國立政治大學商學院 科技管理與智慧財產研究所

碩士學位論文

# AIoT 資訊安全與隱私法律管理

## ——以智慧家庭為例

# AIoT Information Security and Privacy Compliance Management: a Case Study on Smart Home

指導教授:鄭菀瓊 博士

研究生:江 曉 萱 撰

中華民國 一零八 年 七 月



DOI:10.6814/NCCU201900793

# 謝辭

時光匆匆飛逝，一路攻讀至碩士學位之求學過程也即將暫時劃下句點，非常感恩與珍惜這一路走來陪伴的家人、好友與貴人，讓我能夠鑑往知來、往人生夢想不斷前行，並累積成這一篇滿腹熱情的論文，特別銘記與感謝。

本篇論文以智慧家庭、隱私法律為核心，首先感謝指導教授鄭菀瓊老師，當我決定要寫一個創新題材時，給我最多的支持與鼓勵，讓我像小礦工配戴一盞燈，黑暗中摸索、探路總有盞燈引著出口方向。同時也感謝我的論文小夥伴韋廷、薇瑄，每兩週很密集地討論，給我很多方向跟建議。其次，要謝謝我的口試委員，余啟民委員及熊誦梅委員，兩位在口試過程中給我非常精實建議與勉勵。

在撰寫的過程，特別感謝我的貴人兼前輩徐縈瀠副理讓我啟發對於智慧家庭的概念，以及合規管理的實務經驗。此外，感謝常常被我抓來討論的同儕林旻、之涵，尤其是林旻仍在百忙之中特別擔任我的口試小幫手非常感動，感謝昀軒、又祺替我引薦國內重要前輩及指標論著，感謝建宏、明儒、怡伶在訪談之前後提供許多建議與幫忙，感謝虹錦、鈺書、慎敏在我奮鬥的過程中給予不同面向的思考。

最後，感謝政大科智所每位師長、助教和同學，每位老師的教導都是本篇論文堆砌而成之基石，每位同學都是學習過程中不歇的動力。感謝我的父母與家人，我會持續努力「做中學、學中做」，共勉之。

國立政治大學 National Chengchi University



DOI:10.6814/NCCU201900793

# 中文摘要

當大數據、物聯網和人工智慧等技術之發展，帶來人類家庭生活之便利性和改變時，消費者在現今能在家中使用更人性化、便利及貼近需求的創新服務。這些創新開發之家用電器設備音具備物聯網技術，能感知、蒐集、傳送個人資料，搭配人工智慧與大數據分析，即可讓人類過去不想被窺探的個人家庭生活一覽無遺。

緊接在隱私權意識高漲的時代，各國如歐盟、美國及台灣等，已陸續修正個人資料保護相關法制，企業應如何對應潛在的資訊安全和法遵風險也逐漸受到各界重視。然而不可否認的是，在面對企業能夠使用新科技應用消費者之「家庭內部的隱私權及個人資料」比以往更為多元的趨勢下，目前各國並無完整法律能解決可能產生消費者隱私爭議。

本文將從介紹智慧家庭技術及市場現況開始，探討市場參與角色之市場策略，並介紹各國對於隱私權與個人資料保護法的管制現況，探討智慧家庭產生之個人資料爭議案例，進而分析未來應用上潛在個人資料及隱私法律爭議，從中點明業者在智慧家庭中可能面臨的七大法遵、合規風險，並試圖給予智慧家庭市場參與者於制定管理政策之建議。

**關鍵字：**人工智慧、物聯網、智慧家庭、資訊隱私權、個人資料保護法

國立政治大學 National Chengchi University



DOI:10.6814/NCCU201900793

# Abstract

When the development of technologies ,such as Big data, Internet of Things and artificial intelligence, bring convenience and change in human's daily life, consumers nowadays can use innovative products and services that are more user-friendly, convenient and close to their needs at home. These innovatively developed home appliance devices contained IoT technology that can sense, collect, and transmit personal data. Moreover along with artificial intelligence and big data analytics, those companies have ability to give an unobstructed view of the personal family life that humans would not willing to share with the public.

In the era of high awareness of privacy, European Union, the United States, and Taiwan have gradually revised the regulation for personal data protection. The response and management which companies should take to avoid potential information security and compliance risks have gradually gained attention to all perspectives. However, it is undeniable that current legal system and regulation cannot deal with all types of consumer privacy issues due to the variable and diverse characteristic of smart home application.

This article will start with the introduction of smart home technology and market conditions, explore the market strategy of all types of companies, and introduce the current privacy and personal data protection laws. Furthermore, this article will analyze the potential personal data and privacy legal disputes from aggregating the current dispute cases of smart home. Lastly, this article will point out seven legal compliance risks that the industry may encounter in smart home business, and attempt to give compliance management advices for them to develop future policies.

**Keywords：** Artificial Intelligence, Internet of Things, Smart Home, Information Privacy, Data Protection



DOI:10.6814/NCCU201900793

# 目次

**第一章　緒論**.....10

**第一節　研究動機與目的**.....10

**第二節　研究方法**.....12

**第三節　研究範圍與限制**.....13

**第四節　本文架構**.....15

**第二章　智慧家庭技術與應用**.....16

**第一節　智慧家庭定義與背景**.....16

第一項　AIoT 技術.....16

第二項　AIoT 與智慧家庭.....26

**第二節　從市場參與角色看智慧家庭市場概況**.....30

第一項　通訊服務業.....30

第二項　家電廠.....32

第三項　平台廠.....35

**第三節　智慧家庭產業特性分析**.....39

第一項　智慧家庭應用趨勢.....39

第二項　智慧家庭應用差異.....41

**第三章　隱私權與個人資料保護法**.....45

**第一節　資訊隱私權之發展**.....45

第一項　隱私權的起源.....45

第二項　隱私權與個人資料保護.....47

**第二節　歐美個人資料保護規範**.....48

第一項　歐盟.....48

第二項　美國.....59

**第三節　台灣個人資料保護法**.....62

第一項　個人資料定義與分類.....62

第二項　當事人同意與告知義務.....64

第三項　當事人權利與適當安全措施.....65

國立政治大學 National Chengchi University



DOI:10.6814/NCCU201900793

**第四章　智慧家庭應用之消費者隱私爭議 ..... 67**

**第一節　物聯網技術產生的資安風險 ..... 67**
第一項　機密性威脅 ..... 67
第二項　驗證威脅 ..... 69
第三項　近用威脅 ..... 70
第四項　小結 ..... 71

**第二節　智慧家庭應用隱私爭議案例 ..... 73**
第一項　智慧電錶案：Naperville Smart Meter Awareness v. City of Naperville 73
第二項　智慧電視案：In Re: Vizio, Inc., Consumer Privacy Litigation ..... 78
第三項　智慧音箱爭議：Amazon Alexa ..... 86
第四項　小結 ..... 93

**第三節　智慧家庭潛在之隱私爭議 ..... 95**
第一項　蒐集之資料特性與類型 ..... 95
第二項　受規範主體之定位 ..... 101
第三項　資料處理分析之影響與挑戰 ..... 103
第四項　告知義務範圍模糊化 ..... 108
第五項　當事人同意機制不確定性 ..... 110
第六項　企業合法利益與當事人資料自主權之衝突 ..... 112
第七項　平台整合與資訊串聯潛在之風險 ..... 113

**第五章　給予智慧家庭市場參與業者之建議 ..... 117**

**第一節　三大管理策略 ..... 117**
第一項　消費者體驗與個人資料保護程度之衡量 ..... 117
第二項　取最嚴格標準設定管理政策 ..... 119
第三項　以資料運用過程三階段為責任分擔界線 ..... 120

**第二節　對家電業者建議 ..... 122**
第一項　告知義務與當事人同意 ..... 122
第二項　盡可能採取數值蒐集模式並設定內部存取權限 ..... 122
第三項　當事人權利行使和企業揭露範圍 ..... 123

**第三節　對通訊服務業者建議 ..... 124**
第一項　以資料控制者定位進行資料處理 ..... 124
第二項　資料傳輸標準之抉擇 ..... 124

**第四節　對平台業者建議 ..... 126**
第一項　資料共享之限制 ..... 126



DOI:10.6814/NCCU201900793

第二項　行業慣例之去識別化手段.....126
第三項　平台策略與當事人權利行使.....127

**第六章　　結論.....129**

**參考文獻.....130**

**附件一 訪談紀錄.....137**

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

# 表次

表 1 市場參與角色蒐集之資料類型 ..... 97
表 2 市場參與角色的定位 ..... 102
表 3 市場參與角色之資料剖析面向 ..... 107

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

# 圖次

圖 1 資料特性與識別程度分析圖.....100
圖 2 市場參與角色之資料剖析風險圖.....107
圖 3 設定管理政策之標準要點.....119
圖 4 三階段界線與業者首要任務.....120

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

# 第一章　緒論

## 第一節　研究動機與目的

大數據、物聯網和人工智慧等技術之發展，帶來人類生活之便利性，也對個人及社會帶來劇烈的改變。從 2019 國際消費性電子展( Consumer Electronics Show，CES）來看「2019 年關鍵字」顯示，人工智慧是貫穿整年熱門議題，並主宰著消費性產品與服務的走向[1]。

過去，「家」是一個人生活之中心及不想被打擾、被窺探的避風港，因為在家中一個人能夠輕鬆展現最真實的自我及內在需求，因此美國法亦發展出「家即為城堡」( My home is my castle）的至理名言，對於家庭內部之資訊賦予憲法上隱私權的保護。然而在現今，智慧家庭（Smart Home）也因大數據、物聯網和人工智慧等技術之應用，不僅逐漸實踐與誕生，也翻轉傳統上人類對於家庭的概念。當個人智慧終端設備能發展成智慧家庭設備時，消費者能在家中使用更人性化、便利及貼近需求的創新服務，但這些設備的進入也將帶來個人隱私權安全問題。這些家用電器設備透過物聯網技術，具備有感知、蒐集、傳送個人資料的能力，而搭配著人工智慧與大數據分析，過去不想被窺探的個人生活將暴露在公眾之下。

在隱私權意識高漲的此刻，面對不斷修正的歐盟、美國及台灣的個人資料保護法制，企業對於相應的潛在的資訊安全和法遵風險也逐漸重視。然而面對新科技對於「家庭內部的隱私權及個人資料」應用比以往更為多元，目前各國並無完整法律能解決可能產生消費者隱私爭議。當智慧家庭市場參與者所蒐集之能源使用資料能隱含並推導出「自然人的健康資料」時，蒐集範圍屬於特殊性個人資料（敏感性個人資料），抑或一般性個人資料？當未預期之資料蒐集或分析得出之結果，不屬於原始告知義務中個人資料類別時，企業所取得之當事人同意效力為

[1] Foxbussiness 網站，https://www.foxbusiness.com/technology/ces-2019-5-things-to-watch-at-techs-biggest-convention，（最後瀏覽日：2019/6/25）。



DOI:10.6814/NCCU201900793

何？當智慧家庭應用平台所參與之企業不斷擴增時，其面臨的資訊安全和法遵風險及責任應如何分擔？由此可知，不僅是法律必須正視智慧家庭應用所造成隱私權影響與結果多元化且無法預測的問題，智慧家庭的業者面臨創新開發之挑戰，也必須制定相應管理措施。

基於此，本文欲從智慧家庭之技術、市場應用模式開始，討論智慧家庭市場參與角色在營運策略上的特性，而後介紹各國對於隱私權與個人資料保護法的管制現況，探討智慧家庭產生之個人資料爭議案例，進而分析未來應用上潛在個人資料及隱私法律爭議，最後提供具體管理建議，予台灣司法實務及智慧家庭業者參考。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

## 第二節　研究方法

本文採取之研究方法以案例探討、質性研究為主，文獻回顧為輔，試圖歸納未來應用上潛在個人資料及隱私法律爭議，並給予企業管理建議，具體如下：

在案例探討部分，選擇三方市場參與業者通訊服務業、家電業者及平台業者之代表案例，探討其產生之消費者個人資料及隱私法律問題，觀察司法實務對於產業趨勢如何適應既有法治規範，並輔以歐盟、美國及台灣個人資料保護法規，綜合分析潛在消費者隱私爭議與法遵風險。

在質性研究部分，本文將以訪談之方式，邀請台灣於智慧家庭工作多年之開發業者進行直接對話，觀察業者於智慧家庭開發過程之處理及應用、市場現況，並瞭解智慧家庭業者面對創新開發過程時，可能面臨的個人資料及法律議題。

在文獻回顧部分，鑑於台灣於智慧家庭之隱私、個人資料法律問題非常少見，本文將研讀與歸納歐盟、美國及台灣對於智慧家庭技術、應用、個人資料保護法制相關之研究報告、期刊論文，整理出歐盟、美國及台灣針對智慧家庭應用存在之個人資料保護法令要求及責任，試圖找出統一且廣泛之標準，提供司法實務及智慧家庭業者參考。

國立政治大學 National Chengchi University



DOI:10.6814/NCCU201900793

## 第三節　研究範圍與限制

為能充分探索大數據、物聯網和人工智慧發展在未來應用上產生之隱私法問題，本文以智慧家庭為研究核心，聚焦在「科技」、「商業模式」、「法律」三方面進行研讀，並分析三者之考量與衝突，以及未來智慧家庭市場參與者與司法實務應如何調和，其具體研究範圍如下：

一、就科技技術方面，本文聚焦在智慧家庭應用上之相關技術，並特別圍繞在市場參與者將產品及服務安置於消費者家中後，針對消費者資訊或個人資料傳輸並儲存至企業內部過程中，以「蒐集、處理、利用」中所涉及之為主技術。

二、就商業模式方面，根據台灣經濟部工業局智慧電子產業計畫推動辦公室所提供之智慧家庭市場規模報告顯示，目前智慧市場上發展趨勢以美國、亞洲及歐盟為主要之核心區域[2]。因此本文智慧家庭商業模式之研究，以美國、歐盟及亞洲三者作為研究範圍，亞洲部分以在台灣積極發展之企業中華電信、LG 為代表，按其在市場上所扮演之角色，亦即所提供之服務，區分為通訊服務業、家電業及平台業三種進行交互分析。此外，在涉及之智慧家庭服務當中，本文以「能源管理」、「安全監控」、「休閒娛樂」及「家用電器」四大領域為研究範圍，排除智慧醫療方面之探討。

三、就隱私法律方面，鑑於產業分析之範圍為美國、歐盟及亞洲，且具體企業個案以美國、歐盟及台灣為主，故就資訊隱私權及個人資料保護法律之研讀方向遵循體企業個案所在之國家，聚焦在美國、歐盟及台灣之規範。就消費者隱私爭議案例限於目前美國、歐盟及台灣於司法實務上爭訟案例甚微，以目前較為新穎、具體之美國三個案例，進行深入分析與

[2] 經濟部工業局智慧電子產業計畫推動辦公室網站，https://www.sipo.org.tw/industry-overview/industry-status-quo/smart-home-industry-status-quo.html（最後瀏覽日：2019/6/26）。



DOI:10.6814/NCCU201900793

討論，將輔以歐盟及台灣之規定，綜合討論企業可能在三方司法管轄範圍內面臨的難題。此外，本文因特別著重在個人資料保護法方面，故亦排除資訊安全管理法之討論。

四、就質性訪談方面，本文訪談之企業為台灣致力於從事智慧家庭開發之業者，訪談之對象為進行產品及服務創新、業務開發之人員，藉以補足本文對於實際智慧家庭市場現況之觀察，並瞭解具體資訊流通及服務之過程。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

## 第四節　本文架構

本文將以智慧家庭為中心，討論人工智慧與物聯網在資訊安全與隱私法律管理方面之建議，共六個章節：

第一章為緒論，講述本文研究動機與目的、研究方法、研究範圍與限制及本文架構，介紹本文研究之願景與方向。第二章為智慧家庭技術與應用，講述人工智慧與物聯網（AIoT）技術、智慧家庭定義，並從市場參與角色層面，觀察智慧家庭市場現況，進而提出產業特性分析，包含應用趨勢及差異。

第三章為隱私權與個人資料保護法之法制介紹，將從資訊隱私權發展歷程開始，並聚焦在歐盟、美國及台灣在個人資料保護法及相關人工智慧規定，整理出可能對智慧家庭創新應用產生影響之具體規範。

第四章為目前、潛在智慧家庭應用之消費者隱私爭議，首先討論在智慧家庭資料蒐集及傳輸過程中，最常面臨到的三種威脅，包含機密性威脅、驗證威脅及接近使用威脅，進而分析潛在的風險。再者，本文將於本章第二節所討論的智慧型電錶、智慧電視及智慧音箱等案例，最後本章第三節從第二章討論的產品與服務模式切入，以現行法及訪談業者的角度觀之，分析其在智慧家庭應用中個人資料之蒐集、處理及利用階段，可能產生的爭議與問題。

第五章聚焦在給予智慧家庭市場參與業者之建議，將從智慧家庭市場參與者於制定管理政策時應如何進行衡量開始，並針對通訊服務業者、家電業者及平台業者三方給予策略上之具體管理建議。第六章為結論，統整本文之各章節，貫穿本文之中心思想，點出智慧家庭業者應遵循之方向。



DOI:10.6814/NCCU201900793

# 第二章　智慧家庭技術與應用

## 第一節　智慧家庭定義與背景

### 第一項 AIoT 技術

#### 第一款　物聯網（Internet of Things）

物聯網（Internet of Things，IoT），是指於實體或物品之中，如手機、車輛、家用電器等，安裝嵌入式感測器和應用程式開發介面（Application Programming Interface，API）等設備，並透過網際網路達成訊息連結目的，所形成之交換網路[3]。從歷史脈絡切入，「物聯網」一詞，最早係於 1985 年在美國聯邦通訊委員會（Federal Communications Commission，FCC）無線應用會議演講中，由 Peter Lewis 提出的網路趨勢概念，當時他針對網路的未來趨勢應走向「由人員、流程、連接設備和傳感器技術的整合，使這些設備的可以被遠程監控、操作和趨勢評估」[4]。其後於 1999 年，Kevin Ashton 更加明確定義出「Internet of Things」一詞[5]。自 2003 年起，物聯網廣泛出現於報章雜誌之中[6]，其中最重要的探討係由國際電信聯盟(International Telecommunication Union，ITU)於 2005 年，點出物聯網、相關技術細節、其對全球市場機會與挑戰，及對個人生活的影響[7]。

---

[3] SAP 網站， https://www.sap.com/taiwan/trends/internet-of-things.html（最後瀏覽日：2019/3/18）。

[4] 鄭福炯、王岱鑫、劉威成（2017），〈智慧物聯網系統平台－以智慧家庭為例〉，《電腦稽核期刊》，第 35 期，頁 38。

[5] Kevin Ashton, THAT 'INTERNET OF THINGS' THING, http://www.rfidjournal.com/articles/view?4986 (last visited Jun 17, 2019); Cf. Chinese translation reference to Wikipedia, https://zh.wikipedia.org/wiki/物联网_-cite_note-The_Internet_of_Things:_A_survey-3 (last visted June 17, 2019）.

[6] 周碩彥，〈「物聯網發展趨勢展示內容」研究報告〉，https://www.naer.edu.tw/ezfiles/0/1000/attach/95/pta_9695_1581881_06359.pdf，頁 2。

[7] 葉志良（2018），〈因應物聯網發展資料保護法制的革新──歐盟法制的發展與啟示〉，《中原財



DOI:10.6814/NCCU201900793

第一目　物聯網技術、功能及特性

從技術及功能層面切入，物聯網乃基於無線電訊、網際網路等設備，從而迅速發展之技術，其透過自動化位置標示，例如無線射頻辨識（Radio Frequency Identification，RFID）標籤、微型聯網電子系統（Microelectromechanical System）、或其他嵌入式感測器等，使物體能夠相互交換訊息、執行動作，以達成「人員集中管理、控制」的共同目標[8]。因此物聯網的技術核心價值，在於「串聯物體」與「資訊蒐集與反饋」等兩大功能。

物聯網系統（IoT System）大致上包含有五個主要關鍵技術，分別是（1）無線射頻辨識（2）無線傳感器網絡（3）中介軟體（4）雲端運算以及（5）IoT 應用軟體[9]。其中無線傳感器網絡（Wireless Sensor Network，WSN）技術，是將一系列空間分散的感知元件通過其架構之無線網絡進行連接，從而將各自物體中所蒐集到的資訊，通過無線網絡進行傳輸匯合[10]。因此，該傳輸技術乃貫穿物聯網之架構，同時具備計算、通信、傳感器三項技能，是物聯網運作之核心[11]。上開五大關鍵技術，亦可區分為三個系統層級[12]：

一、感知層

感知層，亦即物聯網終端設備（IoT end devices）[13]，其運用嵌入式感測器等半導體感知元件，偵測溫度、濕度、影像、聲音、位置、壓力、速度、光線等資訊[14]。在半導體感知元件上，需具備以下特性：（1）感應器低電化及節電化（2）智慧化及準確度（3）晶片組小型化（4）能與無線感應器網路的感應器連接[15]。

---

經法學》，第 40 期，頁 64。

[8] Luigi Atzori, Antonio Iera & Giacomo Morabito, *The Internet of Things: A survey*, 54 Computer Networks 2787, 2787 (2010).

[9] 同註 6。

[10] Offweek 物聯網站，https://iot.ofweek.com/2017-03/ART-132202-11000-30118661.html（最後瀏覽日：2019/3/18）。

[11] 同前註。

[12] 王文娟（2016），〈物聯網概念及應用〉，《經濟前瞻期刊》，第 168 期，頁 31。

[13] 同註 4。

[14] 同註 12。

[15] 同註 6，頁 23。



DOI:10.6814/NCCU201900793

二、網路層

網路層，亦即物聯網閘道器（IoT gateway）[16]，係利用無線及固網設備，將蒐集到之資訊傳輸上載至雲端平台[17]。此層級最重要在於該如何選擇適性的通訊傳輸技術，目前較為常見通訊傳輸技術如藍芽、ZigBee、WiFi 等[18]。

在考量架設何種傳輸技術時，須考量傳輸之需求，大多的廠商在選擇時，不外乎考量該數據須具備（1）低成本（2）高密度（3）範圍大（4）運作時間長等特性[19]，但由於魚跟熊掌不可兼得乃常態，因此廠商實際上會根據傳輸距離之不同，採用不同設備：在短程距離，通常會採用 ZigBee 無線通訊；中程距離，通常會採用 WLAN；長城距離，則會選擇 WiFi 或 4G 等無線通訊技術[20]。

在智慧家庭之應用，同樣須考量到智慧家庭之耗能率低、相容性及市場可接受度等要求。因此，在家庭自動化設備及智慧型大樓建置上，目前多數研發廠商係以 IEEE 802.15.4 低速率無線個人區域網路（Low-Rate Wireless Personal Area Network，LR-WPAN）結合 ZigBee 無線標準為基礎的發展[21]，作為無線感測網路的基礎通訊協定。

三、應用層

應用層，亦即雲端平台等[22]，通常會存放於網路雲端平台（例如 Amazon 的 AWS[23]）或實體儲存空間，透過雲端運算技術將蒐集資料進行大數據分析，以分析並掌握設備運作情形及使用者習慣。根據分析之結果，得進行設備最適化（optimization）及自動化（automation）的調整等[24]，以提高使用效率、改善客戶

---

[16] 同註 4。
[17] 同註 12。
[18] 同前註。
[19] 同註 10。
[20] Digitimes 網站，https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000293659_ymv5w76t6lv2gy85axfe0，最後瀏覽日：2019/3/18。
[21] 李俊賢（2016），〈無線感測網路與 ZigBee 協定簡介〉，http://www.ecaa.ntu.edu.tw/weifang/WSN/WSN_ZigBee intro.pdf，頁 3。
[22] 同註 4。
[23] Amazon AWS 網站，https://aws.amazon.com/tw/（最後瀏覽日：2019/3/18）。
[24] 同註 12。



DOI:10.6814/NCCU201900793

體驗，或開發新應用軟體。因此，此層級主要重視雲端計算的能力，例如應包含處理器高速化、分散處理等特性[25]。

第二目　物聯網技術標準化與整合

在三個階層當中，為了使物體與物體間，能夠實現串連與資訊反饋的目標，物聯網服務之業者在網路層採用何種「通訊技術」的議題上逐步達到一致性，在應用層上透過彼此間以開放技術方式，吸引更多合作夥伴並達到資源整合效果。以下以智慧家庭應用領域中，廠商多數採用之技術標準作為討論：

一、IPSO 通訊標準

IPSO（IP for smart objects）聯盟[26]，為一非營利組織，其成員包括全球多家通訊和能源技術公司，如 Cisco、Ericsson、Intel 等，旨在推動 IP 協議作為網路連結技術用於感測器節點或者其他的智慧物體，以利於資訊傳輸[27]。該機構之目標，係在瞭解智慧家庭行業及市場後，通過 IP 協議草擬、白皮書發佈、案例研究、標準提升等方法，推動 IP 協議在智慧家庭中的應用及其相關產品及服務的市場行銷。在組織內部之各成員得透過互相操作測試，達成其生產之智慧家庭相關產品和服務共同運行之目的，並滿足相關行業的通訊標準[28]。

二、TaiSEIA 101 通訊標準

智慧家庭物聯網主從通訊架構標準（TaiSEIA 101），前身為 SAANet 通訊標準（Smart Appliance Alliance Network），SAANet 通訊標準最早係於 2002 年由

[25] 同註 12，頁 32。
[26] OMA SpecWorks 網站，https://www.omaspecworks.org/develop-with-oma-specworks/ipso-smart-objects/（最後瀏覽日：2019/3/18）。
[27] 同註 4，頁 41。
[28] 上海情報服務平台網站，http://www.libnet.sh.cn:82/gate/big5/www.istis.sh.cn/list/list.aspx?id=6575（最後瀏覽日：2019/3/18）。



DOI:10.6814/NCCU201900793

工研院綠能所（當時稱為能資所）主導，聯合大同、台灣松下、東元電機、聲寶、歌林、台灣日立及宏柏等家電廠商共同成立「智慧家電產業研發聯盟」（Smart Appliance Alliance，SAA），為使國內發展智慧家電產品順利，所發起並草擬第一版智慧家電監控應用層通訊協定[29]。後續經歷台灣智慧能源產業協會成立及國家經濟部標準局之重視後，更名為智慧家庭物聯網主從通訊架構標準，主要定義出整個智慧家庭物聯網主從通訊之架構，界定智慧家電監控應用層通訊協定、智慧家電產品、網路通訊轉接器產品及家庭閘道器產品等標準[30]，可望帶動提供家庭自動化、家庭能源管理、居家保全、居家照護等，國內智慧家電、智慧型裝置、家庭網路通訊及雲端應用服務之產業[31]。

第二款　人工智慧（Artificial Intelligence）

人工智慧（Artificial Intelligence，AI），係指由人類製造，具有演繹、推理與解決問題能力的智慧主體[32]。從歷史脈絡切入，人工智慧的發展可分為三個階段[33]，分述如下：

第一次的熱潮最早源於 1956 年，是由 John McCarthy 在達特矛斯會議（Dartmouth Conference）上所提出的概念[34]，他認為：「人工智慧就是要使機器的行為，如同是人所表現出的智慧行為一樣。但我們仍無法給出具體的定義，因為我們還無法對於人工智慧之特徵進行描述，亦尚未決定什麼樣的電腦程式稱之為智慧、智能[35]。」舉例而言，當時候最有名的便是「ELIZA」電腦，ELIZA 是

[29] 台灣智慧能源產業協會網站，http://www.taiseia.org.tw/News/news_more?id=15（最後瀏覽日：2019/3/18）。
[30] 同前註。
[31] 同前註。
[32] 維基百科網站，https://zh.wikipedia.org/wiki/%E4%BA%BA%E5%B7%A5%E6%99%BA%E8%83%BD（最後瀏覽日：2019/3/25）。
[33] 大西可奈子（著），許郁文（譯）（2018），《超圖解！〈認識〉AI 人工智慧的第一本書》，頁 26-27，台北：碁峰。
[34] 同註 32。
[35] Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies,*



DOI:10.6814/NCCU201900793

一台能以文字對話的電腦，其作法是透過簡單的模式比對，來完成對話[36]。惟該階段之 AI 技術受限於電腦記憶體容量與處理器處理速度，電腦只能探討找出輸入值跟輸出值的關聯，也就是針對特定問題搜尋出推論的答案，因此僅能做出簡單回覆指令或動作，能完成的事務有限，無法解決實際問題、對生活提供助益[37]。

第二次的熱潮，從 1980 年代開始，人工智慧模型發展至「專家系統」，專家系統是為了某些專業領域所設計的系統[38]，它的方法主要是將大量專業知識輸入電腦中，電腦根據問題對應資料庫中的內容，並判斷答案，能實際解決部份問題[39]。但它的缺點也在於專業知識是無窮無盡的，當電腦遇到資料庫內沒有建檔的事項時，它無法自己判斷或分類「未知的事項」，因此使用的範圍大為受限[40]。

第三次的熱潮，從 2000 年左右開始蓬勃，這個時期的人工智慧模型圍繞在「人工神經網路」（Artificial Neural Network，ANN），這個模型又稱為「類神經網路」，是一種模仿生物神經網路的結構和功能所產生的數學模型，用於對函式進行評估或近似運算[41]。這個模型其實自 1940 年代就開始有研究，但一直至 1986 年，Geoffrey Hinton 提出類神經網路倒傳遞法（Back-propagation Network，BPN）[42]，才確實加快了類神經網路的學習速度[43]，進而將整個模型發展至我們現

---

*and Strategies*, 29 Harv. J.L. & Tech. 353, 359-60 (2016).

[36] 維基百科網站，https://en.wikipedia.org/wiki/ELIZA（最後瀏覽日：2019/3/25）。

[37] Mora Chen（2018），〈人工智慧大歷史〉，https://medium.com/@suipichen/ffe46a350543（最後瀏覽日：2019/3/25）。

[38] 同註 33，頁 30。

[39] 科學月刊網站，http://scimonth.blogspot.com/2018/03/blog-post_56.html（最後瀏覽日：2019/3/28）。

[40] 同前註。

[41] 同前註。

[42] 類神經網路倒傳遞法，又可稱之為「誤差倒傳遞演算法」，利用目標輸出值（Desired Output）與實際輸出值（Actual Output）之間差異，由設計者定義出誤差函數（Error Function）並利用陡坡漸降法（Gradient Steepest Decent）將誤差最小化的方法。王瑞文（2000），《實體模擬技術運用於撥弦樂器，滑音處理與古琴輸入法之人機介面研究》，頁 15，中華大學資訊工程學系碩士論文。

[43] 大和有話說網站，https://dahetalk.com/2018/04/08/%E5%AE%8C%E6%95%B4%E8%A7%A3%E6%9E%90ai%E4%BA%BA%E5%B7%A5%E6%99%BA%E6%85%A7%EF%BC%9A3%E5%A4%A7%E6%B5%AA%E6%BD%AE%EF%BC%8B3%E5%A4%A7%E6%8A%80%E8%A1%93%EF%BC%8B3%E5%A4%A7%E6%87%89%E7%94%A8%EF%BD%9C/（最後瀏覽日：2019/3/25）。



DOI:10.6814/NCCU201900793

今耳熟能詳的機器學習的時代。在這個階段，人工智慧電腦已具有自我決策及預測結果的功能[44]。舉例來說，在 1997 年時，IBM 的深藍電腦已在西洋棋上打敗人類選手[45]，因此整個技術在 2000 年之後，從技術層面研究轉而進入應用層面的研究。

第三階段熱潮，其更近一步發展係在 2006 年，Geoffrey Hinton 他又推出開發出自動編碼器（Autoencoder）的手法，結合既有的類神經網路倒傳遞法，提高多層類神經網路的學習精準度[46]，發展至深度學習的時代，此時電腦已能瞭解各項人事物之特徵，並自建其中規則，並作出自我判斷。

第一目　人工智慧技術、功能及特性

從技術及功能層面切入，現今大多學者採用，由 Stuart Russell 和 Peter Norvig 在《人工智慧：一本現代理論》一書中，所提倡的八種人工智慧定義，並將其分成四個面向：人性思考（thinking humanly）、人性行動（acting humanly）、理性思考（thinking rationally）及理性行動（acting rationally）[47]。因此，廣義的人工智慧，包含專家系統、大數據運用、高度運算技術、機器學習及深度學習等技術在內，只要具有思考推理及解決問題的能力均屬之[48]。惟本文著重在智慧家庭應用方面的人工智慧技術，因此著重介紹「機器學習」及「深度學習」等技術，按者技術是屬於演繹及解決問題能力上層度較高，且本質更能達到推理、自主學習、提出解決方法及實踐，並能帶來人類生活上便利的智慧模型。

---

[44] ARTIFICIAL INTELLIGENCE AND PRIVACY, ARTIFICIAL INTELLIGENCE AND PRIVACY 1–30 (2018), https://www.Datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf (last visited Jun 17, 2019).
[45] Scherer, *supra* note 35, at 360.
[46] 同註 43。
[47] Scherer, *supra* note 35, at 360.
[48] 林勤富、劉漢威（2018），〈人工智慧法律議題初探〉，《月旦法學雜誌》，總號 274 期，頁 3。



DOI:10.6814/NCCU201900793

一、機器學習

機器學習（Machine Learning），意指一組運用電腦，透過累積數據，並運用所創建之數學算法，使其得以「思考」的技術及工具[49]，根據不同的訓練方式可區分為以下三種：

1. 監督式學習（supervised learning）：監督學習是使用人為方式，透過人主動去標記數據的特徵值，訓練模型（也就是電腦）記憶並認知該經過標記數據之特徵值[50]。
2. 非監督式學習（un-supervised learning）：在非監督式學習中，係使用尚未經人為預先標記的數據，使模型自主對該數據進行分組，最後經人為確認該分類是否正確，若為正確再補上分類中的特徵值[51]。
3. 半監督式學習（semi-supervised learning）：與監督式學習類似，僅係降低事前須經標記之數據，用來訓練之數據將會區分為兩部分，其中 80％的數據用於訓練模型，餘 20％用於驗證模型處理未知數據的精準度[52]。如果驗證的結果並非當初標記之意義，則須主動調整模型，可能是調整隱藏層或權重，直到結果近乎一致。
4. 增強式學習（reinforcement learning）：類似非監督式學習的一種，讓模型自主透過觀察來學習以達目標，並根據環境反饋逐步修正答案，最後做出判斷[53]。例如自駕車學習到開車中的一些注意事項，但會根據實際路況，逐步修正該如何前行[54]。

二、深度學習

---

[49] 同註 44，頁 6。
[50] 同註 39。
[51] 同註 44，頁 9。
[52] 同註 39。
[53] 裴有恆、陳玟綺（2018），《AIoT 人工智慧在物聯網的應用與商機》，頁 A-2，台北：碁峰。
[54] 同註 39。



DOI:10.6814/NCCU201900793

深度學習（Deep Learning），係屬於非監督式學習的一種，建立在深度神經網絡（Deep Neural Networks，DNNs）這個與大腦神經網絡具相同原理技術上，該技術結合自動編碼器與類神經網路倒傳遞法，作法上是基於一組已知的數據分類，並運用這些已知數據使其得自主學習算法，進而執行任務[55]。

三、小結

在人工智慧的領域上，基本上就是希望機器能做到「學習」跟「預測」的功能，過程可依序為：（1）需投入大量的數據，讓電腦進行記憶；（2）去訓練電腦「分析」資料，也就是分類、歸納資料並找出規則的能力；（3）再透過新的資料驗證規則是否正確，形成新的「經驗」；（4）最後就能達到預測的效果。預測出的結果可用來直接應用在某些領域，或是可以延伸進行其他分析和研究，目前包含提供影像辨識、文字辨識及消費者行為分析都是非常仰賴人工智慧技術，進而發展而成。

第二目　應用於智慧家庭之人工智慧技術

一、影像辨識技術

影像辨識技術，係指圖形辨識技術之一環，科學家通常是共同使用「MNIST 資料庫（Modified National Institute of Standards and Technology）」，始能開發出更好的演算法[56]。以手寫辨識為例，在 MNIST 資料庫中的每個圖形可分為 784 個維度（28x28 個色塊），可標示上 0-255 個色階，透過隱藏層設定、權重調整，最後得出之輸出層，使電腦得以辨識該圖形的樣式，完成找出特徵值之訓練[57]。舉另一個具體例子，假設我們裝置一台數位攝影

[55] Norwegian Data protection authority, *Artificial intelligence and privacy*, 3(2018), https://www.Datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.
[56] 同註 39。
[57] 同前註。



DOI:10.6814/NCCU201900793

機在家門口，在該攝影機拍攝到影像資料後，其應具備得自動判別門口站立的個人是家庭成員、其他人還是陌生人之功能[58]，至於其是如何判斷？具體而言是運用影像分析，找出該個人之特徵值，進而提供之反饋。

二、語音辨識技術

語音辨識技術，乃自然語言處理（Natural language processing，NLP），目標在於讓電腦能理解並運用人類語言，過程可分為斷詞、理解詞，而後再進行斷句、理解語法（Syntactic Analysis）跟句意（Semantic Analysis）之自動解析[59]，例如，透過麥克風蒐集之語調、音量與頻率，可以分析出說話人的情緒；並可將相應的內容轉化成文字[60]。

三、解析應用情境

人工智慧的技術可運用在大數據分析領域，前二者影像及語音辨識技術著重在於消費者端，能與消費者直接聯繫、反饋之階段。在後端通常進行消費者行為分析，藉以提供符合消費者需求之服務，是目前最大趨勢[61]。例如，中華電信與遠東醫療科技聯手打造之健康雲，就是透過設立於家中之智慧醫療裝置，可自動上傳血糖/血壓之資料，服務商將蒐集來的資料運用人工智慧分析，發現病人可以產生的疾病機率與程度，最後按照相應時程推薦他去看醫生，或自動將資料傳給相應的醫療院所[62]。

[58] 同註 53，頁 1-5。
[59] 研之有物網站，http://research.sinica.edu.tw/nlp-natural-language-processing-chinese-knowledge-information/（最後瀏覽日：2019/4/1）。
[60] 同註 58。
[61] 同註 53，頁 1-4。
[62] 遠東醫療科技網站，http://www.femet.com.tw/product_1015884.html（最後瀏覽日：2019/4/1）。



