置的應用非常廣泛，例如監控鏡頭、智能手錶、玩具、燈具、電器等。物聯網裝置可為生活帶來各種便利，但若裝置存有網絡安全的漏洞，便有機會被駭客破解，用戶的私隱或會透過網絡外洩，甚至可在用戶不知情下從遠端「借用」其裝置發動網絡攻擊，故此物聯網裝置的網絡安全不可忽視。

由於物聯網裝置主要透過智能裝置的應用程式進行遠端操作，物聯網裝置及手機應用程式的網絡安全同樣重要。歐洲電信標準化協會網絡安全技術委員會（European Telecommunications Standards Institute，簡稱ETSI）為物聯網裝置建立網絡安全標準，於2020年6月發布了個人物聯網裝置的網路安全/隱私保護標準ETSI EN 303 645。該標準主要檢視裝置的預設密碼、軟件更新、通訊、數據處理等是否安全。

開放式網路應用程式安全計劃（Open Web Application Security Project，簡稱OWASP）發布的流動應用程式安全標準（Mobile Application Security Verification Standard，簡稱MASVS），主要檢視Android和iOS操作系統的應用程式的網絡通訊、認證、資料儲存、介面設計等是否安全。

安裝家用監控鏡頭的步驟

用戶於智能裝置安裝相關應用程式及建立帳戶

監控鏡頭插上電源，主要透過 Wi-Fi 無線網絡連接家中路由器 (router)

設置監控鏡頭時大多會利用智能裝置或監控鏡頭掃瞄 QR 圖碼

用戶開啟應用程式及登入連接鏡頭時，便會連接至生產商的伺服器

測試樣本及項目

本會委託獨立實驗室參考ETSI EN 303 645及OWASP MASVS標準測試市面10款家居監控鏡頭的網絡安全表現，包括防攻擊能力、資料傳送安全性、應用程式安全性、儲存資料保密性及硬件設計。各樣本的售價由$269至$1,888，全部樣本都提供雙向語音對話、移動偵測、夜視、Amazon Alexa及Google Assistant語音控制等功能。

「arlo」(#1)須另購配件才可把影片儲存於USB記憶棒內，其餘9款樣本的機身設有micro-SD記憶卡內插槽，插入記憶卡便可儲存影片。5款樣本包括「arlo」(#1)、「imou」(#3)、「eufy」(#6)、「SpotCam」(#7)及「reolink」(#9)具備基本防水功能，室內及戶外均可使用，其中樣本#1、#7及#9內置充電池，可靈活擺放較為方便。

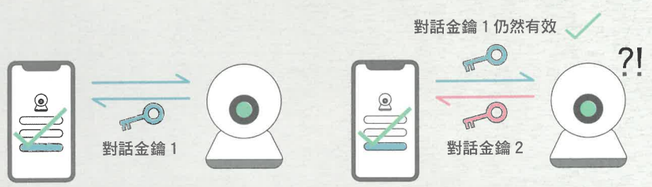
測試結果

防攻擊能力

1 款登出帳戶後仍可觀看影像串流

用戶開啟監控鏡頭的相關應用程式及登入帳戶後便可遙距監控家中的情況，而每次登入連接鏡頭時，都要先連接至生產商的伺服器，因此生產商能提供可靠又安全的連接服務至關重要。理論上，用戶應先登入已連接監控鏡頭的帳戶才可觀看實時動態影像串流(real-time video streaming)。然而測試發現，「reolink」(#9)於同一手機內的應用程式即使已登出帳戶或登入另一個帳戶後，仍可看到已登出帳戶所連接的監控鏡頭拍攝所得的實時動態影像，裝置存在網絡安全漏洞。

圖一



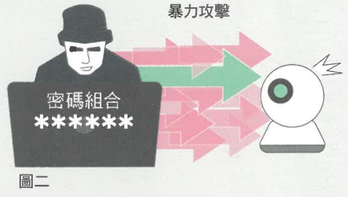
3 款樣本的舊有對話金鑰仍有效

用戶每次登入連接鏡頭時均會使用對話金鑰(session key)。此金鑰就像一個臨時密碼，用於加密及解密互相傳送的資料及數據，當中斷連接後，該次連接使用的對話金鑰便會失效。若用戶重新登入帳戶連接鏡頭，會使用一個新的對話金鑰進行加密及解密。惟測試發現，當用戶重新登入帳戶連接鏡頭時，「BotsLab」(#5)、「SpotCam」(#7)及「reolink」(#9)用於上一次連接的對話金鑰仍然有效，若駭客成功偷取舊有的對話金鑰，便可連接鏡頭。(見圖一)

