國立政治大學法律科際整合研究所

碩士論文

指導教授：李治安　博士

雲端運算時代個資隱私安全之探討
— 以雲端服務條款為中心

研 究 生：孫德沛 撰

中　華　民　國　一百　年　七　月

致謝

時間匆匆，隨著論文的付梓，從公館到貓空的四年即將過去，回首過去四年在指南山腳下的生活，埋頭苦讀於圖書館的日子，很慶幸沒有偏離當初離開台大時想要完成的目標，改念法律，參加國家考試，撰寫論文，為下一階段的人生作準備。這一路上認識許多好友、師長和同道前輩，受到許多人的鼓勵和提攜，感謝之情溢滿胸懷。

能夠完成論文和順利畢業，首先要感謝指導教授李治安老師這一年多來的指導和提攜，也要感謝李老師包容我不斷調整論文方向，還有我拖拖拉拉的進度以及五月去律訓時進度空白的一個月，李老師嚴謹的治學態度還有為人處事的方式讓我受益良多。論文的順利完成還要感謝口試時兩位委員，陳起行老師及余啟民老師，兩位老師學養豐富，給我許多論文上的寶貴意見和方向，讓我能夠更完善我的文章概念及體系。另外還要感謝資科系的胡毓忠老師啟發了我對雲端議題的興趣，胡老師從科技的角度帶給我對雲端法律問題和歐盟安全指令不同的視野。

人生每個重要的時點與轉折總是受到許多人的關心和幫助，我能取得兩個學位和專心準備考試，最要感謝的是父母親及許多家人多年來的栽培和照顧，讓我能無後顧之憂任性地往自己的目標前進。除此之外，還要感謝提供許多精彩課程的所上老師們，所辦的行政人員，法科所同屆的同學們，一起打拼國考的讀書會成員和課輔助教們，還有許多曾經幫助過我而未言及的大家，有了你們的協助和鼓勵，我才能順利完成在政大的學業。當然還有最重要的小綠兒，有妳的陪伴，讓我度過了準備考試和寫論文時的辛苦，感謝妳的相伴，讓我的人生充滿許多色彩。

雲端運算時代個資隱私安全之探討 — 以雲端服務條款為中心

摘要

雲端運算的特性在於只要連線上雲端服務提供者的平台，隨時隨地就可以享受到最新最便利的雲端服務。雲端運算因此具有使用彈性、接觸容易、擴充迅速及即用即付費的優勢，不用在像過去套裝軟體時代花費成本在軟硬體升級上，所以有愈來愈多的使用者踏入雲端行列，雲端運算技術及服務已成為資訊產業關注的焦點。但是雲端運算的這項優勢卻容易讓人忽略是建立在將資訊傳至雲端伺服器來進行處理、運算及儲存的模式，這固然讓使用者享受到雲端服務，但雲端服務提供者也同樣掌握了使用者資訊，使用者因而不再完全控制資訊的應用及流向，使得資訊外流的可能性大幅增加。這些資訊安全風險可能來自於雲端平台的穩定性或安全漏洞，或者是雲端業者基於商業考量的洩漏給其他廣告贊助商等第三人。雲端服務提供者針對這些資訊隱私安全的疑義，訂立許多雲端隱私權政策及使用條款來規範與使用者間的法律關係。本研究即先從美國法及歐盟安全指令等國際公約著手，探討可以作為網路雲端時代的規範基礎，並以此分析雲端服務的隱私權政策及服務條款。根據這些分析討論的結果，再探討在我國民法、消費者保護法及新修正通過之個人資料保護法之體系下，這些雲端隱私權政策及服務條款的適法性問題。

關鍵字：雲端運算、雲端服務、隱私權政策、服務條款、歐盟安全指令、個人資料保護法

雲端運算時代個資隱私安全之探討 — 以雲端服務條款為中心

目錄

摘要.....i
目錄.....ii
第一章　序論.....1
　第一節　研究動機與目的.....1
　第二節　研究範圍與方法.....10
　第三節　研究架構.....11
第二章　雲端運算的發展.....14
　第一節　資訊網路科技的發展.....14
　第二節　雲端運算的發展.....18
　第三節　何謂雲端運算.....21
　　第一項　雲端運算的內容類型.....23
　　第二項　雲端運算的架構關係分類.....25
　　第三項　雲端運算的評估項目.....27
第三章　雲端資訊安全風險的源由.....29
第四章　雲端資訊流通的法令與國際規範.....40
　第一節　美國法制中對個人資訊保護的相關規定.....41
　第二節　個人資訊資保護的國際規範.....51
　　第一項　經濟合作暨發展組織.....51
　　第二項　歐盟個人資訊保護相關規範.....53
　　第三項　亞太經濟合作會議.....58
　　第四項 小結.....59
　第三節　跨境傳輸與國際規範.....60
　第四節　本章小結.....63
第五章　雲端運算的隱私權政策與服務條款.....65
　第一節　雲端隱私權政策.....65
　　第一項　雲端使用者希望獲得的保障.....66

第二項　雲端隱私權政策的具體內容.....72
第三項　小結.....88
第二節　雲端服務條款.....88
第一項　雲端服務條款之探討.....89
第二項　雲端服務條款的具體內容.....91
第三項　小結.....109
第三節　企業使用雲端服務應進行的步驟.....110
第四節　本章小結.....112
第六章　我國法制對雲端運算條款的檢討.....115
第一節　消費者保護法對雲端條款的檢討.....115
第二節　個人資料保護法對雲端條款的檢討.....126
第三節　本章小結.....142
第七章　結論.....146
第一節　本文研究結果回顧.....146
第二節　雲端服務條款探討對其他雲端法律議題的影響及展望.....152
參考資料.....156
一、英文部分.....156
(一) 英文專書.....156
(二) 英文期刊論文.....156
(三) 英文新聞及網路資料.....159
二、中文部分.....165
(一) 中文專書及研究報告.....165
(二) 中文期刊論文.....166
(三) 中文新聞資料.....167
(四) 中文網路資料.....168
三、判決資料.....169
四、雲端運算隱私權政策.....170
五、雲端運算服務條款.....170

第一章　序論

第一節　研究動機與目的

一大清早，小吳昨晚設定的好的Google Calendar透過電腦發出音樂聲將小吳從夢中喚醒。為了今天的工作會報，小吳得早早出門，但沒想到路上碰上車禍塞車，小吳透過手機連上Google Map趕快找條可以替代的路線。到了公司後，小吳打開電腦開始執行Chrome，用Google Docs將開會要用的簡報投影片整理好。開完會小吳回到辦公室後連上網路用公司的MailASP[1]系統收發email來回覆客戶資訊及聯絡廠商，並且以Yahoo字典來翻譯外國客戶的意見，再透過MailASP將客戶訂單輸入到公司系統。中午午休時，小吳又連上券商網站觀看股市行情，順便通知業務員準備要下單了。到了下午的工作，老闆交代小吳要上傳上週在客戶工廠拍攝的的產品照片，於是小吳打開flickr[2]開始整理照片。快下班時，小吳收發自己的Gamil和Yahoo mail，發現Amazon來信說前陣子訂購的書已經寄送到附近的 7-11 請小吳去取貨。晚上回到家後，小吳又上網看到弟弟阿宏的Facebook上分享著網購海苔的心得，看著阿宏那精美的相片和生動的形容，讓小吳趕快連上Yahoo購物中心搜尋一下這間網路海苔店家，透過店家的訂購系統和銀行的線上信用卡服務，小吳也訂了一箱準備來和公司的同事分享。

套句流行語，小吳和你我一樣是資訊時代的新興人類，沒有了電腦、手機或計算機就無法工作生活。資訊世代的生活，讓我們習慣了以e-mail、Facebook和Blog來和人溝通，習慣了「Google」一下問題的答案，出了門要用Google Map和 5284 資訊網[3]規劃一下交通路線，要上醫院看病和買車

[1] Openfind 企業郵件代管系統，http://www.mailasp.com.tw/(查訪日期 2011 年 7 月 8 日)。
[2] flickr，http://www.flickr.com/(查訪日期 2011 年 7 月 8 日)。
[3] 台北市動態公車資訊網，http://www.taipeibus.taipei.gov.tw/(查訪日期 2011 年 7 月 8 日)。

票也習慣線上預約,付帳習慣使用電子信用交易,甚至買各東西也要上PTT和mobile01[4]看看賣家評價和各方意見，以免採到地雷，重視網友和鄉民的意見更甚於到實體店面試吃、試用和試穿。在這樣的情況下，彷彿沒了電腦、手機、行動裝置或各種消費性電子產品，我們就沒法過正常的現代生活。

但是嚴格說起來，我們不是只重視電子產品，我們其實依賴的是透過各種電子產品來使用網路服務。在作業系統當道的時代，作為主流的Windows系統宰制了我們對電子產品的使用習慣，Microsoft用軟體著作權作限制，限定我們只能在一台電腦上使用一套軟體[5]，要在其他電腦上使用相同的軟體功能，很抱歉！Microsoft要我們另外付費。好在資訊技術的蓬勃發展，讓我們得以擺脫被Microsoft價格控制的日子。當然這不是因為軟體拷貝或盜版技術的發達，而是因為網路網頁技術的發展,「雲端時代」來臨了。

就像我們之前提到的主角小吳，小吳工作一整天使用的Gmail、Yahoo Mail、Chrome、Google Docs、Google Map、Google Calender、Facebook、flickr、Amazon、股票電子下單、信用卡網路交易和各種線上服務，大多都是建構在「雲端運算」(Cloud Computing)上的網路服務。對於像小吳這樣的一般使用者而言，雲端運算帶來與Windows作業系統時代最大不同之處在於，現在小吳只要可以連上網，不論是在哪台電腦、手機或各種行動裝置，都可以接觸到相同的線上服務[6]。不用再受限於Microsoft的授權政策，不用限定只能在特定地區或裝置上使用軟體或作業系統，只要能夠連上網，就可以在任何地方和用任何裝置享受到雲端服務。在以往小吳交了授權費後，就被套裝軟體及作業系統的功能綁住，能夠使用的功能無法再

[4] 資訊討論網站 mobile01，http://www.mobile01.com/index.php(查訪日期 2011 年 7 月 8 日)。
[5] 即 Microsoft 著名的「One Machine, One Copy」授權政策，可參考 Microsoft 的網站說明:http://www.Microsoft.com/licensing/default.aspx (查訪日期 2011 年 7 月 8 日)。
[6] David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2216 (2009).

增減，小吳如果要使軟體或作業系統改版升級，不僅需要再另外付一次授權費用，還會因為系統效能最佳化等各種問題，連帶需要升級硬體設備。但在雲端運算時代，只要確保網路的流暢，就可以隨時根據需求要求雲端服務業者改變、更新或增減提供的內容，小吳僅需按照使用服務的質與量即用即付費，而非過去按版權數量的單一計費方式[7]。所以就算Microsoft過去在商場上打敗多少間Netscape，將IE瀏覽器綁在Windows作業系統上[8]，而又不斷更新版本，或者再用同樣方法作不公平競爭[9]，或再故技重施想用同樣方法綁住播放軟體[10]，小吳現在只要透過網路使用如Chrome等各種雲端資源，就能夠隨時下載更新服務，不用再去受作業系統和套裝軟體收費方式的氣。因此雲端運算的收費與運作模式，勢必將衝擊以往套裝軟體及作業系統的銷售模式，比爾蓋茲當年最害怕使用者不再需要作業系統的日子，即將到來[11,12]。

在過去作業系統主導的時代，使用者必須同時取得硬體及軟體資源，整合在一起才能使用，而隨著運算量的增加，必須隨時升級硬體資源，並同時取得軟體的更新及授權[13]。但對像小吳這樣的一般使用者而言，透過網路的連結與傳輸，能夠隨時向服務提供者要求增加運算資源及更佳的相容性和可靠性服務，而不需要在軟硬體上作額外投資[14]。因此雲端時代與

---

[7] Paul T. Jaeger et al., *Cloud Computing and Information Policy: Computing in a Policy Cloud?* , 5 J. INFO. TECH. & POL. 269, 270-271 (2008).

[8] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1, 2 (2008).

[9] 儘管 Microsoft 讓 Netscape「贏了官司，輸了公司」，但仍被法院判定是違法不當競爭。參考 United States v. Microsoft Corp., 253 F.3d 34, 58-78 (D.C. Cir. 2001)。

[10] 歐盟在 2007 年曾發現 Microsoft 藉由優勢的作業系統地位，來包裹 Windows Media Player，參考 Case T-201/04, Microsoft v. Comm'n, 2007 ECJ CELEX LEXIS 554, 2007 WL 2693858。

[11] 比爾蓋茲在 1995 年 5 月 26 日向 Microsoft 員工發表談話的備忘錄，摘自 1995 Internet Tidal Wave memo 中的連結 http://www.justice.gov/atr/cases/exhibit/20.pdf。

[12] Microsoft 為了要保住資訊服務業的龍頭地位，這幾年也推出 Windows Azure 平台，用來提供雲端線上服務所需要的作業系統與基礎儲存與管理的服務，積極搶攻雲端市場的商機。參考 http://www.microsoft.com/windowsazure/ (last visited 2011.07.08)

[13] Mark H. Wittow, Daniel J. Buller, *Cloud Computing : Emerging Legal Issues For Access to Data, Anywhere, Anytime*, 14 NO. 1 J. INTERNET L. 4, 5 (2010).

[14] J. Nicholas Hoover, *Interop: Oracle Predicts Cloud Confusion to Continue*, Informationweek,Sept. 12, 2008, http://www.informationweek.com/news/services/hosted_apps/showArticle.jhtml?articleID=210602225. (last visited 2011.07.08)

作業系統時代最大的差異就是便利性，使用者只要能夠連上網路，就可以使用雲端資源，這連帶也使得電腦業界掀起一股「網路筆電」(Internet notebooks or “netbooks”)的風潮[15]，未來有可能價廉、重量輕及配備簡單的筆電將成為電腦業界的主流。根據Pew Internet和American Live Project的調查，美國有將近69%的一般網路使用者在使用網路郵件服務(例如Gmail)、線上資料儲存或軟體服務(例如Google Docs)[16]，而最大的使用原因在於操作容易及使用方便；另有41%的使用者認為促使他們使用的原因，在於用任何電腦都可以很方便地使用到雲端服務的資源。

就如同小吳這樣的一般使用者受惠於雲端運算來帶的便利，公司企業同樣也可以從中找到運用的優勢。根據Gartner的研究指出，企業每十元的IT投資中，會有約八元是花費在既有軟硬體系統的維護，而非更新升級上[17]，所以如果能將企業內部的IT架構，交給雲端運算的服務業者，即可大幅降低系統維護費用。因此藉由雲端運算的這種「即用即付費」特性，企業用戶可以根據需求增減或甚至停用服務，並要求雲端業者[18]做出相應的調整。例如Animoto是一個專門提供使用者將個人照片轉化為音樂視頻的軟體應用網站，它提供在時下最夯的Facebook上應用的軟體，在開放的前三天裡，使用人數從 2 萬 5 千人激增到 25 萬人，而在熱門時段每小時就增加了 2 萬個新的使用者，該網站所用的伺服器在這三天中從 5 個擴充為 3 千 5 百個，能夠在這麼短的時間內滿足大量使用者的需求，靠的就是雲端運算擴充迅速的彈性和方便性[19]。因此運用雲端運算，企業不再需要建置眾多的

[15] Mark H. Hittow, Daniel J. Buller, *supra* note 13, at 6.
[16] John B. Horrigan, *Cloud Computing Gains in Currency*, PewResearchCenter Publications, September 12, 2008, http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency (last visited 2011.07.08)
[17] 張玉琦，雲端運算風暴來襲，數位時代，2008 年 10 月，頁 91。
[18] 為了行文的流暢與方便，本文中我們所指稱的「雲端業者」或「雲端服務業者」，均係指提供雲端服務的人員或企業。
[19] Animoto’s Facebook Scale-up, Right Scale Blog, http://blog.rightscale.com/2008/04/23/animoto-facebook-scale-up/. (last visited 2011.07.08)

硬體或系統，能夠將原本需要的IT維護費用釋出，進而大幅降低管理開銷[20]。比如我們的主角小吳所服務的公司，就是將公司的郵件系統轉換為Openfind的MailASP線上郵件服務，省去了自行建置郵件系統的成本。當然除了郵件服務的雲端項目外，企業還可以針對客戶關係、物流控制或人力資源管理等項目來選擇不同的雲端服務，例如Salesforce.com提供的顧客關係管理隨選軟體服務、Microsoft提供的CRM、ExChange、Office Communication及SharePoint等服務[21]。

對於像我國為數眾多的中小企業或新創業之公司，有效率地運用雲端資源，可以減少初期的投資，提升公司內部資源的利用率，避免在設備上投資過多的財務風險，企業也因此可以將更多資源專心投入到自己的事業中。例如在 2007 年，著名的紐約時報(New York Times)即採用Amazon的EC2[22]及S3[23]服務，來儲存及處理該報從 1851 年至 1980 年間 1 千 1 百萬筆的報紙掃瞄pdf檔[24]，如此巨大的資料量，Amazon一年僅收費 8 百餘美元，讓紐約時報省下了大筆的硬體費用[25]。

利用雲端運算，企業甚至可以從自身產業發展出新的商業模式。例如美國矽谷一間電玩公司OnLive就將電玩需要的儲存和高效能運算直接放在雲端上，遊戲玩家只需要一台口袋大小的主機和無線控制器，外加連上網路，不必下載和插入磁碟，就能夠將電玩遊戲直接從雲端平台上串流到客廳電視，玩家僅需就遊戲時數付費即可[26]。另外就防毒安全而言，如趨

---

[20] 天下雜誌編輯部，無縫接起智慧新生活，天下雜誌，特刊 31 號，2010 年 2 月，頁 8-9。

[21] 同註 17，頁 99。

[22] Amazon 公司的 Elastic Compute Cloud (EC2)服務，http://aws.amazon.com/ec2 (查訪日期 2011 年 7 月 8 日)。

[23] Amazon 公司的 Simple Storage Service (S3)服務，http://aws.amazon.com/s3 (查訪日期 2011 年 7 月 8 日)。

[24] Miranda Mowbray, *The Fog Over the Grimpen Mire: Cloud Computing and the Law*, 6 SCRIPTED 132, 134 (2009).

[25] 黃亦筠，雲端運算　衝擊台灣硬體業者，天下雜誌，特刊 31 號，2010 年 2 月，頁 18。

[26] John Biggs, *OnLive Cloud Gaming Service Goes Live June 17*, TECHCRUNCH (2010). 中文資料可參見 戴佳慧，雲端電玩 OnLive 美國驚喜上市，數位時代，2010 年 11 月，http://www.bnext.com.tw/article/view/cid/0/id/16566 (查訪日期 2011 年 7 月 8 日)。

勢科技等防毒業者可以在網路上架一朵「防毒雲」，使得企業用戶不用像過去得將病毒碼下載到自己的電腦來進行更新，只要在利用雲端服務時順便連上防毒雲，就能即時在網路上偵測病毒， 既可節省硬碟空間，也可縮短因應病毒爆發的處理時間[27]。

除了民間企業和個人使用雲端服務外，雲端運算所帶來便利和低成本的特性，也讓各國政府紛紛走上雲端的行列。例如美國Obama總統的資訊長(Chief Information Officer) Vivek Kundra最近就宣布成立www.apps.gov網站，將美國政府的效能和服務放上雲端，Kundra並且宣稱未來 10 年是美國聯邦政府推動雲端服務的重要時程，這項計畫如果完成後，每年將可省下 750 億美元的公共預算[28]。英國政府則在 2009 年 6 月提出「數位英國(Digital Britain)」計畫，規劃打造全國光纖網路，並在 3 年內成立G-Cloud平台，讓地方可以分享中央所擁有的應用軟體與雲端服務[29]。日本政府也在 2009 年 5 月提出「數位日本創造計畫(Digital Japan Creation Project)」，預定在 2015 年完成名為「霞關Cloud」的資訊技術基礎設施，強化日本政府各部門間資源整合共享，打造新型的電子政府[30]。我國政府也計畫將電子病例[31]及貨櫃資料中心[32]與雲端相結合，帶動國內產業跟上全球雲端市場發展商機。各國政府莫不將建立e化雲端政府作為當前的重大政策。

如此看來雲端運算好像有著許多優點，小吳和她的公司不再需要實體的硬體設備來儲存及運算資料，不用再負擔軟體升級的費用，使用雲端資源充滿彈性和便利，只需「即用即付費」或根據使用資源的質與量來付費。

---

[27] 趙郁竹，趨勢科技 11 月展示雲端科技系統，數位時代，2010 年 8 月，http://www.bnext.com.tw/article/view/cid/0/id/15842 (查訪日期 2011 年 7 月 8 日)。

[28] Andrew C. Devore, *Cloud Computing: Privacy Storm on The Horizon?*, 20 ALB. L.J. SCI. & TECH. 365, 367 (2010).

[29] 經建會部門計畫處，推動新興智慧型產業系列二 雲端運算，台灣經濟論衡，第 8 卷第 7 期，2010 年 7 月，頁 38。

[30] 經建會部門計畫處，同上註，頁 38。

[31] 中央社，工研院雲端應運 盼 3 年 7 成診所用電子病歷，2009 年 11 月 6 日。

[32] 蘇文彬，工研院雲端運用中心：明年底推出貨櫃資料中心與 OS，iThome，2009 年 12 月 14 日。

但是這麼便利的雲端運算，很容易讓人忽略這是一種建立在將資訊傳送至雲端的操作模式[33]，也就是說雲端業者是要透過網路匯集、整理、儲存和運算小吳的資料後再回傳給小吳，才能讓小吳享受到雲端資源的便利和彈性。這樣也就意謂著小吳無法知道她的資料是怎麼被儲存和被利用，小吳對她自己的資料喪失了百分百的控制。而且小吳一整天下來使用的Gmail、Yahoo mail、Chrome、Google Docs、Google Map、Google Calender、Facebook、flicker等諸多雲端服務，大多是對一般使用者「免費」提供。根據2010年台灣無線網路使用調查報告[34]，台灣有1622萬網路使用人口，其中以「瀏覽資訊、網頁」、「搜尋資訊」和「收發電子郵件」為主要使用功能，而這三項主要功能又是Google和Yahoo等雲端業者主力經營的項目。因此眾多的雲端使用者，可想而知需要大量的主機和運算資源，俗話說「賠錢的生意沒人作」，雲端服務業者也不是在開慈善事業，勢必一定要從「免費」提供的服務中找到新的商業模式。

我們一開始提到小吳一整天如何使用各種雲端服務，現在讓我們更仔細的體會下小吳的感受：

> 小吳昨晚想著明天一早要早起開會，所以要先設定好鬧鐘，打開 Google Calender，看到上週末和男朋友逛街買鞋子的行程就心裡甜甜的，看到右下角 SOGO 的 Diana 女鞋在打折，趕快加進這週六的行程。早上小吳塞在車陣中，要用 Google Map 找條替代路線時，看到旁邊有各「2011 最浪漫情人節約會地圖」，點進去一看是一堆餐廳位置和美食評價。到了公司開始開始工作，要來翻譯外國客戶的意見，打開 Yahoo 字典，右手邊總是出現「TuorABC　英文對你這麼好，你對英文作了什麼」的圖片，再不然就是「30Hrs 告別『坑疤』美語」，老是閃著閃著，總覺得看著很煩。中午午休時，小吳打開瀏覽器想要來看看今天的股市行情，旁邊就跳出了一個

[33] 李治安，當法律漫步在雲端，法學新論，25 期，2010 年 8 月，頁 56。
[34] 財團法人網路資訊中心，2010 台灣無線網路使用調查報告，http://www.twnic.net.tw/download/20307/1007d.pdf (查訪日期 2011 年 7 月 8 日)。

好大的富邦信用卡專屬財神動畫，還不曉得要怎樣把它關掉，得等它結束了才能繼續動作，看各網頁旁邊還有各小框框「TOYOA YARI 新世代 超低月付 3,999」一直在閃，真是煩透了。下午小吳要來收發自己的 mail 而打開 Yahoo，視窗頁面正中間跳出了「台灣房屋女人當家」好大一個畫面，還要想辦法把它關掉。晚上回到家後，小吳訂完阿宏分享的海苔後，看到好姊妹阿秀的臉書上抱怨妮維雅的乳液太貴了，瞄到旁邊屈成氏的露得清乳液在買一送一呢，想說來買買看好了…

好了，我們敘述到這邊就好，免得有商業性置入之嫌。我們從小吳使用的情形很明顯地可以看出來，這些「好心」提供「免費」服務的雲端業者，在像小吳這樣的一般使用者所用的服務中加入了大量廣告，而且怎麼這麼剛好上週小吳才去買鞋子，昨晚就出現Diana的廣告，怎麼看到妮維雅乳液的分享心得就出現了露得清乳液的廣告。可見Yahoo和Google掃瞄了小吳的郵件和網路行為[35]，可見所謂的「好心」和「免費」是有代價的。在過去的套裝軟體時代，我們付錢使用Outlook等軟體，現在我們要忍受Yahoo和Google，甚至Facebook，在我們的視窗網頁中加上一堆廣告。尤有甚者，我們還要忍受Yahoo和Google掃瞄我們的信件和我們在網路上進行的行為，來置入與我們過去網路行為相關的廣告[36]。而且Yahoo和Google這類服務提供者會不會再把我們的資料向廣告贊助商展示[37]，來顯示其雲端線上廣告的效益[38]，進而擴大資料外洩的危害，又或者因為政府或法院的搜查命令而向公部門交出使用者的資料，同時也讓使用者置身於不確定的法律風險[39]，這些都是讓人感到相當憂心的資訊隱私議題。這些對雲端

[35] 廖緯民，論搜尋引擎的隱私權威脅，月旦民商法雜誌，24 期，2009 年 6 月，頁 31。
[36] Randal C. Picker, *supra* note 8, at 6.
[37] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., (2010). *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html
[38] Paul Lanois, *Caught in The Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 NW. J. TECH. & INTELL. PROP. 29, 33 (2010).
[39] David S. Barnhill, *Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless*, 25 BERKELY TECH. L.J. 621, 634 (2010); William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy under the Stored Communications Act*, 98 GEO. L.J. 1195, 1208 (2010).

資料掌握的不確定性，當然也會影響到像小吳服務的公司這樣的企業的使用者;對企業用戶而言，喪失對資料完全的控制，意謂著經營風險的提高，因此企業必須被迫在雲端服務帶來的便利性和較低的軟硬體費用，來和喪失對資料的控制所造成的風險間取得平衡[40]。

此外對於資訊科技產生的安全性漏洞，則更是一個複雜的技術問題。雖然像Amazon和Google這些業者都宣稱，對於技術不足所產生的安全漏洞不負責任，但是到底這些業者在技術上是否有確實盡到安全防護的責任，就已讓使用者心中充滿了問號。電子隱私資訊中心(Electronic Privacy Information Center, EPIC)就在 2009 年對Google提出了質疑，甚至致函美國聯邦貿易委員會(Federal Trade Commission, FTC)，要求FTC調查並禁止Google提供大眾此類有隱私侵害疑慮的服務，其範圍包括Gmail, Google Docs, Google Desktop, Picasa Web Albums and Google Calender，涵蓋許多Google的主要服務項目[41]。

所以我們可以說雲端運算的安全性及資訊隱私權問題一直是使用者最介意的事項，根據統計有 35%的網路使用者覺得放置在網路上的資料和隱私受到了侵害[42]，這些侵害除了起因於雲端系統的安全問題外，更多的則是雲端業者對於雲端服務和使用者資訊的經營態度[43]，雲端業者的這種態度其實就展現在隱私權政策(private policy)與服務條款(terms of service)之中。藉由隱私權政策的宣示，雲端業者表達如何看待使用者資訊的立場；藉由服務條款的制訂，雲端業者規範了與使用者間的權利義務。因此要探討雲端使用者的資訊安全及隱私保護議題，就有必要從這些隱私權政策與服務條款著手，去探討業者與使用者間的法律關係。此外從網路時代開始

[40] Mark H. Hittow, Daniel J. Buller, *supra* note 13, at 6.
[41] EPIC, *Complaint and Request for Injunction, Request for Investigation and for Other Relief*, March 19, 2009, http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf (last visited 2011.07.08)
[42] *Behavioral Advertising Survey*, March 4, 2009, TRUSTe, http://www.truste.com/privacy_webinars/bt_slides.pdf . (last visited 2011.07.08)
[43] 劉靜怡，雲端運算趨勢與個人資訊隱私保護，全國律師，2010 年 2 月，頁 41。

發展時就有許多法令規定，甚至是國際條約，對於經由網路的資訊傳輸作出限制與規範，這些規章制度到了雲端時代仍有其適用，所以雲端服務的隱私權政策與服務條款並不是業者可以隨意制訂的，尚須遵循這些法令與國際規範。因此在本文中，我們將從這些面象來探討雲端使用者面對這些雲端業者時所會產生的權利義務法律關係，以及所發生的法律問題。

第二節　研究範圍與方法

如果我們從雲端產業面的角度來觀察，雲端服務者在建立平台及伺服器中心的前置成本相當高昂，因此只有規模如Amazon、Google和Yahoo等大公司才有可能經營這類的服務。相對於此等實力雄厚的大公司，像小吳這樣的一般使用者或她所服務的中小企業常顯的微不足道，再加上現行實務運作及在雲端業者的條款下，使用者常必須承擔個人資訊隱私洩漏的苦果[44]，使得使用者更加的弱勢。因此有必要從這些使用者的角度切入，來探討雲端運算的隱私權政策與服務條款的內容，是如何影響與界定使用者和服務提供者間的法律關係。至於我們前面所述各國政府的雲端計畫，由於雲端政府上的資訊常涉及大量公部門及民眾資料，需要國家政策與相關法制的配合[45]，因此不論是政府要自建雲端平台或使用委外雲端服務，也都須要詳細探究雲端隱私權政策與服務條款。是以在本論文中，我們將從雲端使用者的角度出發，除了強調法制面對個人資訊安全及隱私的保護，以及深入探討雲端隱私權政策與服務條款外，我們也將從我國法的角度來觀察，這些隱私權政策與服務條款的適法性問題。

---

[44] 李治安，同註 33，頁 59。

[45] Andrea Cascia, *Don't Lose Your Head in the Cloud: Cloud Computing and Directed Marketing Raise Student Privacy Issues in K-12 Schools*, 261 ED. LAW REP. 883, 889 (2011).

雲端運算是目前資訊時代最顯著的網路活動，而美國又是資訊科技的發明及新興大國，雲端運算即起源與發展於美國，從現在大多數的雲端業者均是美國公司即可見之，因此美國也勢必會先面臨各種雲端法律議題。當他國引進雲端技術及服務時，同樣也會再次面對曾發生在美國的相關議題，相應的美國文獻和法院判決將極具參考價值。此外雲端運算是這幾年在我國新興的產業及熱門話題，學界也逐漸發現有許多法律問題需要面對。因此本論文之研究方法將以文獻分析為主，並以美國的法律期刊、論文以及法院判決為研究對象,探討資訊安全、隱私權保護及著作權等相關議題；除此之外，我國原有的電腦處理個人資料保護法及新修訂的個人資料保護法均受到經濟合作暨發展組織、歐盟和亞太經濟合作會議等各國際組織規範的影響，在本文中我們也將從這些國際規範，來探討雲端時代隱私權政策與服務條款的相關議題。

第三節　研究架構

本文共分六各章節，簡述如下：

第一章　序論

第一節　研究動機與目的

第二節　研究範圍與方法

第三節　研究架構

第二章　雲端運算的發展

第一節　資訊網路科技的發展

第二節　雲端服務的發展

第三節　何謂雲端運算

第一項 雲端運算的內容類型

第二項 雲端運算的架構關係分類

第三項 雲端運算的評估項目

第三章 雲端資訊安全風險的源由

第四章 雲端資訊流通的法令與國際規範

第一節 美國法制中對個人資訊保護的相關規定

第二節 個人資訊保護的國際規範

第一項 經濟合作暨發展組織

第二項 歐盟個人資訊保護相關規範

第三項 亞太經濟合作會議

第四項 小結

第三節 跨境傳輸與國際規範

第四節 本章小結

第五章 雲端運算的隱私權政策與服務條款

第一節 雲端隱私權政策

第一項 雲端使用者希望獲得的保障

第二項 雲端隱私權政策的具體內容

第三項 小結

第二節 雲端服務條款

第一項 雲端服務條款之探討

第二項 雲端服務條款的具體內容

第三項 小結

第三節 企業使用雲端服務應進行的步驟

第四節 本章小結

第六章 我國法制對雲端運算條款的檢討

第一節　消費者保護法對雲端條款的檢討

第二節　個人資料保護法對雲端條款的檢討

第三節　本章小結

第七章　結論

第一節　本文研究結果回顧

第二節　雲端服務條款探討對其他雲端法律議題的影響及展望

第二章　雲端運算的發展

在第一章當中，我們藉由小吳的網路使用情形大致說明了在現代資訊時代中雲端運算所扮演的重要角色，而如果要更進一步瞭解雲端運算的內涵，或者要對雲端運算下個定義，那我們必須要先瞭解整個資訊時代的發展，以致於雲端運算的出現所改變的商業服務模式。因此在第二章中，我們將先介紹資訊時代的發展趨勢，並進一步介紹雲端運算的內涵和各種模式。

第一節　資訊網路科技的發展

美國知名的社會思想家及未來學者Alvin Toffler，在他的名著The Third Wave中，將人類的文明發展分成三個階段。第一個階段是農業時代，代表著人類從狩獵採集的生活方式演變成農業社會；第二個階段則是工業時代，肇始於 17 世紀的工業革命，人類發展科技和建立工廠，追求物質的創造、分配和享受[46]；第三個階段則是Toffler觀察到 1960 年代許多國家和社會的演變，提出了「後工業時代」(Post-industrial age)這樣一個名詞，在這個時代充滿了許多變化快速、多元性和無法預測的現象，這一切起因於電腦和網路科技的發展導致資訊的大量產生和傳遞，因此許多人把這個時期稱為「資訊時代」。

在Toffler所提出的三大階段中，又可細分成許多次階段，比如我們觀

[46] Toffler 的原文如下: "The Second Wave Society is industrial and based on mass production, mass distribution, mass consumption, mass education, mass media, mass recreation, mass entertainment, and weapons of mass destruction. You combine those things with standardization, centralization, concentration, and synchronization, and you wind up with a style of organization we call bureaucracy."

察圖 2-1 所示資訊時代的發展[47]，可以發現各個次階段是彼此緊密關連的。

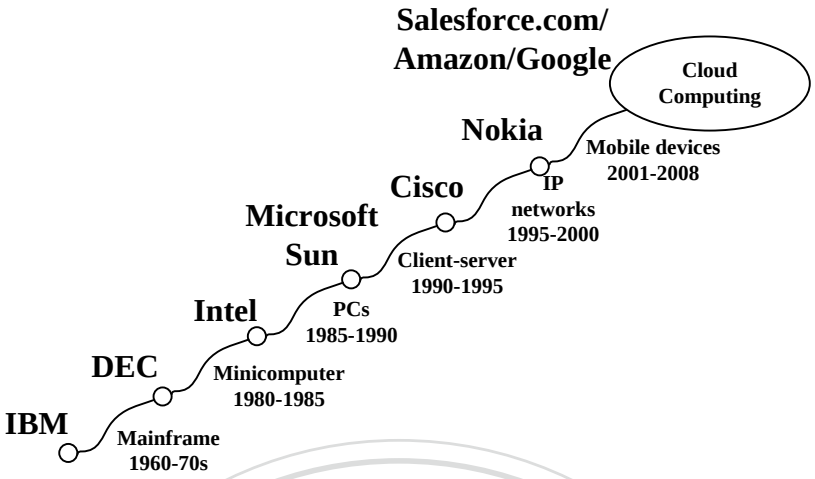

圖 2-1 資訊時代的各次世代發展

資料來源：Tim Mather et al., *supra* note 47, at 3.

在 1960-1970 年代是以IBM大型工作站主機(Mainframe)為主的時代[48]，當時電腦使用人員必須到機房才能工作，使用起來顯得費時、笨重和昂貴，所以接下來 20 年的趨勢就是產業界致力於將電腦縮小到方便使用的年代。經過DEC和Intel等無數業者的努力，逐漸發展出現在的個人電腦[49]。一般個人用電腦的普及，將使得套裝作業系統和軟體需求量大增，而家家戶戶都有機會取得個人電腦後，也將帶動電腦間溝通串連的需求，各種IP架構、主從伺服器架構和網際網路不斷發展出來[50]，因此Microsoft將網路架構加入它的套裝軟體和作業系統，開始主宰了市場[51]。到了 2000 年後，各種次微米和奈米製程的突破，使得電腦或計算機可以縮小到手持行動裝置(mobile device)上[52]，而無線通訊技術的發展與頻譜的開放，讓人們不用再侷限於個人電腦的使用空間，到哪都可以使用電腦和計算機，

[47] Tim Mather et al., Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance 3 (2009).
[48] Ruth L. Okediji, Development in the Information Age: Issues in the Regulation of Intellectual Property Rights, Computer software and Electronic Commerce 11 (2004).
[49] *Id*. at 11-13.
[50] *Id*. at 12-13.
[51] *Id*. at 18-19.
[52] *Id*. at 14.

有了無線通訊任何地方也都可以接觸到網路[53]。既然網路的使用可以微縮到手持行動裝置，而且使用範圍無遠弗屆，產業界開始思考何不把電腦需要的運算和儲存資源放在網路上，只要透過隨時可以接觸到的網路來使用這些資源，那麼就可以減少電腦或手提裝置的體積和重量，進而將減少的重量和空間轉換來增加電池的續航性，使行動裝置的應用更為廣泛。這種遠距離應用網路資源的概念就是所謂的「雲端運算」，也就是如圖 2-1 中許多人認為接下來資訊時代的發展將由雲端運算來主導[54]。

這邊我們藉由圖 2-2 所示，來整體觀察網路及雲端運算發展的過程，從中可以發現所謂的雲端運算和雲端服務提供者(cloud service providers, CSPs)，其實也可以說是起源於網路服務提供者(internet service provider, ISP)的應用模式。

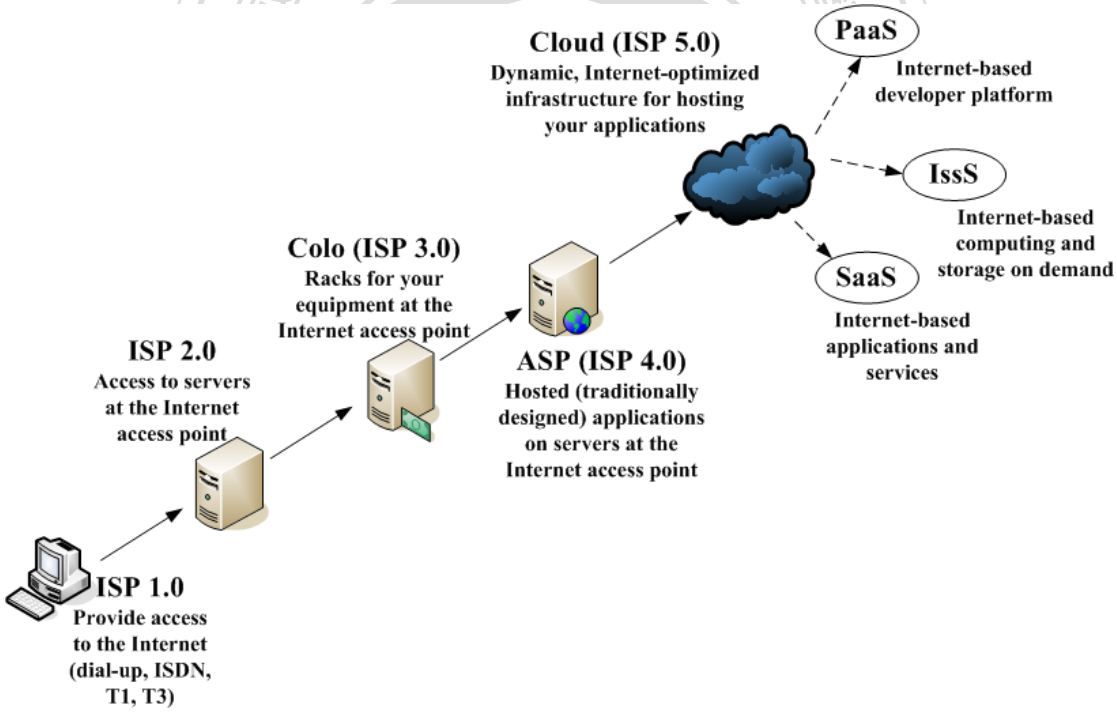

圖 2-2 網路和雲端運算的發展

資料來源：Tim Mather et al., *supra* note 47, at 4.