DOI:10.6814/NCCU201900793

## 第二項 AIoT 與智慧家庭

### 第一款　AIoT 定義

AIoT（Artificial Intelligence of Things），其實就是人工智慧（AI）與物聯網（IoT）的結合[63]，他是智慧物聯連接到智慧應用之趨勢[64]。就智慧應用方面，就是在應用層運用機器學習技術，進行消費者行為模式分析，反饋於產品硬體改良，如預防性的維修或維護；或更進一步提供其他服務，如自駕車、智慧商店、智慧製造及智慧家庭等發展[65]。就 AIoT 的分析，大抵上可區分為兩種：

一、雲端運算

雲端運算（Cloud Computing），係指一種仰賴網際網路的運算方法，其透過網路與其他終端裝置共用的軟、硬體資源和數據資料，並按得按需求提供相應服務[66]。目前許多大廠如 Google 提供 AWS 雲端運算服務、IBM 提供 Cloud 運算服務，及 Nvidia 亦提供加速運算服務[67]。

二、邊際運算

邊際運算（Edge Computing），是指是一種分散式的運算架構，將應用程式、數據資料與服務的分析，由網路中心節點（如中央伺服器），移往邊緣節點（如硬體商品）來處理[68]。簡單來說，其就是就近在物聯網裝置上，執行機器學習運

---

[63] 同註 53，頁 1-1。
[64] 陳計策、賴宛靖（2018），〈迎接 AIoT 智慧時代〉，《工業技術與資訊月刊》，第 315 期，頁 18-19。
[65] 同前註。
[66] 維基百科，https://zh.wikipedia.org/wiki/%E9%9B%B2%E7%AB%AF%E9%81%8B%E7%AE%97，（最後瀏覽日：2019/4/1）。
[67] Nvidia 網站， https://www.nvidia.com.tw/object/gpu-cloud-computing-tw.html（最後瀏覽日：2019/4/1）。
[68] 同註 66。



DOI:10.6814/NCCU201900793

算的工作，並能快速、直接套用物聯網感測器所串流資料[69]。部分業者採用這種模式，認為可以更快速使運算跟決策反饋於消費者身上，此等應用目前在自駕車直接判讀道路情形，自動化進行車輛調整上具有很大功效[70]。

舉例而言，如美國洛克威爾自動化公司（Rockwell Automation）曾使用 AIoT 技術，來檢測工廠內是否有異常的設備，並加快異常情況的預警處理[71]。該公司的做法，是透過在輸送管線旁架設數位攝影機，來觀測異常情形，過去若想要進行人工智慧分析來偵測異常情況，必須先將所有影像上傳至雲端，分析完畢後再傳輸到指定終端，然而這麼一來公司就必須支付高額的網路成本[72]。在 2018 年後，他們改用邊際運算的模式，由攝影機擷取到的影像畫面，直接搭配機器學習模型現場進行分析及預判，快速來幫助他們檢測管線是否異常。當攝影機偵測到異常情況時，不需要將所有畫面上傳至雲端，只須透過雲端發送警示訊息，能大幅度減少成本[73]。

第二款　智慧家庭演變與定義

智慧家庭，又稱智能生活，係指透過家庭網路系統、運算處理器系統、感測器及其控制裝置等，串聯各種自動化家庭設備，使家庭設備得自動執行並提供智能服務的環境[74]。本文認為智慧家庭應用層面，大致包含居家安全、居家管理、居家控制及居家娛樂等四個領域，其發展過程可根據家庭設備自動化程度之不同，而有以下區分[75]：

---

[69] Ithome 網站， https://www.ithome.com.tw/news/127912（最後瀏覽日：2019/4/1）。
[70] 同註 53，頁 1-6 及 1-11。
[71] 同註 69。
[72] 同前註。
[73] 同前註。
[74] 古亞薇、張佳蕙、張家維、莊則敬、許桂芬、陳賜賢、無線與寬頻通訊研究團隊、網路前瞻技術研究團隊（2015），《智慧家庭發展趨勢與應用案例分析》，頁 1，台北：資策會產業情報研究所。
[75] 池煥德（2018），〈智慧家庭中的居家健康需求探索〉，《IEK 產業分析報告》，頁 2-3。



DOI:10.6814/NCCU201900793

一、第一階段：連網家庭

連網家庭（Connected Home），是最基礎的智能生活展現，重點就是把所有設備都用網路或 Zibee 串接起來[76]。在此階段，須由使用者事先依其偏好，編訂一套運作模式，缺點在於若環境或是使用者偏好改變，家庭設備無法自動更新設定[77]。因此，使用者在連網家庭中的日常運作，須花費時間處理設備設定，而且不易調整[78]。

二、第二階段：智慧家庭（Smart Home）

智慧家庭（Smart Home），係指除了將家庭設備串聯起來以外，設備具有自動化的功能，得以自行根據使用者實際需求，調整其設定及運作[79]。這一階段的使用者較連網家庭而言，在日常運作所需花費的設定及調整家庭設備時間已大幅減少，因這些設備會依其實際使用行為，自動調整運作方式[80]。

三、小結

目前現階段的 AIoT 技術與智慧家庭，在人工智慧運算方面，均有廠商按照其需求、資料量大小及服務速度不同，選擇採用雲端運算或邊際運算。在智慧家庭的定義方面，目前正處於第一階段和第二階段之交界處，有不少的智慧音箱推出，如 Amazon Echo、Apple HomePod、Google Home 及 Bosch Mykie 提供語音控制服務，但同時兼採手機應用軟體設定之功能。因此本文不刻意區分連網家庭亦或智慧家庭之用語，一律統稱為智慧家庭，並係指一切能透過網路或 Zibee 串接起來，並能用語音或其他方式，使家庭設備按實際使用者偏好、具體環境，自

[76] Simonlakey 網站，https://simonlakey.com/connected-home-vs-smart-home/（最後瀏覽日：2019/4/1）。
[77] 同註 75，頁 2。
[78] 同前註。
[79] 同註 76。
[80] 同註 75，頁 3。



DOI:10.6814/NCCU201900793

動更新設定並提供服務的家庭環境。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

## 第二節　從市場參與角色看智慧家庭市場概況

智慧家庭市場，從基礎晶片設備商（如 Qualcomm、Intel）、家用電器製造商（如 Whirlpool、Bosch、LG、Panasonic）、智慧型手機系統平台業者（如 Google、Apple）、通訊服務業者（如 AT&T、IBM、中華電信）及線上服務業者（如 Amazon），均提出自己的智慧家庭產品，或是欲發展成智慧家庭的平台中心。這是因爲智慧家庭市場的核心在於完成所有設備的「串聯」，因此只要「成平台中心者，就得天下」！業者認為只要能使其他廠商能把自家產品與自己平台串連在一起，那麼就有市場發話權，得以完善市場生態系。本文將上述業者，區分並著重在通訊服務業、家電廠及平台廠三者介紹，就三種市場參與角色，分述其提供的智慧家庭服務與策略。

### 第一項 通訊服務業

#### 第一款　IBM

IBM 自 2015 年起投資並推出 Watson IoT 平台暨解決方案，在方案中，家電廠商得利用 Watson IoT Platform，快速連接、收集與處理物聯網相關資料，且 IBM 又提供 IBM Cloud 的雲端服務，能滿足廠商不斷擴充儲存資料的需求，並替廠商在隱私及資訊安全風險控管上把關[81]。IBM Cloud 雲端服務，讓廠商可以在雲端平台上，直接利用視覺化、AI 驅動的運算分析服務[82]。就技術層面，IBM Watson 提供一套 API 服務模組，讓智慧家庭產品製造商，得透過開發相應的應用程式 App，串聯至 API 底層的技術介面和資料庫系統，在這種模式底下，廠商得直接使用分析與建議功能，大幅節省自行開發人工智慧和物聯網系統的時間[83]。

如美國知名家電品牌 Whirlpool 於 2016 年開始與 IBM 合作，利用 Watson

---

[81] IBM 網站，https://www.ibm.com/tw-zh/internet-of-things/solutions/iot-platform/watson-iot-platform（最後瀏覽日：2019/4/1）。
[82] 同前註。
[83] 陳佳榮（2017），〈國際平台大廠於智慧家庭發展策略分析〉，《IEK 產業分析報告》，頁 10。



DOI:10.6814/NCCU201900793

IoT 的技術串聯洗衣機與烘衣機上的感測器，將洗衣資訊透過感測器傳輸至 IBM Cloud 上，並透過分析顯示消費者是如何使用他們的機器以及機器本身如何應對，從而使 Whirlpool 更容易根據消費者需求，改良未來的產品設計，並反饋給烘衣機作最佳的節能規劃[84]；Panasonic 則是將 Watson IoT 應用於居家監控系統上，他可透過 IBM Cloud 上看到經分析的拍攝影像，並快速有效識別可能具有威脅性的動作[85]。

IBM 在智慧市場所扮演的角色是全然的服務提供商，其不主動生產家庭設備進入消費者家中，只提供感測器及串聯、分析服務，採用結合的方式，避免家電廠商有競爭疑慮，進而能廣納許多廠商，快速形成自己的生態系。

第二款　中華電信

中華電信於 2007 年開始著手，推出數位家庭產品（eHome），主要是與建商合作開發物業管理系統，當時是以家庭管理、生活資訊、通信整合、影音娛樂四大領域進行開發[86]。在這個階段，我認為中華電信仍處於「連網家庭」階段，消費者需花費更多心力在設定情境，並積極管理家中設備。而後在家庭管理上，於 2015 年推出 Smart Home 智慧家庭商品，安裝感測器、攝影機於家中，結合既有光纖網路，進行安全監控、情境控管及電量效能管理，使消費者能透過手機終端裝置調整情境狀態[87]。在影音娛樂方面，中華電信在 2016 年將 MOD 機上盒改成網路影音串流 OTT 服務，提供更貼近用戶的娛樂服務[88]。自 2017 年起，中華電信陸續推出「健康雲」、「瓦斯雲」等服務，提供更精細的雲端分析與建議推播[89]。在 2019 年，中華電信希望把 MOD 作為主要家中控制器，藉以串聯「智慧家庭

---

[84] IBM 官網，https://www.ibm.com/blogs/internet-of-things/whirlpool/（最後瀏覽日：2019/4/1）。
[85] 同註 83。
[86] 中華電信智慧家庭網站，http://www.dhs.hinet.net/Service_01.html（最後瀏覽日：2019/4/2）。
[87] 中華電信網站，https://www.cht.com.tw/home/enterprise/ict/smart-service/smart-home（最後瀏覽日：2019/4/2）。
[88] 中華電信官網站，https://www.cht.com.tw/home/consumer/broadband/broadband-service/660（最後瀏覽日：2019/4/3）。
[89] Digitimes 網站，https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000556694_B3Q7DLI28VUQQ45GZ5T0P（最後瀏覽日：2019/4/2）。



DOI:10.6814/NCCU201900793

生活」服務，消費者在家中僅須以聲控方式控制 MOD，即可享受影音、視訊、或感測來連結其他應用，如瓦斯雲、智慧音響、及健康雲服務等[90]。

如 2018 年時，中華電信、遠雄建設、Panasonic、台灣大車隊、遠雄悅來咖啡曾在遠雄二代宅聯合推出智慧家庭概念，整合硬體設備及軟體服務[91]。這次的合作是建構在 TaiSEIA 101 臺灣智慧家庭物聯網協定之上，統一通訊標準藉以串連不同廠牌的家電產品，提高家電間相互運作效能，省去個別家電廠商協商系統標準的時間[92]。其主打「智能管家」的服務，消費者得在家中透過聲控方式，執行下列措施：(1)叫車服務、訂餐外送(2)智慧家電互動操控功能(3)獲得家庭環境感知資訊(溫度、濕度、CO2)、家庭能源使用資訊、管理費繳費資訊、瓦斯登錄資訊等(4)安全設備控制，包含燈光情境控制、全熱交換機控制、保全偵測/設定/求救、瓦斯偵測/切斷等[93]。

中華電信作為全台最大的電信服務商，已有完整的通訊網路。其提供之服務已從傳統電信，改推向跨業合作，例如智慧家庭市場，由於其在台灣的市場地位雄厚，對於其他家電業者或平台業者而言與其合作，都是擴大台灣市場的一大助益。雖中華電信並未自行生產家用電器，然而中華電信早有針對消費者提供搭配家用電器之購買服務[94]，未來讓消費者在家中自行用語音選購產品服務的模式，亦是指日可待。

## 第二項 家電廠

### 第一款 Bosch

德國知名家電品牌如 Bosch，因已擁有完整智慧家電產品及安全系統設備，

---

[90] 同前註。
[91] Taiseia 網站，http://www.taiseia.org.tw/Industry/industry_more?id=100（最後瀏覽日：2019/4/3）。
[92] 遠雄企業網站，https://www.farglory.com.tw/news/message/detail/101（最後瀏覽日：2019/4/3）。
[93] 同註 91。
[94] 中華電信網站，https://www.cht.com.tw/home/campaign/CPE/index.html（最後瀏覽日：2019/4/1）。



DOI:10.6814/NCCU201900793

在智慧家庭市場上，Bosch 於 2016 年在 IFA 及 Living Kitchen 展覽上展示新的語音助理「Mykie」，雖然目前 Mykie 仍為一個概念，並非具體產品，但其功能主要是用語音功能，串聯並執行家電啟動、食譜及烹飪教學、冰箱存貨確認、線上訂購等[95]，可以顯見 Bosch 想開發一個主控制器，串接所有的設備。其實除了自主開發 Mykie 語音助理以外，在語音控制器上 Bosch 亦與 Amazon Alexa 合作，讓 Alexa 能與所有相應家庭設備相連[96]。在串聯及分析平台方面，Bosch 除開發自己的 Home Connect 跟 Bosch Smart Home 應用程式外，亦與其他平台廠商合作，例如 Google Nest、IFTTT 等[97]。在智慧家庭的策略上，Bosch 作為知名家電業者，其還是注重在實體家電銷售與佈局上，因此並不讓自家產品只侷限在自己串聯系統上，而是採用自主開發及跨界合作的方式雙管齊下，未來是否發展成獨家生態系仍須靜觀其變。

Bosch 在家庭設備上裝置感測器及相關感應或紀錄設備，讓家庭設備之資訊得以被記錄並上傳[98]。舉例而言，在智慧冰箱方面，Bosch 運用 RFID 自動識別冰箱內之物體或食品標籤，該標籤可能包含食物類型及保存期限的資訊[99]，冰箱可自動將不同標籤訊息傳送到 Home Connect 手機程序裡面，讓消費者從手機直接了解冰箱內食品資訊，若該商品並未有相應的標籤，消費者亦可以選擇手動輸入必要資訊[100]。Home Connect 應用程式會根據食品類型，提供冰箱理想溫度、濕度設置的建議[101]。Bosch 在冰箱內另安裝攝像頭，讓消費者可以透過應用程式隨

---

[95] Home connect 網站，https://www.home-connect.com/global/connected-household/mykie#/Togglebox=4479371-4478593-1/Togglebox=4479371-4478593-2/Togglebox=4479371-4478593-3/Togglebox=4479371-4478593-5/（最後瀏覽日：2019/4/1）。

[96] Home connect 網站，https://www.home-connect.com/global/connected-partners（最後瀏覽日：2019/4/1）。

[97] 同前註。

[98] Bosch 智慧互聯行銷報告（2017），https://media3.bosch-home.com/Documents/MCDOC02048462_Bosch_Home_Connect_PDF_Brochure_1-25.pdf（最後瀏覽日：2019/4/1）。

[99] Bosch 智慧冰箱專利說明書（2014），https://patentimages.storage.googleapis.com/44/a7/69/84e37502b5dd52/WO2014198632A1.pdf（最後瀏覽日：2019/4/1）。

[100] 同前註。

[101] 同註 98。



DOI:10.6814/NCCU201900793

時隨地查看具體內容，並有感測器觀察冰箱門未被完全關閉時會自動通知至應用程式[102]。從這裡不難看出，Bosch 推出智慧冰箱，其提供之服務已不像以往僅是「食物儲存」的功能，一旦冰箱可以自動感測並判別內部物，Bosch 就能為消費者提供一系列與食品相關的服務，例如上述所說的食品管理功能、提醒建議等，未來亦可以與合作夥伴（如 Amazon）在線商店，讓消費者直接透過應用程式或語音助理購買需求品[103]。

第二款　LG

LG 集團在智慧家庭市場上，首先改良其既有家用電器產品，使其智能化。例如 LG 推出智慧洗衣機，其可以自動感測家庭環境或衣物重量、污染程度，選擇最佳洗衣條件，如清洗程序、時間、水量與溫度等，也可以使消費者透過手機遠端控制[104]。在智慧冰箱方面，LG 在冰箱裡內建能與 Amazon Alexa 聲音互動的功能，並裝置廣角相機，使消費者可透過手機關觀看內部食物品項，並透過感測器收集用戶使用模式及環境溫、濕度，藉以分析冰箱開關次數與時間長短，自動調整省電時段[105]。從技術層面來看，LG 在家電產品上應用深度學習技術，使這些家電得透過 WiFi 與各感測器串聯，並將使用資料上傳至雲端，利用雲端運算分析用戶的使用模式[106]。於 2018 年時，LG 集團將這一個智能系列家電，重新定義一個新的系列品牌「ThinQ」[107]，強調 ThinQ 系列的家電都具備智慧學習、視覺識別等功能，且所有產品均可劃分出家居、出遊、辦公室等三種場景進行調整

---

[102] Home connect 網站，https://www.home-connect.com/global/connected-household/fridges-freezers（最後瀏覽日：2019/4/1）。

[103] 如同 Bosch 在洗碗機上目前已有自動訂購洗碗錠之服務，未來對於其他產品之補充品或食品亦可採取相同模式，https://www.home-connect.com/global/connected-partners/shopping-ordering（最後瀏覽日：2019/4/1）。

[104] LG 網站，https://www.lg.com/tw/press-release/20170417-lg-2017-smartthinq-app（最後瀏覽日：2019/4/3）。

[105] 金美敬（2017），〈LG 電子智慧家庭策略分析〉，《IEK 產業分析報告》，頁 6。

[106] 同前註。

[107] 本商標於 2018 年在台灣申請註冊，最早於 2017 年 9 月於歐盟申請註冊，https://twtmsearch.tipo.gov.tw/SS0/SS0201.jsp?showType=1&caseNo=XpJ13RyT4ZVUzWjhPN1FWVkxRVkI4WnNxd2FEUT09&l6=zh_TW&isReadBulletinen_US=&isReadBulletinzh_TW=true（最後瀏覽日：2019/4/4）。



DOI:10.6814/NCCU201900793

[108] 。

另一部分，LG 集團和各大通訊應用業者合作，例如 Line、Kakao Talk、WhatsApp 等[109]，推出 Home Chat 的智慧平台建置在 App 中，作為虛擬控制助理，使用者得向家電發送文字訊息，即可獲得相應狀態，例如冰箱剩下多少食材等[110]，完善遠端控制與管理的功能。在 2019 年起，LG 集團透過開放平台「ThinQ AI」，使其電視具有呼喚 Google Assistant 和 Amazon Alexa 的功能，使使用者得在家庭內使用更方便的語音控制方法[111]。

## 第三項 平台廠

### 第一款 Amazon

Amazon 在 2014 年時候推出 Amazon Echo[112]，稱為智慧音箱或語音助理，使用者只要呼喊「Alexa」或「Echo」就可以完成待辦事項設定、廣播提醒設置、查詢天氣預報、播放音樂和購物（結合 Amazon.com 線上購物功能）等 3000 項功能[113]。除了 Amazon Echo 以外，Amazon 亦已同心圓的方式開放相關產品，在硬體設備方面，如智慧音箱 Musaic、智慧灑水器 Rachio、智慧寵物餵食器 Petnet、安控攝影機 Scout Security；在應用軟體方面，用併購或投資之方式，容納軟體廠商如手勢控制系統之 Thalmic Labs、語音橋接器之 Invoxia、及專門提供自然語音處理訓練資料之 Defined Crowd，逐步擴大、穩固自己的市場[114]。

Amazon 在產品策略上，強調要把 Amazon Echo 發展成最好用的智慧管家、擁有許多功能，且掌握大量的客戶使用者數據與模式[115]，由於 Amazon Echo 的

---

[108] TechOrange 網站，https://buzzorange.com/techorange/2018/01/09/lg-new-thinq-ai-brand/（最後瀏覽日：2019/4/4）。
[109] LG Home Chat 網站，http://www.lghomechat.com/us/（最後瀏覽日：2019/4/3）。
[110] 同註 74，頁 62。
[111] 經濟日報（8/1/2019），〈LG 電子參展 CES 推 ThinQ AI 旗艦電視〉，https://money.udn.com/money/story/5612/3580972（最後瀏覽日：2019/4/5）。
[112] 維基百科網站，https://zh.wikipedia.org/wiki/Amazon_Echo（最後瀏覽日：2019/4/5）。
[113] 同註 53，頁 3-3。
[114] 石立康（2017），〈評 Amazon Alexa 發展策略〉，《IEK 產業分析報告》，頁 1。
[115] 同註 53，頁 3-4。



DOI:10.6814/NCCU201900793

反應速度跟功能多，使用者不會只購買 Echo，亦會選擇添購其他產品。如 Echo Look 是一台可透過 Alexa 下台指令的攝影機，以拍照或錄影的方式，記錄個人穿搭風格，並可以使用內建的「Style Check」運用已結合時尚專家建議之機器學習算法，提供建議，在瞭解使用者的選擇與反饋後，Echo Look 系統也會更了解他的需求，精準地提出合適的穿搭建議[116]。

打出自己的基礎市場之後，Amazon 開始以開放平台策略，來建立自己的生態系[117]。在優勢上，Amazon 長期以來以網路商店、最大線上通路著名，當其以 Echo 進入家庭之中，又具備直接以語音方式訂購商品，節省使用者的消費時間，那 Amazon 就是所有家電廠商最渴望合作的夥伴。因此，自 Amazon 將 Alexa Amazon Voice Service（AWS）雲端運算服務及 Echo 關鍵技術開放給設備商後[118]，許多廠商如 Bosch、LG、Samsung 等均將 Alexa 語音助理與其開發之智能家電設備相結合。Amazon 對於 Alexa 語音助理其實不只是放置在智慧家庭市場中，其在汽車、手機、電腦等交通、通訊設備，均有合作趨勢，整體來說，Amazon 想打造全然的智慧生活生態系[119]。

第二款　Google

Google 最早於 2011 年，就提出「Android@Home」概念，把 Android 系統從手機裝置系統轉向智慧家庭裝置上[120]。於 2014 年時，Google 收購全美智慧恆溫器市佔率最大的 Nest，正式踏入智慧家庭市場[121]。一開始，Google 如 IBM 一般，均在 2015 年以開放 API 方式推出智慧物聯網平台，也就是「work with Nest」計畫，第三方的廠商可以根據 Nest 所偵測到的使用者環境資訊，進一步提出應用服務[122]。惟其發展並不如 IBM Waston 平台一樣順利，其推出的通訊協定接受度

---

[116] 同註 53，頁 3-8。
[117] 同註 114，頁 2。
[118] 同前註。
[119] 北美智權報網站，http://www.naipo.com/Portals/1/web_tw/Knowledge_Center/Industry_Economy/IPNC_180223_0702.htm（最後瀏覽日：2019/4/5）。
[120] 同註 83，頁 3。
[121] 同註 53，頁 3-3。
[122] 同註 74，頁 35-36。



DOI:10.6814/NCCU201900793

不高[123]。而後，其轉戰發展其智慧語音管家，先建立起 Google 與消費者的關係，打進智慧家庭市場，因此其在 2016 年時，推出 Google Home 裝置搭配 Google Assistant 語音助理[124]。

Google Home 是一台智慧管家裝置，用戶只要透過呼喊「Ok Google」或「Hey Google」啟動並下達指令，即可使用音樂播放、Google 查詢、生活提醒、家電操控、查詢日曆及地圖等功能[125]。Google Home 與其他廠商最大的不同，在於其具有超強搜尋引擎的優勢，因此其在發展 Google Home 的產品時，均圍繞在串接既有搜尋功能[126]。從技術層面來看，Google 在打造 Google Assistant 是希望能讓用戶以口語對話方式與家電設備互動，並透過自然語言處理、深度學習及語音合成技術，進而了解使用者需求，達到精準服務效果[127]，但其目前重心主要仍放在精準搜尋的功能，對於後端消費者服務部分，仍未有明顯策略。

在商業模式上，為了能與 Amazon 一較高下，Google 在 2018 年亦設立 Smart Display 平台，讓許多硬體設備商能將 Google Assistant 結合在既有家電產品上，如 Braven、iHome、JBL、LG、聯想、Knit Audio、Sony 等[128]。在未來策略上，Google 似乎想容納更多硬體設備商，並結合既有的 Android 系統和 iCloud 雲端服務，一條鏈達成 B2B2C 的過程[129]。

第三款　Apple

Apple 在 2014 年的時候，推出 HomeKit 智慧家庭平台的概念，當時維持 Apple 一貫風格，其嚴謹地定義出一套標準化的智慧家庭架構，分為五個層次：（1）HMHome 房屋（2）HMRoom 家中空間（3）HMAccessory 家中裝置（4）

---

[123] 同註 114，頁 3。
[124] 同前註。
[125] 同註 53，頁 3-6。
[126] 同註 114，頁 5。
[127] Inside 網站，https://www.inside.com.tw/article/9351-google-ai-google-io（最後瀏覽日：2019/4/6）。
[128] 科技產業資訊室網站，http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=14183（最後瀏覽日：2019/4/6）。
[129] 同註 74，頁 74。



DOI:10.6814/NCCU201900793

HMService 家庭應用服務(5)HMZone 家庭區域分組，目前大多都是 HMAccessory 產品的開發與合作[130]。Apple 是以開放 API 方式解決目前市場上相容性的問題，若要想加入 Apple 智慧家庭成為商業夥伴，就必須符合他的通訊協議（HomeKit Accessory Protocol）及硬體標準[131]。惟正因為 Apple 為了維持整體系統資訊安全，對於合作廠商的要求十分嚴格，如產品必須使用通過認證的 MFi 晶片才可以與 HomeKit 平台串聯[132]，使得其在智慧家庭市場上的發展非常緩慢，加入廠商遠低於 Amzon 與 Google[133]。HomeKit 在智慧家庭中的主要控制器是 Apple TV，一開始 Apple 在發展智慧家庭的藍圖是希望所有的設備最終可與 iPhone、iPad、iPod 等設備串聯[134]，然而這個策略是與其他競爭者截然不同的。Google 跟 Amazon 在行動裝置市場上表現不如 Apple，因此在進入智慧家庭市場時，前者都選擇投入在智慧音箱的研發上。後者就是延續本身優勢，想讓把既有的行動裝置消費者導入到智慧家庭市場，然而其發展速度遠輸給 Amazon，因此在 2018 年時推出 HomePod 語音助理[135]。

HomePod 的運作上，亦是建構在 HomeKit 平台上，結合 Siri 語音系統。消費者用語音要求 HomePod 開啟 App 時，這個指令與 Amazon Echo 的運作不同，不會把資訊直接傳送到雲端上，而是傳送到 iPhone 上執行指令，比起同種類的商品仍須有 iPhone 輔助，感覺智慧程度沒有其他產品那麼高[136]。

---

130 同前註，頁 37。
131 同前註，頁 38。
132 同前註。
133 同註 53，頁 3-3。
134 Feiler Jesse, *Learn Apple HomeKit on iOS*, Apress, Berkeley, 10 (2016).
135 數位時代網站，https://www.bnext.com.tw/article/47919/apple-homepod-price-features-vs-echo-google-home-ipod-history（最後瀏覽日：2019/4/6）。
136 同前註。



DOI:10.6814/NCCU201900793

## 第三節　智慧家庭產業特性分析

### 第一項 智慧家庭應用趨勢

在了解智慧家庭市場的參與角色及發展後，可以顯見所有的參與者在發展上均有許多相似策略與趨勢，以下將著重在市場策略、平台整合與串聯三者進行討論。

#### 第一款　市場策略共通性

##### 第一目　加強消費者關係

智慧家庭之所以能發展，係基於大數據已經累積至一定程度，以及機器學習分析精準度變高。而後所有的市場參與者希望能與消費者建立穩健的關係，並透過提供更細緻、貼近需求的服務，來達到捆綁消費者的效益。因此在市場策略上，第一步都是加強與消費者的關係。舉例來說，家電廠商如 Bosch、whirlpool、LG 等，在傳統家電市場上均佔有一席之地，在創新這個課題上，他們希望做到的是捆住既有消費者、吸引更多新的消費者。他們在產品研發上，都是讓本身的家電產品會思考、會蒐集資訊，來分析他們消費者的需求。像前面所述的 LG 智慧冰箱，LG 透過裝置裝置廣角相機和感測器，可以蒐集用戶使用模式及環境溫、濕度，在下次設計產品時就可以依照消費者實際需求去做調整[137]。

在通訊服務業者及平台廠的眼裡，他們要打入智慧家庭的市場，就是要跟傳統家電廠商合作或是直接競爭。大多的廠商是推出不直接與傳統家電廠商的輔助設備及系統，如同中華電信 MOD、Amazon Alexa、Google Assistant、Apple HomePod 等，透過發明智慧管家或稱之為智慧中樞（Smart Gataway）的設備，讓其他家電廠商得以串接，達到你的消費者也是我的消費者的模式，加強吸引智慧家庭市場中的消費者關係。但本文認為 IBM 走的是另一個策略，IBM 不直接

[137] 同註 105，頁 6。



DOI:10.6814/NCCU201900793

進攻 B2C 的商業模式，走的是純 B2B 商業模式，提供傳統家電廠商升級的助力。如同上一節所述的，在這種模式底下，加上 IBM 的雲端分析運算能力很強，家電廠商的接受度較高。

第二目　產品作為平台

在智慧家庭底下的產品，強調是能與消費者互動、思考並自動調節，雖然每一家的智能程度不同，然而在策略上，他們都希望產品是一個平台，串聯消費者與第三方應用服務業者。以 Bosch 洗碗機為例，Bosch 已在在美國和英國以 Home Connect 這個品牌，推出可自動化計算清洗次數及洗碗錠用量的洗碗機[138]。當洗碗錠數量不足時，會自動連接到 Amazon 線上網站服務（Amazon Dash Replenishment Service），根據用戶的設定直接自動下單洗碗錠，並會發送電子郵件確認，當然用戶亦可事後取消訂單[139]。另外，以 Amazon Alexa 及 Google Assistant 為例，均是以語音軟體的形式，串聯硬體廠商與消費者，讓消費者可以用語音方式，啟動第三方硬體廠商相關產品，而 Amazon 和 Google 可以在智慧家庭市場中，能更直接了解消費者的需求。

第三目　提供數位服務

就許多銷售產品的廠商來說，能夠知道消費者實際的需求、即時提出建議是擴大銷售市場的關鍵。傳統的做法是投放廣告，運用經驗判斷消費族群跟可能投放在哪些實體、虛擬的場域最有效果。在大數據時代，透過機器學習我們更能清楚消費者到底想要什麼。因此，在各大具有智慧功能的產品進駐家庭內時，數位服務就是最後一哩路。

在前述許多市場參與者介紹當中，Amazon 是最有機會完成數位服務提供的人。首先 Amazon 電商服務平台根據 eMarketer 的評比，是全美網購市場最大的贏家，消費者如果需要一個產品有 66%的人會上 Amazon 來查詢[140]。再來，Amazon

---

[138] Home Connect 網站，https://www.home-connect.com/global/connected-partners/shopping-ordering/amazon-dash（最後瀏覽日：2019/4/7）。

[139] 同前註。

[140] Emarketer 網站，https://www.emarketer.com/content/looking-for-a-new-product-you-probably-



DOI:10.6814/NCCU201900793

Echo 其實就具備用語音上網下單的功能，對於喜歡透過網路購物又不喜歡耗費太多時間的人而言，Amazon 是最好的選擇。其他的市場參與者，如傳統家電廠商、通訊服務業者，均是以自己的產品建立連結，使消費者可以執行下訂動作，如同中華電信與遠雄悅咖啡的餐飲運送服務。

第二款　平台整合與串聯策略

智慧家庭相關產品市場，其主要在於預測家庭成員購買行為，消費者的購買行為會影響整個市場的分佈與走向[141]。一般而言，消費者在選購家電的時候，品牌忠誠度並非全然一致，按照不同功能的電器需求，會選購不同的品牌偏好，因此目前大多消費者家裡的家電可能包含五、六種品牌以上。再把家電市場導入連網家庭的時候，通常都是每個家電廠設計自己的 App，讓消費者可以將智慧家庭產品透過網路連接到手機裡操控[142]。然而，如果一個消費者有五六種品牌的產品，就需會下載非常多的 App，使用起來也沒有讓產品皆溝通、快速的優勢。這是智慧家庭市場為何走向平台整合與串聯策略的原因，如同 USB 插槽走向標準化，智慧家庭的設備規格雖然目前世界上並無統一標準，然而透過策略結盟的方式，或讓更多廠商、新創業者群聚，最終走向互相授權、標準化的方式。目前整體看來，各個市場參與者仍停留在平台整合階段，策略目標是一致的，但方法是有略些不同的，這部分詳如後述。

## 第二項 智慧家庭應用差異

第一款　資料儲存方式

在智慧家庭應用層面，為了解消費者的需求、建立穩健的消費者關係，各市場參與者必須竭盡可能的了解實際的應用情境、還有消費者的偏好，因此數據的

searched-amazon（最後瀏覽日：2019/4/7）。

[141] 石立康、鄭淑方（2016），〈智慧家庭之整合性平台與多元應用趨勢〉，《IEK 產業分析報告》，頁 3。

[142] 同前註。



DOI:10.6814/NCCU201900793

蒐集是最重要的一環，而數據資料的儲存地點，就是安全性跟隱私的考量環節。目前資料儲存的方式，大抵上分為兩種：一種是，蒐集直接儲存在雲端上，如 IBM Waston、Amazon Echo、LG 等，Amazon 和 LG 合作會將 Alexa 從家電中蒐集到的資訊直接上傳至 AWS 雲端資料庫，進行分析[143]；另一種是，儲存在當地智慧中樞或稱為智慧管家裡，待用戶使用 App 或其他工具時，才會傳輸到企業後端，如同 Bosch、Apple 等，如 Bosch 推出智慧冰箱或其他智慧家電搭配 Smart Home 或 Smart camera 的 App，只有當用戶連線至 App 時，才會回傳至公司後端[144]。

第二款　資料處理方式

根據上述的分類，將資料直接傳輸至雲端時，採取的作法是雲端運算。將資料儲存在各個產品載體上，大多採取是嵌入式軟體和邊際運算法、集成式傳感器組合[145]。但也可能兩者運算方法均採，若是考量到反應快速、直接回饋的就會採用邊際運算的方法，例如自然語言的處理，像 Alexa、Siri、Google Assistant[146]。處理的方式不同，亦會影響資訊安全層級以及對個人資料的保護，若是以雲端運算的方式，似乎去識別化處理就是關鍵；反之，若採取邊際運算方法，而且上傳回後端的資訊是經過去識別化處理的數據結果，則該產品載體的安全性應為首要考量。

第三款　發展核心策略不同

智慧家庭的設備規格最終走向標準化，相互之間也透過水平、垂直整合的方式完成讓各產品串聯的效果，帶給消費者實際上的便利。但根據每個市場參與者的角色不同，每一家廠商的優勢不同，在平台整合上的策略也略使用不同方法，本文將按照上述市場參與者的角色，大抵區分為三種策略方法。

首先是，通訊業者著重在全面性應用整合，IBM 在這點就是建好堅強的後端

---

143 Amazon 網站，https://aws.amazon.com/tw/solutions/case-studies/lg-electronics/（最後瀏覽日：2019/4/7）。

144 Bosch 網站，https://www.bosch-smarthome.com/uk/en/privacy-statement（最後瀏覽日：2019/4/8）。

145 每日頭條網站，https://kknews.cc/zh-tw/tech/qnoe93o.html（最後瀏覽日：2019/4/8）。

146 隱科技網站，https://www.cool3c.com/article/135498（最後瀏覽日：2019/4/8）。



DOI:10.6814/NCCU201900793

平台，讓他們廠商可以全面性的在後端進行應用分析，整合能力、成本與效果對廠商來說都是很好的選擇。中華電信因在台灣是具影響力的通訊代工廠，也擁有許多台灣通訊消費者的需求資訊，從系統端建立出的平台最能受到家電廠商的歡迎，他們要做的是全面性的整合，因為資源雄厚他整合的模式和其他市場參與者很不同，他們直接切入新的建案，與建商合作讓消費者入住時，及享受最完整的智慧家庭服務。

再者，家電廠著重在產品功能及能源管理這兩塊環節上，這點是建立在這幾年家電廠商多主打「白色家電」環保的理念，強調節能、減碳及永續的作法[147]。他們的作法都是先從安全監控、能源管理、健康娛樂及家用電器四個方向去做產品研發[148]，先建立一套全智慧化的家電設備，在和平台廠或是通訊業者合作，當然談判籌碼就高許多，況且他們長期在家電市場耕耘，對於客群與消費者需求瞭解是最直接的，因此只要口號跟功能做得好，在發展是很有潛力的。

最後，平台廠均以 AI 語音助理為出發，而後建立開放平台或提供通訊架構規範，以 Amazon 將 Echo 整合後端電子商務平台的例子，刺激其他擁有架設平台和運算技術的業者如 Google 和 Apple 等相繼研發與切入[149]。就 Google 發展 Nest 計畫，開放部分用戶數據，得讓各個廠商根據數據設計應用服務[150]，讓各個廠商可以設計出差異化產品，打造自己的生態系。