4 款樣本未能防禦駭客的暴力攻擊

測試發現，3款樣本包括「eufy」(#6)、「EZVIZ」(#8)及「D-Link」(#10)進行實時動態影像串流時，駭客可透過暴力攻擊(brute force attack)以獲得密碼。暴力攻擊主要透過試誤法(trial and error)來破解密碼，透過反覆試驗所有可能的密碼組合，直至成功破解密碼。嘗試破解密碼的次數取決於密碼的長度及複雜性，密碼愈長愈複雜，破解密碼所需的時間便愈長，因此駭客通常使用自動化工具和程式進行暴力攻擊。(見圖二)

「EZVIZ」(#8)及「D-Link」(#10)實時動態影像串流的預設密碼分別為6位字母或數字，密碼強度非常弱。由於預設密碼過於簡單，駭客很快便可把密碼破解並竊取實時串流的影片。故該2款樣本應加強預設密碼的長度及複雜性，例如以混合大小楷字母、數字及特殊符號來提高強度。

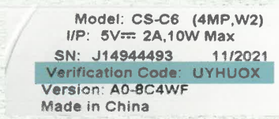


圖二

另外，當使用「SpotCam」(#7)的手機應用程式登入帳戶時，該應用程式未有限制可登入次數，駭客可不斷地重複嘗試登入以獲取帳戶資料。

本會建議樣本#6、#7、#8及#10的生產商為其產品的實時動態影像串流或帳戶登入加入防禦暴力攻擊的設計，例如採用多重認證(multi-factor authentication)及限制嘗試密碼的次數。當來自同一IP地址，短時間多次登入失敗後應封鎖帳戶一段時間，以防駭客進行暴力攻擊。

