論美國網路個人資訊隱私保護型態之轉變

作者：邱祥榮

發表於全國律師二〇〇一年十二月號

壹、 前言

每天上網收到信箱中電子郵件中，有許多是商業廣告。有的是因訂電子報將個人資料同意其使用，因而收到相關企業的新產品廣告；有的則是不認識的寄件者寄來的資料。在確認過沒有給過此人個人的資料後，對於其如何得到個人的電子郵件帳號感到疑惑，再加上網路上使用信用卡消費因而被得知信用卡卡號而被盜刷的事件層出不窮，不禁令人感到對於網路上資訊保護及隱私保護的不足，進而嘗試了解網路上關於個人資料保護的問題。

基本上，對於個人資訊隱私保護分成兩大模式，一為美國模式，另一則為歐盟模式。美國模式代表的是市場機制由下而上的管理模式（bottom-up）以及自我管制；相較於美國，歐盟是光譜的另一端，採取政府積極介、由上而下的管理模式（top-down）以及立法規範（或是具有強制力的指令來規範）。美國是現今世界國家中對外最具影響力的國家，不論是環境法的制定、推動，或者是核能問題，美國都是在世界上主導、要求他國改變配合的國家。就連隱私權的概念，亦是由 Samuel D. Warren 以及 Louis D. Brandeis 於一八九〇年在哈佛法學評論（Harvard Law Review）中發表的一篇專論 The Right to Privacy 中提出的[1]，隨後謂為風潮，而擴散至全世界。然而令人感到驚訝的是，在一百年後全球資訊網（World Wide Web）的技術誕生使得網際網路無遠弗屆的今日，相較於歐洲各國－如德、法等國－在網路隱私此一議題上，致力於個人資料保護不遺於力，美國本身卻是採取寬鬆的、放任的政策、委由市場及企業自制來達成網路上個人隱私的保護。這樣的作法，持續了相當長的一段時間，也備受隱私捍衛人士（privacy advocates）的批評。但是最近美國政府的態度卻起了一百八十度的轉變，究竟是什麼原因促成美國政府如此正視此一問題，筆者欲藉本文一探究竟。

首先，本文論述隱私權的起源，既而論及傳統網路對於個人資料侵害的情形、保護方式以及該傳統保護方式的缺點。接下來，對於最近美國對於網路隱私保護方式的轉變原因加以探究，本文嘗試將其轉變原因分為內在壓力以及外在壓力加以論述。

[1] See Don R. Pember, Mass Media Law, 2000Ed, 2000, The Mcgraw-Hill Companies, Inc., pp233-234

貳、 網路上個人資訊隱私的侵害、傳統保護方式及其缺點

一、 個人資訊隱私的侵害

雖然第一封透過網際網路（Internet）傳送的訊息（message）是發生在人類登陸月球後的第一個月，但是，由於當時網路多只用在學術研究，而且也不易使用，在使用的人少、彼此多能自我約束的情形下，商業界自然也就不會利用網路來做為推銷產品的媒介，也就不會產生個人資訊隱私權侵害的問題。而這種情形在一九九〇年以後，產生了革命性的改變。

一九九〇年代有二件重要的事件發生，因而帶動網路的發展，也引發了今日的個人資料保護的危機。第一件是全球資訊網（World Wide Web）的發明。由於 WWW 的發明，使得網路的使用變得非常容易，而且網站也如雨後春筍般地急遽增加。起先，WWW 是不能做為商業用途的，直到老布希政府（1989-1993）時才開放網路空間做為得以商業用途為目的之使用。而網路空間商業化是影響網路個人資料安全的第二件重要的事件，因為商業網站成為個人資料－特別是以可疑的方式蒐集而來的個人資料－的最主要使用者。

早期商業網站是隨心所欲地蒐集它想要的個人資料，不必得其許可，更不必在蒐集前後通知該人。在蒐集後，也可以任意地使用該項資料，如將其販賣給第三人等。此外，網站也不准許資料被蒐集的人有任何方式接近該項資料，更不必提供其所擁有的個人資料任何的安全保護。通常而言，其以下列幾種方式來幫助資料的蒐集：

