美國能源資料開放運用之資訊安全與隱私權議題研析

蔡博坤
財團法人資訊工業策進會科技法律研究所
bobtsai@iii.org.tw

摘要

在後京都議定書的時代，節能減碳的議題已持續在世界各地發酵，不同科學社群嘗試提出不同的解決方案，而透過資通訊技術(ICT)，連結雲端管理平台和 AMI 等基礎建設以提升能源效率，經相關實證，業成為一個可行之方法。然而，其所產生的巨量資料，所引發的法律議題已逐漸備受關注。本文選定美國作為比較法之研究主體，首先概述美國能源資料開放運用之科技法制政策。其次，將細部探究資訊安全和隱私權兩個重要議題，盼作為我國未來建構能源管理平台和相關資料開放運用之參考。

關鍵詞：能源資通訊(Energy ICT)、雲端運算(Cloud Computing)、巨量資料(Big Data)、隱私權(Privacy)、資訊安全(Information Security)

壹、前言

能源資料(energy data)之開放運用，對許多人來說，甚為陌生。原因在於，目前絕大多數能源用戶所使用之電表，尚屬於傳統物理性之單向式電表(one-way smart meter)，有關電力使用度數等能源資料(energy data)，亦由電力公司派出抄表員定期抄錄之，再按期寄發帳單給用戶。因此，於現階段，在缺乏相關數據資料情形下，電力網絡末端用戶(end user)多仍無從掌握本身能源使用狀況。

近年來，隨著智慧電網(Smart Grid)、智慧電表(Smart Meter)等新興科技之發展，帶來一股能源資通訊之浪潮，結合能源相關之基礎設施(infrastructure)、雲端運算(cloud compting)、物聯網(Internet of Things, IoT)等技術，自可望克服前述用戶無從掌握能源使用之情況。因透過資通訊(ICT)技術，用戶可望在每 15 分鐘或更短的時間內，即時掌握本身能源使用狀況，作出最佳判斷，然而，此也產生若干關於隱私權(Privacy)和資訊安全(Information Security)的疑慮。因此，關於文章之架構，本文將先行檢視美國推動能源資料開放運用(Open Energy Data Movement)之重要科技法制政策，其次，將從比較法的角度，探討相關重要資訊安全和隱私權議題。

貳、美國能源資料開放運用科技政策檢視

一、國家巨量資料研究及發展倡議

白宮科技政策辦公室(Office of Science and Technology Policy, OSTP)於2012年3月發布「國家巨量資料研究及發展倡議」(National Big Data Research and Development Initiative)，擬由聯邦政府出資，整合不同部會，投入巨量資料相關整合性研究。近來，更透過公私協力之合作模式(Public-Private-Partnership, PPP)，聚焦於能源、醫療、資通訊等先進科技領域*。

過去，由政府衛星和地面氣象站所蒐集之氣象資料、以及限軍事用途全球定位系統(GPS)等資訊，基於國家安全(national security)考量，皆單方面由政府所把持和掌握。然而，隨著這些資料的釋出，皆對於產業創新和經濟復甦帶來正面影響。有鑒於此，美國總統歐巴馬於2013年5月份，簽署一道「開放機器可讀取政府資訊」行政命令(Executive Order – Making Open and Machine Readable the New Default for Government Information)，期在過往經驗基礎上，啟動整體經濟之正面循環。

二、綠色按鈕倡議 (Green Button Initiative)

有鑒於能源數據(energy data) 長久以來皆單方面掌握在能源公司手中，用戶幾乎無從近取這些資料，白宮科技政策辦公室(OSTP)首席科技官員 Aneesh Chopra 於2011年提出「綠色按鈕倡議」(Green Button Initiative)，該倡議挑戰美國境內的電力公司(utilities)使消費者能知悉本身能源使用狀況，有效提升節約能源意識†。換言之，從受保護之網站介面，消費者能夠在一個人性化的電子格式上，讀取本身能源使用的資訊。