[53] *Id*.
[54] Tim Mather et al., *supra* note 47, at 2; Gartner, *Gartner Says Cloud Computing Will Be As Influential As E-business*, June 26, 2008, http://www.gartner.com/it/page.jsp?id=707508. (last visited 2011.07.08)

從圖 2-2 中我們可以看到，一開始網路服務提供者僅是透過電話撥接、T1 或T3 專線提供網路連結的服務，這種商業模式可以說是第一代的網路服務 (ISP 1.0)[55]。當個人電腦逐漸普及，不僅擴大網路使用的需求，也使得網路服務的競爭趨於激烈，因此網路服務提供者必須整合資源，除了提供網路連結外，還要開始提供一些有附加功能的服務，比如說收發email，甚至是對客戶主機伺服器提供服務，此時就進展到第二代的商業模式(ISP 2.0)[56]。隨著資訊網路技術的發展逐漸成熟，業界開啟了第三代的商業模式(ISP 3.0)，網路服務提供者開始建立大型的資料中心(data center)來代管客戶的網際網路伺服器，這就是所謂的主機代管(或主機託管)(Co-location facilities)[57]，例如客戶可以將自己的主機或網站搬到中華電信[58]或so-net[59]等提供主機代管服務業者的機房，透過中華電信或so-net的區域網路或其他電信系統與Internet連線，即可讓客戶的主機上線，客戶可以省下自行建立機房與維護的費用。到了第四代的商業模式(ISP 4.0)，網路服務提供者跳脫單純提供網路連結和上網的服務，開始轉型成為應用服務提供者(application service providers, ASPs)，除了主機代管服務外，更針對客戶的個別基礎架構提供各種軟體服務，這就是Web2.0 的雛形[60]，但仍舊是建立在專屬的基礎架構上[61]。到了第五代的商業模式(ISP 5.0)，也就是本書所談論的「雲端運算」，服務提供者不再僅是針對專屬的架構提供服務，更加強應用服務的提供，並且直接在網路上架一朵「雲」，將許多資源整合和分享在雲端，以供客戶使用[62]。

---

[55] Manuel Castells, The Internet Galaxy: Reflections on the Internet, Business and Society 9-11 (2001).
[56] *Id*. at 10-13.
[57] Wikipdeia definition of co-location facilities: http://en.wikipedia.org/wiki/Colocation_facility. (last visited 2011.07.08)
[58] 中華電信的主機代管服務，參考 http://www.cht.com.tw/BusinessCat.php?CatID=223(查訪日期 2011 年 7 月 8 日)。
[59] So-net 的主機託管服務，參考 http://ebiz.so-net.net.tw/idc_intro.html(查訪日期 2011 年 7 月 8 日)。
[60] Wikipdeia definition of web2.0: http://en.wikipedia.org/wiki/Web2.0. (last visited 2011.07.08)
[61] Tim Mather et al., *supra* note 47, at 4.
[62] Krissi Danielson, *Distinguishing Cloud Computing from Utility Computing*, ebiz.net, March 26, 2008, http://www.ebizq.net/blogs/saasweek/2008/03/distinguishing_cloud_computing/. (last visited

根據上述Toffler對人類文明演化概念及網路和雲端運算發展的說明，我們可以發現，透過網路就可以使用到許多雲端的服務和資源，節省許多成本，網路和雲端運算對於現代文明的重要性不言可喻。Nicholas Carr在他的成名之作The Big Switch一書中提出了一個有趣的概念，資訊時代的發展有各重要的現象和工業時代非常相似，他認為資訊時代雲端運算的興起就像工業時代的電氣化(electrification)[63]。在工業時代早期，人們要運轉機器從事生產必須要自己準備動力，例如要建立磨坊，就必須先建立水車或風車來取得動力；但是大規模鋪設電纜線後，人們要使用機器時不用再自備動力，只要將插頭接到電線，就可以享受電氣化帶來的動力[64]。就像動力電氣化般，資訊時代早期人們必須自己準備主機或電腦來做儲存運算(如同自己準備動力)，但是現在只要連接上雲端就可以使用運算資源(即如接電取得動力)[65]，所以Carr預測在不久的將來雲端運算帶來的網路資源將成為類似電力的公用事業，這股趨勢將連許多大企業都無法抵擋[66]。

第二節　雲端運算的發展

透過前節的說明，我們瞭解到雲端運算是現在網路服務發展的趨勢結果。但是早在 1960 年大型主機發展的年代，就已經有串接主機進行運算整合的概念[67]，雖然這樣的串連概念還僅是機房內部的連線，遠非現在網際網路的概念，但是當時就已知名的電腦科學家John　McCarthy提出了「有

2011.07.08)

[63] Nicholas Carr, The Big Switch , Rewiring The World, From, Edison to Google 13 (2009).

[64] *Id*, at 15.

[65] *Id*, at 46.

[66] *Id*, at 115.

[67] R. Buyya, et al., *Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*, FUTURE GENERATION COMPUTER SYSTEMS (2009).

朝一日運算將成為公用事業」[68]這樣的想法[69]，成為了日後雲端運算的概念開端。但實際上「雲端」一詞源於 1990 年代電信網路開始興起時，用來表示虛擬私人網路服務(virtual private network, VPN)的架構，也就是用來表示區域網路的連線型態，後來再衍生為代表網際網路的符號[70]。學術上，則是Ramnath K Chellappa在 1997 年開始使用雲端運算(cloud computing)一詞，用來涵蓋與描述使用者、伺服器、TCP/IP和各種網路基礎架構[71]。

到了 2006 年 3 月Amazon整合網路泡沫化後多餘的運算資源，建立更有效率的基礎架構(infrastructure)來提供給客戶使用，正式揭開雲端運算時代的序幕，Amazon提出的網路服務(Amazon Web Services, AWS)包含了非常有名的EC2 和S3 服務[72]。2006 年 8 月Google執行長Eric Schmidt在搜尋引擎大會(SES San Jose 2006)首次正式提出「雲端運算」這一名詞，宣告Google開始進軍ISP5.0 雲端運算的行列[73]。Google在雲端的發展來勢洶洶，首先在 2007 年推出Google Gears平台，利用雲端技術讓使用者不論連線與否都能使用到雲端網路服務[74]，之後在 2008 年推出劃時代的Chrome瀏覽器，讓使用者可以透過任何電腦接觸到雲端上自己常用的Google工具，顛覆了以往套裝軟體與作業系統的使用習慣[75]，Google更企圖以Chrome為平台，發展出一套全新的雲端作業系統[76]。至於身為作業系統老大的Microsoft

---

[68] 原文為「Computation may someday be organized as a public utility.」

[69] Reinhold Quillen, *Cloud Computing – Hype and Reality,* QUILLEN INFRASTRUCTURETECHNOLOGIES 3 (2010).

[70] Wikipdeia definition of cloud computing: http://en.wikipedia.org/wiki/Cloud_computing. (last visited 2011.07.08)

[71] Amit Mehra, *Evolution of the Cloud*, 8 NO 3, ISB INSIGHT 30, 31 (2010).

[72] Robert D. Holf, *Jeff Bezo's Risky Bet,* Bloomberg Businessweek, November 13, 2006, http://www.businessweek.com/magazine/content/06_46/b4009001.htm. (last visited 2011.07.08)

[73] Donna Bogatin, *Google CEO's New Paradigm: Cloud Computing and Advertising Go Hand-in-hand*, ZDNet News&Blof, August 23, 2006, http://www.zdnet.com/blog/micro-markets/google-ceos-new-paradigm-cloud-computing-and-advertising-go-hand-in-hand/369. (last visited 2011.07.08)

[74] Erick Arvidsson, *Gears API Blog: Going Offline with Google Gears*, Gears API Blog, May 30, 2007, http://gearsblog.blogspot.com/2007/05/posted-by-aaron-boodman-and-erik.html. (last visited 2011.07.08)

[75] Google, *A Fresh Taker on the Browser*, The Official Google Blog, September 1, 2008, http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html. (last visited 2011.07.08)

[76] Google, I*ntroducing the Google Chrome OS*, The Official Google Blog, July 7, 2009, http://googleblog.blogspot.com/2009/07/introducing-google-chrome-os.html. (last visited 2011.07.08)

也不甘示弱，在 2008 年提出Windows Azure平台，企圖在雲端產業中扳回一城[77]。行動裝置王者Apple，也在 2008 年 8 月提出MobilMe服務，將雲端技術用以提升並強化.Mac的功能，讓Apple的雅痞一族可以將儲存於Mac電腦、iPhone和iPad中的通訊錄、電子郵件、照片和其他資料進行同步化[78]。在產學合作方面，2007 年 10 月Google與IBM開始對美國卡內基美隆大學、麻省理工學院、史丹福大學、加州大學柏克萊分校、華盛頓大學及馬里蘭大學等院校，提供軟硬體相關設備與技術支援，希望能夠推廣雲端運算技術的發展[79]。2010 年 7 月，美國國家航空暨太空總署和包括Rackspace、AMD、Intel和Dell等支援協力廠商共同宣布「OpenStack」雲端軟體開放原始碼計畫，更進一步推廣雲端的應用[80]；微軟為了加強與新興對手Google在市場上的競爭力，在 2010 年 10 月宣布加盟OpenStack計畫，並且進行OpenStack與Windows Server 2008 R2 的整合[81]；2011 年 2 月Cisco也正式宣佈加入OpenStack計畫，重點開發OpenStack的網路應用服務[82]。

至於我國雲端運算的發展，2008 年 1 月Google在台灣宣布啟動「雲端運算學術計畫」，將與台大及交大等學校合作，希望能在台灣播下雲端運算的種子[83]。至於我國企業亦開始發展雲端的軟硬體相關產業，例如鴻海

---

[77] Ina Fried, *Microsoft Launches Windows Azure*, CNET NEWS, October 27, 2008, http://news.cnet.com/microsoft-launches-windows-azure/. (last visited 2011.07.08); 中文資料可參考 王炙人，後蓋茲時代，微軟從雲端反擊 Google，數位時代，171 期，2008 年 8 月，頁 43。

[78] Robert Palmer, *Apple Adds Another Month Free for Some MobileMe Trials*, The Unofficial Apple Weblog, July 22, 2008, http://www.tuaw.com/2008/07/22/apple-adds-another-month-free-for-uk-mobileme-trials/. (last visited 2011.07.08)

[79] Steve Lohr, *Google and IBM Join in Cloud Computing Research*, The New York Times, October 8, 2007, http://www.nytimes.com/2007/10/08/technology/08cloud.html?_r=2&ex=1349496000&en=926.27f0f65ea0d75&ei=5090&partner=rssuserland&emc=rss&oref=slogin. (last visited 2011.07.08)

[80] Rackspace, *Rackspace Open Source Cloud Platform; Announces Plans to Collaborate with NASA and other Industry Leaders On Openstack project*, Rackspace Newsroom, July 19, 2010, http://www.rackspace.com/information/newsroom/pressreleases/rackspace-open-sources-cloud-platform-announces-plans-to-collaborate-with-nasa-and-other-industry-leaders-on-openstack-project/. (last visited 2011.07.08)

[81] Microsoft, Openstack is Now Open For Windows Server, Microsoft News Center, October 22, 2010, http://www.microsoft.com/Presspass/press/2010/oct10/10-22OpenStackPR.mspx. (last visited 2011.07.08)

[82] Lew Tucker, *Cisco Joins Openstack Community*, Cisco Blog, February 3, 2011, http://blogs.cisco.com/news/cisco-joins-openstack-community/. (last visited 2011.07.08)

[83] 張德厚，與學界合作 Google 推廣「雲端運算技術」，中廣新聞網，2008 年 1 月 30 日。

在2009年6月與資策會合作建立雲端實驗室，藉由鴻海本身的研製能力，試圖從伺服器硬體跨足到應用端的軟體服務[84]。廣達則是另闢蹊徑，希望藉由雲端技術的發展，將電腦變成載具，從硬體產業進展到系統產業，在到對客戶提供解決方案和服務，徹底改變電腦使用的方式[85]。華碩則是在Eee PC上附上 500G的雲端儲存容量ASUS Webstorage和線上內容ASUS@Vibe，來和Apple的平板電腦iPad作區隔，企圖為被看衰的小筆電加分[86]。國內最大的通訊龍頭中華電信更是信心滿滿，積極整合資通與雲端技術，期望成為國內推動雲端產業的火車頭，並在 2011 年將針對光世代100Mbps以上客戶推出雲端資料櫃(cloudbox)服務，提供客戶雲端儲存等相關服務[87]。

第三節　何謂雲端運算

前面我們介紹了網路服務和雲端運算的發展，那麼到底何謂「雲端運算」？對於這個問題的答案其實眾說紛紜，但實則內容大同小異[88,89]。在這裡我們整合美國國家標準與技術局(National Institute of Standards and

[84] 謝佳雯，鴻海與資策會 共建雲端運算，經濟日報，2009年5月25日。
[85] 黃亦筠，筆電之後是什麼？林百里：我不去藍海，我去雲端，天下雜誌，特刊31號，2010年2月，頁15-17；文茜的世界財經週報，林百里的願景與廣達的雲端佈局，2009年11月22日。
[86] 蘇湘雲，雲端加內容支援 Eee PC嗆聲不怕iPad，NowNews，2010年3月19日。
[87] 倪慈緯，中華電信推出多項計費方式的雲端服務，RUN!PC，2011年2月26日，http://www.runpc.com.tw/news.aspx?id=100531 (查訪日期2011年7月8日)。
[88] 例如 Microsoft 的副總經理暨法務長 Brand Smith 在 Brookings Institution 的演講就對雲端運算下個定義：「a platform for the delivery of software services and other applications through remote file servers. Rather than storing and accessing information on your desktop and computer, your data and software exist on remote servers and are accessible wherever you happen to be.」，參考 Brand Smith, Keynote Address at the Brookings Institution: Cloud Computing for Business and Society, January 20, 2010, http://www.microsoft.com/presspass/presskits/cloudpolicy/docs//20100120_transcript.pdf. (last visited 2011.07.08)
[89] O'Reilly Media 的老闆，同時也是自由軟體和開放原始碼支持者的 Tim O'Reilly，形容雲端運算就是「a network of networks」，參考 S.E. Slack, *Is There Value in Cloud Computing?*, IBM developerWorks, March 31, 2009, http://www.ibm.com/developerworks/architecture/library/ar-valuecloudcomputing//?S_TACT=105AGX01&S_CMP=HP. (last visited 2011.07.08)

Technology, NIST)[90]及歐盟執行委員會(European Commission)[91]的解釋,「雲端運算」可以被定義如下：

雲端運算是一種使用彈性方便的網路資源與計時量付費的網路服務模式，可因應使用者不同需求，動態快速調整使用資源(包括網路、伺服器、儲存、應用和服務)。

當然雲端運算也可以被視為一種平台或架構，容易被控管而且具有彈性。這邊所謂的「容易被控管」係指雲端運算的可靠度問題可以根據使用者的需求來決定,「具有彈性」則意謂著使用資源的調整充滿動態，隨時可以根據需求來予以增減。

所以我們可以歸納出雲端運算的幾項特性[92]：

1. 多租戶技術(multitenancy)：不像傳統的系統資源使用方式是每個用戶分別使用一個資源，雲端服務的提供者可以針對同個運算資源，利用虛擬化技術切割資料庫(database)、系統儲存區(storage)、結構(scheme)或表格(table)來供不同使用者使用[93]。
2. 可擴充性(massive scalability)：不論使用者的需求增加多快速，雲端技術可以讓業者不斷擴充所需的運算資源。
3. 使用彈性(elasticity)：使用者可以根據需求快速增減使用量，並能將不需要的運算資源快速釋出。
4. 依據使用量付費(pay-per-use or pay-as-you-go)：使用者僅需要根據使用量和使用時間來負擔費用。

[90] NIST Definition of Cloud Computing: http://www.nist.gov/itl/cloud/ (last visited 2011.07.08)
[91] European Commission, *The Future of Cloud Computing, Opportunities for European Cloud Computing Beyond 2010, available at* http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf. (last visited 2011.07.08)
[92] Tim Mather et al., *supra* note 47, at 8.
[93] Wikipdeia definition of miltitency: http://en.wikipedia.org/wiki/Multitenancy (last visited 2011.07.08)

5. 自行調控資源機制(self-provisioning of resources)：雲端系統能夠根據使用量來自行調整運算、儲存和網路資源。

實際上有許多人認為「雲端運算」並非是種新的網路技術，而僅是將過去舊有的技術和資源重新整合[94]，這當中包括了分散式運算(Distributed Computing)、網格運算(Grid Computing)、虛擬化技術(virtualization technology)、應用程式介面(application programming interface, API)、儲存裝置(storage device)、資料中心(data centers)、伺服器群(server farm)、高速頻寬(high-speed broadband)、瀏覽器(browser)和接觸裝置(包括個人電腦、筆電或各種行動裝置)等，所以無寧說雲端運算是新興的技術，不如將之定位為新的概念或模式是比較恰當的作法。以下我們將介紹雲端運算的內容、架構關係分類，以及技術上的評估項目。

第一項　雲端運算的內容類型

根據雲端服務業者提供的服務內容，我們可以將雲端內容分成軟體即服務(Software as a Service, SaaS)、平台即服務(Platform as a Service, PaaS)及基礎架構即服務(Infrastructure as a Service, IaaS)等三大類[95]。此外由於運算資源及硬體的配置關係，通常業者會專注在提供特定服務，當然也有業者會同時提供SaaS和PaaS的服務，例如Google App Engine整合了Google Docs就是各明顯的例子[96]。以下我們將針對各種類型作介紹：

1. 軟體即服務(Software as a Service, SaaS)：

---

94 Tim Mather et al., *supra* note 47, at 11.
95 *Id*, at 17.
96 Tectdirt, *Google Finally Realizes It Needs to Be the Web Platform*, April 7, 2008, http://www.techdirt.com/articles/20080407/225749782.shtml (last visited 2011.07.08)

過去使用者要使用軟體，必須在支付授權費用後，才能將軟體安裝在電腦硬體中，有時還必須持續付費才能獲得新的更新檔，因此使用者需要關心的是軟體與作業系統相容性的問題，以及更新檔執行和授權期限等問題[97]。但在SaaS的模式中，使用者是透過網路來使用軟體服務，軟體的使用只要根據使用量來付費(pay-per-use)即可，甚至我們前面提到小吳所用的mail或Google Docs往往都是免費的。對於像小吳服務公司這樣的企業用戶，可以將公司所需的軟體或應用程式委由雲端業者來提供，省掉維持授權或軟體升級的費用。對於雲端業者而言，SaaS模式能夠徹底掌握軟體的著作授權，隨時增減、終止或升級服務，因此可以將軟體著作非法重置或散佈的問題減到最低[98]。例如Gmail、Yahoo Mail、Mint或Salesforce.com等均屬於SaaS服務。

2. 平台即服務(Platform as a Service, PaaS)

在PaaS模式中，業者提供的是一個可供發展的環境平台，讓使用者可以在平台上創作出其他的軟體或應用服務，當然提供平台服務的業者會發展出專屬該平台的介面工具、程式標準、散佈管道及收費方式[99]。因此與SaaS模式相較，SaaS的使用者直接使用的是已經發展好的應用軟體，PaaS的使用者則是透過瀏覽器在這個平台上使用業者的應用程式介面來創作，不用安裝任何工具在使用者的電腦上，就可以快速開發新的軟體或應用服務[100]，而且還能夠直接使用業者的平台系統及伺服器來運作所開發的軟體或應用服務，或分享散佈來讓更多的一般使用者使用到所開發的軟體或應用服務，因此可以降低進入市場與顧客使用管道的費用[101]。以Facebook Platform為例，其上的應用程式介面可以讓使用者

97 Tim Mather et al., *supra* note 47, at 18.
98 *Id*.
99 European Commission, *supra* note 91, at 9.
100 Tim Mather et al., *supra* note 47, at 19.
101 *Id.* at 20.

開發在Facebook網站上執行的程式[102]，例如在第一章提到的Animoto，就是利用Facebook的應用程式介面開發出受人歡迎的音樂視頻軟體[103]。例如Force.com、Google App Engine、OrangeScape、Wolf PaaS或Windows Azure等均屬於PaaS服務。

3. 基礎架構即服務(Infrastructure as a Service, IaaS)

在IaaS模式中，業者可以建立相同的伺服器介面，並藉由虛擬化功能的技術將基礎架構整合起來，類似將旅館分隔成數各房間來供給使用者利用，這當然也意謂著業者可以根據使用者的需求來彈性調整整個基礎架構[104]。IaaS模式又可分成兩種型態：第一種是例如Amazon S3 或SQL Azure[105]等服務，能夠動態調整架構來提供客戶適合的數據儲存空間[106]；第二種則是如Amazon EC2、Zimory[107]或Elastichosts[108]等服務，藉由如虛擬管理裝置(hypervisors)等環境技術，來對使用者提供CPU等運算資源。當然與PaaS 相較，IaaS所涉及的虛擬技術和開發元件相對是比較基本的[109]。

第二項　雲端運算的架構關係分類

前面我們提到所謂的「雲端」一詞原本是用來代表網際網路的連線型態，因此我們可以根據網路是對外開放或對內封閉的架構關係，來將雲端

[102] Wikipdeia definition of Facebook: http://en.wikipedia.org/wiki/Facebook (last visited 2011.07.08)
[103] Animoto's Facebook Scale-up, *supra* note 18.
[104] Tim Mather et al., *supra* note 47, at 22.
[105] SQL Azure, *available at* http://www.microsoft.com/windowsazure/sqlazure/ (last visited 2011.07.08)
[106] European Commission, supra note 91, at 9.
[107] Zimory, *available at* http://www.zimory.com/index.php?id=77 (last visited 2011.07.08)
[108] Elastichost *available at* http://www.elastichosts.com/cloud-hosting/pricing (last visited 2011.07.08)
[109] *Id*.

分成「公共雲」(public cloud)與「私有雲」(private cloud)[110]。簡單言之，公共雲就是對不特定的大眾開放(open to the public)，私有雲則僅是對內供給特定群人來使用(private to some set of people)[111]。

但是這種架構範圍的分類法其實會產生模糊地帶，例如私有雲的使用者可能會是一個人、一個部門、一間公司、一個社群、一個國家或上述任一團體的集合，以使用者的範圍來做界定也僅是範圍大小之別[112]。因此要再加上使用者和服務提供者間的關係來觀察，公共雲是相對架設在使用者的外部，是由提供服務的業者來控制和營運，因此又稱為「外部雲」(external cloud)[113]；私有雲則是架設在使用者的內部，使用者對雲端系統擁有控制權限，因此又稱為「內部雲」(internal cloud)[114]。當然以使用者和控制權限來類型化，同樣也會產生模糊地帶，例如Eucalyptus[115]為供應鍊的上下游廠商建構共同使用的私有雲，但對於也能夠使用這朵雲的其他客戶而言，這其實是朵公共雲。所以這種除使用者可以控管，又可讓外部其他人使用的雲端系統，就是種「混合雲」(Hybrid Cloud)的概念[116]。

討論私有雲、公共雲和混合雲的實益，其實在於讓使用者瞭解雲端服務的本質和產業的方向[117]。私有雲和公共雲的利弊剛好是相對的，使用者利用私有雲固然減少管理上的安全風險，但同樣將喪失公共雲的經濟規模可以帶來的效益，但使用公共雲則相對有安全管理上的風險，所以採用混

---

[110] 2010 Rackspace Partner Leadership Summit, *Public Cloud? Private Cloud? What is the Difference?*, (October 5, 2010), *available at* http://c1776742.cdn.cloudfiles.rackspacecloud.com/downloads/pdfs/PublicCloudPrivateCloudWhatistheDifference_PaulRad.pdf.

[111] *Id.*

[112] Mike Klein, *Public Cloud or Private Cloud?*, OTBlog, September 27, 2010, http://resource.onlinetech.com/public-cloud-or-private-cloud/ (last visited 2011.07.08)

[113] *Id.*

[114] *Id.*

[115] Wikipdeia definition of Eucalyptus: http://en.wikipedia.org/wiki/Eucalyptus_(computing) (last visited 2011.07.08)

[116] David Linthicum, *Why the hybrid Cloud model is the Best Approach*, InfoWorld, January 27, 2011, http://www.infoworld.com/d/cloud-computing/why-the-hybrid-cloud-model-the-best-approach-477(last visited 2011.07.08)

[117] *Id.*

合雲可能是比較適當的解決方式[118]。但是對使用者而言，一朵朵混合雲間如果缺乏轉換性，將產生依賴單一業者的風險，不利建立良性的競爭市場。因此雲端服務提供者應該體認到相關的雲端技術應該是開放的，這也就是OpenStack計畫開放原始碼的精神[119]，不僅建立雲端技術的標準，讓業者能夠自由競爭並避免技術上的冗斷，也降低使用者的各種風險，以利雲端運算的推廣。

第三項　雲端運算的評估項目

前面我們說明了雲端運算的內涵，並且分析了雲端服務可以方便擴充、使用彈性與即用即付費等特性，那麼在技術上如何評估雲端運算，以下我們列舉幾個項目[120]：

1. 彈性(elasticity)：也就是雲端業者能夠根據使用者的需求，快速地動態調整所需的運算儲存資源，並將使用者不需要的資源釋放出來。
2. 可靠度(reliability)：在 2011 年 3 月時，Gamil的使用者最切身的痛就是系統上大量的信件和通訊錄遺失，有超過 15 萬的使用者受到影響[121]。所以可靠度作為夠確保雲端系統持續運作而不會中斷的能力，是非常重要的。可靠度常會和下面要提到的可用性非常相關，但可靠度的考量更著重在確保資料不會損毀、滅失或程式停止運作的能力。
3. 敏捷性和適應性(agility and adaptability)：此即雲端系統的自我動態調整能力，包括調配雲端需求時的即時反應，或改變不同型態和路徑的雲端資源時系統的穩定性等。

---

118 *Id.*
119 Openstack Web, *available at* http://openstack.org/projects/ (last visited 2011.07.08)
120 European Commission, *supra* note 91, at 14.
121 陳炳宏，升級出包？全球 15 萬 Gmail 用戶受駭，自由時報，2011 年 3 月 1 日。

4. 可用性(availability)：是雲端服務非常重要的指標，經常以運算資源釋放的能力及釋放後的穩定性來作為評估標準，也就是系統容許錯誤的能力，涉及資料儲存和暫時存取記憶體間的動態調整。
5. 服務品質(Quality of Service)：除了上述幾項特徵外，雲端系統還要考量到反應時間(response time)、吞吐率或處理能力(throughput)等。

第三章　雲端資訊安全風險的源由

在第一章中我們提到像小吳這樣的一般使用者或像小吳服務公司這樣的企業用戶，愈來愈依賴雲端運算所帶來的便利，也將愈來愈多的信件、檔案、照片、影片或其他資料存放在雲端上，連人與人之間的交往溝通也要依賴架設在雲端上的如 Facebook、Twitter 或 Plurk 等社群網站。但是就如同我們前面提到的，將資料檔案放在雲上就意謂著喪失相當的主控權，連線到雲上進行動作也意謂著所有網路行為都會被雲端業者紀錄下來，因此不管是一般使用者或者企業用戶，都必須承擔使用雲端服務帶來的風險。

雲端業者掌握這些使用者資訊後，當然就是要藉此提供各式各樣的服務，就雲端的企業應用與一些一般使用而言，業者所提供的服務是要收取費用的，但對於多數的雲端一般使用者，例如常見的 Google 或 Facebook 等一般使用，雲端業者通常是「免費」提供服務。不過就如同我們第一章所描述小吳使用雲端服務的情形為例，雲端業者不是在進行慈善事業，業者勢必要在「免費」的雲端服務中開發出新的商業模式，也就是現在最流行的現線上廣告，因此小吳在享受雲端服務便利的同時，也必須忍受很多廣告頁面的干擾，甚至雲端服務業者還針對小吳的信件或使用內容置入相關連的廣告，這種現象是雲端時代與過去套裝軟體和作業系統時代，以及早期網路時代相當大的差異。

各家業者能這麼精確掌握小吳的使用資訊，首先就是使用語意網(Semantic Web)[122]等資訊技術來解讀分析小吳的電子郵件、用Google Docs編寫的文件或Facebook上的內容。我們以Facebook提供的雲端服務為例，除了臉書以社群網站的名義，很高竿的讓小吳等使用者去編寫自己喜愛的

[122] Wikipdeia definition of semantic web: http://en.wikipedia.org/wiki/Semantic_Web (last visited 2011.07.08)

音樂、書籍、電影、運動和休閒愛好等項目外，也藉由掃瞄小吳塗鴉牆和網誌中的關鍵字，來作為分析、比對及整合小吳的完整資訊。此外Facebook更厲害的是還把「讚」鈕作為廣告編輯欄位，當作精準行銷的工具[123]。小吳只要在塗鴉牆、網誌、各種喜好，乃至工作地點、學經歷、居住處所按下了「讚」，Facebook就可以知道這些相關訊息是小吳感興趣的，那麼這就有了商業廣告的價值。當小吳對「5566」的專輯按下了讚，那麼「183」的CD就有向小吳廣告的價值，當小吳對偶像劇「命中注定我愛你」按下了讚，「犀利人妻」的周邊商品廣告就可能會是精準行銷。尤有甚者，除了Facebook平台上的「讚」外，連平台外的網站也可以加入使用「讚」的行列，再加上等下要提到的cookie技術，可以更加精確的定位每個使用者的習性，那麼千千萬萬的Facebook使用者將無所遁形。雖然在雲端運算發展前的網路世代中，網路服務業者就已在掃瞄使用者的檔案，但雲端服務的發展更會讓使用者大量的資訊集中到業者的伺服器上，將使得雲端業者掃瞄與拼湊使用者資訊的情形更加嚴重。

除了分析使用者傳到雲上的資料外，另一個雲端或網路服務業者常用來蒐集使用者資訊的方式就是使用cookie技術。所謂的cookie，是種從網站或雲端伺服器傳送到使用者瀏覽器上而保存在硬碟中具有識別功能的少量檔案，以便在連線時伺服器隨時可以掌握使用者的資訊[124]。舉例來說，當小吳使用Yahoo mail時，cookie會記錄下小吳的使用者名稱(login name)、密碼、利用Yahoo搜尋及瀏覽網頁的內容，以及小吳的網路使用習慣[125]。因此當小吳享受雲端服務的同時，cookie就會將記錄下來的資訊回傳給雲端業者，再加上原本小吳上傳的資料，分析比對之後，就能讓小吳在第一

[123] Will M, *Facebook Ads: "Keywords" Will Change to "Likes and Interests" This Week*, All Facebook, March 7, 2010, http://www.allFacebook.com/Facebook-ads-keywords-will-change-to-likes-and-interests-this-week-2010-03 (last visited 2011.07.08)
[124] Wikipdeia definition of HTTP Cookie: http://en.wikipedia.org/wiki/Cookie_(web) (last visited 2011.07.08)
[125] *Id.*

章中看到鞋子和乳液的網頁內容時就會出現相關的廣告，達到雲端業者和廣告廠商「入戶入腦」的精準商品行銷目的。這種論調當然不是我們在危言聳聽，Wall Street Journal就曾報導一名叫做Ashley Hayes-Beaty的女士，她的 26 歲年齡、田納西州那什維爾的地址及包括公主新娘(The Princess Bride)、我的失憶女友(50 First Dates)、慾望城市(Sex and City)等許多喜歡的電影或影集，都被紀錄在「4c812db292272995e5416a323e79bd37」這串cookie碼當中[126]，而被做為廣告行銷的對象。

然而cookie除了儲存個人資訊外，也被用來紀錄個人在網路上的使用行為，例如記錄使用者在網路及雲端上的動作或是曾經進行過哪些線上購物。所以當小吳上Yahoo拍賣中心網購海苔時所填寫的姓名和地址等個人資訊，就會被cookie紀錄下來，在下次小吳使用這個服務時，cookie就會自動提供小吳的資訊給Yahoo的雲端伺服器。cookie除了會記錄下姓名和地址等個人資訊外，在使用雲端服務時也具有認證的作用，例如確認使用者的位址、儲存和維護登錄名稱及密碼、管理使用者的帳戶，或者確認使用者的瀏覽器狀況等[127]。

Cookie能夠記錄下使用者這麼多的資料，將可能造成資訊安全的重大漏洞，因此會引起關心資安人士的質疑。所以為了平息大眾對於cookie技術的疑慮，有些業者開始從瀏覽器著手，設計一些隱私權的選項，例如Google Chrome、Microsoft Internet Explorer、Konqueror、Mozilla Firefox、Opera和AppleSafari等，都加上了調整或禁用cookie的選項。雖然瀏覽器加上這些措施看似好像能夠阻絕有心人士從cookie來接受使用者的資訊，但是現在的追蹤技術早就不是僅僅調整瀏覽器cookie的隱私設定就能夠高枕無憂，有些技術甚至能夠即時掃瞄使用者的一舉一動，而且變的更不易察

[126] Julia Angwin, *supra* note 37.
[127] Paul Lanois, *supra* note 38, at 31.

覺，更侵入使用者的使用私領域[128]。前面Wall Street Journal的這份調查就指出，美國前 50 大網站及雲端服務就在沒有知會及警告使用者的情況下安裝了 64 種的掃瞄記錄工具，而且這些掃瞄工具或追蹤軟體大多是無法經由調整瀏覽器cookie設定來予以防護個人資訊的洩漏[129]。這些雲端或網路業者不僅在持續蒐集使用者的個人資訊，更恐怖的是業者還利用資訊技術拼湊出使用者的輪廓(user profiles)，甚至這些資訊還有交易市場可供買賣或交換[130]。雖然cookie技術早在Internet萌芽時就已開始發展，但就如我們前面所言，雲端業者須要在免費提供使用者服務時進行商業廣告的獲利模式，因此利用cookie等各種技術手段蒐集使用者資訊，對於雲端業者而言就更形重要。無怪乎Wall Street Journal在這份報告中下了各驚悚的結論，現在網路商業模式中發展最快速的就是蒐集、監視和追蹤使用者的資訊[131]。

對於雲端或網路業者對使用者個人資訊隱私侵害的亂象，其實美國法制在特定項目上對個人資訊的隱私安全及資訊流通方面，還是訂有應該遵守的規範，我們也將在下章中更進一步討論這些規範。但是總體而言美國法上仍缺乏對個資保護、流通、揭露及商業廣告用途的整體規範。雖然美國仍舊有許多人士致力於推動雲端和網路方面個人資訊隱私保護的相關立法，但是雲端網路業者一直宣稱隱私權法案將對網路產業帶來巨大衝擊，會對美國正在成長的線上廣告產業造成經濟上的負面效應，使得相關法案的推動受到龐大阻力，美國國會也因此一直未能取得共識[132]。

雖然美國國會的立法過程一直都不順遂，但仍就有許多使用者在局部的訴訟上取得成果，例如 2010 年 3 月北加州地院就通過著名的Facebook

[128] *Id*.
[129] Julia Angwin, *supra* note 37.
[130] *Id*.
[131] *Id*.
[132] Declan McCullagh, *Tech Firms Warn Privacy Bill Will Harm Economy*, CNET NEWS, July 23, 2010, http://news.cnet.com/8301-31921_3-20011435-281.html. (last visited 2011.07.08)

Beacon和解案[133]。所謂的Beacon(網路信標，或稱網路臭蟲)常是以1像素大小的GIF或PNG圖片形式放在網頁或電子郵件中，可以用來蒐集使用者資訊，並可將蒐集到的資訊寫入cookie內[134]。Facebook在 2007 年推出的Facebook Beacon廣告計畫，就是利用類似的技術，讓使用者在與Facebook有合作關係的雲端平台或購物網站上使用服務或進行下單後，會有彈出式視窗詢問使用者是否要在Facebook上分享自己購物的訊息[135]。也就是說Facebook，利用Beacon技術追蹤了使用者在網路上的行為，然後將這些訊息寫入Facebook的cookie並回傳至Facebook，接著Facebook就把使用者購買什麼商品或使用了哪些服務，廣播給使用者在Facebook上的好友，如此一來就變成使用者自動推薦商品服務給好友的運作模式，讓使用者對好友們變成該商品服務的代言人[136]。

這種社群網路的廣告模式其實是相當高明的商業點子，而且如果就Facebook這種社群網站的本質來看，推薦商品服務給好友們可能無可厚非，但有問題的卻是Facebook是在使用者不知情的情況下，將購買採用哪些商品服務廣播給大家知道[137]，這就已經是踩在使用者隱私權的邊界上了。當然Facebook也的確是有提供選項介面讓使用者在購物後，選擇是否把購物訊息讓好友們知道，不過造成爭議的卻是Facebook把這個選擇介面弄得非常不易察覺，當使用者在消費後，Facebook會有各藏在角落的對話框詢問使用者是否要廣播，要是使用者沒有在10秒內回答，Facebook就預設把這個訊息廣播出去，而且使用者每次購物或享受服務時都要進行這樣的選擇，

[133] Lane v. Facebook, Inc., No. C 08-3845 RS, 2010 U.S. Dist. LEXIS 24762 (N.D. Cal. March 17, 2010).
[134] Wikipdeia definition of web beacon: http://en.wikipedia.org/wiki/Web_beacon. (last visited 2011.07.08)
[135] Pete Cashmore, *RIP Facebook Beacon*, Mashable, September 19, 2009, http://mashable.com/2009/09/19/Facebook-beacon-rip/. (last visited 2011.07.08)
[136] *Id.*
[137] Ellen Nakashima, *Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy*, Washington Post, November 30, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503.html. (last visited 2011.07.08)

Facebook並沒有提供任何設定讓使用者可以調整預設為不要廣播[138]。這種使用者介面的操作方式稱為opt-out，也就是使用者必須自己選擇退出，否則就會被系統自動納入廣告框架中[139]。Facebook這種狡猾又高明的作法，讓很多人的隱私就這樣被廣播出去，甚至有很多使用者根本不知道還有拒絕廣播的選項。Facebook在 2007 年推出Beacon計畫後，立刻遭到如Moveon.org等隱私保護團體和人士的批評[140]。而且Beacon推出時剛好在耶誕假期的前夕，在這個節日季節(holiday season)時刻，許多人都在購買禮物準備送給親朋好友，據說Beacon計畫剛好幫很多人宣傳了他們準備了什麼禮物，掃了大家拆禮物的興致。

這也告訴我們，有時使用者會非常不願意透露在網路或雲端上的行為。在Beacon這個例子中，不單是使用者會非常不願意透露給好友買了些什麼東西，也不僅是購買物品或享受服務本身的問題，而是在於人與人之間的互動本來就不可能會是毫無理由的透明，甚至是需要點空間或距離。所以雲端上的個人資料需要保護，使用者在雲端或網路上的行為也不能無所限制的掃瞄或揭露。像這種送禮的情況，並非使用者要隱藏什麼見不得人的事情，而是要保留驚喜給好友們。人際間的交往本來就是複雜而又難以預料，這種內在心靈活動的完整不受侵犯，正是隱私權所要保護的重要內涵[141]。尤其在資訊網路時代中，人們愈來愈依賴網路及雲端平台來進行各種人際交往的活動，也因此這些個人資訊有其保護的必要，不可任意進行散佈流通。所以不論Facebook Beacon計畫是以商業廣告觀點出發，或者是要更加強社群網路的互動性，都缺少這種複雜心靈活動的呈現，而變得更

[138] June Carlos Perez, *Facebook's Beacon More Intrusive Than Previously Thought*, PCWorld, December 1, 2007, http://www.pcworld.com/article/140182/Facebooks_beacon_more_intrusive_than_previously_thought.html (last visited 2011.07.08)

[139] 與 opt-out 相對的概念就是 opt-in，意即使用者必須自己選擇跳進廣告系統的框架中，否則即預設是在系統外。

[140] Lane v. Facebook, Inc., *supra* note 129.

