

資通安全 法律案例精選



www.icst.org.tw

行政院國家資通安全會報技術服務中心 編印
中華民國一〇四年九月

序

近年資通訊技術的蓬勃發展與快速變遷，翻轉個人與組織的資訊運用模式，而現今與未來所面臨的資安法律議題及風險，顯然更加複雜多元化，需要透過新的視野進行思考與問題解決方式。有鑑於此，世界經濟論壇 (World Economic Forum, WEF) 日前提出 2015 年全球風險報告，即已預警網路攻擊不斷擴大與升級、網路資料偽造與竊取事件層出不窮，將會是全球下一波面臨的嚴峻挑戰。無獨有偶地，美國聯邦貿易委員會 (Federal Trade Commission, FTC) 同年公開的網路安全建議報告中，也指出智慧型裝置可能衍生更多的隱私與安全議題，包括個人資料濫用、駭客攻擊等風險，皆需加以正視與因應。於此趨勢下，資安風險涉及類型多樣化，伴隨而來的法律議題也挑戰我國資安體系。

行政院國家資通安全會報技術服務中心 (以下簡稱技服中心) 長期擔任強化與推廣我國資通安全意識之角色，並發行「資通安全法律案例宣導彙編」，期能透過匯集最新資安時事動態與法律實際案例，深入淺出的說明法律觀點與專業剖析，並與 ISO 27001 資訊安全管理標準之控制條文觀念結合，釋疑資通安全法律案例，以做為各界實務運作參考。

「資通安全法律案例宣導彙編」自民國 91 年發行至今已發行 11 輯，於全球資訊安全生態快速變遷，國內重要資安法律亦與時俱進之際，技服中心於今年挑選具代表性之經典案例，重新編寫並發行「資通安全法律案例精選」，藉此回顧資通安全法律之過去，了解現在，領略未來之趨勢脈動。

誠摯希望本精選之發行，能夠持續為各界利用，成為政府機關與社會大眾進行資訊安全法治教育時之重要參考，帶動新興資訊應用發展應有的基本法律概念。

行政院國家資通安全會報 技術服務中心

劉培文 主任謹識

編者序

行政院資通安全辦公室與行政院國家資通安全會報技術服務中心是國內最主要的資訊安全推動單位，對於建構國家資訊安全體系向來不遺餘力。在全球資安事件頻傳、資安風險不斷提升之情形下，顯得任重而道遠。

為協助建立及推廣國內各界關於資通安全之意識，本所長期投入「資通安全法律案例宣導彙編」編輯與撰寫，希望能夠從法律及管理之角度切入，帶給國人即時、豐富且實用的資安法律資訊。而在這段時間當中，國際環境、資通技術快速變化，國內重要資安法律也接連修正。

為此，在「資通安全法律案例精選」，本所特別挑選具代表性之經典案例，並配合前述相關法規修正、實務見解轉變等多項因素重新編寫，以全新的面貌將經典案例進行整合呈現。在整理設計上，本精選將分為「政府資安素養」及「全民資安素養」兩大章節，區分不同之關注焦點。在各篇之設計上，均先以「精選案例回顧」說明經典案例之時事新聞、判決事實基礎或要旨；其次，在「後續追蹤」將介紹類似案件、相關法規或實務判決之發展、趨勢或轉變。而在「關鍵透析」之部分，則將配合案例重點及法律分析內容進行歸納說明，使讀者透過深入淺出的文字或圖表，迅速提綱挈領，以掌握閱讀重點。

最後，以本精選所挑選之經典案例及法律解析，期待可以做為資訊安全法制領域討論平台，讓讀者以此基礎聚焦並延伸學習，進而帶動整體資訊安全法律之關注與發展。

國巨律師事務所

朱瑞陽合夥律師 謹識

Contents 目錄

Chapter I 政府資安素養

- | | |
|--------------------------------|----|
| 1.機關應依案件性質，判斷公文所涉當事人姓名有無遮蔽必要 | 2 |
| 2.保護手機使用安全，政府推動行動應用 App 資安基本規範 | 6 |
| 3.衛福部將健保資料庫提供學術研究，法院認定符合個資法 | 11 |
| 4.政府採購涉及個資作業之業務，應於契約中約定監督事項 | 16 |
| 5.政院積極推動政府開放加值資料，強化資料釋出並提升品質 | 20 |

Chapter II 全民資安素養

- | | |
|----------------------------------|----|
| 1.民眾使用自動化訂票程式，致干擾網站服務，恐負有刑責 | 26 |
| 2.雇主不得要求應徵者或員工提供與工作無關之隱私資料 | 30 |
| 3.員工在工作場所通訊內容仍受隱私權保護，公司監看應事先告知 | 34 |
| 4.法院以臺灣○○公司並無搜尋引擎業務，駁回球團老闆主張被遺忘權 | 38 |
| 5.為維護法庭秩序，民眾未經許可不得逕為錄音錄影 | 43 |

附 錄

- | | |
|---------------|----|
| 1.自我評量 | 48 |
| 2.資通安全法規更新對照表 | 56 |

機關應依案件性質，判斷公文所涉當事人姓名有無遮蔽必要

精選案例回顧

陳情或檢舉乃是人民參與公共事務、抒發民意的方式之一，由於陳情或檢舉的內容，常涉及對特定機關或公務員之不利事項或指控，也可能包含陳情者或檢舉者的個人資料，行政機關應對陳情者或檢舉者的身分或個人資料予以保密，使民眾無須擔憂陳情或檢舉後可能遭致之不利後果，以鼓勵人民勇於檢舉不法，幫助政府改善行政事務的品質。

過去曾有民眾透過市長信箱投訴官員，當時投訴頁面明確標示「檢舉郵件之檢舉人基本資料將採保密方式處理」，未料機關在作業過程中暴露檢舉人身分，檢舉人竟於數日後接到被投訴者之電話指責。另曾發生退役教官向某部會陳情，該部會卻將陳情書涉及個資之部分，包含陳情人姓名、職稱及電子郵件等資料，一併公佈於網站「常見問題集」，該案件後來由臺北地方法院判決要求該部會賠償，此為公務機關因侵害個人資料判賠的罕見案例。

寫下您的來信

一、檢舉郵件之檢舉人基本資料將採保密方式處理，但因業務需要，承辦機關得調閱陳情人基本資料以供處理

二、為確保他人權益，陳情或檢舉案件，應內容具體或明確列舉事證，否則本府將依規不予處理或不予受理。

*來信主題：

*內容：

內容字數請勿超過1000個中文字(若內容較長，可利用文書編輯軟體(如WORDPAD、WORD)打好後，再用附件夾檔的方式處理)。

發生地點：

設定 清除

是否上傳附件：

否，我沒有附件。

是，(最多3個檔案，每個檔案需小於5MB)

瀏覽...

檢舉郵件之檢舉人基本資料將採保密方式處理

資料來源：○市政府網站

圖 1：○市市長信箱進入頁面

案例出處：

資通安全法律案例宣導彙編第 9 輯【案號：D1000101】

資通安全法律案例宣導彙編第 9 輯【案號：S1000405】

後續追蹤

依「行政院及所屬各機關處理人民陳情案件要點」第 3 點與第 4 點規定，民眾檢舉或陳情時必須附上真實姓名，因此陳情的內容會包含民眾的個人資料。為保護陳情或檢舉的民眾，行政程序法第 170 條第 2 項規定，人民之陳情有保密必要者，

受理機關處理時，應不予公開；又各機關現在也都有相關受理陳情的保密規定，如前述的「行政院及所屬各機關處理人民陳情案件要點」，及各級縣市政府的受理檢舉陳情案件保密實施要點等，但還是常出現陳情人或是檢舉人個人資料曝光的事件。

同樣也是民眾主張權利及參與公眾事務方式的訴願程序，亦曾發生類似的事件。我國目前在政府資訊公開的趨勢下，依政府資訊公開法第 7 條第 1 項第 7 款規定，訴願決定應主動公開，訴願法第 89 條第 1 項第 1 款亦規定，訴願決定書應載明訴願人之姓名、出生年月日、住居所及身分證明文件字號等個人資料。但有媒體於民國 103 年對行政院 12 部會的調查發現，有 7 部會將訴願人姓名直接公開於網路上，該等部會雖是依政府資訊公開法規定主動公開訴願書，但部分經公開的訴願決定書上，還留有訴願人的地址與電話，媒體更依某部會公布的訴願決定書資訊直接找到該訴願人，造成訴願人困擾。該事件發生後，該部會緊急將訴願決定書下架，但仍主張法令沒有規定哪些資料不能公開，並稱精神衛生法與性騷擾防治法僅限制媒體不得揭露訴願人姓名，行政機關的訴願書揭露訴願人姓名，並不在適用範圍。

該部會的回應引發外界批評。對此，政府資訊公開法第 18 條第 1 項第 6 款即規定，政府資訊如公開或提供有侵害個人隱私、職業上秘密或著作權人之公開發表權者，應限制公開或不予提供之。但對公益有必要或為保護人民生命、身體、健康有

必要或經當事人同意者，不在此限。是以，機關依法公開政府資訊時仍應注意該法第 18 條及其他法規（例如，精神衛生法與性騷擾防治法）之特別規定，以確定哪些資訊是應予保護的類型。前項新聞顯示，政府機關處理民眾資訊的方式仍有進步的空間。