在私部門產業主導下，商務部國家標準技術局(National Institute of Standard and Technology, NIST)與業者共同參與「開放自動需量反應溝通標準」(Open Automatic Demand Response Communication Standards, Open ADR)和「開放自動資料傳輸」(Open Automatic Data Exchange, Open ADE)互通性標準(interoperability)之研究計畫，用戶透過本身持有的裝置介面，聯結到所謂的能源雲(energy cloud)，在一個可供下載之標準簡易使用電子資訊格式上，讀取本身能源使用資訊(consumer-specific energy usage data, CEUD)，再透過控制科技(control technologies)，能有效管理用電狀況，提升能源效率(Energy Efficiency, EE) 。

從資訊流之面向觀察，這些智慧電網之發電、傳輸和配電過程中，所產生之一切能

*蔡博坤，〈智慧聯網時代巨量資料法制議題研析-以美國隱私權保護為核心〉，《科技法律透析》，第25卷第10期，頁46-62 (2013)。

† Omer Tene and Jules Polonetsky, “Big Data for All: Privacy and User Control in the Age of Analytics,” Nw. J. Tech. & Intell. Prop., vol. 11, pp. 239-272, 2013.

源資料，其皆儲存在能源公司伺服器中，透過「綠色按鈕下載我的資料」(Green Button Download My Data)之服務功能，用戶(或其代理人)能在經加密之網頁入口網站，登入帳號和密碼，隨時掌握本身能源耗用之情形。同時，在用戶授權(authorization)下，已經有愈來愈多的能源服務公司(Energy Service Company, ESCO)、電信業者(Telecom)、軟體開發商(Software Developer)和系統整合業者(System Integrator, SI)等第三方(Third Party)，透過「開放自動資料傳輸」(Open ADE)互通性標準和「綠色按鈕聯結我的資料」(Green Button Connect My Data)功能取得這些資料，除可提供用戶客製化之節能服務外，也可據以開發出能源資通訊領域之應用軟體和管理系統 (參圖 1)。

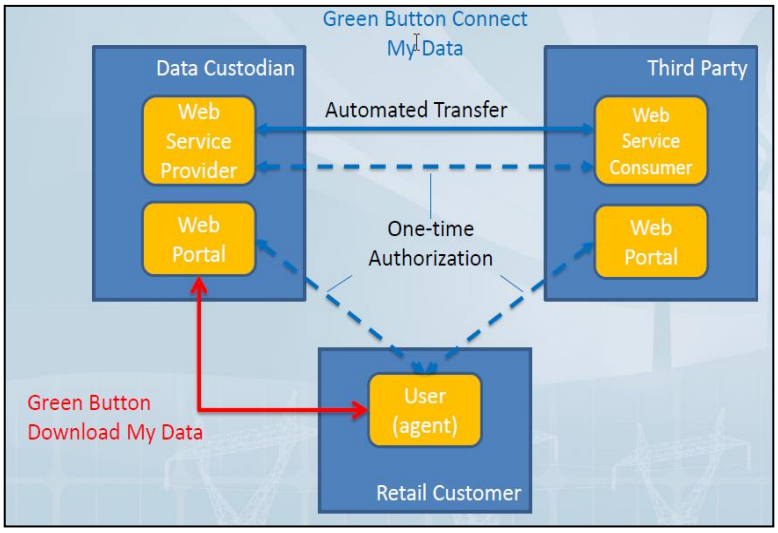

圖 1: 綠色按鈕用戶資料傳輸與授權關係示意圖 (NIST)[‡]

參、關鍵法制議題研析[§]

一、資訊安全議題

由於智慧型電表基礎設施(Advanced Metering Infrastructure, AMI)與一個國家整體之基礎建設息息相關，美國歐巴馬總統於 2013 年 2 月 12 日，簽署一道「改善關鍵基礎設施之網路安全」行政命令(Executive Order 13636 – Improving Critical Infrastructure Cybersecurity)，該行政命令第二款，乃將「關鍵基礎設施」(critical infrastructure)定義為，

[‡] Dr. David Wollman, "NIST Update: Grid Interop and Green Button," Smart Grid Task Force, 2012, http://www.nist.gov/smartgrid/upload/NISTupdate_SGTF_Dec2012_final.pdf (2014/1/8). *See also* David Wollman, "Frameworks and Data Initiatives for Smart Grid and Cyber-Physical Systems," DEBS, 2013, *http://www.nist.gov/smartgrid/upload/DEBS2013-Wollman-July2013.pdf* (2014/1/8).