[141] 陳起行，資訊隱私權法理探討—以美國法為中心，政大法學評論，64 期，2000 年 12 月，頁 299。

加危險和使人難堪，這也正是我們一直強調的放在雲上的資料與在網路上進行的行為就無法再受使用者控制，也是雲端時代對個人資訊保護最大的衝擊[142]。所幸在經過一年多的團體訴訟後，Facebook承認Beacon計畫的失敗，並且願意捐出 950 萬美金成立各專門提倡網路隱私和資訊安全的基金會[143,144]。

Facebook的和解案鼓舞了許多關心雲端網路資訊隱私的人士，紛紛開始對使用不當掃瞄技術而侵害隱私的業者提出告訴。例如 2010 年 7 月，美國中加州地院就受理一起團體訴訟[145]，原告起訴的對象是知名的線上廣告業者Quantcast，還有背後許多巨大的廣告贊助商諸如ESPN、MTV、MySpace、Hulu、ABC和NBC等，原告宣稱Quantcast在這些廣告網頁中的Adobe Flash[146]裡加入了cookie檔案來追蹤使用者，這種Flash cookie不僅不能夠像藉由調整瀏覽器隱私權設定刪除HTTP cookie的方式來刪除，甚至還能加上重建(re-spawn)技術來回覆被使用者刪除的HTTP cookie檔[147]。另一起團體訴訟在 2010 年 8 月同樣繫屬在加州法院[148]，被告是Quantcast在線上廣告業界的老對手Clearspring，Clearspring被起訴說利用介面工具「AddThis」來進行線上監測，這種工具在未告知使用者的情況下安裝在使用者所瀏覽的網站，當使用者瀏覽該網站時AddThis會安裝各標籤在使用者的電腦上，這不僅能追蹤使用者的瀏覽記錄，還能夠建立cookie檔，而這些安裝有AddThis的網站也涵蓋許多知名網站，例如Disney、Playlist、

142 李治安，同註 33，頁 54。

143 David Kravets, *Judge Approves $9.5 Million Facebook Beacon Accord*, WIRED, March 17, 2010, http://www.wired.com/threatlevel/2010/03/Facebook-beacon-2/ (last visited 2011.07.08)

144 Beacon 計畫雖然失敗，但是像 Facebook 這樣的業者仍然需要依賴線上廣告來維持營運，因此也促成之後 Facebook Connect 的成功。Facebook Connect 仍保有 Beacon 的主要概念，但是採用 opt-in 的方式來使隱私權控制更為明顯和清楚，而且也提供一般使用者可以利用的廣告工具，而非僅付費的企業或用戶才能使用，使得應用範圍更加廣泛。

145 Edward Valdez v. Quancast Corp., No. CV10-5484 (C.D. Cal. July 23, 2010).

146 Wikipdeia definition of web adobe flash: http://en.wikipedia.org/wiki/Adobe_Flash (last visited 2011.07.08)

147 Ryan Singel, *Privacy Lawsuit Targets Net Giants over 'Zombie' Cookies*, WIRED, July 27, 2010, http://www.wired.com/threatlevel/2010/07/zombie-cookies-lawsuit/ (last visited 2011.07.08)

148 White v. Clearspring Techs. Inc., No. CV10-5948 (C.D. Cal. August 10, 2010).

Ustream、SodaHead和Warner Brothers Records，也連帶成為該案的被告[149]。另外一間著名線上廣告Specific Media，也同樣因為Flash cookie檔追蹤使用情況的問題而成為另案的被告[150]。

加州大學柏克萊分校有份調查報告的結論與前面Wall Street Journal的結果類似，發現在前百大著名網站中有 54 個網站暗中藉由Adobe Flash cookie來收集使用者資訊，而其中只有 4 個網站告知使用者此事[151]。Flash cookie有別於傳統瀏覽器的cookie，不僅防不慎防，甚至使用者都沒辦法藉由調整瀏覽器的隱私權設定來避開業者的監測，柏克萊分校的報告甚至發現還有更惡劣的業者是採用雙重方式，同時安置HTTP cookie和Flash cookie到使用者電腦，當使用者以為已經刪除了HTTP cookie檔後，再用Flash cookie來回復並追蹤使用者的現況[152]。其中Quantcast和Clearspring又是這份報告中最惡名昭彰的兩間公司，難怪受到關心資安人士的批評與控訴[153]。

當使用者在享受雲端服務或瀏覽網頁時，除了cookie檔讓使用者有揮之不去的陰影外，使用者在使用搜尋引擎或上網時，也會讓像Google或Yahoo等雲端業者獲得使用者的網路搜尋碼(Web Search Query)以及統一資源定位符號(Uniform/Universal Resource Locater, URL)。網路搜尋碼是使用者為了滿足搜索需求而對搜尋引擎下達的檢索字句[154]，統一資源定位符號則是網際網路上標準的資源位址，實際上也就是網路位址[155]。這兩樣資訊看似好像不會洩漏使用者的資訊，但實則Google和Yahoo會記錄這兩樣資

[149] Dean Takahashi, *Lawsuit Alleges Major Web Sites Spied on users via AddThis Tool*, Venture Beat, August 14, 2010, http://venturebeat.com/2010/08/14/lawsuit-alleges-major-web-sites-spied-on-users-via-addthis-tool/ (last visited 2011.07.08)
[150] La Court v. Specific Media Inc., No. CV10-01256 (C.D. Cal. August 18, 2010).
[151] Ashkan Soltani et al., *Flash Cookies and Privacy*, (August 10, 2009) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862. (last visited 2011.07.08)
[152] *Id.*
[153] *Id.*
[154] Wikipdeia definition of web search query: http://en.wikipedia.org/wiki/Web_search_query. (last visited 2011.07.08)
[155] Wikipdeia definition of URL: http://en.wikipedia.org/wiki/URL. (last visited 2011.07.08)

訊，來和使用者的IP位置交叉比對，藉以確認使用者的身份。此外Google和Yahoo也會記錄下使用者搜尋後所點選的網站連結而成為一種商業資訊，供Google和Yahoo的廣告贊助商作為行銷參考。Google當時的隱私權政策甚至明白告訴使用者會比照類似的網站服務，記錄下使用者的檢索資訊、所在的IP位址、瀏覽器種類、檢索語言、檢索語句、時間和其他cookie會記錄下來的資訊[156]。

我們在第一章時就已經提到，雲端服務提供者或網頁業者常是「免費」來提供使用者使用服務，只不過免費的代價是我們要忍受瀏覽器頁面不斷出現的廣告。而這些廣告很多又是和我們的個人資訊息息相關，業者就是透過cookie或Beacon技術，以及紀錄Web Search Query和URL，來刺探追蹤我們的資訊。那如果只是雲端業者將我們的個人資訊作為商業廣告的參考，可能有些人會覺得還可以忍受，但是雲端業者收集到的個人資訊，或者是使用者利用服務而特別存放在雲上的資料，卻極有可能成為被國家搜索的對象。那麼到底雲端業者面對政府的要求或法院的強制令是交還是不交，以Google為例在Gonzales v. Google案[157]中，Google很強硬的以保護使用者隱私權的理由，拒絕了美國政府依據兒童網路保護法(Childrens Online Protection Act)賦予政府監督業者的權責[158]對Google作出交出數千條使用者的Web Search Queries和URLs的要求[159]，但是我們又可以看到Google在面對中國政府時如何立場反覆又軟弱無力[160]。

所以對於掌握在雲端業者手上的使用者資料，到底是要拿來作為商業廣告用途，或者屈服於各國政府的各種法令行政要求，就取決於雲端業者的立場和所持的隱私權政策。此外從第一章開始我們一直提到的使用者除

---

156 Jayni Foley, *Are Google Searches Private? An Originalist Interpretation of The Fourth Amendment In Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 450 (2007).
157 Gonzales v. Google, Inc., 234 F.R.D. 674, 679 (D. Cal. 2006).
158 47 U.S.C. §231(a)(1).
159 Gonzales v. Google, Inc., *supra* note 157.
160 Wikipdeia definition of Google China: http://en.wikipedia.org/wiki/Google_China. (last visited 2011.07.08); *Lara Farrar, Google.cn: R.I.P. or Good Riddance*?, CNN, March, 26, 2010, http://edition.cnn.com/2010/TECH/03/26/china.google.reaction/index.html. (last visited 2011.07.08)

了擔心資訊受到刺探外，還要擔憂雲端系統的穩定性，或者系統是否存在安全性的漏洞，而當資料因這些原因遺失、喪失或洩漏時，責任的歸屬或者問題該如何處理，也取決於雲端業者的政策與服務條款的規定。以Google這幾年的隱私權政策為例，雖已經明確宣示會以偵測cookie檔或用其他科技方式蒐集使用者的資料，不過在未經使用者同意下不會隨便將資料移轉給他人。

但是使用者是否能就此高枕無憂，其實也是大有疑問的，不然電子隱私資訊中心(Electronic Privacy Information Center, EPIC)也不會在2009年致函美國聯邦貿易委員會(Federal Trade Commission, FTC)，質疑Google提供的雲端服務存有許多安全性疑慮，要求FTC調查並禁止Google提供大眾此類有資料洩漏與隱私侵害疑慮的服務[161]，這些服務範圍包括Gmail, Google Docs, Google Desktop, Picasa Web Albums and Google Calender，涵蓋Google許多主要的服務項目[162]。雖然Google宣稱在例如使用Google Docs的服務時，除非使用者自行散佈資料或與人分享，否則Google能確保該資料的安全性及隱私權保障[163]，但Google對於可能的隱私和安全性疏失所造成的損害，卻拒絕擔保及承擔責任[164]，與EPIC及使用大眾的期待相距甚遠。雖然Google在隱私權保護政策上宣示會經過使用者的同意才揭露資訊，但是EPIC還是舉出許多Google未經同意就予以揭露的情況，而且EPIC也發現Google的許多雲端服務存在安全性漏洞，例如Gmail的安全性問題，就能讓有心人士有機會盜用使用者的名稱和密碼[165]。

此外在雲端運算時代，各種雲端網站服務或線上遊戲為了招來人氣，很流行利用各大入口網站如Google、Yahoo、MSN、Facebook或Twitter，甚至巴哈姆特、遊戲基地或Garena競舞台的帳號來作為登入使用，當使用者

161 EPIC, *supra* note 41.
162 *Id.*
163 Google Docs, http://docs.google.com (last visited 2010.11.23)
164 EPIC, *supra* note 41.
165 *Id.*

連上網頁時，該網站會連結至使用者的入口網站伺服器，要求使用者輸入相應的帳號密碼，再由該入口網站傳輸使用者的資訊封包回該網頁。EPIC在這份指控中就宣稱，Google對於使用者資訊流的處理充滿漏洞且相當草率，會讓某些惡意網站利用這些漏洞接觸使用者的資訊，甚至完全掌控使用者整各網路行為[166]。EPIC甚至認為Google連基本的安全措施都沒執行，有時連編碼加密都沒有，只是簡單用各txt檔作成cookie就把使用者的資訊傳遞出去，EPIC嚴厲指控這種行為，是種不誠實的商業和詐騙行為[167]。

[166] *Id.*
[167] *Id.*

第四章　雲端資訊流通的法令與國際規範

在前一章中我們討論了到各種雲端時代中，使用者會面臨到雲端業者所帶來的資訊安全和隱私權的風險，這種情形讓雲端使用者的個人資料和進行的網路行為會被這些雲端業者不斷地蒐集，甚至是散佈給第三人或政府，而對使用者造成更大的危害。在前面的討論中我們也提到了，這些個人資訊的危害讓許多使用者或隱私保護團體起而對抗這些雲端業者，利用訴訟及社會輿論的壓力，迫使業者必須作出個人資訊及隱私保護的宣示，讓這些雲端隱私資訊會如何被應用，或者被「揭露」的範圍如何，要讓業者在隱私權政策及服務條款中進行說明。當然基於法理及商業倫理，提供服務的雲端業者本來就應該要負有保護這些個人資訊的義務，而成為保障個人資料的責任主體。此外除了雲端業者該有的保護義務外，雲端服務使用者利用雲端服務來儲存運算的資料，也可能是其他第三人(資訊主體或資訊當事人)的資訊，這也使得雲端使用者也可能同時成為負有保護義務的責任主體。比如說利用醫療雲的醫院使用服務來管理病歷資料，服務使用者是醫院或其醫護人員，但是在雲上流動的是病患的病歷資料，按照法律規定及醫療倫理的規範，醫院當然也對病歷資料負有保護個人資訊的責任。因此在雲端平台上，提供服務的業者固然藉由隱私權政策來揭示個人資訊保護的方式與流程，服務使用者同樣也要注意該隱私權政策是否也能確保同樣為責任主體的保護義務。

那麼在雲端時代，對於資訊的流通、儲存與運算，何人該為責任主體，責任的內容如何，各國在既有的個人資訊保護規範中訂有許多相關規定，可作為雲端業者在制訂隱私權政策與使用條款時的參考規範。本章中我們將討論美國法和各國際組織的相關規範，探討雲端時代中雲端業者，甚至是服務使用者對個人資訊的保護責任，並且作為第五章我們討論雲端服務

的隱私權政策和服務條款的基礎，以及第六章我國法制下雲端法律議題探討時的參考。

第一節　美國法制中對個人資訊保護的相關規定

美國法制中對於資訊的共享或者特定類型商業服務的資料儲存，並無總則性的法律規範，而是根據資訊內容和資訊主體的型態，以及蒐集處理資訊業者的類別來分別立法[168]，此外尚有許多州針對隱私權保護亦有諸多規定。這些法令雖然大多制訂在雲端運算時代之前，但同樣是針對資訊的處理、流通與傳遞，因此這些法令規範於雲端運算時代同樣有其適用。因此雲端業者在制訂涉及此類服務的隱私權政策與服務條款，或使用者在選擇服務時，皆應當注意美國法上的相關規定。

1. 醫療保險流通與責任法(Health Insurance Portability and Accountability Act, HIPAA)[169]

對於健康醫療資訊是否揭露、揭露的程序為何或如何保護個人健康隱私，最重要的聯邦隱私權法規就是 1996 年制訂的 HIPAA，其立法目的在於規範「擁有」病歷或健康資料的機構或組織，例如醫院、診所、醫護人員或健康照顧等醫療照護單位，必須保障當事人的隱私，原則上不得將可以識別個人健康資訊的資料向第三人揭露。

如若這些醫療照護組織或人員，委外處理部分業務或使用醫療系統軟體服務，或者是使用現在很流行的醫療雲服務，這些提供服務的第三

[168] 張乃文，雲端運算產業發展之策略規劃與法制因應，科技法律透析，2010 年 12 月，頁 31；陳起行，同註 141，頁 328。

[169] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-91, Aug. 21, 1996, 110 State. 1936.

方業者都很可能因此取得健康資料，同樣必須受到HIPAA的規範。HIPAA也要求該醫療單位和服務業者間的商業關連協定(business associate agreement)[170]，需要確立服務業者可以使用資訊的範圍，並且當該協定內容與HIPAA規範相抵觸時，醫療單位與服務業者將會面臨違法風險[171]。此外根據HIPAA的規範，除非是基於行政管理需求或為使醫療單位進行健康照護的資料蒐集，提供服務的業者等第三方人員均不能進一步使用或揭露資訊，這也意謂著建構醫療雲的業者當然不能進行蒐集、掃瞄或整合這些資訊來作為廣告商業用途[172]。雲端業者違反該協定內容時，HIPAA賦予醫療單位隨時終止契約的權利。美國健康與福祉部門(U.S. Department of Health and Human Services)針對HIPAA所擬定的「受託者契約條款範本」，作為醫療單位和這些第三方業者間契約的準則，同樣也適用於提供醫療雲端服務的業者[173]。

另外在某些特別的法案，例如酒精藥物濫用病歷記錄機密規範(Confidentiality of Alcohol and Drug Abuse Patient Records Regulation)[174]，甚至要求採用委外資訊服務的醫療院所，無論是否對相關健康資料進行編碼加密，均不得將該資料傳送給服務提供者，因此雲端業者提供該類服務時也同樣必須注意相關規定，或者建構私有雲的系統來作因應。

2. 經濟與臨床健康科技資訊法(Health Information Technology for Economic and Clinical Health Act, HITECH)

HITECH為2009年美國經濟復甦暨再投資法(America Recovery and

[170] 45 C.F.R §164.502(e), §164.504(e)
[171] Lisa J. Sotto et al., *Privacy and Data Security Risks in Cloud Computing*, 15 ECLR 186, 187 (2010).
[172] Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM, 8 (2009).
[173]「Sample Business Associate Contract Provisions」, Publisher in FR 67 NO. 157 pg.53182, 5326, August 14, 2002; Robert Gellman, *supra* note 172, at 8.
[174] 42 C.F.R. Part2.

Reinvestment Act, ARRA)之部分內容，該法案將原本規定「擁有」健康資訊或病歷資料的機構或組織因洩漏相關資料需要負擔的通知責任，擴及至「接觸、維護、保留、修改、紀錄、儲存、消除，或以其他任何形式持有、使用或揭露安全性不足之健康資訊」的機構或組織也必須因為洩漏相關資料而負有通知該資料當事人(資訊主體)的責任，其範圍將涵蓋藥劑給付管理公司、代理人及保險業者等。這些機構或組織原本與醫療院所或病患間係依據契約關係進行責任規範，但被納入HIPAA的責任主體範圍後，則需依此負擔民、刑事責任[175]。

至於建構健康醫療雲端服務的業者，同樣會「接觸、維護、保留、修改、紀錄、儲存、消除」這些資料，因此也會被認定是HITECH的責任主體，必須注意到因為洩漏資訊而負有的通知義務[176]。HITECH亦規定相關資料洩漏時，必須在知悉外洩事件後 60 天內以適當方式(例如書面、電話或網站公告等方式)通知當事人[177]。此外HITECH中規定應通知的範圍僅限於洩漏「安全性不足之健康資訊」，因此HITECH另規定由美國健康與福祉部門(Secretary of Health and Human Services)制定「個人健康資訊外洩通知責任實施綱領」[178]，定義所謂的「安全」資料係指「無法為第三人使用或辨識」的資料來建構可供防護的安全港條款，因此只要對資料加上適當的加密措施而即使外洩亦無法為他人辨識，或者收回銷毀外洩資訊之儲存媒介(如書面或電子形式)而使他人無法再辨識內容，均屬安全資料範圍。雲端業者在建構相關醫療雲服務時，同樣必須注意對相關資料施以適當的安全措施。

3. 金融服務現代法(Gramm-Leach-Bliley Act, GLBA)[179]

[175] U.S.C. §13402(a).
[176] Lisa J. Sotto, et al., *supra* note 171, at 187.
[177] U.S.C. §13402(d)(1).
[178] U.S.C. §13401(c).
[179] Gramm-Leach-Bliley Act of 1999, Pub. L. 106-102, Nov. 12, 1999, 113 State. 1338.

就金融業者處理客戶資訊而言，1999 年柯林頓政府通過的金融服務現代法中關於金融資訊的流通訂有相關規範。GLBA中有隱私與安全兩大準則(Privacy and Safeguards Rule)，主要規定金融機構對於客戶隱私與其非公開資料負有保密與安全的義務 [180]，並要求金融機必須構建立適當的安全措施來確保客戶個人資料的隱密性，防止可能破壞資料安全性與完整性的攻擊或威脅，以及避免未經授權的資料存取而傷害客戶權益 [181]。

此外GLBA也就金融機構將客戶資訊處理委外處理或使用金融軟體服務，作出了嚴格的規範，禁止取得客戶資料的如雲端業者等第三方人員進行與該金融業者無關業務外的資料利用或另外的揭露傳輸行為 [182]。而且在GLBA的安全準則下，該金融業者在委外或選用金融軟體服務時，必須盡到善良管理人義務，確保所選定的服務提供者有能力進行適當的安全措施(例如對該業者進行事前安全措施的查核)，並須以契約形式載明安全機制的成效、風險責任、資料安全性與機密性等細節事項，且金融機構尚須對服務業者盡到妥善管理、監督履行安全措施的責任。聯邦金融機構檢查會(Federal Financial Institutions Examination Council, FFIEC)就在 2000 年時按照GLBA的授權規定，針對金融機構委外或使用服務訂定管理規範 [183]，作為金融機構和服務業者的參考標準 [184]。雖然 1999 年的GLBA制訂時業界並未有雲端運算的服務，但現在的金融雲端業者一樣是在處理與流通金融資訊，同樣必須遵守GLBA的規範及聯邦金融機構檢查會的相關規定。

[180] 15 U.S.C. §6805(a).
[181] 15 U.S.C. §6801(b).
[182] Lisa J. Sotto et al., *supra* note 171, at 187.
[183] Risk Management of Outsourced Technology Service, November 28, 2000.
[184] Francoise Gilbert, *Cloud Service Contracts May Be Fluffy: Selected Legal Issues to Consider Before Taking off*, 14 NO. 6 J. INTERNET L. 18, 22 (2010).

4. 租片隱私保護法(Video Privacy Protection Act)[185]

1988 年通過的租片隱私保護法對於客戶承租影片的紀錄，有著類似 GLBA 的規定。租片業者在將客戶租片記錄委外處理時，必需盡到善良管理人的注意義務，確保並且持續監督選用的委外服務業者能夠確實保護客戶的租片資訊。此外該法案亦規定，委外提供服務的業者除了在原有服務目的下，不得將客戶的租片資訊另做其他用途與散佈傳播。同樣與 GLBA 相同，租片隱私保護法在雲端時代亦有其適用，因此雲端業者在建構該類服務時，必須遵守相關規定，注意對於取得的客戶承租紀錄除了在原有服務目的下，不得另做其他商業廣告用途或散佈傳播。

5. 纜線傳播政策法(Cable Communications Policy Act)[186]

1984 年制訂的纜線傳播政策法對於有線電視訂戶的訂閱資料，同樣有著類似GLBA及租片隱私保護法的規定。除委外處理客戶訂閱資料外，有線電視業者禁止向非相關第三人散播訂閱資料[187]，而且要藉由訂閱記錄來蒐集個人資料，還必須取得當事人的同意[188]。同樣與租片隱私保護法相同，雲端時代的服務提供者亦有該法的適用，因此雲端業者同樣在建構該類服務時，必須注意對於取得的客戶訂閱紀錄除了在原有服務目的下，不得另做其他用途與散佈傳播[189]。

6. 申報稅務法令

稅務顧問(tax preparer)處理納稅義務人稅務問題時，對於納稅人申報記錄負有保護及隱私保障責任，美國國內稅務準則(U.S. Internal

[185] Video Privacy Protection Act of 1988, Pub. L. 100-618, Nov. 5, 1988, 102 State. 3195.
[186] Cable Communications Policy Act of 1984, Pub. L. 98-549, Oct. 30, 1984, 98 State. 2779.
[187] 47 U.S.C. §551(c)(1).
[188] 47 U.S.C. §551(b)(1).
[189] Robert Gellman, *supra* note 172, at 8.

Revenue Service Rules)[190]訂有許多相關的規範。例如稅務顧問向同事務所的其他顧問揭露納稅人的申報資料是被允許的[191]，稅務顧問向事務所的員工因指示工作而揭露的行為也是合法的[192]，但如果是向美國國外的稅務顧問揭露則需要得到納稅人的同意[193]，此外無論是否得到納稅人同意，均不得向國外的納稅顧問揭露納稅人的社會安全碼(Social Security Number)[194]。所以當稅務顧問要使用雲端服務處理稅務資料，或雲端業者要架構類似的服務時，必需要注意到該準則的相關規範或雲端伺服器是否位在國外等跨境傳輸的相關問題[195]。

7. 反對婦女暴力法(Violence Against Women Act)

2005 年新修訂的反對婦女暴力法，規定除了在得被害人同意、法律規範或法院命令外，不得揭露任何被害人的相關資訊[196]。因此許多社福團體、NGO組織或新聞媒體，對於這些被害人資訊是否要上雲端儲存，應該要注意其相關規範。

8. 兒童網路隱私保護法(Children's Online Privacy Protection Act, COPPA)[197]

1998 年制訂的兒童網路隱私保護法，其旨在保護兒童免於網路犯罪的危害或誘惑，以及協助父母管教兒童遠離不適當的網路內容[198]。COPPA也針對網路上以商業目的蒐集未成年人資訊的行為做出規範，因此只要是涉及到兒童使用或教學授課等網路或雲端服務，均會受其規

[190] 26 U.S.C. §§6713, 7216; 26 C.F.R. §301.7216.
[191] 26 C.F.R. §301.7216-2(c)(2).
[192] 26 C.F.R. §301.7216-2(d)(2).
[193] 26 C.F.R. §301.7216-2(c)(3).
[194] 26 C.F.R. §301.7216-3(b)(4).
[195] Robert Gellman, *supra* note 172, at 9.
[196] 42 U.S.C. §13925(b).
[197] Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, div. C, title XIII, Oct. 21, 1998, 112 State. 2681-728.
[198] 15 U.S.C. §6501-6555.

範。

COPPA最主要規範了13歲以下兒童的資料蒐集必須經過兒童父母的同意後方得為之，而這些資料包括兒童的姓名、地址、電子郵件、電話號碼或社會安全碼,以及其他會連結到兒童及其父母身份的資料[199]，COPPA當然也賦予父母拒絕儲存或使用兒童資訊的權利[200]。而且按照COPPA的規定，網站或網路服務業者在向父母要求同意的說明中，必須列出哪些資料被蒐集，被蒐集的資料形式為何，以及這些資料的用途和流向為何。COPPA也要求業者必須採用合理的安全措施與程序，來保護兒童個人資訊的隱私和安全性,以及避免兒童資訊遭到掃瞄、追蹤、拼湊與整合。違反相關規範者，COPPA亦訂有處罰規定[201]。COPPA制訂之初即是針對網路上的兒童資訊保護,因此依賴網路維繫的雲端運算服務同樣也有該法的適用。

9. 個人資訊的特許保護(Legally Privileged Information)及職業秘密義務

有些特殊的個人資訊是享有法律上的特許保護,例如醫師取得的病患資料、律師取得的客戶訴訟資料或牧師對於信徒的告解等，在法律上僅允許取得資訊但卻不得洩漏與他人[202]。這些因職業上知悉他人的個人資訊或隱私，而享有法律上的特許保護，可以對抗政府、法院或其他機關要求揭露的要求。但是當這些資訊取得者將這些資訊移轉給第三人

199 15 U.S.C. §6501.

200 *Id.*

201 例如2008年FTC就針對Sony BMG Music未取得父母同意而蒐集13歲以下兒童資訊開罰1百萬美金。Sony Music旗下擁有眾多歌手與藝人，其中包括許多深受兒童和青少年喜愛的藝人，但是該公司為旗下歌手及發行唱片設立的網站，要求使用者需提交個人資料才能登入網站，Sony BMG即藉此蒐集了至少3萬筆兒童的個人資料，而且多數未取得其父母同意。Sony BMG 的這些網站有些甚至讓兒童自己建立歌迷網頁，讓他們可瀏覽藝人相簿，並上傳影片、照片，張貼留言，同時也讓兒童直接與該社交網路中的成人互動。Sony Music的行為明顯違反COPPA的相關規定，FTC即對此開罰，並要求該公司刪除所有違反COPPA的個人資料，同時要Sony BMG在未來5年都必須在網站裡加入各種宣導FTC相關規定的說明與連結。資料參考：Elizabeth Montalbano, *Sony BMG to Pay $1M to FTC for COPPA Violation*, COMPUTERWORD, December 11, 2008, available at http://www.computerworld.com/s/article/9123219/Sony_BMG_to_pay_1M_to_FTC_for_COPPA_violations. (last visited 2011.07.08)

202 Robert Gellman, *supra* note 172, at 10.

時，就會破壞法律上的特許保護，例如記者將採訪資料用Google Docs等雲端服務來整理彙整時，就破壞了該記者對資料的特許保護，可能喪失面對政府和法院的拒絕證言權[203]。當然如果對這類特許保護資料持有者提供諸如電子郵件、文書處理或資訊管理等雲端服務，而該雲端業者能夠承諾並確實履行僅就資料提供儲存或運算等服務，應該尚不至於構成特許保護的破壞[204]。但如若雲端業者閱讀、揭露或另外移轉該類資訊，甚至利用這些資訊內容來做廣告時，則將使特許保護的抗辯失效[205]。因此這類人士或特殊資料在使用雲端服務時，均須特別注意雲端業者的隱私政策與服務條款，是否可避免客戶與自身權益受損及會否產生保密義務的相衝突[206]。

美國各州對於這類情況常有不同的規定，例如以律師使用電子郵件等雲端服務為例，美國律師公會(American Bar Association, ABA)就對是否使用加密郵件來與當事人聯絡不作限制[207]，紐約州律師公會甚至認為以資訊技術掃瞄電子郵件來作為廣告依據並無不可，只要是雲端業者和收到廣告人士不知該信件內容即可[208]。但新澤西州、內華達州、緬因州和佛羅里達等州則規定律師處理此類信件必須採取合理的保護措施，並且確保信件內容不能外洩[209]。因此雲端業者和律師在各州提供雲端服務或執業時，必須明瞭當地相關的資訊隱私保護規範。

10. 各州資訊安全規定

美國許多州特別針對商業行為要求企業建構合理的安全措施，而訂

---

[203] *Id*.
[204] *Id*.
[205] *Id*.
[206] Shellie Stephens, *Going Google: Your Practice, the Cloud, and the ABA Commission on Ethics 20/20*, U. ILL. J.L. TECH. & POL'Y 237, 239 (2011).
[207] ABA, STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY, FORMAL OP. 99-413 (1999).
[208] NEW YORK STATE BAR ASS'N, COMM. ON PROF'L ETHICS, OP. 820 (2008).
[209] Lisa J. Sotto, et al., *supra* note 171, at 188.

有許多個人資訊安全的法令與標準，包括阿肯色州、加州、康乃迪克州、馬里蘭州、內華達州、俄勒岡州、羅得島，德州和猶他州等[210]。以加州為例，就要求企業在將個人資訊流通給非相關的第三人時，必須先與原資訊主體以契約形式約定會確實盡到合理安全保護措施的責任，所以雲端業者在加州提供服務時，同樣也必須對個人資料進行合理的安全防護[211]。另外如麻薩諸塞州甚至要求持有麻州居民資料者，必須安置實施資訊保護措施，並且例如企業在將員工或顧客資料移轉至雲端上時，必須盡到確實查核該雲端服務的安全措施是否適當的義務，且需以契約要求雲端業者採取適當的保護個人資料的安全措施[212]。

11. 小結

就如本節我們一開始所言，上述這些美國法上針對個人資訊保護的立法例多是雲端時代來臨前就以存在的法律，但是在雲端時代中仍具有規範效力。此外從這些立法制度，我們可以觀察到兩個面象[213]，首先是擴大資料保護的責任主體，將原本的資料擁有者(可能是原始的資料主體，或如醫院或金融機關等雲端服務使用者)應有的資訊保護責任，擴展至因提供服務而可能接觸、儲存、運算或流通該資料的委外服務業者[214]，因此保護資料的責任不會因為資料移轉而有所降低或消失。就如同我們前面所討論的，這種擴大資料保護責任主體的法令規範在雲端時代同樣有其適用性，但是雲端業者所提供的網路資源與服務內容相較這些法令立法時的技術背景是更加的多元與具有彈性，對於雲上資料如何流通、儲存、處理或運用，使用服務的資料擁有者往往無法掌握整個資訊流的每個部分，雲端系統的安全性也並非這些使用者可以完全控制，

[210] Lisa J. Sotto, et al., *supra* note 171, at 188.
[211] *Id.*
[212] *Id.*
[213] 張乃文，同註 168，頁 33。
[214] *Id.*

因此加諸雲端使用者過多的保護責任可能不是適當的作法，下節中我們將提到的歐盟規範即對此作出了調整。

美國這些法律規範除了區分上述的責任主體外，美國國會也進行衡平資訊擁有者保護責任的立法動作，最主要的就是要求資料擁有者必須進行事前委外作業時的風險或安全評估，美國政府部門也回應國會的立法意旨，針對某些特殊資訊的委外處理訂立許多安全標準。例如前面所討論到的美國健康與人類服務部依據HITECH的規定，在 2009 年公布「個人健康資訊外洩通知責任實施綱領」，採用國家標準與技術研究院（National Institute of Standards and Technology）公布之Special Publication 800-11 及聯邦資訊處理標準 140-2 作為健康資訊或病歷資料處理時的安全規範，因此醫療機構採用委外資訊服務或醫療雲服務時，如能夠確保服務提供的業者採納此種安全標準，即可認定該醫療機構已進行了適當的安全及風險評估。除了安全標準外，美國的立法例也會要求資訊擁有者或服務使用者要利用契約(甚至是契約範本)規範保護責任的範圍，對於委外或採用雲端服務時如何處理、流通或揭露資訊的範圍、目的及最重要的全保護措施，亦須明訂於契約之中[215]。委外服務提供者或雲端服務業者則須按這些使用者的評估要求及契約內容，來履行資料保護的責任。資訊擁有者或服務使用者踐行這些事項後，才能主張已盡相關法規的管理注意義務，如若再發生資料洩漏或危害時，也才能聲明責任應由服務提供者來負擔。因此藉由賦予資訊擁有者或服務使用者的這些責任，美國法上以此來衡平與解決使用者與服務提供者間的責任問題，這也可說是種對資訊主體保護責任的落實與權責劃分。

[215] 張乃文，同註 168，頁 33。

第二節　個人資訊資保護的國際規範

針對個人資料的保護，國際間有多各國際組織訂有相關規範，並對前開所述美國法上的個資保護規定多所影響。這些規範同樣在雲端時代仍有適用，因此不論是提供雲端服務的業者或是使用者，均須注意這些國際組織訂定的相關規範。

第一項　經濟合作暨發展組織（Organization for Economic Co-operation and Development, OECD）

OECD 於 1980 年 10 月通過的「個人隱私資料保護基準」（Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）[216]，作為該組織會員國的立法參考。這份保護基準不僅成為許多國家個資保護的立法基礎，也成為日後多個國際區域組織相關法制的藍圖。我們觀察這份保護基準，可以歸納出八項原則[217]：

1. 限制蒐集原則(Collection Limitation Principle)：進行個人資料的蒐集時應有限制，並符合公正及合法之手段，且於適當之情形，應通知資 料主體及取得其同意。亦即關於個人資料之蒐集，其蒐集對象應有界限，蒐集方法亦應有所限制。
2. 資料內容完整、正確原則(Data Quality Principle)：進行個人資料的蒐集時，蒐集內容須與使用目的具有關連性。並且在合乎原來蒐集目的下，

[216] *See* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. (last visited 2011.07.08)

[217] *Id.*；行政院經建會委託研究報告，資訊服務業者配合政府公權力提供客戶資料之法制研究，計畫共同主持人潘維大、余啟民，2006 年 12 月，頁 17-18。

進行必要及適當之資料蒐集。

3. 資料利用目的明確化原則(Purpose Specification Principle)：個人資料的蒐集目的，至遲於進行蒐集時必須明確，其後目的如若變更亦應明確化，且對於資料的利用，不得與該蒐集目的有所衝突。意即蒐集目的必須明確，且利用資料時應受該目的之限制。
4. 限制利用原則(Use Limitation Principle):除非經過資料主體之同意或依據法律規定，否則所蒐集之資料不應進行蒐集目的以外之應用。簡言之，應於蒐集目的範圍內進行資料的應用。
5. 安全保護原則(Security Safeguards Principle):對於個人資料可能的漏失；不當接觸、破壞、利用、修改、開示等危險，必須以合理的安全措施予以保護。例如進行組織管理及密碼化等安全措施。
6. 公開原則(Openness Principle)：進行個人資料之蒐集時應採公開原則，例如對於資料管理人之特定、資料貯存場所之決定，資料內容與性質、及其主要利用目的等，應以公開方式確定；這種公開方式及政策，並應先以法律明定之。
7. 個人參加原則(Individual Participation Principle)：個人於關於自己之資料，得向資料管理者或其他人確認是否持有關於自己之資料。並且在合理期間內，可以適當之費用及合理之方法，藉本身容易了解之情形，來進行瞭解。對於前開權利之行使，如遭受拒絕時，得對其拒絕理由提出異議；且於異議成立時，得要求資料之消除、修改、完全及補充。
8. 責任原則(Accountability Principle)：資料之管理人，應負責任，遵守上述諸原則，並採取各種措施，使上述原則能發揮實際效果。

第二項　歐盟個人資訊保護相關規範

在歐洲方面，其個人資料保護的立法基礎主要源於 1950 年的歐洲人權保護公約(European Convention for the Protection of Human Rights and Fundamental Freedoms；ECHR)[218]中的第 8 條，該公約闡述人民之私生活及家庭生活應予尊重，公部門必須在有法律授權，或基於國家安全、經濟福祉等公益考量之必要情況下，方得干涉人民之上述權利。

歐洲人權保護公約的意旨，在 1981 年歐洲理事會（Council of Europe）所提出的「自動化處理個人資料之保護協定」(Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data)[219]中獲得重申，並對歐洲理事會的成員產生一定的法效力。該份協定與OECD個人隱私資料保護基準的架構內容相當相似[220]，同樣規範應提供資訊主體獲得告知其資料之蒐集、取得及必要時更正之權利、以及可拒絕某種蒐集資料之方式；同時，亦規範資料保存者應有良好之資料管理措施、及要求蒐集資料之組織或個人應承擔相對義務與責任，而且同樣規範使用資料僅限特定、明確及合法之目的，並須保證資料不致濫用及禁止未獲授權者能取得資料，以及在進行資料蒐集活動應先行通知監理機構等義務。

雖然歐洲理事會成員國基於該份保護協定紛紛制訂相應之國內法，但是由於該協定未對一些重要名詞作具體定義，導致各國在國內法的適用上產生解釋不一的現象，進而造成規範標準的不一致，因此該協定對個資保護的效果實屬有限[221]。為了彌補此一錯誤，歐洲議會(European Parliament)

---

[218] *See* European Convention for the Protection of Human Rights and Fundamental Freedoms, *available at* http://www.eurofound.europa.eu/areas/industrialrelations/dictionary/definitions/europeanconventionfortheprotectionofhumanrightsandfundamentalfreedoms.htm (last visited 2011.07.08)

[219] *See* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (last visited 2011.07.08)

[220] 曾德宜，借鑑歐盟作法，強化我國個人資料保護規範與措施，Taiwan News 財經，文化週刊，2004 年 11 月。

[221] 周慧蓮，英國個人資料保護最新案例發展及其對我國法制之啟示，資策會科技法律中心科技

在 1995 年通過「歐盟個人資料保護指令」[222]，希望能夠調和各國國內法規，使得歐盟內之公民能得到相同保護。該份保護指令並要求其會員國須於 1998 年 10 月 24 日前完成相關立法，並於該年起正式於歐盟境內實施。

歐盟的這份保護指令，首先定義個人資料的處理(processing of personal data)，係指無論是否用自動化方式而對個人資料進行以傳輸、散佈或其他使用、整合、組合、阻斷、消去或破壞為目的的蒐集、紀錄、組織、適應、轉換、回覆或揭露等動作。從個人資料處理的定義出發，該指令進一步區分「資料控制者」(controller)係指在個資處理流程中，單獨或與他人共同決定資料處理「目的」與「方式」的自然人、法人或公務機關，以及「資料處理者」(processor)係指代表資料控制者在受指示或授權範圍內進行資料處理的自然人、法人或公務機關，如若資料處理者超出受指示範圍處理時，則就超出部分應視為資料控制者。歐盟個人資料保護指令中大部分的規範，即圍繞在資料控制者的保護責任上。

但是進入資訊時代後，尤其是在雲端運算時代中，對於資訊流的傳輸及處理顯得更加的複雜與多元。以本文我們的主角小吳為例，小吳利用Gmail收發郵件來與客戶溝通聯絡，利用Google Docs編寫公司會議的報告檔案，利用Facebook來與好友們互動，沒有人會否認小吳使用這些雲端服務不是帶有通訊、工作或交誼的目的，小吳也是基於這些目的來使用這些服務，這其間小吳也不斷經手自己、公司、客戶或其他人的資料至雲端上。但是整個過程中小吳只知道電子郵件已經發出，或只知道報告檔案已經編寫完畢，實際上這些資訊檔案如何被處理，如何被流通儲存，甚至有無被掃瞄分析，小吳其實根本無從掌握，所以小吳能否被視為「資料控制者」

法律透析，2005 年 1 月。

[222] 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 processing of personal data and on the free movement of such data, Official Journal of the European Communities of 23 November 1995 No. L. 281, p. 31. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited 2011.07.08)

其實是有爭議的。反面言之，雲端業者所提供的Gmail、Google Docs或Facebook等服務，它的功能、效能和處理流程其實是早已被設計規劃好的，只是等待使用者來上門享受，嚴格說來這些雲端業者也並非單純的資料處理者。由此我們可觀察到，歐盟個人資料保護指令中對於資料控制者與處理者的定義，及其衍生的保護責任是會產生爭議的[223]。

有鑑於此，歐盟執委會(European Commission)下的個資保護小組(EU Article 29 Working Party)[224]，為使上述爭議得以釐清而作出了說明[225]。該小組認為原本歐盟個人資料保護指令中對於原有的「資料控制者」與「資料處理者」的定義依然可行，但面臨實際狀況時，應採取功能性的分析方式來就資料處理的「目的」與「方式」予以區分。該份說明也舉例提出雲端運算所面臨的兩個問題，一為雲端使用者無法確知資料現在何處進行運算或儲存，二為雲端業者未經授權接觸資料。至於如何區分資料的控制者與處理者，歐盟個資保護小組認為要回到認識資料處理者是否實際認識「目的」與「方式」來作處理。

就如同本章我們一開始所言，雲端服務業者除了提供服務外，還會藉由隱私政策與服務條款來規範與使用者間的法律關係。以小吳使用雲端服務為例，小吳應該透過這些政策與條款來瞭解這些服務的目的及運作方式，例如如何進行傳輸及儲存、是否進行編碼或密碼化、是否進行關鍵字掃瞄分析、是否回傳分析 cookie 檔或是否進行線上廣告等，這些小吳應當瞭解的項目中，小吳既已知悉就當然成為資料控制者而負有保護義務。例如小吳明知該雲端服務對於資訊流會進行掃瞄並作為廣告依據，故當造成客戶困擾時小吳就應負責，不會因為小吳使用或委由雲端服務而阻卻責任。再者按照保護指令與該說明，此時反而會認為小吳既已知悉該目的與方式而

[223] 張乃文，同註 168，頁 29-31。
[224] 該小組是根據歐盟個人資料保護指令第 29 條所設立的工作小組。
[225] Opinion 1/20, adopted on 16 February 2010, reference number 00264/EN/WP 169, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf (last visited 2011.07.08)

使用服務，雲端業者即會被視為資料的處理者。反之，如若雲端業者超出這些政策或條款等小吳應有的認知時，例如在未知會小吳的情況下利用 Beacon 等技術蒐集到客戶資訊進而造成客戶損害，小吳當然不知 Beacon 的目的與施用方式，此時雲端業者即成為資料控制者，小吳不負歐盟規範下資料控制者的責任。

因此在現今的歐盟個人隱私安全架構下，資料控制者或處理者應就資料流程各個環節的「目的」與「方式」的認知或決策來予以區分，而雲端業者的隱私政策與服務條款將會是這些「目的」與「方式」是否認知或決策的關鍵，所以雲端使用者必須注意這些政策與條款。甚至如此都還無法免除法律上責任，使用者還須要進行事前風險評估及事後管理監督。所以像我們的主角小吳，如果使用比較廣泛而隱私政策與使用條款保護程度比較低的 Gmail 來與客戶聯絡，在歐盟架構下是會充滿許多風險，不如使用經過公司建置管理且安全性相對較高的 MailASP 來的保險。

歐盟除了針對資料控制者和處理者作出不同定義和規範外，安全指令的主要內容還包括一般條款、資料處理方面、資料當事人權利、資料保護的相關義務與責任及監督機制[226]。說明如下：

1. 一般條款：係就立法目的、保護客體、適用主體及名詞定義等加以說明。
   (1) 立法目的方面，安全指令明白揭櫫係為保障自然人之基本權與自由，建立最低隱私保護標準，調和各會員國間關於隱私保護立法之分歧，一方面保障會員國境內之個人資訊隱私權，一方面防止他人假隱私保護之名妨害資料流通。
   (2) 保護客體則及於以自動化及非自動化方式處理之個人資料，但對於以非自動化方式處理之資料的保護設有一定要件之限制。
   (3) 安全指令的適用主體兼及於公、私部門。

[226] 行政院研考會委託研究報告，政府機關強化個人資料保護措施之研究計畫主持人林桓副，協同主持人余啟民，2009 年 10 月，頁 9-10。

2. 資料處理方面：

(1) 資料品質原則[227]：資料之蒐集與處理必須公平及合法，且符合特定及合法之目的，而該目的必須自始明確，並禁止不合目的之資料利用。對於資料的處理必須適當、適切及不過當地逾越資料儲存之目的，且確保資料內容的正確，並應以該資料所有人所允許之形式保存，並可於必要時進行更新。

(2) 敏感資料處理原則[228]：原則上禁止對有關種族、血緣、宗教、政治意向、哲學信仰、工會活動、健康及性生活之個人資料進行處理，保護指令另外也舉出可以例外進行資料處理的條款。

(3) 資料處理之正當性原則[229]：個人資料必須於特定條件下使得合法地被處理，諸如得資料當事人之同意、為履行契約之需要、為履行法定義務、為保護個人之重大利益、為維護公益、為資料保管人或為第三人合法權益之所需等。

3. 資料當事人權利：即資訊主體對於被蒐集或處理之資訊所具備之權利，包括當事人的受告知權[230]、查詢請求權[231]、確定及凍結資料權[232]、異議權[233]及拒絕自動化處理權[234]。

4. 資料保護的相關義務與責任：包括規範資料保密[235]、安全義務[236]、登記義務[237]及損害賠償責任[238]。

5. 監督機制：安全保護指令要求各會員國成立專責主管機關，賦予其檢查、調查、監管、參加訴訟等權限。

---

227 Directive 95/46/EC Article 6.
228 Directive 95/46/EC Article 8.
229 Directive 95/46/EC Article 7.
230 Directive 95/46/EC Article 10 and 11.
231 Directive 95/46/EC Article12.
232 Directive 95/46/EC Article 12(b) and 12(c).
233 Directive 95/46/EC Article14.
234 Directive 95/46/EC Article15.
235 Directive 95/46/EC Article16.
236 Directive 95/46/EC Article17.
237 Directive 95/46/EC Article18 to Article 21.
238 Directive 95/46/EC Article 23.

為了針對雲端時代對於資訊處理與隱私保護的快速變遷，歐盟下設的歐盟網路與資訊安全署(European and Information Security Agency, ENISA)提出了雲端運算對於資訊安全的效益、風險和建議(Cloud Computing Benefits, Risks and Recommendations for Information Security)報告[239]，參照歐盟安全指令的原則，這份報告建議雲端使用者應該注意雲端業者所提供服務的目的、安全性、資訊管理流程、雲端網路架構、資訊的範圍及處理程序、與業者間的權利義務及資訊的回復、刪除與終結等相關問題[240]。

第三項　亞太經濟合作會議(Asian-Pacific Economic Cooperation, APEC)

亞太經濟合作會議的電子商務指導小組（APEC Electronic Commerce Steering Group）於 2003 年初成立個人資料隱私權保護分組（Data Privacy Sub-Group），研擬制訂APEC隱私權保護原則（APEC Privacy Principles）[241]以供亞太區域內之企業、消費大眾、法律協會以及保護隱私權的專家做參考，並希望藉此能在大力推動電子商務的同時，也建立起消費者的信任與信心。該隱私權保護分組完成APEC隱私權保護原則草案之擬定，並於 2004 年 11 月間經APEC部長級會議通過，成為APEC各會員國有關個人資料保護之最高指導綱領。值得注意的是我國同時也為APEC之成員國，因此在我國進行之雲端活動同樣也要受該保護原則的規範。APEC隱私權保護原則共有九大原則[242]：

---

[239] European and Information Security Agency, Cloud Computing Benefits, Risks and Recommendations for Information Security 5 (2009), *available* at http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (last visited 2011.07.08)

[240] Timothy D. Martin, *Hey! You! Get Off My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security and Property in Cloud Computing*, 92 J. PAT. & TRADEMARK OFF. SOC'Y 283, 311 (2010).