關鍵透析

不論是陳情或訴願，現行法有許多對於陳情人或訴願人個人資料應保密或公開的規定，但這些條文都使用「必要」兩字（如行政程序法第 170 條、行政院及所屬各機關處理人民陳情案件要點第 18 點，以及政府資訊公開法第 18 條第 1 項第 6 款等）。何謂「必要」是一個不確定法律概念，要如何解釋個案情況是有保密或公開之必要，行政機關享有一定程度的判斷餘地。但由於目前網路科技發達，只要握有部分資訊就可以透過資料的對照、組合連結到特定個人，對於個人資料應採取更周全的保護，更何況陳情與訴願時必須附上真實姓名與聯絡資訊涉及個人隱私，且亦為個人資料保護法（以下簡稱「個資法」）所保護的個人資料。此類資料一經洩漏，不僅會帶給當事人困擾，公務員本身亦可能須面臨刑法與個資法上的相關民、刑事責任，公務機關處理陳情與訴願案件，判斷有無遮蔽當事人個資的必要時，仍應謹慎為上。

保護手機使用安全，政府推動行動應用App資安基本規範

精選案例回顧

日前資訊安全公司測試證實，手機製造商北京○○科技有限責任公司（以下簡稱北京○○公司）生產之手機，會自動將使用者背景資料傳送至北京伺服器。北京○○公司隨後坦承，使用者利用其「網路簡訊服務」時，在未經使用者同意下，該服務會自動將使用者電話號碼、國際行動設備識別碼 (International Mobile Equipment Identity) 及國際行動用戶識別碼 (International Mobile Subscriber Identity)，回傳至北京○○公司位於中國北京的伺服器上。○○公司表示資訊均以明碼傳輸，因此有能力的網管人員確實能夠利用監控工具，竊取使用者電話號碼。

事件發生之後，我國國家通訊傳播委員會（以下簡稱「通傳會」）展開調查，函請該公司之臺灣子公司（以下簡稱「臺灣○○公司」），針對事件始末與後續因應措施提出說明，並

著手調查其他手機業者有無類似情形。行政院指示經濟部工業局與通傳會，針對手機軟、硬體資安進行分工。因此，通傳會鼓勵手機製造廠商進行自願性測試後，公開資訊以利消費者參考，並規劃測試機制，預計最快於民國 104 年底上路。

案例出處：
資通安全法律案例宣導彙編第 11 輯【案號：S1030106】

後續追蹤

依據個人資料保護法（以下簡稱「個資法」）第 51 條第 2 項規定：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法」。而所謂中華民國領域外，係指我國政府法權未及之地域。在本案中，北京○○公司雖為中國電子科技產品生產商，惟手機在臺銷售與行銷事宜則由臺灣○○公司負責。因此，北京○○公司所蒐集的資料，若可識別特定中華民國國民使用者，其資料作業相關活動應有個資法之適用。亦即，北京○○公司在未依法履行告知義務或未取得使用者書面同意之情形下，逕行蒐集使用者資料，將侵害手機使用者之個資，我國○○手機使用者得以北京○○公司違法蒐集個資請求民事損害賠償。

進一步而言，依我國電信法第 42 條之規定，手機等電信終

端設備應符合主管機關訂定之技術規範並經審驗合格，始得輸入或販賣。惟此一規定主要是針對手機或相關硬體而言，至於手機內建軟體之資安認證，則不在審驗範圍。因此，為因應手機軟體或應用程式（以下簡稱「App」）之資安風險控管，以強化行動通訊資安防護機制，保障個人資料與財產安全，經濟部工業局依據民國 103 年 6 月 24 日行政院國家資通安全會報第 26 次委員會議決議，積極研議並推動「行動應用 App 資安基本規範」。與一般法令不同，此項規範係採非強制性方式，鼓勵 App 開發商進行自主管理，以提升行動應用程式安全性與產品競爭力，保障消費者權益。

簡單來說，本規範對於行動應用程式基本資安檢測的安全等級分為三級，依序為：初級（無連網之基礎功能）、中級（含初級、連網及身分認證）及高級（含中級、付費資源）三個類別。而資安基本規範面向有以下五個：（一）行動應用程式發布安全：包括發布、更新與安全性問題回報等。（二）敏感性資料保護：包括敏感性資料蒐集、利用、儲存、傳輸、分享及刪除等。（三）付費資源控管安全：包括付費資源之使用與控管。（四）身分認證、授權與連線管理安全：包括使用者身分認證與授權及連線管理機制等。（五）行動應用程式碼安全：包括防範惡意程式碼與避免資訊安全漏洞、行動應用程式完整性、函式庫引用安全與使用者輸入驗證等。而各個資安檢測等級，必須對應各該資安規範面向之具體要求，其情形如下：

檢測基準安全等級架構

規範面向	安全等級	資訊安全技術要求事項	檢測項目	必要項	非必要項
4.1.1.行動應用程式發布安全	第三級新增(含第一、二級共17項)	4.1.1.1.行動應用程式發布	2	2	0
		4.1.1.2.行動應用程式更新	3	1	2
4.1.2.敏感性資料保護	第一級新增(含第一級共11項)	4.1.2.1.行動應用程式安全性問題回報	2	1	1
		4.1.2.1.敏感性資料蒐集	2	2	0
		4.1.2.2.敏感性資料利用	4	0	4
		4.1.2.3.敏感性資料儲存	7	4	3
		4.1.2.5.敏感性資料分享	3	0	3
4.1.3.付費資源控管安全	第一級新增(含第一級共11項)	4.1.2.6.敏感性資料刪除	1	0	1
		4.1.3.1.防範惡意程式碼與避免資訊安全漏洞	2	0	2
4.1.4.身分認證、授權與連線管理安全	第一級新增(含第一級共11項)	4.1.3.2.付費資源控管	1	0	1
		4.1.3.3.函式庫引用安全	2	0	2
		4.1.4.1.使用者身分認證	1	待訂	待訂
		4.1.4.1.使用者身分認證與授權	2	待訂	待訂
		4.1.4.2.連線管理機制	4	待訂	待訂
4.1.5.行動應用程式碼安全	第一級新增(含第一級共11項)	4.1.3.1.付費資源使用	2	待訂	待訂
		4.1.3.2.付費資源控管	2	待訂	待訂
		4.1.5.2.行動應用程式完整性	1	待訂	待訂
		17	41	10	19

資料來源：財團法人資訊工業策進會，行動應用 App 基本資安檢測基準說明簡報，民國 104 年 6 月，中華民國資訊軟體協會網站

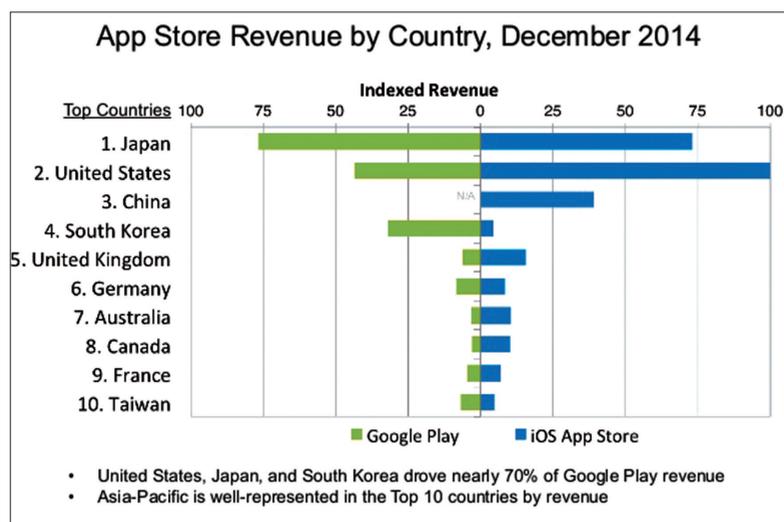
圖 1：資安規範與檢測基準文件架構

關鍵透析

依據國際 App Annie 研究機構統計，亞太地區 App 的發展亮眼；以 2014 年全球行動營收來看，亞太地區國家在前 10 名國家占了 4 名，臺灣排名第 10 名（圖 2），此正突顯出 App 資安的重要性，也呼應「行動應用 App 資安基本規範」為何應運而生。

事實上，手機 App 或相關軟體如涉及個人資料時，自應符合我國個資法之相關規定。然而，手機 App 所涉及之資訊層面

可能更為廣泛，因而必須考慮其他資訊安全層面之議題。目前為止，「行動應用 App 資安基本規範」係採取自願性規範之形式，業者可主動加入，透過自主管理並公布檢測結果之方式，強化消費者的信心。另一方面，此項規範在內容上之設計，是採取分級管理模式，具有相當彈性，業者將可因應軟體產品內容之不同，而選擇最為合適之方式，以落實其安全維護義務。



資料來源：戴彬，App Annie 簡報，民國 104 年 2 月，轉引自數位時代網站
圖 2：2014 年第 4 季 Google Play 和 iOS App Store 的全球營收排行

衛福部將健保資料庫提供學術研究，法院認定符合個資法

精選案例回顧

臺灣人權促進會（以下簡稱「臺權會」）等團體表示，行政院衛生福利部中央健康保險署（以下簡稱「健保署」，原名「行政院衛生署中央健康保險局」），自民國 87 年起建置「全民健康保險研究資料庫」，並將民眾身分證位加密後，提供給學界或研究單位使用。臺權會認為當事人身分欄位雖已加密處理，但仍可能侵犯隱私，故請求相關機關停止提供利用。