[§] 蔡博坤，"談美國需量管理法制政策對台灣綠色產業發展之啟示"，*第十七屆全國科技法律研討會*，國立交通大學科技法律研究所，2013，頁 1051-1069。

「對於美國至關重要，而當其無法運作或遭受損害時，將削弱國家安全、經濟穩定、公共健康或安全之有形或虛擬系統或資產」[**]，遂採取相對廣義之解釋(broad interpretation)[††]。同時，第七款亦指示美國商務部「國家標準技術局」 (NIST)，研議一個「提升關鍵基礎設施資通訊安全之架構」 (Framework to Improve Critical Infrastructure Cybersecurity)，該架構將企業商業機密、隱私權(privacy)和公民自由(civil liberties)等受到美國聯邦憲法(the U.S. Constitution)保障之之重要法益，納入考量範疇。

在行政命令簽署後之同月底，NIST 在美國聯邦法規資料庫(Federal Register)發布專業意見徵求之訊息 (Request for Information, RFI)，將在既有的智慧電網、識別管理、聯邦資訊安全管理法(Federal Information Security Management Act, FISMA)、電力網路安全模型標準及指導原則的基礎上，擬定關鍵基礎設施資通訊安全提升的架構(the "preliminary framework")，討論標準、方法、程序，和涉及資通訊風險的政策、商業實踐、科技研發等多面向的議題，並在同年 5 月份初步彙整了資料蒐集的結果。

NIST 於 2013 年 10 月 22 日發布「遵循 13636 號行政命令改善關鍵基礎設施之初期資訊安全架構」(Improving Critical Infrastructure Cybersecurity Executive Order 13636 Preliminary Cybersecurity Framework)，試圖提出一個關於組織資訊安全風險管理之高位階和策略性架構，其核心乃涵蓋五項主要功能(Five Core Functions): 「指認」(IDENTIFY, ID)、「保護」(PROTECT, PR)、「偵測」(DETECT, DE)、「回應」(RESPOND, RS)與「回復」(RECOVER, RC)，簡述初期架構各項功能所涵蓋的種類內容(category content)於下[‡‡]:

1. 指認(ID): 資產管理(Asset Management, AM)、企業環境(Business Environment, BE)、治理(Governance, GV)、風險衡量(Risk Assessment, RA)和風險管理策略(Risk Management Strategy, RM)；
2. 保護(PR): 近取控制(Assess Control, AC)、人員認知與訓練(Awareness and Training, AT)、資料安全(Data Security, DS)、資料保護方法與程序(Information Protection Processes and Procedures, IP)、操作和資訊系統元件之維護與修復(Maintenance, MA)、科技保護措施(Protective Technology, PT)；
3. 偵測(DE): 異常活動訊息通知與反應(Anomalies and Events, AE)、資訊系統之持續監控(Security Continuous Monitoring, CM)、偵測方法與程序之確保與維護

[**] The term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United Sates that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
[††] The White House, "Executive Order – Improving Critical Infrastructure Cybersecurity," 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (2014/1/8).
[‡‡] NIST, "Improving Critical Infrastructure Cybersecurity Executive Order 13636 Preliminary Cybersecurity Framework," 2013, http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf (2014/1/8).