[241] APEC Privacy Principles, http://www.pmc.gov.au/privacy/apec/meetings.cfm (last visited 2011.07.08)

[242] 行政院研考會委託研究報告，同註 226，頁 7-8。

1. 避免損害原則：有關個人資料之蒐集、處理與利用，不得損害當事人之權益。
2. 告知原則：對個人資料進行蒐集時，應告知當事人蒐集者名稱、蒐集資料之目的、種類與用途等必要事項。
3. 限制蒐集原則：個人資料的蒐集應符合蒐集之目的，且不得逾越必要之範圍，與目的無關之資料，不得任意蒐集。
4. 利用個人資料原則:有關個人資料之利用,應符合當初進行蒐集之目的,未經當事人同意或另有法律規定，該資料不得作其他利用。
5. 當事人選擇原則：有關個人資料之蒐集或利用，當事人有權得選擇「進入」(opt-in)或「退出」(opt-out)模式，資料蒐集者或保有者應尊重當事人之選擇。
6. 個人資料完整原則:保有個人資料檔案者,有責任隨時更新或補充資料,力求該資料之完整正確，避免當事人因不正確之資料，讓其權益遭受損害。
7. 安全維護原則：保有資料者應採取必要之安全維護措施，避免個人資料被偷竊、遺失、毀損或外洩。
8. 當事人查詢及更正原則：當事人隨時有權查詢或閱覽其個人資料，如發現有錯誤或欠缺者，得請求補充或更正。
9. 責任原則：對於違法蒐集或利用個人資料者，應課以法律責任，以保護資料當事人之權益。

第四項 小結

觀察這些個人資訊隱私保護的國際規範，大抵都是參酌 OECD 的規範，

注重個人資料的蒐集目的明確性及正當性、資料利用合理性、及安全保護措施及資訊主體的權利等，由此可見國際間注意個資保護的潮流。雲端運算藉由動態資源的調整，流通與處理使用者的資料，當然也要遵守這些國際規範，這其中又以歐盟安全指令與 APEC 隱私權保護原則最為重要。歐盟作為全球四大經濟體之一，其法制政策的重要性不言可喻，而其安全指令的立法精神、目的與內容也影響全球多數國家及各區域組織的相關立法，此外歐盟執委會亦持續進行個資保護的檢討，不斷提出新的解釋函令以因應全球資訊化的發展，歐盟甚至也針對雲端議題不斷提出報告。APEC 隱私權保護原則同樣也受到歐盟安全指令的影響，我國為 APEC 之會員，故有遵守 APEC 保護原則之必要。我們也將在下章討論雲端隱私政策與服務條款時，探討如何落實這些國際規範。

第三節　跨境傳輸與國際規範

我們在第一章曾經提到Facebook上相當受歡迎的音樂視頻軟體Animoto，在開放的前三天裡，使用人數從 2 萬 5 千人激增到 25 萬人，該網站所用的伺服器在這三天中從 5 個擴充為 3 千 5 百個，能夠在這麼短的時間內完成擴充，就是利用了雲端運算的便利性[243]。而雲端業者能夠在短時間達成任務，想必也是早就建置好了大量的雲端伺服器，以供應各種商業上的需求。根據美國INTAC公司的調查，Google目前擁有 100 多萬台的伺服器居於全球之冠，其他各大雲端網路服務業者也各有數萬台的規模[244]。這麼大量的伺服器機組需要龐大的電力供應，以Google為數百萬台伺服器

[243] Animoto's Facebook Scale-up, *supra* note 18.
[244] INTAC, Who Owns the Most Servers?, Aprial 13, 2010, *available at* http://www.intac.net/a-comparison-of-dedicated-servers-by-company_2010-04-13/ (last visited 2011.07.08)

為例，全部運轉時每小時需要使用五百兆瓦特的電力，相當於半個舊金山市區的電力消耗[245]。因此雲端業者為了節省電力成本，勢必有誘因將伺服器中心移往電費便宜或有政策優惠的國家或區域，如此一來將造成資料的流動和伺服器位置不同而產生雲端運算跨境傳輸的問題[246]。此外雲端運算的特性之一就是能夠迅速動態地調整與釋放雲端資源，實際操作時就會因系統調整而在不同伺服器上移轉使用者的資訊，如若當這些伺服器位在不同國家或區域時，亦同樣會發生雲端資訊的跨境傳輸問題。

雲端資料跨境傳輸之所以會成為問題，原因在於雲端伺服器所在國家或區域對於個人資料的相關法令不盡相同，而且涉及到不同管轄權競合的問題[247]。就算雲端業者事先公告說伺服器所在的位置，但是雲端的特性之一就是資源的彈性動態調整，而且實際上使用者的資訊可能會被儲存在多個國家或地區的伺服器，因此將造成掌握資料儲存處所的困難，雲端業者也不大可能因為資源動態調整就隨時通知使用者。

歐盟資訊安全指令就針對雲端資料跨境傳輸法律上的權利義務提出一個規範模式。在該指令的第 4 條規定只要在歐盟區域內處理他人資訊者，就會受到該國的法令規範，而如果是在歐盟區域內處理了非歐盟國家的使用者個人資料，同樣要受到歐盟法令的規範，因此只要個人資料適用到歐盟規範，那就會永遠都適用，而且會對該筆資料是否可以流通至第三國產生限制。至於雲端運算服務，當然也會受到歐盟規範的影響[248]。例如一間美國公司使用伺服器位在法國的雲端服務時，那麼該筆資料就會受到法國法律的保護，對於該資料是否能夠回傳至美國將會產生許多限制，甚至法國法律上對資料接觸、遺失或修正的通知義務也將一併產生規範效力。因此站在雲端業者的角度而言，一旦個人資料「沾惹」上某個歐盟會員國的

[245] 黃亦筠，同註 25，頁 8。
[246] Paul T. Jaeger et al., *supra* note 7, at 271.
[247] Konstantinos K. Stylianou, *An Evolutionary of Study of Cloud Computing Services Privacy Terms*, 27 JMARJCIL 593, 598 (2010).
[248] Robert Gellman, *supra* note 172, at 19.

保護法令時，就沒辦法使資料在該國或歐盟的管轄範圍內脫離法律的保護[249]。

此外根據歐盟資訊安全指令的規範[250]，歐盟會員國只能在歐洲經濟區域內之國家(European Economic Area, EEA)[251]流通個人資訊，或其他受到歐盟執委會認可且採取適當資訊保護措施的非歐洲經濟區(non-EEA)之國家[252]。例如美國商務部便與歐盟執委會簽訂安全港協議[253]，符合安全港協議的美國雲端業者即可接收與流通自EEA的個人資訊，而為了符合該份安全港協議，美國的業者必須採取以下措施：(1)建構符合安全港協議的保護機制；(2)制訂符合安全港協議的隱私政策與條款；(3)遵守有關隱私保護的法律規範。此外安全港協議也訂有與歐盟保護指令內容類似的通知、選擇、移轉、安全、資料完整和執行等原則，並對資料的收集、儲存、二次傳輸及使用作出了規範[254]。

如若傳輸之目的地非歐盟經濟區域或非歐盟執委會認可之國家，在符合下列情況時，僅需在跨境傳輸前通知資料主體或資料當事人，而無須取得歐盟執委會的同意[255]：(1)為履行與資料主體間之契約內容，或因應資料主體需求，為準備締約所採取的必要措施；(2)資料控制者為資料主體利益而與他人契約中必要之行為； (3) 為公眾利益或法律規範；(4)為保護資料主體重要利益之必要行為；(5)該資料係依法提供大眾或開放公眾閱覽，或其他證明有法律上利益者。

除這些情形之外，要進行跨境傳輸必須取得歐盟執委會的授權。而要取得授權，必須先採取充分的個人資訊保護措施，還要在與資訊接受方

---

[249] *Id*.
[250] Directive 95/46/EC Article 25and 26.
[251] EEA 包含全體歐盟成員國，及挪威、冰島、列支敦士登。
[252] 這些國家包含安道爾共和國、阿根廷、澳洲、加拿大、瑞士、法羅群島、澤西、根西島、馬恩島嶼美國。*See* http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm (last visited 2011.07.08)
[253] *See* http://www.export.gov/safeharbor/. (last visited 2011.07.08)
[254] *Id.*
[255] Directive 95/46/EC Article 26(1).

(data importer)的契約中要求建置必要的保護措施。歐盟還為此訂定契約範本[256]，作為與取得歐盟執委會授權時的依據。此外為了因應全球化下資訊處理與新型商業模式的快速發展，資訊處理委外或再委外的情形頻繁，歐盟於 2010 年修正此契約範本[257]；要求跨境傳輸而接受到資訊的接受方，在委外訂約處理資訊時，必須先通知並取得資料控制者的同意，而且資訊接受方僅能在與資料控制者間的契約內容所允許範圍內委外處理資訊，且與委外者間的契約還要供資料控制者備查。

APEC也參考歐盟的經驗，在2007年1月通過跨境隱私保護規則(Cross Border Privacy Rules, CBPR)[258]，建立蒐集或處理資訊的業者於跨境傳輸個人資料時應遵循的規則，並且將重點放在建立及規範APEC各組織成員國間跨境傳輸的合約或備忘錄範本，以及對參與跨境傳輸個人資料的業者進行隱私保護的認證機制[259]。我國為APEC之成員國，不論雲端業者是將雲端伺服器建立在我國境內，亦或將雲端資訊流經我國區域，均會受到APEC相關跨境傳輸規定的規範，因此雲端業者與使用者均須注意相關的規範。

第四節　本章小結

在本章中我們討論到了美國法上如何針對個人資訊隱私進行保護，以及歐盟等各區域組織的資訊安全規範，並且提到了美國商務部和歐盟之間

[256] Commission Decision (2002/16/EC) of 27 December 2001 under the Directive 95/46/EC. *See* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0016:EN:NOT. (last visited 2011.07.08)

[257] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. *See* http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/ip_10_130_en.pdf. (last visited 2011.07.08)

[258] APEC Data Privacy Subgropu Meeting, *APEC Corporation Arrangement for Cross-Border Privacy Enforcement*, Febryary, 28, 2010. *available* at http://www.ftc.gov/os/2010/02/1002apecprivacyenforce..pdf. (last visited 2011.07.08)

[259] *Id*.

簽署的安全港協議。如果我們繼續探究這份安全港協議，會發現除了美國雲端業者基於商業考量想要打入歐洲市場外，另一項更重要的因素在於美國與歐盟間對於資訊隱私的保護規範有很大的差異，而這份差異來自於美國與歐盟對於資訊隱私保護的範圍不同[260]。雖然美國針對金融、醫療及兒童等不同領域的個人資料訂有類似或甚至比歐盟安全指令嚴格的保護規範，例如資訊蒐集應用合目的性、資訊揭露得當事人同意等，但是就如同前面我們所言缺乏整體的隱私保護總則[261,262]。這也意謂著除了這些特殊的個人資料外，雲端使用者的其他資料保護將不足夠，而不像歐盟安全指令對使用者的所有個人資料均有適用。因此美國商務部必須與歐盟簽訂此份安全港協議，提醒美國的業者必須注意美國與歐盟之間隱私保護規範的差異。從這些美國及歐盟的法律規範，以及兩個法體制間的對話磨合，我們可以從中發現對於雲端業者來說，雲端服務的發展有全球化的趨勢，因此這些業者在對不同地區或國家的使用者提供服務時必須注意各自的法令規定，此時各區域組織的公約或規範就將扮演相當重要的角色。對雲端服務的使用者而言，除了達到使用服務的目的外，最重要的是要保障自身的資訊安全，各國的法令乃至於這些國際規範，都可以作為選用雲端服務或者權利救濟的重要依據。

[260] James Sunosky, *Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles*, 9 CURRENTS INT'L TRADE L.J. 80, 88 (2000).
[261] 張乃文，同註 168，頁 31。
[262] 這也是前面提及的在美國國會立法受挫的隱私保護法案。

第五章　雲端運算的隱私權政策與服務條款

現今資訊技術快速發展，各種新型態的商業模式不斷推陳出新，對個人資訊隱私安全將產生重大衝擊，致使個人資訊隱私的保護愈來愈受到重視。從前面我們所討論到的美國隱私保護立法例乃至歐盟的安全指令，都可以發現要透過網際網路提供各種電子商務服務的業者，必須要採取各種措施來跟上時代的潮流。雲端服務提供者通常是藉由隱私權政策(Privacy Policy)的宣示來表達如何保障使用者的資訊安全，並且藉由服務條款來規範與使用者間的法律關係。一般而言，雲端服務提供者會在契約或服務條款中表示參照隱私權政策來對使用者的資料進行保護，因此我們可以將隱私權政策也視為雲端契約或服務條款的一部份，而且也是相當重要的一部份。本章我們即針對雲端隱私政策與服務條款進行討論。

第一節　雲端隱私權政策

雲端服務提供者的隱私權政策(Privacy Policy)，係指提供雲端服務的業者對於使用者的資料和隱私如何蒐集、分析、利用和保護的宣示，這會牽涉到諸如資訊隱私、安全性、匿名性、電信容量、政府監視、系統可靠性與責任等諸多項目。例如Google在 2007 年推出一系列的文件編輯或影音視頻等雲端服務，開始大量儲存使用者的資訊，希望將這些個人資訊導入商業廣告的用途，但這種商業模式也勢必會引起關心資安人士的憂心，Google亦從善如流聲明注意到這些雲端服務會有資訊安全的問題，因此透過隱私權政策的制訂來試圖平息外界的疑慮[263]。

[263] Kevin J. Delaney et al., *Google Plans Service to Store User's Data*, WALL ST. J., (2007). *available*

按照現在雲端服務使用的模式，一般使用者在享受原有的雲端服務時，必須忍受業者的各種廣告行為[264]，這些廣告行為又常會與使用者的資料內容密切相關，而且現今的雲端業者也大量依賴線上廣告提供的商機，因此雲端隱私政策可謂是使用者資訊隱私的保障與業者商業獲利間的平衡。這兩股力量牽拉制衡而互有消長，每當雲端業者採用新的技術或商業模式來偵知使用者資訊，並且廣告行為太過侵犯使用者的隱私權時，總會引起使用大眾的抗議，迫使雲端業者必須進行調整，Facebook由於使用者及隱私保護團體的抗議，決定取消Facebook Beacon計畫就是一例。另外對於雲端企業用戶而言，雖然是有償在使用雲端服務，原則上可以透過契約控制雲端業者來探知資訊與進行廣告的行為，但是這些企業用戶仍然必須透過隱私政策來明瞭服務提供者如何建立可供信賴的資訊安全保護機制。

第一項　雲端使用者希望獲得的保障

站在使用者的觀點，雲端運算使用者會在意雲端服務業者能否對以下兩大點作出保障[265]：

- ✧ 可靠度(reliability)與責任(liability)：我們在第二章就提過，使用者會希望雲端服務是種可靠度高的運算資源，這對企業用戶在進行商業活動時尤其重要，此外使用者也會要求釐清在重大事故發生時的責任問題。
- ✧ 安全性(security)、隱私(privacy)及匿名性(anonymity)：使用者會希望雲端資料和帳號密碼不會被未經授權的接觸或偵知，而機密性的資料尤其要確保隱私。使用者也不會希望在網路和雲端上進行的行為受到任

at http://online.wsj.com/article/SB119612660573504716.html (last visited 2011.07.08)

[264] Randal C. Picker, *supr*a note 8, at 6.

[265] Paul T. Jaeger et al., *supra* note 7, at 277-278.

意第三人、政府部門、甚至是雲端服務業者的監測，除非這些監測行為是原本就預計在雲端使用的目的範圍內。

這些使用者們的期望和心聲，其實也就是雲端業者在制訂隱私政策時需要考慮的事項，以下我們將分別進行討論：

1. 可靠度與責任

雲端服務的可靠度代表雲端資料不會損毀、喪失或程式停止運作的能力。而使用者為什麼會對雲端可靠度這麼在意，原因在於雲端運算的一項本質就是使用者資訊的移轉，移轉到雲上進行運算或儲存，移轉到雲端網路進行流通，那麼這些資訊的移轉必須不會產生風險，或者是風險是在可接受的範圍。2008 年 2 月時就發生Amazon的S3 雲端儲存服務中斷了 2 小時，造成許多企業用戶的業務活動被迫終止，並且得緊急在公司內部建立應急的伺服器措施，這讓許多採用Amazon S3 服務的公司意識到將企業重要資訊放在雲上除了安全上的疑慮，光是服務中斷的情況可能就難以承受[266]。而且這種大型雲端業者一發生伺服器當機或服務中斷的情形時，受影響的絕對不會僅是單一個人或用戶。3 年後，於 2011 年 4 月間Amazon又發生雲端伺服器機房大規模當機的事件，這次甚至連Amazon的招牌EC2 服務都中斷了 3 天才復原，影響美國上千個網站及無數的企業用戶[267]。

儘管近年來雲端技術的進步，讓服務品質提高，但服務失靈中斷的情況仍時有所聞。觀察這幾起雲端運算發生的意外，可以發現系統失靈的時間都不算太長，很快雲端服務就可以重新運作，因此除了服務中斷

[266] Thomas Claburn, *Amazon S3 Crash Raises Doubts Among Cloud Customers*, InformationWeek, July 21, 2008, http://www.informationweek.com/news/services/storage/showArticle.jhtml?articleID=209400122. (last visited 2011.07.08)

[267] Julianne Pepitone, *Amazon EC2 Outages Downs Reddit, Quora*, CNNMoney, April 22, 2011, http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm. (last visited 2011.07.08)

造成使用者直接的損失外，使用者另外還會擔心雲端資料會不會因為系統失靈而遺失或損壞，也就是雲端資料是否能保持「完整性」，例如 2011 年 3 月Gamil就發生系統上的失靈，導致 15 萬用戶的信件和通訊錄通通遺失[268]。除此之外，雲端資料經過運算處理後是否「正確」，也是雲端服務另一個可靠度的重點評估項目，例如採用金融雲的投信投顧業者，要是傳至雲上進行運算或儲存的數據資料產生錯誤，將可能造成客戶股票投資的損失。

儘管近年來雲端技術的進步，讓類似事件較少發生，但是也沒有任何一個業者敢 100%保證雲端系統不會再出現任何問題。那麼最重要的就是，雲端系統因為中斷或失靈的問題，需要由誰負責或承擔？是雲端使用者要自行承擔，要認為這是合理的商業經營風險嗎？畢竟就算使用者是自行架設主機伺服器、操作作業系統或套裝軟體，一樣也會有當機失效的情況發生。還是要認為這是雲端業者的責任？但是實際上也沒有哪個雲端業者願意在合約或使用條款中明確擔保服務的品質，甚至是對所有損失負賠償責任，要是雙方僵持不下的情況，可能必須考慮由保險業者等第三方來承擔損失填補的責任。保險實務上，國外就「資料保護保險」已行之多年，我國金管會也在 2010 年 9 月間核准該類型保單，可供未來雲端使用者分攤使用雲端服務時帶來的風險[269]。

2. 安全性、隱私及匿名性

使用者除了希望雲端服務的可靠度獲得保障外，其次要關心的就是服務安全性、雲端資訊隱私及匿名性的問題。雲端運算透過網路來流通資訊，對於使用者隱私和匿名性的保護一般而言不會高於使用個人電

[268] 陳炳宏，同註 121。
[269] 洪凱音，企業資料險 求償最高 2 億，經濟日報，2010 年 9 月 28 日。

腦[270]，因此要保護雲端使用者的隱私，必須從保護使用者資料與使用者在雲端網路上的行為著手，例如對於企業用戶而言，關心的是放在雲端上的客戶資料或財產明細；對於研究人員來說，擔心的是放在教育雲上的研究資料、實驗數據或者創新發明是否過早被揭露而影響其學術表現；另外一般雲端使用者在乎的則是個人機密資料是否流出。近年來我們幾乎每個人都親身經歷到許多電話或網路詐騙事件，有些詐騙手法純粹是恐嚇或嚇人的手段，不過更多的案件卻是讓人感覺到許多個人資料遭到了洩漏，例如最近很流行的MSN點數詐騙手法[271]就是如此。雲端時代標榜的資料上雲端，更有可能助長這些資訊外洩的危險。

我們在第二章提到雲端系統最大的特性就是能夠動態調整、分割或重新組合運算資源來提供各種服務，雲端業者藉此就能提供使用者相對便宜的服務價格。但這也意謂著每個使用者的資訊都可能會和他人共享在同一個伺服器或雲端基礎架構中，對於敏感的個人資訊(諸如身份證字號、個人識別記錄、醫療記錄或交易記錄等)將會是一大威脅。這種情形對於企業用戶而言將更加嚴重，例如對於使用金融雲的銀行業者，雲端業者要盡力避免銀行資料不會因為跟其他資料混雜而被植入病毒、破解或被偵測監看，可能寧可要喪失雲端服務的效能，也要對這些金融資料進行加密化[272]，甚至對這些金融用戶而言，有時利用雲端服務進出股市或操作外匯基金進行投資佈局的動作，反而比放在雲上的財產明細等金融資料更為重要。此外也有可能兩家互相競爭的企業用戶使用同

[270] 李治安，同註 33，頁 57。

[271] 筆者曾差點就是這種詐騙手法的受害人。筆者使用的 MSN 服務就曾經接到某個多年未曾聯絡的同學所傳的訊息，居然要求甚至拜託筆者代買 MyCard 的點數 6000 點，還很好心的告知每點要 1 元新台幣，筆者當下還覺得奇怪怎麼這位同學會有這樣的要求，不過轉念一想多年未見的友人哪有連哈拉都沒沒幾句，就一開口要幫買什麼 MyCard 點數，還一買就 6000 點。這就是時下很流行的 MSN 加上 MyCard 詐騙新手法，其實也就是筆者這位同學的 MSN 帳號密碼被盜了，連帶的 MSN 上的通訊錄，甚至 msn 信箱中的資料也遭到外洩。另參考：湯蕙如，資安/MSN 好友要你買 MyCard?小心，可能是騙局！，NOWnews，2010 年 11 月。

[272] Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government back Doors in the Web 2.0 ERA*, 8 J. TELECOMM. & HIGH TECH. L. 359, 374. (2010).

各雲端業者的服務，雲端業者必須非常小心處理雙方的資料，除了避免存放在同各伺服器中，也必須採用適當的防護措施，避免惡意或未經授權的接觸這些資料。因此雲端業者可能有必要為此建構專屬的私有雲系統，或是經濟效益與安全性較均衡的混合雲系統，企業用戶甚至要有再保險來攤平風險的規劃。現在的雲端業者也可能需要參考過去Wesabe和Mint金融網路服務的經驗，針對客戶的資料進行隱私封護(privacy seal)或敏感資料的機密保護 [273]。所以雲端業者要進行哪些保護措施或是提供保險建議，都有必要在隱私政策上進行說明。

除了雲端系統安全性的漏洞外，使用者另外還會在意雲端業者除了在服務目的外，是否還對使用者的資料進行了哪些動作。對一般的使用者而言，常是「免費」在使用雲端服務，其代價就是使用者的資訊和網路行為會被雲端業者以 Beacon、cookie、AddThis 或其他技術來掃瞄偵測，而被作為雲端線上廣告的目標。使用者享受 Google Docs 或 Gmail 等雲端服務，其目的不外乎利用這些網路資源來進行文書處理或收發信件，被動接收廣告絕非使用者的本意與目的，因此如若雲端業者不在隱私政策中說明如何蒐集資訊以進行廣告的機制，按照前節我們討論到的歐盟安全指令規範，雲端業者就會被視為是資訊控制者，而必須負擔相關資訊安全的責任。縱使雲端服務不會蒐集使用者資訊來作廣告，或者廣告的行為不會與使用者資料相關，雲端業者也有必要在隱私政策中加以說明。企業用戶雖然可以透過使用條款或契約來阻絕雲端業者的廣告，但是相對於一般使用者而言，企業用戶更在乎的則是涉及到商業機密的資料是否可能外洩，或者企業在雲端上進行的商業行為是否被隨意偵測，這些也是雲端業者在隱私政策中需要交代的事項。

此外，雲端運算涉及大量的資訊流通，因此在資訊流傳遞的過程中，有相當風險被其他第三人攔截和監測，而造成個人資訊的外洩，例如前

[273] Paul T. Jaeger et al., *supra* note 7, at 282.

面提到的MSN帳號，或個人、企業的機密資料、各種線上遊戲的帳戶密碼、各種工商資料等。因此，為了確保資料的安全性，雲端業者必須採取必要的防護措施，例如雲端業者要對使用者的帳號密碼採取匿名或加密措施的管制，甚至是從雲端基礎架構到使用者端都進行點對點網路(peer-to-peer networks)的匿名措施[274]，而且除了要對資料流向進行匿名措施外，也要對資料本身進行編碼的加密防護[275]。我們在本章第一節提到EPIC對當時Google的指控其中一項就是，Google僅使用簡便的txt檔來傳遞使用者資訊，而並未進行任何加密的措施。

雲端業者要對於雲端資訊進行加密或匿名措施，勢必比一般的資料處理需要更多的運算容量，這將增加業者伺服器處理能力及記憶體的成本[276]，因此雲端業者一定會對哪些使用者資料需要進行保護有所取捨。那麼是所有的雲端資料都要加上保護措施嗎？還是僅部分資料才享有安全措施的保障？這不僅取決於業者的經營策略外，更有賴於法律規定及區域組織規範的保障。就如同前章我們所討論到的，歐盟與美國之間就隱私保護的範圍不盡相同，使用者必須特別留意雲端業者是否會根據服務所在地區不同而有不同的保護。

雲端運算隱私安全的另一個問題就是雲端資料的再移轉問題，例如使用者採用A業者的服務，並且明瞭A業者的隱私政策與各種保護機制，A業者通常也會利用自己的雲端資源來處理運算使用者的資料。但有可能A業者的運算資源調配出了問題，需要臨時、緊急或短暫的移轉使用者資料，甚至是移轉使用者的帳號密碼到B業者的雲端平台上進行運算處理，這種資料的再移轉或再委外處理有可能並未知會使用者，此即產生資料再移轉的問題。A和B二業者的隱私政策與保護機制可能不盡相

[274] Aameek Singh et al., *Agyaat: mutual anonymity over structured P2P networks*, 16 NO.5 INTERNET RESEARCH 189, 209-210 (2006).
[275] 因為雲端資料的內容，很可能就內含使用者的辨識資料。
[276] 劉靜怡，同註 43，頁 41。

同，如果B業者的隱私保障較高，那可能僅有是否要經過使用者同意移轉的問題；但如若B業者的隱私保障較低，就會產生保護的落差，如果發生資料外洩或雲端服務失靈等情況，光誰要負擔責任就將產生許多爭議。歐盟安全指令及其所擬定的契約範本[277]即對此作出規範，在未得使用者或資訊當事人同意下的資料移轉或再委外處理，會被認定已經超出原先資料處理的目的，將視擅自移轉或委外處理的雲端業者就此部分為「資料控制者」，而必須負擔相關責任。因此，雲端業者有必要在隱私政策中聲明因為雲端資源調整問題而移轉或委外處理資料時，是否要取得使用者的同意，或者保證再移轉或委外單位的隱私與安全措施不低於原先提供的雲端服務。

第二項　雲端隱私權政策的具體內容

對於雲端運算一般的使用者而言，除了要享受雲端服務的便利外，就是要求盡可能減少產生的風險，包括存放在雲端的資料不會毀損滅失或個人資料不會外洩等，而這些風險有些是雲端系統技術上的原因、有些是受到惡意第三人的攻擊，但是更多的則是雲端業者自己的行為。不過就雲端業者的認知，提供一般使用者的服務幾乎無收取金錢費用，因此業者勢必要開發新的商業模式，也就是要對一般使用者進行廣告。事實也證實這是非常成功的商業模式，而且這種線上廣告模式愈來愈精準，愈來愈有針對性，原因就在於雲端業者應用了使用者的資料和網路行為[278]。如果我們從商業的角度來觀察，人氣越多的雲端服務，就越有商業廣告的價值，而要招來廣大人氣，當然最重要的是有吸引人的服務，Google和Facebook會火

[277] Commission Decision (2002/16/EC) of 27 December 2001 under the Directive 95/46/EC, *supra* note 233.
[278] Randal C. Picker, *supra* note 8, at 6.

速竄起就是因為廣受歡迎的服務。但除此之外，如果雲端服務的安全性一團糟，個人資料外洩嚴重，也會產生反效果，讓該服務成為眾矢之的，Google和Facebook也都曾經，或甚至目前都還持續受到資安人士的關心。雲端業者因此必須在使用者的隱私保護和業者商機間取得平衡點，也就是必須要藉助隱私政策宣示要如何對待使用者的個人資訊，來取得使用者的信任。另外對於雲端企業用戶而言，雖然不會有廣告的困擾，但是同樣也會憂心資訊外洩的問題，而且這些資訊一旦外洩將可能造成難以估計的商業損失，因此企業用戶同樣必須從隱私政策來瞭解雲端業者要進行哪些保護措施，並且在契約條款中確保隱私政策的執行。

那麼要落實資訊安全的保護，要保障使用者就雲端可靠度、安全性、隱私或匿名性的權益，雲端運算的隱私政策必須具備以下幾點[279]：

1. 雲端業者蒐集那些資料類型

按照 OECD 個人隱私保護基準及歐盟個人資料保護指令的規範，雲端業者必須在資料蒐集、利用及處理的初步階段就將這些行為的目的告知雲端使用者，這當中即須先告知使用者何種資料將被蒐集、利用及處理，此即 OECD 隱私保護基準中限制蒐集及限制利用原則之展現。至於使用者在雲端上進行的資訊和動作五花八門，涉及的範圍相當廣泛，這些資訊不斷的在雲端業者的伺服器和使用者裝置間移動，都有可能被雲端業者蒐集起來，包括：

(1) 使用者主動提供的個人資料：當使用者首次註冊雲端服務時，雲端

[279] Google 隱私權政策，參考 http://www.google.com.tw/intl/zh-TW/privacy/privacy-policy.html; Yahoo 隱私權政策，參考 http://info.yahoo.com/privacy/tw/yahoo/; Facebook 隱私權政策，參考 http://www.facebook.com/privacy/explanation.php#!/policy.php; Plurk 隱私權政策，參考 http://www.plurk.com/privacy; Twitter 隱私權政策，參考 http://twitter.com/privacy; Amazon 隱私權政策，參考 http://www.amazon.com/gp/help/customer/display.html?nodeId=468496#share; Windows Azure 隱私權政策，參考 http://privacy.microsoft.com/en-us/fullnotice.mspx#use; Xuite 隱私權政策，參考 http://member.cht.com.tw/html/MemberCenter2/privacy.html; 痞客邦 PIXNE 隱私權政策，參考 http://www.pixnet.net/privacy.

業者常會要求使用者提供必要的註冊資訊，例如姓名、電子郵件、出生日期、性別、工作、職位、個人喜好興趣等。通常雲端服務是允許使用者以代碼的方式建立使用者的帳號，或不會要求使用者提供詳實的個人資料。但是少部分的服務則會嚴格要求，或甚至審查使用者的資料,例如Facebook就曾經要求使用者必須提供真實姓名，並且執行將代號、綽號或匿名等名稱停權的政策[280]，使用者必須自行衡量是否要揭露這些資訊。

(2) Cookie：就如同我們前面提到 cookie 會記錄使用者的偏好設定、網頁要求、與服務間之互動情況、IP 位址、瀏覽器類型、瀏覽器語言、瀏覽記錄、連線的時間日期等資訊，業者透過 cookie 將可瞭解使用者的所有網路行為，是雲端業者進行線上廣告的一大利器。

(3) 使用者在雲上進行的資訊和動作：簡言之就是使用者在服務目的下進行的各種動作和儲存、上傳的資訊，例如用 Google Docs 編輯的文件檔案、用 Gmail 寄信收信的內容、用 MSN 傳遞訊息、在 Facebook 上進行留言、編輯、上傳照片或按「讚」等。

(4) 使用第三方開發的應用程式行為或以此產生的資料：現在許多雲端業者除了向使用者提供服務的 SaaS 模式外，還另外提供 PaaS 模式的服務，建構應用程式介面平台，讓第三方能夠在上面開發各種應用軟體，甚至提供各種收費獲利機制，例如我們在第二章提到的 Google App Engine 和 Facebook Platform 就是其例。使用者可能是利用這些元件開發各種應用軟體供其他使用者使用，也可能是一般使用者使用他人開發好的軟體或以此產生的資料，這些網路行為或以此產生的資料，均會被雲端業者進行蒐集。

(5) 與其他雲端平台或網站間的關聯服務：意即使用者利用雲端服務與

[280] Susan Boyle, *Facebook Defends its "Real Name" Policy*, NBC NEWS, May 20, 2009, http://www.ncbayarea.com/news/business/Facebook-Defends-its-Real-Name-Policy.html. (last visited 2011.07.08)

其他平台進行的流通資訊。例如使用Google或Yahoo帳號來進行網頁遊戲或其他平台服務的帳號，Google或Yahoo就會記錄下使用者這些連結的資訊[281]；或者例如Faccebook在其他網頁上設下的「讚」鈕，就可以蒐集到使用者感興趣的資訊。

(6) 位置資料：有些雲端服務會提供使用者地圖位置服務，甚至會和 GPS 連結，例如使用「Google 地圖」或「Google 定位」，就可能使雲端業者透過 GPS 蒐集到使用者的實際位置等資訊。

2. 雲端業者蒐集哪些資料內容

雲端業者會蒐集前述各種類型與格式的資料，這些資料有可能會涉及兒童、種族、血緣、宗教、政治意向、哲學信仰、工會活動、健康及性生活等資料。但是根據美國COPPA法案的規定，蒐集和處理兒童資料須得父母之同意，歐盟安全指令也針對敏感資料的蒐集和處理訂有許多規範，我國個人資訊保護法也參酌歐盟安全針對特種資料的蒐集、處理或利用訂有規範。不過站在雲端業者的商業角度來看，當然會希望蒐集到的使用者資料愈多愈好，因此這些業者不會在隱私政策中宣示哪些內容的資料不會被蒐集，反而是在服務條款中訂出相對應的條款，利用要求使用者承諾或得其同意的方式，來符合美國法制或歐盟安全指令的規範，例如要求使用者年齡必須大於 13 歲以符合COPPA的規定[282]，或要求使用者同意雲端業者可以處理這些敏感資料等。

3. 雲端業者如何利用這些資料

[281] 這種利用入口網站等雲端服務的帳號自動登入其他服務者，稱為「自動登入服務」機制。筆者為了測驗與證實雲端業者會對自動登入服務的網路行為蒐集資訊，利用 Google、Yahoo、MSN 和 Facebook 帳號一口氣登入了 10 幾個線上網頁遊戲，果真現在筆者的這些帳號都必須飽受線上遊戲廣告之苦。

[282] 例如 Plurk 的隱私權政策就對使用年齡訂出 13 歲及 13-18 歲不同的聲明，參考 Plurk 隱私權政策，同註 279。

對於使用者的資料，雲端業者除了在原有的雲端服務項目下進行資料的蒐集或處理外，也需要如我們一直強調的在隱私政策中交代如何利用這些使用者的資訊，以符合OECD和歐盟安全指令的規範。一般而言，大型雲端業者都會在隱私政策中宣示除了應用在原有服務外，還會應用在其他方面，例如管理雲端服務、優化使用者的介面、與使用者溝通聯絡、促進社群網路的互動、以及最重要的廣告活動等。Google的隱私政策就聲明：「提供、維護、保護及提升我們的服務(包括廣告服務)及開發新服務」[283]，Yahoo也宣稱：「改進為你提供的廣告及網頁內容、完成你對某項產品的要求及通知你特別活動或新產品」[284]，Facebook甚至大方承認會利用使用者的資訊來進行針對性的廣告服務[285]。所以在這些雲端業者的認知當中，進行廣告原本就是服務的項目之一，對使用者進行廣告就是在提供雲端服務，所以蒐集使用者資訊用於廣告的行為也就會符合服務提供的目的，因此雲端業者藉由隱私權政策宣示將廣告行為納入原有服務之「目的」，也告知使用大眾與取得其同意會用個人資訊作為廣告的依據。所以當使用者利用Google Docs、收發Yahoo Mail和在臉書上與好友互動是使用一部分服務，在雲端服務介面中讓我們的主角小吳感到痛苦但得忍受的廣告也同樣是服務的一部分，而且雲端業者既然已經在隱私政策中如是宣示，那小吳還來使用，就可能表示小吳也認知並同意雲端廣告是服務的一部分，同意進行廣告是蒐集小吳資訊的目的，這真的是非常高明的請君入甕手法。另外當然按照歐盟安全指令的規範，超出原有服務及廣告外的資訊使用方式，就會被認定是與原雲端服務的目的不同，業者必須在隱私政策上預作說明會徵求使用者的同意[286]。

[283] Google 隱私權政策，同註 279。
[284] Yahoo 隱私權政策，同註 279。
[285] Facebook 隱私權政策，同註 279。
[286] Google 即宣示：「如果此資訊的使用方式與當初蒐集的目的不同，我們會在使用前先徵求您

我們在第一章就曾提到例如Google、Yahoo和Facebook等雲端服務常是「免費」提供給一般使用者使用，而雲端業者要維持這些服務就必須對使用者進行廣告行為，廣告行為要精準有針對性就必須從使用者資料著手[287]。但使用者在利用雲端服務收發Yahoo Mail、使用Google Docs或Facebook時，其目的純粹只是在收發郵件、編寫文件或與好友聯絡，在使用服務的過程中不斷跳出的廣告頁面其實是雲端業者硬加進來的，而且這些廣告還和使用者的網路行為和個人資訊大有關連。雲端業者在隱私權政策中一開始就告訴我們會蒐集使用者的各種資訊，而且還會把這些資訊用來對使用者作廣告，因此實際上對一般使用者而言，我們認為這並非是無償使用服務，而是以個人資訊被蒐集偵知作為廣告依據的對價模式來使用雲端服務。根據eMarketer的預估[288]，2011 年排名前 3 名的網路和雲端服務業者Google、Yahoo和Facebook的線上廣告收益將達到 12.39 億、3.40 億及 2.19 億美元，從這些收益金額可見進行雲端線上廣告「服務」的商機是多麼的龐大，雲端服務的一般使用者其實並未佔業者的便宜，反而是愈多使用者加入雲端行列，愈增加業者的廣告規模。因此，就算雲端業者在服務條款聲明是免費提供服務，以及在隱私政策中聲明廣告是雲端服務的一部份，都無法改變我們所主張的這種雲端業者與使用者間的法律關係[289]。從這種對價關係的概念出發，雲端業者就應該對使用者及其資料負有一定責任，例如必須採取適當的安全防護措施或須負擔一定的資訊安全責任，我們主張的這種概念也會延續至下章所要討論的雲端消費關係。

相較於雲端的一般使用，雲端業者會根據企業用戶使用的運算量和

的同意」。Google 隱私權政策，同註 279。

[287] Randal C. Picker, *supra* note 8, at 6；李治安，同註 33 書，頁 57。

[288] eMarketer, *Google and Yahoo Still Take More Overall Online Ad Dollars*, March 1, 2011, *available at* http://www.emarketer.com/Article.aspx?R=1008252. (last visited 2011.07.08)

[289] 如若因為這種法律關係發生爭議，我們也很懷疑法院是否會採納業者的主張，畢竟當事人間的法律關係，並非由契約標題或內容文字決定，法院自得實際審查當事人間的權利義務關係。

時間進行收費 [290]，此即雲端運算即用即付費的特性。因此，在收取費用的情形下，雲端業者通常不會對企業用戶進行廣告服務，但這些使用雲端服務的企業仍要注意業者如何處理其相關的資訊，確保雲端業者在服務目的下利用這些資訊，以及超出服務目的時需徵得企業用戶的同意。

4. 雲端資訊的流通及分享

雲端業者掌握使用者資訊，除了提供原有服務與進行廣告外，還可能分享流通給第三方，因此雲端業者有必要在隱私政策中作出說明。大體而言，業者的資訊流通有下述四種方式：

(1) 雲端業者通常會聲明將個人資訊流通或分享給第三方時，會徵得使用者的同意，以符合美國法及歐盟安全指令的規範。此外有些雲端業者也會宣示，不會將使用者的個人資訊販賣或借出給他人使用。

(2) 除了(1)以外的情況外，提供雲端服務的業者會聲明讓使用者同意業者可以分享流通使用者資訊給雲端業者的子公司、關聯企業、其他可信賴的企業或人員、與其他人士或企業共用資料才能夠提供服務之人員，其目的在於處理使用者的個人資訊及提供更佳的服務品質 [291]。但雲端業者的這項政策將使得資訊流通的範圍過於廣大，對於付費使用服務的企業用戶而言，就必須利用服務條款約定企業用戶資料散佈的範圍，並且要求雲端業者負擔監督資料散佈的安全性。但是在一般使用雲端的情況時，根據我們一直討論的雲端廣告模式，使用者可能應該要擔心的是雲端業者會不會將使用者資訊向廣告贊助商展示 [292]。按照我們前面的討論，雲端業者認為提供給一般使用

[290] Dion Hinchcliffe, *What does Cloud Computing Actually Cost? An Analysis of the Top Vendors*, ebiz, August 22, 2009, http://www.ebizq.net/blogs/enterprise/2009/08/what_does_cloud_computing_actu.php.

[291] 例如 Google 的隱私權政策即如是規定，參考 Google 隱私權政策，同註 279。

[292] Julia Angwin, *supra* note 37.

者的服務就包含了廣告服務，所以進行廣告或拿個人資料進行廣告原本就在服務「目的」之中而不需要再得使用者的同意。但廣告業務來自於背後的廣告贊助商，這些廣告贊助商必定會對雲端廣告效益進行評估，雲端業者就極有可能將蒐集整理後的使用者資料作為廣告效益的指標而流通給廣告贊助商。那麼該如何歸類這些可能知悉使用者資料的廣告贊助商，而讓廣告贊助商取得資料也受到規範？是要將之歸類為關聯企業或其他可信賴的企業或人員，亦或雲端業者認為進行廣告是要與廣告贊助商共用資料才能提供的服務？我們實際查訪各大雲端業者及利用雲端系統的網站，其中Plurk及Twitter[293]就坦承會將個人資訊與廣告贊助商做連結，Google、Yahoo、Xuite及痞客邦PIXNET等業者[294]則是語焉不詳或回避此問題，僅有Facebook聲明原則上不會而只有在得使用者同意下才會與廣告贊助商分享資訊[295]。雲端業者實際上應該也不會把廣告贊助商歸類為需要得使用者同意之第三人，這不僅自找麻煩，也與業者擴大廣告獲利的商業模式相違背。

不過按照OECD與歐盟安全指令中資料利用處理明確性的規範，資訊的蒐集與處理之目的應該要予以明確，知悉由何人進行資料的處理即理應構成明確化的一部分。此外參照前章所述 2010 年歐盟所提出的契約範本[296]中要求跨境傳輸而再委外處理資訊時應先通知並取得資料控制者同意的概念，要取得使用者同意就必須明確告知使用者資訊再流通的範圍，因此歐盟安全指令的精神應是認為資訊的再流通固然應得資料擁有者的同意，且再流通的範圍亦應予以明確。因此，雲端業者這種模糊不清的流通分享條款，是有可能違反OECD

[293] Plruk 及 Twitter 隱私權政策，同註 279。
[294] Google、Yahoo 及痞客邦 PIXNE 隱私權政策，同註 279。
[295] Facebook 隱私權政策，同註 279。
[296] Commission Decision, *supra* note 256.