案例出處：
資通安全法律案例宣導彙編第 10 輯【案號：S1010102】

後續追蹤

健保署委託國家衛生研究院（以下簡稱「國衛院」）建置「全民健康保險研究資料庫」，並對外提供學術機關運用，因而引

發民眾與臺權會等公民團體的質疑¹。有民眾於民國 101 年間，寄發存證信函予健保署，請求停止此利用行為，但健保署答覆表示「依法辦理並有嚴格之資料管理措施，以保障研究資料被合法合理使用」，並未依民眾之請求予以刪除或停止利用。故民眾進而提起行政訴訟，請求健保署停止將其健保資料，提供予國衛院與衛福部健康資料增值應用協作中心（簡稱「衛福部協作中心」）對外提供增值應用。

臺北高等行政法院就本案適用法規首先闡明，鑒於新版個人資料保護法（以下簡稱「新個資法」）第 6 條關於特種個資蒐集處理之規定，尚未施行，因此就涉及特種個資部分應回歸電腦處理個人資料保護法（以下簡稱「舊個資法」）處理²。因此，就「衛福部將民眾資料提供予國衛院建置資料庫，是否構成特定目的外利用」部分，法院認為尚在衛福部本身法令職掌必要範圍內，且該利用目的，雖與衛福部原先基於全民健康保

¹ 臺灣人權促進會、民間監督健保聯盟、受試者保護協會、臺灣女人連線，[新聞稿] 誰允許國家販賣全民健保資料？，101年2月20日，查詢自<http://www.tahr.org.tw/node/786>。

² 參見臺北高等行政法院103年訴字第36號判決。依法院判決指出：「新個資法就公務機關對個人資料之蒐集、處理及利用，區別第6條第1項之敏感特種資料及其他一般個人資料兩類，分別加以規範；而前揭第15條、第16條係新法對於相對於敏感特種之一般個人資料所為規定，因此本件被告所利用之個人健保資料，原屬敏感特種資料，然既不適用新個資法第6條規定，自不應適用新個資法第15、16條規定，仍應適用未區分敏感特種及一般資料之舊個資法第7、8條之相關規定。至於新個資法其他未區別敏感特種資料及一般資料之其他條文，本件自得適用。」循此意旨，新個資法關於當事人權利行使之規定，並未區分一般或特種個資，本件自得適用。

險醫療費用審查等蒐集目的，未盡相符，但衛福部將資料提供予國衛院與衛福部協作中心建置資料庫，是基於學術研究，且衛福部將身分欄位加密後，才交由國衛院製作成各項增值資料檔案，無從以直接或間接方式識別特定當事人；而國衛院對外提供增值利用前，亦會依每一申請案別或每一申請人別再進行加密，有助於資料外洩時鑑別資料來源，更進一步限制資料的散布。故法院認定此利用方式，符合舊個資法第 8 條第 7 款所定「為學術研究而有必要且無害於當事人之重大利益者」之要件。

另，就「民眾請求衛福部停止利用」部分，法院認為衛福部是基於執行法定職務而蒐集健保資料，並非經當事人書面同意，因此法律若已限制當事人事前同意權，亦應同時限制其事後排除權，否則個資蒐集主體得無庸經個人同意利用其資料，個人卻能任意行使排除權，導致法律所欲達到合理利用個人資料或增進公共利益之目的無以達成，故認定本案民眾請求事後退出，尚屬無據。

本案經民眾上訴至最高行政法院，最高行政法院以原判決適用法律有誤，且事證尚有未明，應由原審法院再為調查審認為由，將原判決廢棄發回³。最高行政法院指出，本案所涉健保資料，屬新個資法第 6 條所稱「有關醫療或健康檢查」之特種個資，而在該條尚未施行前，公務機關應依新個資法第 15 條及

³ 參見最高行政法院103年度判字第600號判決。

第 16 條規定辦理。故原審法院依舊個資法規定，判斷健保署得否將健保資料提供予衛福部協作中心利用，即有適用法律錯誤之情形。

表 1：健保資料庫案大事記

期間 (民國)	大事紀
101 年 5 月至 6 月間	數位民眾以存證信函向衛福部表示，拒絕衛福部將其個人健保資料釋出給第三者，用於健保相關業務以外之目的
101 年 6 月至 7 月間	衛福部分別函覆表示，對外提供利用時，均依行為時電腦處理個人資料保護法之規定辦理，並有嚴格之資料管理措施，以保障研究資料被合法合理使用等語
101 年 10 月	新個資法施行
103 年 5 月	臺北高等行政法院判決民眾敗訴，認定衛福部將其健保資料提供予國衛院及衛福部協作中心，符合舊個資法之規定
103 年 11 月	最高行政法院發回更審，認定「有關醫療或健康檢查」之個人資料蒐集、處理及利用，仍應依新個資法第 15 條、第 16 條規定辦理，故原審法院適用法律有所違誤

資料來源：本文整理

關鍵透析

公務機關將可得識別特定當事人的資料，提供予其他機關建置資料庫時，應有個資法適用。對於公務機關而言，若將資料釋出從事與原初蒐集目的不同之利用用途，即應符合個資法關於公務機關得為特定目的外利用之法定事由。本案涉及衛福

部將全民健保資料檔案提供予國衛院與衛福部協作中心，是否構成違法之特定目的外利用，以及民眾得否請求衛福部停止利用之議題。而本案原審法院首先認為，在新個資法第 6 條尚未施行前，就本案所涉健保資料等類特種個資，應適用舊個資法，故以衛福部提供利用行為，是否符合「未影響當事人重大利益」，以及「資料處理後是否已無從識別特定當事人」的要件⁴，加以判斷。本案原審法院認為，衛福部將健保資料提供國衛院等機關建置資料庫，雖有構成特定目的外利用情事，但尚符合舊個資法之規定。然而，本案經最高行政法院審理後，認定應依新個資法第 16 條規定，判斷衛福部利用行為是否符合法律規定，故發回高等行政法院審理。

是以，更審法院將須依新個資法第 16 條，判斷健保署提供健保資料予國衛院之利用行為，是否已達到「依其揭露方式無從識別特定之當事人」之要件，故衛福部宜再補強關於去識別化操作的說明，以主張確實符合個資法特定目的外利用事由之規定。再者，更審法院是否支持原審法院認定「當事人事後退出權利行使應受限制」之立場，亦值得留意，考量到我國類似大型資料庫均可能面臨受理當事人請求停止利用或刪除，以致影響資料完整性並增加作業負擔的風險，本案判決對於我國推動開放資料加值應用之法律界線與作業規範，影響重大，故後續法院判決見解仍待繼續觀察。

⁴ 應注意的是，依舊個資法第 8 條規定，公務機關對於學術研究之目的外利用行為，舊法並無應將個資去識別化的明文規定。

政府採購涉及個資作業之業務， 應於契約中約定監督事項

精選案例回顧

YouBike 廣受歡迎，○市現已建置 163 個租借站，註冊會員卡數高達 4,076,732 件。日前○市議員曾質詢指出，民眾租借 YouBike 必須提供姓名、手機號碼、電子信箱及悠遊卡號等資料，註冊成為會員，但會員服務條款允許經營公共自行車業務的 A 公司，將個資用於「其他經營公共事業業務」與「其他經營合於營業登記項目或組織章程所訂之業務」。議員甲質疑 A 公司營業項目五花八門，個資恐遭不當使用。

議員甲另指出，○市政府交通局（以下簡稱○市交通局）與 A 公司簽訂契約明定「不得將○市公共自行車資料洩漏予第三人」，但 A 公司卻將會員資訊，包含登錄、傳輸及保全全都分包給 B 公司，該公司網站還稱「看不到的後台會員、金流系統，B 公司都默默地 24 小時監看」，更有個資外洩之虞。

○市交通局科長乙稱，A 公司承攬公共自行車業務時，有籌

組團隊，包含 B 公司與 C 公司等。乙強調會員資料僅在租借系統與發送會員通知信使用，針對議員甲之質疑，該局將會檢討修正服務條款，限縮個資使用範圍。

案例出處：
資通安全法律案例宣導彙編第 11 輯【案號：S1030107】

後續追蹤

本案 YouBike 公共自行車系統，係由○市交通局委託 A 公司所組團隊營運，包含 A 公司經營該 YouBike 租借所蒐集、處理或利用個人資料之業務。此時，A 公司係受公務機關委託蒐集、處理或利用個人資料，並將會員資料之登錄、傳輸及保存等事宜分包予 B 公司，依個人資料保護法（以下簡稱「個資法」）第 4 條與個人資料保護法施行細則（以下簡稱「個資法施行細則」）第 7 條規定，A 公司與 B 公司（以下合稱「承包商」）將視同委託機關，並應遵守委託機關適用之相關法規。而○市交通局將 YouBike 租借等相關蒐集、處理及利用個人資料之業務，委託承包商辦理，依法須對其進行適當之監督，包含個資蒐集、處理或利用之範圍、類型、特定目的及其期間，以及所採取的適當安全維護措施等事項，以確保委託處理個人資料安全管理。