(Detection Processes, DP)；

4. 回應(RS): 回應方法與程序機制之策劃(Response Planning, RP)、內部和外部利害關係人對於事件之回應(Communication, CO)、分析(Analysis, AN)、避免負面效應擴大之行動(Mitigation, MI)、改進方案(Improvements, IM)；
5. 回復(RC): 回復方法與程序機制之策劃(Recovery Planning, RP)、改進方案(Improvements, IM)、關於修復活動之協調與溝通(Communications, CO)。

二、隱私權議題

近年來，在聯邦政策之導引下，用戶透過綠色按鈕(Green Button)，即可掌握能源使用之情況。然而，伴隨此波龐大能源資訊流之釋出，相關隱私權議題已然浮現，例如「消費者能源使用資料」 (Consumer-specific Energy Usage Data, CEUD)當否歸屬於「敏感性個人資料」範疇，而應受到管制保護? 針對此一課題，論者目前仍莫衷一是。究其緣由，應與「消費者能源使用資料」 (CEUD) 長久以來皆由電力公司(utility)單方面持有有關。過往，針對這些能源資料，僅多由州層級之公共事業委員會(Public Utility Commission, PUC)透過行政的手段進行管制。以加州為觀察，加州公共事業委員會(California Public Utility Commission, CPUC)乃強制要求三大電力公司(PG&E、SCE 和 SDG&E)必須提交「年度隱私權報告」給委員會，且必須進行獨立資料隱私權和安全實施之稽核作業(independent audits of data privacy and security practices)§§。以下將試從聯邦法制政策的角度，探討此一課題。

根據白宮 2011 年 6 月所發布的「21 世紀智慧電網政策綱領」，其指出: 目前「消費者能源使用資料」(CEUD)尚未被歸屬到特定聯邦法規底下[***]。然而，探究 CEUD 之本質，其應該被歸屬於「敏感性個人資料」(sensitive information)之範疇，當須被妥善地蒐集、處理、利用之[†††]。因此，在法律沒有明文規定下，該綱領建議，聯邦與州主管機關應嘗試以 OECD 1980 年「公平資訊使用原則」(Fair Information Practice Principles, FIPPs)[‡‡‡]作為出發點，進而思索適用於能源領域之特殊性議題，除能確保消費者能源使用資訊(CEUD)得有效被保護，也將建立起消費者對於智慧電網科技的信任感(trust)，建構一個共通、全面卻相對彈性的管制架構(a general, comprehensive, yet flexible, framework for

§§ The Public Utilities Commission of the State of California, "DECISION ADOPTING RULES TO PROTECT THE PRIVACY AND SECURITY OF THE ELECTRICITY USAGE DATA OF THE CUSTOMERS OF PACIFIC GAS AND ELECTRIC COMPANY, SOUTHERN CAIIFORNIA EDISON COMPANY, AND SAN DIEGO GAS & ELECTRIC COMPANY," 2011, http://www.smartgrid.gov/sites/default/files/doc/files/Decision_Adopting_Rules_Protect_Privacy_d_Security_Electric2.pdf (2014/1/8).

*** The White House, "A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future," 2011, http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf (2014/1/8).

††† Energy usage information can and should be protected like other sensitive information.

‡‡‡ Daniel J. Solove and Paul M. Schwartz, *Information Privacy Law*, Aspen, 2011.

smart grid privacy)。

能源部(Department of Energy, DOE) 於 2012 年 1 月底舉辦一場「智慧電網隱私權座談會」(Smart Grid Privacy Workshop)，指出推動 AMI 三項重要議題，即: 消費者能源使用資訊(CEUD)使用、教育宣導(Education)[§§§]和管轄權(Jurisdiction)[****]，據以達成以下幾點共識(consensus): 第一，將建構起一個第三方就消費者能源使用資訊之近取架構(Establishing a Framework for Third Party Access to Consumer-Specific Energy Use Data)，即當資料釋出給第三方時，必須先取得消費者的同意 (consent)，而消費者應有權利知悉該第三方後續如何使用其個人資料；第二，擬由 NIST 「智慧電網互通性專家諮詢小組」(Smart Grid Interoperability Panel, SGIP) 編制下之「資訊安全工作小組」(Cyber Security Working Group, CSWG)，在互通性標準平台上，起草第三方就 CEUD 近取遵循守則(Guidelines)，納入隱私權考量；第三，聯邦政府將持續在「資訊流之鼓勵」和「資訊隱私權暨安全之確保」間取得一個平衡，同時，因應科技發展，也將更新推動「國家隱私權保護架構」; 第四，將從設計著手保護隱私 (privacy by design, PbD)[††††]。