本文認為「共用數據、資訊」是三個市場參與者串聯、建立平台，最終共同會邁向的趨勢。因為對市場參與者而言，讓自己的聯盟研發出的產品更貼近消費者的需求，是雙贏的局面。因此，能獲得更多數據共同進行研發，是勢在必行的。舉例來說，Bosch 在智慧家庭上與 Amazon Alexa 合作，其就在隱私聲明中指出：「您可以選擇以 Amazon Alexa 語音方式控制智慧家庭產品。首先你必須手動進

147 陳右怡（2017），〈居家機器人大戰開打，智慧家庭領導業者洗牌中〉，《IEK 產業分析報告》，頁 3。
148 石立康（2016），〈智慧家庭市場大趨勢〉，《IEK 產業分析報告》，頁 3-5。
149 同註 147。
150 同註 122。



DOI:10.6814/NCCU201900793

行串聯設定，當您完成設定時，即可能必須通過 Amazon 將個人數據傳輸到相應產品，反之亦然。再者，若您將 Alexa 和 Bosch 帳戶完成串聯，則表示您同意 Smart Home 產品可透過 Amazon Alexa 進行控制，而且要求並指示我們( Bosch ) 提供、交換相應數據與亞馬遜 Alexa[151]。」然而，平台之間共用數據的型態、方式就是下一個課題。

國立政治大學
National Chengchi University

[151] 同註 144。



DOI:10.6814/NCCU201900793

# 第三章　隱私權與個人資料保護法

智慧家庭按照上一章所闡述的，市場參與者希望透過「更加了解消費者」，來建立消費者關係。廠商為能精確地了解消費者，蒐集消費者的資訊及其使用習慣是在所難免，但這樣的蒐集、後續處理及利用，可能產生資訊隱私權的問題。

這樣的資訊隱私問題，不同於大眾討論網路科技發達所產生之網路空間的隱私權問題，如 Facebook 和 Google 蒐集用戶瀏覽習慣等，因為網路平台某方面來說是屬於公開的場合，但在智慧家庭領域，消費者被蒐集的資訊是來自於「家庭場所」，自古以來家庭場所都是個人想放鬆，不被打擾的一個區域，因此智慧家庭應用的隱私權問題及重視程度，是需要被關切跟討論的。再者，在智慧家庭開放平台上，共用數據、資訊是未來的趨勢，但數據共享這件事，到底帶來的方便性？還是會產生更多隱私疑慮和影響呢？一開始智慧家庭開發商在考量商業模式的時候，也可能無法預期這樣的營運，可能會衍伸出隱私或法律課題。本章將著重在討論何謂「資訊隱私權」，家庭場所的隱私權是否別具不同意義。此外，歐盟、美國及台灣對於隱私權及消費者個人資料之保護上，從法制面來看，採用何種立法模式及立場，進而接續討論智慧家庭應用，可能產生的隱私問題何在。

國立政治大學 National Chengchi University

## 第一節　資訊隱私權之發展

### 第一項 隱私權的起源

#### 第一款 自由與尊嚴的價值：不受干擾的權利

在英美法（Common Law）和大陸法（Civil Law）上對於隱私權的保護價值是不同的，大陸法強調的是對於尊嚴（a right to respect personal dignity）的人格



DOI:10.6814/NCCU201900793

權保護，其目的在於保護人的肖像、姓名及名聲等權利[152]，這是因為大陸法系國家一向偏重與尊嚴相關的「個人公共形象」，而這可追溯到中世紀貴族階級維持體面身分及對特權追求的結果[153]；而英美法保護隱私權的出發點是自由權的價值（values of liberty）[154]。

在英美法上，首篇論及隱私權（Right of Privacy）的論著始於 1890 年，由 Samuel D. Warren 和 Louis D. Brandeis 共同完成之作品[155]，當時的隱私權概念仍是建構在侵權行為法（Torts）底下，用來解決當時媒體報導緋聞、八卦專欄，所帶來的隱私和嚴重影響公眾形象的問題[156]。他們認為隱私權（Right of Privacy），是人享有不受干擾的權利（Right to be let alone），這樣的權益是源自於英美法重要的概念：「家即是一個人的城堡」（A man's house as his castle）[157]，一個人享有在自己家中能夠輕聲細語談論，且不受公開宣揚的自由（what is whispered in the closet shall be proclaimed from housetops）[158]。

第二款 自主控制的權利

在現今新聞媒體及資訊傳遞非常快速的時代，保護隱私的理由已無法全然單一方面去考量，有論者認為隱私權的出現，基本上就是要保護個人尊嚴、個人身份認同及其個人自主性[159]。隱私不應該是屬於被動、請求不被干擾的權利，不應侷限在不讓他人取得與自己相關的資訊，而該是一個主動的權利，應該賦予該個人擁有控制個人資訊使用與流向的能力[160]。

---

[152] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151, 1161 (2004).
[153] 余瑞陞（2014），《權利化的隱私－反思現代國家法律下的個人隱私》，頁 31，國立政治大學碩士論文。
[154] Whitman, *supra* note 152, at 1161.
[155] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[156] Samantha Barbas, *Saving Privacy from History*, 61 DePaul L. Rev. 973 (2012).
[157] Brandeis, *supra* note 155, at 220.
[158] 劉靜怡（2002），〈網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河〉，《資訊管理研究》，第 4 卷第 3 期，頁 143。
[159] 同前註，頁 144。
[160] 同前註。



DOI:10.6814/NCCU201900793

進一步言，這個隱私理論稱之為「控制理論」(Control Theory)，認為隱私保障就是使一個人可以決定他的資訊，如何被蒐集、共享、使用、保留或以其他方式操縱[161]，這也是資訊自主權的出現，大眾開始討論個人享有知道、查詢、請求處理其相關資訊的權利。

## 第二項 隱私權與個人資料保護

隱私權與個人資料保護是多數會談及到一個相輔相成的概念，個人資料保護法的建立是源自於隱私權的保障，是保護隱私權其中一種最具為具體的手段。隱私權，係就私生活或工商業所不欲人知之事實有不被他人得知之權利[162]，未經該個人同意者不得擅自公開、揭露或窺探他人隱私。有論者，將台灣司法院釋字第 603 號解釋，區分為「空間隱私」和「私密隱私」二者進行討論[163]，其中空間隱私是不受干擾的控制權，而私密隱私是指保障人民關於資訊揭露的決定權和更正權[164]，這種立論模式是融合了不受干擾理論（Right to be alone）和控制理論（Control Theory）的價值。

從立法保護來看，隱私權的保護最先從保護個人擁有「秘密」、不被窺探的角度來進行。於民法上，以侵權行為法（民法第 184 條 1 項、195 條）作為保護手段；於刑法，以妨害秘密罪章進行保護（刑法第 315 條至 319 條）。若要構成隱私權保護，首先該達成一定標準，台灣司法院釋字第 689 號解釋，採取與美國最高法院「合理的隱私期待理論」(reasonable expectation of privacy)[165]相同見解，認為若該個人主觀上對於該資訊具有隱私期待，而客觀上該環境與空間，一般社會大眾亦認為會具有隱私期待者，則受到隱私權的保護，即使在公

---

[161] Sheri B. Pan, *Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze*, 30 Harv. J.L. & Tech. 239, 241 (2016).
[162] 法務部（71）法律字第 9168 號函。
[163] 尤重道（2017），〈個人資料保護之概念與蒐集處理利用暨違法責任（上）〉，《全國律師》，第 21 卷第 7 期，頁 88。
[164] 司法院釋字第 603 號。
[165] *See* Katz v. United State, 389 U.S. 347 (1967).



DOI:10.6814/NCCU201900793

眾場合情形下，個人仍應有一定程度之不受侵擾之自由[166]。

個人資料保護，是規範個人資料之蒐集、處理及利用模式，其目的不僅是在於避免人格權受侵害，更重要的是其希望達成促進個人資料之合理利用[167]，並以「公共利益」作為隱私權保護和資訊進步的界線[168]。從促進個人資料之合理利用的目的來看，顯然在個人資料保護上，各國也面臨到企業的壓力，希望能界定個人資料使用及不得使用的範疇，給予企業一個遵循的方向。

## 第二節 歐美個人資料保護規範

目前各國面對科技進步對於個人資料的需求，以及國人隱私權的保障，均採取相應的立法保護，實際立法和管制模式些許不同，然實則都是希望採取適當界線，達到社會進步與權利保護的平衡。面臨物聯網、人工智慧以及大數據的時代，個人資料之蒐集、處理及利用更加多元且不可預測，各國對於相應陸續提供看法，本節將介紹歐盟、美國針對個人資料保護之規範，並著重討論各國對於人工智慧、機器人應用上，對道德規制、個人資料限制等政策或立法面考量。

### 第一項 歐盟

#### 第一款 一般資料保護規則 General Data Protection Regulation

因電腦時代盛行，歐盟最早在 1995 年及制定了相關指令《1995 年的歐盟個人資訊保護指令》( Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

[166] 司法院釋字第 689 號解釋部分協同及部分不同意見書。
[167] 台灣個人資料保護法第 1 條。
[168] 同註 163，頁 89。



DOI:10.6814/NCCU201900793

processing of personal Data and on the free movement of such Data）[169]，要求會員國應制定相應法令來保護隱私權並針對個人資料處理給予明確限制[170]，然當時各個國家對於個人資料保護的規定的程度並不一致。幾年之後，歐盟於 2000 年所制定之《歐洲聯盟基本權利憲章》（Charter of Fundamental Rights of the European Union）[171]，將隱私權及個人資料保護視為人憲法所賦予之基本權利。具體而言，《歐洲聯盟基本權利憲章》第七條保障的是隱私與家庭權利（Everyone has the right to respect for his or her private and family life, home and communications），而第八條強調人享有個人資料保護的權利（Everyone has the right to the protection of personal Data concerning him or her）[172]。

由於歐盟提升了隱私權及個人資料保護的位階，其於 2016 年 4 月 14 日推出了《一般資料保護規則》（General Data Protection Regulation，GDPR）並取代了《1995 年的歐盟個人資訊保護指令》，根據《歐盟歐洲聯盟運作條約》（Treaty on the functioning of the European Union）之規定[173]，GDPR 的位階是屬於規則（Regulation）而非指令（Directive），因此不需藉由各國進行轉換立法方式來落實相關規定，各會員國直接受拘束力，就立法執行面而言，是加深了對於個人資料保護的重視程度[174]。本文就 GDPR 中可能與智慧家庭應用相關[175]，如自動化蒐集、處理及利用等規定介紹如下：

---

[169] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[170] Michael L. Rustad, Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 Harv. J.L. & Tech. 349, 359 (2015).

[171] *Id.* at 357.

[172] 《歐洲聯盟基本權利憲章》，http://www.europarl.europa.eu/charter/pdf/text_en.pdf（最後瀏覽日：2019/4/19）。

[173]《歐洲聯盟運作條約》第 288 條，https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT（最後瀏覽日：2019/4/19）。

[174] 劉靜怡（2019），〈淺談 GDPR 的國際衝擊及其可能因應之道〉，《月旦法學雜誌》，第 286 期，頁 5。

[175] 特別說明歐盟於 2017 年 10 月提出了《電子隱私規則》（Regulation on Privacy and Electronic Communications）規範電子通訊之隱私權議題，然因仍未獲通過，本文暫不討論。另參考歐盟委員會網站，https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010（最後瀏覽日：2019/7/25）。



DOI:10.6814/NCCU201900793

第一目 個人資料定義與分類

GDPR 在 Article 4(1)定義了什麼是個人資料（Personal Data），係指「得以直接或間接地識別特定自然人之任何資訊」，並「列舉姓名、身分證字號、定位資訊、網路資訊或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體可識別的要素」[176]。而該特定自然人亦在同條被定義為資料主體（Data Subject），此定義更加清晰表示歐盟在個人資料保護上，期望自然人擁有對其資料的控制權，因此定義為其是資料之主體。

比較特別的是，GDPR 在個人資料定義上，考慮了人工智慧與大數據可能對個人資料的操作，特別寫明「生物特徵識別資料」（Biometric Data）的定義，亦即「透過特定技術處理所得關於資料主體身體、生理或行為特徵而允許或確認其特定識別性之個人資料」，例如臉部圖像或診斷資料[177]。這個生物特徵識別資訊（Biometric Data），也就是本文在第二章說明人工智慧技術時，須由人類或電腦標記出的「特徵值」，除了法條中明文列舉出的臉部圖像、診斷資料運用在辨識技術，亦可能包含運用在語音控制、語音文字轉換的聲音資料，及在活動中人的肢體動作等行為特徵資料。

觀 GDPR Article 5 及 Article 9 的規範模式，其將個人資料大抵上區分為兩類別「一般性個人資料」及「特殊性個人資料（special categories of personal Data），所謂的「特殊性個人資料」是指顯示其種族或人種、政治意見、宗教或哲學信仰或貿易聯盟會員之個人資料、基因資料、生物特徵識別資料、與健康相關或與自然人之性生活或性傾向有關之個人資料[178]；而「一般性個人資料」則是非

[176] GDPR, Article 4(1). 翻譯另參照國家發展委員會網，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9iNGZiZTA0OS1jYWQ1LTQ3MGEtYjhlMy00ZGU0NjhmOWIxMGMucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5pys5paH6YOo5YiGLnBkZg%3d%3d&icon=..pdf（最後瀏覽日：2019/4/22）。

[177] GDPR, Article 4(14). 翻譯另參照國家發展委員會網，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9iNGZiZTA0OS1jYWQ1LTQ3MGEtYjhlMy00ZGU0NjhmOWIxMGMucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5pys5paH6YOo5YiGLnBkZg%3d%3d&icon=..pdf（最後瀏覽日：2019/4/22）。

[178] GDPR, Article 9(1).



DOI:10.6814/NCCU201900793

屬於特殊性個人資料者外之個人資料均屬之。就「特殊性個人資料」，根據 Article 9 之規定除有 Article 9（2）列舉之事由外，原則上禁止處理；而「一般性個人資料」，則是符合 Article 5 之要求即可進行處理，其要求包含應保持合法性、公正性及透明度、目的限制原則、最小化蒐集原則等，且資料控制者（Data Controller）就是否符合以上要求負擔舉證責任[179]。

第二目 當事人同意與告知義務

GDPR 針對個人資料之蒐集，強調資料控制者須善盡告知義務且取得資料主體的同意，正如同其他國家個人資料保護法制一般。然從文義來看，GDPR 對於同意權及告知義務有更具體、嚴格的定義。

當事人同意（Consent）於 GDPR Article 4(11)中，指資料主體基於其意思，透過聲明（statement）或明確肯定之行動（clear affirmative action），所為自主性（freely given）、特定（specific）、經告知的（informed）及具體明確（unambiguous indication）之表示同意處理與其有關之個人資料[180]。對於當事人同意，GDPR Article 7 設有諸多限制，其中包含在考量自主性（freely given）時，應特別考慮該個人資料之處理是否為履行契約所必要[181]。於處理「特殊性個人資料」時，GDPR Article 9（2）（a）則規定資料控制者須取得資料主體「明確同意」（Explicit consent）之程度。

就告知義務的部分，GDPR 於 Article 14（1）規定資料控制者在向資料主體取得其個人資料時，應提供完整的「應告知資訊」，如資料控制者身分及聯繫方式、資料保護官（Data Protection Officer）聯繫方式、處理目的及法律依據、所

[179] GDPR, Article 5.
[180] GDPR, Article 4(11). 另翻譯參照國家發展委員會網，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9iNGZiZTA0OS1jYWQ1LTQ3MGEtYjhlMy00ZGU0NjhmOWIxMGMucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5pys5paH6YOo5YiGLnBkZg%3d%3d&icon=..pdf（最後瀏覽日：2019/4/22）。
[181] GDPR, Article 7(4).



DOI:10.6814/NCCU201900793

涉及個人資料類型、接收者或接收者類型等[182]。告知方式則規範在 Article 12(1)，要求資料控制者應以簡明、透明、易懂且方便取得之方式，採用清楚簡易之語言，提交上開告知資訊給資料主體[183]。當然承如上開說明，資料控制者須就其已善盡告知義務並取得資料主體之同意，負擔舉證責任。

第三目 自動化決策與當事人權利

資料主體在 GDPR 規範中，擁有資料接近使用權(Article 15)、更正權(Article 16)、刪除權或被遺忘權(Article 17)、限制處理權(Article 18)、資料可攜權(Article 20)及拒絕權(Article 21-22)等當事人權利，藉以彰顯資料主體得以決定、控制其個人資料的流向與影響。因應人工智慧與大數據的應用，GDPR 明文規範「個人化之自動化決策」(automated individual decision-making)應如何處理與管制。其定義自動化決策的過程－「剖析」(profiling)為任何對個人資料之自動化處理行為，包括使用個人資料來分析、評估或預測與該資料主體有關之個人特徵，如工作表現、經濟狀況、健康、個人偏好、興趣、可信度、行為、地點或動作等[184]。

面對到剖析和自動化決策所帶來的影響，GDPR 強調資料主體應有權，不受僅因剖析和自動化決策所造成之法律效果或其他類似重大決策所影響、拘束[185]。因此，GDPR 除在前階段要求資料控制者須符合一定要求使得採用剖析和自動化決策之處理者外，亦特別賦予當事人權利以決定或控制其範圍。在前階段部分，因特徵剖析(profiling)涉及到個人資料的處理，因此 GDPR 強調須取得當事人之同意，若為特殊性資料之處理，如生物特徵識別資料等，原則上為禁止，除非能舉證到已取得當事人明確同意(Explicit consent)或有其他法定事由[186]。此外，在取得資料主體同意前，資料控制者須最遲於第一次溝通時，以清楚與

[182] GDPR, Article 14(1).
[183] GDPR, Article 12(1).
[184] GDPR, Article 4(4).
[185] GDPR, Article 22(1).
[186] GDPR, Article 21(4).



DOI:10.6814/NCCU201900793

其他資訊區別且明顯之方式，提醒資料主體注意其享有拒絕之權利，始算善盡其告知義務[187]。即便符合一定要求，資料主體可以在剖析和自動化決策過程中或後介入，以最重要的兩個權利為例如下：

壹、接近使用權

當事人享有接近使用權（Right to access），根據 GDPR Article 16(1)之規定，當資料控制者採用剖析和自動化決策進行個人資料處理時，資料主體得以請求資料控制者提供處理過程中之所涉及的邏輯性資訊（例如演算法等）以及可能預設之結果[188]，有論者認為這也代表當事人有權利要求資料控制者解釋處理的過程，因此稱之為「解釋權」（Right to explanation）[189]。

貳、拒絕權

當事人享有拒絕權（Right to Object），若該剖析和自動化決策之處理係因符合公共利益（public interest）或委託行使公權力（in the exercise of official authority）所必須者，或追求正當法律利益（legitimate interests）之目的所必須者，資料主體仍有權基於與其具體情況有關之理由，隨時拒絕之[190]；若該剖析和自動化決策之處理係因直接行銷目的者，該資料主體則不須附理由，隨時得拒絕資料控制者基於行銷目的進行個人資料處理[191]，且在資料主體提出反對的意思時，即須立即停止其個人資料之處理。

第四目 設計及預設資料保護

GDPR 針對資料控制者賦加其在處理個人資料之義務，亦即資料控制者應採取適當科技保護措施和組織規範，來確保其已遵循 GDPR 之要求[192]。此外，GDPR Article 25 提出了「從設計著手保護隱私」（Privacy by Design）和「使隱

[187] GDPR, Article 21(3).
[188] GDPR, Article 16(1)(h).
[189] 同註 174，頁 13-14。
[190] GDPR, Article 21(1).
[191] GDPR, Article 21(2).
[192] GDPR, Article 24(1).



DOI:10.6814/NCCU201900793

私成為預設機制」（Privacy by Default）兩個概念。

前者「從設計著手保護隱私」（Privacy by Design）是指，資料控制者或著是企業在創造新技術、新產品時，研發人員須考慮考量到現有技術、執行成本以及個人資料處理之性質、範圍、內容及目的、可能造成當事人隱私風險，並牢記個資蒐集運用應符合最小化原則[193]。後者「使隱私成為預設機制」（Privacy by Default）是指，資料控制者應採取適當科技措施和組織規範，以確保該個人資料之蒐集符合處理之特定目的，且應考量涉及的個人資料量、處理程度、存儲時間和可訪問性等，讓資料主體在一開始使用時不需透過更改設定，即在系統預設的情形下，就受到 GDPR 程度之保護[194]。透過要求資料控制者再提供產品及服務時，考量隱私權之設計及預設，更能增強對於資料主體的個人資料保護政策。

第五目 資料保護影響評估

面對使用人工智慧和大數據分析的情形日益增加，GDPR 要求資料控制者應主動進行資料保護影響評估（Data Protection Impact Assessment），亦指針對將使用新科技之處理方式，如人工智慧和大數據分析等，資料控制者應於考量該處理之本質、範圍、使用情形及目的、風險時，一併實行該處理對於個人資料保護之影響評估[195]。GDPR 於 Article 35(3)載明，於下列情形應執行資料保護影響評估：

1. 使用剖析和自動化決策進行大規模且系統性的個人特徵評估時，且該個人特徵評估將會對該自然人產生法律效果或其他重大影響。
2. 處理大量之特殊性個人資料或個人犯罪資料。
3. 以系統性方式大規模監控公共場所。

從上可看出，GDPR 針對使用人工智慧和大數據分析的企業，特別要求他們

[193] GDPR, Article 25(1).
[194] GDPR, Article 25(2).
[195] GDPR, Article 35(1).



DOI:10.6814/NCCU201900793

應進行資料保護影響評估，且應設置個人資料保護官，並於進行評估時尋求個人資料保護官之意見[196]。藉以透過此種風險評估機制以及專業人員的引進，從企業內部落實個人資料保護的管理制度。

第二款 人工智慧道德準則 Ethics guidelines for trustworthy AI

歐盟委員會（European Commission）於 2018 年 6 月組成人工智慧專家小組（High-Level Expert Group on Artificial Intelligence，AI HLEG）著手針對人工智慧（AI）議題規劃發展戰略，並草擬法遵方向[197]。AI HLEG 在 2019 年 4 月推出正式版的《人工智慧道德準則》(Ethics guidelines for trustworthy AI）[198]，目的在於促進可信賴 AI 之發展，並表示作為可信賴 AI 因具備三個構成要件:(1）合法的（Lawful），亦即 AI 應尊重人類的基本權利，並遵守法規；(2）道德的（Ethical），也就是 AI 應遵守道德原則和價值觀（3）技術穩健的（Robust），係指因從技術層面確保 AI 是穩健的而不造成傷害[199]。《人工智慧道德準則》建構出一個遵循架構（Framework），分成三個章節，從抽象到具體：第一部分，提及可信賴 AI 因遵循的基本權利、原則和價值觀；第二部分，列出了對於可信賴 AI 的七個要求，如人力監督、具技術穩健性和安全性、隱私權和數據治理、透明度、多樣性、非歧視和公平性、創造環境和社會福祉、責任等，亦包含對於技術方法與非技術方法的規定；最後在第三部分，提供具體詳盡的評估表，用來審核是否達成「可信賴 AI」的規範[200]。其中《人工智慧道德準則》亦著重在隱私權與數據治理（Privacy and Data Governance）的議題上，本文將著重介紹此部分之內容與要求。

---

[196] GDPR, Article 35(2).
[197] 歐盟委員會網站，https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1#privacy（最後瀏覽日：2019/4/24）。
[198] 歐盟委員會網站，https://ec.europa.eu/futurium/en/ai-alliance-consultation（最後瀏覽日：2019/4/24）。
[199] High-Level Expert Group on Artificial Intelligence (2019), *Ethics guidelines for trustworthy AI*, 2, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58477.
[200] *Id.* 2-3.



DOI:10.6814/NCCU201900793

《人工智慧道德準則》在隱私權與數據治理（Privacy and Data Governance）議題上，表示代表可信賴 AI 應尊重人類隱私權、重視資料品質及完整性以及人類對資料的訪問權限（Including respect for privacy, quality and integrity of Data, and access to Data）[201]，分述如下：

第一目 隱私權及個人資料保護

在隱私權及個人資料保護上，AI 系統須在整個運作生命週期的所有過程中保護隱私權及個人資料，包含從最開始蒐集用戶所提供之資料及在與用戶互動的過程中產生的用戶資料[202]。舉例而言，AI 系統可能會透過人類行為記錄，推斷個人的偏好、性取向、年齡、性別、宗教或政治觀點，因此為了使人類相信 AI 系統的運作，AI 系統就必須確保蒐集不會被用於非法之處或是產生不公平地歧視的疑慮[203]。《人工智慧道德準則》在第三章透過具體評估表，要求審查以下事項作為評估[204]：

1. 根據您實際使用的案例，您是否建立了機制，允許其他人在 AI 系統的資料蒐集（機器訓練和操作）、處理過程中，標記與隱私或個人資料保護相關的問題？
2. 您是否評估了資料庫中，資料的類型和範圍（例如它們是否包含個人資料）？
3. 您是否考慮過如何開發 AI 系統？是否在沒有或極少使用特殊性個人資料的情況下，訓練該 AI 模型？
4. 您是否根據實際使用的案例，建立能即時通報和控制個人資料的機制（例如有效同意和撤銷的可能性）？
5. 您是否採取措施增強隱私保護功能（例如採用加密、去連結化和彙整）？

[201] *Id.* 14.
[202] *Id.* 17.
[203] *Id.*
[204] *Id.* 28.



DOI:10.6814/NCCU201900793

6. 如果您設有個人資料保護官（Data Protection Officer），您是否在 AI 系統早期階段讓其參與運作？

第二目 資料品質及完整性

在資料品質及完整性這個要求上，強調資料質量會影響 AI 系統的性能，若蒐集資料的過程中資料質量不佳，可能會導致最終產生社會構造的偏差、不准確和錯誤的資訊發生，因此這個問題須在蒐集資料及訓練 AI 系統的過程中改善[205]。此外，AI 系統亦應確保資料的完整性，必須在每個步驟（例如規劃、訓練、測試的過程中，確認並記錄所使用的流程和資料庫[206]，以避免歧視性或不公平的問題。在具體評估表中，得以運用以下問題進行審查[207]：

1. 您的系統是否符合與廣泛使用的相關通訊標準（例如 ISO、IEEE 等）一致？
2. 您是否建立了個人資料蒐集、儲存、處理和利用的監督機制？
3. 您是否已評估所使用的外部資料質量？
4. 您是否透過定義流程，來確保資料質量和完整性？您考慮過其他流程嗎？您如何驗證資料庫未曾遭到入侵？

第三目 資料訪問權限

在處理個人資料的過程中，應建立資料訪問權限的管理制度，且該管理制度應寫明誰具備訪問權限、什麼樣的資料德被訪問以及在何種情況下得以訪問等內容[208]。針對該管理制度，《人工智慧道德準則》表示因僅具備能力、訪問需求的合格人員才能被授與該權限[209]，其具體評估內容為[210]：

---

[205] *Id.* 17.
[206] *Id.*
[207] *Id.* 28.
[208] *Id.* 17.
[209] *Id.*
[210] *Id.* 28.



DOI:10.6814/NCCU201900793

1. 您遵循哪些通訊標準、流程和程序，來管理和確保數據治理？
2. 您是否評估了誰在什麼情況下，得以訪問用戶資料？
3. 您是否確保這些具備訪問權限的人員，具備了解資料保護政策的能力與資格？
4. 您是否確實採用監督機制，來記錄資料訪問的時間、地點、方式、人員和目的？

第四目 人工智慧識別及持續追蹤問題

AI 作為可以使大眾及私法人機構有效地識別個人的方法，其中 AI 識別技術中特別受到關注的是，臉部辨識和使用生物辨識或其他非自願識別方法，如謊言檢測、通過微表情偵測的性格評估、自動語音檢測等[211]。AI 識別技術可能產生的影響亦有正面及負面的效果，《人工智慧道德準則》認為若可信賴 AI 的運用符合道德原則極為正面理想的效果，例如運用在偵測欺詐、洗錢或恐怖主義、洗錢行為方面。然而，自動化識別的負面笑果，就是可能引起大眾對於隱私的強烈關注及法律問題，因為大眾對於它可能產生的心理和社會文化影響仍無法預估[212]。

因此，《人工智慧道德準則》認為應清楚地定義 AI，並且區分出是何時以及如何能使用「自動化識別」、「持續追蹤個人」及「目標監視」和「大規模監視」的界線[213]。必須透過現行法律來確證這些技術應用符合界線內，假設這些技術應用的法律依據是同意（Consent），則必須證明這樣的同意是「明確且經核可的同意」（meaningful and verified consent），這樣的機制也適用於經去連結化的個人資料（anonymous personal Data）經再識別化（re-personalized）的情形[214]。

[211] *Id.* 33.
[212] *Id.*
[213] *Id.* 34.
[214] *Id.*



DOI:10.6814/NCCU201900793

## 第二項 美國

### 第一款 憲法增修條文第四條 The Fourth Amendment

在美國談論到隱私權時，憲法增修條文第四條（The Fourth Amendment）總會映入眼簾。美國憲法增修條文第四條的內容並無明確指出隱私權（Privacy）一詞，而是表示：「人民享有其身體、住宅、文件和財產不受無理搜查和扣押的權利，不得侵犯…」（The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…）[215]，強調人民不受無令狀搜索之侵擾。在 1967 年 Katz 一案中，人民不受無令狀搜索之侵擾是基於對隱私權的保護，而被告是否受到隱私權之保護取得於其是否具有「合理隱私期待」（reasonable expectation of privacy），包含質其對於經搜索或扣押之區域及物件有主觀隱私期待；且被告的主觀隱私期待對社會來說是客觀合理的[216]。

然而，美國憲法增修條文第四條雖然凸顯了隱私權的重要性，但是卻始終圍繞在政府對於人民身體財產侵害一環。有論者認為這是增修條文第四條的死亡（death of the Fourth Amendment），因為在 Katz v. United State 中，最高法院定義出了「第三人原則」（Third Party Doctrine），亦指如果一個人自願的交出提交個人訊息與第三人，則其不得享有隱私權的期待利益[217]。在這種情況下，消費者其實在使用商品與服務的情形下，很容易交出自己的個人資料（personally identifiable information，PII），進而受到第三人原則拘束，喪失了美國憲法增修條文第四條隱私權的保護。面對美國憲法增修條文第四條的漏洞，美國對於消費者隱私保護法制仍有發展，方法上與歐盟大為不同，詳如後述。

---

[215] 康乃爾法學院網站，https://www.law.cornell.edu/constitution/fourth_amendment（最後瀏覽日：2019/4/24）。

[216] 林利芝（2016），〈Katz v. United States（三）－電子監聽科技侵犯個人隱私的經典案例〉，《台灣法學雜誌》，第 303 期，頁 171。

[217] Morgan Hochheiser, *The Truth Behind Data Collection and Analysis*, 32 J. Marshall J. Info. Tech. & Privacy L. 32, 40(2015).



DOI:10.6814/NCCU201900793

第二款　消費者隱私保護法制與草案

第一目 現行消費者隱私保護法制

如同前面所說明的，與大陸法系認為隱私權是基本人權不同，英美法系之代表美國從自由權的概念出發。就政府對於刺探或侵害人民隱私的問題，自 1967 年 Katz v. United State 一案之後，美國於 1974 年制定隱私法（Privacy Act of 1974）加以管制[218]。而私人間的個人資料問題，雖然有第三人原則的適用，但美國是透過市場機制調節方式，由業者自行制定自律規範（Code of Conducts）來處理個人資料的問題，並認為業者最能制定符合市場需求的自律準則，並能快速因應經濟及科技發展而調整[219]。

然而，這樣的管制相較於歐盟為寬鬆，產生的消費者隱私問題日益浮濫，因此美國於 2000 年之後，採取部門立法模式（sectoral approach），按特殊性個人資料的種類於不同類型的法律之中規範個人資料的使用限制[220]，如電信類的通訊資料規範在「電子通訊隱私法」（Electronic Communications Privacy Act）[221]，金融類的財務資料規範在「金融現代化法」（Gramm–Leach–Bliley Act）[222]，醫療類的健康資料規範在「醫療保險攜帶和責任法」（Health Insurance Portability and Accountability Act）[223]，教育類的青少年網路資料規範在「兒童線上隱私保護法」（Children's Online Privacy Protection Act）[224]。一般消費者隱私訴訟產生的時候，係用《聯邦貿易委員會法》（Federal Trade Commission Act[225]）來解決[226]。具體而言，乃由聯邦貿易委員會（Federal Trade Commission，FTC）根據

---

[218] 美國司法部網站，https://www.justice.gov/opcl/privacy-act-1974（最後瀏覽日：2019/4/25）。
[219] 翁清坤（2018），〈賦予當事人個人資料財產權地位之優勢與侷限:以美國法為中心〉，《臺大法學論叢》，第 47 卷第 3 期，頁 959-960。
[220] 同前註，頁 960。
[221] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.
[222] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
[223] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.
[224] hildren's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2006).
[225] 15 U.S.C. § 45 (1982).
[226] Hochheiser, *supra* note 217, at 35.



DOI:10.6814/NCCU201900793

《聯邦貿易委員會法》15 U.S.C.§45 之規定，負責管制並審查該企業或個人是否以不真實的隱私安全政策進行商業行為，而認定其有任一「不公平競爭行為（unfair methods of competition in or affecting commerce）或詐罔行為（deceptive acts or practices in or affecting commerce）」者[227]。若 FTC 認定其違反 15 U.S.C. §45 之規定者，便會採取行政處分之處罰（Injunctive Remedies），如罰款（Fine）、禁制令（Injunction）[228]。

第二目 消費者隱私法草案

鑑於歐盟於 2015 年討論草擬 GDPR 之後，歐巴馬總統（Barack H. Obama）於同年推出《2015 年消費者隱私法草案》Consumer Privacy Bill of Rights of 2015）[229]，惟由於國會認為該法案定制過於寬鬆、保留過多空間與產業決定，因此未獲實現[230]。然而，從歐巴馬總統提倡以在《2015 年消費者隱私法草案》中，仍不難看出美國有試圖欲跳出將隱私權幾乎交由市場機制調節的作法，用專法方式以呼應在網路與大數據時代下，國際上對於隱私權保護手段提升的趨勢。

《2015 年消費者隱私法草案》在內容上強調幾個點：個人控制權（Individual Control）、透明度（Transparency）、安全性（Security）、尊重完整性（respect for context）、訪問權限與準確性（access and accuracy）、注重資料蒐集（focused collection）和責任（Accountability）[231]。簡言之，消費者有權控制其被蒐集的個人資料，了解受規範主體如何處理使用該個人資料，採取適當措施確保受規範主體遵守法令。而受規範的主體（如企業），在處理消費者隱私時應具備透明性，例如提供簡單明瞭的隱私政策，介紹個人資料揭露及存取機制，以讓消費

[227] *Id.*
[228] Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 541 (2019).
[229] The Consumer Privacy Bill of Rights Act of 2015 was proposed by the Persident Obama in April 2015, and did not receive a congressional sponsor.
[230] 資策會科技法律所網站，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=148&d=6852（最後瀏覽日：2019/4/27）。
[231] Kulevska, *supra* note 170, at 378.