依據個資法施行則第 8 條規定，委託他人蒐集、處理或利用個人資料時，委託機關應對受託廠商為適當之監督；受託者

亦僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。對於委託機關應監督之事項也有明確規定，其至少應包括以下內容：

- 受託廠商所蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
- 受託廠商所採取的適當安全措施。
- 是否有複委託之情形。如有，其約定之受委託者為何。
- 受託廠商或其所屬人員，如違反個資法相關規定之通報或補救措施。
- 委託機關對受託廠商是否有保留指示。
- 委託關係終止或解除時，相關載體返還以及資料之刪除。

事實上，除了上述必要監督事項外，機關將涉及個資之業務委外時，亦可斟酌個案特性需求，適度增加監督事項並將之納入招標文件與採購契約條款中，以利受託廠商注意與遵循。

關鍵透析

因應政府財政資源與施政內容之發展，政府業務委外之情形益趨常見，其中更是不乏涉及資訊業務，甚至是個人資料的委外處理。事實上，機關將各項業務委外時，不應僅將焦點置重於行政負擔之減輕，亦應同時對受託廠商之管理與監督予以強化。

以個資業務委外之情形為例，依據個資法施行細則之規定，不僅要求委託機關必須對委外業務負起監督責任，並且對於委辦機關應監督之具體事項予以規範。然而，委託機關自可因應委外業務個案之特性需求不同，自行斟酌增加，並明訂於招標文件與採購契約當中。而在後續執行與監督上，受託廠商僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料；此外，並應定期確認執行情形，且加以記錄。倘未確實遵守此點，則就受託廠商違反個資法之行為，將可能被視為委託機關之行為，而應依個資法負賠償責任。

政院積極推動政府開放加值資料，強化資料釋出並提升品質

精選案例回顧

行政院推動政府資料釋出供民間應用，行政院國家發展委員會（以下簡稱「國發會」，原「行政院研究發展考核委員會」）表示初步開放資料類型將以民生資訊優先，包括食、醫、住、行、育樂、就業、文化、經濟發展及生活品質等九大類的資料。另國發會亦將參考國際開放資料的格式，制定臺灣的開放資料格式、資料發布及查詢標準，並以五星級的標示方式註明各種開放資料的可用程度。

而國發會為建立開放資料集中化管理並提供單一入口服務，建置「政府開放資料平臺」，供民眾使用單一平台查詢所有部會釋出的資料集。但某民眾反映，在該平臺上檢索資料，下載一筆電信設備審驗合格清單，開啟檔案後卻發現內容為民國 99 年至 102 年間不知名學校學生人數統計資料，顯有品質管理問題。國發會接獲民眾反映後，已通知資料所屬主管機關進行更

正，並表示民眾如發現資料集內容有錯誤或其他建議，可直接於該項資料集下方表達意見。

案例出處：

資通安全法律案例宣導彙編第 10 輯【案號：D1010103】

資通安全法律案例宣導彙編第 11 輯【案號：D1030102】

後續追蹤

我國行政院於民國 101 年 1 月 3 日發布「行政院及所屬各機關行動化服務發展作業原則」，鼓勵政府機關因應智慧型行動裝置普及趨勢，發展各項主動化服務，並考量開放資料提供民間發展創新應用之可能性。

現行政府資訊公開法雖規範政府主動公開資料範圍，以及受理民眾申請被動公開之作業程序，但就政府資料公開方式、資料格式與使用規範等，仍有不足。因此，行政院為進一步提升便民服務與促進產業創新，而於民國 102 年 2 月 23 日發布「行政院及所屬各級機關政府資料開放作業原則」（以下簡稱「本原則」），作為行政院及其所屬機關推動開放政府資料的基本作業架構。本原則明訂政府資料以公開與無償提供為原則；而針對品質維護議題，本原則亦要求政府機關設立網站提供政府資料開放服務時，應建立意見回饋機制、資料正確性回報及問題諮詢管道，以持續維護與改善。最後，為便於民眾可從單一入口檢索所有資料集並下載利用，本原則規範各機關資料集，

均須集中列示於政府資料開放平臺 (data.gov.tw) 。



資料來源：國發會政府開放資料平臺 (截至民國 104 年 8 月已有 1 萬餘筆資料集)

圖 1：國發會政府開放資料平臺首頁

因應巨量資料風潮，為確保政府資料在可供機器識別讀取的前提下，促進後續運算利用，本原則規定政府資料應以「開放格式」釋出，但釋出方式與開放格式類型不甚明確。故行政院嗣於民國 102 年 3 月 1 日發布「政府資料開放資料集管理要項」，提供各機關盤點內部資料與釋出格式的依據，以促進政府開放資料後得相互連結與彙整分析，進而打造有助於資料加值應用的環境。

關鍵透析

配合雲端運算與行動服務時代來臨，我國行政院推動第 4 階段電子化政府發展的重要主軸，即是整合運用政府開放資料，推動政府資料開放加值應用，以發展各項跨機關便民服務，因此近年來在行政院積極推動下，陸續發布「行政院及所屬各級機關政府資料開放作業原則」與「政府資料開放資料集管理要項」等法規，以強化政府資訊公開法未能詳盡規範的部分。



資料來源：國發會政府開放資料平臺

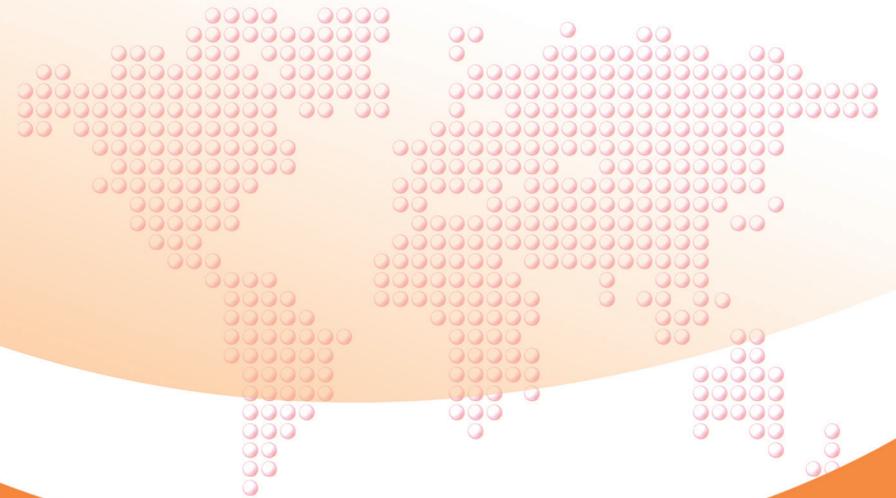
圖 2：為國發會政府開放資料平臺互動專區，提供民眾反應意見

在行政院明確建立開放政府資料作業方向後，政府開放資料不再僅是有限、被動或單向釋出，政府資料原則上應公開，

並主動釋出具有便利民眾生活、提升生活品質及擴大運用價值等優勢的資料集，且政府機關亦須透過意見回饋機制，提供民眾反應使用建議或需求等，以營造雙向互動的使用環境，並藉由群眾力量共同持續提升政府開放資料品質。惟政府在開放資料時，仍應注意資料本身是否具有依法不得公開或應限制公開之情況，以符合其他法律之要求。

Chapter II

全民資安素養



民眾使用自動化訂票程式，致干擾網站服務，恐負有刑責

精選案例回顧

每到農曆春節或中秋節期間，返鄉人潮眾多，車票往往一票難求，臺灣鐵路管理局（以下簡稱「臺鐵」）訂票系統屢次遭到電腦駭客入侵，導致系統當機。在民國 94 年間，調查局與警方曾一共查獲 11 名入侵系統的駭客，而該案經臺北地方法院檢察署偵辦後，檢察官考量這些駭客並無任何前科，且犯後深具悔意，因而全部給予緩起訴處分。

隨後，類似案例仍相繼出現，且犯罪手法不斷翻新。在民國 96 年曾有江姓電腦工程師為圖方便，涉嫌使用惡意程式冒用親人與陌生人身分證字號訂票後再取消，在 6 年間冒名訂票 31 萬餘張。而與上開判決結果不同，江姓電腦工程師在民國 104 年經高等法院更一審依偽造文書罪判處 4 年 6 個月有期徒刑。

案例出處：
資通安全法律案例宣導彙編第 6 輯【案號：S970401】

後續追蹤

有關民國 94 年「駭客訂票案」，11 名電腦駭客利用自行撰寫或網路下載的電腦程式，連結到臺鐵訂票系統自動且連續訂票，造成臺鐵訂票系統伺服器及主機代管之中華電信網路伺服器的損害。因此，當時檢方以刑法第 360 條干擾他人電腦及相關設備罪偵辦，惟考量這些駭客均無前科，且犯後深具悔意，惡性並非重大，除命其中兩名被告，須支付新臺幣 8 萬元與 3 萬元的緩起訴處分金外，其餘僅需於 1 年內在春節連續假期期間，分至各地臺鐵車站協助疏導人潮，以服勞務。不過，當時期類似案例也有不同結果，在花蓮地方法院 95 年度花簡字第 686 號刑事判決中，行為人則被依違反刑法偽造文書罪、干擾他人電腦及相關設備罪起訴，惟經考量係為服務軍官而非圖私利，且犯後態度良好，判處有期徒刑 5 月，緩刑 3 年。