與歐盟安全指令的規定。不過既然雲端業者在隱私權政策中作了這麼不明確資訊流通範圍的聲明，等於又用了次讓使用者同意的花招，那麼更重要的問題其實是雲端業者如何對這些個人資訊的再傳輸與流通進行保護，例如Google就聲明：「...要求此等人士同意根據我們的指示處理此類資訊，並遵守本《隱私權政策》和其他適用的任何保密和安全措施。」[297]，這樣的聲明就意謂著Google應該要對此等人士的資訊安全保障措施負責，但是我們在其他多數的雲端服務中卻發現缺乏像Google這樣的聲明。因此，雲端業者既然認定廣告是服務的一部分，而且又在隱私權政策中藉由如是宣示來取得使用者的認知，但卻曖昧模糊地好像讓使用者同意移轉分享給廣告贊助商或其他人士的個人資訊不需要再得其同意，以規避美國法或歐盟安全指令個資再流通的相關規定，那麼將個人資訊流通給廣告贊助商或這些人士時就應視為雲端業者整體服務中的一部分，而同樣必須適用業者的隱私權政策與獲得業者聲明的安全措施的保障。是以，就算雲端業者不再對之多作聲明，也當如是解釋流通給這些人士的個人資訊享有業者隱私權政策保障的延續，如此才能對使用者的個人資料產生基本的保護作用。

(3) 除此之外，雲端業者均會宣示遵從所有適用的法律、法規、法律程序或具有效力的政府機關之要求，而將使用者資訊交給政府部門。因此，享有資料特許保護及須遵守執業秘密義務的使用者必須注意這類型的隱私條款，並且有必要藉由付費使用的方式，來向提供服務的雲端業者要求轉換為適當的條款。

(4) 另外如果雲端業者進行服務整併，或者雲端業者間進行合併或服務收購，甚至是為了取得更多使用者資料而整併其他雲端服務，就有

[297] Google 隱私權政策，同註 279。

可能發生使用者資料再次移轉的情形，雲端業者除了必須要聲明如何在整併的過程中保障使用者原本付費或使用服務時的權利，亦要聲明在資料移轉過程中如何進行個人資訊進行保護，例如確保對這些資料的資訊保密、說明新的隱私政策及新舊隱私政策如何銜接等問題。例如在 2010 年 7 月間Yahoo在台灣經營已久的交友服務宣布停止營運，並將與「愛情公寓」進行合併 [298]，Yahoo隨即宣布一系列付費會員權益移轉的機制，並且推出個人資料打包移轉的機制與說明，並且聲明原使用者未同意移轉資料時，Yahoo將不會主動移轉使用者的資訊[299]。但在雲端業者因為要進行整併而終止服務時，光是使用者未同意移轉而業者即不進行資料移轉是不夠的，接下來我們即將討論到此時業者還須進行資料的刪除與終結，方能完善資訊安全及個人隱私的保護。

5. 雲端資料的保存與刪除

雲端時代蓬勃發展，雲上的資訊龐雜大量，業者勢必用到各種資料格式或技術來保存或儲存使用者的資訊，但是這些資料會保存多久或者有無資料刪除的機制，卻是多數雲端業者都迴避的問題 [300]。我們會提出這樣的問題，著眼在於現代資訊技術的發展日新月異，各種網路或雲端服務不斷推陳出新，業者之間合併、整合或併購導致服務改變或中斷的情形時有所聞，以前很流行的ICQ和台北林克，現在也很明顯地被MSN和無名小站[301]取代，前述Yahoo的交友服務與愛情公寓整併即是一

[298] 參考 Yahoo!奇摩，中文維基百科：http://zh.wikipedia.org/wiki/Yahoo!%E5%A5%87%E6%91%A9 (查訪日期 2011 年 7 月 8 日)。

[299] 林亞蓁，徐美渝，Yahoo！奇摩交友 11 月 30 日終止服務，MOL 銘報即時新聞，2010 年 10 月 10 日。另外參考當時 Yahoo 的說明，http://blog.xuite.net/monthday/bation/39230839. (查訪日期 2011 年 7 月 8 日)。

[300] Konstantinos K. Stylianou, *supra* note 247, at 607.

[301] 無名小站在商業化過過程中也遭到使用大眾的質疑與排斥。參考無名小站，中文維基百科 http://zh.wikipedia.org/wiki/%E7%84%A1%E5%90%8D%E5%B0%8F%E7%AB%99.

例，臉書的出現更是造成一窩風的熱潮進而排擠到其他社群網站的發展，現在又有Google+加入社群網站的市場[302]。所以使用大眾很可能因為新服務的產生而不再繼續原有的服務，也有可能因為業者自身因素停止該服務的運作，這種現象同時也會出現在雲端時代之中，那麼這些使用者之前上傳的資料該如何處理將成為重要的議題。

對於運雲端資料的刪除可以分成兩個部分，其一是使用者還在使用服務時在雲端上增刪修改資料或者刪除cookie記錄檔，雲端業者有必要對是否會將這些資料進行備份保留或者保留時間的久暫進行說明，這也才能符合OECD保護基準與歐盟安全指令中所揭示的個人資訊參加原則及當事人的請求及確定資訊凍結權，即落實保障使用者的「資訊自我決定權」[303]。例如Google經過Authors Guild v. Google Book和解案後，就在隱私權政策中說明原則上允許使用者免費增刪修改放在雲端上的資訊，不過會因為Google的雲端系統需要一段時間才會將殘留的檔案副本從伺服器中刪除，而可能還保留有備份檔案，但遺憾的是Google仍未說明這些備份檔案可能會被保留多久，或者這些備份檔案會不會被另作他用[304]。其次則是使用者停用服務或業者終止服務時，仍留在雲上的資料該如何處理。面對這種情況，企業在使用雲端服務時，必需要注意透過使用者條款來對服務終止及終止後資料的處理進行規範。對於一般者用者而言，我們前面已一再強調雲端服務並非「無償」，而是以使用

[302] 劉翰謙，Google+，真正的 Facebook 威脅？，數位時代，2011 年 6 月 29 日，參考 http://www.bnext.com.tw/article/view/cid/0/id/19085 (查訪日期 2011 年 7 月 8 日)。

[303] 余啟民，由肺結核病患名單資料外洩談公務機關就醫資訊管控與監督，月旦民商法，24 期，2009 年 6 月，頁 13。

[304] Authors Guild v. Google Book 和解案中涉及到著作權侵害與使用者隱私等相關議題，Google 僅願意支付金錢給 Google Books Platform 中可能侵權的作者們，並保有該類書籍的掃瞄複製檔，但是參與該案中的如 Consumer Watchdog 和電子前鋒基金會(Electronic Frontier Found)等團體，對 Google 要求的並不僅是著作權方面的議題，更多的是希望 Google 對蒐集到使用者的閱讀習慣等資料作出保存的限制，不過當時仍未得到 Google 正面的回應。See *Authors Guild v. Google*, ELECTRONIC FRONTIER FOUND., http://www.eff.org/cases/authors-guild-v-google. (last visited 2011.07.08); William R, Denny, *Survey of Recent Developments in the Law of Cloud Computing and a Software and a Service agreement,* 66 BUS. LAW. 237, 238-239 (2010).

者資料被用作廣告等其他用途來作為對價。那麼既然雲端服務已然停用或終止，作為對價的「使用者資料被另作利用」也應該同樣停止「支付」方為合理。因此服務一旦停用或終止，雲端業者即不能在對使用者資訊有所利用，這些不再被利用的資訊不能僅是保障不會被任意存取或接觸，雲端業者必須建立適當的永久刪除機制。

我們可以理解服務一旦停用或終止後，雲端業者需要進行系統調整來處理及終止這些使用者的資訊，但很遺憾的是目前多數雲端業者的隱私權政策與服務條款都對如何永久刪除使用者資訊或保存多久後進行刪除等部分付之闕如或不盡完整。以Facebook的隱私權政策為例[305]，雖然宣稱使用者可以自行增刪臉書上的資訊內容或可以停用帳號，並保障停用帳號後原本的資訊內容不會再讓其他人接觸到，但Facebook也同樣表明會保留備份這些增刪與停用帳號的資料，理由居然是Facebook很體貼地給予使用者回復資料與恢復帳號使用的機會。Facebook之前就曾經採行真實姓名的管理帳號政策[306]，而且上面有大量使用者的個人資訊，包括臉書網誌、塗鴉牆、照片、居住地、工作職業、學經歷及喜好興趣等資料，這些資訊不需要再經任何處理整合就可以在現實生活中清楚呈現出每個使用者的輪廓，如果當使用者停止使用帳號時，按照Facebook的「善意」雖然會保證不再顯示與不會有第三人接觸這些資訊，但是這些個人資料會保留到地老天荒直到使用者回心轉意重回Facebook的懷抱，那麼我們不禁要問，既然使用者已經結束帳號停用服務，Facebook不就已經喪失經由臉書向使用者進行廣告的管道嗎？就算現在資訊儲存技術進步快速，但是保留使用者的資料仍要付出成本，那麼到底Facebook保留這些不讓人見著的資料要作什麼？Facebook保留

[305] 參考 Facebook 隱私權政策，同註 279。

[306] 以筆者自己的臉書好友們為例，有一半好友採用真實的中文姓名名稱作為帳號，剩下的一半是以中文英譯的名稱作為帳號，僅有非常少數採用其他命名方式。這種現象固然和臉書所標榜的交友社群要貼近真實生活有關，但也和 Facebook 採用真實姓名管理的政策不無相關。

這些資料只是在增加資訊隱私安全的隱憂，這恐怕很難是Facebook用等待使用者回心轉意的理由就可以搪塞過去的。此外就算Facebook停止了臉書服務或被併購而終止或改變服務，這些停用帳號的個人資料該如何處理，我們同樣也未見Facebook作出說明[307]。

6. 雲端資訊利用及安全措施

除了上述這些雲端業者可以從商業操作面調整的隱私權政策外，在雲端資訊技術層面上，雲端業者也有可能會建置以下兩大類的資訊利用及安全保護措施：

(1) 選擇及調整介面：有些雲端業者基於過去訴訟或和解的經驗，會設計一些介面與選項，提供使用者進行隱私權的設定。例如 Google提供廣告偏好設定，讓使用者可以停用或管理廣告顯示，並且提供停用cookie的方式，與說明cookie檔內會記錄的資訊內容與格式[308]；Yahoo也提供「選擇退出網頁」選項，讓使用者可以不要見到針對使用者的客製化廣告[309]；又例如Facebook提供使用者內容隱私的設定，讓使用者決定可否讓個人資料對外顯示，而且在Beacon計畫失敗後所推出的Facebook Connect方案，也提供廣告選項，讓使用者選擇是否接觸到廣告[310]。但是我們觀察這些介面選項，多是前面我們提到的opt-out模式，意即使用者必須另外進行調整才能退出雲端業者的「廣告服務」，並非讓使用者可以自行選擇是否接觸廣告的opt-in模式，而且這些介面也被業者設計的非常不容易操作，由此可見雲端業者是多麼地積極要對使用者進行精準針對性的廣告。此外，這些

[307] Facebook還是我們找到願意公開承認與找各理由說明在服務停用後要保存使用者資訊的雲端服務，其他絕大多數的雲端業者幾乎迴避這個問題。Yahoo也僅在服務條款中聲明停用或終止帳號時，Yahoo「得」刪除全部或部分資料，參考 Yahoo 隱私權政策，同註 279。

[308] Google 隱私權政策，同註 279。

[309] Yahoo 隱私權政策，同註 279。

[310] Facebook 隱私權政策，同註 279。

雲端業者也僅是建置不讓使用者接觸到廣告的介面，而非使用者調整廣告介面後，就不再蒐集分析使用者的資訊或者就不再流通資訊給前述範圍不明確的相關第三人，亦可見雲端業者充分利用使用者資料的商業企圖是多麼的強烈。

(2) 資訊安全措施：除了隱私及廣告設定外，不論是一般使用者或企業用戶，另一個關心的重點就是上傳到雲端的資訊如何受到的保護。雲端業者大多會宣示，對於使用者在雲端平台上登入的帳號密碼會以加密方式來保護，也大多會聲明對使用者的個人識別資料，例如姓名、身份證字號、電話或地址等，進行加密化的保護[311]。對於使用者其他的資料，雲端業者也大多會聲明採用「適當」、「當時科技水準」或「盡最大努力」施以保護機制，防止未經授權的資料存取、竄改、揭露或損毀，並且及於資料的蒐集、儲存及處理等過程[312]。不過雲端業者也僅是作如此宣示，用「適當」或者「當時科技水準」的文字來滿足OECD、歐盟和APEC要求採取「適當」保護措施的規範，但實際上採取什麼樣的安全措施，施以什麼樣的加密保護、SSL加密憑證[313]、防火牆或實體防護等安全措施[314]，大多在隱私權政策中付之闕如。此外如果這些安全措施有效運作固然保障資訊安全，但倘若因為系統安全發生問題時則將產生責任歸屬的問題。對於企業用戶而言，這當然必須在使用條款中予以規範；但對於一般的雲端使用者，業者卻常是在定型化的使用條款中拒絕承諾或保證任何安全性的責任，使用者常必須因此承擔因為雲端技術問題所造成之損失[315]。

311 參考 Google、Yahoo 及 Facebook 等雲端業者的隱私權政策，同註 279。
312 同上註。
313 Wikipdeia definition of Secure Sockets Layer: http://en.wikipedia.org/wiki/Secure_Sockets_Layer. (last visited 2011.07.08)
314 Christopher Soghoian, *supra* note 272, at 394-397 (2010).
315 李治安，同註 33，頁 59。

7. 雲端資料處所及跨境傳輸

雲端運算為何會需要跨境傳輸使用者資料已如前述，然而從資訊安全保護的角度來觀察，雲端跨境傳輸會產生兩個重要的問題：首先是資料伺服器所處之位置，這將牽涉到資料保護適用的法令；其次則是雲端業者採取的保護措施。但是大多數的雲端業者幾乎都逃避將使用者資料儲存和運算於何地處所伺服器的問題，不僅在隱私權條款中付之闕如，當然也更不會宣示該對資料跨境傳輸時該如何進行資訊安全的保護。再者雲端運算的一大特色就是系統能夠根據需求，自動且即時動態地調整運算儲存資源，以Google全球百萬台伺服器為例，實務上Google也很難知悉哪筆使用者的資料位在哪台伺服器上，因此Google就在隱私權政策中承認會用位在不同國家或地區的伺服器處理使用者資訊[316]，由此可見這種宣示意謂著雲端業者承認資訊跨境傳輸會是整體雲端服務的一環，那麼這種跨境傳輸資訊的安全就應該享有業者隱私權政策的保護。另外對於適用法規的部分，由於雲端資訊可能會流經多個國家或區域的伺服器，各地資訊隱私法規保護的程度不一，適用何處法律規範或如何解釋適用將造成諸多爭議，因此有可能發生爭議時會以服務條款中約定的準據法作為處理的依據。此外像Google這類雲端業者也會聲明已註冊美國商務部的安全港計畫，因此如若資料流經位在歐盟區域的伺服器，那就應該有前述歐盟安全指令保護的適用。另外針對雲端企業用戶而言，為了避免跨境傳輸可能的安全漏洞，或是適用法規的疑義，亦有必要在協商條款時約定企業資訊流通的範圍，以杜絕上述爭議。

8. 政策執行與認證

[316] Google 隱私權政策，同註 279。

我們在前面的討論中曾經提到過，雲端業者需要的伺服器群組會因為電力需求或其他因素散佈在全球各地，而造成雲端資訊的跨境傳輸問題，因此許多美國跨國大型雲端業者會向美國商務部的安全港計畫進行註冊，以符合歐盟安全指令的規範，例如Google、Facebook、Amazon和EasyLink[317]等業者就取得安全港的註冊，使用者至少可以瞭解到這些雲端服務是符合歐盟的資料安全標準。對未有安全港註冊或聲明遵守歐盟安全指令的雲端服務，同樣也要注意雲端資料儲存伺服器處所和跨境傳輸的資料保護問題。有些雲端業者另外也會尋求TRUSTe的隱私標章認證，來讓使用者感受到業者保護資訊隱私的誠意，例如Yahoo、Microsoft、Oracle和Facebook等雲端業者均獲得該項認證[318]。此外雲端業者也會在隱私權政策中聲明，提供聯絡管道來與使用者進行隱私政策討論或資料保護疑義的處理。

9. 隱私權政策的變更

雲端業者可能根據訴訟結果、使用大眾的意見或技術及服務的發展，隨時想要更改隱私權政策，例如在 Google 的頁面中我們就可以查詢到過去 Google 的隱私權政策版本。但是我們前面也討論到隱私權政策是屬於使用者條款的一部分，因此隱私權的變更是改變雲端服務兩造的權益，須得對方之同意方可為之。是以雲端企業用戶必須特別注意，要透過使用條款規範此類情事。至於一般使用大眾則顯得特別弱勢，因為大多數的雲端業者又在隱私政策中聲明保留隨時變更的權利，所以使用者必須特別注意業者是否聲明不會降低隱私保護及減少使用者的權益，並注意業者是否會在重大隱私政策變更時通知及用何方式進行通知。

[317] EasyLink 隱私權政策，參考 http://www.easylink.com/utility/legal/privacy-policy.php
[318] Wikipdeia definition of TRUSTe: http://en.wikipedia.org/wiki/TRUSTe (last visited 2011.07.08); *See* also http://www.truste.com/about_TRUSTe/

第三項　小結

基本上對於雲端隱私權政策的討論，我們是按照雲端的使用對象區分成企業用戶與一般使用的兩種模式，在下節雲端服務條款的討論中，我們也將採取此種方式進行討論。就一般的雲端使用來說，不論業者要怎麼利用文字修飾隱私政策或條款內容，或如何利用「服務」的字眼來形容對使用者進行的廣告，我們都認為這是以使用者資料被用作廣告等其他用途來作為使用雲端服務的對價。從這個角度來觀察，我們就可以發現到雲端業者單方制訂的定型化隱私權政策，對於使用者而言是存有許多不公平之處，例如讓使用者同意範圍過廣的雲端業者相關第三人的流通對象、讓業者可以擅自變更隱私權政策、讓使用者接受廣告為服務的一部分等；此外還有對使用者不明確而缺乏保障的條款，例如在隱私權政策中缺少服務停用後資料如何刪除的說明，缺少跨境傳輸資料保護與爭議處理的條款，以及並未說明採取何種適當的資料保護措施等。我們也藉由這些討論提醒企業用戶，雲端隱私政策的內容關係到企業資訊的流通與安全，涉及到企業正常運作與否與營業秘密的保護，因此必須特別注意這些我們討論到的雲端隱私政策相關議題。

第二節　雲端服務條款

除了上述提到的隱私權政策外，提供雲端服務的業者與使用者間最重要的就是服務條款。服務條款(Terms of Services)，或有稱為使用條款、服務品質協定(Services Level Agreement, SLA)[319]或顧客協定(customer

[319] Robert H. Carpenter, *Walking from Cloud to Cloud: the Portability Issue in Cloud Computing*, 6WASH.J.L. TECH. & ARTS 1, 3 (2010).

agreement)者[320]，係指服務提供者與使用者間的協定，規範彼此間的法律關係與權利義務，包含服務品質(quality of the service, QoS)、責任、擔保等項目，與隱私權政策共同構成雲端服務契約。在此我們還是延續之前的說明，並參照市面上多數雲端業者提供的內容，將雲端服務提供者與使用者間的契約內容，分成隱私權政策與服務條款。隱私權政策的部分就如同我們前面所討論，是業者對如何保障使用者資訊隱私安全的聲明，除此之外的法律關係，我們則將之歸類在服務條款中進行討論。

本節我們將進行的討論，也同樣著重在雲端服務的一般使用觀點，來說明服務條款應該注意的事項。畢竟現在市面上提供雲端服務的業者如Google、Yahoo或Amazon等，多屬跨國大型業者，對於一般使用大眾多是提供定型化的隱私權政策與使用條款，這些條款內容甚至適用於中小型企業用戶。在實務上要這些大型雲端業者對廣大的一般用戶或中小型企業用戶進行一對一的協商，應屬不可能或過於缺乏效率之事[321]。我們提出的這些觀點，也同樣能夠對較有經濟實力的企業用戶，作為和雲端業者進行磋商時的參考。

第一項　雲端服務條款之探討

雲端運算服務，是雲端業者提供雲端運算資源或應用服務，使用者支付相應費用作為對價，因此服務內容與費用構成雲端契約的兩項必要之點。這兩項必要之點，也是雲端的一般使用或企業用戶，在選擇雲端運算服務時需要進行考量與評估的事項，也是雙方在雲端服務條款中需要載明之事

[320] Davide M. Parrilli, *Legal Issues in Grid and Cloud Computing*, *in* CLOUD COMPUTING: A BUSINESS PERSPECTIVE ON TECHNOLOGY AND APPLICATIONS 97, 99 (Katarina Stanoevska-Slabeva et al. ed., 2009).
[321] *Id.*

項。我們以下分別說明服務條款之內容：

1. 雲端服務內容

使用者要採用哪種雲端服務，當然首先是這套服務內容能達成使用者的需求，例如用 Gmail 就是要來收發信件溝通聯絡、採用 Amazon 的 EC2 和 S3 服務就是要應用雲端的運算與儲存資源、利用 SalesForce.com 的雲端系統就是要進行企業管理項目等。除了服務項目能達到使用者目的之外，使用者還要對雲端服務進行我們在第 2 章所提到的雲端評估項目，包括雲端系統的彈性、可靠度、敏捷性、適應性、可用度、反應時間、吞吐率或處理能力等項目。評估這些項目的目的在於瞭解雲端系統的整體效能，是否能達成使用者的需求；更重要的是企業用戶必須藉此瞭解，在網路或雲端技術上或者是否有其他因素會影響雲端服務在線運作的時間，以及是否需要建置備用方案，來避免服務中斷時影響企業活動的正常運作，亦或進行保險以分攤可能的風險。

2. 費用

針對雲端企業的使用或部分的一般使用，雲端業者會根據前述的服務內容及服務品質進行收費。但對於多數的一般使用而言，雲端業者通常會在使用條款中聲明是「免費」提供使用者服務 [322]，不過根據我們之前的討論，我們認為這種條款解釋起來僅是在金錢上不收取對價的「免費」，並是以使用者資料作為廣告基礎為利用服務的對價，實際上 Google也承認在服務中載入的廣告是作為授予使用者取得及使用服務之權利的對價 [323]。不過因為雲端業者基於這種「免費」的認知，所以會在之後我們要進行討論的服務條款內容當中作出免責聲明，不願意承

[322] 例如 Facebook、Plurk 和 Twitter 等雲端服務。

[323] Google 服務條款第 17.3 條：「台端同意，Google 得於服務上載入該等廣告，作為 Google 授予 台端取得及使用服務之權利之對價。」，參考 http://www.google.com.tw/accounts/TOS。

擔使用者的損賠責任。因此一般使用者在利用這類雲端服務處理較帶有機密性資訊時，必須格外注意是否適當，及使用者是否能承擔相應之風險。

3. 安全性

雲端服務資訊安全性問題，在前面的部分我們已經多有討論，並且在雲端隱私權政策中進行過深入分析。即便如此，我們還是把安全性這個項目放在此處，就是希望再次強調雲端安全性的隱私政策面與資訊技術層面都是使用者必須特別重視的部分，尤其是對於企業用戶涉及到營業秘密或商業經營的資訊，特別需要多加注意。

第二項　雲端服務條款的具體內容

雲端運算契約除了前述的服務內容、費用及安全性等必要之點外，尚包括雲端業者與使用者間其他的權利義務及法律關係，這些都會規範在服務條款之中[324]。我們同樣也會將重點放在雲端一般使用的定型化服務條款，並藉由這些討論提醒企業用戶在與雲端業者進行服務條款的磋商時應該注意的事項。

1. 雲端契約的成立或生效與雲端服務條款的接受

按照我國民法體系，契約之訂立與成立分成契約成立要件與契約生

[324] Google 服務條款，同註 323；Facebook 服務條款，參考 http://www.facebook.com/terms.php?ref=pf Plurk 服務條款，參考 http://www.plurk.com/terms; Windows Azure 服務條款，參考 http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Copyright/Default.aspx; Twitter 服務條款，參考 http://twitter.com/tos; Yahoo 服務條款，參考 http://tw.info.yahoo.com/legal/utos.html; Amazon 服務條款，參考 http://aws.amazon.com/terms/； Xuite 服務條款：http://member.cht.com.tw/html/MemberCenter2/service.html；痞客邦 PIXNE 服務條款：http://www.pixnet.net/regulation.

效要件[325]，雲端契約亦不例外。雲端服務的企業使用，當然可以經由雙方協商契約成立生效及服務上線運作的時間。但現今的一般雲端服務，通常是由兩種方式開展，其一為使用者向雲端平台申請帳號，在申請過程中除了填寫個人基本資料外，提供雲端服務的業者可能會設計讓使用者點選同意接受服務條款，或者當使用者按下申請確認鍵時視為同意接受該條款[326]；條款接受後雲端業者除了提供服務外，當然就按照隱私權政策和服務條款開始對使用者資料進行處理，並以此來標定該帳號用戶以進行廣告活動。其二則是使用者直接使用服務，例如我們直接利用Google來搜尋資料或利用Google Map來找尋地圖、地標或方位等，這種情況下雲端業者會在服務條款中說明實際使用服務即視為接受該服務條款[327]。雖然在第二種情況下並非使用帳號來進行服務，業者並無使用者登錄的個人資料，但不要忘記我們前述所討論的隱私權政策，雲端業者也是會蒐集與記錄使用者IP、所在位置、瀏覽內容、瀏覽器種類及瀏覽器語言等資訊，同樣能夠對使用者作辨識與標定來進行精準的廣告行銷。

2. 對於雲端服務內容的規範

雲端一般使用者除了利用主要的服務項目和忍受廣告的騷擾外，對於這些服務內容還要注意到雲端業者通常會採用的規定：

(1) 雲端業者提供的服務有可能出現令使用者感到冒犯、粗鄙或反感的內容，但這些業者通常會聲明「有權利但無義務」對這些內容進行過濾或消除，例如利用Google可以搜尋到色情、暴力或血腥的內容，但是Google在使用條款中聲明不會對此負任何責任，這種聲明往往

[325] 王澤鑑，債法原理(一)，頁 171，2006 年 9 月版。
[326] 參考 Google、Yahoo、Facebook 等雲端業者的服務條款，同註 323 及 324。
[327] Google 服務條款，同註 323。

成為各國政府管理雲端網路的藉口[328]，Google為此也推出SafeSearch或其他付費軟體的設定，提供使用者過濾清除色情內容的工具[329]。像Google這類的雲端業者是否要對服務內容進行控管，這個問題涉及言論自由或網路中立性等議題，不是本文我們所要討論的重點，在此我們只是要提醒一般使用者注意此一現象。另外對於企業用戶而言，當然是必須透過服務條款避免不相干的服務內容出現，以維持企業活動的正常運作。

(2) 雲端業者就所提供的服務，通常也會聲明這些包括資料檔案、書面文本、電腦軟體、圖片、影音視頻、甚至包括廣告或贊助等服務內容均受到智慧財產權的保護，雲端業者的商號、商標、服務標章、標誌、區域名稱或其他顯著品牌特徵亦受到相關的保護，因此會在服務條款中提醒使用者除明確為法律所許可外，或基於合理的使用目的及範圍外，必須經過雲端業者或相關內容所有人的同意，否則不得任意修改、承租、出租、借貸、出售或經銷這些內容，或者是對服務軟體進行逆向工程、反編輯或其他試圖提取原始碼之行為[330]。雲端業者通常也都會告知使用者有尊重智慧財產權的義務，如有違反則應負相關的損害賠償責任。

(3) 雲端運算的一大特色就是服務透過網路傳送至使用者的電腦或手提裝置，服務的升級同樣也是透過網路傳輸讓使用者即時享用，讓使用者不用在更新硬體及提升配備。因此雲端的一般使用，常會有服務升級、調整、變換或改版的現象，同時也可能因為雲端業者經營策略的改變或其他因素而必須永久終止或暫時中斷服務，業者對這

[328] Simon Elegant, *Chinese Government Attacks Google over Internet Porn*, TIME, June 22, 2009, http://www.time.com/time/world/article/0,8599,1906133,00.html; Maggie Shiels, *Google Tackles Child Pornography*, BBC, April 14, 2008, http://news.bbc.co.uk/2/hi/7347476.stm.

[329] Google SafeSearch，參考 http://www.google.com/support/websearch/bin/answer.py?hl=en&answer=134479.

[330] 參考 Google 服務條款，同註 323；Facebook、Plurk、Windows Azure、Twitter、Yahoo 及 Amazon 服務條款，同註 324。

種情形多半會聲明可以不經使用者同意就自行變換服務，或聲明無須通知或得使用者同意就可以中斷服務，並且說明使用者可能無法再接觸到已經在雲端上的資料[331]。這類條款其實對一般的使用大眾存有公平性的疑慮，而且業者同樣將之包裹在定型化服務條款中，一經使用者申請帳號或使用服務就視作使用者同意該條款。如果雲端服務的升級變換能夠讓服務效能更好或更便於操作，當然會受到使用者歡迎，但問題在於雲端服務升級後可能產生的風險和後果。把這類條款跟下述要討論到的責任條款互相參照，會發現業者對於升級變換服務的風險是聲明不負任何擔保責任的，2011 年 3 月Gmail就疑似版本升級導致使用者的郵件和通訊錄遺失[332]，Google對使用者的損失當然就會主張使服務款中的免責條款。此外根據前述我們對隱私權政策的討論，雲端業者在任意中斷服務後，使用者除了喪失使用服務的權利外，雲上資料不僅不能再被使用者接觸來進行資料保全或刪除的動作，業者同樣也缺乏對個人資料如何處理或是否完全刪除的說明，可以說簡直是置使用者於雙重不利的境界。同樣對於雲端企業用戶而言，除了享受升級的服務外，也必須留意業者如何進行升級改變服務、對服務暫停或中斷的說明和處理，以及之後會提到的服務終止條款，這些事項會涉及服務的內容品質、業者的支援項目及責任問題，亦應當一併注意。

3. 雲端服務的使用及限制

雲端業者除了提供服務供使用者利用外，還會在服務條款中制訂一些服務的使用及限制規定。

[331] 參考 Google 服務條款，同註 323；Facebook、Plurk、Microsoft Azure、Twitter 及 Yahoo 服務條款，同註 324。
[332] 陳炳宏，同註 121。

(1)　對於一般的雲端使用，雲端業者通常會如Google對使用者聲明「授與使用者一個人、全球使用、免費、不得轉讓且非排他性之權利使用服務」[333]，其中「免費」的問題我們已經討論多次，「全球使用」則代表雲端運算的特性，只要是網路能夠連結的地方就都可以享受到服務，至於「一個人、不得轉讓且非排他性」則充滿了許多意涵。正如我們前面所言，提供一般雲端服務的業者要靠眾多人氣來擴大廣告營收，因此會限制每個雲端帳戶僅得供一人使用且不得轉讓，就是希望有愈多的使用者來利用服務，可以蒐集到更多的個人資訊作更多精確的廣告「服務」。但是網路匿名的先天特性，讓雲端業者不太可能會知道每個帳號操作的背後都是該名申請使用者，要求提供一般雲端服務的業者進行將帳號綁定固定IP或者是每次登入連線時進行通訊鎖解鎖等動作，將可能使雲端業者負擔過多成本，也可能讓使用者在利用雲端服務時充滿不便。因此，雲端業者大都會聲明這是「非排他性」的使用服務權利，這也意即雲端系統是認帳號密碼不認人，連帶的在責任條款中，雲端業者也會聲明對於帳號密碼被盜用所衍生的損失是不負擔責任，所以也會在隱私權政策中宣導使用者必須自行建立帳號密碼的保護機制，例如加密化、經常進行電腦病毒掃瞄或者不在不安全的使用裝置上登入帳號，以避免像MSN盜帳號的MyCard詐騙事件 [334]發生。實際上雲端業者也多半會建立帳號被盜時的通知機制，但亦會聲明使用者在未通知或未知悉時仍應對該帳號的活動負責任的條款，如若該帳號被盜用而侵害雲端業者時，該使用者仍是必須負上責任的。

將這種條款和企業用戶的條款作比較就可以發現，企業用戶基於商業上的原因必定要限制雲端服務的接觸人員與地點，甚至可能

[333] 參考 Google 服務條款，同註 323。
[334] 湯蕙如，同註 271。

必須將雲端服務和企業網路IP綁定或者加上通訊鎖等措施，企業用戶以金錢作對價固然該享受到較周全的保護，但這不也意謂著一般雲端服務的業者打著「免費」的認知與條款來減少對一般使用大眾的保護嗎？雖然我們也承認要讓Google或Facebook這種擁有全球上億用戶的大型雲端業者針對每個一般使用者建立確認機制是不可行的，又或者現今一般雲端使用帳號的申請容易且氾濫，但業者最少要明確說明進行哪些保護帳號密碼或個人資料的機制，而非僅是在隱私權政策中聲明會確實努力進行保護機制，但在服務條款中又聲明對所有責任都不負責。按照我們對雲端一般使用以個人資料作為線上廣告依據的對價概念，雲端的一般使用者並未佔業者的便宜，因此不論是雲端的企業應用或一般使用，各類型的雲端使用者在法律上所能取得的保護應無高低之分[335]，皆須受到業者同樣的重視。

(2) 在雲端的一般使用中，有些雲端業者會在使用者申請帳號登入服務時要求使用者提供個人資訊，例如身份或聯絡資料，並且聲明如果因為資料不實而導致使用服務的權益受損，則使用者當自行承擔。雖然雲端網路的匿名特性，讓使用者的真實身份很難查核，而且要重新申請使用帳號也是相當容易，但我們在此只是要提醒一般雲端使用者，是否要填寫詳實資料，必需要視雲端服務的性質而定，例如Facebook過去的真實姓名政策就標榜拉近現實與網路社群的互動，並聲明不實資料會造成使用權益的受損。是以，雲端的一般使用者必須衡量自身的情況，並應該要在登入資料前詳讀雲端服務條款與隱私權政策的相關規定。

(3) 目前多數的雲端服務均會要求使用者年齡要達到法律規定的要求，例如要求使用者滿足 COPPA 的 13 歲規定，或者利用雲端平台進行

[335] 李治安，同註 33，頁 57。

線上交易者要符合成年或根據交易內容符合年齡之相應行為能力人。雖然同樣基於雲端網路匿名的特性，雲端業者不太可能查核使用者之年齡，不過有些業者會聲明管教兒童及青少年上網或登入雲端的責任在於父母，是否在雲端上傳兒童及青少年之資料決定權亦在於父母。這種條款其實也再次呈現了雲端網路時代的匿名性問題，提供雲端一般使用服務的業者實際上也不太可能花上成本去審查使用者的資格，就算進行了審查也無法確保使用該帳號登入者確實為本人，因而才會有這種雲端業者轉換要求使用者自律的條款。

(4) 雲端服務內容包羅萬象，而且網路的世界無遠弗屆，因此很容易讓有心人士利用作為犯罪工具，故雲端業者也會在服務條款中聲明使用者利用雲端服務時，不得違反所在地之法律規定，不得從事侵害他人權益或違法之行為，或者不得進行任何對該雲端平台的侵害。

4. 使用者對內容之授權

一般而言，雲端業者多承認使用者於服務上或透過服務提交、張貼或展示之內容享有應有之著作權或其他權利。但也因此雲端業者多在服務條款中強制使用者授權與業者及其相關單位、人員或企業，例如Google就將這類條款規定為「授予雲端業者就這些內容物的全球使用、免費、不得撤銷及非排他性之權利，而可進行以公益、展示、散佈、推廣、宣傳或經營服務為目的的複製、改編、修改、變更、翻譯、發佈、公開演出、公開展示、散佈。」[336]，其他雲端業者也均有內容類似的條款[337]。這類型的條款有著許多值得進一步討論的內含與意義：

(1) 首先按照這類型條款的規定，雲端業者要求使用者進行授權的內容幾乎就是在雲端上進行的各種資訊與網路行為，而且這種授權目的

[336] Google，同註 323。

[337] 參考 Yahoo、Facebook、Twitter、Plurk、Xuite 之服務條款，同註 324。

的範圍幾乎無所不包，舉凡進行升級服務、進行廣告服務、傳遞資訊予第三方、傳遞使用者資訊供廣告贊助商參考，到提供使用者資料予政府單位等均包括在內。

(2) 此外「全球使用、免費、不得撤銷」的條款，也意謂著雲端業者可以在全球各地進行這些行為，可以免費利用使用者資訊來對使用者作廣告，使用者對於雲端業者的這些行為是不得撤銷的，而且這種授權並不僅授權予該雲端業者，尚可能及於那些在隱私權政策中可與雲端業者分享使用者資訊的相關單位、人員或企業。

(3) 我們或許過於危言聳聽，畢竟雲端業者也是可能會在隱私權政策中宣稱不會將使用者資料交給非相關第三人或廣告贊助商，或者會聲明遵守法律規範與歐盟安全指令，比如按照歐盟安全指令的規範要求資訊的蒐集與應用要在原目的範圍內。但是觀察這個「以公益、展示、散佈、推管、宣傳或經營服務為目的」的授權條款，其範圍之廣能夠讓業者要進行的各種應用授權的商業模式都有可能被解釋符合這個條款，例如我們的主角小吳利用Google Docs編輯的文件、Gmail和Yahoo Mail上的信件內容、附檔和通訊錄、上傳到Yutube的影片和在Flicker上的照片，這些在雲端上進行的內容通通就被授權給了雲端業者；如果本文我們討論的這些內容是用Google Docs來編寫，那麼我們討論多少和撰寫多少的內容，Google就相應取得多少授權；按照這個條款的規定，如果雲端業者將這些取得授權的雲端資料集結成冊另作出版而有營收，也可能被解釋為這些收益將被用作維持原本雲端服務的費用，是在「經營」對使用者「免費」提供的服務。除非這些資料屬於其他資訊主體所有，或是有關健康、金融或兒童等特殊領域的資料，還有HIPPA、HITECH、GLBA和COPPA等我們前面討論過的美國法制上的適用，否則多數使用者自行提供

或上傳到雲上的資料均會受到這個條款的影響而被授權予雲端業者[338]。原本雲端業者就已經在隱私權政策中聲明，會掃瞄和利用使用者資訊作為廣告依據，現在又在這個條款中強制取得使用者資訊的授權，這簡直就是在榨取使用者資訊的剩餘價值。我們原先對於雲端服務「對價」的概念為此有必要作些修正：使用者是以資訊被掃瞄偵知作為廣告依據和讓雲端業者取得資料授權為使用雲端服務的對價。

(4) 雲端業者在隱私權政策中對使用者資料的移轉流通，雖然按我們前面的討論是有許多不足之處，不過多少還有點節制和規範，但對於雲端業者自行使用這些資料，這些服務提供者們就顯得毫不退讓。按照雲端業者的隱私權政策，掃瞄偵知使用者資訊來進行廣告是原本雲端服務的目的與方式之一，但是雲端業者在服務條款中另外聲明取得使用者的授權而可進行其他的資料利用，可見雲端業者不認為這些資料的其他利用是包含在原本服務目的之內。此外觀察「以公益、展示、散佈、推管、宣傳或經營服務為目的」這項條款，可以發現業者對於這些授權資料如何進行應用是相當模糊不清的，不似業者在隱私權政策中直接宣稱資料除在原有服務目的外會明確被用以作為廣告。而且其實雲端業者要求的資料授權到底為何，在業者這類型的條款也看不出各所以然，是要對利用 Google Docs 所編寫的文件、在上傳至 Facebook 的照片，或者是對利用雲端服務創作出的圖形、圖案、造型或影音取得著作權授權上傳？還是取得的是這些圖形、圖案、造型或影音未來可能成為商標或新式樣專利時的授權？亦或是在雲上傳遞資料所包含的營業秘密、交易資訊或金融資訊的分享？還是上述這些都屬於這類型條款所要涵蓋的範圍內？由此可見，這類範圍不明確及解釋適用困難的條款，是雲端業者為

[338] Miranda Mowbray, *supra* note 24, at 141-142 (2009).