(1)明白地要求使用者的資料
(2)藉由網站/消費者（website/consumer）的互動來取得消費者的資料，比如說網站會要求消費者個人住址以便通知相關訊息的方式取得其個人資料。
(3)有些網站會以附條件地進入的方式來取得個人資料。譬如說，要求使用者先填妥個人資料，始得進入。
(4)隨後，網站又發明了一種更精密的技術-cookies[2] -來蒐集個人資料。此種技術

[2] 所謂 Cookies 此種技術，目的為解決歷史記錄的方法，係為一種由瀏覽器所保留，內含有關該瀏覽器在某網站曾經做過的要求的純文字資訊。可以追蹤 Web 要求的狀態資訊，並將這些小量資訊儲存在瀏覽器軟體裡，以供後續使用。這項資訊是存放在客戶端的硬碟裡，只能被產生它的網站伺服器所使用。資料來源：http://www.ecpress.com.tw/Cookies.htm，搜尋日期，2001/6/19。藉由此種技術，使用者在該網站點選的主題便能被記錄下來，而該網站便可藉此了解該使用者的

使得網站得輕易在不被上網的消費者察覺的情形下，獲得其上網的資料。

商業網站任意的資料蒐集，造成了個人下面幾種損害。首先，是身分的盜用（identity theft）。亦即，在一個人的身分會被另外一個人有意地僭取。特別是利用被僭取之人的名義在網路上購物，造成該人的損害。第二個問題是，網站在蒐集個人資料時並不區分成人與兒童，甚至發生掠食兒童（predation on children）資料的情形。因為兒童對於有問題的網站的抵抗力，抗誘惑力是最低的，比如說，網站會用報名網路比賽的方式、註冊電子筆友（electronic pan pel）、或玩網路遊戲來吸引兒童提供個人資料，在面對五花八門這麼多的有吸引力的誘惑下，自然而然會提供資料給該網站。最後的這種損害，是當初沒有料想到但是卻是今日最嚴重的損害。早期許多公司網站蒐集個人資料的便利，對其前來應徵工作的人事先蒐集個人資料的就診紀錄、病歷資料等等，再以此為決定是否要雇用該人。例如，有美國前五百大的公司中，有三分之一曾利用個人醫療資訊來決定是否雇用、昇遷或是解雇該人，因而造成許多人減少或者不敢在生病時接受診療[3]。

二、 傳統保護方式及缺點

面對上述的侵害，最直接的作法就是向法院起訴主張損害賠償。然而除了司法救濟外，行政或立法在此時均未多涉入，基於市場機制的理念，希望能由網路自我發展出一套規範來約束其網站自身的行為。以下討論透過法院以及透過自我管制兩個面向來分析傳統保護方式及其缺點

（一） 透過法院

由於早期的網站的任意蒐集資料，造成許多人的傷害。既有損害，一般最普通的方式就是以訴訟的方式來加以解決。傳統上，美國關於隱私權保護的事項，屬於侵權行為法的範疇。然而，以訴訟的方式雖然可以在勝訴後獲得賠償，但是私人藉由法院來對抗資訊隱私的侵害時，往往有下述的不利益：

1.尋求實體正義困難

傳統隱私權的保護，美國各州並非全然接受。有些州法院完全不承認隱私權，有些州只承認部分的隱私權得加以主張，比如說 Minnesota 和 North Dakota 的法院拒絕承認隱私侵害為侵權行為之一，而 Vermonet 以及 Wyoming 法院，至今仍未

偏好。

[3] See Steven A. Hetcher, The Emergence of Website Privacy Norms, 7Mich, Telecomm. Tech. L. Rev. I.A.的說明。由於該篇文章是透過 Lexis-Nexiser Academic Universe 取得，該電子資料上並無頁碼，故將引註方式略做變更。

接獲任何隱私案例[4]。所以，除此之外，傳統隱私權的保護，除了少數的法律外[5]，並未有一全面性的成文法典，更遑論網路隱私的保護。便使該州法院承認網路隱私應予保護，受害人進行訴訟時，往往亦須取決於證據的取得及法院的心證，獲得勝訴實為不易。