對比之下，在民國 96 年「濫用訂票」案中，一審法院認為，江姓工程師明知臺鐵網路訂票系統，應以自己或他人授權同意之國民身分證統一編號訂票，用以驗證身分並限制訂票張數，竟基於行使偽造準私文書之犯意，冒用他人身分證號，並登錄乘車車次、起站、到站代碼及訂票張數等訂票資料，導致臺鐵網路訂票系統對於真正訂票者之身分有所誤認，足以生損害於臺鐵對於網路訂票管理之正確性，及被冒用者與一般旅客之訂購車票權益，因而依刑法第 216 條行使偽造私文書罪判處 8 個

月有期徒刑；此情形至二審判決仍維持同一立場。其後，案件上訴最高法院後發回高等法院，高等法院認為江姓工程師犯行明確，且犯罪時間長達 9 年，甚至發回更審時仍在犯罪中，所訂得之車票有紀錄可查者，遠超過 30 萬張，使用高達 31 人的身分證字號訂票，剝奪花東旅客與居民其旅遊與返鄉之權利，因而改判處 4 年 6 個月之重刑。

關鍵透析

網路搶票之情形時有所聞，惟因應科技之日新月異，犯罪手法也不斷翻新。利用身分證自動產生器，冒用他人名義訂票並領票使用，主要涉及刑法第 216 條行使偽造私文書罪；若以機器人程式大量訂票，以致影響系統運作或造成其負擔時，則可能成立刑法第 360 條干擾他人電腦與相關設備罪。

從司法實務來看，利用身分證自動產生器或機器人程式訂票之行為，將可能同時成立刑法第 216 條及第 360 條之罪，並無見解上之紛歧。而民國 94 年「駭客訂票案」及民國 96 年「濫用訂票案」在處罰效果上之懸殊，其實並非國內判決趨勢之變更，重點仍在於使用訂票軟體大量訂票，除影響其他民眾訂票權益，如造成訂票系統擁塞或當機，將損及被冒用人與公眾公平訂票旅行與返鄉之機會。因應此一發展，組織應加強電腦系

統（例如，訂票系統）之安全管控，如遇有使用惡意程式干擾或癱瘓電腦系統之情形，亦可透過刑事程序尋求協助。

雇主不得要求應徵者或員工提供與工作無關之隱私資料

精選案例回顧

部分企業於招募人員或是管理企業內部時，會要求留置求職者或員工的國民身分證、工作憑證或其他證明文件，或要求其提供與工作無關的資料，例如「性傾向」、「驗孕報告」或「身心障礙」等隱私資料，引發外界質疑若干企業如此要求提供資料，有侵犯隱私權之疑慮。

為明確保護求職者和員工之權益，民國 101 年 11 月 2 日即修正公布就業服務法第 5 條規定。該條於修正後，已明文規定雇主招募或僱用員工時，不得有違反求職人或員工意思，留置國民身分證、工作憑證或其他證明文件，或要求提供非屬就業所需的隱私資料，違者將處以新臺幣 6 萬元以上 30 萬元以下罰鍰。

案例出處：
資通安全法律案例宣導彙編第 10 輯【案號：S1010108】

後續追蹤

勞工被雇主要求提供個人資料時，部分資料涉及隱私，常讓勞工十分為難。其實雇主如此要求，是極有可能違反就業服務法相關規定的。近期即有「電話客服案」與「百貨公司案」可供參考與注意。

「電話客服案」為全國第一例對雇主要求求職人提供非就業所需資料開罰的案例。新北市一名女子向新北市勞工局檢舉，表示曾應徵某家派遣公司的電話客服人員，但在錄取後竟被告知需檢驗梅毒，讓她相當不滿。該派遣公司表示，由於擔心人員輪班休息時在休息室蓋棉被可能傳染疾病，故在體檢表單上要求應徵者檢驗梅毒。勞工局調查後，認為梅毒與電話客服工作內容毫無關係，且梅毒並非勞工安全衛生法規定之必要檢驗項目，派遣公司也無法提出曾有員工在休息室感染梅毒的事證，於是認定該派遣公司的要求，違反就業服務法第 5 條第 2 項第 2 款「不得要求提供非屬就業所需隱私資料」之規定，依照同法第 67 條規定得裁罰新臺幣 6 萬至 30 萬元。然考慮當時此規定剛修法通過，雇主對隱私保護不甚理解，最終對該派遣公司處以新臺幣 3 萬元罰鍰。

「百貨公司案」則是臺北市某百貨公司招募客服人員與電話行銷人員時，在錄取報到通知書上，要求求職者提供「警察刑事紀錄證明書」與「個人信用報告」等資料，並表示如未補

齊資料，將視同未完成報到手續，薪資也將保留至繳齊資料為止。臺北市政府勞動局接獲檢舉後，至該百貨公司進行了解，該百貨公司表示要求提供刑事紀錄與個人信用資料，係為保護消費者交易安全。但臺北市政府勞動局認為，雇主招募員工如法令已有任用條件限制，則從其規定。如雇主招募之職缺無相關法令規範，則應尊重求職者，不應要求求職者提供上述隱私資料，因此判定百貨公司此舉違反就業服務法第 5 條第 2 項第 2 款規定，處以新臺幣 6 萬元罰鍰。

至於公司是否可主張，已請員工簽署蒐集、處理、利用及保有個人資料的書面同意書，而得排除適用就業服務法相關規定，法務部曾作出函釋表示¹，雇主要求求職人或員工提供隱私資料，應尊重當事人之權益，不得逾越基於經濟上需求或維護公共利益等特定目的之必要範圍，並應與目的間具有正當合理之關聯，若有違反，則依就業服務法第 67 條第 1 項規定處以罰鍰。故公司之「蒐集、處理及利用員工個人資料告知暨同意書」，就算已載明公司得蒐集、處理、利用及保有員工個人資料類別，仍應先視有無違反上述就業服務法相關規定，不得僅依據該書面同意書而予以免責。

關鍵透析

雇主在招募員工時，向員工要求提供隱私資料，必須符合法令規定，或符合求職目的與工作內容所需。例如，雇主依勞動基準法規定備置勞工名卡，即負有保存員工特定個人資料之法定義務；又如保全從業人員受限於保全業法規定，雇主即有向求職者索取「警察刑事紀錄證明書」之必要，以確認求職者有無保全業法中「不得擔任保全人員」之事由，進一步保障民眾生命與財產安全。若職位的業別，無相關法令規範，雇主要求提供資料之範圍又與工作內容無關，例如要求求職者或員工提供與工作無關的生理個資、要求測謊或提供信用紀錄等，超過該工作內容之必要範圍，恐遭主管機關依就業服務法第 67 條處以新臺幣 6 萬元至 30 萬元之罰鍰，雇主應特別留意。

¹ 法務部民國102年12月5日法律決字第10200683890號函、102年12月5日法律決字第10200683900號函。

員工在工作場所通訊內容仍受隱私權保護，公司監看應事先告知

精選案例回顧

隱私權保障之議題，日益受到重視，並且從一般日常生活當中，延伸到員工的工作場所。員工隱私權之爭議，最常發生在電子郵件與辦公電話之監看或監聽。過去曾有實際的案例，即○公司發現 A 副理擅自寄發電子郵件予客戶，因而予以懲處。A 副理認為公司逕自從公司伺服器備份內擷取電子郵件之行為，已侵害其隱私權，因而依民法第 184 條第 1 項前段規定，請求賠償新臺幣 100 萬元。

實務也曾發生過，X 公司董座懷疑 B 秘書經常在半夜帶人進入辦公室、話費過高等「行徑可疑」，乃以「安全維護」為由，派人在 B 秘書辦公室電話裝竊聽設備，連續監控其通話長達 3 個多月。B 秘書發現後，隨即以 X 公司侵害其隱私權為由追究其刑事責任，並依民法第 184 條第 1 項與第 195 條第 1 項前段

規定提起附帶民事訴訟，請求高達新臺幣 10 億元之天價賠償。

案例出處：

資通安全法律案例宣導彙編第 8 輯【案號：M990102】

資通安全法律案例宣導彙編第 10 輯【案號：M1010101】

後續追蹤

在「郵件監看案」中，主要關鍵在於公司是否有監看員工電子郵件的權利。對此，一審法院¹認為關鍵在於員工是否有合理隱私期待。簡單來說，如果公司對於員工電子郵件監看政策有明確宣示，或是員工曾簽署同意監看的文件，則對於隱私不具有合理期待。在本案中，由於○公司曾事先告知全體員工，公司會至伺服器內查看員工備份的檔案資料，且 A 副理對公司查看政策並無反對意思，因而一審法院判其敗訴。二審法院²維持同一見解。

在「電話監聽案」中，也面臨到類似的處境。對此，一審法院³認為，隱私權是指個人不受外界干擾的權利，職場固然是公開場所，然而員工仍然保有以私密方式履行其職務的權利，並非於職場之行為全無隱私。因此，公司除非事先告知員工，