在落實上述更新推動「國家隱私權保護架構」相關工作，白宮於 2012 年 2 月份提出一個「消費者隱私權法案」(Consumer Privacy Bill of Rights)，研訂七項客觀要素(objectives)，其中關於「精確近取」(Access and Accuracy)，乃賦予消費者享有在一個可讀取之格式上，得以讀取修正相關敏感性個人資料之權利(right)，並且防止資料不精確和任何負面效果風險，也將持續落實「綠色按鈕」是項倡議，使更多人能簡單得知本身能源使用的資訊[‡‡‡‡]。另在保障消費者能源使用資訊(CEUD)方面，聯邦貿易委員會(Federal Trade Commission, FTC)也進一步提出一個「消費者隱私權保護架構」(Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers)，將智慧電網所產生之消費者能源使用資訊(CEUD)試圖納入個人資料定義範疇，同樣在「公平資訊使用原則」(FIPPs)基礎上，據以研訂「從設計著手保護隱私」 (privacy by design, PbD)、「簡化選項」 (simplified choice for business and consumers)和「更佳透明化」(greater

[§§§] Education will be required regarding how the data will be used to help improve gird operations and how end users can use the information to better manage their electricity use. It is also agreed that it's important to gain consumer consent prior to the data being released to a third party. Consumers need to be aware how third parties will use the data in order to feel confident in the security of data transfers and to understand who controls the data at each transfer point.

[****] The issue is whether the jurisdiction belongs to the state or the federal?

[††††] The U.S. Department of Energy, "U.S. Department of Energy Smart Grid Privacy Workshop Summary Report," 2012, http://www.smartgrid.gov/sites/default/files/doc/files/Privacy%20report%202012_03_19%20Final.pdf (2014/1/8).

[‡‡‡‡] The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (2014/1/8).

transparency)三個重要準則[§§§§]。

肆、代結論

在全球暖化氣候變遷的今天，不同科學社群(scientific communities)嘗試提出不同的解決方案(solutions)，而透過資通訊技術(ICT)，連結雲端管理平台和 AMI 等基礎環境建設，進而提升能源效率(EE)即為一例。從正面角度觀察，此將帶動新一波能源資通訊市場之興起，相關參與者除了固有的電信業者(Telecoms)、電力公司(Energy Company/Utility)、資通訊硬體製造廠商(ICT Manufacture)、軟體開發商(Software Developer)外，新型態的能源服務業者(Energy Service Company, ESCO)和系統整合者(System Integrator, SI)將扮演重要的角色(參圖 2)，相關商機自可期待。

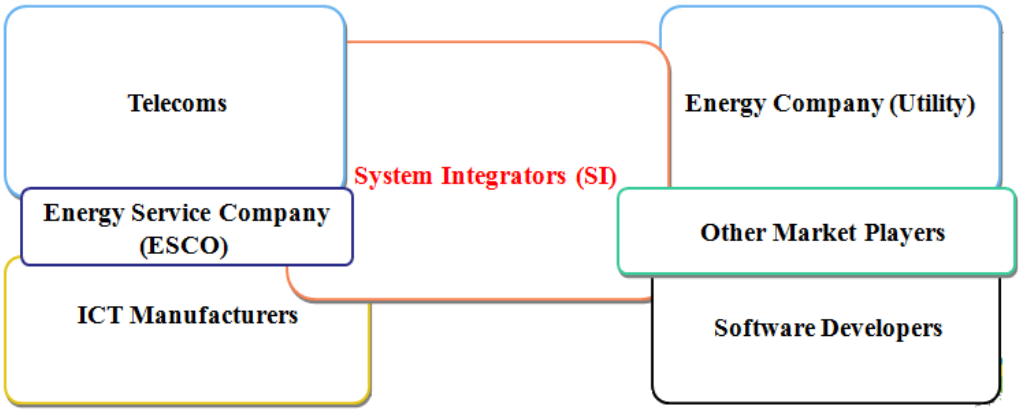

圖 2 能源資通訊市場分佈概況圖 (本研究自行繪製)

