Proposed Code of Practice on Operation and Management of Internet of Things Devices for Public Telecommunications Services

Telecommunications Regulatory Affairs Advisory Committee

28 March 2019

OFCA 通訊事務管理局辦公室
OFFICE OF THE COMMUNICATIONS AUTHORITY

Background

- Internet of Things (IoT) service providers provide wireless connections for their customers to connect IoT devices to the public telecommunications networks using

  - Narrowband-IoT operating in the frequency spectrum assigned for the provision of public mobile services

  - Low-Power Wide Area Network (LPWAN) such as Sigfox or LoRa operating in the 920 – 925 MHz band on a shared and uncoordinated basis

sigfox LoRa™

Regulatory Requirements

- General Condition 5.1 of the Unified Carrier Licence (UCL) and the Wireless IoT (WIoT) Licence
  - The licensee is required to provide a good, efficient and continuous service in a manner satisfactory to the Communications Authority (CA)

- Special Conditions 1.2 of the UCL and the WIoT Licence
  - The CA may issue code of practice or guidelines for the purpose of providing practical guidance to the licensees in respect of the provision of satisfactory service and the protection and promotion of the interests of consumers of telecommunications goods and services.

Need for Proper Operation and Management of IoT Devices

- Characteristics of IoT devices and applications
  - automated machine-to-machine type applications such as lighting control, energy meter management, etc.
  - collect information such as battery status and other environment data for monitoring, surveillance and control purposes

- Advent of 5G and new smart city applications bring challenges for proper data protection and security
  - massive number of IoT devices deployed for a wide range of applications including sophisticated and mission critical applications
  - collection/processing of a vast amount of data using IoT devices

- Need of safeguarding the interests of both businesses and consumers in the IoT era

Article in Choice Magazine – Consumer Tips for Using Smart Devices to Safeguard Privacy

- Understand the product design before purchase
- Check the background of the manufacturer and find out if it has been involved in any deception, theft or other illegal behaviours
- Set a unique password for each device and never divulge the passwords to other people
- Adjust the security and privacy settings to higher levels before using the devices
- Perform regular security update of the software of IoT devices
- Disable functions and turn devices off if they are not in use
- Enquire about the network condition for IoT devices if anything unusual is observed
- Think clearly if the product will bring significant benefits to your daily lives before purchase

• 編者的話 •

智能產品洩漏個人資料風險不容忽視
官商民三方合作提升消費保障

選擇

3月15日是「全球消費者權益日」，今年的主題是「可以信賴的智能產品（Trusted Smart Products）」，響應國際消費者聯會的號召，《選擇》月刊今期發表一份有關智能家居的報告，呼籲消費者留意智能產品或存有洩漏私隱的風險。

科技發展帶來無限可能，以往出現在科幻電影的「未來」家居 — 只要一聲指令便能控制全屋燈光、電器等，甚至有機械管家為人類清潔打掃、烹調餐飲，到了今天已略見雛形，透過物聯網（Internet of Things），我們可以將家居電器與手機互連，即使不在家，亦可用手機操控冷氣機、吸塵機等電器產品，為生活增添舒適。

物聯網把物聯網裝置和設備之間連繫起來，通過收集例如啟用冷氣機前，物聯網裝置可以按當日的天氣狀況、據」，指令冷氣機調整製冷溫度和送風強度。物聯網應用政府落實建設的智能城市，都必須依賴物聯網的技術。

有人甚至把物聯網與人工智能、納米技術、無人車、預期會全面改變企業、商業和消費者的互動方式，改變人多的實時資訊以提高生產效率；也方便政府蒐集和分析數化的設備提升生活質素。

物聯網亦可以將消費者的喜好、舉動能夠無遠地記錄徒入侵，不僅威脅用戶的私隱，更可能造成金錢損失甚或危

這些風險並非危言聳聽。比利時的消費者保障組織「備，包括電子門鎖、監控鏡頭、吸塵機及雪櫃等，兩名網絡星期之後，成功「攻陷」近半數安全系統。測試當中，網絡專用戶設定，並可遙控開啟門鎖；而屋內設有的保安監察及警

隨着智能電話及網絡迅速發展，擁有「智能」連線功能長，按不少測試結果顯示，這些產品的保安水平參差不齊，格和功能，往往會忽略產品的保安性能。

由於這些智能產品經網絡連接多個智能裝置，黑客只便有可能入侵其他裝置，例如個人電腦，甚至是持有大量個歐洲就有黑客透過攻破連接電腦的打印機、家居路由器及傳至不同裝置，首20小時已有65,000部裝置受影響，最終

作為消費者有何自保方法？數碼發展不能逆轉，如因應用層面愈見廣泛的智能手機，不設實際，倒不如切實做更新產品的軟件、設定較複雜的個人密碼並定期更改、將要使用公共網絡進行敏感交易等。

為保障個人資料，所有智能裝置的保安措施應有嚴格人資料，應小心處理以防洩漏之餘，更不應將客戶資料在個私隱監管部門進行的調查顯示，有59%的智能裝置未有法、用途及應用等。企業在這方面的工作仍要加多把勁！