2.程序利益無法兼顧

(1)進行訴訟的不經濟

由於法院是以個案（case-by-case）的方式來解決此項問題，而進行訴訟又須要花費許多的勞力、時間及費用。諸如聘請律師，出庭應訊以及調查證據等等的費用支出，徒增原告的負擔，同時也會用盡有限的司法資源以及造成該司法資源在其他類型訴訟上的應用。

(2)司法預算及人員有限，法院無法處理所有的紛爭

即使今天立法機關訂立了相當明確的指導原則，在今日產生如此大量的資訊隱私侵害案件的情形下，法院不可能解決所有的紛爭，蓋因司法預算及人員有限之故。

(3)維持訴訟進行之不易原告財力及時間的不足

許多受侵害的人在進行訴訟之後，發現要抗爭到底須要相當的毅力、時間及金錢的配合，是以，在絕大多數的案件中，原告均因沒有充分的時間和財力去持續進行訴訟，以致於半途而廢[6]。

---

[4] See 註 1，pp233,234。此外，關於那些州部分承認隱私權，可參酌該書 pp234 下面的附註。

[5] 如對於政府蒐集個人資料限制的法律只有一九七四年隱私權法（Privacy Act of 1974），對於私人的限制，也只有一九七一年公平商業徵信法（Fair Credit Reporting Act of 1971），一九八四年有線電視通訊政策法（Cable Communications Policy Act of 1984），一九八六年電子通訊隱私法（Electronic Communication Privacy Act of 1986），一九八八年錄影帶隱私保護法（Vediotape Privacy Protection Act of 1988）以及一九九四年駕駛人隱私保護法（Driver's Privacy Protection Act of 1994）。See Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in Ratcheting Up of U.S. Privacy Standards, Yale J. Int'l L, winter, 2000, pp23-25。

[6] See 註 4，pp.37。

（二） 透過自我管制（self-regulation）

1.主張自我管制的理由

除了上述向法院請求救濟外，亦有許多人主張應由網路發展出自我管制的機制來加以規範。此種說法為美國的主流見解。主要是因為美國自獨立以來一直是強調市場經濟及自由競爭的國家，政府一直保持有限政府（limited government）的模式。所以在大多數的議題中，均交由市場機制以及市場自我管制來解決問題，非不得已，國家不會介入。基於此種想法，論者多認為市場是由看不見的手（invisible hand）在推動，政府的介入是自由與市場的絆腳石，這雙強有力的手（heavy hand）將會影響自由競爭及自由創新。此外，既然以市場為導向，就自然會主張「由下而上」（bottom-up）地形成規範。換言之，認為應該透過自我管制來管理網際網路上的問題，政府不應由上而下（top-down）的介入[7]。問題是，自我管制的理念是否可能落實，或者只是網路業者高舉的煙幕（smoke screen）而已呢？以下將藉由競賽理論（game theory）來討論自我管制的可能性。

2. 自我管制的可能性－由競賽理論（game theory）來分析

傳統上認為提供消費者較佳的隱私保護為網路業的一種利益。也就是說，如果網路業對消費者提供更多的個人隱私保護的尊重，將可獲得消費者對於網路消費的信任及信心，而可根本地增加電子商務的成長。然而，這樣的想法，是相當有問題的。問題在於我們是將所有網路業視為一個行動一致的整體，但在現實上並非如此。由理性、經濟的觀點來說，每一個網站其實都是自私自利的，都在追求最大的利潤，因此對於一個網站而言，最好的方法是搭便車在其他網站的努力上（free ride on the contributions of the other sites），因為這可減少因尊重隱私權而須付出的成本。這藉由經濟學上的競賽理論獲得證明。首先，吾人可將報價矩陣（payoff matrix）圖示如下：

	a *不尊重*隱私保護	a *尊重*隱私保護
其他網站*不尊重*隱私保護	（2，2）	（1，4）
其他網站*尊重*隱私保護	（4，1）	（3，3）

[7] See Paul M. Schwartz, Internet Privacy and the State, 32 Conn. L. Rev., spring 2000, pp815, 844.