¹ 臺灣臺北地方法院99年度勞訴字第227號民事判決。

² 臺灣高等法院100年度勞上易字第121號民事判決。

³ 臺灣新北地方法院98年度重訴字第24號民事判決。

或有合理懷疑之理由認為進行監聽、監視、錄音或錄影可蒐集員工與工作相關之犯罪證據，或為工作相關之目的有實施監聽、監視、錄音或錄影，且使用手段方法與目的間具有合理關聯時，方可未得員工之同意而監聽、監視、錄音或錄影外，否則不可以任意進行監聽。在本案中，法院認為 B 秘書在公司之活動或行為仍然有隱私權；X 公司如欲制止 B 秘書以公用電話撥打私人號碼之行為，大可直接禁止或勸導，且「長達 3 月之監聽行為」並不足以達成禁止的目的。因此，法院認為公司之行為已侵害秘書隱私權，因而判命賠償新臺幣 35 萬元。二審法院⁴維持同一見解。

表 1：我國司法實務趨勢：員工職場通訊內容及隱私保護

態樣	電子郵件監看	公務電話監聽
代表性判決	侵害員工隱私權，應予以賠償（99 年度勞訴字第 227 號）	侵害員工隱私權，應予以賠償（98 年度重訴字第 24 號）
員工隱私權	肯定	肯定
可監看之情形	<ul style="list-style-type: none"> • 事先告知監看政策 • 取得員工同意 	<ul style="list-style-type: none"> • 事先告知員工 • 有合理懷疑之理由而進行犯行蒐證 • 與工作相關且手段與目的符合比例原則
目的與手段之合理關聯	未提及	有要求

資料來源：本文整理

關鍵透析

處理公司監控議題的最大困難，在於公司內部管理與員工隱私權如何取得平衡。以目前國內實務見解而言，主要取決於兩項關鍵，其一是「員工有無合理之隱私期待」，其二則是「公司管理手段是否符合目的性與比例性」。

對此，目前實務見解普遍揚棄員工於職場內一律不具隱私之看法；換言之，員工於職場上之活動仍具有某程度合理隱私期待。而為確保員工之合理隱私期待，公司倘欲進行監看或監聽，依我國實務見解，在以下情形較能避免侵權疑慮：（一）告知後取得員工同意。（二）揭示公司資訊監看政策且員工未有反對。（三）有合理懷疑而進行犯行蒐證等。（四）與工作相關且符合目的性與比例性。而「公司管理手段是否符合目的性與比例性」，是指公司如欲採取監看或監聽之行為，必須與其管理目的有合理的關聯，且不得對於員工權益造成過度侵害。公司在未遵循前述原則之情況下對員工進行監看或監聽，依國內現行實務見解，將構成對員工隱私權之侵害，可能因此負有民、刑事責任。

⁴ 臺灣高等法院98年度上易字第959號民事判決。

法院以臺灣○○公司並無搜尋引擎業務，駁回球團老闆主張被遺忘權

精選案例回顧

歐盟法院 (Court of Justice of the European Union) 在 2014 年 5 月間作出具指標意義的判決，認為在個人資料顯然已過時且不相關時，一般民眾有權利要求美國網際網路搜尋巨擘 Google，刪除由該公司的搜尋引擎檢索出的連結，亦即行使「被遺忘權」(right to be forgotten)。該案起因於一西班牙公民指控，只要在 Google 以他的姓名進行搜尋，就會連結到先前房地產遭拍賣的新聞，雖然債務糾紛早已透過司法程序解決，但相關紀錄仍能透過網路搜尋查得，讓他深受其擾。

歐盟法院在本案判決指出，搜尋引擎以自動化、系統性方式蒐集網路資料，加以記錄、儲存並以清單方式提供使用者閱覽，符合歐盟個資保護指令定義之個人資料蒐集與處理活動，自應遵循歐盟個資保護指令相關要求。故判決認定當使用者網路檢索結果連結到的網頁資料，已為過時、無關或逾越原初處

理目的範圍的資訊時，搜尋引擎業者原則上應配合使用者提出的請求，於搜尋結果中移除該類網頁的連結。

案例出處：
資通安全法律案例宣導彙編第 11 輯【案號：S1030102】

後續追蹤

Google 為遵循歐盟法院判決，隨後於 2014 年 5 月底宣布受理歐盟地區民眾提出「被遺忘權」，民眾只要在受理頁面上填具姓名、電子郵件及證件，並列出他們希望從搜尋結果移除的網址，與說明對於該結果為何「無關、過時或不恰當」後，Google 將會進行審核¹。Google 表示會考量申請移除的資訊，是否牽扯到公共利益，例如金融詐欺、刑事定罪或政府官員公眾行為等，再決定是否移除。而此服務上線第一天，申請人數就達到 1 萬 2,000 人，超乎預期²。

我國近年法院亦曾作出涉及被遺忘權議題的判決，受到相當矚目。本案為職棒某球團老闆○先生，於民國 97 年間遭報紙指稱買職棒球隊打假球，甚至因此事件遭檢察官以詐欺等罪起訴，雖然○先生後來獲判無罪，但以其名字為關鍵字在 Google

¹ Google, Search removal request under data protection law in Europe, available at https://support.google.com/legal/contact/lr_eudpa?product=websearch。

² 參考自由時報，「谷歌受理網路『被遺忘權』首日湧入萬筆」，民國103年5月31日，查詢自<http://m.ltn.com.tw/news/life/breakingnews/1021217>。

搜尋，仍能發現相關網頁新聞轉貼內容，因此○先生於民國 103 年間，以 Google 搜尋服務已侵害其名譽權與隱私權，並違反消費者保護法等，訴請美商○○國際有限公司臺灣分公司（以下簡稱臺灣○○公司）移除網頁搜尋結果與「搜尋建議關鍵字」。

Personal information

Name used to search *
This should be the name that, when used as a search query, produces a list of results from which you are requesting that a result, or results, be removed

Full name of requester
Your own name, if you are representing somebody else (if you're sending a request for someone else, you must have the legal authority to act on their behalf)

If you are submitting this request on behalf of someone else, please specify your relationship to that person (for example: "parent" or "attorney")

Contact email address *
(where emails about your request will be sent)

Search results you want removed from the list of results produced when searching for the name

資料來源：Google³

圖 1：Google 提供歐盟地區民眾行使被遺忘權的頁面

本案一審法院認為 Google 搜尋引擎網站係由 Google Inc. 公司所經營，該公司所在地在美國加州且未經我國主管機關認許，並無在我國經營業務，而○先生起訴對象即臺灣○○公司，與 Google Inc. 分屬不同法人主體；再者，臺灣○○公司營業項目雖包含電子資訊供應與一般廣告等業務，但難以此推論認為

Google Inc. 有授權臺灣○○公司管理搜尋引擎服務，因此法院認定○先生請求臺灣○○公司移除建議搜尋字串及以相關檢索結果，並無理由，而判決敗訴⁴。

關鍵透析

我國個人資料保護法（以下簡稱「個資法」）第 3 條明定個資當事人享有請求個資蒐集主體停止蒐集、處理、利用及請求刪除之權利，以維護當事人資訊自主權利。因此，除非個資當事人請求停止蒐集、處理利用或刪除的資料，尚在法定保存期間內、有理由足認刪除將侵害當事人值得保護之利益，或有其他不能刪除之正當事由⁵，否則個資蒐集主體在受理當事人請求後，即應依個資當事人請求予以處理。

本案為臺灣涉及請求搜尋引擎服務業者移除檢索結果的案例，但本案法院認為臺灣○○公司並非 Google 搜尋引擎之管理者或經銷者，且消費者保護法所保護之法益不包含名譽權

⁴ 參照臺灣臺北地方法院103年度訴字第2976號民事判決。

⁵ 個資法第11條第3項：「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。」同法施行細則第21條：「有下列各款情形之一者，屬於本法第11條第3但書所定因執行職務或業務所必須：一、有法令規定或契約約定之保存期限。二、有理由足認刪除將侵害當事人值得保護之利益。三、其他不能刪除之正當事由。」

及隱私權，故○先生依民法侵權行為與消費者保護法請求臺灣○○公司移除 Google 搜尋引擎顯示的搜尋結果，尚無理由而予以駁回。因此，本案並未處理到搜尋引擎業者儲存頁面資料並呈現「可得識別特定個人」的搜尋結果，是否構成個資法上所稱蒐集或處理行為⁶，亦未進一步依個資法認定搜尋引擎業者是否負有受理當事人權利行使的義務。但據悉本案已提起上訴，因此臺灣法院是否會承認被遺忘權，仍可持續觀察二審法院態度。

⁶ 個資法第2條：「本法用詞，定義如下：三、蒐集：指以任何方式取得個人資料。四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。」另，法務部就「民眾陳請移除透過網際網路搜尋引擎功能所揭示之資料，是否符合個人資料保護法第19條第1項第7款但書及第2項規定」乙案，認為事涉網際網路搜尋引擎適用本法相關疑義，建請先行徵詢網際網路搜尋引擎目的事業主管機關經濟部之意見，參法務部民國104年3月11日法律字第 10403502390號函釋。」

為維護法庭秩序，民眾未經許可不得逕為錄音錄影

精選案例回顧

A 女曾多次至地檢署按鈴申告，但她認為地檢署吃案，故後來戴著有錄音錄影功能的眼鏡出庭，竊錄偵查庭活動，並上傳至網站供人點閱。某日開庭，A 被檢察官當場抓包並命法警取走眼鏡，但 A 竟然抓咬、踹踢法警。當時 A 稱其竊錄開庭的目的是維護自身權益，而且她是當事人，應有權公布開庭過程。又檢察官是在執勤公務，她沒有侵犯他們的隱私。激烈抵抗是因為開庭時與檢察官有言語爭執，沒有妨害公務的意圖。