推廣和鼓勵科技發展固然重要，一個良時代並進，例更是不可或缺。政府作為市場的監察者，有需要密切監在現也萬變的數碼消費世界，為消費者提供適當的保障。

安全使用連網產品錦囊

面對危機應以常識來應對防範，購買或使用連網產品應注意以下各項：

- **充份瞭解產品設計**：購買任何須連網才能使用的產品，除要看清製造商提供的產品資料外，不妨上網搜尋與產品相關的第三方評論、文章或媒體報道，以瞭解產品有否被發現牽涉任何安全或私隱問題；瞭解產品是否容許以更改密碼及調整私隱等設置來提高保安；有否定期提供軟件更新以修補安全漏洞等。
- **瞭解製造商的背景**：不要盡信製造商對保護用戶個人私穩政策的聲稱，因為不排除製造商的行為與其說法不一致；有些品牌的產品或許價格較低，但如果製造商過去有牽涉欺詐、盜竊或各種違法行為，其誠信及道德操守便值得懷疑，產品的軟體層面或軟件包含對用戶不利的流氓程式、暗藏後門或間諜程式的可能性相對較高，必須有所警惕，最好先查清楚及瞭解製造商的背景，並只選擇信譽良好、值得信任的製造商的連網產品。
- **設置高強度密碼及須保密**：連網產品出廠預設的密碼通常都可輕易查得以致攻擊者可輕易進入，因此用戶必須替每一裝置及服務設置獨一無二的登入密碼，密碼長度愈長愈好，並應混合大小楷字母、數字和特殊符號來提高強度，密碼當然不應向任何人士透露。
- **設置最高保安及私隱**：不少連網裝置或服務預設最低安全保障，收集顧多用戶的重要個人資料，因此應改動至較高安全及私隱的設置，如果攻擊者入侵了裝置，可能會植入惡意程式，因此宜定期將裝置完全還原重設，以清除任何植入的程式；如果得悉任何安全事件或會影響使用中的裝置，應到生產商的網站或聯絡供應商尋求協助。
- **定期更新軟件**：大部分生產商會發放更新以修補安全漏洞，用戶應查清楚每一裝置檢查更新的方法，然後每月都做更新，如果裝置或程式設有自動更新功能，應將功能開啟，而安裝在智能手機上用於操控裝置的應用程式，同樣要接受更新。
- **關閉不需要的功能**：裝置的很多功能可能在用戶沒有預期和需要下持續監察用戶，為避免這種情況，在不使用相關功能時，不妨將之關閉，包括裝置上的拍攝鏡頭、收音咪及定位追蹤程式等，在完全不使用裝置時，應完全關機。
- **定期檢查網路**：用戶應定期檢查物聯網裝置對應網路的狀況。當發現有異常情況，例如傳輸速度下降或有不明的裝置連結網路時，應盡快向專業網路安全人員求助。
- **衡量必要性及意義**：有些產品要不停更新程式才能運作，有些會頻密地推送通知而增添煩擾，有可能令本來簡單的操作複雜化，也有些連網產品表面上很有趣味性，但實際上只是花巧玩意，買回來用的話，新鮮感過後也許會逐漸覺得可有可無，實用性不高，故不宜輕易受商家軟神影響，應先想清楚產品是否在日常生活上帶來很大幫助才決定購買。

資料由香港警務處提供

Overseas Developments on Best Practices on Operation and Management of IoT Devices (1)

- The “Code of Practice for Consumer IoT Security” of the United Kingdom
  - no default passwords; implement a vulnerability disclosure policy;
  - keep software updated; securely store credentials and security-sensitive data; communicate securely;
  - minimise exposed attack surfaces; ensure software integrity;
  - ensure that personal data is protected;
  - make systems resilient to outages; monitor system telemetry data;
  - make it easy for consumers to delete personal data;
  - make installation and maintenance of devices easy; and
  - validate input data

Overseas Developments on Best Practices on Operation and Management of IoT Devices (2)

- The "GSMA IoT Security Guidelines" issued by the GSM Association
  - IoT Security Guidelines Overview Document;
  - IoT Security Guidelines for IoT Service Ecosystem;
  - IoT Security Guidelines for IoT Endpoint Ecosystem; and
  - IoT Security Guidelines for Network Operators

- General principles of security challenges
  - availability: ensuring stable connectivity between IoT devices and IoT networks and servers;
  - identity: authenticating IoT devices, services and the end-user operating the IoT devices;
  - privacy: reducing the privacy issues associated with the use of IoT devices by end-users; and
  - security: ensuring that system integrity can be verified, tracked, and monitored

The Proposal

- A voluntary Code of Practice (CoP) will be developed on the operation and management of IoT devices connecting to public telecommunications networks of IoT service providers to
  - ensure the provision of satisfactory service by IoT service providers
  - strengthen consumer protection
  - enhance user confidence in using IoT devices connecting to public telecommunications networks
  - serve as a reference for non-telecommunications licensees (such as device manufacturers, vendors, application developers) in formulating requirements and practices regarding the operation and management of IoT devices/services

Views Sought

- Members are welcome to share their views and comments on the proposal

- OFCA will prepare and circulate a draft CoP for comments by IoT service providers before adoption by the CA

Thank You

通訊事務管理局辦公室
OFFICE OF THE COMMUNICATIONS AUTHORITY