DOI:10.6814/NCCU201900793

者能了解個人資料是如何被蒐集及使用。

在後續 2018 年，參議院民主黨（Senate Democrats）亦推出了《同意法案》（The Customer Online Notification for Stopping Edge-provider Network Transgressions Act，CONSENT Act）[232]，希望運用聯邦立法的方式管制個人資料（PII）被販售運用的問題，如邊際服務商（edge provider）蒐集個人資料時，分享或出售該個人資料之前，應獲得該人的明確同意（opt-in consent），且需要向該資料主體詳細說明、通知其個人資料使用、共享或銷售的所有方式[233]，邊際服務商的定義非常廣泛，包含運用網路直接、間接連接到設備並提供服務的人[234]，根據此定義提供智慧家庭服務的業者、平台廠均在範圍內[235]。目前《同意法案》仍審理中，其雖然精簡，不如 GDPR 詳盡明確，但可以看出美國越發重視私人間利用個人資料問題，以及相應的隱私權保護手段。

## 第三節　台灣個人資料保護法

### 第一項 個人資料定義與分類

根據《個人資料保護法》第 2 條 1 款之規定，個人資料係指「自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料」。其中，台灣根據同法第 6 條之規定，又將有關病歷、醫療、基因、性生活、健康檢查及犯罪前科等個人資料，認定為特殊性個人資料[236]。從第 2 條的立法模式來看，台灣除了將個人

[232] S. 2639, 115th Cong. (2017-2018).
[233] *Id.* § 2 (b)(2)(B).
[234] *Id.* § 2 (a)(5)(B)(ii).
[235] Comparitech 網站，https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/（最後瀏覽日：2019/4/29）。
[236] 劉定基（2010），〈「個人資料保護法」初論〉，《台灣法學雜誌》，第 159 期，頁 2。



DOI:10.6814/NCCU201900793

資料區分為一般資料及敏感性資料以外，亦可將個人資料區分為二種：可直接識別之個人資料及可間接識別之個人資料，就「可間接識別之個人資料」，根據個人資料保護法施行細則第 3 條規定，係指與其他資料對照、組合、連結等，始能識別該特定之個人的資料[237]。然有論者認為，台灣實務見解對於「個人資料是否具有識別性」之認定十分分歧，採取肯定見解者，重視個人資訊隱私權之保護，而採否定見解者，如同法務部 103 年 11 月 17 日法律字第 10303513040 號函：「個人資料保護法第 1、2、16、20 條規定參照，如將公務機關保有的個人資料運用技術去識別化而呈現方式已無從直接或間接識別特定個人，即非屬個人資料…」，強調個資之合理利用，一經去識別化或無法識別者，即不屬於個人資料，不受個人資料保護法之規範[238]。就此實務見解，學界採取不同看法，認為去識別化是個人資料的蒐集、處理與利用的合法手段，即使經過去識別化的資料，仍是屬於個人資料[239]。

就一般性個人資料之蒐集、處理或利用，台灣《個人資料保護法》第 5 條規定：「應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」就特殊性個人資料的部分，則是原則上禁止蒐集，除非有符合下列任一條件者[240]：

一、法律明文規定。

二、屬於公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

三、當事人自行公開或其他已合法公開之個人資料。

---

[237] 同註 163，頁 90。

[238] 范姜真媺（2017），〈大數據時代下個人資料範圍之再檢討—以日本為借鏡〉，《東吳法律學報》，第 29 卷第 2 期，頁 28。

[239] 李建良（2017），〈資料流向與管控環節-個資保護 ABC〉，《月旦法學雜誌》，第 272 期，頁 26。

[240] 個人資料保護法第 6 條。



DOI:10.6814/NCCU201900793

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其方式無從識別特定之當事人。

五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

### 第二項 當事人同意與告知義務

《個人資料保護法》中於 15、16、19、20 條，強調「取得當事人同意」的規定，係源自於控制理論的概念及釋字 603 號解釋：「保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權。」於蒐集及處理時之當事人同意，係指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示[241]。若該個人資料之利用，不在蒐集之目的範圍時，須由當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，再行單獨所為之意思表示者，始達同意之效果[242]。關於當事人同意，台灣法保護的程度較 GDPR 高，除了該同意須明確以外，仍須以書面形式為之[243]。有論者強調同意須為當事人自主、自由的決定，也就是當事人在決定過程中沒有被詐欺、脅迫等情事發生，若今日當事人拒絕同意將遭受重大不利益，或其事實上沒有選擇的餘地而有顯失公平的情形，則同意的效力將會有疑慮[244]。

而在蒐集其個人資料、取得其同意的同時，應善盡告知義務，包含應明確告

[241] 個人資料保護法第 7 條 1 項。
[242] 個人資料保護法第 7 條 2 項。
[243] 個人資料保護法第 6 條 2 項。
[244] 劉定基（2013），〈析論個人資料保護法上「當事人同意」的概念〉，《月旦法學雜誌》，第 218 期，頁 164-165。



DOI:10.6814/NCCU201900793

知當事人其機關名稱、蒐集之目的、蒐集之個人資料類別、個人資料利用之期間、地區、對象、方式以及當事人依得行使之權利及方式等[245]，當然機關也可以明確說明當事人若不提供個人資料時，可能對其權益之影響，例如無法使用完整商品與服務。其告知的方法，包含言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式均屬之[246]。

### 第三項 當事人權利與適當安全措施

根據《個人資料保護法》第 3 條，當事人就其個人資料，享有查詢或請求閱覽（接近使用權）、請求製給複製本（接近使用權）、請求補充或更正（補充更正權）、請求停止蒐集、處理或利用（停止權）及請求刪除（刪除權）等權利，此乃釋字 603 號解釋保障「人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權」之展現。再者，若企業將當事人之個人資料用於行銷時，則當事人亦可以主張拒絕權[247]。台灣《個人資料保護法》關於自動化剖析並無描繪，但就台灣停止權及刪除權的定義而言，應包含當事人得以停止或拒絕機關使用剖析和自動化決策的行為。

對於機關蒐集、處理及利用個人資料者，其須採取適當安全措施來保護其個人資料不被入侵、外洩，根據個人資料保護法施行細則第 12 條之規定，得包括配置管理之人員及相當資源、界定個人資料之範圍、個人資料之風險評估及管理機制、事故之預防、通報及應變機制、個人資料蒐集、處理及利用之內部管理程序、資料安全管理及人員管理、認知宣導及教育訓練、設備安全管理、資料安全稽核機制、使用紀錄、軌跡資料及證據保存、個人資料安全維護之整體持續改善等，以上並非全部需具備，而係根據其所欲達成之個人資料保護目的間，按比例原則認定其是否已具備適當措施。這個作法與 GDPR 具體要求設置 DPO，並進

[245] 個人資料保護法第 8 條。
[246] 個人資料保護法施行細則第 16 條。
[247] 個人資料保護法第 20 條 2 項。



DOI:10.6814/NCCU201900793

行資料保護影響評估不同，就保護程度上，台灣要求的似乎並非嚴格。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

# 第四章　智慧家庭應用之消費者隱私爭議

## 第一節　物聯網技術產生的資安風險

當個人智慧終端設備能發展成智慧家庭設備時，個人智慧終端設備的安全性問題，是消費者最在意，也是智慧家庭關切的問題[248]。智慧家庭的驅動是靠物聯網的技術產生，就如同前面第二章所談到的可分為感知層、網路層和應用層，其中「網路層」靠的是網路傳輸技術，即使是使用不同的通訊協定，仍然須透過該通訊媒介來進行資訊的傳遞與控制。現在有可用於智慧家庭的通訊協定非常多元，如藍牙、Zigbee、以太網、Wifi 等均屬之，每個通訊協定或我們稱之為媒介均有自己的優點和缺點，但面對安全管理方面也都有重大挑戰[249]。此外，目前大多數人也對於智慧家庭的來源與應用，也就是對「應用層」中大數據安全性存在嚴重疑慮，認為大數據應用不安全[250]。根據歐盟第 29 條資料保護工作組（Article 29 Working Party）的調查結果，物聯網資訊安全問題，通常來自於資料蒐集過程的「感知層」，在目前設備商大多數採用的感測器中，主要關注在電池耗能低及體積最小化的功能，因此根本無法在感測器上，建立可信賴的加密安全措施[251]。基於此，本文將討論在資料蒐集及傳輸過程中，也就是感知層及網路層最常面臨到的三種威脅：機密性威脅、驗證威脅及接近使用威脅，進而分析潛在的風險。

### 第一項 機密性威脅

機密性（Confidentiality）係指使資料具備隱密性，讓僅經授權的用戶（人和電

---

248 Dongpo Zhang, *Big Data Security and Privacy Protection*, PROCEEDINGS OF THE 8TH INTERNATIONAL CONFERENCE ON MANAGEMENT AND COMPUTER SCIENCE, 242(2018).

249 Huichen Lin & Neil W. Bergmann, *IoT privacy and security challenges for smart home environments*, 7(3) INFO. 44, 46(2016).

250 Zhang, *supra* note 248, at 276.

251 Ellen P. Goodman, *THE ATOMIC AGE OF DATA: POLICIES FOR THE INTERNET OF THINGS*, 42(2015).



DOI:10.6814/NCCU201900793

腦）始可接觸到該資料[252]，這也是智慧家庭使用者最在意的問題之一。在智慧家庭網路上進行資料傳輸的過程中，若是以未加密方式傳輸個人資料，只要一有網絡配置錯誤的情形發生，就可能使這些個人資料透過無線網絡被全世界的人知曉[253]。因此，在運用物聯網進行資料資料傳輸的過程中，使用「加密功能」以確保資料安全的是非常重要的，而密碼學（Cryptography）正是實現此項「機密性和加密功能」的關鍵技術[254]。

智慧家庭的運作通常建立在一個內網平台上，以訪談為例，就是由【A 公司】這個系統商來營運，這樣的內網平台其實是屬於封閉性的網路。然而在不同的設備商，他們本身的設備也含有自己的訊號器，例如與【A 公司】平台串聯的設備商【P 公司】就有自己的資料庫和機房，可透過兩種模式將資料傳輸出去，其一是透過【A 公司】的網路，根據既定的協定方式轉換出去；其二可能是透過本身其設備連接的網路。每一個服務商在運行過程中，僅保證其服務端的資訊安全，例如【A 公司】僅保證從智慧家庭端到【A 公司】機房的安全，若該資料傳輸的位置是向國內、外任一設備商的機房，則會改透過任一家 ISP( Internet Service Provider )的外部網路，該系統端的安全性則存有疑慮[255]，屬於機密性的威脅。

所謂的機密性威脅（Confidentiality threats），是指導致特殊性資料（Sensitive Data）洩露的風險[256]，例如家庭監控系統如果遭入侵或傳輸過程中資料遭擷取，可能得以從用戶日常的吃藥習慣、症狀，判定其犯有何種疾病。當然，即便是一般性個人資料遭到入侵，雖然危險性不如特殊性個人資料受到關注，然而對於每個人來說，都會覺得他們的隱私仍有明顯威脅存在。舉例來說，內部家庭溫度、濕度設定的習慣，可用於判定房屋內是否有人，有心人士可能拿來作為是否入室盜竊的工具[257]。但若是單純的密碼丟失，而非遭到外力入侵者，即非屬於機密性威脅，而歸入

[252] Bergmann, *supra* note 249, at 45.
[253] Goodman, *supra* note 251,at 40.
[254] *See* Bergmann, *supra* note 249, at 45.
[255] 參見附件一訪談紀錄第二段第 36-60 行。
[256] *See* Bergmann, *supra* note 249, at 47.
[257] *See Id.*



DOI:10.6814/NCCU201900793

到近用威脅。

### 第二項 驗證威脅

驗證（Authentication）是用於驗證該資料未在傳輸過程中經篡改，並且可以驗證資料是否由原發出者所發送的[258]。根據訪談，我們可以了解資料可能區分為許多類型的資訊，但就傳輸訊號來看，通常可大致上分成類比訊號（Analog signal）跟數位訊號（Digital signal）二者，以機器使用的頻率跟耗能來說會使用類比訊號進行傳輸，以聲音、影像等資料來說，會使用數位訊號進行傳輸[259]。後者需要透過加密變成封包的方式，來確保安全性，而封包則由接收者透過密碼解密來讀取資料，若在傳輸的過程中封包遭到破壞，就很有可能出現資料竄改的問題，尤其是語音資料的解密序列是非常重要的，如果序列錯誤，則極有可能改變原來的意思或是讓原始資料的意義滅失，這便是驗證方面的威脅。

驗證威脅（Authentication threats），係指資料或是指令被篡改的風險，例如「查看警報」的指令如果在傳輸過程中被竄改成「開啟警報」，則該系統警報可能會讓門禁開關的控制器，誤以為存在緊急情況並自動打開門窗作為緊急逃生使用，然而實際上卻可能造成非法進入情形，而有安全性威脅[260]。舉另外例子來看，在智慧家庭的物聯網網路底下，駭客很容易可以操控設備或直接追蹤到用戶的位置，這種模式很有可能對人身安全構成直接威脅[261]，例如美國俄亥俄州一對家長發現，一名駭客曾利用嬰兒監控服務（Baby Monitor）的漏洞，透過監視器上的麥克風，向熟睡的幼兒大喊大叫，或是另一個具體明顯但非智慧家庭的事件，2015 年 7 月克萊斯勒（Chrysler Group LLC）就證明過，有一群研究人員曾透過遠端駭客攻擊來控制

---

[258] Bergmann, *supra* note 249, at 45.
[259] 參考附件一訪談紀錄第十二段第 17 行開始。
[260] Bergmann, *supra* note 249, at 47.
[261] Swaroop Poudel, *Internet of things: underlying technologies, interoperability, and threats to privacy and security*, 31 Berkeley Tech. LJ 997, 1015(2016).



DOI:10.6814/NCCU201900793

旗下自動駕駛吉普車的轉向和啟動等，而有召回的案例[262]。

從另一個觀點來看這個問題，為了把智慧家庭的應用做到最廣，開放物聯網串聯技術是最快的方法，可以更好地促進競爭，並達到服務創新[263]。然而，當物聯網串聯技術被開放，許多應用程序可能可以輕易嵌入系統中，每一個額外的 loT 設備即代表了入侵者多了一個漏洞點可以去入侵[264]。因此，網路越大、越被入侵跟竄改的機率就會越大，這也會使系統面臨額不安全問題，而且為了保護資料完整性、正確性，業者也會要面臨到加強安全性可能會產生的額外維護費用。

### 第三項 近用威脅

近用（Access）是指僅允許經過適當授權的用戶能夠接觸到資料、通訊基礎設施和運算資源，並確保這些經授權的用戶的接近使用權利不會被禁止[265]。而所謂的近用威脅（Access threats）是指有未經許可、授權的用戶能夠接觸到資料、通訊基礎設施和運算資源等情形發生之風險[266]。關於近用威脅，大抵上可分成兩類。

第一類，可能是物聯網設備本身就容易受到攻擊，因為通常這些物聯網設備的製造商，都是消費型的家電廠商，我們扣除語音設備助理來看，通常能串連的家電製造商，大都是傳統的家電廠商，如 Bosch、Panasonic 等，在與平台廠或系統廠相比之下，對於資訊安全的問題就缺乏經驗[267]。

第二類，如同前面所說的，這可能是不適當的密碼管理所造成的。密碼管理在這裡可能再區分成兩種，一種是消費者有手機 App 或平台得以登入帳號管理智慧家庭的設備，在這種有消費者帳號管理的情形，根據 10 種最受消費者歡迎的物聯網應用研究顯示，大部分的設備都存有密碼保護不足、加密不足的問題，大多數人

---

[262] 石立康（2016），〈智慧家庭資安防護技術及解決方案〉，《IEK 產業分析報告》，頁 3。
[263] Goodman, *supra* note 251,at 38.
[264] Poudel, *supra* note 261, at 1015.
[265] Bergmann, *supra* note 249, at 45.
[266] Bergmann, *supra* note 249, at 47.
[267] Poudel, *supra* note 261, at 1015.



DOI:10.6814/NCCU201900793

只有透過蒐集某些類型的個人資料，如姓名、地址、出生日期、身分證字號或信用卡號，就可以輕易拼湊出密碼[268]。其二種，可能就是設備商在建置設備時候的加密碼，這類的問題在於，如果設備商在很難在智慧家庭設備上，安裝定期更新或修補具有自動安全性修復等功能的話，就很容易使它們在使用中暴露出其製造時不存在或預期的威脅。因為這樣的功能通常在他們進行在產品設計、製造時，基於成本的理由，通常不容易被納入考量[269]。

### 第四項 小結

機密性、驗證還是接近使用的威脅，可能是三種智慧家庭市場參與角色，包含通訊服務業、家電廠及平台廠，共同需要面臨的安全性風險。從本文訪談中，我們可以了解到在智慧家庭運作中，通訊服務業不是全然負責網路通訊的安全，負責產品設計的家電廠商以及他們所合作搭配的平台廠，都會有相應的自行通訊網路及消費者帳號設置，在目前市場上的運作模式，都是屬於各廠商須各自承擔其負責運營或是使用的通訊網路安全性問題[270]。但當智慧家庭市場走向平台整合與串聯策略，透過策略結盟的方式讓更多廠商、新創業者群聚，走向互相授權、標準化的方式，即使可能選擇如 IPSO 通訊標準、TaiSEIA 101 通訊標準等大型的標準互相合作，但在細部的安全性又該如何確保？智慧家庭的使用者如果發生資安外洩的事情，在整個策略聯盟的情形下，誰又應該承擔相應的風險？以 IBM 為例，他們建好堅強的後端平台，讓他們廠商可以全面性的在後端進行應用分析，家電廠商 Whirlpool 仍要負擔在產品上的安全性問題，而且他們合作的網路服務業者也要負擔在傳輸過程安全性，然而實際發生用戶資安風險時，這些廠商的責任需如何釐清？從管理層面來看，這些業者除了需要追求通訊協定上統一，更需

[268] Goodman, *supra* note 251,at 40.
[269] Poudel, *supra* note 261, at 1015.
[270] 參考附件一訪談紀錄第二段第 55 行開始。



DOI:10.6814/NCCU201900793

要責任風險減輕的標準。換言之，業者需要一套可遵循的法制化標準，確保他們符合國家、法治的期待，藉以降低潛在的法遵風險、確定運營的成本。

因此，本文的下一節以美國案例為主，將著重在實際具體在智慧市場上運用 AIoT 技術推出產品時，若業者沒有作好資安、隱私權的把關及合理利用，且政府或立法單位在尚未推出合適的準則時，可能發生潛在的合規風險與法律爭議為何。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

## 第二節　智慧家庭應用隱私爭議案例

### 第一項 智慧電錶案：Naperville Smart Meter Awareness v. City of Naperville[271]

#### 第一款　案例事實

本案的原告係一非營利組織（Non-profit organization），反對政府推行智慧電錶的政策，因此對內珀維爾市政府（City of Naperville），提起訴訟主張智慧電錶（smart meters）蒐集個人資料之行為違反美國憲法增修條文第四條（the Fourth Amendment of the U.S. Constitution）及伊利諾伊州憲法第 I 條 6 項（Article I § 6 of the Illinois Constitution）之隱私權保護[272]。本案源自於 2009 年美國復甦與再投資法案（The American Recovery and Reinvestment Act of 2009），爲實現國家電網現代化的目標，該法案提供資金，要求能源部根據智慧電網投資補助計劃提撥給下級政府單位[273]。透過這個計畫，內珀維爾市被選中獲得 1,100 萬美元來更新程式內的電網，並開始採用「智慧電錶」來取代安裝在用戶家中的傳統電錶[274]。

使用傳統電錶的時候，公營事業通常必須每月一次地向用戶蒐集他們的能量消耗資料，也就是我們常見的「抄電錶」作業程序，非常耗費時間和人力[275]。相比之下，智慧電錶能更頻繁地記錄消費情況，通常每月能自動蒐集數千個數值，並透過消費頻率曲線，智能電錶能顯示了家庭內部實際使用電量以及實際使用的各個時間[276]。該資料能夠顯示有關房屋內發生事件的資訊，因為每個家用電器的能量消耗模式或乘載訊號（load signatures）都不同，因此可以由消耗率推敲出用

---

[271] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018).
[272] *Id.* at 523.
[273] *Id.* at 524.
[274] *Id.*
[275] *Id.*
[276] *Id.*



DOI:10.6814/NCCU201900793

戶在家中是使用何種電器[277]，例如冰箱的耗電率與電視、呼吸器或室內燈都不同，研究人員只要將縱向耗能資料與後台端的家電承載資料庫進行比對，就可以預測該家中存在著哪些類型的家電設備以及用戶何時使用這些家電設備[278]。當然資料蒐集頻率以及使用的分析工具複雜程度，會影響到預測結果的精準度[279]。

在推行智慧電網計畫的時候，部分城市允許由居民自行決定是否更換成智慧電錶，然而內珀維爾市政府並無提供用戶選擇餘地，如果內珀維爾市民想在家中使用電力，那他們只能必須從公營事業單位購買，且無法選擇不加入智慧電錶的使用[280]。內珀維爾市政府所安裝的智慧電錶設定，以間隔十五分鐘就蒐集一次用戶的能源使用資料，而且這些資料將資料均存儲長達三年之久[281]。

原告作為非營利組織，是由一群公民所組成，他們將該組織稱為「內珀維爾智慧電錶自覺組識」（Naperville Smart Meter Awareness），並聲稱內珀維爾的智慧電錶顯示出「城市內電能消費者的個人親密細部資訊」，例如人們何時在家、房屋何時空置、人們睡眠時間、飲食習慣、家中使用的特定電器類型以及電動車充電次數等資料，而且這些資料可被用於識別個人旅行的習慣和過往[282]。據於此，原告主張根據美國憲法增修條文第四條之規定，被告內珀維爾市政府蒐集這些資料構成不合理搜查（unreasonable search），以及根據伊利諾伊州憲法第 I 條 6 項之規定，屬於從事不合理搜查和隱私侵犯（unreasonable search and invasion of privacy）行為[283]。

在訴訟過程中，地方法院駁回了原告的兩項主張，當原告要求追加第三項主張的同時，地方法院亦拒絕了這個請求，因為它認為追加訴訟主張是徒勞無功的，因為即使提出了第三項主張，仍然沒有辦法合理地證明被告的行為違反增修條文

[277] *Id.*
[278] *Id.*
[279] *Id.*
[280] *Id.*
[281] *Id.*
[282] *Id.*
[283] *Id.*



DOI:10.6814/NCCU201900793

第四條或違反伊利諾伊州憲法，進而判定原告敗訴[284]。原告基於地方法院拒絕追加速送主張為由，向本案之巡迴上訴法院提起了上訴[285]。

第二款　重要爭點

在本案論證以前，本案法院指出美國憲法增修條文第四條保護的是「人民享有其身體、住宅、文件和財產不受無理搜查和扣押的權利，不得侵犯…」(“the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”)；伊利諾伊州憲法第 I 條 6 項同樣地也保障，人們「享有其人身、住宅、文件及其他財產不受竊聽或不合理搜查、扣押、侵犯隱私或經攔截通訊的權利」(“the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means.”)[286]。基於此聯邦及州憲法上的主張，本案的爭點在於：其一，智慧電錶蒐集資料是為美國憲法增修條文第四條及伊利諾伊州憲法第 I 條 6 項所稱之搜索？其二，若該智慧電錶蒐集資料構成搜索，該搜索是否屬於不合理搜索[287]？ 根據這兩個爭點，於下敘明。

第一目　智慧電錶蒐集資料構成搜索

本案法院首先表示美國憲法增修條文第四條的保護，以前與侵權行為法中的侵入行為（Trespass）有關，但現在判例演進的方式下，美國憲法增修條文第四條的保護在科技的發展中應包括政府應用更複雜技術來進行搜索[288]。進一步來說，過去政府可能要派員物理侵入家中才能進行搜索，知道屋子裡的細節，然而現在憑藉科技技術，政府就可以理解家中的資訊，在這種情形下，即使政府不無進入

[284] *Id.* at 524-25.
[285] *Id.* at 525.
[286] *Id.*
[287] *Id.*
[288] *Id.* at 525-26.



DOI:10.6814/NCCU201900793

房屋內，其只要對家中從事「監控」行為，理解上就算是一種搜索[289]。本案法院引用 Kyllo v. United States[290]為例，執法機關在 *Kyllo* 案中，透過熱影像（thermal images）表現出「車庫屋頂和房屋側牆的溫度」相較於房屋的其他部分較熱，而且也比周圍的房屋溫暖得多，進而推敲出該區域可能種植著大麻[291]。該熱影像設備並沒有直接顯示牆內的人或活動，也不能穿透牆壁或窗戶來顯示屋內人的對話或活動，但最高法院卻認為，在該案中使用蒐集熱影像的行為構成了房屋的搜索[292]。

原告在本案中主張，被告依靠智慧電錶每隔十五分鐘蒐集的耗能資料，能夠顯示人們何時在家、何時離開，何時睡覺、何時吃東西、家中使用什麼類型的家電以及何時使用這些家電，就手段上比起 *Kyllo* 僅是透露出家中的某些物品會以熱量形式散發出大量能量，屬於更為複雜的搜索[293]。*Kyllo* 法院並未採納，其案原告主張任何從蒐集來的資料所推敲出的結論都非屬於搜索的論點[294]。*Kyllo* 案中，執法部門透過熱影像得出「該家庭居住者使用燈在房子裡種植大麻」是基於來自過多熱量，而運用本案被告以智慧電錶每隔十五分鐘蒐集耗能資料的方式，執法機關能夠更加發掘出「該家庭居住者使用燈在房子裡種植大麻」，是根據房屋耗能功率顯示他們正在使用這種燈，這樣的耗能資料蒐集本案法院認為更具有侵入性[295]。當然在 *Kyllo* 案中，最高法院認為當該具有侵入性的技術，是目前廣泛並且一般大眾經常使用（widely available and routinely used by the general public）的技術時，使用該技術並不構成是一種搜索[296]。不過本案法院認為，依靠智慧電錶每隔十五分鐘蒐集的耗能資料這項技術，是由部分高度專業化的電力公司所採用的，並不屬於是一種目前廣泛並且一般大眾經常使用的技術，在這種科技發展

[289] *Id.* at 526.
[290] Kyllo v. United States, 533 U.S. 27 (2001).
[291] Naperville, 900 F.3d at 526.
[292] *Id.*
[293] *Id.*
[294] *Id.*
[295] *Id.*
[296] *Id.* at 526-27.



DOI:10.6814/NCCU201900793

侵害隱私的情形下，本案法院認定這是一個搜索行為[297]。

另外，被告內珀維爾市政府認為，本案應適用第三人理論（third-party doctrine），根據該原則，若是個人自願性地與第三人分享其個人訊息，其屬於放棄了其對於該訊息隱私的期待[298]。據於此，當內珀維爾市政府從第三方（公營事業）蒐集時，不會違反美國憲法增修條文第四條之隱私保護[299]。本案法院反對此見解，因為在蒐集資料過程中，公營事業單位並非第三人的角色，而且即便我們把公營事業單位當作是第三人，本案中電力消費者基於美國復甦與再投資法案所要求的一定只能選擇更換，那就電力消費者而言他們根本沒有選擇[300]。法院也點出，消費者不會願意承擔每天被監控的風險，來換取電力的使用[301]。

第二目　智慧電錶蒐集資料並無構成不合理搜索

本案法院接下來討論的是，被告運用智慧電錶蒐集資料是否構成不合理搜索的這個爭點，如果被告的搜索是合理的（reasonable），那即使被告的搜索缺乏令狀（warrant），也不會違反美國憲法增修條文第四條之隱私保護[302]。本案因為不是刑事調查的問題，因此法院選擇採用透過衡量「對個人美國憲法增修條文第四條隱私利益侵犯程度與促進合法政府利益」（"by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests."）來判定搜索是否屬於合理的（reasonable）[303]。

就個人美國憲法增修條文第四條隱私利益侵犯程度這點，本案法院認為雖然耗能資料與隱私權有相關，且它被蒐集的頻率很高，但跟美國憲法增修條文第四條對家庭搜查的概念比起來是非常輕微的[304]。在本案，被告並不是要基於起訴家庭成員的意圖來蒐集這些資料，蒐集、利用這些資料的人員是該公營事業的從業

297 *Id.* at 527.
298 *Id.*
299 *Id.*
300 *Id.*
301 *Id.*
302 *Id.* at 528.
303 *Id.*
304 *Id.*



DOI:10.6814/NCCU201900793

人員，而非執法單位，因此電力的消費者也沒有因為耗能資料被蒐集而有被起訴的風險[305]。此外，被告蒐集這些資料並沒有實際進入房屋內，根據 Camara v. Municipal Court[306]中最高法院的標準，認定實際進入房屋內會帶來對個人和家庭安全的嚴重威脅（the "serious threat to personal and family security" posed by physical entry），本案中沒有這樣的嚴重威脅[307]。再者，內珀維爾市所修訂的《智慧電網客戶權利規章》（Smart Grid Customer Bill of Rights）中，明確澄清了該市的公營事業單位不會將客戶資料提交給第三方，包括缺乏搜索令的執法單位，因此本案中對於隱私的侵害程度有限[308]。

就智慧電錶所促進合法政府利益這點來看，基本上，電網現代化的計畫是內珀維爾市政府及聯邦政府目前最優先政策，而智慧電錶在電網現代化計畫中扮演著至關重要的角色，例如它們可以使公營事業在電力中斷時更快地恢復服務、提供基於使用時間的電力報價，並可以透過耗能資料的蒐集，分析、鼓勵消費者在高峰需求時期降低用量，也可以減少公營事業的勞力成本，因為不需要派員手抄電錶[309]。因此簡言之，智慧電錶能使公營事業單位降低成本、提供更便宜電力給消費者、鼓勵提高能源效率以及能提高電網穩定性[310]。

綜上所述，在衡量本案中對於隱私的侵害程度有限，以及智慧電錶能帶來的好處來看，本案法院認為被告依靠智慧電錶每隔十五分鐘蒐集的耗能資料是合理的，進而支持地方法院的判決[311]。

## 第二項 智慧電視案：In Re: Vizio, Inc., Consumer Privacy Litigation[312]

### 第一款 案例事實

[305] *Id.*
[306] Camara v. Municipal Court, 387 U.S. 523 (1967).
[307] Naperville, 900 F.3d at 528.
[308] *Id.*
[309] *Id.* at 528-29.
[310] *Id.* at 529.
[311] *Id.*
[312] In Re: Vizio, Inc., Consumer Privacy Litigation, 238 F. Supp. 3d 1204 (C.D. Cal. 2017).



DOI:10.6814/NCCU201900793

被告 Vizio 是智慧電視（Smart TVs）的第二大製造商，這種智慧電視內建有能使消費者能夠連結到網路和服務的軟體，如可連結到 Netflix、Hulu、Pandora 等，這些軟體被稱為 Vizio 網錄應用軟體（Vizio Internet Apps）、網路加值應用軟體（Internet Apps Plus）和智慧投放（SmartCast），能預先裝置在智慧電視內，且能夠自行更新安裝[313]。Vizio 除了販售智慧電視以外，並將針對能連接娛樂、電影、電視節目等功能收取額外費用，因為智慧電視能無時無刻提供消費者直接點播視頻內容[314]。

本案的原告是代表 Vizio 智慧電視的消費者提起訴訟，他們認為 Vizio 的智慧電視在未善盡告知義務的情形下，內建「智慧互動」（Smart Interactivity）這個自動識別內容的軟體，專門來蒐集消費者的歷史觀看內容，這個軟體已蒐集了高 1000 億個「瀏覽紀錄」以及相關消費者詳細個人資料，例如消費者的 IP 地址、郵政編碼、MAC 位址、產品型號、軟硬體版本、芯片組 ID、區域和語言設置以及其他類似能連接到同一網路的設備資訊[315]。「智慧互動」軟體慧將此這些資料傳輸到 Vizio 後端的數據服務平台（Inscape），在該平台上 Vizio 會將「瀏覽紀錄」與現有內容資料庫進行比對，來識別消費者一直在觀看的內容為何，並將所有的資料出售給廣告商和媒體服務商，以便他們能夠在 Vizio 智慧電視以及能連接到同一網路的智慧型手機、平板電腦或電腦上，投放精準的廣告[316]。此外，Vizio 實施了一個遊戲計劃（game plan），將個人與他們的觀看紀錄連結在一起，Vizio 曾公開揭露過一個「可識別數位資訊」（digital identifier），也就是一個 MAC 位址，而這個 MAC 位址通常與個人姓名有關，也能用於辨識特定的地理位置[317]。即使一個 MAC 地址不足以識別某個人，該資料在與 Vizio 公開的其他資料結合時，就可以很容易地識別個人，例如與 IP 地址、郵政編碼、產品型號、軟硬體、芯

[313] *Id.* at 1211.
[314] *Id.*
[315] *Id.*
[316] *Id.*
[317] *Id.* at 1211-12.



DOI:10.6814/NCCU201900793

片組 ID、區域和語言設置等資訊相結合[318]。為了支持這一項論點，原告提供了兩個研究報告證明，研究人員只要透過分析有關這些資料，就能夠識別出相當大比例的個人[319]。原告還指出了 Vizio 自己在股權招募說明書上，強調了 Inscape 數據服務平台是能夠「高度準確地提供大規模、特定的觀看紀錄資料」[320]。

除了強調被告 Vizio 持續透過智慧電視蒐集消費者個人資料，並進行分析比對以外，原告表示被告 Vizio 並沒有在他們的隱私政策上公開揭露這些事情[321]。消費者僅能在「重置和管理」的選單下方，以非常小的字體查看到，Vizio 只會蒐集「非個人」和「匿名」(“non-personal” and “anonymous”)的資料，並且不會將這些資料賣給第三人[322]。例如 Vizio 智慧電視在外包裝上行銷有強調「網路應用」和「網路應用增強版」二種，但卻未提及如果消費者使用這些功能，Vizio 的智慧互動軟體會蒐集和傳播有關其歷史觀看紀錄和可識別的數位資料，而且在設定 Vizio 智慧電視的過程中，消費者也無法自行設置 Vizio 的智慧互動軟體，若消費者要關閉智慧互動軟體，也必須事後在設定選單中自行勾選取消，而在該選單中也沒有描繪具體智慧互動軟體的功能是什麼[323]。更重要的是，只要消費者勾選還原原廠設定，智慧互動軟體的功能也會自動重新啟用，而且 Vizio 並不會主動告知消費者智慧互動軟體的功能已經重新開啟[324]。

原告表示消費者在購買 Vizio 智慧電視時，並未意識到 Vizio 會進行個人資料的蒐集和利用。被告僅提供有關 Vizio 智慧電視的資訊，例如型號、可購買的城市、區域，並解釋如何使用 Vizio 智慧電視觀看視頻內容等[325]。在知悉 Vizio 的智慧互動軟體的功能後，消費者立即停止讓智慧電視連網，或觀看線上的視頻內容，並表示當初如果知道 Vizio 會進行資料蒐集與揭露的話，消費者就不會購買

---

318 *Id.* at 1212.
319 *Id.*
320 *Id.*
321 *Id.*
322 *Id.*
323 *Id.*
324 *Id.* at 1213.
325 *Id.*



DOI:10.6814/NCCU201900793

Vizio 智慧電視，或者會支付較少費用[326]。

基於此，原告根據 13 個州法和聯邦法向被告提起訴訟。就聯邦法而言，原告根據視頻隱私保護法（Video Privacy Protection Act，VPPA）和監聽法（Wiretap Act）提出損害賠償；就州法而言，原告提起侵權行為法（Torts）下之「詐欺與虛偽不實陳述」（Fraud And Negligent Misrepresentation Claims），以及加州消費者法律救濟法（California's Consumers Legal Remedies Act）、加州不正競爭法（California's Unfair Competition Law，UCL）、加州廣告不實法（California's False Advertising Law）、佛州詐欺與不公平貿易行為法（Florida's Deceptive and Unfair Trade Practices Act）、紐約州一般商業法（New York's General Business Law）第 349 和 350 條、麻州一般商業法第 93A 章（Massachusetts's Chapter 93A）、華盛頓州消費者保護法（Washington's Consumer Protection Act）之消費者保護之訴[327]。此外，他們亦根據州法隱私保護（state law privacy claims），如加州憲法（California Constitution）、加州隱私侵害法（California's Invasion of Privacy Act）、麻州隱私法（Massachusetts Privacy Act）和相關州視頻隱私法規等提出訴訟主張，表示被告侵害隱私權[328]。最後，原告亦主張不當得利（unjust enrichment）[329]。

第二款　重要爭點

在本案中，被告提出了駁回原告之訴（motion to dismiss）之主張，表示原告並未提出足夠的證據及主張，以符合美國憲法第三條（Article III）之構成「案件或爭議」（case or controversy）的核心要件，簡言之就是當事人適格的要件[330]。因此，本案著重討論爭點在於：（1）原告之主張是否符合美國憲法第三條（Article III）之要求？（2）原告根據上述法律所提出之主張是否充分[331]？本文將著重在

326 *Id.*
327 *Id.*
328 *Id.*
329 *Id.* at 1214.
330 *Id.*
331 *Id.*



DOI:10.6814/NCCU201900793

與隱私權及個人資料最為相關之主張及法院見解進行介紹與討論。

第一目　美國憲法第三條爭點（Article III Issues）

本案法院開宗明義表示，成立美國憲法第三條之當事人適格要件，為以下三者：（1）事實上損害（Injury in Fact），亦即「具體且特定」和「實際且緊急」的損害，而不是透過推測或假設出的結果，（2）因果關係（Causation），亦即這個損害必須可被追朔到是被告的行為所致，（3）可救濟性，亦即該損害就可以透過司法救濟能被糾正[332]。美國憲法第三條要求傷害必須是具體、真實的，而不能是抽象的，但傷害不一定是有形的，透過我們過往的立法過程與見解，即使是無法量化的傷害也是能成立的[333]。

根據美國國會的立法過程，國會強調隱私侵害是指「不合理和嚴重干擾他人，不將私事告訴他人或不將個人形象、興趣展現給公眾的權利」[334]，且也表示攔截電子通訊資料以及未經授權揭露他人的觀看歷史記錄是非常有害的，因此無形的傷害（Intangible Harms）也能符合美國憲法第三條之要求，該被揭露的人得以據此主張隱私權訴訟[335]。因此，被告主張他們揭露的資訊並非可識別之個人資料，且不具有侵害性，不成立美國憲法第三條之當事人適格要件的主張是不合理的[336]。

第二目　視頻隱私保護法爭點（VPPA Issues）

《視頻隱私保護法》於 1988 年所制定，其 18 U.S.C. § 2710(b)(1)規定：「錄像帶服務提供商（video tape service provider）故意向任何人揭露有關其消費者的任何可識別個人資料（personally identifiable information）者，應對受害者負責.....」[337]。根據同法 18 U.S.C. § 2710(a)(4)規定，所謂的錄像帶服務提供商（video tape

[332] *Id.* at 1215.
[333] *Id.*
[334] *Id.*
[335] *Id.* at 1216.
[336] *Id.* at 1217.
[337] *Id.* at 1220.