但檢察官認為，基於偵查不公開，偵查庭的過程是「非公開之活動」，A 未經檢察官與檢察事務官同意錄影與錄音，即是無故竊錄他人非公開活動，且侵犯其隱私權。而且法警奉命取下 A 眼鏡，卻遭抓咬踹踢，A 已構成妨害公務等情事。一審法院判決合併處 10 個月徒刑，得易科罰金。

案例出處：
資通安全法律案例宣導彙編第 11 輯【案號：S1030403】

後續追蹤

本案後來經 A 提起上訴，高等法院就妨害秘密部分撤銷了原判決¹。理由在於，雖然地方法院以 A 用眼鏡錄下的法庭活動、檢察官與檢察事務官的面容，確屬個人資訊自主權的範疇，而 A 聲稱竊錄是怕地檢署吃案，惟 A 可透過其他訴訟程序來主張權利，因此不符合比例原則。但高等法院認為，偵查不公開的立法目的，是基於無罪推定原則，為維護偵查程序之順利進行與真實發現，兼顧保障被告、犯罪嫌疑人、被害人或其他利害關係人之名譽、隱私及安全。因此，偵查不公開約束的是檢察官、檢察事務官、司法警察官及辯護人，而不包括告訴人。法院並認為，檢察官執行公務並非隱私權的範圍，不是刑法第 315 條之 1、第 315 條之 2 立法目的所要保障的活動。又被告只有就她本人出席的偵查庭錄影，並不是「他人」的非公開活動，因此上訴法院撤銷原判決妨害秘密的部分，改判無罪。

此外，對於訴訟程序的法庭活動，民眾可否擅自錄音錄影？答案是不可以的。民國 104 年 7 月法院組織法經修正第 90 條規定，並增訂第 90 條之 1 至第 90 條之 4 規定。依法院組織法第 90 條第 3 項，在庭之人非經審判長許可，不得自行錄音、錄影；未經許可錄音、錄影者，審判長得命其消除該錄音、錄影

的內容，並且對此處分不得聲明不服。依「法庭錄音錄影及其利用保存辦法」第 3 條第 2 項規定，審判長為前項許可時，應審酌錄音、錄影目的及對法庭程序進行之影響，並得徵詢其他在庭之人意見；但有依法不公開法庭審理或其他不適宜情形者，則不應許可。此外，法院組織法第 90 條之 4 則規定，持有法庭錄音、錄影內容之人，不得散布、公開播送或為非正當目的使用該錄音、錄影之內容，否則得處 3 萬元以上 30 萬元以下罰鍰。也就是說，現行法明文規定，原則上民眾不得擅自對法庭內活動錄音錄影。

關鍵透析

依偵查不公開作業辦法第 8 條第 1 項第 6 款及第 11 款規定，蒐證之錄影、錄音，或偵查中之錄音帶或錄影帶等重要文件或物品，除法令另有規定者外，於案件偵查中均不得公開或揭露。而「臺灣高等法院檢察署暨所屬各級法院檢察署偵查庭管理要點」第 8 點第 2 項，亦要求法警於偵查庭執行職務時，應注意並檢視當事人有無攜帶錄音、錄影等通訊器材或具有錄音、錄影功能裝置之手機，並委婉請其關機，必要時得保管至偵訊完畢。本案原審以「偵查不公開」作為檢察官與檢察事務官隱私權的具體依據之一，但上訴審法院認為偵查不公開的目的，並不是在保護檢察官等司法人員執行職務行為的個人隱私，而是

¹ 臺灣高等法院臺中分院103年上易字第1316號刑事判決。

在約束司法人員執行公務的行為，故本件被告攝錄及上傳開庭內容，尚不構成刑法第 315 條之 1 第 2 款、第 315 條之 2 第 3 項之妨害秘密罪。

此外，針對訴訟程序中之法庭活動，法院組織法修正後，依照該法第 90 條第 3 項規定，民眾對於法庭活動非經許可，不得自行錄音、錄影，且審判長得命其消除該錄音、錄影的內容。司法院指出：「本次修正緣由係鑑於法庭錄音或錄影為訴訟資料之一部分…涉及人格權之保障，允宜以法律規範之，爰修正法院組織法有關法庭錄音、錄影之規定，滿足人民之司法近用權及法庭之公開透明，以增進司法品質與效能，提升司法公信力，兼顧訴訟當事人及在庭活動之人之權益。」而審判長就聲請自行錄音、錄影之許可與否，或審判長命消除未經許可之錄音、錄影內容等處分，均是屬於維持法庭秩序之行為。

雖有學者認為，此規定並不能達到「陽光法院」公開透明的目標，但現行法明文規定民眾未經許可，不得自行錄音錄影，民眾仍應遵守法庭秩序。若想取得法庭錄音、錄影內容，除經審判長許可外，應依法院組織法第 90 條之 1 等相關規定向法院請求交付，並且應注意不得對外散布或為不當目的之使用，否則將面臨處罰。

附錄

附錄一

自我評量



第一部分：是非題

1. (○) 為保護手機使用安全，手機等電信終端設備依電信法第 42 條規定，應符合相關技術規範並經審驗合格。而針對軟體部分，App 開發商可參考「行動應用 App 軟體資安基本規範」，以自行遵循。

解析：針對手機使用安全，我國係採取軟硬體分離管理之模式，硬體方面主要適用電信法第 42 條規定，軟體方面，經濟部工業局訂有「行動應用 App 軟體基本資安規範」，供業者自主遵循。

2. (○) 將個資業務委外時，委託機關仍應對受託廠商進行監督。

解析：依據個資法施行則第 8 條規定，委託他人蒐集、處理或利用個人資料時，委託機關應對受託廠商為適當之監督。

3. (○) 未經他人同意，假借他人身分證號或利用身分證號自動產生器，以他人名義購買車票並領票使用，有可能涉及刑法行使偽造私文書罪。

解析：司法實務認為，在網際網路上輸入身分證字號而製作網路訂購資料，使前揭資料顯示於電腦處理影像之

螢幕上，用以表示其為真正身分證字號持用人以其所有之身分證字號購買之意，性質上屬電磁紀錄，而屬於刑法之準文書。因而倘透過未經他人同意而冒用身分證字號進行購票並領票使用，可能涉及刑法第 216 條行使偽造私文書罪。

4. (X) 職場並非住家，因此依我國司法實務，員工在工作場所的通訊，完全不受到隱私權保護。

解析：依我國實務見解，若員工對於本身在職場上通訊隱私，具有某程度合理隱私期待，而公司未告知資訊政策或取得員工同意即監看員工通訊時，恐侵害員工隱私。

5. (X) 雇主為確保員工能勝任職務並配合所有職務規劃，得於招募員工時強制所有員工必須說明目前結婚或懷孕計畫，並提供良民證以證明身家清白。

解析：為保護求職者和員工之權益，就業服務法第 5 條第 2 項第 2 款明文規定，雇主招募或雇用員工時不得要求提供非屬就業所需之隱私資料，包含信用紀錄、犯罪紀錄、懷孕計畫或背景調查等個人生活資訊，若違反將可依同法第 67 條第 1 項處新臺幣 6 萬元以上 30 萬元以下罰鍰。

6. (X) 精神衛生法與性騷擾防治法僅限制媒體不得揭露當事人姓名，所以行政機關的訴願決定書中若涉及罹患精神疾病或性騷擾案件的當事人，均無庸遮蔽當事人姓名資料。

解析：訴願決定書是政府資訊的一種，依政府資訊公開

法第 7 條第 1 項第 7 款，原則上應主動公開。雖然「精神衛生法」與「性騷擾防治法」為針對媒體報導時的限制，但依個資法第 5 條與政府資訊公開法第 18 條第 7 款，當涉及個人隱私時，機關仍應採取適當遮蔽措施或限制公開。

7. (X) 刑事訴訟法第 245 條偵查不公開，是為了保護檢察官、檢察事務官在偵查程序執行職務的隱私權。

解析：刑事訴訟法關於偵查不公開的目的，是基於無罪推定原則，為維護偵查程序順利進行與真實發現，並兼顧保障被告、犯罪嫌疑人、被害人或其他利害關係人的名譽、隱私、安全，而約束司法或執法人員履行職務的行為，非在保障其隱私。

8. (X) 鑒於新修正個資法關於特種個資蒐集、處理及利用之第 6 條尚未施行，因此目前公務機關蒐集、處理及利用個人病歷或基因等特種資料，完全不受電腦處理個人資料保護法或新個資法的規範。

解析：我國最高法院判決認為新個資法第 6 條尚未施行前，公務機關應依新個資法第 15 條及第 16 條規定辦理，故特種個資蒐集處理及利用仍受個資法規範。

9. (X) 依據行政院及所屬各級機關政府資料開放作業原則之規定，政府資料以公開及使用者付費為原則。

解析：行政院及所屬各級機關政府資料開放作業原則為行政院及其所屬機關推動開放政府資料的基本作業架構，其明定政府資料以公開與無償提供為原則。

10. (O) 歐盟法院判決認為搜尋引擎提供使用者，以自動化、系統性方式蒐集、儲存，並以清單方式提供使用者閱覽檢索結果的服務，屬於個人資料蒐集與處理活動，故仍應適用歐盟個資指令。