了在除利用使用者資料作為廣告用途外的商業模式預作伏筆。

(5) 再者就算是資料被強迫授權予雲端業者，業者要進行超出原本服務目的外的應用，但這也算是業者在利用使用者的資訊，對這種資料的利用亦應享有雲端業者隱私權政策的保護方為合理。不過很遺憾的是業者同樣缺乏對這些授權資料利用的隱私保護進行說明，這種情形將會成為資訊安全上的一大漏洞。而且按照 OECD 保護基準與歐盟安全指令的規範，這種不明確的資料應用處理目的，會讓服務提供者置於資料控制者的角色，但雲端業者又再玩了一次定型化服務條款讓使用者同意的把戲，為將來利用使用者資料的新型態商業模式而產生爭議或進行訴訟時留下相罵本，反正雲端業者爭論失敗時就再藉由擬定定型化條款優勢，如同將廣告也算做服務目的的方式，把這種新型商業模式納入原本的服務目的就好。原本很多人還會擔心雲端資料會被另作利用，不過雲端業者和他們的律師很聰明地告訴使用者不需要再擔心這個問題，因為服務條款就已賦予雲端業者幾無受限的權利，而且使用大眾一經使用或成功申請帳號就同意這些條款而要受其規範。

(6) 尤有甚者，例如Google、Yahoo和Plurk等雲端業者[339]甚至在服務條款中聲明這種授權是一「永久」的權利，這種「永久」權利的聲明會產生兩個問題。首先雖然雲端業者大多會在隱私權政策中聲明賦予使用者永久刪除資料的權利，一但這些資料永久自雲端伺服器刪除後，理論上應當也終止了該資料使用的授權，而且按照OECD保護基準與歐盟安全指令中所揭示的當事人請求及確定資訊凍結權，雲端使用者對於業者應有請求刪除資料及不在利用資料的資訊自決權利，但這種資訊自決概念很明顯抵觸業者要求的「永久」授權，

[339] 參考 Google、Yahoo、Plurk 之服務條款，同註 323 及 324。

不過很遺憾的是主張永久權利的業者大多對此缺乏說明，未來如果因此產生紛爭將可能造成解釋適用上的爭議。其次則是我們之前也曾討論過的問題，當使用者停用雲端服務或業者自行終止服務但雲端伺服器仍保有使用者資料時，這些業者的隱私權政策固然缺乏這種情況下的資料永久刪除條款，現在再加上永久授權條款，是否意謂著服務停用或終止後雲端業者仍享有這些資料內容的使用授權，這與我們一直強調的雲端服務是以利用使用者資料為對價，且服務停用或終止後業者不得在利用與傳遞流通這些資訊的主張背道而馳。當然也是有並無強調永久授權的如Twitter和Xuite等雲端業者[340]，不過這些業者也同樣缺乏授權終止條款及資料永久刪除的隱私權政策。Facebook則是在這個項目上有比較完整且對使用者有利的條款[341]，並聲明在使用者刪除資料與停用帳號時，均終止這些資料對Facebook的授權。

(7) 這些對資料的授權不僅在雲端的一般使用條款中常見，在雲端企業應用中也有可能出現，Amazon和Windows Azure的服務條款[342]同樣也有這種「全球使用、免費及非排他性之權利」的授權條款，Amazon甚至還出現「永久」授權的規定並且沒有任何授權終止條款，僅Windows Azure聲明在使用者刪除雲端資料時終止該項授權，但仍缺乏服務停用或終止後授權終止的條款。這種條款的存在，對於雲端企業用戶而言是非常不利的，企業用戶放在雲上的資料可能具有高度商業機密性，能夠讓雲端業者自行、隨時和任意地使用這些資料，比任意散佈流通這些資料來得更加嚴重。當然這種條款並非不得撤銷或排除，因此雲端企業用戶在與業者協商條款時，必須特別注意

[340] 參考 Twitter 和 Xuite 之服務條款，同註 324。
[341] 參考 Facebook 之服務條款，同註 324。
[342] 參考 Amazon 和 Windows Azure 之服務條款，同註 324。

是否有此類條款的存在，以免未能享受到雲端帶來的優勢，反而造成企業活動與經營佈局受到損失。又或者企業用戶在無法改變必須授權的情況時，有必要藉由多負擔費用等其他方式轉換成授權範圍較小的條款，例如可以參考Yahoo基本的授權條款 [343]與Yahoo 知識加授權條款 [344]就資料內容差異性，轉換為是否為可供Yahoo進行推廣或經營Yahoo奇摩及其相關服務之授權條款，意即企業用戶可以參考Yahoo 知識加的授權條款，就企業特殊資料與一般性資料區別差異性的授權條款。

5. 著作權保護條款

雲端業者除了我們前面提及的，要求使用者不得侵害業者自身的服務、軟體或對其進行逆向工程之外，大多會如 Google、Yahoo 和 Facebook 等雲端業者在服務條款中聲明如若使用者違反國際智慧財產權法(包括美國的數位千禧年著作權法)而有侵害他人著作權情事時，雲端業者有權進行相關處理。這些雲端業者也多會設置侵害著作權處理的相關流程與機制，以供權利人進行檢舉申訴之用。

6. 停用或終止條款

雲端運算服務的終止條款應該包含以下三個部分：

(1) 停用或終止的情況：這是絕大多數雲端業者會在服務條款中制訂的項目，涉及到使用者自行停用服務或雲端業者單方面終止服務的情況 [345]。就雲端一般使用而言，雲端業者多會允許使用者可以隨時停用服務，或者會建立停用及聯絡業者的機制。雲端業者要終止服務

[343] Yahoo 之服務條款，同註 324。
[344] Yahoo 知識加之服務條款，參考 http://tw.knowledge.yahoo.com/info/tos.html.
[345] 參考 Google、Yahoo、Amazon、Windows Azure、Facebook、Twitter、Plurk、Xuite 之服務條款，同註 323 及 324。

時，也會在服務條款中說明是在哪些情況下為之，例如使用者於一定時間未使用服務、使用者為詐欺或違法行為、未依約支付金錢費用、違反服務條款，或依法律規定、法院政府機關命令，或者雲端業者因為各種因素無法繼續該服務的提供、服務內容進行實質變更、服務不再具商業可行性，這些情況中有些是因為使用者自身因素，有些則單方面是雲端業者的商業因素。企業用戶也必須特別注意這些條款，以及雲端服務業者是否有任何隨時終止服務的條款[346]。

(2) 停用或終止後的資料處理：我們最關心的就是服務停用或終止後的資料如何處理，這個議題應該也是資訊安全相當重要的一環[347]，畢竟只要在雲端網路上留下資訊，就很容易被有心人士蒐集和拼湊辨識而出[348]，所以對於雲端網路服務停用或終止後的資料，應該要進行妥適地處理[349]，這是雲端服務提供者不可逃避的責任，也是OECD保護基準與歐盟安全指令中所揭示資訊自決權的重要概念。因此，就如同我們前面所討論，不管是使用者自行停用或雲端業者單方面終止服務時，又或者是使用者自行刪除的資料，這些資料都應被永久刪除而不得進行備份。此外對於自行刪除的資料，以及停用或終止後仍留存在雲端上的資料，業者都應喪失在服務條款中要求使用者對這些資料進行的授權。我們提出的這項議題，不僅雲端一般使用者應該要多加注意，企業用戶在與雲端業者擬定這類條款時更應審慎評估。

(3) 停用或終止後的權利義務：有些雲端業者會聲明服務停用或終止後，該服務條款雖一併終止，但是業者原已享有的權利仍不受終止條款

[346] Robert Gellman, *supra* note 172, at 25.
[347] W. Michael Ryan et al., *Insights into Cloud Computing*, 22 NO. 11 INTELL. PROP. & TECH. L.J. 22, 25-26 (2010).
[348] Robert Sprague, *Cloud Privacy: Normative Standards for Information Privacy Management Within Cloud Computing*, 2010 AAAI Spring Symposium Series 164, 165.
[349] Chris Conley, *The Right to Delete*, 2010 AAAI Spring Symposium Series 53, 54-55.

的影響。這種條款某種程度是為停用或終止後雲端業者仍享有資料的授權建立起權源依據，因此使用者也必須特別留意這類條款。此外這類型條款亦會將準據法和管轄法院延伸至服務停用或終止後的時期，亦應對此留心注意。

7. 責任條款

對於雲端的一般使用，業者在服務條款中所擬定的定型化責任條款，實際上不如說是業者的責任排除、限制和免責條款。在這些條款當中，雲端業者首先會聲明僅根據適用法律而不排除和不限制業者的保證或責任，所以根據適用法所不允許排除的保證、條件，或不允許限制或排除因過失、違約或違反暗示條款之損害，或不允許排除或限制對附隨或衍生性損害之責任，業者才會負起責任或保證。簡言之就是雲端業者聲明只在適用法律內負擔責任或保證，除此之外業者就用此概括條款免除或限制可能須負的責任或保證，並例示其他可能免責或限制的情況。以下我們則整理這些雲端業者例示免責或限制的條款[350]：

(1) 雲端業者可能會聲明在服務正常運作下，使用者必須自行承擔使用服務之風險。

(2) 除了適用法律外，雲端業者多會聲明未對使用者保證服務符合使用者的要求、服務將不中斷且即時、安全、無錯誤，或未聲明保證使用者操作的雲端資訊會準確可靠、使用者採用的各項雲端服務不會出錯或功能瑕疵會獲得改善。這也意即雲端業者不會對服務的可靠度、敏捷性、服務品質、效能及安全性等作出保證，也難怪多數雲端業者僅在隱私權條款中聲明會採取「適當」的資訊隱私保護措施，不願明言到底進行何種保護機制。有鑑於此，企業使用者在採用雲

[350] 參考 Google、Yahoo、Amazon、Windows Azure、Facebook、Twitter、Plurk、Xuite 之服務條款，同註 323 及 324。

端服務前就必須先多方瞭解，以進行適當的評估。

(3) 使用者可能利用雲端服務下載或以其他方式取得非業者之服務或資料，雲端業者多認為這些屬於使用者自己的行為，因此對這些流通資訊的風險不負相關責任。如若使用者透過服務下載或以其他方式取得業者的服務或資料，雲端業者當然必須負擔相關責任。此外，雲端業者也有可能會聲明，雲端服務中進行的廣告，如果像前述夾帶有 Adobe cookie、Beacon 或其他掃瞄工具而造成使用者資訊受到侵害所產生的損失，雲端業者也不負責任。

(4) 使用者利用雲端平台與他人或廣告贊助商進行交易或產生任何法律上關係，而可能導致使用者的損失損害，雲端業者也可能聲明概不負責。對於雲端平台上可能包含他人網路資源的連結，雲端業者也多會聲明不對這些外部資源的安全性及可用性負責[351]。

(5) 另外，不論基於任何原因或責任理論下，由使用者行為所發生的直接、間接、特殊、衍生性或懲罰性損害、直接或間接的利益損失、商譽或業務聲譽損失、任何資料損失、替代物品、服務購置費用或其他有形無形損失，雲端業者和其相關企業可能會聲明均不對此負責任[352]。這種責任條款的出現顯露出雲端業者企圖要面面俱到免除責任，如果是因為使用者故意或過失行為導致這些損失損害，業者不負責任即為在理。但如若在正常使用情況下發生的這些損失損害，在法制健全與法理完善的管轄區域均有很大可能會歸責於提供雲端服務的業者，更何況現今這些大型美國雲端業者多選擇加州或華盛頓等州為適用法及管轄法院[353]，難道這些州的適用法律及法院會容許雲端業者如此隨便免除責任？再者，前述的概括條款已聲明在適

[351] 同上註。
[352] 參考 Google 之服務條款，同註 323。
[353] 參考 Google、Yahoo 及 Facebook 之服務條款，同註 323 及 324。

用法律內會負擔責任或保證，這種不區分原因的不負擔責任條款很可能會和適用法律的規定相抵觸而無效，那麼雲端業者制訂這種條款豈不矛盾，或者是心存訴訟或法律上的僥倖，無怪乎EPIC批評這些雲端業者正在進行不誠實及詐欺的商業行為[354]。

(6) 雲端業者多會在前述的服務條款或隱私權政策中聲明，希望使用者能提供準確的個人帳戶資料，以及確實妥善保管帳號密碼或對雲端資料進行保密，因此而產生的損失損害，雲端業者也會聲明概不負責[355]。

(7) 對於雲端技術資訊的部分，雲端業者通常會聲明對於服務的變更、升級、為暫時或永久停止服務進行的變更，或者雲端上流通、維持或傳輸的任何內容資訊，或對資料的刪除、毀壞或未予儲存，所造成使用者的損失損害，雲端業者均不負責[356]。這也意謂著 2011 年 3 月Gmail遺失 15 萬用戶的信件內容資料[357]，這些使用者按照服務條款將很難要求Google負起損失損害的賠償責任。

上述這些對於一般雲端使用的免責或限制條款，對於雲端企業用戶仍就有可能出現。企業用戶當然可以藉由與業者協商時，要求雲端服務內容不會出現使用目的以外的廣告、他人資訊或連結，而不會發生與廣告贊助商或他人間交易或連結安全性的問題。但是企業用戶仍必須注意到兩項責任條款，首先是企業用戶在服務正常運作及正常使用時產生的損失損害，對於何種正常情況時須要歸責於雲端業者，企業用戶有必要預先要求釐清，以避免前述法律規定、概括條款和免責條款衝突矛盾時解釋適用上的爭議。其次則是在雲端服務失靈或中斷時，如何界定雲端業者的責任。如果是在契約或服務條款未另有規定的情況下，雲端業者的故

354 EPIC, *supra* note 41.

355 參考 Google、Yahoo、Amazon、Windows Azure、Facebook、Twitter、Plurk、Xuite 之服務條款，同註 313 及 314。

356 同上註。

357 陳炳宏，同註 121。

意或過失導致服務的失靈或中斷，業者當然需要對使用者的損失負責，縱使未造成使用者任何損失，亦有不完全給付的相關責任[358]。不過實際上我們都知道透過契約可以排除業者的部分責任，上述對一般使用的條款就是其例，就算是Google、Yahoo、IBM、Amazon或Microsoft等跨國大型科技業者針對中小型企業用戶制訂的服務條款可能也不例外，因此缺乏談判能力的企業用戶除了必須瞭解業者的隱私政策與使用條款，知道雲端業者對那些責任作出限制，還要就雲端服務的安全性、服務品質和效能事先進行評估。另外就算可以透過契約或服務條款規範增加雲端業者的責任，但是實際上作為新興產業的雲端運算服務，還是有許多技術上的問題或其他因素會導致服務失靈或中斷，這種情形恐怕就很難進行責任的歸責。因此有學者提出建議採用記帳制度(credit system)[359]，例如雙方約定服務在線的時間是每月可運作時間的 99.95%，不足的時數將在費用上有相對應的折扣。但是這種方式可能產生兩個問題，首先是服務中斷失靈不見得是來自於技術上的問題，有可能是因為電力短缺、網路線路中斷、戰爭、天然災害等不可抗力因素，而有預先排除的必要；其次則是對於有些企業使用者而言，服務中斷失靈造成的損失遠比折扣的費用還少，例如對於醫療院所的雲端用戶，服務中斷失靈可能導致病患健康權益受損或甚至死亡，而使這些用戶面臨昂貴的賠償及醫療訴訟，因此對於這類型的雲端使用者實際上需要的是備用或應急措施[360]，所以除了事前必須進行詳細的雲端服務評估外，還要與雲端業者協商預先建立備用措施及如何對鉅額損失的賠償進行平衡，或者甚至是要導入保險理賠的機制，將保險業者納入雲端運算的體系中，就如同產業界因應可能停水停電的情形而投保的企業財產保險，而來平衡使用雲端服務可能的風險。

[358] Davide M. Parrilli, *supra* note 320 at 109.
[359] *Id* at 110.
[360] *Id* at 111.

8. 條款變更

就如同前面所言，雲端業者有可能像修改隱私權政策般，保有隨時對服務條款進行修改的權利，業者同時也會聲明進行修改時可能不會通知使用者，或者僅是在網頁或服務介面中進行公告。有些較有良心的業者會聲明在條款修改後使用者再使用或再登入服務時，就視為接受更新的條款，而非一經修改就迫使使用者同意新條款。對於這類型的條款，我們同樣認為對使用者是相當不合理的，並且懷疑這類條款是否能夠通過某些準據法的檢驗，而有被宣告無效的可能。因此我們認為雲端業者變更條款時不僅應該通知使用者，並且在有重大變更時要特別標示出來，或者設計「Click 確認鍵」讓使用者能夠知悉並確認已瞭解重大變更，以及建立讓使用者不同意時的退場機制，包括服務停用、使用者資料刪除及資料授權停止等措施。至於雲端企業用戶是否會出現單方變更條款，雖然端視商業經濟談判力的強弱，但是企業用戶仍必須特別注意是否有條款變更後的通知條款或適當的退場機制。

9. 其他條款

除了上述條款之外，雲端服務條款也會有些常見的契約條款：

(1) 目前多數大型的雲端業者多屬美國公司，因此提供的隱私權政策與服務條款均是以英文撰寫，少數如Google會提供中文版譯文，亦會聲明使用者與Google間之關係以英文版本為主[361]。

(2) 正如本節我們一開始所提到，雲端業者多會在服務條款中載明遵照隱私權政策的內容進行資料保護，因此隱私權政策可視為服務條款或雲端契約的一部分。

(3) 雲端平台標榜的就是內容豐富，可以讓使用者享受到各種網路服務，

[361] 參考 Google 之服務條款，同註 323。

因此有時使用者可能使用到其他人提供的服務或購買他人之商品，雲端業者對此通常會聲明使用者與他人之間應依其條款辦理，雲端業者的服務條款不影響使用者與該他人間的法律關係。

(4) 契約條款通常會載明準據法與專屬管轄，雲端運算契約或服務條款亦不例外。例如 Google 及 Fcebook 採用加州法律為準據法及加州聖克拉拉郡為管轄法院、Yahoo 及 Xuite 採用中華民國法律為準據法及台北地院為第一審管轄法院、Twitter 採用加州法律為準據法及舊金山法院為管轄法院、Amazon 則採用華盛頓州為準據法及管轄法院。

第三項　小結

對於雲端服務條款的討論，我們同樣大致分成企業使用與一般使用的兩種模式進行。在雲端運算的一般使用中，業者藉由定型化條款的規定，讓使用者一經使用或申請帳號即同意條款的方式，並在條款中加入許多對使用者不利的規定，例如可任意變動服務內容及服務條款、強制使用者對資料內容進行不公平的授權、太過廣泛的免除責任條款、缺乏停用或終止後資料如何刪除及授權是否終止的條款等。此外檢討這些雲端服務條款後我們赫然發現，使用者利用雲端服務的對價，不僅是讓業者取得檢索資料作為廣告的權利，還讓業者取得幾無不受限制的資料授權，這兩樣雲端服務的對價，涵蓋既有的和未來任何雲端業者想要發展的商業模式。

雲端時代依靠網路來流通和處理資訊，但不可否認相關技術未臻成熟的階段，因而產生許多系統上的失靈、漏洞、或讓有心人士進行未經授權的資訊接觸等情況，但是根據我們上述的討論可以發現，雲端業者不僅不見得在努力防止這些危害，在服務條款的制訂上甚至助長資訊安全漏洞的

擴大，例如業者僅在隱私權政策中聲明採取「適當」的保護措施，卻不願在服務條款中承擔資訊安全漏洞的責任，這不啻使雲端業者缺乏誘因與動力採用及研發更安全的保護機制。此外，這些業者還藉由定型化條款強制使用者進行授權目的及對象不明確的資料授權，不僅讓使用者無法評估資訊被流通與被應用的風險，更讓使用者完全喪失對資訊的掌控。尤有甚者，業者也缺乏服務終止中斷後資料如何永久刪除及停止授權的聲明，這將使得後續資料如何保存或者如何被應用相當的不明確，亦將造成這些資訊長期處於不確定的危險狀態。我們討論的這些條款除了出現在一般雲端使用的定型化契約外，也有可能會出現在與企業用戶的約款之中，如此將使得資訊缺乏保障，並使得企業用戶無法確實掌握資訊的安全性，這種情況導致的資訊安全事故往往會對商業經營產生重大影響，因此企業用戶也要特別注意服務條款中是否有出現這類致企業於不利地位的規定。

第三節　企業使用雲端服務應進行的步驟

本節我們主要說明雲端企業用戶在選用雲端服務時應有的程序，這些程序項目也可作為一般使用者要進行付費服務時的參考。對於雲端企業用戶而言，最重要的就是確保使用、終止或中斷服務時資料的完整、安全、機密、可用性等項目，要盡可能使上了雲端的資料更能夠掌控及獲得更多安全保障，因此企業用戶必須進行事前查核、契約談判、合約管理及服務終結處理等步驟[362]。

1. 事前查核(pre-contract due diligence)

企業用戶在選用雲端服務前，必須先進行相關的評估，這些評估程

[362] Francoise Gilbert, *supra* note 184, at 20.

序可分成內部查核(internal due diligence)及外部查核(external due diligence)。所謂的內部查核係指使用者必須考量自身的狀況，首先必須了解自己的資料是屬於哪種類型，例如是否涉及金融、健康或兒童等資料，又或者這些資料是否有相關規定應予遵守，這些特殊類型資料對於雲端服務的選用、資料的移轉及後續管理有相當大的影響。其次則是要考量自身對服務的需求，需要何種雲端服務內容，是否要選用 SaaS 或其他哪種類型的雲端服務等。外部查核則係指對於所挑選的雲端服務進行評估，需要評估我們在第二章中所提及的雲端彈性、可靠度、敏捷性、適應性、可用度及服務品質，以及最重要的雲端服務的安全機制等項目。

2. 契約談判

對於雲端服務條款和隱私權政策等相關問題，前面我們已經多有討論，在企業用戶與雲端業者磋商進行談判時，需要瞭解是否有這些條款的存在，並避免不利條款的出現。但如果談判能力差距過大，或者是對中小企業用的定型化約款，這些企業用戶也要注意是否能夠避免將機密資料流傳至雲端而產生不利商業經營的安全性漏洞，這種情形也必須納入事前查核及評估的項目中。

3. 合約管理

雲端企業用戶在合約條款簽訂，開始享受雲端服務後，也要隨時注意、監管、測試及評估服務內容是否符合契約要求，資料保護措施是否持續運作等。這些監督管理步驟也有可能受到法律的規範，例如美國 GLBA 法案就要求金融機關委外處理資訊或利用金融雲時，必須隨時監督金融資訊的安全措施是否確實履行。

4. 資料終結處理

就如我們前面所述，雲端服務會因為各種原因終止或中斷，這時對企業用戶而言最要的是如何追究雲上資料的後續處理，因此在契約談判時必須注意是否有相關條款，服務停用或終止時也須確實監督雲端業者履行對資料後續的相關處理。

第四節　本章小結

在本文前面的部分中，我們說明了雲端資訊安全風險發生的原因，有些是雲端平台或雲端的特性使然，但更多的則是雲端網路業者的自身行為及商業模式或服務內容提供者所造成的，例如Facebook Beacon的爭議，Quantcast和Clearspring等線上廣告業者就雲端廣告安置夾帶的Flash cookie、Beacon、AddThis等其他監測工具，亦或者類似EPIC指控Google未對使用者帳號密碼進行加密措施等。在其後的篇幅，我們也討論了美國法及各國際公約對雲端資訊安全的保障，及對雲端業者應有的限制。但是經由本章的討論，我們可以發現這些提供雲端服務的業者藉由定型化的約款來迫使一般使用者放棄該有的權利，例如讓使用者同意業者可以擅自變更雲端隱私政策與服務條款而放棄與之協商的權利等。此外業者也藉由這些約款調整雙方的權利義務，例如讓使用者接受廣告為服務的一部份、讓使用者同意範圍過廣的資料流通對象，甚至讓使用者同意幾無保障的免責條款。更讓人氣結的是，雲端業者對使用者吃盡了豆腐後，還要在這些約款中要求使用者幾無限制的資料內容授權。更好笑的是，雲端業者已經在這些條款中用模糊及範圍不確定的條文，來為其資料不明確目的的蒐集、處理、應用、散佈和分享打了預防針之外，還有些雲端業者會在條款中加入「如果

此資訊的使用方式與當初收集目的不同，我們會在使用前先徵求您的同意」這樣的約定[363]，這簡直是在欺負不懂法律或條款文義的使用者。本章最後我們也藉由對這些對雲端一般使用服務條款的討論，提醒企業用戶在與雲端服務提供的業者磋商時應該注意的事項。

那為何提供雲端服務的業者要制訂這些不公平，甚至通不過歐盟安全指令與法院檢驗的條款？其實雲端業者的目的就在於要廣泛的掌握使用者資訊，瞄準龐大的針對性精準廣告商機。根據前述eMarketer的預估[364]，2011 年排名前 3 名的網路和雲端服務業者Google、Yahoo和Facebook的線上廣告收益分別將達到 12.39 億、3.40 億及 2.19 億美元，而且這塊線上廣告的市場還在不斷成長當中，因此雲端業者更有誘因去開發出更多可能侵害使用者資訊隱私的廣告商業模式。我們從前述的隱私權政策和服務條款的討論就可發覺，這些業者們經由訴訟和解的經驗也不斷在進步，不過不是朝向更保護資訊隱私的方向前進，而是在隱私政策和服務條款中不斷面面俱到地擴大業者的權利，一來直接藉由定型化約款讓使用者同意給予雲端業者掃瞄資訊進行廣告的權限，以符合歐盟安全指令和美國法上就資料控制處理目的同意的規範，二來又讓使用者同意業者能夠不對雲端服務品質和安全性負最起碼的保證責任。尤有甚者，雲端業者為了將來各種可能商業模式的發展，還讓使用者同意賦予業者幾乎不受限制的資料授權，可見業者是多麼企圖要挖掘使用者資訊做廣告外的其他剩餘價值。

2010 年起茉莉花革命藉由網路雲端的串連，在中東地區造成巨大影響，讓各國政府見識到網路世界的威力，也讓諸多獨裁體制的國家體認到有必要掌控人民在網路上的言論，甚至進而掌握人民在雲端上的資訊。所幸身在民主國家的我們，還有民主的機制來制衡政府，而且對於是否要讓公部門掌握個人資訊時我們總是戒慎恐懼，害怕國家力量會不受控制而剝奪人

[363] 參考 Google 的隱私權政策，同註 323。
[364] eMarketer, *supra* note 288.

民的隱私基本權利[365]。不過絕大多數的網路或雲端使用者在面對私部門可能侵害隱私時總是漫不經心，再加上「免費」使用雲端服務確實讓人感受到科技帶來的便利，但卻在不知不覺之中失去對雲端資料的控制，而讓個人輪廓和內心最深沈的心靈活動被雲端業者及有心人士掌控。「免費」的服務並不一定真的免費，其代價有可能才是最「昂貴」的！

[365] 陳起行，同註 141，頁 323。

第六章　我國法制對雲端運算條款的檢討

雲端時代最大的特性就是藉由網路動態調整與串連伺服器及使用者，並以此來流通處理資訊，讓使用者可以隨時運用各種雲端資源。但這意謂著使用者有大量的資訊存放在雲端伺服器上，使用者不再能夠完全掌控這些資訊，這些資訊的流向和處理幾乎取決於雲端服務提供者或雲端業者的態度。在前面的章節我們先討論了美國法上對雲端時代可資參照的法律規定，及國際間以歐盟資料安全指令為主的協定，藉由這些規範來分析雲端運算的隱私權政策與服務條款，並且從中發現許多對使用者不公平的條款。至於在我國法制中，則有新修正的個人資料保護法(下稱個資法)規範個人資料之蒐集、處理及利用，作為雲端運算時代資料運作處理的重要規範。雲端運算作為目前資訊時代最熱門的話題，是種以提供各種雲端服務供使用者利用的商業模式，因此構成使用者利用雲端服務的消費關係，而有消費者保護法(下稱消保法)的適用，提供雲端服務的業者所提出的隱私政策與服務條款必須通過我國消保法的檢驗。在本章中我們將探討在我國消費者保護法及個人資料保護法的體制下，如何界定雲端業者與使用者間的法律關係，以及這些條款的適法性問題。

第一節　消費者保護法對雲端條款的檢討

如同我們在第二章對雲端運算所下的定義，雲端運算可謂是一種使用彈性方便的網路資源與計時量付費的網路服務模式，提供雲端服務的業者能動態快速調整運算資源，使用者則根據需求並透過網路來接受不同的服務內容。以下我們按照消保法保護消費者的各項重要概念，來分析前章所

討論的雲端運算隱私權政策與服務條款：

1. 提供雲端服務的業者與使用者構成消保法上之消費者及企業經營者

消保法上所稱之消費者，根據消保法第 2 條第 1 款[366]的定義，係指以消費為目的而交易、使用商品或接受服務者。像我們的主角小吳使用Facebook就是用來和好友們互動聯絡感情，使用Google Docs就是要用來編寫文件，雲端時代最顯著的現象就是像小吳這樣為數眾多的雲端使用者透過網路或通訊裝置接受各種雲端服務，因此像小吳一樣的雲端一般使用者就是受到消保法所保護之消費者。至於有無支付對價，不論是有償或無償接受服務，並非決定是否成為消費者之因素[367]，何況經由我們前面的討論，我們也不認為雲端一般使用者是無償在接受雲端服務。同理，另外根據消保法第 2 條第 2 款[368]的定義，像Google及Facebook這類向小吳提供雲端一般服務的業者屬於消保法中須要受到規範的企業經營者。

一般討論消費者保護時，大多將重點放在自然人，但是消費者是否僅限於自然人或應否包括其他法人等企業經營者，則可能產生疑問。我國通說認為由於消保法並未對消費者限制為自然人，因此只要是以消費為目的而非供轉售或製造用途而係自用時，這些企業經營者所購買的商品或服務仍屬消費關係[369]，因此像小吳所屬公司這類的企業用戶使用Openfind的MailASP系統、Amazon的EC2 和S3 服務或Windows Azure服務時就屬消費者，而提供服務的Amazon或Windows等業者則屬企業經營者。不過按照通說見解，基於企業經營者基於轉售或其他目的所為購

366 消保法第 2 條第 1 款：「消費者：係指以消費為目的而為交易、使用或接受服務者。」

367 馮震宇、謝穎青、姜志俊、姜炳俊合著，消費者保護法解讀，2005 年 5 月，頁 15。

368 消保法第 2 條第 2 款：「企業經營者：指以設計、生產、製造、輸入、經銷商或提供服務為營業者。」

369 馮震宇等，同註 367，頁 16；黃立，消費者保護法：第四講 消保法的定型化契約條款(一)，月旦法學教室，14 期，2004 年 1 月，頁 99。

買商品或接受服務時，不屬消保法所稱之消費者[370]，因此像Animoto利用Facebook Platform上的元件創作出受人歡迎的視頻軟體，這類型的企業經營者利用雲端資源再開發出可供下游雲端使用者利用的服務，即符合通說見解中再為製造的其他目的要件，而不屬消保法保護的範疇。

2. 雲端隱私政策與服務條款屬定型化契約條款

依據消保法第 2 條第 7 款及第 9 款對定型化契約及條款的定義，定型化契約條款是企業經營者所提出單方預先擬定且為與不特定多數人訂立同類契約之用而擬訂之契約條款，不論是以書面、放映字幕、張貼、牌示、網際網路或其他方法表示，均屬之。

根據我們前面章節的討論，雲端運算的一般使用是建立在對使用者進行廣告的商業模式上，提供雲端服務的業者因而會需要大量的使用者來加入該雲端平台，以擴大線上廣告的利基。此外，雲端業者也會藉由網頁來揭示隱私政策與服務條款，並以此界定與使用者間的法律關係，而且雲端業者對於一般使用者也僅願意依此條款訂約。如同我們前面所討論的 Facebook 和 Google 等幾個訴訟或和解案例，一般使用者或隱私保護團體除非對這些雲端業者興訴或者訴諸輿論壓力，否則一般的雲端使用者只能依這些定型化契約條款，選擇訂立或不訂立，以及選擇其他的雲端應用服務，而不能決定這些條款的內容。因此這些條款即屬於雲端業者單方預先擬定來與不特定多數使用者間的定型化契約條款。

至於雲端的企業應用而言，我們前面也曾討論過目前的雲端服務產業是像 Google、Amazon 和 Windows 這類的大型業者在主導市場，除非也是同等具有經濟談判實力的企業使用者，否則對於眾多中小型的企業用戶還是會受制於這些大型雲端業者的約款內容，就以前章我們所討

[370] 同上註。

論到的 Amazon 和 Windows Azure 條款為例，對中小型企業用戶而言還是屬於消保法上所謂的定型化契約條款。

3. 雲端服務條款之解釋

企業經營者所使用的定型化契約條款，應該讓平均水準的顧客能夠瞭解，而這種認定標準應以未受法律訓練的平均水準顧客，對條款的認知無待律師或其他法律顧問的協助即可瞭解為準[371]。因此，企業經營者制訂的定型化約款應盡可能避免使用艱深的法律專有名詞，並宜明確分段，結構清晰，且配置適當之標題以協助瞭解[372]。如果企業經營者有使用模糊字眼時，依照消保法第 11 條第 2 項[373]之規定應朝向有利於消費者作解釋，企業經營者如故意對特定事項，多次重複規定，卻將關鍵字句隱藏在契約款中時，亦應有消保法該條規定之適用[374]。雲端服務業者所揭示的隱私權政策和服務條款等定型化契約條款，同樣有該規定之適用。我們以Google目前的服務條款為例[375]，Google在該條款的第 14 條保證排除及第 15 條責任限制當中，用了許多否定或雙重否定的字眼，來表示Google不願對使用者做出任何保證或聲明，只不過Google這種聲明的前提是建立在第 14 條一開始宣稱的「不排除或限制Google根據適用法律不得合法排除或限制之損失保證或責任」，這種條款的敘述方式過於零碎且結構不清晰明確，而且運用許多曖昧模糊的字眼，將使得Google的損賠責任不易明確，如果在適用我國準據法的情況下，這類型的條款應該要朝有利於雲端使用者的方向解釋。

4. 雲端服務業者的責任

[371] 黃立，消費者保護法：第五講 消保法的定型化契約條款(二)，月旦法學教室，15 期，2004 年 2 月，頁 76。
[372] 黃立，同前註，頁 76。
[373] 消保法第 11 條第 2 項：「定型化契約條款如有疑義時，應為有利於消費者之解釋。」
[374] 黃立，同註 369，頁 77。
[375] 參考 Google 服務條款，同註 323。

消保法中針對企業經營者責任最重要的條文就是第七條有關商品與服務之無過失責任規定[376]，因此所有商品製造人與服務提供人，在無法確保該商品或服務符合可合理期待的安全情況下，都要負起無過失的損害賠償責任。不過該條規定亦有但書，企業經營者可以確保其所提供之商品或服務，符合當時可合理期待之安全性，因此企業經營者應盡善良管理人之注意義務，而就當時科技或專業水準可得知或可預見之危險加以避免，非指企業經營者應負絕對的責任而言[377]，可謂商品無過失責任的衡平[378]。

雲端運算是雲端業者透過網路向使用大眾提供各種服務資源，行政院主計處也將提供網路資訊處理或服務的業者納入服務業中[379]，因此這些業者是為該條提供服務之企業經營者。學說和消保法立法過程中雖有討論服務業是否適用無過失責任的爭議，但這些反對將服務業納入無過失責任體系者多為醫師、律師或會計師等專業團體[380]，現今的雲端運算商業模式是向不特定多數的使用大眾廣泛性的提供，而且參照這些雲端業者的條款，還帶有過去套裝軟體授權的概念，是授權使用者使用這些雲端服務，因此就現行我國消保法的規定而言，這些提供雲端服務的業者應負無過失責任。

因此以約定準據法為我國法的Yahoo條款為例[381]，Yahoo在第8條：「…Yahoo!奇摩對於您因使用（或無法使用）本服務而造成的損害，除故意或重大過失外，不負任何賠償責任。」，以及第13條：「您明確了

[376] 消保法第7條：「從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性(第一項)。商品或服務具有危害消費者生命、身體、健康、財產之可能者，應於明顯處為警告標示及緊急處理危險之方法 (第二項)。企業經營者違反前二項規定，致生損害於消費者或第三人時，應負連帶賠償責任。但企業經營者能證明其無過失者，法院得減輕其賠償責任 (第三項) 。」

[377] 馮震宇等，同註367，頁25。

[378] 王澤鑑，侵權行為法第二冊 特殊侵權行為，2006年7月，頁317。

[379] 行政院主計處，中華民國行業標準分類(第9次修訂)，參考 http://www.stat.gov.tw/ct.asp?xItem=28854&ctNode=1309

[380] 馮震宇等，同註367，頁38-39。

[381] 參考 Yahoo 服務條款，同註324。

解並同意： Yahoo!奇摩對本服務及軟體不提供任何明示或默示的擔保，包含但不限於權利完整、商業適售性、特定目的之適用性及未侵害他人權利。本服務及軟體乃依其「現狀」及「提供使用時」之基礎提供，您使用本服務及軟體時，須自行承擔相關風險。...」Yahoo在這兩條定型化契約條款中以讓使用者同意的方式限縮了Yahoo的責任範圍，但按消保法第 1 條之立法目的在於保護消費者權益，而其中最能體現該意旨的條文即立法者特別制訂的企業經營者的無過失責任，因此消保法第七條之規定應屬民法第 71 條之強制或禁止規定，像Yahoo這類的雲端業者以定型化契約讓使用者同意並且排除無過失責任損害賠償的條款，應屬無效。

消保法第 7 條的無過失責任看似對雲端使用者非常有利，但實際上在操作時仍會有許多窒礙難行之處。由於消保法並未對企業經營者損害賠償的成立要件加以規定，因此要回歸到民法損害賠償的要件[382]：(1)必須有損害；(2)須具有歸責原因；(3)二者間具有因果關係之存在。以本文我們一直強調的雲端資訊安全為例，使用者因為雲端資訊外洩而確認有財產上的損失，但必須證明財產上的損失與雲端業者間具有歸責原因。主觀上故意或過失的歸責原因有消保法上無過失責任的立法，使用者不需要去證明雲端業者有無故意或過失[383]。不過對於客觀的歸責原因，使用者必須去證明雲端業者對於雲端資訊的處理存有瑕疵、安全上的漏洞或者其他可歸責於業者的因素而導致資訊的外洩。實則在雲端時代中，按照消保法與我國法制下這種舉證方式已經是在要求使用者去檢討與提出雲端運算服務技術上的缺失，對於資力平常又不具備資訊科學專門知識的一般使用者而言，幾乎無舉證的可能性，而且實際上我們前述的EPIC隱私保護團體就曾發現Google曾經僅用未經加密的文件檔在

[382] 馮震宇等，同註 367，頁 157。
[383] 同上註，頁 159。

傳輸使用者的資訊[384]，可見雲端業者提供的服務本身確實存有安全性漏洞的可能。

雖然按照消保法第 7 條之 1 第 1 項的規定，這些企業經營者可以主張所建構的安全機制符合當時的科技或專業水準，並且賦予企業經營者就科技或專業水準可合理期待之安全性的舉證責任，但該規定是在讓企業經營者能夠阻卻無過失的主觀歸責原因[385]，我國消保實務上確實也少有企業經營者主張該條成立者。不過該規定對於消費者有利之處，是在於客觀歸責原因事實明確的消保案件中無庸再去舉證企業經營者的主觀歸責原因，但對於像雲端時代的各種資訊洩漏或帳號被盜事件，使用者是透過各種裝置連結網路享受雲端服務，雲端業者很容易就能找到理由抗辯使用者是在其他環節產生資安外洩，例如網路傳輸部分遭到侵入或者使用者自己的電腦遭安裝有木馬程式等[386]，使用者與業者將在雲端與網路資訊技術舉證間進行攻防，最終雲端使用者也還是必須去證明資料外洩是源自於業者的安全性問題或其他可歸責於業者的事由。

實際上，我們也承認雲端時代資訊的流通有多個環節需要重視，使用者資訊會遭到外洩不見得在客觀上可歸責於雲端業者。但是按照消保法第 7 條及第 7 條之一的立法目的，立法者是希望企業經營者能盡最大努力提供消費者符合當時科技或專業水準的商品及服務。因此在雲端時代中，由於使用者必須負擔沈重的客觀歸責原因舉證責任，提供服務的雲端業者就有必要本於誠實信用原則，在隱私權政策及服務條款中說明進行哪些安全機制，而非僅用「適當」、「符合現狀」或「符合當時科技水準」等詞句宣示會保障使用者的資訊安全，甚或還在責任條款中以定型化約款的形式免除責任。縱使雲端使用者在面對這類資安事件時可依消保法第 49 條之規定集合眾多雲端消費者提起團體訴訟，以眾多小蝦

384 EPIC, *supra* note 41.
385 馮震宇等，同註 367，頁 98。
386 行政院研考會委託研究報告，同註 226，頁 274。

米之力對抗大鯨魚，或許能找到熟習雲端資訊安全技術人士或關心資安團體的助力，但仍舊必須得面對嚴格的舉證責任問題。

5. 定型化契約條款之無效

定型化契約條款應本於消保法第 11 條第 1 項[387]所揭示之平等互惠原則，第 12 條第 1 項[388]進一步規定違反誠信原則而對消費者顯失公平之定型化契約條款無效，作為我國消保制度對定型化契約的審查依據。消保法第 12 條第 2 項[389]則規定違反平等互惠原則等三種定型化契約推定顯失公平的情況，另外在消保法施行細則第 13 條[390]則規定對判斷是否違反誠信原則之定型化條款所應考量的因素，細則第 14 條[391]亦明確規定四種顯屬違反平等互惠原則之情事。因此審查定型化契約條款效力時，宜先以消保法第 12 條第 2 項為標準，符合第 2 項規定之情形即可推定該定型化條款顯失公平而無效，這當中最常用的又是可參照細則第 14 條所規定四種違反平等互惠原則之情形，否則仍應依消保法第 12 條第 1 項所規定誠信原則的抽象裁量標準[392]。

根據我們前面就雲端隱私政策與服務條款的討論，除了前述雲端業者不願意公開說明進行哪些安全保護機制和過渡免除責任的條款外，雲端時代對使用者產生的最大不安全感來自於無法掌握雲端業者對資訊的如何處理與流向。雲端運算固然帶來便利，但這些便利的因素背後來自於消費者負擔了不能控制資訊的風險，這就必須透過業者的隱私政策

[387] 消保法第 11 條第 1 項：「企業經營者在定型化契約中所用之條款，應本平等互惠之原則。」
[388] 消保法第 12 條第 1 項：「定型化契約中之條款違反誠信原則，對消費者顯失公平者，無效。」
[389] 消保法第 12 條第 2 項：「定型化契約中之條款有下列情形之一者，推定其顯失公平：一、違反平等互惠原則者。二、條款與其所排除不予適用之任意規定之立法意旨顯相矛盾者。三、契約之主要權利或義務，因受條款之限制，致契約之目的難以達成者。」
[390] 消保法施行細則第 13 條：「定型化契約條款是否違反誠信原則，對消費者顯失公平，應斟酌契約之性質、締約目的、全部條款內容、交易習慣及其他情事判斷之。」
[391] 消保法施行細則第 14 條：「定型化契約條款，有下列情事之一者，為違反平等互惠原則：一、當事人間之給付與對待給付顯不相當者。二、消費者應負擔非其所能控制之危險者。三、消費者違約時，應負擔顯不相當之賠償責任者。四、其他顯有不利於消費者之情形者。」
[392] 馮震宇等，同註 367，頁 116。

與服務條款來消除使用者的疑慮。因此，按照消保法與施行細則的規定，雲端業者的定型化條款必須盡可能消除雲端消費使用者所不能控制的資訊風險，也就是必須在條款中明確說明資訊的處理目的，讓使用者瞭解資訊如何被處理及應用，這也是歐盟安全指令和 APEC 隱私權保護原則中相當重要的核心意旨，下節我們將談到的我國個人資料保護法亦有相關規範，在前面的討論中我們也還主張同樣要將雲端資訊流通範圍明確性納入這種概念之中。

但是經過前章對這些條款的分析，我們發現雲端業不僅沒有藉這些條款減輕使用者的疑慮，反而加重了使用者所不能控制的資訊風險。首先是提供服務的業者要求使用者對上傳至雲端的個人資料和內容進行授權，不過雲端業者卻僅是用很概括的條款，但卻不明確說明這些授權內容的用途為何；業者藉由定型化約款讓使用者對資訊進行授權，授權了的資訊內容還是屬於使用者的資訊，應該也同樣要受到歐盟安全指令資訊處理明確性的規範。其次雲端業者也藉由這些定型化條款，讓使用者同意業者將這些資訊流通給與雲端業者有關之其他第三人，這種流通條款的範圍亦如我們前面所論的過於廣泛而且不明確，而雲端業者就資訊的再流通必有其應用或利用目的，因此流通範圍的不明確也意即對資訊處理的不明確，這類型條款同樣也違反歐盟安全指令資訊處理明確性的規範。