DOI:10.6814/NCCU201900793

service provider）是指任何從事跨州或國外貿易、租賃、銷售或交付預先錄製之錄像影帶或類似之視聽物品等業務之人或對該等業務具有影響力之人[338]。在此，本案法院認為是否屬於從事該業務之人，係從其工作內容之重點、職責等方面來觀察[339]。被告抗辯表示在所有交易過程中，只會存在一個錄像帶服務提供商，而他們合作的內容提供商（如 Hulu 或 Netflix 等）確實符合視錄像帶服務提供商之定義，因此 Vizio 僅是提供智慧電視之販售，不屬於視錄像帶服務提供商之定義[340]。再者，被告抗辯如果錄像帶服務提供商的解釋範圍如此之大，進而認定 Vizio 也是視錄像帶服務提供商的話，那現在市面上無數的產品和服務，如運輸服務、藍光播放器、智慧型手機、應用程序商城、有線電視盒、無線路由器、個人電腦、視頻遊戲機、甚至汽車的服務商，也都屬於視錄像帶服務提供商[341]。就此，本案法院表示《視頻隱私保護法》並無明確說明在所有交易過程中，只會存在一個錄像帶服務提供商，被告亦沒有提出明確的解釋關於這個抗辯[342]。另外，本案法院指出被告所提及的這些產品或服務商，大多為極外圍或被動地涉及視頻內容的傳送行為，而難以被合理地解釋成他們的業務包含傳送視頻內容[343]。根據 18 U.S.C. §§ 2710(a)(1)和(b)之規定，錄像帶服務提供商的消費者是指「其商品或服務的承租人、購買者或訂購用戶」，根據此說明，Vizio 確實開發了一種能與消費者進行視頻內容交流的產品，創建了可以直接向消費者提供視頻內容（包括與 Netflix 和 Hulu 等內容提供商達成協議）的生態系，因此符合《視頻隱私保護法》錄像帶服務提供商的定義[344]。

再者，被告主張他們所揭露的資訊並非可識別個人資料（personally identifiable information），而是可識別的設備資料（device identifying information）

[338] *Id.* at 1221.
[339] *Id.*
[340] *Id.* at 1222.
[341] *Id.*
[342] *Id.*
[343] *Id.*
[344] *Id.*



DOI:10.6814/NCCU201900793

[345]。本案法院認為根據國會的立法過程，可清楚看出國會認為《視頻隱私保護法》不僅僅保護一個人的姓名或實際地址，而且根據第一上訴巡迴法院在 Yershov v. Gannett Satellite Info. Network, Inc.[346]案中的見解，認為「可識別個人資料」不只是一個人的姓名而已，仍包涵得以「合理地和可預見地顯示原告曾觀看過的視頻內容有哪些」等資料[347]。在本案中，原告已充分表達 Vizio 的 Inscape 平台揭露了消費者可識別數位資訊（digital identifier），包含一個 MAC 位址，而這個 MAC 位址通常能與個人姓名產生連結性，也能用於辨識特定的地理位置，並在與 Vizio 公開的其他資料結合時，就可以很容易地識別個人，例如與 IP 地址、郵政編碼、產品型號、軟硬體、芯片組 ID、區域和語言設置等資訊相結合的情形下[348]。此外，原告也充分指出了 Vizio 自己在股權招募說明書上，強調了 Inscape 數據服務平台是能夠「高度準確地提供大規模、特定的觀看紀錄資料」，基於上述理由，本案法院認為係爭資料屬於可識別個人資料（personally identifiable information）[349]。

第三目　隱私權侵害爭點（Invasion of Privacy and Intrusion Upon Seclusion Issues）

本案法院認為在原告根據各州隱私權侵害（Invasion of Privacy and Intrusion Upon Seclusion）的主張，其構成要件都是相似的[350]。加州、佛州和華盛頓州都採取相同侵權行為（tort）的定義，亦即（1）有一個故意侵害（intentional intrusion）的行為，而這個行為是以實體或用其他方式故意侵害他人不受侵擾、享受獨自一人的自由權；（2）這個行為對於以客觀第三人（reasonable person）而言，是屬於非常冒犯的（highly offensive）[351]。加州憲法和麻州隱私法在隱私侵害的規範上也有類似的構成要件：（1）當事人有法律上保護之特定隱私利益經識別（“the

[345] *Id.* at 1223.
[346] Yershov v. Gannett Satellite Information Network, Inc., 104 F.Supp.3d 135 (D. Mass. 2015).
[347] In re Vizio, Inc., 238 F. Supp. 3d at 1224.
[348] *Id.* at 1225.
[349] *Id.*
[350] *Id.* at 1232.
[351] *Id.*



DOI:10.6814/NCCU201900793

identification of a specific, legally protected privacy interest”），（2）而該當事人在該特定情形下具有合理隱私期待（“a reasonable expectation of privacy under the circumstances presented”），以及（3）該隱私利益遭被告嚴重侵害（“a sufficiently serious intrusion upon the privacy interest by the defendant”）[352]。就前該所討論的隱私利益（privacy interest），加州已承認兩大類別，包含（1）資訊隱私（information privacy），係指排除他人散佈或濫用其敏感和保密個人資料的權利;（2）自主權（autonomy privacy），係指能根據自我意識做出親密的個人決定或進行個人活動，而不受他人觀察、干涉或介入的權利[353]。基於此，本案法院駁回被告 Vizio 主張原告對於被存取視頻瀏覽紀錄的詳細資料，沒有明顯隱私利益，因為根據上述許多的州均立法保護消費者的視頻觀看紀錄，而本案中原告已特定出「觀看歷史紀錄」這個敏感性的隱私利益[354]。

此外，本案法院指出美國法院一直搖擺不定，是否要將隱私權侵權行為（tort of invasion of privacy）的範圍擴張到例行性蒐集可別識別個人資料（the routine collection of personally identifiable information）的行為[355]。這裡的例行性蒐集可別識別個人資料並非是特殊性的個人資料，本案法院明確指出蒐集親密或特殊性個人資料可能構成極具攻擊性的侵害[356]。在本案，如果被告無視消費者的隱私選擇權卻同時認為自己是尊重消費者隱私權的，那麼對消費者來說，這些例行性的個人資料蒐集可能是非常冒犯的（highly offensive）[357]。另外，原告指出消費者在設定 Vizio 智慧電視的過程中，消費者也無法自行設置 Vizio 的智慧互動軟體，若消費者要關閉智慧互動軟體，也必須事後在設定選單中自行勾選取消（Opt-out），而且只要消費者勾選還原原廠設定，智慧互動軟體的功能也會自動重新啟用，而且 Vizio 並不會主動告知消費者智慧互動軟體的功能已經重新開啟，而這

[352] *Id.*
[353] *Id.*
[354] *Id.*
[355] *Id.* at 1233.
[356] *Id.*
[357] *Id.*



DOI:10.6814/NCCU201900793

些作法都與業界慣例不符合，這些主張已經足以可以斷言被告有高度冒犯（highly offensive）的行為[358]。綜上所述，考慮到被告所蒐集個人資料的數量與性質，並未能尊重消費者的隱私選擇權，以及明顯與行業慣例的不同，原告已充分主張 Vizio 的蒐集行為構成極具攻擊性的侵害[359]。

第三款　本案結論與後續發展

關於本案被告主張駁回原告之訴請求，本案法院一部准許、一部駁回，關於隱私權的侵害部分均駁回，而肯認原告已提出相當事證證明消費者受有侵害[360]。在同年 3 月 23 日，原告提交了他們的第二次訴狀，除了監聽法（Wiretap Act）損害賠償主張未撤銷外，其餘在本案被法院駁回的主張均已去除，被告 Vizio 不久後針對原告第二次訴狀提出了第二次的駁回原告之訴主張（Motion to Dismiss），要求駁回原告的監聽法（Wiretap Act）損害賠償主張和禁令救濟賠償（claims for injunctive relief）的主張，在該案中法院亦駁回被告之主張，然因與消費者隱私之主張較無相關，本文不多加以介紹[361]。美國聯邦貿易委員會（Federal Trade Commission）在與被告協調數月後，在 2018 年 10 月 3 日向法院提出審理「正式和解協議」的請求[362]。該和解金額約為 17,000,000 美元，作為律師費、和解管理人管理費、其他開支及消費者的賠償金，加州聯邦地方法院於 2019 年 1 月 4 日作出裁決（Order）同意雙方和解[363]。

## 第三項 智慧音箱爭議：Amazon Alexa

第一款　背景事實

如同第二章所討論的，Amazon Alexa 在智慧音箱的市佔率極高，Amazon

---

358 *Id.*
359 *Id.*
360 *Id.* at 1234.
361 In re Vizio, Inc., Consumer Privacy Litig., Order Granting Plaintiffs' Motion For Preliminary Approval Of Class Action Settlement, Doc. 282, 4 (C.D. Cal. 2019).
362 *Id.*
363 *Id.*



DOI:10.6814/NCCU201900793

Alexa 在與消費者互動的過程中，是以「語音傳輸」方式蒐集其個人資料。我們從本文訪談的過程中，可以了解到 Amazon Alexa 是靠語音封包傳輸到 Amazon 的資料庫進行比對分析再傳回來的過程，Amazon 的資料庫可能是在國外，而且在語音下達指令的過程中，當指令不夠精確或簡短，可能辨識的結果就會不精確，因此 Amazon 需要一些方法來改善他們的用戶體驗與服務[364]。對此，美國彭博社（Bloomberg）於 2019 年 4 月 11 日報導表示，Amazon 聘用了一個全球團隊，負責收聽透過 Echo 從業主家中和辦公室蒐集來的語音資料，並以人工的方式將語音剪輯成片段，並轉錄成文字，並加以註釋，並將其反饋到 Alexa 軟體中，藉以協助改善 Alexa 對人類語音的掌握，從而使其在未來能夠更有效地做出適當反饋[365]。

彭博社透過訪問七位內部員工，得知該團隊係由承包商和 Amazon 正式員工組成所組成，範圍從波士頓、哥斯達黎加、印度到羅馬尼亞，這些工作人員均簽署了保密協議，禁止他們公開談論該計劃[366]。再者，根據兩名在布加勒斯特（Bucharest）辦事處工作的 Amazon 員工所述，他們每天工作須 9 小時解析多達 1,000 個音頻片段，從他們的辦公室外觀來看，並無任何 Amazon 的字樣或招牌[367]。在波士頓（Boston）的員工表示，他曾經為標示特定話語，例如「Taylor Swift」一詞，挖掘了 Alexa 累積的語音資料，並對該詞語進行了註釋，表示「Taylor Swift」是指一名音樂藝術家[368]。有時候這些員工也會聽到一些 Echo 消費者可能寧願保有隱私的資訊，例如一個女人在洗澡時唱歌但卻嚴重破音，或是一個孩子在一邊尖叫著尋求幫助，也曾經聽到令人不安或可能是犯罪的錄音檔，其中兩名員工表示他們認為是性侵過程的錄音檔[369]。在團隊間碰到需要他人協助解

---

[364] 參見附件一訪談紀錄第九段第 16-42 行。
[365] Bloomberg（4/11/2019），〈Amazon Workers Are Listening to What You Tell Alexa〉，https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio（最後瀏覽日：2019/5/13）。
[366] 同前註。
[367] 同註 365。
[368] 同註 365。
[369] 同註 365。



DOI:10.6814/NCCU201900793

析混亂詞彙或碰到有趣的錄音檔的時，他們會使用內部聊天室來共享這些內容，而當聽到令人不安或可能是犯罪的錄音檔時，他們亦可能會在內部聊天室上分享這些經驗，以紓解本身的壓力[370]。Amazon 表示，Amazon 已制定相應的程序，來處理當他們的工作人員聽到這些令人痛苦的事情時的應對措施，然而兩名羅馬尼亞員工卻表示，他們曾經按照內部程序彙報此類事件，卻被告知他們不應該干涉這類事情[371]。

在這事件發布之後，Amazon 向 CNN Business 證實該公司確實有雇用員工聽取客戶對 Alexa 的評價，但 Amazon 會嚴肅處理「客戶個人資料的安全性和隱私性」，關於這個團隊的工作只是提供註釋，這些錄音檔是隨機取樣的且少量的，而且僅用於改善用戶體驗[372]。Amazon 的發言人表示，Amazon 有嚴格的技術和操作保護措施，讓員工無法直接連結並識別客戶或帳戶的資料，所有的客戶資料都具有高度機密性[373]。然而根據彭博社的訪談，這些員工雖然無法直接看到客戶全名或地址，但確實能夠察看這些音檔的設備序號和相連結的 Amazon 帳號[374]。

再者，雖然 Amazon Alexa 的隱私政策有表示，語音資料會用於回答客戶的問題、滿足客戶的要求、改善用戶體驗和服務，但在政策中卻沒有明確告知他們使用真人來處理、利用這些語音資料[375]。在 Alexa 的隱私設置中，Amazon 提供了「禁止使用其錄音來開發新功能」的選項給消費者勾選，但 Amazon 表示，即使用戶選擇退出該計劃，他們的錄音檔可能仍會在正規的審查程序中經手動分析[376]。

---

370 同註 365。
371 同註 365。
372 CNN Business（4/11/2019），〈Amazon reportedly employs thousands of people to listen to your Alexa conversations〉，https://edition.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html（最後瀏覽日：2019/5/13）。
373 同前註。
374 同註 365。
375 BBC 中文（4/12/2019），〈智能語音與人工收聽：竊聽和隱私界限在哪〉，https://www.bbc.com/zhongwen/trad/science-47911570（最後瀏覽日：2019/5/13）。
376 同註 365。



DOI:10.6814/NCCU201900793

第二款　潛在爭點

Amazon Alexa 提供的服務非常具有方便性，但是從彭博社的報導和訪談中，可以得知在 Amazon 在處理、利用這些語音資料時，可能存在有隱私權的侵害。Amazon Alexa 為語音助理設備，與上開兩個判決的標的物「智慧電錶」、「智慧電視」同時具有能「自動蒐集語音資料」、「深入消費者家中取得資訊」、「消費者不清楚這些資料蒐集會被如何處理及利用」等特性，因此本文擬就上述兩個判決美國法院的見解，就彭博社報導 Amazon Alexa 有真人收聽紀錄的事件來初步討論潛在的隱私權爭議問題。具體分述如下：

第一目　Amazon 使用真人收聽用戶音檔是否構成隱私權侵害？

根據 *In Re: Vizio, Inc.* 案，該案法院表示國會強調隱私侵害是指「不合理和嚴重干擾他人，不將私事告訴他人或不將個人形象、興趣展現給公眾的權利」[377]。因此，本文在這裡要討論「Amazon 使用真人收聽用戶音檔是否屬於不合理將用戶的私事、形象、興趣展現給公眾？」在 *In Re: Vizio, Inc.* 案中，被告 Vizio 係將用戶之觀看紀錄在後端 Inscape 數據服務平台上進行分析，再提供給其他廣告商作使用，以收取廣告費用，很明確有第三方的「公眾」介入在資料的蒐集與利用中，而且用戶並不知悉。雖然本案 Amazon 未有明確提供給其他廠商的情形，但承包商及其員工會在內部軟體上分享語音內容，亦會在辦公室直接與其他員工討論、分享語音的內容這事，就本質上會使用戶的資料讓多數人能有共聞共見，訊息傳播的範圍也可能跨越半個地球，即便他們的員工有簽訂保密協議，對消費者來說都存有私事被洩露的高度風險。

再者，雖然 Amazon 強調這個團隊的員工無法看見用戶的真實姓名和地址，但根據彭博社的報導與訪談，員工可以知道該用戶的設備序號及 Amazon 帳號，

[377] *See* In re Vizio, Inc., 238 F. Supp. 3d at 1215.



DOI:10.6814/NCCU201900793

以 *In Re: Vizio, Inc.* 法院的觀點，若一項消費者的可識別數位資訊（digital identifier）通常能與個人姓名產生連結性，也能用於辨識特定的地理位置，並在與 Vizio 公開的其他資料結合時，就可以很容易地識別個人者，就可能屬於可識別個人資料（personally identifiable information）[378]。據此，Amazon 員工知道該用戶的設備序號、Amazon 帳號及用戶的聲音特徵，從用戶的設備序號、Amazon 帳號等數位資料來看，存有能與個人姓名產生連結的特性，而且在與公開的其他資料或收聽的語音內容結合時，亦存在容易地識別個人的可能。綜上所述，本文合理懷疑 Amazon 使用真人收聽用戶音檔一事，存有可識別個人資料或消費者隱私被洩露的高度可能性。

第二目　Amazon 並未在隱私政策揭露會使用真人收聽，是否構成隱私權侵害？

根據 *In Re: Vizio, Inc.*，許多美國州法，如加州、佛州和華盛頓州等，都採取相同侵權行為（tort）的定義，亦即（1）有一個故意侵害（intentional intrusion）的行為，而這個行為是以實體或用其他方式故意侵害他人不受侵擾、享受獨自一人的自由權；（2）這個行為對於以客觀第三人（reasonable person）而言，是屬於非常冒犯的（highly offensive）[379]。從彭博社的報導與訪談中，我們得知員工在聽到部分音檔內容的時候，直覺認為 Echo 消費者可能寧願保有這些資訊的隱私權，但 Amazon 的隱私政策中卻沒有明確告知他們使用真人來處理、利用這些語音資料。事實上，讓真實存在卻不認識的人聽到自己在家中的嘀咕或是進行的活動，就一般人而言都是不自在的，加上「使用真人」這事並未被完整揭露給 Amazon Alexa 的用戶，本人合理認為 Amazon 並未在隱私政策揭露會使用真人收聽，亦即高度剝奪「享受獨自一人自由權」及「控制自己隱私的權利」，可能是屬於非常冒犯的行為。

再者，根據 *In Re: Vizio, Inc.* 案，例行性的個人資料蒐集可能是非常冒犯的

[378] *See Id.*
[379] *See Id.* at 1232.



DOI:10.6814/NCCU201900793

（highly offensive），加上如果被告的作法都與業界慣例不符合，就足以可以斷言被告有高度冒犯（highly offensive）的行為[380]。根據 Google 提供給 BBC 的資訊，Google 有透露會使用審聽人員來處理 Google Assistant 的語音片段，而且因為 Google Assistant 在大多數手機或家庭智慧音箱上就有，可辨識度較低，這些語音不會與可識別個人資料有串聯，在使用真人收聽的過程中，他們還會修改用戶的聲音，以防止用戶的身份遭識別[381]。根據 Apple 的隱私安全政策，他們用真人來處理的語音資料不會包含個人資料，並且這些語音資料會自動鏈接到一個隨機識別號碼，每次關閉 Siri 時，該識別號都會被都會重置，而且其審聽人員在收聽過程中，也不會獲得可識別用戶個人資料或者隨機識別號碼[382]。基於此，Amazon 的去識別化作法都遠低於其他同業，如 Google 和 Apple，我們可以合理推斷言 Amazon 在此，有高度冒犯（highly offensive）的行為[383]。

第三目　即使用戶勾選拒絕使用其錄音來開發新功能卻仍遭手動分析，是否構成隱私權侵害？

根據 In Re: Vizio, Inc.，該案法院指出美國法院一直搖擺不定，是否要將隱私權侵權行為（tort of invasion of privacy）的範圍擴張到例行性蒐集可別識別個人資料（the routine collection of personally identifiable information）的行為，且在該案法院明確指出蒐集親密或特殊性個人資料可能構成極具攻擊性的侵害[384]。當被告無視消費者的隱私選擇權卻同時認為自己是尊重消費者隱私權的，那麼對消費者來說，這些例行性的個人資料蒐集可能是非常冒犯的（highly offensive）[385]。在 Amazon Alexa 的隱私政策中，提到即使用戶勾選拒絕使用其錄音來開發新功能卻仍會面臨到手動分析，用戶勾選拒絕使用其錄音的選擇明顯是失效的，因此

---

380 *See Id.* at 1233.
381 同註 375。
382 同註 375。
383 *See* In re Vizio, Inc., 238 F. Supp. 3d at 1233.
384 *See Id.*
385 *See Id.*



DOI:10.6814/NCCU201900793

本文認為 Amazon 有高度無視消費者的隱私選擇權的可能發生。綜上所述，考慮到 Amazon 所蒐集的語音資料的數量與性質，加上 Amazon 未能尊重消費者的隱私選擇權，本文可以合理推論 Amazon 的蒐集行為構成極具攻擊性的侵害。

第四目　Amazon Alexa 語音服務能否能主張適用第三人理論？

根據 Naperville 案，美國法院表示第三人理論（third-party doctrine），是指當一個人自願性地與第三人分享其個人訊息，即屬於放棄了其對於該訊息之隱私期待，從而第三人蒐集的行為並不會違反美國憲法增修條文第四條之隱私保護[386]。同時，法院表示從消費者角度來看若消費者在整個過程中根本沒有選擇，就不能算是自願性地與第三人分享其個人訊息[387]。因此第三人理論的核心爭議在於「消費者是否擁有真實的選擇權」，而考量的點是消費者會不會願意承擔每天被監控的風險，來換取第三人提供的服務[388]？換言之，就是法院必須分析「第三人提供服務之利益」以及「消費者必須承擔之風險」，用二者衡量一般消費者是否會自願性的放棄，來判定消費者是否具備真實選擇權。

首先在「消費者必須承擔之風險」方面，從法院這個觀點切入，在 Amazon 一案中如前面所討論的，存在有「讓真實存在卻不認識的人聽到消費者在家中嘀咕或是進行哪些活動」的事實。本文認為一般人對於這樣的事實發生都是不自在的，因為這代表消費者必須承擔每天被監控其在家中生活模式的風險，而往往在家中生活模式是一個人不想被陌生人輕易觸碰的隱私領域。

再者在「第三人提供服務之利益」方面，以 Amazon 所提供服務而言，就是用聲控取代實際手指按鈕的操控，即使不使用語音也不會造成在家庭生活中生活極度不方便，因此從其所帶來的利益來看，跟 Naperville 案中消費者不安裝智慧電錶就無法使用電力相較之下較為低。從 Naperville 案法院的觀點，即使是需求度高、利益較大的電力使用，都不能認定消費者會為此自願性放棄其在家中隱私

386 *See* Naperville, 900 F.3d at 527.
387 *See Id.*
388 *See Id.*



DOI:10.6814/NCCU201900793

權，本文認為消費者會為了「能使用語音助理」而自願性放棄家中隱私的可能性就更低了。此外，消費者並不知悉 Amazon 使用真人來收聽 Alexa 語音資料，本文認為消費者在未清楚明白資料如何被使用情形下，所提出之任何同意都非屬於自願性放棄對於該訊息隱私的期待，Amazon 很難主張有第三人理論之適用。

### 第四項 小結

在本節所介紹之三個實際美國爭議案例之中，三家業者 Naperville 公營電力單位、Vizio、Amazon 具體在智慧市場上運用 AIoT 技術推出產品時，均發生隱私權、個人資料蒐集、處理及利用的問題。從智慧家庭市場中的角色來看，三家公司略有不同，首先 Naperville 公營電力單位的立場屬於基礎建設，與智慧家庭通訊業者角色相似，而 Vizio 是美國消費電子品牌廠商致力於研發視覺方面產品，是傳統的家電廠商。Amazon 就是從網路平台上出發，從而研發新的產品 Echo。

從產品特質上來看，智慧電錶著重在能源管理服務，Vizio 智慧電視是娛樂性服務，而 Amazon 多元化的生活管家，但這些產品所蒐集的資料類型也非常不同，再利用階段所產生的結果可能是一種個人資料卻與原蒐集的資料不同，譬如 Naperville 案中，它們所蒐集的是電力使用的類比訊號，但卻可能得出用戶何時在家、房屋何時空置、睡眠時間、飲食習慣、家中使用的特定電器類型等不同資訊，這也是新科技中會面臨到的難題，個人資料的蒐集可能多元化無法預測，所造成的影響與結果也同樣無法預測。

從法院在各個案例中切入角度來看，本文發現能源管理服務因過往都是政府直營或多為公營單位，法院會從美國憲法增修條文第四條、第三人理論來檢視，討論政府與人民間的隱私權拉鋸問題。若是娛樂性的家電爭議，就會從既有法制下討論是否有隱私權的爭議，但如同前面討論的美國是採取部門式立法以及各州自行立法，消費者如何要新科技所造成的隱私權侵害中，合理地找到可依據的法源並非容易之事。因此在新科技時代下，是否設立統一的隱私權與個人資料保護



DOI:10.6814/NCCU201900793

法是個新議題，當然還有針對不同的應用要如何確保既定法律無僵化也是迫在眉睫的問題。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

## 第三節　智慧家庭潛在之隱私爭議

前面本文分別討論了目前智慧家庭的應用、現行歐美及台灣的個人資料保護法制，以及目前及潛在此應用之下產生的消費者隱私爭議。從中發現目前的智慧家庭業者處於正逐漸進入市場佈局的階段，但在對照各國現行個人資料法制體系與規範下，可能存在有消費者隱私保護不夠完善的問題。正如同前面一節所討論的智慧型電錶、電視及音箱等案例，美國法院逐漸意識到新科技對於「家庭內部的隱私權及個人資料」應用比以往更為多元，進而造成的隱私權影響與結果也同樣多元化且無法預測。本節欲從前述討論的產品與服務模式，以現行法及訪談業者的角度觀之，分析其在智慧家庭應用中個人資料之蒐集、處理及利用階段，可能產生的爭議與問題。

### 第一項 蒐集之資料特性與類型

歐盟與台灣採取相似的個人資料的分類方法，區分為兩大類，兩類別「一般性個人資料」及「特殊性個人資料」，通常「特殊性個人資料」又稱可為敏感性個人資料。就個人資料的型態，皆採取列舉主義之方式，例如自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動等，並輔以概括性文字，如載明其他得以直接或間接方式識別該個人之資料均屬之[389]。GDPR 比較特別之處，在於其定義個人資料時，特別表示「定位資訊」、「網路資訊」或「一個或多個該自然人之身體、生理、心理、經濟、文化或社會認同」等在數位時代下的產物也屬於該自然人之個人資料[390]。在「特殊性個人資料」方面，兩國法制特別載明有關病歷、醫療、基因、性生活、健康檢查及犯罪前科等個人資料須取得當事人的具體明

[389] 台灣《個人資料保護法》第 2 條 1 項參照。
[390] GDPR, Article 4(1).



DOI:10.6814/NCCU201900793

確之同意[391]。美國針對這些特殊性個人資料也大多採取部門立法的方式加以保護，尤其是金融之財務資料、醫療病歷資料等最受到重視。就現行法制對於個人資料的定義與分類，本文發覺智慧家庭市場參與角色所涉及之個人資料有些許不同，例如從訪談中顯示業者在架設智慧家庭設備時，所會涉及的資料可能包含單純數字之類比訊號，例如能源管理方面之家電設備；亦可能包含語音、影像等數位資訊，例如家庭監控設備及語音裝置[392]。從各個市場參與角色的面向，本文整理其蒐集之資料類型，如下表所示：

| 市場參與角色 | 代表型企業 | 資料類型 |
|---|---|---|
| 通訊服務業 | IBM | 洗衣資訊(使用量及時間)、影像資料、消費者基本資料 |
| | 中華電信 | 能源使用資料(如瓦斯使用量)、環境資訊、語音資料、消費者基本資料 |
| | Naperville 電力公司 | 能源使用資料(如電力使用量)、消費者基本資料 |
| 家用電器廠 | Bosch | 家電使用模式、時間、RFID 感測數值、影像資料、消費者購買紀錄、消費者 App 帳戶資料 |
| | LG | 家電使用模式、時間、影像資料、消費者基本資料、消費者通訊軟體帳戶資料 |
| | Vizio | 觀看歷史紀錄、購買紀錄(如產品型號、序號及數位資訊) |
| 平台業者 | Amazon | 語音資料、操作時間、消費者帳號資料、購買紀錄(如產品型號、序號及數位資訊) |
| | Google | |
| | Apple | |

[391] GDPR, Article 9 和台灣《個人資料保護法》第 6 條參照。
[392] 參見附件一訪談紀錄第十二段第 16 行開始。



DOI:10.6814/NCCU201900793

表 1 市場參與角色蒐集之資料類型

資料來源：本研究彙整[393]

第一款　如何界定所蒐集的資料屬於「個人資料」？

從訪談中，業者認為類比訊號（單純數值資料）屬於必要維護、改善產品設備所需之資料，而語音、影像等資料則因涉及消費者隱私，特別需要當事人同意才可蒐集[394]。第一個問題就是「類比訊號」所展示該自然人之能源使用資料是否為個人資料？就此問題而言，可以從最具代表性的 *Naperville* 智慧電錶案來看，在該案中的智慧電錶設定，係以間隔十五分鐘就蒐集一次用戶的「能源使用資料」，雖然簡單的阿拉伯數字訊號，然而卻有證據證實有極高程度能顯示出該資料主體之「個人親密細部資訊」，例如人們何時在家、房屋何時空置、人們睡眠時間、飲食習慣、家中使用的特定電器類型以及電動車充電次數[395]。從正面角度來看，業者蒐集的是設備之「能源數值資料」，然而從另一面來觀之，業者蒐集的資料很大成分隱含著「自然人生理、心理、社會生活習慣」等個人資料，且可透過比對或與其他資料結合識別自然人[396]，因此即使是簡單的類比訊號也有極大比例被認定為可間接識別之個人資料。

但在認定蒐集之個人資料類型時，面臨到蒐集的資料因其可能衍伸、被輕易推導的資訊更多時，更加難以區分其所蒐集的是哪一種類型的個人資料。舉例來說，若今天 *Naperville* 智慧電錶業者所蒐集的能源使用資料能隱含並推導出「自然人的健康資料」時，屬於蒐集特殊性的個人資料還是一般性個人資料？若今天 Vizio 智慧電視蒐集消費者的觀看紀錄，能推導出消費者的「性傾向」時，又該如何認定？這個問題，展現在科技日益進步、能分析更多自然人特質的同時，業者也很難去釐清、明確告知當事人，在此項智慧家庭服務當中可能會涉

[393] 本表為本文所繪製，其中消費者基本資料，如消費者姓名、電話及住址等在購買行為中所必要蒐集之消費者個人資料。

[394] 參見附件一訪談紀錄第一段第 15 行開始。

[395] Naperville, 900 F.3d at 524.

[396] 葉志良（2016），〈大數據應用下個人資料定義的檢討：以台灣法院判決為例〉，《資訊社會研究》，31 期，頁 10。



DOI:10.6814/NCCU201900793

及的個人資料有哪些，進而無法落實告知義務，並取得當事人明確同意。但事實上，當個人資料保護法將所蒐集的個人資料範疇僅限於蒐集時具體內容，例如智慧電錶所蒐集的就是單純的「能源數值」，可透過比對或與其他資料結合識別自然人，屬於可間接識別之一般性個人資料時，這些業者可能會因為其蒐集個人資料的性質單純，而容易忽略掉潛在問題。譬如業者直接認為使用類比訊號的模式蒐集，就不會有特殊性個人資料的蒐集問題，進而忽略個人資料保護法之要求，造成個人資料及隱私權的保護不周或有規避的現象。

第二款　智慧家庭所蒐集之資料是否具「可識別性」？

大部分透過智慧型家用電器自動上傳之資料，有極大比例將與購買該設備之消費者的基本資料、產品序號或消費者帳戶資料進行結合。從家電廠商蒐集資料的案例來看，例如 Bosch 智慧冰箱在運作模式上，運用 RFID 自動識別（感測器）冰箱內之物體或食品標籤，該標籤可能包含食物類型及保存期限的資訊，冰箱可自動將不同標籤訊息傳送到 Home Connect 應用程式上，讓消費者從手機直接了解冰箱內食品資訊，這種模式就是將冰箱內消費者所購買的物品資料與消費者的 App 帳戶資料進行結合，在透過 Home Connect 應用程式會根據食品類型，提供冰箱理想溫度、濕度設置的建議[397]。Bosch 的智慧冰箱不僅是具備「食物儲存」的功能，亦可以執定自動感測並判別內部物，能夠蒐集消費者的「購買食物偏好」，然而通常在家庭之中該冰箱可能展現的是「一個家庭的購買食物偏好」，而不一定是「一個人的購買食物偏好」，即便是能與該消費者之 Home Connect 帳戶資料做結合，該購買偏好也不一定完整且具有可識別性，能夠判定這樣的「購買食物偏好」能連結到該特定自然人。另外 LG 在智慧冰箱方面，除內建能與 Amazon Alexa 聲音互動的功能並裝置廣角相機，使消費者可透過手機關觀看內部食物品項，並透過感測器蒐集用戶使用模式外，能與通訊軟體 Line 結合，讓消費者可

[397] 同註 98。



DOI:10.6814/NCCU201900793

直接透過 Line 得知其冰箱內部的情形[398]，某方面來說 LG 亦能將「購買食物偏好」與該自然人之「通訊軟體基本資料」整合，然而是否「購買食物偏好」能特定出該自然人卻仍存有疑慮。上面兩個市場案例顯示出智慧家庭所蒐集之個人資料存在的問題，就是通常在「家庭內部之資料」多數情形不是特定自然人的資料，而是特定一群具有共同生活關係之自然人的集體資料，在這種情形之下所蒐集而來的個人資料，是否具備識別性？

從平台業者運用智慧音箱蒐集個人資料來看，Amazon Echo 跟 Google Home，讓使用者透過語音下達指令，例如只要呼喊「Alexa」或「Ok Google」就可以完成待辦事項設定、廣播提醒設置、查詢天氣預報、播放音樂和購物。在這種模式下，Amazon 跟 Google 均會蒐集消費者之語音資料，語音資料與前述的家用電器之使用量資料不同，語音資料因涉及個人音調、口氣之紀錄，其對於特定自然人之識別程度較高。尤其是 Apple 在 HomePod 的運作上，是讓消費者用語音要求 HomePod 開啟 App 時，直接將語音資料傳送到 iPhone 上執行指令[399]，因此與 iPhone 上的個人資料結合程度更高，況在 Apple 對於使用者的資料建置上，有使用「家庭帳號」的功能，係在一個母帳號底下，更細分子帳號，因此有極高比例能夠將特定之子帳號與該語音資料作結合，識別特定自然人之程度更高。

綜上所述，本文從而得以歸納出當業者所蒐集之資料是與該特定人直接程度較高，如屬於語音、影像等資料，能識別該特定自然人程度較高。再者，當業者能夠藉由設立子帳號的方式分類該自動蒐集之資料時，能識別該特定自然人的程度也較高，概念如下圖所呈現：

[398] 同註 105。
[399] 同註 135。



DOI:10.6814/NCCU201900793

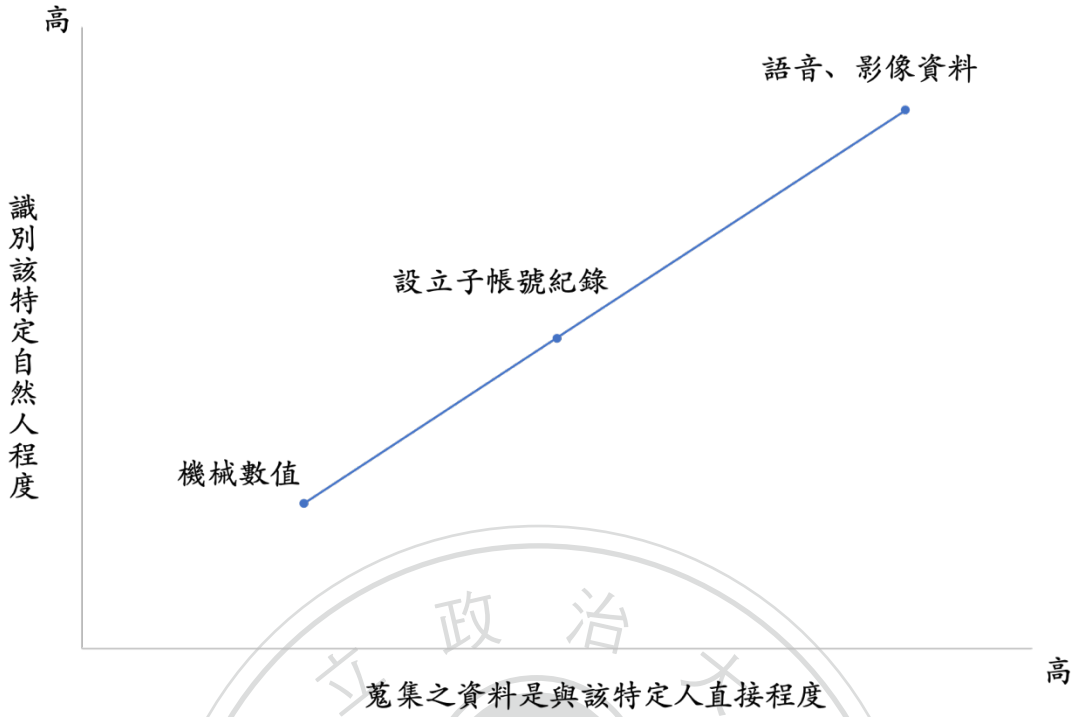


圖 1 資料特性與識別程度分析圖[400]

第三款　一般性個人資料轉變成特殊性個人資料的難以預測性？

目前各國對於個人資料之分類大多區分為，「一般性個人資料」及「特殊性個人資料」，然而本文認為這樣的二分法難以因應科技變化所衍生的隱私權影響，如我們前面談到的 *Vizio* 智慧電視案，該案中 Vizio 透過「智慧互動」(Smart Interactivity)這個軟體，專門來蒐集消費者的歷史觀看內容[401]，然而這些資料在後端數據服務平台(Inscape)上可以與現有內容資料庫進行比對，來識別消費者來進行精準行銷服務[402]，該業者極度有可能在分析觀看紀錄的同時，得知出該消費者之宗教信仰、性傾向等，對於消費者之隱私權有極大影響。在 *Vizio* 案中，該案法院認為「觀看歷史紀錄」是屬於敏感性隱私利益[403]，也就是特殊性個人資料。一般來說，消費者的「觀看歷史紀錄」屬於可間接識別之一般性個人資料，但在 *Vizio* 案中顯示出在有「推論出特殊性、敏感性資訊的可能性」時，一般性

[400] 本圖為本文所繪製。
[401] In re Vizio, Inc., 238 F. Supp. 3d at 1211.
[402] *Id.*
[403] *Id.* at 1232.



DOI:10.6814/NCCU201900793

個人資料可能會被變更，改為認定該個人資料屬於是「特殊性個人資料」。這種情形，對於市場參與角色是難以預測的，在設計推出產品之前也無法確定本身產品所蒐集的個人資料，會不會因科技的變化，而被改認定成是「特殊性個人資料」，進而違反個人資料保護之規定。

## 第二項 受規範主體之定位

GDPR 將受規範主體採取二分法，區分為「資料控制者」(Data Controller)、「資料處理者」(Data Processor)，「資料控制者」係指自行或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構[404]，而「資料處理者」係指代替、協助資料控管者處理個人資料之自然人或法人、公務機關、局處或其他機構[405]。在台灣個人資料保護法之規定，受規範之主體區分為「公務機關」和「非公務機關」，前者係指依法行使公權力之中央或地方機關或行政法人；後者係指公務機關以外之自然人、法人或其他團體[406]。根據 *Naperville* 案在美國之規範下，若該企業屬於政府持有之公營企業者，在蒐集資料過程中並非第三人的角色，則不適用第三人理論且須遵守美國憲法增修條文第四條之規定；若為一般私人企業則適用第三人理論或其他隱私法規[407]。按照 GDPR、美國及台灣個人資料保護法的分類上，市場參與角色的定位可歸納如下表：

---

[404] GDPR, Article 4(7).另其翻譯參照國家發展委員會網，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9iNGZiZTA0OS1jYWQ1LTQ3MGEtYjhlMy00ZGU0NjhmOWIxMGMucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5pys5paH6YOo5YiGLnBkZg%3d%3d&icon=..pdf（最後瀏覽日：2019/4/22）。

[405] GDPR, Article 4(8).另其翻譯參照國家發展委員會網，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9iNGZiZTA0OS1jYWQ1LTQ3MGEtYjhlMy00ZGU0NjhmOWIxMGMucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5pys5paH6YOo5YiGLnBkZg%3d%3d&icon=..pdf（最後瀏覽日：2019/4/22）。

[406] 台灣個人資料保護法第 2 條第 7、8 項參照。

[407] Naperville, 900 F.3d at 527.