#8



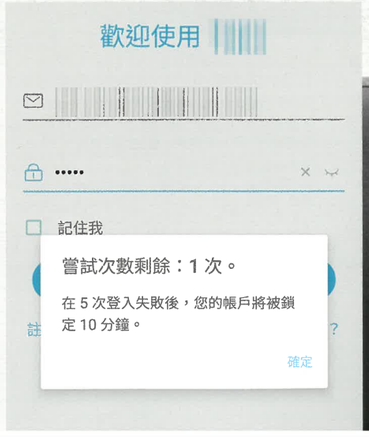
#10

「EZVIZ」(#8)及「D-Link」(#10)的預設密碼分別只有6位字母或數字，強度非常弱。

5 款樣本沒有加密傳送 資料易外洩

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

用戶多次登入失敗後會被封鎖帳戶一段時間，以防駭客進行暴力攻擊，防禦設計較理想。

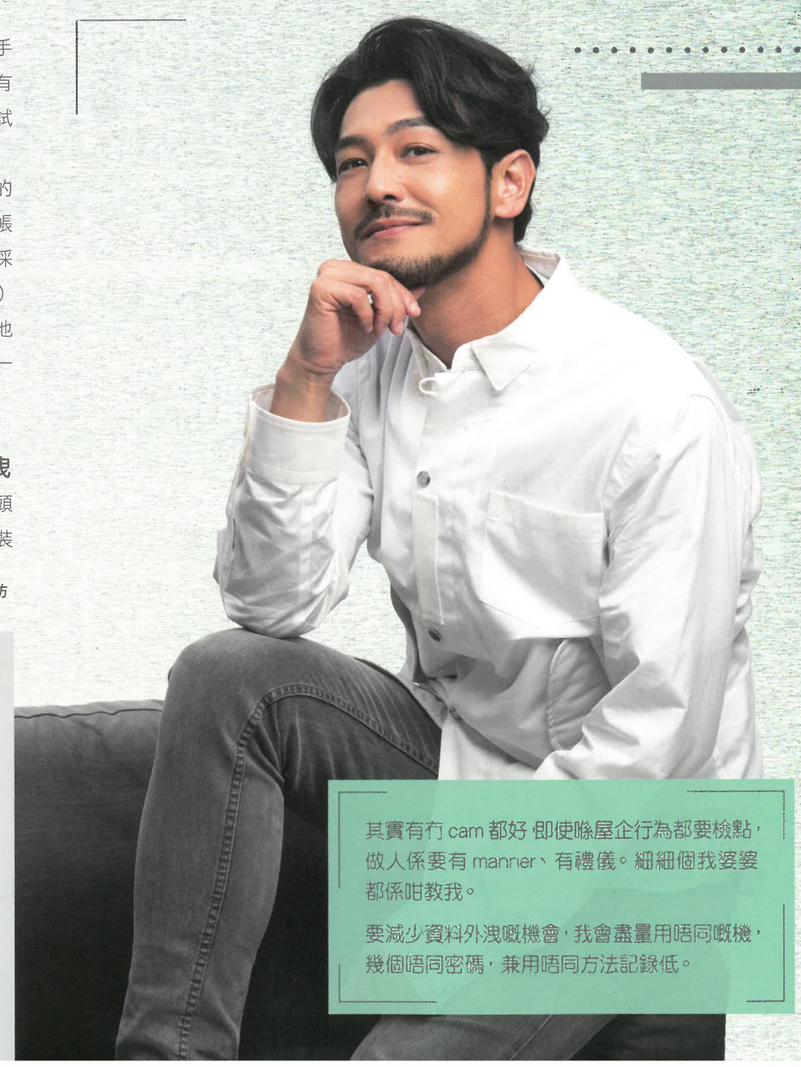


多國積極推動物聯網裝置的網絡安全

由於物聯網產品愈來愈普及，不少國家已採取不同方式推動物聯網裝置的網絡安全。

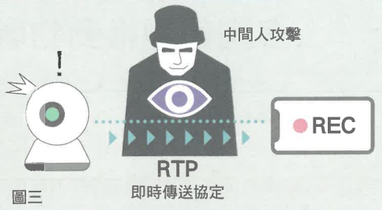
新加坡、德國、芬蘭及美國等國家已推出物聯網裝置的網絡安全標籤認證計劃，若裝置的網絡安全符合計劃的要求，便可獲得標籤。部分國家亦已互相認可雙方的標籤計劃。

歐盟已將網路及通訊安全的要求加入無線電設備指令(Radio Equipment Directive，簡稱RED)，並將於2024年8月強制生效，規定製造商在產品的設計和生產上都必須符合ETSI EN 303 645及其他相關標準，英國亦正研究立法規管。本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。

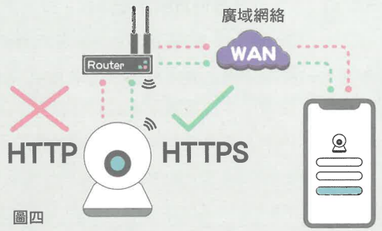


置，故傳送影片的安全性亦相當重要。4款樣本包括「imou」(#3)、「TP-Link」(#4)、「EZVIZ」(#8)及「D-Link」(#10)採用即時傳輸協定(Real-time Transport Protocol，簡稱RTP)來進行實時動態影像串流，沒有把影片數據進行加密，故傳送影片時有機會受到中間人攻擊(man in the middle attack)，駭客可輕易窺探影片內容，侵犯用戶的私隱(見圖三)。本會建議生產商使用安全即時傳輸協定(Secure Real-time Transport Protocol，簡稱SRTP)，此協定可提供數據加密、訊息認證(message authentication)和完整性(integrity)保證等。

「reolink」(#9)透過mysimplelink服務連接用家的Wi-Fi無線網絡時，沒有進行身分驗證(authentication)，只使用超文本傳輸協定(Hyper Text Transfer Protocol，簡稱HTTP)傳送資料，沒有把敏感資料加密，駭客可從普通文字檔找到路由器(router)的帳戶資料，資料存有外洩風險。本會建議生產商採用較安全的超文本傳輸安全協定(Hyper Text Transfer Protocol Secure，簡稱HTTPS)，以提高傳送數據時的安全性。(見圖四)



圖三



圖四

應用程式安全性

5款樣本可透過Android應用程式存取裝置檔案

若應用程式內嵌瀏覽器(WebView)，用戶毋須切換應用程式便可直接瀏覽網頁。測試發現，「imou」(#3)、「TP-Link」(#4)、「eufy」(#6)、「EZVIZ」(#8)及「D-Link」(#10)Android版本的應用程式內嵌瀏覽器沒有封鎖存取檔案的權限，駭客可植入程式碼以存取裝置檔案，令用戶私隱外洩。另外，「小米Mi」(#2)、「imou」(#3)、「eufy」(#6)及「D-Link」(#10)iOS版本的應用程式內嵌瀏覽器使用已過時的UIWebView或沒有停用JavaScript，駭客可進行跨網站指令碼攻擊(Cross Site Scripting，簡稱XSS)。本會建議生產商使用WKWebView或SFSafariViewController，並停用JavaScript。