按照歐盟安全指令等國際規範就資料蒐集及利用明確性的概念，其目的在於讓資料主體或使用服務者能瞭解資料是如何被蒐集與利用，也藉由讓資料主體或使用服務者瞭解蒐集與被利用的目的、範圍及其影響為何，讓資料主體或使用服務者能夠參與並評估資料被蒐集與處理所帶來的效益及風險。但是我們前述討論到的這兩個散佈流通範圍及授權目的不明確的定型化契約條款，無法讓雲端使用者瞭解其資訊被作何利用、

範圍及其影響為何，因此我們認為這些條款將增加使用者利用雲端服務時的風險。雲端業者藉由定型化契約讓使用者同意這兩個條款，就是讓使用者必須額外承受所能控制範圍外的資訊安全風險，是違反消保法施行細則第 14 條第 2 款不得讓消費者負擔非其所能控制危險之規定，這些條款也因而違反消保法平等互惠原則而會失其效力。

此外，我們前述討論亦提到有些雲端業者會要求使用者對資料內容進行「永久」的授權，這種永久授權的條款也與我們前述認為使用者被迫進行授權時應有時間限制的主張背道而馳，這種永久授權的條款可能也通不過消保法施行細則第 14 條第 1 項給付與對待給付顯不相當的檢驗，而違反消保法所揭示的平等互惠原則。

6. 雲端條款的任意變更

雲端服務變化快速，雲端業者隨時能透過網路向使用者傳送或更新成最新的服務，業者們常需要根據服務變更而隨時修改雲端隱私政策或服務條款，因而會在與使用者的定型化契約中約定隨時保有修改的權利，甚至也可能聲明條款進行修改時可能不會通知使用者。但在民事交易中，訂約雙方以條款約定彼此間的權利義務，在訂約後如欲變更法律關係則應得對方之同意，此為我國民事法律的基本法理。因此雲端業者以定型化契約條款預先排除使用者可與之協商改變條款的權利，除了違反消保法平等互惠原則之外，也違反民法第 247 條之 1 第 3 款不得預先使他方當事人拋棄權利之規定。

但雲端網路時代，資訊技術日新月異，雲端業者在提升服務的同時，可能也要對這些約款進行調整，要雲端業者寧可遵照法律規定不得任意更改條款也不提供更新的服務，實則是在開雲端網路發展之倒車。消費者保護委員會基於網路世界的快速變遷，在線上遊戲定型化契約範本第

24 條[393]的規定中容許企業經營者能夠修改定型化約款，但是賦予企業經營者必須公告或通知消費者的義務，未公告或通知消費者時該變更的條款無效，並且賦予消費者 15 天的猶豫期間(超過 15 天未為通知企業經營者反對即視為接受條款變更)，以及賦予消費者能夠反對該條款變更而終止契約的權利。線上遊戲同樣是遊戲業者透過網路傳遞服務的模式，按照消保會就該定型化契約範本的意旨，雲端或網路業者並非不得保留隨時變更條款的權利，而是必須建立適當的公告通知及讓使用者不同意條款變更時的退場及資訊終結機制，該定型化契約範本就條款變更的規定值得雲端業者作為建立相關機制時的參考。

7. 雲端定型化契約的管轄條款

絕大多數消費關係中，常見企業經營者以定型化契約條款方式與消費者合意彼此間消費訴訟的管轄法院，但立法者顧及消費者就消保案件中就約定管轄而起訴及進行訴訟之不便利，而可能降低消費者行使其法定權益的意願，因此在消保法第 47 條規定：「消費訴訟，得由消費關係發生地之法院管轄。」藉該條文來緩和定型化契約的操作合意決定管轄或民事訴訟法第 24 條合意管轄規定，所造成消費者在消費訴訟中程序待遇的不平等[394]。

我們前面所舉的雲端服務條款中也幾乎都有約定管轄法院之規定，因此按照消保法第 47 條之規定，雲端使用者可以在消費關係發生地提起訴訟。雖然雲端運算的特性之一就是可以隨時隨地接觸雲端資源，往往可能很難界定使用者是在何處連上雲端，但至少消保法第 47 條賦予

[393] 線上遊戲定型化契約範本第 24 條：「乙方修改本契約時，應於遊戲網站首頁及遊戲之登入頁面公告之，並以書面或電子郵件通知甲方(第一項) 。乙方未依前項進行公告及通知者，其契約之變更無效(第二項)。甲方於第一項通知到達後十五日內：一、甲方未為反對之表示者，視為甲方接受乙方契約變更之內容。二、甲方為反對之表示者，視為甲方對乙方終止本契約之通知(第三項)。」

[394] 馮震宇等，同註 367，頁 55。

雲端使用者可以在自己的住居所連上雲端，進而在該地法院提起訴訟，至少不用受到如Google或Facebook約定加州法院為管轄法院之拘束。另外如果雲端使用者提起的是損害賠償 10 萬元以下之小額訴訟，同樣有民事訴訟法第 436 條之 9 不受約定管轄規定之適用[395]。

第二節　個人資料保護法對雲端條款的檢討

資訊科技的進步，固然帶來許多生活及工作上的便利，但也造成個人資訊愈來愈容易受到侵害，尤其是網路科技的發展更是助長這種兩面現象，因此各國有鑑於資訊科技進步的同時，在立法上也致力於向個人資料保護的方向前進[396]。現行「電腦處理個人資料保護法」自 1995 年立法通過後，因為資訊環境快速變化，該法立法時考量之情況已發生變動，致使法律適用上效果不彰，早已受到各方議論，是以修正個人資料保護機制，近年來逐漸成為社會各界的共識[397]。我國自 2003 年開啟修法時程，歷經立法院跨屆的多年審查，終於在 2010 年 4 月 27 日通過個資法修正草案(修正後名稱為「個人資料保護法」，下稱「個資法」)。在雲端運算高度蓬勃發展之今，個資法的通過適逢其時，正可作為檢驗雲端運算服務條款適法性的依據。

但是個資法通過後，高達新台幣 2 億元的賠償上限[398]，讓社會各界不

[395] 民事訴訟法第 436 條之 9：「小額事件當事人之一造為法人或商人者，於其預定用於同類契約之條款，約定債務履行地或以合意第一審管轄法院時，不適用第十二條或第二十四條之規定。但兩造均為法人或商人者，不在此限。」

[396] 程法彰，我國為因應重視個人資訊保護的趨勢所為對「個人資料保護法」修正的立法評析，萬國法律，173 期，2010 年 10 月，頁 90。

[397] 劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月旦法學雜誌，183 期，2010 年 8 月，頁 147。

[398] 參考個人資料保護法第 28 條第 4 款：「對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。」

得不開始關注該法案，並重視起資訊安全。由於茲事體大，該法案自總統於 2010 年 5 月 26 日公布後，並未開始施行，僅是將原電腦處理個人資料保護法(下稱舊法)第 19 至 22 條及第 43 條之規定刪除，施行日期則由行政院在公布施行細則後另行定之[399]，意即除刪除之規定外，原電腦處理個人資料保護法其他條文仍有適用。以目前的時程來看，法務部預計要在 2011 年 6 月底將施行細則草案送交行政院，比原本預定 2011 年 11 月 25 日前送交行政院之時程提早，該細則草案送交行政院後，行政院將視情況召開會議，而後公布施行細則正式版本，並同時公布法案正式施行日期[400]，因此在可預見的未來個資法即將施行。雖然原電腦處理個人資料保護法其他條文仍有適用，但為適應新法之規定，我們接下來仍以新修訂的個人資料保護法為討論的重點，分析雲端隱私權政策與服務條款在即將施行的個資法下的適法性問題。此外由於在本文中，我們所分析的雲端服務隱私權政策與服務條款是將重點放在討論雲端業者與使用者間的法律關係，而我們所舉的Google、Yahoo、Facebook、Amazon及Windows Azure等雲端業者所提供的服務，不論是供給雲端的一般使用者或企業用戶，均多不涉及公權力的行使，因此按照個資法第 2 條第 8 款及第 9 款之規定，本文中我們所討論的雲端業者應屬個資法所規範的非公務機關，我們接下也將分析這些非公務機關的雲端業者所制訂的雲端條款在個資法體制下的適法性問題。

1. 雲端時代個資法資料保護之範圍

個資法第 2 條第 1 款[401]就個人資料的定義大致上參酌舊法的列舉規定，但將舊法第 3 條第 1 款「其他足資識別該個人之資料」之例示規

399 參考全國法規資料庫，個人資料保護法生效狀態，http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=I0050021 (查訪日期 2011 年 7 月 8 日)。

400 張維君，個資法施行細則 定義 12 項適當安全維護措施，資安人，2011 年 4 月 25 日，http://www.isecutech.com.tw/article/article_detail.aspx?aid=6108 (查訪日期 2011 年 7 月 8 日)。

401 個資法第 2 條第 1 款：「本法用詞，定義如下：一、個人資料：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。」

定修正為「其他得以直接或間接方式識別該個人之資料」，學者大致認為修正後是對個人資料保護適用範圍的擴大[402]，但仍有學者認為「其他得以直接或間接方式識別該個人之資料」的修法，在執行上或是保障上仍有疑慮[403]。

實際上根據前章我們所討論，雲端業者在隱私權政策中所宣稱會蒐集的使用者資料，包括使用者主動提供的資料、cookie、使用者在雲上進行的資訊和動作、利用第三方應用程式的動作及其產生的資料，以及與其他雲端平台或網站間的關聯服務，這些資料有許多是可以直接或間接辨識標定出特定使用者。除此之外現在的雲端服務有許多是需要帳號密碼才可登入使用或者是綁定 IP 的情況，因此對於像企業雲端、金融雲或教育雲等需要帳號密碼登入的情形，其帳號內當然是包括諸如企業商業活動、投資人、教員或學生等可資辨識出使用者或資料當事人的個人資料；另外在一般雲端使用帳號底下進行的雲端活動，如 Yahoo Mail、Gmail 或 Google Docs，雲端業者也能夠將帳號內的資料跟 IP 或 cookie 作連結而識別出特定個人，尤其還有像 Facebook 等雲端服務甚至進行過要真實姓名方能登入的政策，更是能夠直接標定出特定使用者。就算是對於單純的上網行為，例如瀏覽網頁或利用搜尋引擎進行檢索，雲端網路業者也是會蒐集使用者的 IP、cookie、Web Search Query 及 URL，這些資料也可以用來辨識出使用者的輪廓，就算使用者使用的是浮動 IP 及經常進行清除 cookie 的動作，但是在上網的當下，一般使用者也很難防止業者即時置入的 cookie，這些 cookie 很可能透露出使用者的瀏覽器語言、瀏覽器種類及瀏覽的內容，甚至還可能包含使用者的電腦名稱或網路卡號等足供識別個人的資訊。因此無論是雲端的一般使用或

[402] 劉靜怡，同註 397 書，頁 148；程法彰，同註 396 書，頁 91；劉定基，「個人資料保護法」初論，台灣法學雜誌第 159 期，2010 年 9 月，頁 2 以下。

[403] 王郁琦，優質網路社會下個人資料保護法制之因應，台灣科技法律與政策論叢，5 卷 2 期，2008 年 12 月，頁 27。

企業應用，使用者所上傳的資料及進行的網路行為，我們都認為是受到個資法所規範保護的個人資料。

除此之外個資法第 6 條第 1 項[404]參酌歐盟安全指令之規範[405]，針對醫療、基因、性生活、健康檢查及犯罪前科等特種資料規定原則上不得進行蒐集、利用或處理，僅在該規定的例外情況下方得為之。學者間對於該條規定多有批評及討論，例如「病例資料」是否在此特種資料的範圍內[406]，所謂之「性生活」除了立法理由中的性取向外是否包括性行為的偏好、曾進行性交易或婚外情等資訊[407]，又或者對學術機關就特種資料的蒐集、利用或處理的規範不足等議題[408]。除了這些學者們的批評外，我們認為在雲端時代中個資法有關特種資料的相關條文也是存有其他問題。例如現在有許多非公務機關或民間醫療院所經營醫療或健康照護事業[409]，這些非公務機關本身可能蒐集或處理相當多病患的醫療或健康檢查等特種資料，按照個資法第 6 條第 1 項之規定，這些非公務機關蒐集或處理特種資料或許還可以歸類為該條第 1 款之法律明文規定或第 2 款之非公務機關履行法定義務之必要，不過這類型的機關常為了資料管理或營運的成本考量或需求，必須將相關業務委外處理或使用現在很流行的醫療雲端服務，但對於提供委外服務或醫療雲服務的業者，是否該當於個資法第 6 條第 1 項所規定得例外蒐集處理特種資料之情況其實是有疑義的。另外個資法對於特種資料的蒐集處理保護或安

[404] 個資法第 6 條第 1 項：「4 有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、公務機關執行法定職務或非公務機關履行法定義務所必要，且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。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，且經一定程序所為蒐集、處理或利用之個人資料。」

[405] 劉靜怡，同註 397，頁 152。

[406] 余啟民，同註 303，頁 8。

[407] 劉定基，同註 402，頁 5。

[408] 劉靜怡，同註 397，頁 155。

[409] 例如私立法人醫院、老人安養中心、月子中心、仲介外勞照護中心，甚至是保險公司等機構。

全規範也是相當抽象，僅在第 6 條第 2 項[410]及第 27 條第 2 項[411]規定中央目的事業主管機關會同法務部制訂相關規範，也就是例如對於醫療等特種資料的蒐集處理，應由衛生署會同法務部制訂相關規範，或由衛生署對這類使用或提供醫療雲的非公務機關訂定資料安全標準等。對此我們認為既然我國制訂個資法是為求個人資料保護的總則性規範，那對於特種資料的蒐集、處理或利用應可制訂更詳盡的規範，而非僅是作抽象條文的規定，亦或者在個資法中規定要求在施行細則中由法務部會同中央目的事業主管機關制訂較詳細的準則。例如可以參考美國HIPAA及HITECH法案的規定，規範這類醫療院所蒐集處理特種資料時的善良管理人注意義務及應有的資料安全維護措施，以及更重要的是規定委外處理特種資料時與提供服務的業者間的協定或契約，必須包含特種資料的處理、流通及應用範圍，禁止特種資料的再分析、比對、揭露及作為廣告用途，加重提供服務業者責任，以及前章我們所討論企業使用雲端服務進行合約管理時應該注意的項目等相關規定。

2. 個人資料蒐集、處理或利用的同意：

按照個資法第 7 條第 1 項之規定[412]，蒐集或處理個人資料，需告知當事人個資法所應告知事項，即第 8 條第 1 項[413]各款所規定應告知事項，並得當事人書面之同意。參照同法第 8 條第 1 項第 2 款之規定，個人資料的利用期間、地區、對象及方式也是需明確告知當事人之事項，

[410] 個人資料保護法第 6 條第 2 項：「前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。」

[411] 個資法第 27 條第 2 項：「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」

[412] 個資法第 7 條第 1 項：「第十五條第二款及第十九條第五款所稱書面同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。」

[413] 第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：一、公務機關或非公務機關名稱。二、蒐集之目的。三、個人資料之類別。四、個人資料利用之期間、地區、對象及方式。五、當事人依第三條規定得行使之權利及方式。六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

因此超過此範圍之資料利用，須遵守個資法第 20 條第 1 項[414]各款之規定，其中最重要者就是第 6 款經當事人書面之同意。對此「書面」之要求，鑑於網路資訊科技的發達，應肯認可經由網路的形式或由電子簽章方視為之[415]。不過探究個資法有關「書面」規定之意旨，是在於讓當事人瞭解資料如何被蒐集、處理或利用，所以才要求當事人要以書面「回應」表示同意。

但實際上雲端業者是藉由在隱私權政策和服務條款的網頁來說明如何進行資料的蒐集、處理或利用，並且當使用者申請帳號或使用服務時，即視為同意雲端業者對資料之行為。雲端業者採用的是第 19 條第 1 項[416]第 2 款「與當事人有契約或類似契約之關係」的規定，按照前章我們的討論，使用者申請帳號或使用服務即同意了與雲端業者間的契約法律關係，因此業者可以進行資料的蒐集或處理。但是雲端業者如果利用資料超出原本宣示在隱私權政策或服務條款中的資料利用範圍，業者仍然還是要經過使用者「書面」同意的「回應」方可為之。

3. 雲端個人資料蒐集、處理與利用目的明確性

早在電腦處理個人資料保護法立法之時，立法者就秉持OECD隱私保護基準對資料蒐集、處理及利用限制與目的明確化的概念，在舊法第 18 條就已納入資料的蒐集或電腦處理目的必須特定的規定。個資法制

[414] 個資法第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。六、經當事人書面同意。」

[415] 呂丁旺，淺析修正「個人資料保護法」，月旦法學雜誌，183 期，2010 年 8 月，頁 136。

[416] 第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。五、經當事人書面同意。六、與公共利益有關。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。」

訂時亦參考歐盟安全指令及APEC隱私保護原則遵循OECD個人隱私保護基準以來對資料蒐集、處理及利用明確性的規範要求[417]，在個資法第8條第1項規定應明確告知當事人對資料「蒐集之目的」及「個人資料的利用期間、地區、對象及方式」。除此之外在第5條規定對個人資料的蒐集、處理或利用不得逾越該明確之特定目的，第19條第1項及第20條第1項前段亦再次重申資料的蒐集、處理或利用應有特定明確之目的及在該目的範圍內為之。因此可見我國個資法在修正制訂時，對於資料處理明確化的及求與標準是與國際規範一致。

根據前章中我們對雲端隱私政策與服務條款的討論，雲端業者蒐集、利用或處理使用者資訊，除了基於雲端運算原有的服務目的外，還會為了要用於提供、維護、保護及提升原有服務，這些都是使用者可以理解與接受的資料蒐集、利用或處理的目的。就算是雲端業者增加了就使用者資料作廣告的目的，我們也只能自我解嘲，雲端的一般使用是建立在免金錢費用但以進行精確廣告為對價的商業模式。但除此之外，雲端業者還藉由定型化約款要求使用者進行資料內容的授權來作為享受服務的對價，我們當然不是說雲端業者不能向使用者要求其他享受雲端服務的對價，只是這種對價若建立在對使用者個人資料的處理及利用就必須符合個資法的規範，業者必須先明確聲明這種資料的處理及利用目的為何。不過遺憾的是依據我們之前的討論，雲端業者雖然在條款中要求使用者進行資料授權，但幾乎都未明確說明如何對這些授權資料進行使用、應用、處理或利用。就如同前面我們所討論，雲端業者放入這種條款是在為將來其他利用使用者資料的商業模式預作準備，這也可見雲端業者目前還不知道取得這些資料授權有何利基，如果業者能夠從中發掘出新的商業模式，早就將之加入定型化約款中作為原有的服務目的，來達成

[417] 余啟民，同註303，頁11-12；參見法務部，立法院三讀通過「個人資料保護法」新聞稿，2010年4月27日，http://www.moj.gov.tw/public/Data/0427164423187.pdf (查訪日期2011年7月8日)。

資料處理利用目的明確化之要求。

對於這類型的條款，或許有雲端業者會抗辯說這種要求使用者進行資料內容授權的情形，是個資法第 20 條第 1 項為特定目的外之利用，業者將之登載於定型化約款中經由使用者申請帳號或使用服務時而同意，即是依照該規定之第 6 款得使用者書面之同意。但是根據我們前面的討論，對於特定目的外之利用的「書面」同意，是要讓當事人瞭解資料如何在原先目的及範圍外被處理或利用，而且按照第 7 條第 2 項之規定 [418]，也要明確告知當事人這種原先特定目的外之利用的目的、範圍及同意與否對其權益之影響。而且本文我們所討論的Google、Yahoo、Facebook及Amazon等雲端業者所提供的服務多屬民間的一般使用或商業應用，並非為增進公共利益或為免除當事人生命、身體或財產上之危險等個資法第 20 條第 1 項其他款得於特定目的外之利用情況。因此，雲端業者這種要求使用者進行資料授權，但卻無法明確說明授權之目的、範圍及影響的定型化條款，不能被視為已得使用者書面「回應」之同意，也違反個資法目的明確性的規定，亦同時違反OECD保護基準及歐盟安全指令之規定。

除此之外，前章我們也曾提到雲端業者的條款中有資訊再流通分享予第三方範圍過廣及對象不明確的問題，我們亦曾討論過雲端業者將資訊的再流通或分享給第三方必有其目的，雲端業者通常會宣稱這是為了要處理使用者的個人資訊或提供更佳的服務品質，可見業者的再流通資訊是為了處理及利用資訊。再者按照個資法第 8 條第 1 項及第 19 條第 1 項之規定，機關對資料的蒐集、處理或利用目的均須明確告知當事人，這意謂著要讓當事人明確知悉的不僅是資料集、處理或利用的目的，還

[418] 個人資料保護法第 7 條第 2 項：「第十六條第七款、第二十條第一項第六款所稱書面同意，指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，單獨所為之書面意思表示。」

要讓當事人明確知道是哪個機關在蒐集、處理或利用個人資訊。個資法第 8 條第 1 項第 1 款規定應向當事人明確告知蒐集機關的名稱，在解釋上該機關同樣須對當事人明確說明資訊再傳遞與分享的其他第三方對象為何。因此，雲端業者要藉由定型化契約，讓使用者同意其進行資料的再流通或分享，就必須明確告知使用者資料的流通或分享範圍，這類流通分享範圍不明確的條款即會違反個資法的相關規定，亦違反 OECD 保護基準及歐盟安全指令之規範。

4. 個資法所保障雲端使用者的資料自決權及業者的資料終結義務

按照個資法第 3 條之規定：「當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。」該條規定在舊法第 4 條即已存在，而且同樣也是源自OECD、歐盟和APEC對於當事人資訊自決權和資訊隱私保障的概念，這些資訊自決及隱私保障的概念皆屬人格權之內容，可與人性尊嚴相連結[419]。對於個資法第 3 條前 3 款之規定，大致上雲端業者在條款中都會同意並且遵守，尤其是給予使用者能夠補充或更正雲上資料的權利，讓雲端資料能夠更正確與充足而讓業者的廣告更為精準，本來就符合業者廣告服務的商業目的。但是對於後 2 款資料終結之規定，雲端業者的條款就顯得不夠完備。一般而言，在使用者還在使用雲端服務時，業者多會同意使用者能夠隨時永久刪除雲上資料，頂多是因為雲端主機系統刪除暫存或刪除備份資料的時間差異而已。但如若是因為使用者停用服務或雲端業者終止服務時，根據我們前章的討論，此時雲端業者在條款中對於使用者的資料採取何種態度卻是曖昧不明，業者也多半未說

[419] 余啟民，同註 303，頁 13。

明此時是否會主動刪除或停用這些資訊。

個資法第 11 條第 3 項規定:「個人資料蒐集之特定目的消失或期限屆滿時,應主動或依當事人之請求,刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者,不在此限。」對雲端運算的資料終結看似提供了法源依據,但實際上立法者將「主動」後加上「或依當事人之請求」,就有可能造成解釋適用上的問題。究竟是資料蒐集機關本應主動進行資料的終結動作,在當事人請求時更應為之,亦或蒐集機關可以主動進行終結或也可以被動等待當事人來請求,這二者間的差異將造成資料當事人權益保障的不同。我們參考同法第 11 條第 1 項[420]規定在維護個人資料之正確時亦有「主動或依當事人之請求更正或補充之」等文字,參照該項之修正理由說明[421]「資料蒐集機關發現資料正確性有誤,應主動予以更正或補充,爰修正本項及第二項」,因此可見立法者在使用「主動或依當事人之請求更正或補充之」等文字作為立法條文時,是要求該機關主動為規定之行為,在當事人請求時則更應積極為之。我們也因此認為個資法第 11 條第 3 項規定中的文字字義應修正為:「...,應主動刪除、停止處理或利用該個人資料,當事人亦得請求為刪除、停止處理或利用該個人資料。...」,以避免解釋適用上的爭議,甚至第 11 條其他各項規定中的文字字義亦應作類似之修正,以除解釋適用上的疑義。

因此按照如斯解釋,雲端使用者自行停用服務或業者終止該服務時,即原先就資料用於原服務目的或用於廣告等目的應已消失,不論雲端業者是否將之載入定型化條款中,業者都負有在該規定下主動刪除、停止處理或利用該個人資料之義務,我們也一貫主張與呼籲雲端業者要在隱

[420] 個資法第 11 條第 1 項:「公務機關或非公務機關應維護個人資料之正確,並應主動或依當事人之請求更正或補充之。」

[421] 參考電腦處理個人資料保護法修正草案條文對照表,thinktank.nat.gov.tw/public/Attachment/610314213371.doc (查訪日期 2011 年 7 月 8 日)。

私權政策與服務條款中載入這種主動終結資料的條款，一來宣示保護使用者個人資訊的決心，二來也讓多數不懂法律規定的使用大眾瞭解業者的個資保護機制。像前述Facebook宣稱在使用者停用服務後會保留資料到使用者回心轉意而重新使用服務的條款[422]就是明顯違反個資法的規定，Yahoo聲明在停用或服務終止時得刪除全部或部分資料的條款[423]也會通不過個資法的檢驗，Yahoo不能「得」或「部分刪除」，而是必須主動且全部刪除這些資料。另外個資法第 11 條第 3 款所規定「個人資料蒐集」，應係指第 2 條第 3 款「以任何方式取得個人資料」而言，因此不論是雲端業者自行利用cookie，或自行記錄使用者URL或Web Search Query，亦或是使用者自行上傳至雲上的資料，如在Facebook上編寫網誌或照片，或用Google Docs編寫文件等，皆屬雲端業者「以任何方式」取得的資料，皆有第 11 條第 3 項規定之適用，在服務停用或終止時雲端業者均應主動對這些資料進行刪除。

除此之外，我們對於雲端運算服務的討論一貫主張，就是不論雲端服務是以利用一般使用者資料為對價或企業用戶付費使用服務，一旦服務停用或終止後，雲端業者即不得在利用與流通傳遞這些資訊，這也符合個資法就資料蒐集目的消失後的資料終結規定。因此對於雲端業者要求使用者進行資料授權，而資料授權必有其處理或利用目的，當原先的資料蒐集目的消失時，業者就這些資料取得的授權也應歸於消滅而不得再為處理或利用，就算雲端業者不在定型化條款中載明，同樣不影響業者喪失該資料內容的授權。是以Google、Yahoo、Amazon和Plurk要求「永久」授權的條款[424]不僅違反第 11 條第 3 款蒐集目的消失時應停止或利用資料的規定，也是以約款方式讓使用者預先拋棄或限制其行使第

[422] 參考 Facebook 隱私權政策，同註 279。
[423] 參考 Yahoo 隱私權政策，同註 279。
[424] 參考 Google、Yahoo、Amazon 和 Plurk 的服務條款，同註 323 及 324。

3 條第 4 款所規定請求停止資料處理或利用的權利，這類型條款是嚴重違反個資法之規定，也與OECD及歐盟等國際規範所倡導當事人應有的資訊自決權等概念背道而馳。實際上也是有Facebook等業者宣稱刪除資料與停用帳號時終止授權的條款[425]，可見亦有符合個資法規定的業者。

不過雖然目的消失時資訊的主動終結屬於雲端業者的義務，但按照第 8 條第 1 項所規定應向當事人說明之事項，其中第 5 款參照第 3 條的規定，雲端業者只要向使用者說明具有請求資料終結的權利即可，並不需要說明業者必須在目的消失時主動進行資料的終結程序，由此可見這是個資法規範上的漏洞，而且實際上我們也未發現有雲端業者在條款中作如此詳細的說明。另外對於特殊的雲端應用，例如銀行、電信、醫院、保險等雲端服務，因保有大量且重要之個人資料檔案，其所負之安全保管責任應較一般行業為重，個資法第 27 條第 2 項[426]亦賦予中央目的事業主管機關得訂定這些特殊應用的業務終止後個人資料處理方法。

5. 雲端個資時代適當的安全措施

按照個資法第 27 條第 1 項之規定:「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」第 27 條第 2 項中央目的事業主管機關甚至可以針對特定機關訂定個人資料檔案安全維護計畫。但實則何謂「適當」之安全措施，個資法未明文規定，當然就立法技術上而言，雲端科技進步的幅度遠超過立法步調，因此立法時宜以概括性條款定之，將技術細節部分交予行政主管機關以施行細則作規範。惟應賦予主管機關按時檢討科技變化而

[425] 參考 Facebook 的服務條款，同註 324。

[426] 個資法第 27 條第 2 項:「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。」

隨時修正施行細則之權責，例如按照美國 DMCA 法案規定要求其著作權局每三年要定期檢討一次，或我國著作權法第 80 條之 2 第 4 款要求主管機關定期檢討等規定，但個資法第 27 條只規定中央目的事業主管機關就非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法訂定相關事項辦法，並未規定主管機關須定期檢討科技環境適時作出該事項辦法之修正，此為個資法規範疏漏之處。

目前法務部草擬的施行細則中一項重點就是對何謂「適當」安全維護措施作出定義[427]，不僅規定非公務機關的善良管理人注意義務，亦明訂安全維護事項，包括(1)必要的組織；(2)界定個人資料範圍；(3)個人資料蒐集、處理或利用的程序；(4)當事人行使權利的處理程序；(5)資料安全；(6)資料稽核；(7)人員管理及教育訓練；(8)設備管理；(9)紀錄與證據之保存；(10)緊急應變措施及通報；(11)改善建議措施；(12)其他安全維護事項，以作為資訊保護的機制。經濟部商業司也鑑於個資法通過後各界對資訊安全措施如何進行的疑慮，委託資策會研擬「臺灣個人資料保護與管理制度」（Taiwan Personal Information Protection and Administration System, TPIPAS），來協助各界建構個人資料保護管理制度[428]。

但實際上如我們前章所討論，目前的雲端業者只是在隱私權政策或服務條款中說明會進行「適當」的資安措施，幾乎照本宣科個資法的條文，卻並未進一步說明進行何種適當的措施，而施行細則雖然有對「適當」安全維護措施進行定義，但也仍未要求業者要在定型化約款中進行說明。雲端企業用戶或許還有能力進行雲端安全措施的評估，不過對於眾多無能力進行評估的一般使用者似乎僅能仰賴主管機關對雲端業者

[427] 張維君，同註 359。

[428] 廖珮君，TPIPAS 上路 個資保護有標章可循，資安人，2011 年 4 月 11 日，http://www.isecutech.com.tw/article/article_detail.aspx?aid=6094 (查訪日期 2011 年 7 月 8 日)。

進行稽查，因此主管機關有必要在未來制訂雲端服務契約範本時要求業者在隱私權政策中說明與揭示進行哪些安全防護措施，一來讓廣大的雲端一般使用者及關心雲端資訊安全的團體一起來瞭解及監督業者保護機制的運作，二來也減少主管機關進行稽查業務的壓力。

6. 資訊安全事件發生時的通知義務

按個資法第 12 條規定：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」該條規定增定公務及非公務機關於資料被竊取、洩漏、竄改或其他侵害等資訊安全事件發生時的查明及通知義務，足以彰顯新法的進步性。但個資法該條規定係以「...違法本法規定，致個人資料被...」為通知義務發生的前提，而可能產生該機關自行認定並未違反個資法規定，或雖有違法行為但非導致個資危害的原因，從而拒不通知的情形[429]。再者個資法缺乏賦予當事人在發生資安事件時向該機關要求揭示及檢視安全措施的規定，亦缺乏主管機關更多調查資安事件權限的規定，這都將使業者不為通知的可能性增加。

雖然個資法的立法未盡周全，不過至少對雲端使用者而言，具有要求業者在發生資安事件時進行查明及通知的法源依據。當然我們在檢視雲端業者的隱私政策與服務條款時，也是發現缺乏這樣的約款，不過業者雖不在定型化約款載入這類規定，但並不影響業者的該項義務。

7. 個資法的損害賠償責任：

依照個資法第 29 條第 1 項之規定[430]，對於非公務機關違反個資法

[429] 劉定基，同註 402 書，頁 8。

[430] 個資法第 29 條第 1 項：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

所造成的資安事件，採同樣民法第 184 條第 2 項所規定的「推定過失」責任，雖然保護程度不若消保法第 7 條所規定的「無過失責任」，也雖然如同我們在前節就消保法的討論中，雲端使用者必須負擔沈重的客觀歸責原因舉證責任，但仍如我們在消保法中的討論，個資法該條之規定不容許雲端業者在定型化條款中以特約排除其資安事件的責任。另外個資法亦有如消保法就團體訴訟之規定，在第 34 條規定資安事件時進行團體訴訟之規定，該規定或許能夠聚集眾多受害之雲端使用者一起向業者求償，但仍須依據我國個資法及侵權行為法之體系負擔一定的客觀歸責原因舉證責任，尤其雲端業者未充分揭露所進行個資保護措施，而個資法亦未要求業者必須進行揭露或為舉證責任轉換之規定，因此就算是進行個資法上的團體訴訟，使用者仍須面對嚴苛的舉證責任。

8. 個資法的專屬管轄

依照個資法第 33 條第 1 項[431]之規定，對非公務機關提起損害賠償訴訟者，專屬其主事務所、主營業所或住所地之地方法院管轄，但在同條第 3 項[432]則規定法人之非公務機關現在我國無主事務所或主營業所者，專屬中央政府所在地之法院管轄。因此就算是雲端業者在定型化條款中約定外國法院管轄，對於外國籍的雲端業者如Google或Facebook等公司，通常主事務所和主營業所不在我國境內，使用者仍可按照個資法在我國法院尋到管轄的法律基礎。

9. 雲端個資保護時代主管機關的權責

個資法承襲歐盟和APEC等國際規範，其中規定要求資訊蒐集、處

[431] 個資法第 33 條第 1 項：「依本法規定對於公務機關提起損害賠償訴訟者，專屬該機關所在地之地方法院管轄。對於非公務機關提起者，專屬其主事務所、主營業所或住所地之地方法院管轄。」

[432] 個資法第 33 條第 3 項：「第一項非公務機關為自然人以外之法人或其他團體，而其在中華民國現無主事務所、主營業所或主事務所、主營業所不明者，專屬中央政府所在地之地方法院管轄。」

理及利用須要明確，且必須明確告知當事人資訊蒐集、處理及利用的目的[433]，但雲端業者卻在條款中載入不明確目的授權及資訊再流通分享對象不明確等條款，這種條款明顯違反個資法的相關規定，甚至業者在提供雲端服務時由於該不明確條款的存在而可能存有違反個資法的事由，例如業者可能已經將資訊流通給不明確的第三方。我們在此要提醒這些業者，個資法第 22 條第 1 項[434]之規定賦予主管機關就違反個資法規定之虞時得進入及檢查雲端業者，如有違法情事，主管機關得為第 25 條規定之處分，並可依第 47 條第 2 項及第 3 項進行罰鍰處分。此外更嚴重的是按第 41 條第 1 項[435]之規定，刑事罰責是只要處罰「足」生損害於他人的危險犯，而非「致」生損害於他人的實害犯，雲端業者載入這類不明確條款，縱使未實際散佈流通資料於不明確第三方，亦可能構成「足」生損害的情狀。另按第 41 條第 2 項[436]之規定，意圖營利犯前項之罪者還會加重刑事責任，因此雲端業者要是再發展出可以從使用者資料授權而獲利的商業模式，都可能面臨該條款規定刑責的追訴。所以按照個資法的相關規範，雲端業者在定型化條款中載入這些不明確目的的條款，實非明智之舉。

除此之外，按照法務部施行細則的時程，細則公布與個資法施行指日可待，屆時在細則中將會有較明確的適當安全保護機制定義。個資法雖然沒有要求資料蒐集處理機關要向當事人說明所進行的個資保護機制，但個資法第 22 條第 1 項同樣賦予主管機關進行進入及檢查之權責，

433 參照個資法第 8 條第 1 款及第 20 條第 1 款之相關規定。

434 個資法第 22 條第 1 項：「中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。」

435 個資法第 41 條第 1 項：「違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。」

436 個資法第 41 條第 2 項：「意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」

並且在安全措施不適當或未符合細則規定時，主管機關可依個資法第48條第4款之規定進行罰鍰處分。

綜合以上所述，我們可以發現，雲端業者除了在條款中載入不明確而有違法之虞的條文外，基本上我們還認為在這些定型化約款中，不應僅只記載個資法第8條第1項雲端業者應明確告知使用者的事項，還應該記載一些法律並未規定須載入但業者必須遵守的義務，例如目的消失後的終結資料義務[437]、資安事件發生時的通知義務，甚至包括說明業者實際上進行何種安全保護措施等，讓雲端使用者不論是企業用戶或一般大眾，均能確實瞭解到使用雲端運算服務時該有的權益。上述這些議題的落實，也有賴於個資法的中央主管機關會同消費者保護委員會制訂出符合雲端運算服務的定型化契約範本。

第三節　本章小結

接續前章我們對雲端隱私政策與服務條款的討論，在本章一開始我們討論了這些條款在我國消費者保護體系下的適用性問題，按照消保法的規定，提供雲端服務的業者和接受服務的使用者為消保法所定義下的企業經營者和消費者，雲端業者所制訂的雲端隱私政策與服務條款則為消保法上的定型化契約條款。經由本章的討論我們發覺這些雲端業者制訂的條款常有語句過於模糊，並且利用太多否定、雙重否定或負面表列的方式詮釋雙方的法律關係，條款的結構有時也過於零碎且不清晰明確，對於一般的使

[437] 包含掌握在雲端業者手中的個人資料，例如因為使用者在使用服務時自行刪除或修改而終結的資料，及因為停用或終止服務而致目的消失時須停止蒐集、處理及利用的資訊與同時喪失這些資料的授權。

用大眾而言，會有閱讀及理解的困難，因此發生爭議時除非法院朝向有利使用者方向作解釋，否則會對使用大眾相當不利。

除此之外我們也發現雲端業者也常藉由定型化契約條款讓使用者同意的方式，來規避消保法所規定的無過失商品或服務責任，這類型的條款明顯違反消保法的相關規定。不過縱使這類型的條款失其效力，雲端業者要負上無過失的責任，但對於利用雲端服務的使用者而言，仍在舉證損害客觀歸責原因上困難重重。這種情形固然源自立法時處在消保案件客觀歸責原因比較單純的時代，但這也與雲端業者不願說明進行何種資安保護措施，未能讓使用者能夠明瞭雲端平台保護機制是否足夠，亦未能更進一步瞭解是在網路或雲端哪個環節產生問題有關。另外也如前章我們一直在強調的議題，雲端業者制訂的定型化約款充滿不少資訊處理及利用不明確的條文，最典型的就是業者要求使用者進行目的不明確的資料內容授權，以及讓使用者同意進行範圍過廣且對象不明確的資訊分享及流通，這兩類條款不僅違反 OECD 及歐盟的規約，違反了個資法資料處理及利用明確性的規定，也加重使用者所不能控制的資訊風險，同樣違反消保法的誠信原則而會失其效力。最後對於雲端消費者保護的檢視，我們也提出業者在任意變更條款時應該要參照線上遊戲定型化契約範本對條款變更的相關規定，以保障雲端使用者的權益。另外對於雲端消保案件的法院管轄，也有消保法第 47 條及民事訴訟法第 436 條之 9 等規定之適用，讓雲端使用者不用受到業者定型化約款管轄不利法院的拘束。

本章另一個部分我們也進行了個資法對雲端條款的檢視。按照個資法的規定，本文我們所討論的雲端業者多屬個資法中的非公務機關，進行蒐集、處理及利用使用者資料來提供各種雲端服務，這些資料能夠直接或間接辨識出使用者的面貌，因此符合個資法所欲規範的個人資料範疇。個人資料保護法制訂後雖有許多不完備之處，學者見解對此多有討論，我們也

提出許多可供修正的意見，但個資法的修正制訂後仍揭示了我國個資保護的新頁，並大幅度完善我國個人資料保護的體系，讓個人資料的保護成為一個整體的概念。按照我們前述對個資法的討論，以下我們列出這個資訊保護的體系：

(1)資料類型　→ §2I，§6

(2)個人資料蒐集、處理或利用要合於特定目的及要件 → §8，§19I，§20I

(3)應告知事項　→ §8

(4)適當的安全措施　→ §27I

(5)資訊自決及資料終結　→ §3，§11

(6)資安事件的通知義務　→ §12

(7)資安事件的損害賠償責任　§29I → 推定過失責任

(8)個資法的專屬管轄 → §33

(9)主管機關權責 → §22 行政機關檢查權，§25 及§47 處分規定，§41 罰責

在這個概念體系適用於雲端運算服務時，個資法賦予雲端業者有向使用者明確說明資料蒐集、處理、利用、散佈及流通的目的及範圍的義務，以及向使用者說明享有的資訊自決和保護的權利，個資法雖未規定業者有向使用者說明進行何種安全措施的義務，但細則公布後則會對業者所採取的安全措施產生規範。其次當業者超出原本資料的應用目的及範圍時，必須明確向使用者說明新的應用目的及範圍，並須取得使用者的「書面」同意回應。如若發生資安事件，雲端業者還負有查明及通知使用者的義務，以及推定過失的責任，個資法亦對雲端使用者有較有利的專屬管轄規定。最後當使用者停用服務或業者終止服務時，個資法還賦予業者必須主動進行資料終結的義務。要確保這一系列個資保護的概念及規定能夠落實，個資法還賦予主管機關進入及檢查雲端業者的權責，並規定有雲端業者違反該法規定時的行政處分及刑事罰責。如此構成我國個資法完整的個人資料

保護體系。

經由個資法的體系分析檢視雲端業者的定型化約款，我們發覺這些條款有許多值得改善的地方。對於不明確目的條款的存在，我們呼籲業者應主動將之刪除，以免有觸法之虞；對於業者該有的義務，但法未明文規定應予告知使用者的事項，我們也是建議雲端業者要將之載入雲端隱私政策與服務條款之中，以保障雲端使用者的資訊安全及隱私人格權免受侵害，並促進雲端資料之合理利用的個資法第 1 條立法目的的達成。我們所提出的這些觀點，也可作為未來主管機關會同消費者保護委員會在制訂雲端運算服務定型化契約範本的參考。

第七章　結論

第一節　本文研究結果回顧

在本文一開始我們以主角小吳使用雲端運算服務為開端，介紹在資訊時代中，各種雲端運算服務開始取代過去套裝軟體與作業系統，雲端服務逐漸成為生活的重心。人們不用再像過去需要持續升級軟硬體來追求更新更好的服務，現在只要利用個人電腦、筆電或智慧型手機，隨時隨地都可以透過網路使用到最新最棒的服務，而且不論是一般使用者或企業用戶，都能享受到雲端科技進步帶來的便利。我們也藉此介紹從大型工作站主機到網路，再到雲端運算這一系列資訊時代發展的過程，雲端運算可謂「是一種使用彈性方便的網路資源與計時計量付費的網路服務模式，可因應使用者不同需求，動態快速調整使用資源」，雲端運算也可說是資訊網路發展到今日的成果，而且還不斷在進步創新中。從這些雲端技術發展的討論中我們也更能瞭解到雲端運算的內含，軟體即服務、平台即服務與基礎架構即服務三種不同的雲端運算類型，以及私有雲、公共雲和混合雲三種不同的雲端架構關係，我們也歸納出一些評估雲端運算須要注意的項目，例如彈性、可靠度、敏捷性、適應性、可用性及服務品質等。