DOI:10.6814/NCCU201900793

| 市場參與角色 | 代表型企業 | 受規範主體之定位 |
| --- | --- | --- |
| 通訊服務業 | IBM | 資料處理者、非公務機關、私人企業 |
| | 中華電信 | 資料控制者、非公務機關、公營企業 |
| | Naperville 電力公司 | |
| 家用電器廠 | Bosch | 資料控制者、非公務機關、私人企業 |
| | LG | |
| | Vizio | |
| 平台業者 | Amazon | 資料控制者、非公務機關、私人企業 |
| | Google | |
| | Apple | |

表 2 市場參與角色的定位[408]

根據上表 2，可發現歐盟、美國及台灣在認定受規範主體時，採取不同的區分標準，而在對應的分類下，各市場參與角色可能會被認定為不同的規範主體。其中，最具代表的問題，在於若通訊服務業者所提供的服務是傳輸過程的協助，是否會被歸類為資料處理者，而非被認定為資料控制者？根據訪談中之智慧家庭服務開發者表示，通訊服務業係以系統商之定位，提供一個平台給設備商進行資料之傳遞，例如【A 公司】、【B 公司】及【P 公司】的智慧家庭專案來說，【P 公司】設有 DONGO 感測器於其智慧家電設備之中，而這顆 DONGO 裡的資料必須要透過【A 公司】的 E-Panel 傳輸管道，將相關指令傳輸至【P 公司】的後端系統[409]。從【A 公司】這通訊服務業的角度，資料控制者為【P 公司】而【A 公司】僅是扮演代替其處理個人資料之「資料處理者」，因要蒐集哪些類型的資料係由【P 公司】決定，【A 公司】僅是確保傳輸安全性、提供加密服務的管道。

然而本文認為通訊服務業者是否純然屬於「資料處理者」，須依個案情形認

408 本表為本文自行繪製。

409 參見附件一訪談紀錄第十二段第 3 行開始。



DOI:10.6814/NCCU201900793

定。舉例而言，從訪談中可得知【A 公司】及【P 公司】在合作的過程中，會事先協商好串接之 protocol 介面（如使用 DCPIP 或 ODP 資料庫作為媒介）進行資訊的交換，雙方將資料傳輸到這個介面，再從這個介面對應到適當的家用電器或後端平台，且雙方針對傳輸之指令亦有協調[410]，因此本文認為【A 公司】仍存在有「與他人共同決定個人資料處理之目的與方法」的可能性，難謂能直接被推定為代替其處理個人資料之「資料處理者」。這也顯示出通訊服務業如 IBM、中華電信等，很難一蓋而定免除 GDPR 或個人資料保護法賦予他們的告知義務及相關資料控制者應遵循之要求。

再者，雖台灣明文規定受規範主體區分為「公務機關」和「非公務機關」，且侷限於「依法行使公權力之中央或地方機關或行政法人」，然而參考前述 *Naperville* 案，美國對於公營事業單位在執行公權力委託之事項時，仍可能被認定為公務機關而受到美國憲法第四條增修案之限制，對於「公務機關」之認定，可能亦有變更之餘地，公股民營企業在委託行使公權力之情形下，是否仍可被認定為公務機關仍待未來個人資料保護法之發展觀察。

### 第三項 資料處理分析之影響與挑戰

就資料處理之階段，根據訪談表示以目前智慧家庭之業者應用之現況，係以將智慧家電設備之數值或資訊傳遞到後台設備之中，或直接進行資訊交換進而控制其他智慧家電設備[411]，這個環節之中涉及到資料傳輸、儲存及處理的安全性跟隱私管理，就資訊傳輸的安全性方面，如同本章第一節所描述，存在有機密性威脅、驗證威脅及接近使用威脅。在資料儲存方面，從訪談中之市場開發業者角度來看，不同於系統商單純進行資料傳輸，智慧家電設備廠商為了解產品使用情形、確認消費者的需求、建立穩健的消費者關係，有極大可能將數據、資料儲存在後

[410] 參見附件一訪談紀錄第十五段第 26 行開始。
[411] 參見附件一訪談紀錄第九段第 17 行開始。



DOI:10.6814/NCCU201900793

台端進行研究[412]，目前資料儲存的方式分為「雲端儲存」和「邊際儲存」，前者係將蒐集來之資料直接儲存在雲端空間，以 IBM、Amazon、LG、Google、Vizio 及 Naperville 電力公司為代表，舉例而言 Amazon 和 LG 合作會將 Alexa 從家電中蒐集到的資訊直接上傳至 AWS 雲端資料庫，進行分析[413]。後者係將蒐集來之資料儲存在當地智慧中樞內，待用戶連結至對應 App 或其他工具時，才會傳輸到企業後端，以 Bosch、Apple 為代表，舉例而言 Bosch 推出智慧冰箱或其他智慧家電搭配 Smart Home 或 Smart Camera 的 App，只有當用戶連線至 App 時，才會回傳至公司後端[414]。

第一款　資料處理與去識別化的困境

就資料處理的層面，根據資料儲存方式之不同，業者亦會採取不同之運算方式，分別搭配的是「雲端運算」和「邊際運算」，當然即便是採取邊際運算的業者，仍有可能性將處理過之資料傳輸至雲端進行其他運用，例如 Apple 在 HomePod 產品上採取邊際運算之方式提供 Siri 的服務，然而這些 Siri 的語音資料根據 Apple 之隱私聲明，亦會傳輸回內部進行自然語言處理之加值服務。根據訪談，智慧家庭若選擇採取機器學習或深度學習來分析資料，需要有龐大的 GPU 處理器及適合的設備及環境，因此即便是採取邊際運算方法之廠商，仍有需求將部分資料傳回設計研發中心進行反饋，否則在單個感測器上難以處理龐大資料或進行額外運用，因此幾乎所有廠商都可能涉及到雲端運算之運用。

在雲端運算的過程中，去識別化處理就是符合個人資料保護法之關鍵，根據本文前述得出之歸納結果，業者所蒐集之個人資料若具識別化程度較高者，如屬於語音、影像等資料，應採取較高之去識別化手段；若所蒐集之個人資料具識別化程度較低者，如單純數值資料等，採取之去識別化程度則不須如此嚴格。通常採取之去識別化手段分為兩種，假名化（Pseudonymization）與去連結化

412 參見附件一訪談紀錄第十二段第 37 行開始。
413 同註 143。
414 同註 144。



DOI:10.6814/NCCU201900793

（Anonymization），前者係指將資料單獨保存之方法，而不連結到該個人，但在需要時仍可還原成可識別之資料；後者，大多又稱為「匿名化」，係指永久性的處理，使該資料永遠不會被連結至個人[415]。然而，許多學者認為在現今大數據之應用底下，事實上已不存在完全「去識別化」的情形，即便是已明顯經去連結化處理之資料仍存有相當之機率，在與其他大數據資料庫內之資料結合後，能夠重新鏈結至該特定自然人[416]。例如 Amazon Alexa 智慧音箱爭議中，負責進行 Alexa 語音資料之處理的員工，能夠知道知道該用戶的設備序號、Amazon 帳號及用戶的聲音特徵，雖然 Amazon 宣稱這些員工無法得知該個人之姓名、住址等而已確實做到去識別化之處理，但只要從用戶的設備序號、Amazon 帳號等數位資料的鏈結程度來看，均存有能與個人姓名產生連結的特性，在與公開的其他資料或收聽的語音內容結合時，就存在容易地識別個人的可能，也印證智慧家庭業者在去識別化處理之難處。

第二款　資料剖析之影響

不同於美國和台灣之規定，GDPR 特別強調如特徵剖析（profiling）涉及到個人資料的處理須取得當事人之同意，且若為特殊性個人資料之處理，如生物特徵識別資料等則原則上為禁止，除非能舉證到已取得當事人明確同意（Explicit consent）或有其他法定事由[417]。舉 *Vizio* 智慧電視案為例，Vizio 透過「智慧互動」（Smart Interactivity）這個軟體，專門來蒐集消費者的歷史觀看內容並透過後端數據服務平台（Inscape）可以與現有內容資料庫進行比對，來識別消費者來進行精準行銷服務[418]。就「使用 Inscape 之現有內容資料庫」分析消費者喜好這件事，某程度就是透過特徵剖析（profiling）來進行個人資料之處理與利用，亦即使用個人資料來分析、評估或預測與該資料主體之個人偏好和興趣。在智慧家庭市場

[415] 蔡敦仁、蘇俊吉、許博堯、吳佩霏、林政諺，〈「通傳事業去識別化技術與相關技術規範研究」補助研究報告〉，https://www.ncc.gov.tw/chinese/files/18031/3923_38917_180315_1.pdf，頁 156。

[416] 鍾孝宇（2017），《巨量資料與隱私權—個人資料保護機制的再思考》，頁 138-139，國立政治大學碩士論文。

[417] GDPR, Article 21(4).

[418] *See* In re Vizio, Inc., 238 F. Supp. 3d at 1211.



DOI:10.6814/NCCU201900793

中運用特徵剖析（profiling）並不少見，例如在 IBM 和 Whirlpool 的合作上，就利用 Watson IoT 的技術串聯洗衣機與烘衣機上的感測器，將洗衣資訊透過感測器傳輸至 IBM Cloud 上藉以分析消費者是如何使用家電以及家電本身如何應對，從而使 Whirlpool 更容易根據消費者需求[419]，在這個例子方面 IBM 就是運用特徵剖析（profiling）來分析、評估該資料主體之行為。因此，本文將各市場參與角色之潛在的個人資料特徵剖析（profiling）情形，從「產品在智慧家庭中是否多元、多樣」以至於能獲得之資料面向是否全面，及「能透過產品推導出資料之種類」，歸納如下：

| 市場參與角色 | 代表型企業 | 資料特徵剖析之面向 |
|---|---|---|
| 通訊服務業 | IBM<br>中華電信<br>Naperville 電力公司 | 1. 產品較多元，能剖析之資料面向亦較廣。<br>2. 推導出身體、心理、社會生活習慣（如使用家電行為）及健康資料。 |
| 家用電器廠 | Bosch<br>LG<br>Vizio | 1. 產品較單一，能剖析之資料面向亦較不全面<br>2. 推導出消費者偏好（如使用家電行為）及連結至其他相應服務資料（例如自動化下單服務）。 |
| 平台業者 | Amazon<br>Google<br>Apple | 1. 涉及語音資料蒐集，能剖析之資料面向亦較全面且直接。<br>2. 推導消費者偏好（如使用家電品牌喜好）、連結潛在帳號取得其他個人資料（例如 iPhone 或 |

[419] 同註 84。



DOI:10.6814/NCCU201900793

| | | |
|---|---|---|
| | | Amazon 帳號 )。 |

表 3 市場參與角色之資料剖析面向[420]

市場參與角色之資料特徵剖析之面向，可以從產品在智慧家庭中是否多元、多樣」來看，可以綜合討論其風險如下表：

| 單一家庭蒐集之情形 | 產品分佈廣且多元 | 產品分佈單一 |
|---|---|---|
| 剖析之資料具直接性 | 風險極高 | 風險較高 |
| 剖析之資料具間接性 | 風險較高 | 風險較低 |

表 4 市場參與角色之資料剖析風險表[421]

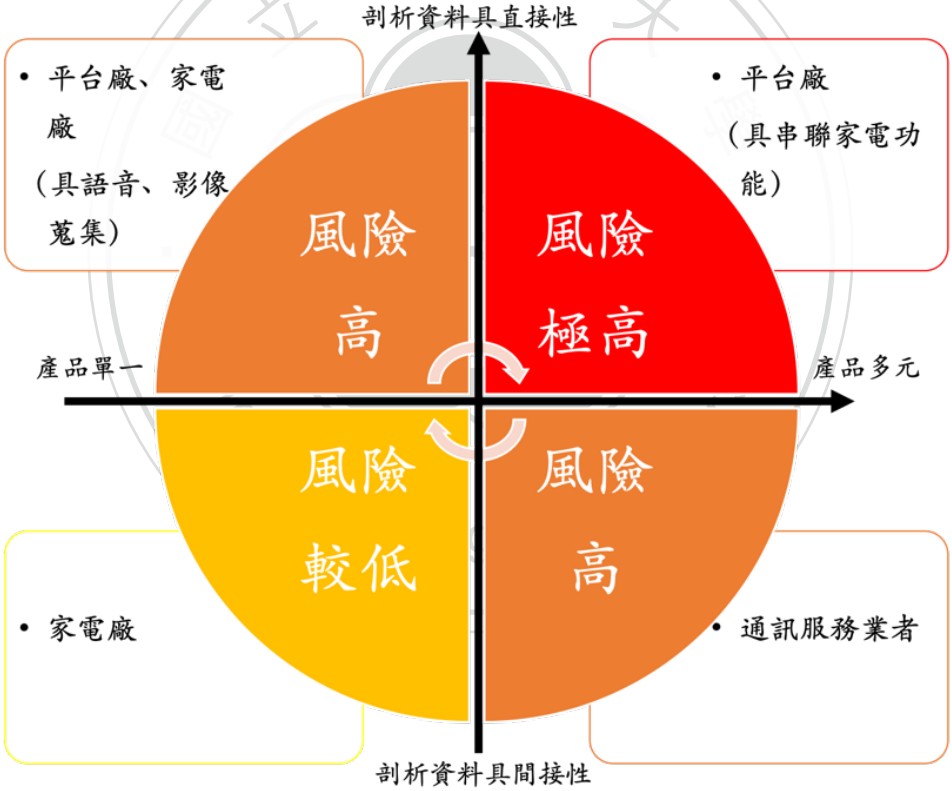


圖 2 市場參與角色之資料剖析風險圖[422]

以通訊服務業者來看，大多以系統商、後端分析商為主，產品也大多以環境控制、安全監測並搭配智慧型家電，營造智慧情境，因此其能剖析之資料面向較

[420] 本表為本文所繪製。
[421] 本表為本文所繪製。
[422] 本圖為本文所繪製。



DOI:10.6814/NCCU201900793

廣泛，且具備推導出身體、心理、社會生活習慣及健康資料的能力。家電廠商方面，按照目前大眾購買家電的習慣，多數家電並非均為同一品牌、更廠商亦有其主打之系列產品，使得目前各家電廠商能佈置在家庭之中的產品較為單一，因此能剖析之資料面向亦較不全面，能推導出之資料包含消費者偏好，例如家電使用行為，或是其他相應服務資料，例如連結至自動化下單服務內之帳戶資料。平台業者因大多採用語音助理之裝置控制其他品牌之家電設備，因此其多涉及語音資料蒐集，能剖析之資料面向亦較全面且具直接性，能推導出消費者偏好，例如從何做串聯之業者推導出使用家電品牌喜好，且從提供網路訂單或串連手機等服務中，取得其他個人帳戶資料（例如 iPhone 或 Amazon 帳號）等。綜上所述，業者在智慧家庭中所經營之產品較為多元、多樣者，例如消費者同時購買該企業之產品多達兩個面向以上者，則該業者能獲得到之該特定消費者之資料面向也較全面，所能推導出之該消費者資訊也較為廣泛，因此造成之消費者分析，對該消費者之影響也較為顯著。

### 第四項 告知義務範圍模糊化

個人資料之合理利用，在隱私權理論發展之下，特別強調賦予當事人控制之權利，因此各國在制定合理利用之規定時，著重在資料控制者善盡「告知義務」以獲取當事人同意。GDPR 就告知義務的部分，規定資料控制者應以簡明、透明、易懂且方便取得之方式，提供完整的「應告知資訊」給資料主體，如資料控制者身分及聯繫方式、資料保護官聯繫方式、處理目的及法律依據、所涉及個人資料類型、接收者名稱或接收者類型等[423]。而台灣個人資料保護法規範，資料蒐集機關應以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式，善盡「告知義務」，包含明確告知當事人其

[423] GDPR, Article 14(1) & 12(1).



DOI:10.6814/NCCU201900793

機關名稱、蒐集之目的、蒐集之個人資料類別、個人資料利用之期間、地區、對象、方式以及當事人依得行使之權利及方式等[424]，亦可以明確說明當當事人不願意提供個人資料時，可能對其權益產生之影響，例如該自然人將無法使用完整商品與服務。

從前述本文所討論之個人資料蒐集之類型，便可知悉智慧家庭市場參與者難以界定其蒐集之個人資料之類型與種類。譬如以 *Naperville* 智慧電錶案為例，資料控制者應告知資料主體，其蒐集之資料類別是屬於「能源使用資料」還是「個人親密細部資訊」，甚至必須到表達出「人們何時在家、房屋何時空置、人們睡眠時間、飲食習慣、家中使用的特定電器類型以及電動車充電次數」等資料[425]，才屬於落實「善盡告知義務」？再者，智慧家庭業者在進行應用分析時，須明確告知當事人關於其「個人資料利用之期間、地區、對象、方式」，然正如前面所談到，業者在該自然人家中所存在之產品類型可能很多元，能蒐集、剖析出之資料面向也大不同。

以 Whirlpool 和 IBM Watson IoT 合作之情形來看，係由 Whirlpool 向消費者蒐集其個人資料，再委由 IBM 負責在雲端上分析顯示消費者是如何使用他們的機器以及機器本身如何應對，並提供後續產品改善或應用服務[426]，在這種情形之下，IBM 是否屬於個人資料之接收者或是個人資料之利用對象，使得 Whirlpool 須在隱私聲明中揭露其合作夥伴之資訊是首要問題。此外，考量「個人資料利用之方式」需被揭露，但在 AIoT 技術下使用機器學習或深度學習的過程中，業者無法完全在蒐集個人資料時，即知道這些個人資料未來可能被推導的可能性。究竟在智慧家庭應用之下，業者需要揭露之「利用與分析」的資訊應達何種程度，得以屬於落實個人資料保護法或 GDPR 之規定。以利用方式而言，善盡告知義務是否也代表 Whirlpool 須要求 IBM 向大眾揭露其分析個人資料之

[424] 個人資料保護法第 8 條。
[425] Naperville, 900 F.3d at 524.
[426] 同註 84。



DOI:10.6814/NCCU201900793

技術？因此，本文認為在智慧家庭應用之下，業者涉及之告知義務範圍有模糊化之趨勢。

## 第五項 當事人同意機制不確定性

從訪談中，清楚可以知道業者非常了解他們在運用智慧家庭設備蒐集個人資料時，必須善盡告知義務且取得當事人之同意[427]。在 GDPR 規定之中，當事人同意（consent）須由資料主體透過聲明（statement）或明確肯定之行動（clear affirmative action），所為自主性（freely given）、特定（specific）、經告知的（informed）及具體明確（unambiguous indication）之表示，其同意處理與其有關之個人資料[428]，若涉及到「特殊性個人資料」處理時，則須取得資料主體「明確同意」（Explicit consent）之程度，不論是何者在討論資料主體之同意自主性（freely given）時，應特別考慮該個人資料之處理是否為履行契約所必要[429]。然而，GDPR 並未說明何謂達成取得資料主體「明確同意」（explicit consent）之程度乃目前實務上的困境。台灣《個人資料保護法》中當事人同意，係指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示[430]。

### 第一款 自願性同意可能失效

以目前見解，強調該同意須為當事人自主、自由的決定，也就是當事人在決定過程中沒有被詐欺、脅迫等情事發生，若今日當事人拒絕同意將遭受重大不利益，或其事實上沒有選擇的餘地而有顯失公平的情形，則同意的效力將會有疑慮[431]。參考 *Naperville* 智慧電錶案，美國法院討論第三人理論（third-party doctrine）適用性時，在討論當事人是否屬於「自願性同意」時會考慮消費者是

427 參見附件一訪談紀錄第一段第 18 行開始。
428 GDPR, Article 4(11).
429 GDPR, Article 7(4).
430 個人資料保護法第 7 條 1 項。
431 同註 244。



DOI:10.6814/NCCU201900793

否具有選擇權，例如在該案中電力消費者係基於法案之要求一定只能選擇更換，那就電力消費者而言他們根本沒有選擇[432]。因此以目前實務及學界看法，在新科技應用之下，當事人所提供之「自願」同意，可能是一種「被迫的自願」同意，因為在科技時代下為了使用這些產品，不得不貢獻出自己的個人資料[433]，這會使得業者即使取得了當事人同意，也極度有可能在事後被法院認定為其取得之同意無效。

第二款　未預期之資料蒐集或分析結果可能導致同意失效

對於個人資料的目的外之利用情形，台灣與歐盟採取不同作法。台灣個人資料保護法，若該個人資料之利用不在蒐集之目的範圍時，須由當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，再行單獨所為之意思表示者，始達同意之效果[434]。但這種「事後補救措施」並無在 GDPR 中明確展現，因此當今天業者進行特定目的外之其他利用時，其所取得之當事人同意可能因之而失效。

在智慧家庭應用中，一但消費者開始在家中安裝智慧家庭設備時，這智慧家電就具備能夠連續蒐集一些資料，這些資料可能包含「未經預期之資料」或「被動蒐集之資料」[435]。舉例而言，在 Amazon Alexa 爭議中，Amazon 蒐集的是語音資料，然而負責收聽並檢視的員工曾聽到其他涉及消費者隱私的個人資訊，例如一個女人在洗澡時唱歌但卻嚴重破音，或是一個孩子在一邊尖叫著尋求幫助，也曾經聽到性侵過程的錄音檔[436]，在這些情形下可能蒐集了那些特定自然

---

[432] Naperville, 900 F.3d at 527.

[433] 劉靜怡（2002），〈網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河〉，《資訊管理研究》，第 4 卷第 3 期，頁 154。

[434] 個人資料保護法第 7 條 2 項。

[435] Sharma, Madhav, and David Biros, *Information Privacy Concerns in the Age of Internet of Things*, KSU PROCEEDINGS ON CYBERSECURITY EDUCATION, RESEARCH AND PRACTICE, 5 (2018).("Once a user possesses, configures and installs an IoT device (a wearable or home automation platform comprising sensors and actuators), the device has the capability to collect previously 'not anticipated Data' and 'passive Data' continuously, which may or may not be stored for organization's use.")

[436] 同註 365。



DOI:10.6814/NCCU201900793

人「唱歌會破音」、「受過家庭虐待」、「遭受過性侵害」等涉及隱私及敏感性個人資料的資訊。這些未預期之資料蒐集或分析得出之結果，當然也有很大的可能性因不在當初說明的個人資料類別之中，而使得其取得之同意無效。然而取得或知悉當事人這些涉及個人資料之「未經預期資料」或「未經預期的分析結果」，大多數情形業者並不一定能在一開始就料想到會有這些影響，當當事人同意失效之風險越增時，業者在推行智慧家庭時將會受到極大的阻礙或是面臨嚴峻的法遵挑戰。

### 第六項 企業合法利益與當事人資料自主權之衝突

在智慧家庭業者進行資料之剖析和自動化決策過程中，GDPR 規定當事人享有接近使用權（right to access），當資料控制者採用剖析和自動化決策進行個人資料處理時，資料主體得以請求資料控制者提供處理過程中之所涉及的邏輯性資訊以及可能預設之結果[437]。再者，當事人亦享有拒絕權（right to object），除非該剖析和自動化決策之處理係因符合公共利益（public interest）或委託行使公權力（in the exercise of official authority）所必須者，或追求正當法律利益（legitimate interests）之目的所必須者，資料主體有權基於與其具體情況有關之理由，隨時拒絕之[438]。但「處理過程中之所涉及的邏輯性資訊」及「可能預設之結果」某方面來說屬於該企業之營業秘密或是智慧資產，若屬於合法之方式蒐集處理，應有極大機率屬於該企業之正當法律利益（legitimate interests）。若無限制開放當事人擁有「揭開公司面紗」般的極大權利，將使智慧家庭業者對於投入大量資金進行智慧家庭應用與創新開發感到怯步。

然而，有其他論者認為雖然人工智慧與大數據之應用能夠進一步幫助消費者，

[437] GDPR, Article 16(1)(h).
[438] GDPR, Article 21(1).



DOI:10.6814/NCCU201900793

以比較有效率的方式、帶來生活上之便利[439]，但在未經消費者同意的情況下，蒐集、處理、利用或公開消費者之個人資料時，將損及於消費者之隱私及尊嚴[440]。因此不應過度開放當事人資料自主權之排除條款，仍應賦予當事人能夠真正自主控制其個人資訊的使用與流向之權利。從訪談之中，智慧家庭開發之業者表示對於科技業者而言，演算法的設定、消費者資訊的結果是在搶佔市佔率的關鍵[441]，因此本文認為若當事人資料自主權能夠讓企業之營業秘密或是智慧資產無影遁形時，將對智慧家庭開發之業者具有極大之影響。

### 第七項 平台整合與資訊串聯潛在之風險

從前面的市場觀察來看，各市場參與者均有屬於本身之競爭優勢，通訊服務業者，或訪談業者所稱之為系統商，具備全面性應用整合之能力；家電廠著重在產品功能及能源管理這兩塊環節亦有實力；平台廠進行 AI 語音助理處理之技術日益成熟，得以建立開放平台或提供通訊架構規範。因此，對於三方來說共同進行串聯、建立平台會是最終共同邁向的趨勢，而「共用數據、資訊」是三個市場參與者無法避免之途徑。然而對智慧家庭之消費者來說，平台整合與資訊串聯能帶來家庭生活上之便利性，但也可能帶來潛在之隱私風險，分述如下：

#### 第一款　當事人之同意是否涵蓋新加入之整合聯盟商業夥伴

如前面所介紹，智慧家庭之市場進行平台整合與資訊串聯已是必然，以訪談為例，【A 公司】與【B 公司】、【P 公司】合作共同開發智慧家庭架構時，均有將其網路與平台系統串聯【P 公司】之冷氣、冰箱和洗衣機等進行跨域整合，亦有與【B 公司】合作使消費者得以使用語音進行自動化下單外送服務[442]。以該案來說，因消費者在選購該智慧家庭套裝時，就能夠清楚知道【A 公司】與【B

[439] 同註 433，頁 145。
[440] 同註 433，頁 146。
[441] 參見附件一訪談紀錄第十段第 10 行開始。
[442] 參見附件一訪談紀錄第一段第 38 行開始。



DOI:10.6814/NCCU201900793

公司】、【P 公司】屬於共同開發之業者，因此對於消費者來說風險較低。

然而實際上，在智慧家庭開發之中，為了想把這塊市場餅作大，消費者在選購完智慧家電或建置智慧家庭網路系統後，有其他市場競爭者或合作夥伴被邀請進入該智慧家庭開發業者的平台，共同進行智慧家庭之開發與研究。這時當初販售智慧家庭產品時，取得之當事人同意範圍，是否能涵蓋新加入之整合聯盟商業夥伴？Google 就曾為了發展 Nest 計畫，開放部分用戶資料給各個產品設計商，讓他們得根據這些用戶資料設計應用服務[443]。根據目前各國之個人資料保護法制，「個人資料利用之期間、地區、對象、方式」須在蒐集時明確被告知，且當事人同意範圍限於蒐集時所清楚載明之範圍，因此只要這些新加入之合作夥伴不在當初說明之範圍者，極可能會讓這樣的資料共享處於未經當事人同意之利用。

然而各家業者在販售智慧家庭產品及招兵買馬建立平台，往往是平行在持續開發之業務，面對不同時期購買之消費者、不同時期加入合作之商業夥伴，智慧家庭市場參與者要取得所有消費者之「明確同意」非常困難且繁瑣。

第二款　整合聯盟間之科技保護措施及責任應如何分擔

GDPR 針對資料控制者賦加義務，要求資料控制者在處理個人資料時，應採取適當科技保護措施和組織規範[444]。此外，GDPR 還要求資料控制者應遵循「從設計著手保護隱私」（Privacy by Design）和「使隱私成為預設機制」（Privacy by Default）兩個概念，在創造新技術、新產品時，企業須考慮考量到現有技術、執行成本以及個人資料處理之性質、範圍、內容及目的、可能造成當事人隱私風險，並牢記個資蒐集運用應符合最小化原則[445]，並且應考量涉及的個人資料量、處理程度、存儲時間和可訪問性等，讓資料主體在一開始使用時不需透過更改設定，

[443] 同註 74，頁 35-36。
[444] GDPR, Article 24(1).
[445] GDPR, Article 25(1).



DOI:10.6814/NCCU201900793

即在系統預設的情形下，就受到 GDPR 程度之保護[446]。台灣個人資料保護法要求機關在蒐集、處理及利用個人資料時，應採取適當安全措施來保護其個人資料不被入侵、外洩，例如配置管理之人員及相當資源、界定個人資料之範圍、個人資料之風險評估及管理機制、事故之預防、通報及應變機制、個人資料蒐集、處理及利用之內部管理程序、資料安全管理及人員管理、認知宣導及教育訓練、設備安全管理、資料安全稽核機制、使用紀錄、軌跡資料及證據保存、個人資料安全維護之整體持續改善等[447]。有論文談到以資訊工程之實務發展，因個人資料處理具有複雜性和多變性，因此現階段技術上仍欠缺系統性與整合性的方法，實踐所謂的「從設計著手保護隱私」（Privacy by Design）和「使隱私成為預設機制」（Privacy by Default）[448]。基於此，當智慧家庭業者在策略上都希望產品是一個平台，能夠串聯消費者與第三方應用服務業者時，這些要求與責任對於建立平台整合聯盟的業者是非常困難執行的，因為在平台之中，每個處理個人資料之業者涉及之個人範圍跟風險都難以估計，不同的業者是否該採取相同或是不同之「適當安全措施」標準，智慧家庭之業者也無從依循。

以 Bosch 為例，Bosch 智慧型洗碗機可自動化計算清洗次數及洗碗錠用量，當洗碗錠數量不足時，會自動連接到 Amazon 線上網站服務（Amazon Dash Replenishment Service），根據用戶的設定直接自動下單洗碗錠，並會發送電子郵件確認[449]。若一方在前端建立完善個人資料處理及利用之內部管理程序，惟另一方在提供線上網站服務被認定未採取「適當安全措施」時，對於合規之一方而言，是否仍需要一同面臨違反個人資料之風險？另外，以 Amazon Alexa 及 Google Assistant 為例，消費者可以用語音方式，啟動第三方硬體廠商相關產品或服務。今在平台間共享資料、提供產品或服務時，因疏於完善資料安全稽核機制，造成

446 GDPR, Article 25(2).

447 個人資料保護法施行細則第 12 條參照。

448 徐彪豪（2016），〈物聯網時代的資料保護防線－以歐盟 GDPR 為中心〉，《科技法律透析》，第 28 卷第 10 期，頁 66。

449 同註 138。



DOI:10.6814/NCCU201900793

消費者個人資料外洩時，應負擔責任之業者為何人？不論是建立平台之主要業者、前端蒐集資料之業者，亦或是所有參與合作之業者，均可能面臨到此違法風險。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

# 第五章　給予智慧家庭市場參與業者之建議

因應大數據、物聯網和人工智慧等技術之誕生，智慧家庭產品與服務提供之業者，均期盼能透過新技術結合既有產品之研發，擴大其市場佔有率藉以獲利。從前述我們可知市場參與角色之策略，在於加強與消費者關係、讓產品作為一個平台、提供數位服務，並以平台或策略聯盟方式，帶給消費者便利性。然而觀察歐盟、美國及台灣關於資訊隱私權及個人資料保護之規定，業者盡心研發之智慧家庭應用可能存在有極高的法遵、合規風險，例如前述討論新科技所帶來之個人資料的蒐集可能多元化無法預測，所造成的影響與結果也同樣無法預測。

對於業者在智慧家庭中可能產生之法遵、合規風險，本文在前章詳細描述七大方面，包含蒐集之資料特性與類型、受規範主體之定位、資料處理分析之影響與挑戰、告知義務範圍模糊化、當事人同意機制不確定性、企業合法利益與當事人資料自主權之衝突、平台整合與資訊串聯潛在之風險等，本章將從智慧家庭市場參與者於制定管理政策時應如何進行衡量開始，並針對通訊服務業者、家電業者及平台業者三方給予策略上之建議。

國立政治大學 National Chengchi University

## 第一節　三大管理策略

### 第一項 消費者體驗與個人資料保護程度之衡量

在制定管理措施、政策時，若按照各國法規之要求，須以簡明、透明、易懂且方便取得之方式明確載明「應告知資訊」，以取得當事人具體明確之同意。為避免「自願性同意失效」之情形，並提升個人資料保護程度，智慧家庭市場參與者在銷售產品時，或消費者開始使用該產品時，以明顯方式，如彈跳窗格、頁面



DOI:10.6814/NCCU201900793

強制閱讀選項等，要求消費者確實閱讀並勾選同意。然這提升個人資料保護程度、落實完善機制，會造成消費者體驗不佳的難題。一般消費者對於產品及服務使用，講究輕鬆、快速及方便性，若在一開始購買、使用這產品時，即有繁瑣的閱讀程序，將導致消費者觀感及體驗不好，對於相關業者在進行行銷時，也會缺乏方便性。

再者，根據前述所談及，業者究竟需要達成何種程度始稱之為「落實告知義務」的難題，也對消費者體驗造成影響，若要達成個人資料保護程度高，那相較之下其「應告知資訊」的範圍及深度也會擴大，消費者閱讀起來也會比一般更為繁複。對此，本文認為即便「應告知資訊」寫得非常明確，仍無法涵蓋所有未來可能對消費者個人資料產生之影響與結果，因此已盡管理義務的標準，提及目前已知蒐集之個人資料類型、個人資料利用之期間、地區、對象、方式等，來平衡個人資料保護程度及消費者體驗，並輔以彈跳窗格、要求消費者自行勾選同意選項的方式為之。當然智慧家庭市場參與者亦應注意「應告知資訊」擺放之位置應清楚，避免如 *In Re: Vizio, Inc.* 案般，讓消費者僅能在「重置和管理」的選單下方，以非常小的字體查看到相關資訊[450]，而是應於取得當事人同意前，以舒適觀看之字體落實告知義務，並於設計介面上保留易於查找之「個資蒐集中止同意」（opt-out）欄位，以便消費者得在不耗費大量查找成本下，提出停止其個資蒐集之要求。

[450] In re Vizio, Inc., 238 F. Supp. 3d at 1212-13.



DOI:10.6814/NCCU201900793

## 第二項 取最嚴格標準設定管理政策

圖 3 設定管理政策之標準要點[451]

按照現行歐美及台灣的個人資料保護法制，三個體制下各有其強調且較為嚴格之規定，由於目前物聯網、網際網路之發達，個人資料之傳輸範圍可達全世界，接受服務之消費者可能片及全球，因此取三個法制下最為嚴格之標準設定管理政策，即可降低違反法令之風險。本文認為歐盟對於個人資料類型、當事人同意標準，美國對於商業行為準則（Code of Conduct）重視，及台灣對於「書面」同意之要求[452]，可以納入企業個人資料保護管理政策之考量。具體來說，智慧家庭市場參與者應載明個人資料類型，並以「具體明確」之當事人同意標準來訂定，從企業內部亦應將個人資料保護要求載入商業行為準則之中。

舉例而言，Amazon 應於 Alexa 隱私政策中，明確表示語音資料除會用於回答客戶的問題、滿足客戶的要求、改善用戶體驗和服務外，其處理方式係使用真人利用這些語音資料，使達到完善告知義務之程度[453]。再者，本文建議 Amazon 應制定商業行為準則（Code of Conduct）告知其承包商及員工禁止在任何地方，包含內部軟體上分享 Alexa 所蒐集之語音內容，並避免他們辦公室直接討論、分享語音內容。

---

[451] 本圖為本文所繪製。

[452] 特別說明自 2014 年台灣個人資料保護法修正後已大幅降低書面同意之要求並不限於紙本，經符合《電子簽章法》第 4 條之規定後，即可採用電子之方式。

[453] 同註 375。



DOI:10.6814/NCCU201900793

### 第三項 以資料運用過程三階段為責任分擔界線

由於智慧家庭應用涉及之市場參與者可能眾多，且共同策略上都希望產品是一個平台，能夠串聯消費者與第三方應用服務業者時，個人資料保護措施及管理機制之要求與責任對於建立平台整合聯盟是具有執行難度的。如前所述，個人資料處理所涉及之範圍與風險都難以估計，亦難以抉擇該採取相同或不同之「適當安全措施」標準。鑑於此，本文認為為推行智慧家庭應用，應使平台聯盟中之業者有責任分擔之機制。本文建議以資料運用過程三階段，包含蒐集、處理及利用來作為劃分界限，以家電業者主要負責蒐集端之要求、通訊服務業者負責處理端之安全規格，平台業者作為智慧家庭架構之主人負責利用端之管理措施，其具體應注意之事項將敘明於下方與下圖。

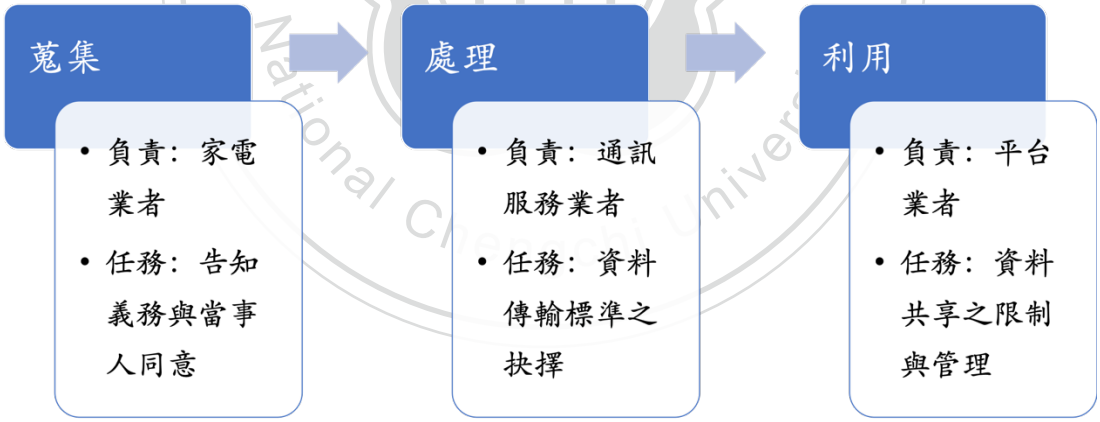


圖 4 三階段界線與業者首要任務[454]

在此，特別強調不論是資料運用過程三階段哪個環節，在提供產品及服務時應運用「從設計著手保護隱私」(Privacy by Design)和「使隱私成為預設機制」(Privacy by Default)之機制，雖然目前現階段技術上仍欠缺系統性與整合性的

[454] 本圖為本文所繪製。



DOI:10.6814/NCCU201900793

方法[455]，但以注意義務、管理責任之角度，落實現階段「一般業者大多數採取之措施」即有效果能證明以完善個人資料保護措施。以 In Re: Vizio, Inc. 案為例，美國法院就以業界慣例來認定，Vizio 並不會主動告知消費者智慧互動軟體的功能已經重新開啟，屬於高度冒犯（highly offensive）消費者的行為[456]。由此可見，就實務見解，採取「業界慣例」或「一般業者大多數採取之措施」作為「從設計著手保護隱私」（Privacy by Design）和「使隱私成為預設機制」（Privacy by Default）之機制是可行的。

國立政治大學
National Chengchi University

455 同註**錯誤! 尚未定義書籤。**，頁 66。
456 In re Vizio, Inc., 238 F. Supp. 3d at 1233.