1款樣本的Android應用程式加密方式不安全

「BotsLab」(#5)Android版本的應用程式使用已過時的數據加密標準(Data Encryption Standard，簡稱DES)，金鑰長度較短，只有56位，並非一種安全的加密方法。本會建議生產商使用較安全的進階加密標準(Advanced Encryption Standard，簡稱AES)，金鑰長度不少於128位。

5款樣本的手機應用程式存取過多權限

測試同時檢視了應用程式的Android及iOS版本所要求的權限，發現5款樣本包括「小米Mi」(#2)、「imou」(#3)、「BotsLab」(#5)、「eufy」(#6)及「EZVIZ」(#8)的應用程式存取權限過多，而當中部分樣本存


1


6

家居監控鏡頭測試結果

編號		1	2
牌子		arlo	小米 Mi
產品名稱	[1]	—	智能攝影機2K雲台版
型號	[1]	Pro 4	MJSXJ09CM
大約零售價	[2]	$1,888	$269
總評	[3]	★★★★	★★★½
防攻擊能力	[4]	●●●●●	●●●●●
資料傳送安全性	[4]	●●●●●	●●●●●
應用程式安全性	[4]	●●●●●	●●● gi
儲存資料保密性	[4]	●●● k	●●●● k
硬件設計	[4]	●●●●●	●●● l
樣本資料[1] 影片[5] 最高拍攝解像度		2560x1440	2304x1296
樣本資料[1] 影片[5] 幀率(fps)/編碼		24/H.265	20/H.265
樣本資料[1] 影片錄影功能 儲存錄影	[6]	m	no
樣本資料[1] 影片錄影功能 免費雲端		試用3個月	—
樣本資料[1] 影片錄影功能 付費雲端		■	—
語音控制功能	[7]	pqr	pr
接駁方式	[8]	s	s
適用位置		室內及戶外	室內
內置充電池		■	—
體積(闊x高x深，毫米)		52x89x78.4	78x115x78
保用期(年)		1	1

註
■ 表示該項適用或有該功能。
— 表示該項不適用、沒有該功能或代理商沒有提供資料。
[1] 資料源自產品規格或由代理商提供。
[2] 售價是約數，乃由代理商提供或本會於今年2月在市面調查所得。不同零售商的售價或有差別。
[3] 總評分比重：
防攻擊能力 25%
資料傳送安全性 25%
應用程式安全性 20%
儲存資料保密性 20%
硬件設計 10%
若樣本在防攻擊能力、資料傳送安全性、應用程式安全性或儲存資料保密性等表現不理想，便會啟動限制因素，總評分會受局限。


2


3


4


5


7


8


9


10

	3	4	5	6	7	8	9	10
	imou	TP-Link	BotsLab	eufy	SpotCam	EZVIZ	reolink	D-Link
	Knight Outdoor Smart Security Camera	2K Pan / Tilt Home Security Wi-Fi Camera	Indoor Cam Pan & Tilt	Outdoor Cam Pro	Wire-Free FHD Security Camera	Smart Home Camera C6 2K+	—	2K QHD 無線網路攝影機
	IPC-F88FIP-V2	Tapo C210	P4 Pro	T8441X	Solo 2	CS-C6	Argus 3 Pro	DCS-8350LH
	$1,380	$319	$598	$899	$1,270	$630	$959	$699
	★★★	★★★	★★★	★★★	★★½	★★	★★	★★
	●●●●●	●●●●●	●● a	●● b	●◐ a b	● b c	●◐ a d	● b c
	●●● e	●●● e	●●●●●	●●●●●	●●●●●	●●● e	◐ f	●●● e
	●●● g i	●●●◐ g j	●●●● h i j	●●●◐ g i	●●●●●	●●● g i j	●●●●●	●●●◐ g
	●●●◐ k	●●● k	●●●◐ k	●●●◐ k	●●● k	●●●◐ k	●●◐ k	●●● k
	●●● l	●●● l	●●● l	●●●●●	●●●●●	●●● l	●●● l	●●● l
	3840x2160	2304x1296	2304x1296	2560x1920	1920x1080	2560x1440	2560x1440	2560x1440
	15/H.265	15/H.264	20/H.264+	15/H.265	30/H.264	25/H.265	15/H.265	25/H.265
	no	no	n	no	n	n	n	no
	試用30日7天錄影	—	—	—	1鏡頭雲端儲存7天	試用30日7天錄影	1鏡頭1GB雲端儲存7天	3鏡頭1天錄影
	■	■	■	■	■	■	■	■
	pr	pr	pr	pr	pr	pr	pr	pr
	s	s	s	s	s	st	s	s
	室內及戶外	室內	室內	室內及戶外	室內及戶外	室內	室內及戶外	室內
	—	—	—	—	■	—	■	—
	146x127x156	86.6x117.7x85	79x115.6x79	66x66x58	81.5x81.5x74.1	100x96.5x100	56x90x121	66.7x111.4x65.7
	1	3	1	1	1	1	2	3