例如，有一個網站ａ不尊重隱私權保護，其他網站均尊重隱私權的保護時，ａ網站若搭便車於其他網站尊重隱私權的行為上時，將可獲得最大的利益。這是因為當大多的網站尊重隱私權時，消費者較不懼怕上網，因此，也較傾向於參與網路上的電子商務消費活動。而這樣的情形，將使ａ網站更易於藉由其不尊重隱私的行為來獲取利益，因為消費者本於與其他網站間的正面經驗，會很自然地提供個人資訊網站ａ，而造成ａ可既可不付出保護隱私的成本，又可因而獲得最大的利益４。

雖然全部的網站都力行尊重隱私權保護的話，所有網站將會獲得次高的利益３，但是因為每一個網站都是自私自利的，都要追求自己公司的最大利潤，所以均會選擇與ａ公司相同的模式，亦即，不尊重隱私權的保護。但是，當所有的網站都選擇不尊重隱私權保護時，所有的網站均只能獲得次低的利益２，而無法獲得最高的利益４。[8]

由上面的討論可以得知，在所有的網站均自私自利追求最小成本、最大利潤的情形下，自我管制的最終結果，就是全部的網站都不尊重隱私的保護。所以，想要藉由自我管制的方法達到保障網路上個人資訊隱私保護的目的，似乎是一種不切實際的奢望。

參、 隱私權保護方式轉變及原因探究

傳統上是透過法院及自我管制來約束網路上個人資訊隱私的侵害。但是，正如前所已說明的，其缺點甚多且成效不彰。近年來，美國的行政及立法單位，已正視此一問題，逐漸介入影響市場關於網路個人資訊隱私保護政策的形成與執行，例一九九八年立法通過的兒童線上隱私保護法（Children's Online Privace Protection Act of 1998）[9]、美國聯邦貿易委員會（Federal Trade Commission，下稱FTC）的積極介入、商務部（Departament of Commerce）於一九九九年四月公布「安全港原則」（Safe Harbor Principles），再加上許多網站都逐漸公布其網路資料隱私保護政策。美國在保護網路資料隱私上沈寂已久後有如此重大轉變？本節將分成內在壓力與外在壓力來論述其轉變的原因。

[8] See 註 2， I.B.2 的說明。
[9] See 註 6，pp.856.

一、 內在壓力

（一）聯邦貿易委員會的積極介入

一九九五年，美國國會要求 FTC 調查與網路資料庫有關的隱私權危機。從此之後，FTC 便逐漸涉入線上隱私（online privacy）的議題之中。FTC 嘗試藉由影響消費者以及網路業的行為，來推動更加尊重網路隱私的規範。早期，FTC 致力於教育大眾有關他們個人資料在網路業的使用，支持提供資訊來幫助想要尋求個人自我隱私的消費者的網站，以及主持網路業代表和隱私權運動人士聚首的研習會。但是，FTC 近來認為，單單只靠他們自身付出教育的努力並不足夠，必須同時促使改變既有的規範構，才能達到效果。亦即，這樣的結合必須能增進網站本身的利益。所以，首先 FTC 開始以更具體的條文教育網站「對於隱私適當程度的尊重」。其次， FTC 於一九九八年，威脅網路業，要求改變既有的自治規範節構，宣稱如果網路業不發展出一套尊重隱私的自我管制方式的話，就會要求國會立法來解決。鑑於 FTC 最近才成功的影響國會通過兒童線上資料隱私保護的立法，故此一威脅性言論並非只是紙上談兵，網路業若真的不予理會，依然故我的話，等到國會立法後，將會大幅增加美國網路公司關於隱私保護的支出。是以，在 FTC 發出此一威脅後，造成許多公司開始轉變其態度[10]。