然而，伴隨而來的，卻是一連串攸關系統之資訊安全和與人民權益息息相關之隱私權風險，觀察近來相關科技法制政策之發展，美國聯邦政府較偏向將「消費者能源使用資料」(CEUD)歸類於個人資料保護之範疇，因此，能源公司自當應遵循聯邦行政機關所發佈重要政策文件和各州層級公共事業委員會(PUC)規範，妥善蒐集、處理這些能源資料，並就第三方利用這些資料，當落實授權同意機制(參圖 1)，盼此作為我國未來建構能源管理平台和相關資料開放運用之參考。

[誌謝]

本文部份曾發表於由國立交通大學科技法律研究所主辦之第十七屆全國科技法律研討

§§§§ The Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," 2012, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (2014/1/8).

會，作者感謝國立交通大學科技法律研究所給予之寶貴機會。作者亦感謝經濟部技術處「產業創新體系法制建構計畫」(2/3)和經濟部能源局「能源資通訊系統技術應用政策工具規劃」(2/4)經費補助，對本研究助益甚多，也感謝資策會科技法律研究所 孫文玲副所長、吳兆琰主任、李科逸組長等長官同仁，在研究上所給予之指導與支持。本文研究成果係屬作者個人看法，不必然代表委託單位及任職單位之立場。

參考文獻

[1] Omer Tene and Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics," *Nw. J. Tech. & Intell. Prop.*, vol. 11, pp. 239-272, 2013.

[2] Dr. David Wollman, "NIST Update: Grid Interop and Green Button," Smart Grid Task Force, 2012, http://www.nist.gov/smartgrid/upload/NISTupdate_SGTF_Dec2012_final.pdf (2014/1/8).

[3] Dr. David Wollman, "Frameworks and Data Initiatives for Smart Grid and Cyber-Physical Systems," DEBS, 2013, http://www.nist.gov/smartgrid/upload/DEBS2013-Wollman-July2013.pdf (2014/1/8).

[4] The White House, "Executive Order – Improving Critical Infrastructure Cybersecurity," 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (2014/1/8).

[5] NIST, "Improving Critical Infrastructure Cybersecurity Executive Order 13636 Preliminary Cybersecurity Framework," 2013, http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf (2014/1/8).

[6] The Public Utilities Commission of the State of California, "DECISION ADOPTING RULES TO PROTECT THE PRIVACY AND SECURITY OF THE ELECTRICITY USAGE DATA OF THE CUSTOMERS OF PACIFIC GAS AND ELECTRIC COMPANY, SOUTHERN CAIIFORNIA EDISON COMPANY, AND SAN DIEGO GAS & ELECTRIC COMPANY," 2011, http://www.smartgrid.gov/sites/default/files/doc/files/Decision_Adopting_Rules_Protect_Privacy_d_Security_Electric2.pdf (2014/1/8).

[7] The White House, "A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future," 2011, http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf (2014/1/8).

[8] Daniel J. Solove and Paul M. Schwartz, Information Privacy Law, Aspen, 2011.

[9] The U.S. Department of Energy, "U.S. Department of Energy Smart Grid Privacy Workshop Summary Report," 2012, http://www.smartgrid.gov/sites/default/files/doc/files/Privacy%20report%202012_03_19%20Final.pdf (2014/1/8).

[10] The White House, “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,” 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (2014/1/8).

[11] The Federal Trade Commission (FTC), “Protecting Consumer Privacy in an Era of Rapid Change,” 2012, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (2014/1/8).

[12] 蔡博坤，〈智慧聯網時代巨量資料法制議題研析-以美國隱私權保護為核心〉，《科技法律透析》，第 25 卷第 10 期，頁 46-62 (2013)。

[13] 蔡博坤，”談美國需量管理法制政策對台灣綠色產業發展之啟示”，*第十七屆全國科技法律研討會*，國立交通大學科技法律研究所，2013，頁 1051-1069。

[作者簡介]

蔡博坤，法律研究員，財團法人資訊工業策進會，美國賓州州立大學(Pennsylvania State University, University Park)法學院畢業。