使用雲端運算服務只要基本的配備，透過網路就可以隨時隨地接觸到雲端資源，讓雲端的使用無遠弗屆，但雲端運算便利的因素也是造成它有風險的原因，人們在享受雲端服務的同時很容易忽略這是建立在使用者將資訊上傳至雲端伺服器進行處理或儲存的模式，人們不在像套裝軟體時代在自己的硬體上儲存運算資料，從而不再完全掌握資訊的流向。在雲端時代中，將資料透過網路交給雲端伺服器享受各種服務，同時也就讓雲端服務提供者或雲端業者分享了資料的控制及流向，人們不在能夠完全掌握自

己的資訊，於是資訊安全的風險大幅提高，各種資安事件開始大量發生。本文接下來我們即探討這些雲端時代資訊安全風險的源由，發現一般的雲端服務常是以免付費的方式提供給大眾使用，但是像 Google 和 Facebook 這類雲端業者提供的服務是需要大量的成本來架構服務內容及伺服器，因此雲端業者們有必要在這種免付費的模式中找到新的商業利基，這就出現了時下最流行的線上廣告服務，雲端業者手中掌握的大量使用者資料就成為精準個人廣告最好的參考依據。除了利用使用者自行上傳至雲上的資料作為廣告依據外，我們也發現許多雲端網路業者還會透過 cookie、Beacon 或其他掃瞄工具來蒐集使用者的資訊及網路行為，這些都嚴重侵害到使用者的個人隱私，而且雲端業者所蒐集到的這些資訊會否再流通轉交給其他第三人造成更大的傷害，也成為使用者無法控制與揮之不去的夢魘。對於雲端的企業使用而言，雖然企業用戶使用的雲端服務內容需要支付費用而不會有線上廣告的困擾，但仍舊會有雲端業者蒐集資訊及再流通給第三人的問題，對於商業機密資訊外流產生的損害，往往都是企業用戶所無法承受。另外雲端的一般使用和企業應用，同樣也都會關心雲端安全防護的問題，雲端業者是否建置有適當的防火牆及安全措施，是否對帳號、密碼或機密資料進行加密處理，都是眾多使用者關心的議題。

這些雲端運算服務產生的議題很多都取決於雲端業者所採取的態度，取決於雲端業者除了提供服務外要怎麼利用這些使用者資訊，或者要不要更加強雲端資訊處理與傳輸的安全防護措施。在本文中我們討論了許多關心資安人士或團體針對雲端業者所提出的質疑和訴訟，在這些爭議中我們看到雲端個資隱私保護議題不斷的被提出，每當隱私保護團體取得勝利時，雲端業者就必須去修改他們對待使用者和其資訊的方針，也就是業者們要在雲端隱私政策和服務條款中去宣示對個資保護更有利的措施，實際上雲端業者也藉由這些條款來規範與使用者間的權利義務等法律關係，那我們

就有必要針對這些政策與條款進行討論。尤其是目前提供雲端服務的業者，如 Google、Facebook、Amazon 和 Windows 等業者多屬跨國大型企業，多用定型化約款的方式來制訂隱私政策與服務條款，一般使用者和中小型企業用戶常顯得相當弱勢，因此更有深入討論這些約款的必要。

本文我們主要部分即由此開展，我們先討論了美國法中的醫療保險流通與責任法、經濟與臨床健康科技資訊法、金融現代法、租片隱私保護法、纜線傳政策法、反對婦女暴力法、兒童網路隱私保護法及各州資訊安全規定等法規中關於個人資訊處理及流通的相關規定，探討這些美國法上對雲端運算時代個資保護可資參考的規範。除此之外我們也討論了 OECD 的個人隱私資料保護基準、歐盟安全指令及亞太經濟合作會議的隱私保護原則等國際規範，甚至包括跨境傳輸的相關規定。這些規範不僅影響我國個人資料保護法的修正，也揭示了個人資料處理、利用、流通及再流通目的明確性等相當重要的原則，及個人資訊自決及安全保護的重要概念。

藉由這些對美國法及各國際規範的討論，我們更進一步來分析雲端業者的隱私權政策與服務條款。首先我們發現雲端業者藉由定型化約款的方式宣示，讓使用者在申請雲端服務帳號或使用服務時就同意了該隱私權政策與服務條款，這種同意方式也就讓使用者認可了所有雲端業者宣示的約款內容。但這種雲端業者單方面制訂的定型化條款，我們發現幾乎充斥的都是雲端業者的權益保障，包括讓使用者同意除了自行上傳的資料外，還同意讓業者蒐集 cookie、使用者在雲上進行的資訊和動作、利用第三方應用程式的動作及所產生的資訊、與其他雲端平台或網站間的關聯服務及位置資料等，也讓使用者同意業者進行的針對性廣告是服務的一環、業者可以將資訊流通給與其有關連但範圍不明確的第三方、甚至讓使用者同意對業者進行雲端資料應用不明確的授權。雲端業者對使用者作這麼多的要求，就在於業者認為對一般的使用大眾是在「免費」提供服務，但實際上以此

思維也僅是使用者免付金錢上費用，使用者其實是讓雲端業者就資料進行廣告及授權業者這些資料內容作為使用雲端服務的對價，這也是我們一貫的主張。使用者不是單方佔了雲端業者的便宜，而是同樣有所付出，甚至有時我們看來這種付出換來的資安風險可能遠遠超過享受雲端服務的實益。

不過更讓我們感到憂心的是，在這些定型化隱私政策與服務條款中，雲端業者對使用者作了這麼多要求，卻不願明確說明到底對使用者資訊進行哪些適當的安全措施，也不願說明在使用者停止服務或業者終止服務時這些個人資訊該如何處理，而且基於我們一貫的立場，我們認為雙方既有對價關係，這種對價在服務停止及終止時就應結束，此時雲端業者即不得再對使用者的資料進行任何的處理、利用及散佈，使用者對業者的資料內容授權也應終止，甚至業者還得將這些資料進行全部永久刪除的資料終結動作，但很遺憾的是業者大多沒有在隱私政策與服務條款中對這些議題上進行說明。尤有甚者，雲端業者還藉由定型化條款，大幅免除發生資安事件時的責任問題；縱使危害來自於雲端業者，在這種條款下使用者勢必將求助無門。另外由跨國性大型雲端業者制訂的定型化條款，約定外國準據法及外國管轄法院，對使用者權益缺乏保障自然也不在話下。這些條款不僅出現在雲端的一般使用中，我們同樣也發現類似的條款出現在許多定型化的雲端企業應用契約中，企業用戶在選用雲端服務時，除了考量雲端服務的內容、效益、穩定性符合需求外，還要深入評估業者的隱私政策與服務條款所產生的影響。

對於這些隱私權政策與服務條款的分析，我們發現了許多對使用者不利及不公平的條款，將這些條款放入我國消保體系中檢查，可能都會違法而失其效力。例如這些條款常過度使用否定及雙重否定的字句來表達其含意，結構也常零碎及不清晰明確，造成使用者在閱讀理解上的困擾；或

者雖然因為雲端資訊的環境使然，使用者面對個資事件時的客觀歸責事由很難舉證，但雲端業者過度排除責任的條款，是違反消保法無過失責任及相關損害賠償的規定。此外雲端業者資料流通不明確及授權目的不明確的條款，同樣也會違反消保法及其施行細則不得加重消費者不可控制風險的規定；業者的外國法院管轄條款，也是會違反消保法保障弱勢消費者而以消費地定管轄的相關規定。

除了我國消保體系的檢驗外，我們也將這些定型化約款納入新修訂的個人資料保護法來作檢討，同樣也可以發現業者不明確目的的資料流通及資料內容授權條款是明顯違反個資法的相關規定，個資法也同樣規定雲端業者在資安事件發生時的推定過失責任而不得在條款中過度進行免責聲明，以及有利於雲端使用者的管轄法院條款。除此之外，按照個資法的規範，雲端業者在服務停用或終止時具有必須主動進行資料終結的義務，發生資安事件時必須進行查明及通知，而且在個資法施行細則通過後，再搭配經濟部建立的資料隱私保護標章制度，未來雲端業者必須建立符合規範的個資安全保護措施，這些部分雖然個資法沒有要求雲端業者要向使用者進行說明，實際上業者的定型化約款也缺乏這些事項的記載，但仍舊不影響業者的該項義務。另外個資法也有許多民事賠償、行政處罰、甚至刑事罰責的規定，我們也建議業者有修訂這些條款的必要，以避免觸犯相關法規。個資法修正後雖然不盡完善，但也讓我國在雲端個資保護時代建立了重要的里程碑，不過個資保護的落實仍然必須仰賴主管機關積極的進行查核和監督工作，因此我們也建議主管機關應該會同消費者保護委員會制訂更完善及更有利於使用大眾的雲端運算服務定型化契約範本，將這些我們關心的議題及個資法上雲端業者應該有的義務納入規範，讓使用者更明確瞭解及監督雲端算時代的權利義務及個資隱私保障，這不僅減少主管機關的稽查業務壓力，也能讓社會大眾明白在雲端時代個資保護應與消費者保

護受到同等的重視。

以下我們嘗試列出按照前述雲端條款的分析，以及經過消保法和個資法討論後對於雲端使用者較公平與對雲端業者較合乎法令規範的雲端條款，為本論文的研究回顧做各總結：

(1) 雲端服務條款何時視為接受與生效，例如當使用者註冊申請帳號或使用服務時，雲端服務條款即視為接受與生效。

(2) 說明蒐集、利用與處理哪些使用者的資訊、些資訊的內容類型為何，以及蒐集、利用與處理資訊的目的為何，例如除了進行雲端服務的提供外，是否進行線上廣告或其他的資訊應用，服務的內容為何及是否受到智財權的保護，此外蒐集、利用與處理資訊的目的亦須明確告知使用者。如若業者要求使用者進行資料的授權，亦須明確說明授權的範圍及利用目的為何。

(3) 使用者資料流通的範圍為何，流通的對象必須可得特定，例如是否流通給子公司或其他的廣告業者，而且必須說明進行這些資料流通時亦受到也者的隱私權保障。另外亦須說明在雲端服務進行整併時，資料如何進行流通或終結處理。

(4) 具體說明採取何種「適當」的安全措施，個資事件發生時主動向使用者進行說明的義務，以及合於法令應負擔的損賠責任。

(5) 說明使用者如何進行資料的增刪修改，何時可以停用服務，業者在什麼情況時可以終止、中斷或暫停服務，以及這些情形發生時資料的終結機制及業者對資料的終結義務。

(6) 符合消保法及個資法規定的管轄條款及準據法條款。

(7) 業者可以保有隨時修改條款的權利，唯須提供使用者不同意時的退場與資料終結機制。

第二節　雲端服務條款探討對其他雲端法律議題的影響及展望

雲端運算服務能夠成為目前資訊時代的主流，就是因為建立在使用者將資訊傳至雲上進行運算及儲存的模式，讓使用者能夠透過網路隨時隨地接觸到雲端資源，但這種模式也讓提供雲端服務的業者接觸到使用者的資訊，隨之而來的就是本文我們討論到的許多雲端個資風險，這當然就必須要從雲端服務的隱私權政策與服務條款著手，讓雲端業者和使用者間的法律關係立於平等的基礎，來建立對使用者相對有保障的雲端使用環境。

不過除了這些雲端業者帶來的風險以外，雲端業者掌握的這些個人資訊，也讓政府部門更容易及更有誘因對雲端進行大規模的監視或搜索。在雲端時代，各種資訊和網路行為上雲端，雲端服務即將取代傳統個人電腦的使用方式，連帶也使得這些雲端業者成為政府機關進行數位搜索扣押的關鍵，這也意謂著在雲端時代中要搜索數各嫌疑人的資料，政府機關不用在像過去勞師動眾逐個搜索嫌疑人的電腦或資料，現在可能只要要求雲端業者揭露相關資料即可，大幅降低政府進行搜索的成本。那麼我們所討論的雲端條款就對這種公部門搜索雲端的情況產生很大的作用，雲端業者必須告訴使用者在哪些情況會配合公部門的搜索行動，對公部門哪些不合理的行為業者會堅定拒絕等等。這些公部門搜索雲端的情況當然也會衍生出刑事訴訟的正當法律程序、通訊監察、甚至隱私人格權保障等等法律議題，或者雲端業者是否為我國刑事訴訟法第 247 條所規定之該管機關，檢察官得否要求進行必要之報告，這些議題都值得進行更深入的研究。

除了公部門搜索雲端侵害隱私的議題外，雲端服務的便利與彈性，同樣也能夠促使政府部門採用雲端服務，從美國歐巴馬政府的 www.apps.gov 計畫、英國政府的 G-Cloud 平台計畫、日本政府的霞關 Cloud 計畫，到我國政府計畫將電子病例及貨櫃資料中心與雲端相結合，各國政府莫不將建

立 e 化雲端政府作為當前的重大政策。但是 e 化雲端政府同樣有可能產生各種資訊安全的問題，而且雲端政府處理的是大量公部門及民眾資料，一旦產生資訊安全漏洞或是管理不當，將造成國家安全及全民福祉的重大傷害。尤其我國政府除了有要將全民健康資料及經濟資料雲端化的政策規劃外，甚至連國防部都計畫引進雲端平台，要利用雲端技術將公文官章和會議紀錄上雲端，並且建構智慧卡系統及軍方 MSN 系統，取代進出營區的識別及公文上的電子戳章，其目的在於減少電腦伺服器的使用及推動公文無紙化，達到政府節能減碳的政策目的。雖然這種政策方向立意良好，但是雲端上放置大量國防機密資料，勢必成為網軍攻擊及間諜活動的目標，一旦國防雲產生系統或人為的漏洞，對國家安全的危害將不言可喻，特別是在 2010 年底我國國安系統才遭逢羅奇正間諜案的重創，國安單位是否有能力保障國防雲的安全,有必要對管理面及政策面好好進行檢討。因此，不管公部門上雲端是要委外建立雲端平台或政府自行建立，本文我們針對雲端隱私政策與服務條款進行的討論對於未來這些議題的研究都相當值得參考。尤其當政府要委外建立雲端平台時，特別要注意我們一再強調的安全保護機制的確立與落實、明確資訊處理的目的及流通的範圍、如何確實進行資料終結，以及公共雲更不可再讓委外雲端業者取得資料的授權等等議題。

雲端服務的使用者除了會希望能隨時隨地接觸到雲端服務外，可能會有另一個期望就是在雲上的創作能夠受到著作權法的保護，或者是在雲上使用的軟體及服務能能夠免去著作權的爭議。例如使用者已經取得某軟體的授權，但是傳統的軟體授權方式卻僅是針對單一機器的使用，那麼這種授權方式是否也能在雲端時代有所適用？雲端運算最大的一項特點就是使用者會將數據資料移轉至雲端上進行運算，但是一般的軟體授權卻是禁止再行散佈，所以對於雲端上使用這些授權軟體就會產生問題，而且在許

多情況下，使用者只是利用雲端資源在進行運算，實際上提供雲端服務的業者並非傳統意義下在使用這些授權軟體。這種情形也不僅只發生在授權軟體或服務上，雲端服務的便利也讓許多影音視頻業者開始在雲端上建立服務平台，例如全美最大電影租借網站 Netflix 就宣布將大幅改用 Amazon 的雲端服務來取代原本的資料中心，並且從雲端直接提供給用戶影音串流、影片推薦等服務，這類型的影音著作物分享應用模式同樣也只是在雲端上進行儲存、流通或處理的動作，雲端業者也並非傳統意義下在使用這些影音著作物，更類似的概念可能是像倉儲或物流公司在流通傳遞這些著作物。因此也有必要重新檢討這些軟體或服務授權與影音著作物利用雲端服務的性質，以及著作權法上對於著作物複製、散佈或合理使用的相關議題，本文我們針對雲端條款進行的討論，也可以對這些問題進行啟發，例如對於這些軟體或影音著作資料的終結如何處理等，都可以留待未來進行這方面研究時的參考。

雲端運算是個還在發展中的新興技術及產業，因此不時會有新的產業應用與商業模式產生，也不斷衝擊原有的法律規範，讓原本的民事法律、消費者保護、個人資料隱私保護及著作權法的體系跟不上科技發展的腳步，現在就連公部門也想上雲端，或者利用雲端運算的特性對民眾進行更全面的搜索或監控。這些現象的產生，很多是因為雲端使用者將資訊交予雲端伺服器，讓雲端業者也掌握分享了使用者資訊，使得資訊隱私的風險大幅提升。於這些風險有必要藉由雲端隱私權政策與服務條款來平衡，但是業者自訂的這些條款顯然並不是在緩和風險，反而還可能是提高風險而導致資訊安全的危害，而大多數的使用者卻不瞭解隱私政策與服務條款的內容為何，使得雲端業者藉由資料的蒐集與分析比對瞭解使用者太多，但使用者對於享受雲端運算服務時所產生的權利義務卻瞭解太少。因此，我們希望藉由本文的分析討論，讓更多使用者瞭解到雲端隱私權政策與服務條款

的內含為何，使用者在享受雲端服務時知道有哪些權利應該被保障，並且期待能夠喚醒更多關心個資安全的人士來共同關注雲端時代個資安全及隱私保護的議題。

參考資料

一、英文部分

(一) 英文專書

1. TIM MATHER ET AL., CLOUD SECURITY AND PRIVACY: AN ENTERPRISE PERSPECTIVE ON RISKS AND COMPLIANCE (2009).
2. RUTH L. OKEDIJI, DEVELOPMENT IN THE INFORMATION AGE: ISSUES IN THE REGULATION OF INTELLECTUAL PROPERTY RIGHTS, COMPUTER SOFTWARE AND ELECTRONIC COMMERCE (2004).
3. MANUEL CASTELLS, THE INTERNET GALAXY: REFLECTIONS ON THE INTERNET, BUSINESS AND SOCIETY (2001).
4. NICHOLAS CARR, THE BIG SWITCH , REWIRING THE WORLD, FROM, EDISON TO GOOGLE (2009).
5. REINHOLD QUILLEN, CLOUD COMPUTING – HYPE AND REALITY, QUILLEN INFRASTRUCTURETECHNOLOGIES (2010).
6. EUROPEAN AND INFORMATION SECURITY AGENCY, CLOUD COMPUTING BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY (2009).
7. KATARINA STANOEVSKA-SLABEVA ET AL. ED., CLOUD COMPUTING: A BUSINESS PERSPECTIVE ON TECHNOLOGY AND APPLICATIONS (2009).
8. 2010 AAAI SPRING SYMPOSIUM SERIES (2010).

(二) 英文期刊論文

1. David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009).

2. Paul T. Jaeger et al., *Cloud Computing and Information Policy: Computing in a Policy Cloud?* , 5 J. INFO. TECH. & POL. 269 (2008).
3. Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1 (2008).
4. Mark H. Wittow, Daniel J. Buller, *Cloud Computing : Emerging Legal Issues For Access to Data, Anywhere, Anytime*, 14 NO. 1 J. INTERNET L. 4 (2010).
5. Miranda Mowbray, *The Fog Over the Grimpen Mire: Cloud Computing and the Law*, 6 SCRIPTED 132 (2009).
6. John Biggs, *OnLive Cloud Gaming Service Goes Live June 17*, TECHCRUNCH (2010)
7. Andrew C. Devore, *Cloud Computing: Privacy Storm on The Horizon?*, 20 ALB. L.J. SCI. & TECH. 365 (2010).
8. Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., (2010)
9. Paul Lanois, *Caught in The Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 NW. J. TECH. & INTELL. PROP. 29 (2010).
10. David S. Barnhill, *Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless*, 25 BERKELY TECH. L.J. 621 (2010).
11. William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy under the Stored Communications Act*, 98 GEO. L.J. 1195 (2010).
12. EPIC, *Complaint and Request for Injunction, Request for Investigation and for Other Relief*, March 19 (2009).
13. Andrea Cascia, *Don't Lose Your Head in the Cloud: Cloud Computing and Directed Marketing Raise Student Privacy Issues in K-12 Schools*, 261 ED. LAW REP. 883 (2011).

14. R. Buyya, et al., *Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*, FUTURE GENERATION COMPUTER SYSTEMS (2009).
15. Amit Mehra, *Evolution of the Cloud*, 8 NO 3, ISB INSIGHT 30 (2010).
16. European Commission, *The Future of Cloud Computing, Opportunities for European Cloud Computing Beyond* (2010).
17. Ashkan Soltani et al., *Flash Cookies and Privacy* (2009), *available* at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862
18. Jayni Foley, *Are Google Searches Private? An Originalist Interpretation of The Fourth Amendment In Online Communication Cases*, 22 BERKELEY TECH. L.J. 447 (2007).
19. Lisa J. Sotto et al., *Privacy and Data Security Risks in Cloud Computing*, 15 ECLR 186 (2010).
20. Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM, (2009).
21. Francoise Gilbert, *Cloud Service Contracts May Be Fluffy: Selected Legal Issues to Consider Before Taking off*, 14 NO. 6 J. INTERNET L. 18 (2010).
22. Shellie Stephens, *Going Google: Your Practice, the Cloud, and the ABA Commission on Ethics 20/20*, U. ILL. J.L. TECH. & POL'Y 237 (2011).
23. Timothy D. Martin, *Hey! You! Get Off My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security and Property in Cloud Computing*, 92 J. PAT. & TRADEMARK OFF. SOC'Y 283 (2010).
24. Konstantinos K. Stylianou, *An Evolutionary of Study of Cloud Computing Services Privacy Terms*, 27 JMARJCIL 593 (2010).
25. James Sunosky, *Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles*, 9 CURRENTS INT'L TRADE L.J. 80 (2000).
26. Kevin J. Delaney et al., *Google Plans Service to Store User's Data*, WALL ST. J., (2007).
27. Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and*

Government back Doors in the Web 2.0 ERA, 8 J. TELECOMM. & HIGH TECH. L. 359 (2010).

28. APEC Data Privacy Subgropu Meeting, *APEC Corporation Arrangement for Cross-Border Privacy Enforcement*, Febryary, 28, 2010. *available* at http://www.ftc.gov/os/2010/02/1002apecprivacyenforce.pdf.
29. Aameek Singh et al., *Agyaat: mutual anonymity over structured P2P networks*, 16 NO.5 INTERNET RESEARCH 189 (2006).
30. William R, Denny, *Survey of Recent Developments in the Law of Cloud Computing and a Software and a Service agreement*, 66 BUS. LAW. 237 (2010).
31. Robert H. Carpenter, *Walking from Cloud to Cloud: the Portability Issue in Cloud Computing*, 6WASH.J.L. TECH. & ARTS 1 (2010).
32. W. Michael Ryan et al., *Insights into Cloud Computing*, 22 NO. 11 INTELL. PROP. & TECH. L.J. 22 (2010).
33. Robert Sprague, Cloud Privacy: Normative Standards for Information Privacy Management Within Cloud Computing, 2010 AAAI Spring Symposium Series 164.
34. Chris Conley, The Right to Delete, 2010 AAAI Spring Symposium Series 53.

(三) 英文新聞及網路資料

1. Flickr, http://www.flickr.com/
2. Microsoft, http://www.Microsoft.com/licensing/default.aspx
3. Windows Azure, http://www.microsoft.com/windowsazure/
4. J. Nicholas Hoover, *Interop: Oracle Predicts Cloud Confusion to Continue*, Informationweek,Sept. 12, 2008, http://www.informationweek.com/news/services/hosted_apps/showArticle.jhtml?articleID=210602225.
5. John B. Horrigan, *Cloud Computing Gains in Currency*,

PewResearchCenter Publications, September 12, 2008, http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency

6. Animoto's Facebook Scale-up, Right Scale Blog, http://blog.rightscale.com/2008/04/23/animoto-facebook-scale-up/
7. Elastic Compute Cloud (EC2), http://aws.amazon.com/ec2
8. Simple Storage Service (S3), http://aws.amazon.com/s3
9. *Behavioral Advertising Survey*, March 4, 2009, TRUSTe, http://www.truste.com/privacy_webinars/bt_slides.pdf
10. Gartner, *Gartner Says Cloud Computing Will Be As Influential As E-business*, June 26, 2008, http://www.gartner.com/it/page.jsp?id=707508
11. Krissi Danielson, *Distinguishing Cloud Computing from Utility Computing*, ebiz.net, March 26, 2008, http://www.ebizq.net/blogs/saasweek/2008/03/distinguishing_cloud_computing/.
12. Robert D. Holf, *Jeff Bezo's Risky Bet*, Bloomberg Businessweek, November 13, 2006, http://www.businessweek.com/magazine/content/06_46/b4009001.htm.
13. Donna Bogatin, *Google CEO's New Paradigm: Cloud Computing and Advertising Go Hand-in-hand*, ZDNet News&Blof, August 23, 2006, http://www.zdnet.com/blog/micro-markets/google-ceos-new-paradigm-cloud-computing-and-advertising-go-hand-in-hand/369.
14. Erick Arvidsson, *Gears API Blog: Going Offline with Google Gears*, Gears API Blog, May 30, 2007, http://gearsblog.blogspot.com/2007/05/posted-by-aaron-boodman-and-erik.html.
15. Google, *A Fresh Taker on the Browser*, The Official Google Blog, September 1, 2008, http://googleb log.bl.
16. Google, *Introducing the Google Chrome OS*, The Official Google Blog, July 7, 2009, http://googleblog.blogspot.com/2009/07/introducing-google-chrome-os.ht

ml.

17. Ina Fried, *Microsoft Launches Windows Azure*, CNET NEWS, October 27, 2008, http://news.cnet.com/microsoft-launches-windows-azure/.
18. Robert Palmer, *Apple Adds Another Month Free for Some MobileMe Trials*, The Unofficial Apple Weblog, July 22, 2008, http://www.tuaw.com/2008/07/22/apple-adds-another-month-free-for-uk-mobileme-trials/.
19. Steve Lohr, *Google and IBM Join in Cloud Computing Research*, The New York Times, October 8, 2007, http://www.nytimes.com/2007/10/08/technology/08cloud.html?_r=2&ex=1349496000&en=926.27f0f65ea0d75&ei=5090&partner=rssuserland&emc=rss&oref=slogin.
20. Rackspace, *Rackspace Open Source Cloud Platform; Announces Plans to Collaborate with NASA and other Industry Leaders On Openstack project*, Rackspace Newsroom, July 19, 2010, http://www.ra.ckspace.com/information/newsroom/pressreleases/rackspace-open-sources-cloud-platform-announces-plans-to-collaborate-with-nasa-and-other-industry-leaders-on-openstack-project/.
21. Microsoft, *Openstack is Now Open For Windows Server*, Microsoft News Center, October 22, 2010, http://www.microsoft.com/Presspass/press/2010/oct10/10-22OpenStackPR.mspx
22. Lew Tucker, *Cisco Joins Openstack Community*, Cisco Blog, February 3, 2011, http://blogs.cisco.com/news/cisco-joins-openstack-community/
23. Brand Smith, Keynote Address at the Brookings Institution: Cloud Computing for Business and Society, January 20, 2010, http://www.microsoft.com/presspass/presskits/cloudpolicy/docs//20100120_transcript.pdf.
24. S.E. Slack, *Is There Value in Cloud Computing?*, IBM developerWorks, March 31, 2009, http://www.ibm.com/developerworks/architecture/library/ar-valuecloudco

mputing//?S_TACT=105AGX01&S_CMP=HP.

25. NIST Definition of Cloud Computing: http://www.nist.gov/itl/cloud/.
26. Tectdirt, *Google Finally Realizes It Needs to Be the Web Platform*, April 7, 2008, http://www.techdirt.com/articles/20080407/225749782.shtml
27. Wikipdeia definition of co-location facilities: http://en.wikipedia.org/wiki/Colocation_facility
28. Wikipdeia definition of web2.0: http://en.wikipedia.org/wiki/Web2.0
29. Wikipdeia definition of cloud computing: http://en.wikipedia.org/wiki/Cloud_computing.
30. Wikipdeia definition of miltitency: http://en.wikipedia.org/wiki/Multitenancy.
31. Wikipdeia definition of Facebook: http://en.wikipedia.org/wiki/Facebook.
32. Wikipdeia definition of Eucalyptus: http://en.wikipedia.org/wiki/Eucalyptus_(computing).
33. Wikipdeia definition of semantic web: http://en.wikipedia.org/wiki/Semantic_Web.
34. Wikipdeia definition of HTTP Cookie: http://en.wikipedia.org/wiki/Cookie_(web)
35. Wikipdeia definition of web beacon: http://en.wikipedia.org/wiki/Web_beacon.
36. Wikipdeia definition of web adobe flash: http://en.wikipedia.org/wiki/Adobe_Flash.
37. Wikipdeia definition of web search query: http://en.wikipedia.org/wiki/Web_search_query.
38. Wikipdeia definition of URL: http://en.wikipedia.org/wiki/URL.
39. Wikipdeia definition of Google China: http://en.wikipedia.org/wiki/Google_China.
40. Wikipdeia definition of Secure Sockets Layer: http://en.wikipedia.org/wiki/Secure_Sockets_Layer.
41. Wikipdeia definition of TRUSTe: http://en.wikipedia.org/wiki/TRUSTe.
42. SQL Azure, *available at*

http://www.microsoft.com/windowsazure/sqlazure/.

43. Zimory, *available at* http://www.zimory.com/index.php?id=77.
44. Elastichost *available at* http://www.elastichosts.com/cloud-hosting/pricing.
45. 2010 Rackspace Partner Leadership Summit, *Public Cloud? Private Cloud? What is the Difference?*, October 5, 2010, http://c1776742.cdn.cloudfiles.rackspacecloud.com/downloads/pdfs/PublicCloudPrivateCloudWhatistheDifference_PaulRad.pdf.
46. Mike Klein, *Public Cloud or Private Cloud?*, OTBlog, September 27, 2010, http://resource.onlinetech.com/public-cloud-or-private-cloud/.
47. David Linthicum, *Why the hybrid Cloud model is the Best Approach*, InfoWorld, January 27, 2011, http://www.infoworld.com/d/cloud-computing/why-the-hybrid-cloud-model-the-best-approach-477.
48. Openstack Web, *available at* http://openstack.org/projects/.
49. Will M, *Facebook Ads: "Keywords" Will Change to "Likes and Interests" This Week*, All Facebook, March 7, 2010, http://www.allFacebook.com/Facebook-ads-keywords-will-change-to-likes-and-interests-this-week-2010-03.
50. Declan McCullagh, *Tech Firms Warn Privacy Bill Will Harm Economy*, CNET NEWS, July 23, 2010, http://news.cnet.com/8301-31921_3-20011435-281.html.
51. Pete Cashmore, *RIP Facebook Beacon*, Mashable, September 19, 2009, http://mashable.com/2009/09/19/Facebook-beacon-rip/.
52. Ellen Nakashima, *Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy*, Washington Post, November 30, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503.html.
53. June Carlos Perez, *Facebook's Beacon More Intrusive Than Previously Thought*, PCWorld, December 1, 2007, http://www.pcworld.com/article/140182/Facebooks_beacon_more_intrusive_than_previously_thought.html

54. David Kravets, *Judge Approves $9.5 Million Facebook Beacon Accord*, WIRED, March 17, 2010, http://www.wired.com/threatlevel/2010/03/Facebook-beacon-2/.
55. Ryan Singel, *Privacy Lawsuit Targets Net Giants over 'Zombie' Cookies*, WIRED, July 27, 2010, http://www.wired.com/threatlevel/2010/07/zombie-cookies-lawsuit/.
56. Dean Takahashi, *Lawsuit Alleges Major Web Sites Spied on users via AddThis Tool*, Venture Beat, August 14, 2010, http://venturebeat.com/2010/08/14/lawsuit-alleges-major-web-sites-spied-on-users-via-addthis-tool/.
57. *Lara Farrar, Google.cn: R.I.P. or Good Riddance*?, CNN, March, 26, 2010, http://edition.cnn.com/2010/TECH/03/26/china.google.reaction/index.html .
58. Google Docs, http://docs.google.com.
59. Elizabeth Montalbano, *Sony BMG to Pay $1M to FTC for COPPA Violation*, COMPUTERWORD, December 11, 2008, http://www.computerworld.com/s/article/9123219/Sony_BMG_to_pay_1M_to_FTC_for_COPPA_violations.
60. APEC Privacy Principles, http://www.pmc.gov.au/privacy/apec/meetings.cfm.
61. INTAC, *Who Owns the Most Servers?*, Aprial 13, 2010, http://www.intac.net/a-comparison-of-dedicated-servers-by-company_2010-04-13/.
62. Dion Hinchcliffe, *What does Cloud Computing Actually Cost? An Analysis of the Top Vendors*, ebiz, August 22, 2009, http://www.ebizq.net/blogs/enterprise/2009/08/what_does_cloud_computing_actu.php.
63. Thomas Claburn, *Amazon S3 Crash Raises Doubts Among Cloud Customers*, InformationWeek, July 21, 2008, http://www.informationweek.com/news/services/storage/showArticle.jhtml?articleID=209400122

64. Julianne Pepitone, *Amazon EC2 Outages Downs Reddit, Quora*, CNNMoney, April 22, 2011, http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm.
65. Susan Boyle, *Facebook Defends its "Real Name" Policy*, NBC NEWS, May 20, 2009, http://www.ncbayarea.com/news/business/Facebook-Defends-its-Real-Name-Policy.html.
66. Simon Elegant, *Chinese Government Attacks Google over Internet Porn*, TIME, June 22, 2009, http://www.time.com/time/world/article/0,8599,1906133,00.html.
67. Maggie Shiels, *Google Tackles Child Pornography*, BBC, April 14, 2008, http://news.bbc.co.uk/2/hi/7347476.stm.
68. eMarketer, *Google and Yahoo Still Take More Overall Online Ad Dollars*, March 1, 2011, http://www.emarketer.com/Article.aspx?R=1008252.

二、中文部分

(一) 中文專書及研究報告

1. 王澤鑑，債法原理(一)， 2006 年 9 月版。
2. 王澤鑑，侵權行為法第二冊 特殊侵權行為，2006 年 7 月版。
3. 馮震宇、謝穎青、姜志俊、姜炳俊合著，消費者保護法解讀，2005 年 5 月版。
4. 行政院經建會委託研究報告，資訊服務業者配合政府公權力提供客戶資料之法制研究，計畫共同主持人潘維大、余啟民，2006 年 12 月。
5. 行政院研考會委託研究報告，計畫主持人林桓副，協同主持人余啟民，政府機關強化個人資料保護措施之研究，2009 年 10 月。

(二) 中文期刊論文

1. 陳起行，資訊隱私權法理探討—以美國法為中心，政大法學評論，64 期，2000 年 12 月。
2. 余啟民，由肺結核病患名單資料外洩談公務機關就醫資訊管控與監督，月旦民商法，24 期，2009 年 6 月。
3. 李治安，當法律漫步在雲端，法學新論，25 期，2010 年 8 月。
4. 劉靜怡，雲端運算趨勢與個人資訊隱私保護，全國律師，2010 年 2 月。
5. 劉靜怡，不算進步的立法：「個人資料保護法」初步評析，月旦法學雜誌，183 期，2010 年 8 月。
6. 廖緯民，論搜尋引擎的隱私權威脅，月旦民商法雜誌，24 期，2009 年 6 月。
7. 張乃文，雲端運算產業發展之策略規劃與法制因應，科技法律透析，2010 年 12 月。
8. 周慧蓮，英國個人資料保護最新案例發展及其對我國法制之啟示，資科技法律透析， 2005 年 1 月。
9. 黃立，消費者保護法：第四講 消保法的定型化契約條款(一)，月旦法學教室，14 期，2004 年 1 月。
10. 黃立，消費者保護法：第五講 消保法的定型化契約條款(二)，月旦法學教室，15 期，2004 年 2 月。
11. 程法彰，我國為因應重視個人資訊保護的趨勢所為對「個人資料保護法」修正的立法評析，萬國法律，173 期，2010 年 10 月。
12. 劉定基，「個人資料保護法」初論，台灣法學雜誌第 159 期，2010 年 9 月。
13. 王郁琦，優質網路社會下個人資料保護法制之因應，台灣科技法律與政策論叢，5 卷 2 期，2008 年 12 月。

14. 呂丁旺，淺析修正「個人資料保護法」，月旦法學雜誌，183 期，2010 年 8 月。
15. 經建會部門計畫處，推動新興智慧型產業系列二 雲端運算，台灣經濟論衡，第 8 捲第 7 期，2010 年 7 月。

(三) 中文新聞資料

1. 張玉琦，雲端運算風暴來襲，數位時代，2008 年 10 月。
2. 天下雜誌編輯部，無縫接起智慧新生活，天下雜誌，特刊 31 號，2010 年 2 月。
3. 黃亦筠，雲端運算 衝擊台灣硬體業者，天下雜誌，特刊 31 號，2010 年 2 月。
4. 戴佳慧，雲端電玩 OnLive 美國驚喜上市，數位時代，2010 年 11 月。
5. 趙郁竹，趨勢科技 11 月展示雲端科技系統，數位時代，2010 年 8 月。
6. 中央社，工研院雲端應運 盼 3 年 7 成診所用電子病歷，2009 年 11 月 6 日。
7. 蘇文彬，工研院雲端運用中心：明年底推出貨櫃資料中心與 OS，iThome，2009 年 12 月 14 日。
8. 王炙人，後蓋茲時代，微軟從雲端反擊 Google，數位時代，171 期，2008 年 8 月。
9. 張德厚，與學界合作 Google 推廣「雲端運算技術」，中廣新聞網，2008 年 1 月 30 日。
10. 謝佳雯，鴻海與資策會 共建雲端運算，經濟日報，2009 年 5 月 25 日。
11. 黃亦筠，筆電之後是什麼？林百里：我不去藍海，我去雲端，天下雜誌，特刊 31 號，2010 年 2 月。
12. 文茜的世界財經週報，林百里的願景與廣達的雲端佈局，2009 年 11

月 22 日。

13. 洪凱音，企業資料險 求償最高 2 億，經濟日報，2010 年 9 月 28 日。
14. 蘇湘雲，雲端加內容支援 Eee PC 嗆聲不怕 iPad，NowNews，2010 年 3 月 19 日。
15. 陳炳宏，升級出包？全球 15 萬 Gmail 用戶受駭，自由時報，2011 年 3 月 1 日。
16. 德宜，借鑑歐盟作法，強化我國個人資料保護規範與措施，Taiwan News 財經，文化週刊，2004 年 11 月。
17. 湯蕙如，資安/MSN 好友要你買 MyCard?小心，可能是騙局！，NOWnews，2010 年 11 月。
18. 林亞蓁，徐美渝，Yahoo! 奇摩交友 11 月 30 日終止服務，MOL 銘報即時新聞，2010 年 10 月 10 日。
19. 劉翰謙，Google+，真正的 Facebook 威脅？，數位時代，2011 年 6 月 29 日。

(四) 中文網路資料

1. Openfind 企業郵件代管系統，http://www.mailasp.com.tw/.
2. 台北市動態公車資訊網，http://www.taipeibus.taipei.gov.tw/.
3. 資訊討論網站 mobile01，http://www.mobile01.com/index.php.
4. 倪慈緯，中華電信推出多項計費方式的雲端服務，RUN!PC，2011 年 2 月 26 日，http://www.runpc.com.tw/news.aspx?id=100531.
5. 無名小站，中文維基百科 http://zh.wikipedia.org/wiki/%E7%84%A1%E5%90%8D%E5%B0%8F%E7%AB%99.
6. 無名小站，中文維基百科 http://zh.wikipedia.org/wiki/%E7%84%A1%E5%90%8D%E5%B0%8F%

E7%AB%99

7. 張維君，個資法施行細則 定義 12 項適當安全維護措施，資安人，2011 年 4 月 25 日，http://www.isecutech.com.tw/article/article_detail.aspx?aid=6108.
8. 廖珮君，TPIPAS 上路 個資保護有標章可循，資安人，2011 年 4 月 11 日，http://www.isecutech.com.tw/article/article_detail.aspx?aid=6094.
9. 法務部，立法院三讀通過「個人資料保護法」新聞稿，2010 年 4 月 27 日，http://www.moj.gov.tw/public/Data/0427164423187.pdf
10. 行政院主計處，中華民國行業標準分類(第 9 次修訂)，參考 http://www.stat.gov.tw/ct.asp?xItem=28854&ctNode=1309.
11. 財團法人網路資訊中心，2010 台灣無線網路使用調查報告，http://www.twnic.net.tw/download/20307/1007d.pdf

三、判決資料

1. United States v. Microsoft Corp., 253 F.3d (D.C. Cir. 2001)
2. Case T-201/04, Microsoft v. Comm’n, 2007 ECJ CELEX LEXIS 554, 2007 WL 2693858。
3. Lane v. Facebook, Inc., No. C 08-3845 RS, 2010 U.S. Dist. LEXIS 24762 (N.D. Cal. March 17, 2010).
4. Edward Valdez v. Quancast Corp., No. CV10-5484 (C.D. Cal. July 23, 2010)
5. White v. Clearspring Techs. Inc., No. CV10-5948 (C.D. Cal. August 10, 2010).
6. La Court v. Specific Media Inc., No. CV10-01256 (C.D. Cal. August 18, 2010).

7. Gonzales v. Google, Inc., 234 F.R.D. 674, 679 (D. Cal. 2006).

四、雲端運算隱私權政策

1. Google 隱私權政策：
   http://www.google.com.tw/intl/zh-TW/privacy/privacy-policy.html
2. Yahoo 隱私權政策：http://info.yahoo.com/privacy/tw/yahoo/
3. Facebook 隱私權政策：
   http://www.facebook.com/privacy/explanation.php#!/policy.php
4. Plurk 隱私權政策：http://www.plurk.com/privacy
5. Twitter 隱私權政策：http://twitter.com/privacy
6. Amazon 隱私權政策：
   http://www.amazon.com/gp/help/customer/display.html?nodeId=468496#share
7. Windows Azure 隱私權政策：
   http://privacy.microsoft.com/en-us/fullnotice.mspx#use
8. Xuite 隱私權政策：
   http://member.cht.com.tw/html/MemberCenter2/privacy.html
9. 痞客邦 PIXNE 隱私權政策：http://www.pixnet.net/privacy

五、雲端運算服務條款

1. Google 服務條款：http://www.google.com.tw/accounts/TOS
2. Yahoo 服務條款：http://tw.info.yahoo.com/legal/utos.html
3. Facebook 服務條款：http://www.facebook.com/terms.php?ref=pf

4. Plurk 服務條款：http://www.plurk.com/terms
5. Twitter 服務條款：http://twitter.com/tos
6. Amazon 服務條款：http://aws.amazon.com/terms/
7. Windows Azure 服務條款：
   http://www.microssoft.com/about/legal/en/us/IntellectualProperty/Copyright/Default.aspx
8. Xuite 服務條款：
   http://member.cht.com.tw/html/MemberCenter2/service.html
9. 痞客邦 PIXNE 服務條款：http://www.pixnet.net/regulation