解析：搜尋引擎以自動化、系統性方式蒐集網路資料，加以記錄、儲存並以清單方式提供使用者閱覽，符合歐盟個資保護指令定義之個人資料蒐集與處理活動，自應遵循歐盟個資保護指令相關要求。



第二部分：選擇題

- 1.(4) 以下哪個規範面向，不屬於「行動應用 App 資安基本規範」之內容？(1) 行動應用程式發布安全。(2) 付費資源控管安全。(3) 行動應用程式碼安全。(4) 以上皆是。

解析：資安基本規範面向有以下五個：(1) 行動應用程式發布安全。(2) 敏感性資料保護。(3) 付費資源控管安全。(4) 身分認證、授權與連線管理安全。(5) 行動應用程式碼安全。

- 2.(2) 將個資業務委外時，下列哪個事項與委託機關依個資法及其施行細則負有監督義務的事項無關，而不一定要規範在招標文件或採購契約中？(1) 受託廠商所蒐集、處理或利用個人資料之範圍。(2) 受託廠商之最低員工人數。(3) 受

託廠商所採取的適當安全措施。(4) 委託關係終止時，相關資料之刪除或返還。

解析：依據個人資料保護法施行細則第 8 條第 2 項規定：「前項監督至少應包含下列事項：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第 12 條第 2 項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。」

3.(4) 以利用身分證自動產生器或利用他人身分證字號並以機器人程式，冒用他人身分執行網路訂票時，下列哪項敘述正確？(1) 機器人程式不是人，所以絕對不會成立犯罪。(2) 依目前國內最新實務，此類情形一律不會起訴。(3) 可能涉及刑法第 320 條竊盜罪。(4) 可能涉及刑法第 216 條行使偽造私文書罪，以及同法第 360 條干擾他人電腦與相關設備罪。

解析：利用身分證自動產生器，冒用他人名義訂票並領票使用，主要涉及刑法第 216 條行使偽造私文書罪；若以機器人程式大量訂票，以致影響系統運作或造成其負擔時，則可能成立刑法第 360 條干擾他人電腦與相關設備罪。

4.(2) 公司為進行考核而對員工活動從事監看時，下列何種方式較無疑慮？(1) 逕自在員工使用話筒安裝錄音設備。(2) 公告資訊監看政策並經員工同意。(3) 雇主本可無限制監看員工活動。(4) 查看員工通訊軟體私人對話紀錄。

解析：員工在工作場所仍享有某程度合理隱私期待，雇主未事先告知或經其同意，除有正當事由以外，尚不得任意監看員工通訊。

5.(2) 下列有關雇主要求求職者提供資料的敘述，何者正確？(1) 只要雇主想知道的資料都可以要求提供。(2) 與工作內容明顯無關的資料不可以要求提供。(3) 雇主取得求職者書面同意就可以免責。(4) 雇主要求求職者提供隱私資料不違反就業服務法。

解析：依我國主管機關函釋見解，雇主要求求職人或員工提供隱私資料，應尊重當事人之權益，不得逾越基於經濟上需求或維護公共利益等特定目的之必要範圍，並應與目的間具有正當合理之關聯。若職位業別無相關法令規範，雇主要求提供資料之範圍又與工作內容無關，將違反就業服務法之規定。

6.(4) 關於人民提起訴願所涉個資蒐集與資訊公開作業，以下何者正確？(1) 人民提起訴願不得以匿名方式為之。(2) 訴願決定書為依法公開資料。(3) 訴願決定書內容若涉及個人隱私或營業秘密時，得採限制公開方式。(4) 以上敘述均是正確的。

解析：(1) 依訴願法第 89 條第 1 項，提起訴願應載明姓

名等資料。(2) 訴願決定為政府資訊公開法所定機關應主動公開之內容。(3) 依個資法與政府資訊公開法第 18 條意旨，機關就資訊公開所涉隱私權益與公共利益衝突進行利益權衡，並應符合比例原則，必要時採取遮蔽措施或限制公開方式。

7.(3) 如果案件當事人想要取得法庭的錄音錄影，可以採取何種方式？(1) 開庭時只要告知在場人員後，就可直接自行錄音。(2) 以針孔攝影機偷錄。(3) 依法院組織法第 90 條之 1，向法院請求交付。(4) 法庭錄音錄影屬於公務機密，不得提供給案件當事人。

解析：依法院組織法第 90 條之 1 第 1 項，當事人及依法得聲請閱覽卷宗之人，因主張或維護其法律上利益，得於開庭翌日起至裁判確定後六個月內，繳納費用聲請法院許可交付法庭錄音或錄影內容。

8.(3) 若民眾認為搜尋引擎檢索結果所連結關於其個人資料的網頁內容，已過時、無關而影響其個人資料正確性時，可能得向以下何者請求移除該檢索結果連結？(1) 法務部。(2) 經濟部。(3) 搜尋引擎服務業者。(4) 縣市政府。

解析：參考歐盟法院判決意見，搜尋服務提供者以搜尋程式連結含有特定檢索字串之資訊，符合我國個資法所謂蒐集之定義，且搜尋服務提供者將檢索結果，以特定方式排列並提供使用者點選查閱，亦符合我國個資法關於處理活動之定義，而當搜尋服務提供者其資料蒐集處理活動應適用我國個資法時，當事人得依個資法向該個資蒐集者行

使停止利用或刪除之權利。

9.(4) 請問以下何者不是「行政院及所屬各級機關政府資料開放作業原則」所揭示的原則？(1) 政府資料以公開為原則。(2) 應建立意見回饋機制。(3) 力求資料之正確性及即時性。(4) 排除政府資訊公開法與個資法之適用。

解析：政府資料原則上應公開，並主動釋出具有便利民眾生活、提升生活品質及擴大運用價值等優勢的資料集，且政府機關亦須透過意見回饋機制，提供民眾反映使用建議或需求等，以營造雙向互動的使用環境，並藉由群眾力量共同持續提升政府開放資料品質。

10.(4) 請問以下何者「並非」政府機關將其保有個資檔案提供予第三人處理利用時，得主張符合個資法上特定目的外利用之事由？(1) 依法律規定。(2) 符合公共利益。(3) 基於學術研究而有必要，且資料處理後依其依其揭露方式無從識別特定。(4) 資料為機關無償提供。

解析：機關將本身保有含有個人資料檔案提供予第三人利用時，若非屬原先特定目的範圍，即應符合個資法第 16 條所定其一事由。



附錄二

資通安全法規更新對照表

領域	法規名稱	最新修正日期 (民國)	資訊安全管理相關條文	資訊安全管理面向修正 / 規範重點
資料保護	個人資料保護法	99/5/26	全文	<ul style="list-style-type: none"> •擴大保護客體，針對特種個資強化保護 •增加行為義務，包含告知、事故通知及委外監督等 •強化行政監督 •刪除行業限制，普遍適用主體 •提高民刑事與行政責任
	國家機密保護法	92/2/6 制定迄今未修正	全文	<ul style="list-style-type: none"> •明定國家機密之分級及核定權責 •明定國家機密之保護措施 •明定侵害或洩漏國家機密之罰則
	營業秘密法	102/1/30	全文	<ul style="list-style-type: none"> •新增侵害營業秘密之刑罰規定 •為因應跨國經濟間諜，針對域外利用營業秘密情形，加重處罰
	刑法	妨害秘密罪章 最新修正日期為103/1/15， 修正第315-1條	妨害秘密罪章 妨害電腦罪章	<ul style="list-style-type: none"> •明定構成以不當侵害他人隱私之行為樣態與刑責 •明定構成洩漏職務上或業務上應保密資訊之行為樣態與刑責 •明定構成不當入侵、干擾系統或電腦設備，或竊取、竄改電磁紀錄之行為樣態與刑責
	醫師法	101/12/19	保密義務	醫師不得無故洩漏病人病情等資訊

領域	法規名稱	最新修正日期 (民國)	資訊安全管理相關條文	資訊安全管理面向修正 / 規範重點
資訊公開	政府資訊公開法	92/12/28 制定迄今未有修正	全文	<ul style="list-style-type: none"> •政府機關應主動公開之資料範圍 •政府機關受理申請公開之方式 •政府機關必要時得拒絕或限制公開之事由 •政府機關公開資料之方式與時點
資訊監察	通訊保障及監察法	103/1/29	全文	<ul style="list-style-type: none"> •新增檢察官及司法警察官聲請調取 •明定他案監聽、逾越監聽目的、違法監聽所得之內容不得作為證據 •新增法官、檢察官違法監聽之行政及刑事責任
	電信法	102/12/11	6、7	明定他人不得盜接、盜錄或以其他非法之方法，侵犯通信秘密
資訊應用	電子簽章法	90/11/14 制定迄今未有修正	全文	<ul style="list-style-type: none"> •建立網路環境中識別相對人身分與確保電子文件完整性之方式 •電子文件效力與得否依法作為書面提出或保存

資通安全法律案例精選

發行人：行政院國家資通安全會報

地址：臺北市中正區忠孝東路 1 段 1 號

電話：02-3356-6500

委辦單位：行政院國家資通安全會報技術服務中心

執行單位：國巨律師事務所

出版日期：民國 104 年 9 月

「資通安全法律案例精選」著作權為行政院國家資通安全會報所有，機關單位若有任何進一步利用需求，歡迎洽詢聯繫。