DOI:10.6814/NCCU201900793

## 第二節　對家電業者建議

### 第一項 告知義務與當事人同意

作為最前端的蒐集方，家電業者除無法避免被認定為資料控制者外，如同守門員般，須於前端確實作好告知義務，取得當事人同意。本文認為就當事人同意部分，有兩點須特別注意，其一係因智慧家庭可能涉及之個人資料種類橫跨一般性個人資料及特殊性個人資料，因此應一律採取高標準之「具體明確」當事人同意，使消費者自行勾選同意以落實其隱私選擇權外，亦讓消費者了解其個人資料將被如何運用，始能避免違法之風險。例如訪談中，個案之消費者在選購該智慧家庭套裝時，就能夠清楚知道【A公司】與【B公司】、【P公司】屬於共同開發之業者，因此其所可能獲得之消費者同意較不易失效。

再者其二，係因應台灣個人資料保護法要求，對於特殊性個人資料應獲得當事人之書面同意，因此本文建議，對於可能於日後被認定為敏感性資料之個資類型(包含如前章分析，透過比對可間接得知或高度確信所蒐集個資為當事人健康、性生活/傾向之相關類型等)，即使採取電子應告知說明及同意選項，可考慮採用電子簽名之技術，更加穩固同意之效力。

### 第二項 盡可能採取數值蒐集模式並設定內部存取權限

因語音資料、影像資料與該特定人直接程度較高，因此能識別該特定自然人程度較高，故本文建議當業者可以採取數值資料之蒐集時，盡量避免直接進行語音、影像資料之蒐集，或可事先採用邊際運算之方式，將語音、影像資料先進行初步去識別化、匿名化之處理，以降低對於特定自然人個人資料或隱私權之侵害。

不論是數值、語音或是影像資料，當匯入家電業者或合作商業夥伴之後端雲



DOI:10.6814/NCCU201900793

端平台時，應確保落實內部存取權限之設定，並在內部相關單位，如研發部門、行銷部門需取用相關資料時，加入法務部門、個人資料保護官（DPO）之事前許可機制，以確保在個人資料處理、利用過程中，不存在極高的違法可能，以降低風險。例如 Amazon Alexa 智慧音箱爭議中，負責進行 Alexa 語音資料之處理的員工，能夠知道知道該用戶的設備序號、Amazon 帳號及用戶的聲音特徵，這些資料雖然單獨觀察無法得知具體特定該自然人，然而透過連結可能推敲出特定人[457]，因此在這些語音資料處理及利用之過程中，應設定更嚴格之權限，避免員工能知道該用戶的設備序號、Amazon 帳號，僅提供用戶的聲音特徵跟代碼，並在前階段使法務部門、個人資料保護官（DPO）參與其中，評估相關流程及風險。

### 第三項 當事人權利行使和企業揭露範圍

根據歐盟之個人資料保護法規定，資料主體得以請求資料控制者提供處理過程中之所涉及的邏輯性資訊以及可能預設之結果[458]。本文認為在兼顧企業之營業秘密或是智慧資產保護，和當事人權利衡量之下，家電業者必須揭露其特定當事人之個人資料係如何被使用，例如可能被用來推敲何種資訊、作為何種行銷、研究之方向，並且推導出之結果為何等。

此外本文建議關於「處理過程中之所涉及的邏輯性資訊」應包含揭露在處理過程中所有可能涉及之廠商，已確保其真正知悉、自主控制個人資訊的使用與流向。然而揭露之範圍不應包含處理之人工智慧演算法之技術細節。因本文認為演算法的設定與個人資料之利用雖有關聯，惟對當事人個人資料最有影響應是「可能預設之結果」，演算法設定對於科技業者來說具備營業秘密或智慧資產之成份較大，因此仍因保留適度商業保護空間。

---

[457] 同註 365。
[458] GDPR, Article 16(1)(h).



DOI:10.6814/NCCU201900793

## 第三節　對通訊服務業者建議

### 第一項 以資料控制者定位進行資料處理

雖然目前智慧家庭市場上，通訊服務業有以系統商之定位，提供一個平台給設備商進行資料之傳遞，認為自身並非是資料控制者，不進行個人資料之蒐集。然而在其傳遞資料之過程中，仍存在有「與他人共同決定個人資料處理之目的與方法」的可能性，且可能直接被推定為資料控制者。因此，本文建議通訊服務業者應全面採取資料控制者之立場，來進行個人資料之處理，且不可輕易認為本身得免除 GDPR 或個人資料保護法，賦予他們的告知義務及相關資料控制者應遵循之要求。例如根據訪談中之【A 公司】、【B 公司】及【P 公司】的智慧家庭專案，【P 公司】設有 DONGO 感測器於其智慧家電設備之中，而這顆 DONGO 裡的資料必須要透過【A 公司】的 E-Panel 傳輸管道，將相關指令傳輸至【P 公司】的後端系統[459]，雙方除須事先協商好串接之 protocol 介面進行資訊的交換外，應特別注意其合作之家電業者是否落實當事人告知義務，並在傳輸串接之過程，符合加密、安全性之要求。

### 第二項 資料傳輸標準之抉擇

在資料傳輸過程中，可能面臨到機密性、驗證還是接近使用的安全性風險。尤其是在跨界合作的同時，全球又有非常多的通訊協定，如 IPSO 通訊標準、TaiSEIA 101 通訊標準等。目前就傳輸過程之安全性，分為兩種方式，其一是由各業者自負擔其資料運輸、蒐集之線路，如同訪談業者所採取；其二係由單一業者統一負擔。目前為了分散風險與成本大多採取第一種模式，然而本文認為雖然

[459] 同註 409。



DOI:10.6814/NCCU201900793

第二種模式將造成通訊服務中者產生之責任較大，但統一之安全性規範可能更加降低消費者之個資多方傳輸風險，且在安全性完善之過程亦更容易成為市場的領導品牌。因此本文認為兩種模式均可提供予智慧家庭業者做為參考，進行管理政策之衡量。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

## 第四節　對平台業者建議

### 第一項 資料共享之限制

平台業者其主要策略為串聯所有家電、第三方服務業者，在未來趨勢上極有可能成為智慧家庭主要市場核心。因此其應扮演制定資料安全稽核機制之業者，並要求、監督所有智慧家庭市場參與者在平台間共享資料、提供產品或服務時，落實相應資料安全稽核機制。對於「資料安全稽核機制」或「適當安全措施」，本文建議平台間共享之之資料應限制在「數值」，且不具備串聯至特定自然人之帳號，除非經過該自然人明確具體之同意。

再者，若是平台業者透過雲端分析所得之結果，有共享之利益時，本文認為可以採用總體趨勢圖的方式，共享給其他平台業者。以 Bosch 智慧型洗碗機為例，家電業者 Bosch 與平台業者 Amazon 合作，使其洗碗機得自動化計算清洗次數及洗碗錠用量，且當洗碗錠數量不足時，會自動連接到 Amazon 線上網站服務（Amazon Dash Replenishment Service）進行下單之服務[460]。在這種聯盟模式之下，雙方係根據用戶的設定直接自動下單洗碗錠，並會發送電子郵件確認，屬於經過該自然人明確具體之同意，而連結到該特定自然人之帳戶。然而後續若 Amazon 或 Bosch 想針對消費者使用資訊進行分析、共享時，除非有當事人具體表示同意其分析、共享，否則採取總體趨勢圖方式共享應較為妥當。

### 第二項 行業慣例之去識別化手段

由於實務見解 In Re: Vizio, Inc. 案及前述 Amazon Alexa 智慧音箱爭議案，例行性的個人資料蒐集可能是非常冒犯的（highly offensive），且會透過行業慣例之

[460] 同註 138。



DOI:10.6814/NCCU201900793

比較，來斷定業者是否存有有高度冒犯消費者隱私權的行為[461]。以目前平台業者而言，不論是 Google、Apple 或 Amazon，均有設置智慧音箱來控制家庭設備或提供家庭娛樂服務。參照幾家去識別化方法，本文建議就語音資料審聽部分應以片段為之且不得與可識別個人資料有串聯，可採取隨機識別號碼方式做標記。此外在使用真人收聽的過程中，修改用戶聲音（如採取變音方式），以防止用戶的身份遭識別。

作為個人資料利用之中心，平台業者也應以契約之方式要求其他商業合作夥伴一同遵守個人資料保護法之要求，例如採取相同標準之去識別化手段，以免在平台上傳輸、共享及利用過程中侵害消費者個人資料和隱私權，連帶損及平台業者之商業利益及聲譽。

### 第三項 平台策略與當事人權利行使

由於本文大膽推測平台業者係未來智慧家庭應用之核心，且本文認為平台業者因涉及語音資料蒐集，能剖析之資料面向亦較全面且具直接性，能推導出消費者偏好較為廣泛，造成之消費者分析影響也較為顯著。因此，本文認為平台業者應作為當事人權利行使應對及處理窗口。例如 Apple 或 Amazon 可以從串聯之業者推導出使用家電品牌喜好，且從提供網路訂單或串連手機等服務中，取得其他個人帳戶資料（例如 iPhone 或 Amazon 帳號）等，也可以知悉該帳戶可能串聯之業者包含何者，因此對於平台間應如何訂定個人資料審查、彙報程序因較為容易。

本文建議平台業者得建立相應管理機制和程序，要求所有商業合作夥伴執行，當消費者有個人資料爭議時，統一由平台業者進行處理與應對。再者，因應彙整各式消費者的隱私問題後，平台業者更能定期修改隱私政策，與其他業

[461] In re Vizio, Inc., 238 F. Supp. 3d at 1233.



DOI:10.6814/NCCU201900793

者討論並向消費者定期更新隱私政策，以落實個人資料保護法制之要求。

國立政治大學
National Chengchi University



DOI:10.6814/NCCU201900793

# 第六章　結論

大數據、物聯網和人工智慧等技術之發展，使個人智慧終端設備能發展成智慧家庭設備時，帶來人類之生活之方便性，也帶來個人隱私權安全問題。美國法上俗稱之「家即為城堡」(My home is my castle)已被智慧家庭的物聯網技術打破，只要透過感知層、網路層，即可將家中個人資訊進行傳遞和控制。面對潛在的資訊安全和法遵風險，在現行歐美及台灣的個人資料保護法制以及目前及潛在應用之下，無法避免可能產生消費者隱私爭議，和隱私保護不夠完善的問題。面對新科技對於「家庭內部的隱私權及個人資料」應用比以往更為多元，不僅是實務見解必須正視其造成隱私權影響與結果多元化且無法預測，智慧家庭的業者面對創新挑戰，也必須制定相應管理措施。

因此在分析市場參與角色之市場策略，包含加強與消費者關係、讓產品作為一個平台、提供數位服務，並以平台或策略聯盟方式，帶給消費者便利性後，本文點明業者在智慧家庭中可能面臨的七大法遵、合規風險，例如蒐集之資料特性與類型、受規範主體之定位、資料處理分析之影響與挑戰、告知義務範圍模糊化、當事人同意機制不確定性、企業合法利益與當事人資料自主權之衝突、平台整合與資訊串聯潛在之風險等。

最後，本文建議智慧家庭市場參與者於制定管理政策時，應取最嚴格之標準作為基礎，並以資料運用過程三階段(蒐集、處理及利用)作為責任分擔界線，並參考本文給予通訊服務業者、家電業者及平台業者策略上之建議，進行下一步戰略之擬定。

國立政治大學 National Chengchi University



DOI:10.6814/NCCU201900793

# 參考文獻

一、中文文獻

（一） 專書


1. 大西可奈子（著），許郁文（譯）（2018），《超圖解！〈認識〉AI 人工智慧的第一本書》，台北：碁峰。
2. 古亞薇、張佳蕙、張家維、莊則敬、許桂芬、陳賜賢、無線與寬頻通訊研究團隊、網路前瞻技術研究團隊（2015），《智慧家庭發展趨勢與應用案例分析》，台北：資策會產業情報研究所。
3. 裴有恆、陳玟綺（2018），《AIoT 人工智慧在物聯網的應用與商機》，台北：碁峰。


（二） 期刊


1. 尤重道（2017），〈個人資料保護之概念與蒐集處理利用暨違法責任（上）〉，《全國律師》，第 21 卷第 7 期。
2. 王文娟（2016），〈物聯網概念及應用〉，《經濟前瞻期刊》，第 168 期。
3. 李建良（2017），〈資料流向與管控環節-個資保護 ABC〉，《月旦法學雜誌》，第 272 期。
4. 林利芝（2016），〈Katz v. United States（三）－電子監聽科技侵犯個人隱私的經典案例〉，《台灣法學雜誌》，第 303 期。
5. 林勤富、劉漢威（2018），〈人工智慧法律議題初探〉，《月旦法學雜誌》，總號 274 期。
6. 范姜真媺（2017），〈大數據時代下個人資料範圍之再檢討—以日本為借鏡〉，《東吳法律學報》，第 29 卷第 2 期。
7. 徐彪豪（2016），〈物聯網時代的資料保護防線－以歐盟 GDPR 為中心〉，《科技法律透析》，第 28 卷第 10 期。
8. 翁清坤（2018），〈賦予當事人個人資料財產權地位之優勢與侷限:以美國法為中心〉，《臺大法學論叢》，第 47 卷第 3 期。
9. 陳計策、賴宛靖（2018），〈迎接 AIoT 智慧時代〉，《工業技術與資訊月刊》，第 315 期。
10. 葉志良（2016），〈大數據應用下個人資料定義的檢討：以台灣法院判決為例〉，《資訊社會研究》，31 期。
11. 葉志良（2018），〈因應物聯網發展資料保護法制的革新——歐盟法制的發展與啟示〉，《中原財經法學》，第 40 期。
12. 劉定基（2010），〈「個人資料保護法」初論〉，《台灣法學雜誌》，第 159 期。
13. 劉定基（2013），〈析論個人資料保護法上「當事人同意」的概念〉，《月旦法學雜誌》，第 218 期。
14. 劉靜怡（2002），〈網際網路時代的資訊使用與隱私權保護規範：個




DOI:10.6814/NCCU201900793

人、政府與市場的拔河〉,《資訊管理研究》,第 4 卷第 3 期。
15. 劉靜怡(2019),〈淺談 GDPR 的國際衝擊及其可能因應之道〉,《月旦法學雜誌》,第 286 期。
16. 鄭福炯、王岱鑫、劉威成(2017),〈智慧物聯網系統平台－以智慧家庭為例〉,《電腦稽核期刊》,第 35 期。

(三) 研究報告

1. 石立康(2016),〈智慧家庭市場大趨勢〉,《IEK 產業分析報告》。
2. 石立康(2016),〈智慧家庭資安防護技術及解決方案〉,《IEK 產業分析報告》。
3. 石立康(2017),〈評 Amazon Alexa 發展策略〉,《IEK 產業分析報告。
4. 石立康、鄭淑方(2016),〈智慧家庭之整合性平台與多元應用趨勢〉,《IEK 產業分析報告》。
5. 池煥德(2018),〈智慧家庭中的居家健康需求探索〉,《IEK 產業分析報告》。
6. 李俊賢(2016),〈無線感測網路與 ZigBee 協定簡介〉,http://www.ecaa.ntu.edu.tw/weifang/WSN/WSN_ZigBee intro.pdf。
7. 周碩彥,〈「物聯網發展趨勢展示內容」研究報告〉,https://www.naer.edu.tw/ezfiles/0/1000/attach/95/pta_9695_1581881_06359.pdf。
8. 金美敬(2017),〈LG 電子智慧家庭策略分析〉,《IEK 產業分析報告》。
9. 陳右怡(2017),〈居家機器人大戰開打,智慧家庭領導業者洗牌中〉,《IEK 產業分析報告》。
10. 陳佳榮(2017),〈國際平台大廠於智慧家庭發展策略分析〉,《IEK 產業分析報告》。
11. 蔡敦仁、蘇俊吉、許博堯、吳佩霏、林政諺,〈「通傳事業去識別化技術與相關技術規範研究」補助研究報告〉,https://www.ncc.gov.tw/chinese/files/18031/3923_38917_180315_1.pdf。

(四) 碩博士論文

1. 王瑞文(2000),《實體模擬技術運用於撥弦樂器,滑音處理與古琴輸入法之人機介面研究》,中華大學資訊工程學系碩士論文。
2. 余瑞陞(2014),《權利化的隱私－反思現代國家法律下的個人隱私》,國立政治大學碩士論文。
3. 鍾孝宇(2017),《巨量資料與隱私權—個人資料保護機制的再思考》,國立政治大學碩士論文。

(五) 司法裁判

1. 司法院釋字第 603 號。

(六) 網路資源

1. Amazon AWS 網站,〈Amazon Web Service(AWS)－雲端運算服務〉,https://aws.amazon.com/tw/。
2. Amazon 網站,〈AWS Case Study: LG Electronics〉,https://aws.amazon.com/tw/solutions/case-studies/lg-electronics/。



DOI:10.6814/NCCU201900793

3. Bosch 智慧互聯行銷報告（2017），https://media3.bosch-home.com/Documents/MCDOC02048462_Bosch_Home_Connect_PDF_Brochure_1-25.pdf。
4. Bosch 智慧冰箱專利說明書（2014），https://patentimages.storage.googleapis.com/44/a7/69/84e37502b5dd52/WO2014198632A1.pdf。
5. Bosch 網站，〈Privacy statement〉，https://www.bosch-smarthome.com/uk/en/privacy-statement。
6. Comparitech 網站，〈Consumer privacy bill of rights〉，https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/。
7. Digitimes 網站，〈ZigBee 無線感測網路技術自動控制應用環境〉，https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000293659_ymv5w76t6lv2gy85axfe0。
8. Emarketer 網站，〈Looking for a New Product? You Probably Searched Amazon〉，https://www.emarketer.com/content/looking-for-a-new-product-you-probably-searched-amazon。
9. Foxbussiness 網站，〈CES 2019: 5 things to watch at techs biggest convention〉，https://www.foxbusiness.com/technology/ces-2019-5-things-to-watch-at-techs-biggest-convention。
10. Home Connect 網，〈Amazon Dash〉，https://www.home-connect.com/global/connected-partners/shopping-ordering/amazon-dash。
11. Home connect 網站，〈Connected Partners〉，https://www.home-connect.com/global/connected-partners。
12. IBM 網站，〈Watson IoT platform〉，https://www.ibm.com/tw-zh/internet-of-things/solutions/iot-platform/watson-iot-platform。
13. Inside 網站，〈從新一代 TPU 到 Google.ai，詳解 Google I/O 首日人工智慧五大亮點〉，https://www.inside.com.tw/article/9351-google-ai-google-io。
14. OMA SpecWorks 網站，〈IPSO Smart Objects〉，https://www.omaspecworks.org/develop-with-oma-specworks/ipso-smart-objects/。
15. Ithome 網站，〈【2019 年關鍵趨勢】3AIoT 技術商品化，帶起企業新型態物聯網應用浪潮〉，https://www.ithome.com.tw/news/127912。
16. LG Home Chat 網站，〈關於我〉，http://www.lghomechat.com/us/。
17. LG 網站，〈LG 2017 年全系列物聯網智慧家電強勢登台！業界最完整內建 WiFi 智慧家電 SmartThinQ APP 一指全串聯，立即啟動便利、安心、節能美好生活〉，https://www.lg.com/tw/press-release/20170417-lg-



DOI:10.6814/NCCU201900793

2017-smartthinq-app。
18. Mora Chen（2018），〈人工智慧大歷史〉，https://medium.com/@suipichen/ffe46a350543。
19. Nvidia 網站，〈雲端運算解決方案〉，https://www.nvidia.com.tw/object/gpu-cloud-computing-tw.html。
20. SAP 網站，〈什麼是物聯網 (IoT)？〉，https://www.sap.com/taiwan/trends/internet-of-things.html。
21. Simonlakey 網站，〈Connected home vs Smart home〉，https://simonlakey.com/connected-home-vs-smart-home/。
22. TechOrange 網站，〈【CES 2018】LG 梭哈智慧家電：發布 ThinQ AI 平台，讓所有家具能夠互相聊天！〉，https://buzzorange.com/techorange/2018/01/09/lg-new-thinq-ai-brand/。
23. Valuewalk 網站，〈Smart Homes Are So Yesterday. Today It's About Intelligent Homes〉，https://www.valuewalk.com/2018/10/intelligent-home-next-stage-evolution/。
24. 上海情報服務平台網站，〈IPSO 聯盟介紹〉，http://www.libnet.sh.cn:82/gate/big5/www.istis.sh.cn/list/list.aspx?id=6575。
25. 大和有話說網站，〈完整解析 AI 人工智慧：3 大浪潮＋3 大技術＋3 大應用〉，https://dahetalk.com/2018/04/08/%E5%AE%8C%E6%95%B4%E8%A7%A3%E6%9E%90ai%E4%BA%BA%E5%B7%A5%E6%99%BA%E6%85%A7%EF%BC%9A3%E5%A4%A7%E6%B5%AA%E6%BD%AE%EF%BC%8B3%E5%A4%A7%E6%8A%80%E8%A1%93%EF%BC%8B3%E5%A4%A7%E6%87%89%E7%94%A8%EF%BD%9C/。
26. 中華電信智慧家庭網站，〈服務介紹〉，http://www.dhs.hinet.net/Service_01.html。
27. 中華電信網站，〈智慧家庭商品介紹〉，https://www.cht.com.tw/home/enterprise/ict/smart-service/smart-home。
28. Taiseia 網站，〈AI 語音智能管家報到 中華電信 eHome 智慧家庭再進化〉，http://www.taiseia.org.tw/Industry/industry_more?id=100。
29. 北美智權報網站，〈語音助理大戰，Alexa 大勝 Siri〉，http://www.naipo.com/Portals/1/web_tw/Knowledge_Center/Industry_Economy/IPNC_180223_0702.htm。
30. 台灣智慧能源產業協會網站，〈智慧家庭物聯網主從通訊架構標準正式發佈〉，http://www.taiseia.org.tw/News/news_more?id=15。
31. Offweek 物聯網站，〈一文了解物聯網：定義、概念到應用〉，https://iot.ofweek.com/2017-03/ART-132202-11000-30118661.html。



DOI:10.6814/NCCU201900793

32. 每日頭條網站，〈瞄準碎片化 IoT 市場，看清 Bosch 在傳感器領域三大策略！〉，https://kknews.cc/zh-tw/tech/qnoe93o.html。
33. 研之有物網站，〈斷開中文的鎖鍊！自然語言處理 (NLP)〉，http://research.sinica.edu.tw/nlp-natural-language-processing-chinese-knowledge-information/。
34. 科技產業資訊室網站，〈谷歌想利用 Smart Display 打破亞馬遜於智慧家庭優勢〉，http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=14183。
35. 科學月刊網站，〈機器是如何學習與進步？人工智慧的核心技術與未來〉，http://scimonth.blogspot.com/2018/03/blog-post_56.html。
36. 國家發展委員會網，〈歐盟 GDPR 法規〉，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY5MS9iNGZiZTA0OS1jYWQ1LTQ3MGEtYjhlMy00ZGU0NjhmOWIxMGMucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2bd6K236KaP5YmH5pys5paH6YOo5YiGLnBkZg%3d%3d&icon=..pdf。
37. 康乃爾法學院網站，〈Fourth Amendment〉，https://www.law.cornell.edu/constitution/fourth_amendment。
38. 經濟日報（8/1/2019），〈LG 電子參展 CES 推 ThinQ AI 旗艦電視〉，https://money.udn.com/money/story/5612/3580972。
39. 經濟部工業局智慧電子產業計畫推動辦公室網站，〈智慧載具產業現況〉，https://www.sipo.org.tw/industry-overview/industry-status-quo/smart-home-industry-status-quo.html。
40. 資策會科技法律所網站，〈美國發布了「消費者隱私權法」草案〉，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=148&d=6852。
41. 維基百科網站，〈ELIZA〉，https://en.wikipedia.org/wiki/ELIZA。
42. 維基百科網站，〈人工智慧〉，https://zh.wikipedia.org/wiki/%E4%BA%BA%E5%B7%A5%E6%99%BA%E8%83%BD。
43. 遠東醫療科技網站，〈合作案例-中華健康雲〉，http://www.femet.com.tw/product_1015884.html。
44. 遠雄企業網站，〈遠雄二代宅 2.0 革命性智慧躍升〉，https://www.farglory.com.tw/news/message/detail/101。
45. 數位時代網站，〈果粉醒醒！蘋果智慧喇叭 HomePod 五個讓人不買的理由〉，https://www.bnext.com.tw/article/47919/apple-homepod-price-features-vs-echo-google-home-ipod-history。
46. 歐盟委員會網站，〈Requirements of Trustworthy AI〉，https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1#privacy。



DOI:10.6814/NCCU201900793

47. 歐盟委員會網站，〈EUR-Lex - 52017PC0010 - EN〉，https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010（最後瀏覽日：2019/7/25）。
48. 隱科技網站，〈Computex 2018 ： Arm 展示低功耗邊際運算人工智慧，以及智慧城市、智慧家庭應用〉，https://www.cool3c.com/article/135498。

（七） 其他

1. 法務部（71）法律字第 9168 號函。
2. 司法院釋字第 689 號解釋部分協同及部分不同意見書。

二、英文文獻

（一） 專書

1. Goodman P. Ellen, *THE ATOMIC AGE OF DATA: POLICIES FOR THE INTERNET OF THINGS*(2015).

（二） 期刊論文

1. Atzori Luigi, Iera Antonio & Morabito Giacomo, *The Internet of Things: A survey*, 54 Computer Networks 2787(2010).
2. Barbas Samantha, *Saving Privacy from History*, 61 DePaul L. Rev. 973(2012).
3. Feiler Jesse, *Learn Apple HomeKit on iOS*, Apress Berkeley(2016).
4. Hochheiser Morgan, *The Truth Behind Data Collection and Analysis*, 32 J. Marshall J. Info. Tech. & Privacy L. 32(2015).
5. Lin Huichen & Bergmann W. Neil, *IoT privacy and security challenges for smart home environments*, 7(3) Info. 44(2016).
6. Nguyen Vincent, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535(2019).
7. Pan B. Sheri, *Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze*, 30 Harv. J.L. & Tech. 239(2016).
8. Poudel Swaroop, *Internet of things: underlying technologies, interoperability, and threats to privacy and security*, 31 Berkeley Tech. LJ 997(2016).
9. Rustad L. Michael, Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 Harv. J.L. & Tech. 349(2015).
10. Scherer U. Matthew, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 Harv. J.L. & Tech. 353(2016).



DOI:10.6814/NCCU201900793

11. Warren D. Samuel & Brandeis D. Louis, *The Right to Privacy*, 4 Harv. L. Rev. 193(1890).
12. Whitman Q. James, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151(2004).

（三） 研究報告

1. ARTIFICIAL INTELLIGENCE AND PRIVACY, ARTIFICIAL INTELLIGENCE AND PRIVACY 1–30 (2018), https://www.Datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.
2. Zhang Dongpo, *Big Data Security and Privacy Protection*, PROCEEDINGS OF THE 8TH INTERNATIONAL CONFERENCE ON MANAGEMENT AND COMPUTER SCIENCE(2018).
3. High-Level Expert Group on Artificial Intelligence (2019), *Ethics guidelines for trustworthy AI*, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58477.
4. Sharma, Madhav, and David Biros, *Information Privacy Concerns in the Age of Internet of Things*, KSU PROCEEDINGS ON CYBERSECURITY EDUCATION, RESEARCH AND PRACTICE(2018).

（四） 司法裁判

1. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018).
2. In Re: Vizio, Inc., Consumer Privacy Litigation, 238 F. Supp. 3d 1204 (C.D. Cal. 2017).
3. Yershov v. Gannett Satellite Information Network, Inc., 104 F.Supp.3d 135 (D. Mass. 2015).
4. In re Vizio, Inc., Consumer Privacy Litig., Order Granting Plaintiffs' Motion For Preliminary Approval Of Class Action Settlement, Doc. 282(C.D. Cal. 2019).
5. Camara v. Municipal Court, 387 U.S. 523 (1967).
6. Kyllo v. United States, 533 U.S. 27 (2001).

（五） 政府報告

1. Norwegian Data protection authority, *Artificial intelligence and privacy*, 3(2018), https://www.Datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

（六） 網路資源

1. Kevin Ashton, THAT 'INTERNET OF THINGS' THING, http://www.rfidjournal.com/articles/view?4986.



DOI:10.6814/NCCU201900793

# 附件一 訪談紀錄

一、訪談概要

（一）受訪談者：甲、乙，【A 公司】智慧家庭服務開發者。

（二）研究者：丙。

二、訪談過程

（一） 第一段

甲：其實像我講的。我應該這樣子講，【A 公司】它是一個系統商，不是設備商，所以基本上我們是提供平台，那設備商，他們會去發展他們的應用，他可能會實際上碰到什麼樣子的應用時候，他透過系統商這個介面跟平台來傳出去。那我們是系統商的時候，我們其實會有一些客戶的資料，甚至客戶在傳送的時候，他用了多少的量，因為系統就跟你的行動電話有關，我今天知道說這個行動電話是誰申請的，他打了多少錢？ 打了多少電話？ 講了幾分幾秒？ 我才有辦法去批價，對不對？ 我才有辦法去批價，所以系統商一定會有這個資料，只是說系統商拿了這個資料，它必須做了那些應用，那我覺得供應商阿，我不知道他們會不會收這個。但他們一定會有說，這個產品開發處，User 在使用這個產品的時候，他可能會回饋一些訊息，好不好用？或怎麼樣？他會有一些抱怨回來？那你就會對這些資訊去做改善，對不對？ 我相信設備商他們一定也會做這塊，那其實，以我們的角度的時候，其實就很簡單，我們就是提供一個平台，然後給設備商做這個資料傳遞。

乙： 我先針對你目前列的大項目議題，我要先跟你說一下，因為有一些寫的可能方式有問題的，我們先從第一點，智慧家庭是否會蒐集的資料或習慣的部分。這個來講，以目前台灣的環境，它是沒有被允許可以是蒐集客戶的資訊，就法律層面上來講是不允許的，因為就算我們在系統建置完成後，客戶交屋的情況下，沒有給客戶所謂的承諾切結，他願意提供這樣的資訊回饋給我們。所以智慧家庭系統，它好比就像一棟建築物，Building 建置在裡面，而這個屋主買了這個房子之後，這就是他的產權，所以你必須尊重這屋子是他的，裡面所有任何事情都是他的，如果他同意我才能蒐集，所以以目前台灣的市場來講，還沒有一家可以提供說，我無條件蒐集資訊，而你無條件提供給我分享，這都需要客戶的同意。可是以目前的系統來講，大家沒有去做這個資料的蒐集。所以像你第一點的部分，蒐集的資料是什麼樣的類型？這個憑良心來講，他沒有蒐集的前提，但是呢？對於我們智慧家庭系統，因為你先前有研究過，所以你可以很清楚地去把它分成兩大類，或者是三大類。第一類是屬於安防的部分，第二類是所謂的加值，也就是所謂的情境控制，第三類就是有關能源管理，像家裡人員的用電、用水資訊，大概可以分成這三代類型。那這三大類型裡面，因為你裡面有寫到家中的影像使用次數或使用習慣、偏好的部分，這其實應該是要去解讀成，比如說，如果我們今天家裡有瓦斯遮斷閥這個安全設備，是跟瓦斯表一起整合的，可是相對的，他是跟廚房天花板裡的瓦斯偵測器，像假如我瓦斯洩漏的時候，他會去做連結連動，



DOI:10.6814/NCCU201900793

那這個部分才是對客戶來說是必備的基本功能，可是呢？你要以客戶的角度去思考是說，我今天冬天外面 10 度，我還要出去外面開瓦斯跟關瓦斯，是不是很麻煩，所以這時候，你的情境功能就會出來，就可以去幫客戶預設說，我幫他做一個連動開關，可以讓他在家裡面，不用出後陽台，我就可以去把這個功能去開啟或者關閉，這是一個貼心的服務，亦即是精緻化的應用，那這是安全的部分。所以你家電使用次數的習慣部分我會把它解讀成，比如說家電，我們會有冷氣電視等等，連同現在【A 公司】，畢竟跟【P 公司】合作，那跟他們所謂冷氣／冰箱／洗衣機都有做整合，所以這是有點導入 IoT 的感覺，所以他可以藉由這些 IT 化的設備，我們幫他做所謂的開光的連結，也就是說冷氣，我們室內有搭配溫度、濕度的感測，我感測到室內溫度過高，冷氣可以自動打開，我有設置這個情境允許它可以去這個動作，所以這個資料蒐集，我們沒有必要去蒐集他，因為每個家庭的環境不一樣，今天這個家庭 10 個人，隔壁 1 個人，他條件是不同的，所以我蒐集他這個 Data 是沒有意義的，因為我沒有辦法去分析這是不是可以普及化應用的東西。但是這個是屬於說，這是什麼樣的房子？什麼樣的人來買？要符合到她什麼樣的條件？好比今天是自己買的房子，它標榜就是要科技，可是你如果一般消費客戶來講，他沒有辦法去負擔這樣子的支出，因為它可能光買一個基礎的房子就已經是極限，他沒有辦法在賦予你裡面還要有所謂的特殊功能，因為目前所有的智慧家庭，他都會牽扯到智慧，都是附加的，就好比今天我汽車可以買標準品也可以買豪華品，那就是它裡面的配備不同。

甲：林志穎為什麼要買科技？

乙：林志穎他的家是很科技的，他會去把很多可兜起來的東西兜再一起，它其實在很早之前就已經兜起來了，當然對在那個時代，設備的演進還沒有那麼快，所以相對他要附加的，比如說她要在家裡建置一個 Sever 機感，那才可以去達到目前我們看到這些的東西，因為時代的演進，連同現在軟體的平台，比如說 Android／IOS 平台的普及，大家去寫這個 App 就很快、很方便，他就可以去產生這個連動的動作。

（二） 第二段

乙：那第三點你說，資料傳輸的過程次否要加密？加密這個動作是必須的，只是他今天是在一個屬於內部環境的網路系統，他不會對外連，這是一個智慧家庭系統裡面，他最基本的環境，他一定是封閉是內網。那加密一定是必然的，因為畢竟我是戶對戶，所有的資訊串聯到中控室或者防災中心，去做這個所謂資料的傳輸跟加密化，那加密的過程中，勢必會有資料產生，所以以我們的系統來講，不僅加密之外，我們還會在各戶設置一個防火牆，那這樣子，他才有辦法去阻擋一些基本的駭客，那當然你是有心人，那勢必還是有辦法可以突破，沒有任何一個軟體系統沒有辦法被突破。

乙：那第二點你說是否會透過外部網路或協力廠商來協助？畢竟這個部分【A 公司】的產品，所以是由我們的數據公司跟研究院共同開發的，那以目前來講，我



DOI:10.6814/NCCU201900793

的使用習慣下來，這套平台算是最穩定的。那就樣講當然會很臭屁，但我只能講說我們在這套平台上的運作，我們客訴率跟相對其他 SI 比起來是比較低，那當然你說跟國外的比，像 Apple 他也有出所謂的 E-home，Amazon 也出了聲控系統部分，後續也會出來，這個跟國外比起來，我很難去評斷，告訴你說是不是更穩定。因為畢竟國際品你還有一個最重要的傳輸問題，你今天這個聲控系統，這講得有點遠，可是他可以延伸到很多東西是，你這個聲控喇叭，我買的是 Google 或 Amazon 的，它的 Data 資料庫 Server 在哪裡？是在他們的國家，所以你是要藉由，不管你是哪一家 ISP 業者網路，連到那邊去，而且已經離開台灣再回來。如果 Google 現在是在板橋那要設所謂的企業總部，那可能或許他們有些東西會直接回到這邊，但我相信絕大部分的數據資料，尤其聲控的部分，它的訊息會回到他們家的 Server，或在國外，如果【A 公司】海纜或其他業者海纜斷線，很抱歉你的聲控系統是失效的，所以這個很難去跟你斷定，就是說它穩不穩定，因為當海纜斷了，你就是一個獨立的線了，但是以我們自己內部台灣建置的環境下，我們是內部完善，除非是你這這棟大樓被砍斷了，要不然原則上我們並沒有所謂的出去再回來的問題，那第二個問題，剛提到的，這個系統若是真的有心人，這個聲控我把訊號傳出去，中間被抽走了，你是不會發現的，這個風險先對是更高的，而你這段訊息出去的過程中，是沒有經過任何阻擋的，所以任何時間點他是可以插入的。