[4] a 重新登入帳戶連接鏡頭時，用於上一次連接的對話金鑰仍然有效。
b 登入帳戶或進行實時動態影像串流時，欠缺防禦暴力攻擊的保護。
c 實時動態影像串流的預設密碼為6位數字或字母，密碼強度非常弱。
d 於同一手機的應用程式內登出帳戶或登入另一個帳戶後，仍可看到影像串流。
e 進行實時動態影像串流時，沒有把影片數據進行加密，傳送方式欠缺安全。
f 鏡頭連接Wi-Fi無線網絡時，沒有進行身分驗證，傳送資料時沒有把敏感資料加密。
g 應用程式內嵌瀏覽器沒有封鎖存取檔案的權限、使用已過時的UIWebView及/或沒有停用JavaScript。
h Android版本的應用程式使用已過時的數據加密標準，加密方式不夠安全。
i 手機應用程式存取過多權限。
j 登入應用程式時會彈出訊息顯示帳戶並不存在。
k 於應用程式內儲存資料時欠安全，部分敏感資料儲存於普通文字檔，相隔一段時間後才把資料移除。
l 沒有移除電路板上的除錯埠，把外殼移除及於除錯埠接駁合適的接頭，便可訪問操作系統命令介面。
[5] 以最高解像拍攝影片，樣本每秒可錄製的畫面幀數。
[6] 儲存錄影
m 用戶可付費購買配件Smarthub，影片儲存於USB記憶棒內。
n micro-SD記憶卡
o 網路儲存伺服器(Network Attached Storage)或網路錄影機(Network Video Recorder)
[7] 語音控制功能
p Amazon Alexa
q Apple HomeKit
r Google Assistant
[8] 接駁方式
s Wi-Fi無線網絡
t 乙太網路(Ethernet)

裝 cam 都要小心考慮位置，太私人嘅地方，例如洗手間等，梗會唔會裝啦。

作為現代人，對監控呢啲問題一定要敏感啲。定期改吓密碼、檢查觀看紀錄，同埋部機有冇俾人開過。

我之前都拍過一啲被人監控嘅戲。未來，如果有機會拍吓好似《Panic Room》呢類驚悚電影，咁就太好啦！

取的資料亦較為敏感，例如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，裝置內的敏感資料有機會因而外洩。

用戶安裝及使用監控鏡頭的應用程式前，須留意應用程式要求存取用戶資料的權限，因一旦下載程式及完成安裝，有關權限就會容許程式自動存取相關資料而毋須再經用戶同意，用戶亦無法知悉相關資料會如何及何時被使用。

3 款應用程式的訊息顯示有待改善

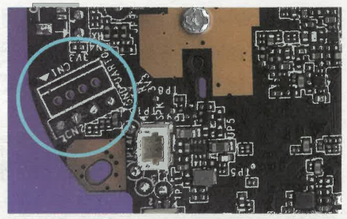
若在「TP-Link」(#4)、「BotsLab」(#5)及「EZVIZ」(#8)的應用程式的登入版面輸入不存在的帳戶，程式會彈出訊息顯示該帳戶並不存在，駭客便可透過不斷嘗試找出真實存在的帳戶名單，設計欠理想。

應用程式儲存資料安全性欠理想

測試發現，全部樣本於應用程式內儲存資料時的安全性不足，包括會將用戶部分敏感資料例如電郵地址、帳戶名稱或密碼等儲存於普通文字檔，而在相隔一段時間後才把資料移除，沒有使用加密技術來保護資料，令駭客或可輕易取得該等用戶資料。本會建議生產商在儲存用戶的敏感資料前，先把資料加密處理，以加強保障用戶的敏感資料的安全性。