丙：　那這樣子，比如我在台灣買 Alexa，因為會連網路，那如果是連【A 公司】的網路，那他錄音的之後，它是透過【A 公司】的網路傳到國外去？

乙：　他會是用封包，比如說 1MB 的封包，我可能會割成 100 個小封包，然後在同時傳出。

甲：　這就變成跑 Internet 了。

乙：　對！

甲：　因為你這個是，我們語音的東西要在網路上跑，因為網路上我們跑的是 IP，那語音的訊號是類比，所以他一定要把他打包成 IP 的封包，然後丟到 IP 的網路上去傳，但是這個有個聲控丟掉公用網路上去傳的時候，會有一個 Issue。有一個問題是，因為 Voice 的是很 Real Type、直接的，比如說，我現在講一句話：「我肚子餓了」，他就打說「我肚子餓了」然後打包，打了以後，然後傳到那邊去，收到的時候，他一樣要解包，而且他要按照順序的解包，我不曉得你們有沒有經過…

乙：　沒有啦！　就像比如說不是會有壓縮檔 rar，那檔案太大，會分成 4、5、6、7、8、9、10，那我中間有一個段點不見了，我們是解不開這個封包的。

甲：可是我告訴你喔！你 DATA 沒有關係喔。你 DATA　Delay 就 Delay，也就是說，以前早期頻寬沒有這麼大的時候，你今天傳到一個網站上去，你可以看到他的 Home place，他可能上面出來了，下面也出來了，但中間才出來，Data 無所謂，反正你是看的。可是，當你變成 VOICE 的信號就不行了，一定是要按照這個順序的，『我肚子餓了』，打包完之後，傳到那邊你不能說『餓了我肚子』，所



DOI:10.6814/NCCU201900793

以你還是要按照這個順序到那邊，一直等那個語音在網路上跑，等到他時間超過了，中間漏掉一個封包，”我餓了”但”肚子”不見了。語音在網路上跑，除非你是跑在 VPN 上面，不然一定是會漏掉。所以其實大家我們都知道用 LINE 阿，用什麼東西都可以講，國際電話越來越少這樣，可是一個問題是說，請問一下問什麼語音在網路上跑不用錢、那麼便宜？卻到現在沒有辦法完完全取代電話，那就會有一些這些問題，安全性問題。論封包呀，因為你在網路上找，網路有一個很大的特點是，網路是 Guarantee，我不做任何保證，【A 公司】租給你的 30MB／100MB，那是從你們家 Guarantee 到我們【A 公司】，你進了 ISP 再到美國去，我沒有任何保證。這個很容易了解，假設你今天上了一個網站，他的網站設在那邊，他主要出的頻寬沒不大，沒有像 30MB 這麼大，因為費用問題，他就會有一個比擬在那邊，所以網路就是說他沒有做任何的 Guarantee。

（三） 第三段

乙：我們在往下，那我們剛提到的是，以國際這個系統來講，所以 Amazon 這個語音設備，就像 APPLE SIRI 一樣，我這樣講，他是在他的設備本體，卻把他的關鍵字講出來，然後幫妳把它作分析。可是以台灣語音市場來講，他是逐字、逐次收費，所以台灣市場為什麼聲控其實還有很大的進步空間，最大原因就在這，還有台灣的語音 Data 庫的量跟國外還差太遠了，所以他還要逐字逐次跟你收費，你講得越多字越多次，就要跟你收越多費用，但對我們來說建置商來講，我們沒有那個本錢。除非我跟客戶的合約有明定要用聲控要跟你收月租費，那才有可能是這個情況，所以這個就是取決於市場，還是市場導向問題。

乙：那第四點，資料傳輸到企業內部後要如何進行建檔跟管理？以目前來講，這個都是屬於個人系統，以社區來講，這都是個人財產，所以這個 data 不會進公司，不會進我們公司。但是我們跟【Ｂ公司】合作的時候，我們都會再跟客戶另外一邊做所謂的客戶滿意度調查，也就是說客戶對於目前我們建置的系統滿不滿意？有沒有缺點？甚至對什麼功能很滿意，好比剛提到的，他們很滿意，我們就可以在 Panel 上面把瓦斯抄錶的功能做進去，以後他不需要在電機抄錶，他不需要跟管理員說我家的瓦斯用了多少度，甚至於那個台電公司還要來家裡抄錶，這多會是很困擾的事情，所以會有一些客戶滿意度的功能調查，那這個調查是客戶自己提供，就沒有牽涉到客戶所謂的，我們蒐集客戶的資料問題，那．．

（四） 第四段

丙：那其時這我想要表達的資料是，某方面來說，我的方面很廣，可能不止是他的使用習慣，某方面來說，像溫度會不會紀錄？因為在有時候在控制這些產品，可能會想要怎麼改善產品或系統，所以可能會透過記錄瓦斯筏控制的次數去做相應調整的模式？就比如說數值，對數值的記錄，他可能不一定是多久開一次電視等等這種資訊，而是比如說，像溫度我大概知道這些地方的溫度設置是怎麼樣的環境，然後在做相關的改善，所以這個資料不一定是具體、是這個個人。



DOI:10.6814/NCCU201900793

乙：這個會牽涉到所謂的，你這個問題不通則，你這個是比較狹義的定義，不是廣義的定義，就先講你剛提到的，溫度濕度的控制去蒐集他的資訊，這我會定義他為狹義是因為每一個家庭的燈光數、瓦數都不同，所以會產生的顯熱量跟潛熱量不同，那這樣的情況下，你很難去定義出來一個廣義值，比如說這個社區都不能用，那狹義的就是客變的行為，是客戶變更的行為。那這樣的情況下，你客變的時候，我就必續要客戶同意我去蒐集這些資料分析，然後我們在來幫他糾正所謂的使用習慣或智慧家庭的行為模式再去做修正，但以現在的市場來說，客戶還沒有這樣的習慣，因為他們會認為因為熱了就開冷氣，或是悶了就引進新鮮空氣進來，導入這東西。那廣義的定義來講，那因為台灣在某些區域，好比新北市中和區，今天的室外溫度濕度、連同空氣的懸浮微粒 PPM 多少？就是在網站上都有公告，像空氣不好不要出門，他就有一個基本的 DATA，這就是台灣的天氣，那這個 DATA 是套用他的 DATA 然後再去參照國際標準那個 ISO 室內空氣品質，濃度在 900 PPM 以下是舒適的，多少以上是不舒適的。室內溫度在 26 度舒適，當達到 27 度就不舒適，這個情況下開空調，所以他是廣義的定義，如果你要很狹義的定義，其實也沒有必要，因為當你的人數多，然後家電量又多的話，你的溫度升溫的快，但我還是在 27 度定義就開空調，自然你的溫度還是會降下來，縱使你會有稍微感到不舒服的一段時間，但不會很久，所以他並沒有強迫到馬上要，但客戶可以提出可不可以改設定到 26 度就開了，可以那我們可以自訂，也就是他還是在一個程式上的環境，不會像是 IOS 作業系統，把程式寫死了，除非你越域，否則你就沒有得到開發商的權益，我們把大部分可以讓客戶自己修改的數值、參考條件甚至於今天的 CO2 濃度在 900 他可以自己下修到 800，以這樣的方式他可以去調整到需要的舒適懷境，因為這樣你才有彈性，你沒有辦法說老人家的使用習慣跟年輕人一樣，或許不一樣，老人家可能會覺得比較省電，所以我可以忍耐，年輕人可能覺得我要舒服、不要忍耐，所以使用環境條件不一樣。

（五） 第五段

乙：然後第六點是，建模採用的模型是專家學習或深度學習，這其實你要講的是 AIoT，那 AIoT 是這一年左右，才新創出來的名詞，他其實本質是 AI 加 IoT，那大家都通稱它叫 AIoT，那就我其實看來本質上還差得遠，那 AI 是 AI，IoT 是 IoT，以台灣的市場 5G 都還沒有導入，那 IoT 能推行的就更有限，那 AI 早在兩年前，郭董就講過我要做機器人，到目前為止，其實還沒有看到太多的產品出現，所以你說建這個模型的部份去學習它，這可能會是未來的願景，但現階段沒有辦法回答你這個問題，因為這個專家系統要如何定義它是專家，而機器人能夠取代，這個機器人不是單純只建一個機械人，你可以把它當成一個電腦，藉由我講，讓他自己學習分析，自己進行下一步。可是以目前智慧家庭系統，在怎麼樣你都還是要跟她講說，請幫我開冷氣，請幫我開電風扇，他並不會很直覺的跟你說我可以幫你把你的需求直接告訴你，沒有到那麼神，所以這個專家系統，或是機器人學習及深度學習的建模等，現階段不太可能。



DOI:10.6814/NCCU201900793

（六） 第六段

丙： 那其實我會寫這個的話是因為我看了這個，去年我看了這張圖，我那時候就想說，這是個建模，了解這個就是什麼？

乙： 這個沒有，以現階段來說沒有，它的 API 入口界接語音辨識於語音合成影像辨識這個有，可是上面這個深度學習環境這個部分，其實是不純熟的，還有以目前的系統來講，我們還有很長一段路要去修正。目前台灣任何一家，現在都還沒有穩定性，那大家目前還是在聚焦在下面、下層，也就是他這個語音辨識、影像辨識，但合成還只是個概念，所以語音辨識可以辨識的清楚你講的話，其實每個人的口音都不太一樣，它能辨識就是一個很大的困難，就好比拿 LINE 手機，我傳我今天要吃什麼我傳出去，可是當我傳我要吃什麼，它的辨識率還是會有誤差，光這一點就是一個很大的問題點，那影像辨識是比較沒有問題的地方是因為現在的攝影機鏡頭進步的非常快，所以相對來說，它 200 萬畫數 300 萬畫數，他的鏡頭不貴，所以他能夠辨識的東西，照的夠清楚就知道就是飛碟，這是一個鐵盒，所以他可以很清楚地去辨識出來，可是在語音的部分，它還有很長的路要去修正，所以對於你的 API 入口界接，OK 它有做，但在上層的深度學習環境，有做但還有很長一段路要去執行它，這個 PAS 跟 CAS 當初我們有在走，因為它需要的 DATA 量跟它後端分析精進的部分，還有很長一段路要走，尤其它下面還要靠 ICE 的 GPU，這個其實是有雲端的概念，那他會把這些 DATA 全部丟到超級電腦上做分析應用，但是這個部分，台灣的超級電腦在那裡？我講白一點就是這樣子，如果你找得到，那我相信你可以拿來賣。

甲： 好認真吻，你還看【A 公司】的內部簡報。

乙： 這應該是內部資料，你怎麼可能拿得到？

丙： 沒有，這是 YOUTUBE 上面的，它是一個會議，某個研討會、某個人名字就寫在上面，是一個公開的資料，那時候我是看到，有一個資料儲存的服務，就想說應該有資料傳輸這個中心，就好奇這個資料大概是什麼類別？

乙： 這其實說穿了就是資料大數據庫，但是台灣現在正在做。

（七） 第七段

丙： 所以就包含影像、語音也都有嘗試在做這樣？

乙： 對阿！這個其實是，你要把語音這塊坐起來，你對於機器人的 AI 才起得來，而國外的模型，因為畢竟國外都講英文，所以他們的模型都很大，可是我們中文，我們跟中國大陸口音就不一樣了，再加個客家語，那你說這些語言怎麼共通，所以他一個 DATA 量要多，可是能用得不多，所以就很難去把這個 DATA 建個完整，不要說建不起來，要建的完整很難。

丙：所以那時侯看到個很有趣，很好奇學習是怎麼做，因為一般我在了解機器學習，大概會分很多種，一種我是直接告訴你這個東西是什麼，就像人類一對一的訓練它，或是第二種，讓它去跑，跑完後，你再將特徵值貼上去，然後最後一種，



DOI:10.6814/NCCU201900793

其實最後一種，就是比較偏入深度學習，然後最前面那種就跟比較偏向專家系統，我告訴你這是什麼，但是它的發展空間就會比較有限。

乙： 所以他要建的 DATA 量很大，也就是我要告訴你同一個關鍵字，這個可以代表他，這個也可以代表他，比如說，我跟你說就個是杯子，我可說它是水杯，可以說它是鋼杯，你要知道它可以代表什麼東西。所以它的 DATA 量要非常的大，也很笨。

（八） 第八段

丙 ： 所以我好奇說，目前台灣要做的時候，它大概會採用哪種模式？

乙： 我們只能說以時代的演進來講，它會從最笨的開始，所以不可能做跳躍式的。除非你像中國大陸，它是落後封閉的鎖國 10 年，然後再出來吃人家的系統，吃人家的資料庫，它是直接用躍進的，可是它沒有底。這牽扯到它沒有底，它沒有所謂的基礎，那我們國家的特徵來講，我們是打底為先，所以會很笨，會用最笨的方式在起步，可是要起步多久？不知道，因為這也牽涉到 5G 的導入，還有所謂的 IPP4 跟 IPP6，IPP6 已經出來多久了？十年了，它的普及率，好像現在才要慢慢的要準備推出來，所以這還有很長的一段路。但這不是踢皮球，只是說就是看得到我們目前的網路演進或是說網路結合的系統演進，它有在進步，但客戶的接受度、客群的接受度，或許會有一些觀念上的落差，它不願意接受，不願意改變，就好比之前推 ETC，有一些反對的聲浪，可是放放眼望去看中國大陸或是美國市場，他們是願意去接受它，所以牠們飛行的速度很快，那當然可能在他們國家有反對的聲浪，但是比如說，我們先前出國去玩的時候，你會發現我們台灣才剛發展，可是人家已經很完整了，那就是客戶接受度的問題。

（九） 第九段

丙：然後我為什麼會在蒐集第一段的時候會列這樣的主題，是因為，就是我剛看了那個圖之後，介紹它採用了這樣的模式，但這感覺是你們的，但現在是做得到聲控的嗎？

乙：有。所以這就跟你講這個是 By 次數算的，所以我們後來覺得有點負荷不了。

丙： 因為它 DATA 量其實要很大。

乙： 台灣的 DATA 不大，但客戶用了之後，後續要我們，我們付錢給客戶用，所以變成我們會有點吃不消，它上面就講，這個是，這個人我知道是誰做的？ 反正這個人我認識，那這個聲控系統，確實做起來了，所以在【Ｂ公司】中和的案件，大概這兩年的建案，如果你們有會去參訪或是去選購或購買的時候，以目前這些系統，就會看到這些聲控。

丙： 所以他這個聲控，就比如可以直接說幫我打開冷氣。

乙： 對。

丙： 那如果，我在想說，如果你是用專家系統的話，就是你的字數，對的不夠精準，就會跑步出結論。



DOI:10.6814/NCCU201900793

乙：　所以你要多講幾次。

丙：　所以你要換不同方式去訓練它？

乙：　現在有比較好，其實這不是我們要去訓練它，這個是這個語音辨識 DATA，我講完了，它馬上封包立即傳到台灣的聲量資料庫比對完，再把它拋回來。然後再去做這個動作”開啟”，那當然這個傳輸你會覺得會不會很久。不會，因為聲音封包的 DATA 非常小，那傳出去到對方彈回來，你可能還沒有感受到，可能就已經結束了，因為你會講關鍵字，不會講一長串，因為將一長串它聽不懂，只能像講開冷氣、看新聞，今天幫我開燈

丙：　但如果講比較複雜的話，可以幫我把燈打開嗎？　就是…

乙：　可以

丙：　它會不會…就是排列組合？

乙：　你講的這個就是當初我們講的設定上都已經調進去了，除非你前面講了一段不相關的，然後再講這個關鍵字，那它可能就辨識不出來，但你剛講的那句，它一樣可以辨識出來。

甲：　我們去吃飯，可以幫我把冷氣打開嗎？

乙：　那它可能會掛掉，會停住。

丙：　那它大概就一句話，然後含關鍵字

乙：　對，所以你可以去網路 YOUTUBE 或 GOOGLE，中國大陸有個叫”問問”的，問問裡面那個影片也是這樣寫的，「問問幫我開門，問問幫我開燈」，所以中國大陸那個影片問問，Amazon 的叫 Alexa；中國大陸的叫問問，那我們台灣叫…

丙：是【M 設備】嗎？

乙：不是【M 設備】，這個聲控要是搭配我們的系統，掛在我們系統之後，在跟【M 設備】結合，然後這個技術結合，我們早在先前就整合完成，所以連同前面你提到的其實你一開始，我以為你講的喇叭是指的是家庭劇院，比如說我今天把管家系統跟家庭劇院整合進來，那今天我藉由這個 APP，我可以開電視，把音響打開，串燈控的劇院模式一起把它做出來，你講的是這一塊，因為這在早期大概 3 年前的建案就有了。後來下個世代，就是聲控系統，只是台灣聲控 DATA 量還有待加強，且收費也還在溝通。

（十）　第十段

丙：　因為像我那時候，會想了解這個原因是，像 LINE，如果你語音問它，因為有官方帳號，它如果答不出來，基本上它會把你的問題再拿去做訓練，這樣在我下一次的時候回答就會更精準，更可以抓住訊息，所以會做到這樣子嗎？

乙：　這個就是我講的，我們是系統商，我不是聲控建置商，所以聲控 DATA 再聲控的 SERVER 中，我只是把這段話傳給它分析，它把 DATA 傳給我，它把它拆好割好，跟我講斷點在哪裡？

甲：　其實應該要這樣子講說，基本上這些東西都有個演算法，因為有個演算法，這個演算法要怎麼寫？



DOI:10.6814/NCCU201900793

乙： 這個演算法是取決於聲控廠商或是在我家？

甲： 那個演算法就是說，它怎麼辨識，它去寫這個演算法，就像 GOOGLE 等，在 GOOGLE 還沒有出來的早期，在 Search，Search 跑個老半天，但到 GOOGLE 出來以後，它就可以很快 Search 出來了，那就是它的演算法寫的比較好。對不對？所以從這個 GOOGLE 以後，演算法大躍進這樣子，那這個東西以後會不會變成一個，它 DATA 也會碰到這個樣子。它可能像你剛講的，我一個意思會面講了幾百句， “請幫我把電燈打開”講了幾百句，可是它演算法可以很快的把它辨識出來，我覺得應該是這個樣子。

丙： 所以聲控的部份是跟做聲控的廠商合作，你們只做單系統的這段。

乙： 對！ 因為聲控的話，【A 公司】沒有辦法投入，因為 DATA 量太大。

丙： 因為我一開始看到【M 設備】聲控，我以為是像 “【M 設備】幫我把電視打開”，然後【M 設備】就會幫我把電視打開。

乙： 它是架構在這個系統之下，它是用【A 公司】的線路，然後這個【M 設備】整進來。

甲： 照理講，我覺得這樣解釋就是說，【M 設備】它有網路。

乙： 所以你看它這個系統，是它要跟 AI 雲端語音做分析，那這段我們先撇開不談，這個假設它是成立的，也就是這個聲控廠商它是統整的情況下，這些系統是要跟這個聲控系統做整合，所以我是在這個 E-HOME 的平台上去按了【M 設備】，它去做連動打開或者藉由這個喇叭，我們跟他講了，這個聲音傳給我的 PANEL，告訴它就好比我手指頭按了哪個動作，之後它們去對他下指令，它基本的做法是這樣。

丙： 所以這是個手機 APP？

乙： 這是手機 APP，然後這個是 PANEL。

（十一） 第十一段

乙： 好，那下一個是？

丙： 那下一個是，就是在問具體案例，其實這個具體案例，就是剛，我想問在搜尋方面有沒有具體案例，就是那個分析，主要是因為這個，我看到有個 AI 的人臉辨識門禁，想說智慧家庭應該也會有門禁管制，所以它是運用這種方式去辨別，去拍攝家庭成員的臉，然後也後就可以快速的進入嗎？

甲： 這應該很多了！！這個我們之前在幫一家公司做，它們就是用人臉打卡

乙： 這個技術門檻不高，它的演進時代，大概從虹膜到指紋辨識，到現在的人臉辨識，那人臉辨識現在會出來，我會說它門檻技術不高是說我前面講，因為攝影機鏡頭它的演進，百萬畫數以上的鏡頭很普及且不貴，所以在這個設備上，我可以捕捉影像之後，我先把你的 DATA 建起來，去比對你的臉，這是不難的，所以你看我們現在的 APPLE 手機，你可用人臉 FACE ID 就可以開鎖，這是一樣的道理，所以並沒有什麼太大的門檻。

丙： 我想問的第一個，是這個資料是怎麼來的？



DOI:10.6814/NCCU201900793

乙：　這個訓練資料怎麼來的是，你要先把所有的人臉拍起來，然後藉由臉部辨識軟體，就好比我們把它當作車牌辨識，車牌它就是長的四四方方，可是你面有英文字母跟數字，所以它可以藉由英文字母跟數字去比對，就可去幫你捕捉出來這個車牌的號碼，一樣的道理，臉部特徵只要抓到你的眼睛，就可以抓到兇手是誰？所以犯案的人，基本上要把你的眼睛閉來，被拍到眼睛，大概就跑不掉了。

丙：　所以我在想【A 公司】在做這樣子的訓練跟應用的時候，它這個東西，比如聲控會有聲控服務商直接去做，但在做這個辨識的時候，是【A 公司】自己做還是它找了個專做辨識的設備商在做這件事情？

乙：　因為這個是研究院的產品，我沒有接觸到，所以這個我沒有辦法回答你。

丙：　所以在智慧家庭上，實際有用到這個的技術了嗎？

乙：　近期會推出，因為剛好我們客戶這邊也有提出來做人臉辨識的事情。

丙：　所以那最後如果，那就等於說，我會在我家門口方一個 CAMERA 嗎？去拍進來的人是誰這樣？

乙：　我應該這樣講，這就是取決到費用問題，也就是你客戶那個的買屋的基金，假設如果它今天是一個豪宅，那它可能或許在進大門社區，會藉由臉部辨識抓到你這個影像，它會跟你講，某某某歡迎光臨。然後你到梯廳，照到你的影像，自然而然可以幫你門打開，那你進這個門，知道你住幾層樓，直接幫你按電梯，這個是人臉辨識。那你要投入的費用就會很高，客戶能接受到多少？

甲：　你剛講的那個，我好像有看過，實際上有飯店，就那個無人飯店！

乙丙：　不用無人飯店啊！那個無人超商，在市府站那邊就有一個無人超商，它也是利用這個，它就是人進去前，在那個扎道通關機就幫你拍照了，然後就幫你的臉部特徵抓出來，它其實說穿了，就是把你這張照片照的很清楚，之後它就把妳的特徵通通都給…

甲：　我之前在看中國大陸的節目，介紹中國大陸的車站，它西來人往的人很多，那他的攝影機也夠多，那我覺得它應該是大數據，它那個不是說某一個特徵值，它那個應該是攝影機多，它那個不叫人臉辨識，那個叫做行為辨識。所以它可以看你的行為，像看各個角度照到的，把這些東西蒐集起來，都到它的資料庫裡去，然後判斷這個人是誰？　因為你在走，所以你所有的影像都被攝影機記錄下來，蒐集下來，其實它就有 Data　Base，然後它就可以去判斷是誰？他們報導說，準確率高達 90％幾，他們甚至都是用這個東西在抓一些通緝犯。

丙：　有！張學友演唱會就抓了許多通緝犯，他們其實做測試，結果其實有效，因為它們有通緝犯的照片，所以它們去抓它得特徵值，然後在會場，它就直接在演唱會上照所有人的臉，然後照完它就去比對，就抓到五六個通緝犯

甲：　因為我跟你講，這個技術，像那個攝影機的解析度，我們曾經看過，現在能已經沒有什麼了不起了，有一個長官在做介紹，那時在做大巨蛋，你要來做那個攝影機，它就是在一個很大的棒球場，遠遠的照著，那突然就往場中間丟個煙霧蛋，這時候這麼多人就很緊張，很容易發生事故，所以它把 ROOM 一直放大，因為我這樣子一過去，你可以從這個區域丟出來，你可以看到，可是到底是誰丟



DOI:10.6814/NCCU201900793

的？　它那個 ROOM 就是一直放一直放，放到最後那個人臉就出來了。
乙：　那個是千萬級攝影機！
甲：　那個我們請廠商報過價，非常驚人。
丙乙：　那只能用在特殊場合。
乙：　所以建模，就是剛提到的，沒有什麼建模需求，以目前現在的系統來講。
丙：　所以剛那個人臉辨識是設備商？
乙：　對啊！那就是個套裝軟體，它就已經可以幫你把臉部特徵分析出來，然後你只要把照片輸入進去就結束了，像設備廠商實佑、國貿或是 Bosch，他們這些設備商，他們其實都已經有這些技術，只是在於說你要花多少錢買這個設備，但對【A 公司】來講，它不需要去開發這個，因為我去開發了軟體出來，我必須要生產自己的設備，而以目前看到【A 公司】的 E-home 應用系統是，我們開發出軟體，找可以配合的硬體商去做 OEM 的部分，那【A 公司】今天如果還要去管像門禁這個小東西，我還要再去找 OEM 廠商，那要付出的費用代價可能會更高，所以以商業的立場來講，要去衡量投入的定位、投報率有沒有達到需求水準。

（十二）　第十二段
乙：　那你第三點就到分析阿！
丙：　那其實就像剛你們說的，我找到一個盲點就是，我一直以為是，有點像【A 公司】，我的邏輯是，資料到【A 公司】再到設備商，但有可能會不會是設備商直接可以透過這個平台得到這個資訊呢？　就是【A 公司】變成是個橋樑的感覺。
乙：　華為可以
甲：　我覺得，因為【A 公司】基本上就是一個業者。所以我們會做的時候，我們是作一些共同的，那其他的設備商，除非你是國際級的像 Amazon。那像本土的廠商，它可能比較侷限在那塊，我今天公司五六個，有專門開發人臉辨識、車牌辨識，所有的軟體硬體，我就去找廠商合作，然後一般會做的模式，就是說我去找一家比較大的公司，我賣給它，那【A 公司】是一個標的，人家會跟你說，我來找你合作，那因為我們公司夠大，所以我們就去跟民間業者說我們去幫你規劃幾個東西，第一個最簡單的 Structure，把光纖牽到你家，因為光纖到你家，所以網路有了，我資料就可以開始傳，那這個廠商它提供的這些東西可以幫你說人臉辨識搭配門禁，那廠商其實去蒐集這些資料，到底有沒有用？　我個人覺得說，一般是不太會拉，設備商它最主要的目的是說，我今天設備要賣的出去，我錢賺到了。
乙：　其實它還有一個重點，我們先講回來到 E-HOME 智慧系統這些家庭裡的設備，目前全部的設備都是採用類比訊號，那其實不是 IP，那它的 IP 是藉由我們這個 PANEL 後端的核心設備去做類比跟數位的轉換，類比跟 IP 的轉換，它今天現場這輩才會看起來像是活的，可以應用它，那是因為我們這個心臟去驅動它，所以這些設備商的設備都是類比訊號，不是 0 就是 1，它沒有蒐集，它沒辦法蒐集，它沒有 DATA 的傳輸，所以它就沒有辦法像剛提到的，【A 公司】做一個媒


DOI:10.6814/NCCU201900793

介，現場端的設備透過【A 公司】這個平台訊號傳給設備原廠，它是達不成共識，因為他們設備本身只有類比，它類比訊號不是 0 就是 1，它沒有辦法再把這個訊息透過包裝僞裝，然後藉由【A 公司】的平台偷偷的跑回家，這是傳統的系統。

乙：那如果是聲控喇叭就不一樣，畢竟那顆喇叭是跟別人合作，如果是【A 公司】自己開發的，那可能要去研究一下【A 公司】的喇叭，但是你是跟 Amazon 合作的，或跟 GOOGLE 合作的那顆喇叭，它會把這個 DATA，因為這個喇叭必須建置在有網路的狀態下，沒有網路它是沒有辦法動作的，它是 IP 的，它有了這顆喇叭之後，它有了網路，它可能就不需要【A 公司】的平台傳回去，它是有兩個 Rules，一個是傳動【A 公司】的平台來去驅動 PANEL 把東西打開，然後另外一個 Rule 是直接回它家，那是不一樣的情況，所以這個聲控喇叭是唯一可能會被擷取資料的地方，那其他的現場終端，像緊急按鈕或是開關燈的模組，那其實都是類比訊號。

丙： 所以今天如果一個家電它也是有連 WIFI，它就有可能傳到設備商手中？因為它就不一定是類比。

乙： 對呀！就像那個電冰箱，我們家一般電冰箱它能連回去【P 公司】嗎？ 不能，可是我們現在賦予它 IoT，也就是它要在外掛一顆可以連網的設備的那顆就做 DONGO，這個網路設備它就是可以，你要插網路線或 WIFI，它就可以把這個資訊，偵測裡面這個的，比如說我定義這個是蔬菜，那它重量不見了，我們會通知屋主說你家青菜沒了，可以跟賣場連線，幫我買青菜進來，這是未來趨勢，那這樣的情況下，它可以把這個資訊傳回去給【P 公司】去蒐集，可是蒐集的意義在哪裡？它要有個實際的效能，除非【P 公司】說我今天要來開生鮮，那它可以去做，或者去跟生鮮廠商做結合，那我直接把訊號拋給你，你直接幫我出貨，那這也是未來的商業模式。

甲： 我覺得這種機會不大，因為要某個廠商敢這樣子做，被知道的時候…

乙： 這就牽涉到隱私問題，那講最快的，國際的官司最有名就是 FACEBOOK，它把這個個資，只要當初所有有來申請過的廠商，我都可以吐給你，它就犯了個最大的錯誤，所以它到現在被罰了很慘。

丙： 對被罰得很慘。

乙： 這就是它的問題，就是它當初沒有考慮好所謂隱私權所謂的重要性，所以今天其實我一開始看到的隱私權問題，我就已經覺得有…

丙： LG 有，LG 它的作法是，但它的設備商敢這麼做一定會想好招，比如說它就是跟它的手機這樣，所以 LG 你是可以在 LINE 上面（在韓國）

甲： 你是指 LG 的手機？

丙： 是它的冰箱。

乙： 它的冰箱搭配它的手機可以，然後可以把封包偽裝的很好。可是現在的人太厲害了！那韓國在怎麼樣是帝國主義，那這套在他們的國家行的通，因為畢竟 LG 是政府支持的，那可是你賣到世界上去之後，你就會被受檢討，那國際觀就會出現，那就不見得會去蒐集國外的資訊，國內人的資訊它會把這個閘道開啟，



DOI:10.6814/NCCU201900793

國外的閘道它關閉就好了，而且你不要小看這一支手機在台灣，它是經過 NCC 各方面審核監測之後，才讓它進來的，所以其實很多功能，就好比 APPLE WATCH，APPLE　WATCH 在美國它可以做心律調整的監測器，可是在台灣不行，這很清楚，所以你說的 LG 冰箱、LG 手機在台灣未必可行，因為它會有所謂的個資問題，那就如同剛剛所講的 APPLE　WATCH 一樣。

丙：　這其實是一個很好的議題，　因為在台灣的做法是，在國外他們設個叫做個資保護的機構就是局，那在台灣做法，假如今天我，　因為一定是ＢＳＭＩ做檢測，ＢＳＭＩ東西收到要做檢測，它就跟你說只要是通訊類的東西都找 NCC，那只要它有可能是醫療器材你就要通過衛生署的核准，那這樣的模式，台灣的管理做法是這樣，好處當然是很專業。

乙：　可是它沒有辦法整合！

丙：　對！　很難整合

乙：　所以這是台灣，也就是進步的問題。

丙：　很多領域（智慧家庭…）

乙：　那也就是所謂的自由度，如果你自由度不夠高，那你相對能夠跳躍的方式不會很大，這也就是為什麼我們那個手機支付推不起來的原因，因為某個單位太多了，所以你會導致它．．可是你仔細思考這個問題也對啦！　為什麼？　因為台灣的市場畢竟小，中國美國市場大，如果你讓這個所謂的支付系統可以上線的時候，萬一它裡面有駭客把這個金流偷走了，以台灣的市場金流太小了，你可能會讓這個廠商瞬間垮掉，可是你如果像阿里巴巴或者像微信它們這種十幾億人口，這麼多人在用，所以你偷它 1%，才站它營業額多少？　它才不在乎，但以台灣這個市場量來講，1%來說可能不行，因為它可能最多就賺 3%。

（十三）　第十三段

丙：　所以其實我想問的是發展頻頸跟困境在哪裡？　其實很重要的一個點是……

乙：　那這個未來發展的頻頸跟困境，第一個就是台灣的經濟要好，台灣經濟不好，你任何的高度智慧化產品推不出來，因為它的費用太高了，沒有人會去接受它，台灣的市場很小，這個是重點，你要賣到國外去，你要競爭的贏人家，台灣在國際上較的出名字的只有台積電，那當然聯發科或者是宏碁可以，可是以台積電的名聲比起來，那才叫做佔有一席之地。而且人家都說未來的市場只有三家，GOOGLE、亞馬遜、阿里巴巴，所以原則上來講，台灣經濟要先起來，那才有能力去消費，那消費了之後，目前遇到的困難跟頻頸就是整合度的問題，也就是剛剛提到的，在未來的 AIoT 領域，它因為有了經濟的支撐，大家願意去消費它之後，這個頻頸也就是語音，它才能夠有重大的突破，因為這個語音目前沒有辦法突破，台灣的辨識率太差了，我只跟他講，『嘿！　SIRI 你幫我打電話給某某某』，現在講可以通，等下講不見得可以通，穩定地的，最大的是聲音辨識的問題。

甲：　你看看你電腦裡面 26 個英文字母，中文就要兩個半…．



DOI:10.6814/NCCU201900793

乙： 然後另外一個，台灣其實並不是跑在前端，所以另一個頻頸是鏡頭的部分，是因為目前看到你說的人臉辨識沒有瓶頸，是因為人家國外，因為這些鏡頭都是國外生產的，比如說日本的 SONY 或 Nicon，這些鏡頭都是國外生產，人家都已經跑在前面，而它只是把它的，講難聽一點是把庫存貨倒給我們，那或許，它就賣比較便宜就比較能接受，那這個頻頸就是，目前會侷限於在聲控，聲控做起來了之後，下一個就是倒 AI 連動，那這個 AI 連動的資料庫，它就可以無限的放大，可是這個 DATA 有了之後，平台誰寫？ 要怎麼寫？ 這是下一步，但是你要先有這個大 DATA，如果這個大數據已經先有了，我藉由目前現有的大數據，雖然不多，平台一樣可以去發展去跟它結合，可是現在能做出來的東西，DATA 是有限的。

（十四） 第十四段

丙： 所以目前最多就只能做到串聯？

乙： 對！ 可是你放眼望去看，APPLE 的產品，APPLE 在它們網站上也有他們的影片，Homekit 它這個我記得我很早以前有看過，但現在它有沒有再進步？我不清楚，但它說穿了也是串聯，那它把家裡的窗戶磁簧或者是那些壓扣，它是用 BLUETOOTH 在做連線，那對於安防這一塊，就我們是建置商系統整合商來講，我會打一個問號？因為你走 BLUETOOTH，畢竟還是要吃電流，它會有用電問題，所以他今天真的發生一個問題，而且是人摔倒要按壓扣卻沒電，就慘了！！！

丙： 所以是電的問題。

乙： 對！

丙： 那 Zibee 呢？

乙： 一樣，它也是吃電，它的設備本體背後要背一顆水銀電池，它才能縮小它的眼睛，你去背一顆三號、四號電池，那個設備就大了，它一定是用水銀電池，那當然以現在來講這些鋰電池，他們有沒有辦法突破它？我是不知道，那或許他們現在發展的無線充電，那在未來或許可以應用到這些東西上，它可以藉由無線的方式去幫它充電，那個可能又是 10 年後的事了！

（十五） 第十五段

丙： 那我滿想要問的是，跟【Ｂ公司】還有【P 公司】合作，比如說我可以在【Ｂ公司】的房子裡面，然後跟它講叫車的服務？

乙： 這已經有了，就是台哥大整合，台哥大掛平台整合，App 建在我們應用平台裡，他們叫車的 Code 碼給我們，我們把它這個東西建進去，

丙： 所以是兩個平台串在一起？

乙： 對！這就是跨系統整合，連同【Ｂ公司】的某飯店，因為他們有些區塊它們是有所謂的咖啡廳進駐，那它就可以幫樓上的住戶 Call 樓下幫我送咖啡，或者是你先幫我預約保留座位，那這個就是跨台平整合連同我們剛講的能源管理部分，能源管理有數位水表跟電表，最基本的這兩款，那水表電表這個是跟資策會，



DOI:10.6814/NCCU201900793

當初是跟資策會整合的，所以我們也可以把這個數據資料拋給資策會，資策會可以在平台上看到這些 DATA，去看到它的歷史紀錄資料，用電用水資料有沒有異常去做分析，那個是後面下一個階段的事，但是這個都有整合過。

丙： 所以就是把這幾個服務商的平台跟【A 公司】的平台來做一個整合？

乙： 對！ 我們當前端，他們是我們的後台，然後把這個東西跟它串聯。

丙： 那【P 公司】呢？ 它是單純做設備而已嗎？ 還是也可以串聯？

乙： 對！ 這顆 DONGO 是跟【P 公司】的 SERVER 連的，可是它這個 DONGO 這個資訊必須要透過【A 公司】的 E－PANEL 再把指令在丟出去，所以它變成說它沒有獨立作業，那當然也有人會認為說，我不要透過你【A 公司】，也就是改機，它就是用最原始的，本來就是【P 公司】那一套，應該說【A 公司】叫做改機，因為你會被我綁住，你會先進來之後才可以再出去，我不會把多餘的資訊吐出去，因為我必須要對我的客戶負責，那如果你是原先【P 公司】那一套 DONGO 直接就出去了，它就直接出去了，它可能被偷取資料。

丙： 所以它有兩種方法？

乙： 對！ 這是不一樣的

丙： 所以如果是透過【A 公司】，【A 公司】本身出去怎樣的資料…．

乙： 我們就是講清楚，用什麼 Protocol 界接，比如說 DCP IP 或只是我用 ODP 的資料庫跟你做交換，那用這樣的方式定義好，那你就把你的資料去進來，我把這個資料轉出去，那你是告訴我，比如說要開冷氣，我只是接受這個資訊之後，是藉由我在吐另外一個開冷氣的資訊出去給它，它幫我把訊號回傳回來這樣。

丙：好，謝謝！

國立政治大學 National Chengchi University



DOI:10.6814/NCCU201900793