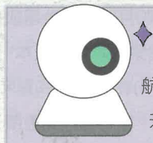
7 款樣本沒有移除除錯埠

為了設計產品及偵測產品的各種漏洞，家用監控鏡頭的電路板大多備有除錯埠（debug port），是次檢測發現，7款樣本包括「小米Mi」(#2)、「imou」(#3)、「TP-Link」(#4)、「BotsLab」(#5)、「EZVIZ」(#8)、「reolink」(#9)及「D-Link」(#10)沒有移除電路板上的除錯埠，用戶只需把監控鏡頭的外殼移除及於除錯埠接駁合適的接頭，便可訪問操作系統命令介面，及進一步讀取監控鏡頭儲存於記憶體的資料或修改軟件。以上7款樣本均存有安全風險。



大部分樣本沒有移除電路板上的除錯埠

安裝監控 家傭有權知



根據香港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》：「人們應被清楚告知他們是受到閉路電視監察」。若用戶於家中安裝監控鏡頭，除了應通知家中每一位成員(包括家傭)外，也應告知所有訪客(包括親友、上門補習老師及上門維修人員等)。用戶亦須考慮監察的範圍和程度，包括是否需要長時期進行監察。

聘請了家傭的消費者應充份理解香港個人資料私隱專員公署發出的《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，當中包括：

- 任意在家中使用攝錄機監察家傭的活動在本質上侵犯了家傭的私隱。
- 應評估進行監察的需要，了解有否其他較不侵犯私隱的替代方法。
- 在考慮過所有因素後仍決定在家居進行攝錄監察的僱主，應考慮監察方式的「合理性」、告知僱員有關監察活動的「公開性」，以及妥善處理攝錄記錄的方法。

合理性是評定在監察僱員的過程中收集個人資料的方法是否公平的一個準則。如因家居情況致有需要透過攝錄機監察家傭的活動，僱主應以公開的方式進行監察，除非有特殊情況支持隱蔽式監察活動。

有關於家中安裝監控鏡頭涉及的個人資料私隱問題，消費者可向香港個人資料私隱專員公署查詢，或瀏覽該公署網頁www.pcpd.org.hk。

教授意見

香港城市大學電子工程系副教授曾劍鋒先生認為本會是次測試的部分家用監控鏡頭樣本的網絡安全問題較大，例如非授權服務器訪問、不安全數據傳輸，不安全數據加密，對消費者構成的可能風險包括隱私洩露、手機數據洩露等。曾教授表示網絡的資訊安全有3個重要元素，包括機密性（confidentiality）、完整性（integrity）及可用性（availability）。機密性指保護資訊免向未經授權人士披露；完整性指保護資訊免受未經授權人士更改；可用性則指讓資訊可供已獲授權人士在需要時取用。由於家用監控鏡頭的產品設計及應用程式均由生產商負責，故只能促請生產商改善產品的網絡安全，而消費者只能倚賴生產商提高產品質素。曾教授指生產商可參考IEEE技術標準2668物聯網裝置的成熟指數，以改善產品的機密性、完整性及可用性。

此外，消費者可善用防火牆（firewall）及漏洞掃瞄（vulnerability scanning）等工具以改善網絡安全，惟該等措施亦未能完全解決網絡安全的漏洞。消費者使用物聯網裝置時，設定的密碼要有足夠的強度，並要小心保管帳戶及密碼，及避免讓別人設定或操控個人的物聯網裝置。

選購及使用貼士

- 消費者不應購買沒有品牌或來歷不明的產品，除了品質沒有保證外，網絡安全未必很完善。
- 消費者於智能裝置的應用程式建立帳戶時，密碼應有足夠強度並定期更改。密碼的長度不應少於8位，並混合大小楷字母、數字及特殊符號來提高密碼強度，以防被駭客輕易破解。
- 若監控鏡頭由專人上門安裝及設置，安裝後應立即更改密碼。
- 消費者在有需要時，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。
- 消費者應善用防火牆、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。
- 消費者應使用個人智能裝置登入鏡頭觀看畫面，不應使用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，以防帳戶資料被暗中記錄及盜取。
- 消費者應不時檢查及更新韌體（firmware），因生產商在產品出廠後會透過韌體改善產品的運作及修補漏洞，使用更安全。
- 若懷疑鏡頭內部系統曾被入侵或植入程式，不妨重刷一次官方韌體及全機還原出廠狀態，重新安裝時亦可建立一個全新帳戶及密碼。