（二）大型企業（網站）對於小型企業（網站）的影響

網站的規模有大有小，在上述 FTC 的威脅下，大網站在隱私保護上會比小網站做得好，其主要原因在於大網站容易成為 FTC 殺雞儆猴的對象。因為它是規模大的網站，若帶頭不尊重 FTC 的要求時，很可能會成為被 FTC 第一個開刀的對象。相較於大網站，小網站的主流偏好還是不提供隱私保護的方案，主要就是因為它小，所以較易在 FTC 的雷達掃瞄追蹤下安全通過。因此，小網站的地位就很像前面所提的競賽理論中的 a 網站，當其他的網站都遵守隱私權的保護時，不遵守的小網站便可搭便車，而獲得最大的利益。

面對這樣的情形，大網站發展出一套方式來要求小網站遵守資訊隱私規範。即大網站開始威脅那些不對隱私採取適當尊重的小網站，不許其刊登廣告。IBM、微軟、迪士尼等大公司最近均宣稱，他們將不讓那些採用適當隱私保護的網站上在其網站刊登廣告。許多小網站不願與這些大網站產生對立，所以開始提供保護隱私的方案。須注意的是，大網站所可以威脅的小網站，並不限於重覆與其有互動的小網站，甚至只有與其接觸過一次的小網站也會受其影響。因為這些

[10] See 註 2，II.A.的說明

小網站普遍地希望能有被這些大網站允許在該網站上刊登廣告，而不希望一點刊登的機會也沒有。因此，大網站藉由此種方式，迫使小網站均尊重隱私的保護，使得搭便車的情形下降，增加大網站本身的利益增加，亦即使全體網路的利益朝向報價矩陣的右下角移動[11]。

（三）小結

總之，FTC 在資料隱私保護的介入，使得原先的完全自我管制的情況改觀。但是與其說所有的網站均受其影響，毋寧是只有大型網站受 FTC 直接的影響，而再透過大型網站對於小型網站廣告限制的壓迫，促使小型網站亦增強其對於隱私的保護。也就是 FTC 透過大型網站對於小型網站產生間接的影響。但無論如何，美國網路隱私的尊重不能不歸功於 FTC 的積極介入。

二、外在壓力－歐盟指令（EU Directive）

（一）．歐盟指令產生緣由

在經濟全球化（economy globalization）的影響下，每一個國家對於該國資料隱私的保護均會影響到其他的國家。為了保障歐洲各國人民的資訊自主以及個人資訊不受外流的影響，歐盟在一九八八年十月二十四日通過關於保護個人資料處理及此種資料自由運動指令（European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data）。歐盟指令的產生原因主要有下列幾點：

1.個人資料保護必須合作互助

就實證的觀點來說，保護個人隱私的目標與確保在歐盟內交易自由化的目標是不可分的。上述兩者之所以不可分，並非是因為其為天然地聯結在一起，而是因為政治上的原因使然。換言之，歐盟會員國中之一若採取對於資料隱私控制採取較不嚴格的管制方式，將會產生重要的外部性（externality）效果。而此種外部性效果，將會影響其他會員國的國民。例如，德國雖然對於資料的蒐集與傳送的控制採取較嚴格的方式，但是，若德國的公司可自由地傳送資料到採取較不嚴格管制標準的義大利時，德國本身對於資料蒐集與傳送的控管的目的將無法達成，蓋在義大利境內，可自由地、不受限制地將該資料傳送到其他國家。又，因為德國與義大利為二個不同的司法管轄權，德國司法機構對於義大利境內的資料傳送將無法管制，所以義大利對於個人資料較鬆散的管制，將產生外部效果，而

[11] See 註 2，II.A.的說明，並請參閱本文貳、二、（二）的報價矩陣。

影響到德國的居民。因此，歐盟的會員國若欲達到資料隱私保護的目的時，非藉由各國的互助不可。

2.德國與法國對於高度資料隱私保護的需求

由於德、法兩國須要的個人資訊隱私保護較他國為高，而進入該國的市場對於各國又相當的重要，所以這些會員國便在歐盟貿易自由化的規則中要求實行相當高的資料隱私保護。因此，此一指令也可說是在已具有保護資料隱私法的會員國（如德國、法國）威脅其他較不重視資料隱私保護的會員國（如義大利）的前提下協議成立的。為促成全歐盟會員國均提供相近的資料隱私保護，也為了確保創立單一內部市場（a single internal market）自由貿易的經濟利益，歐盟會員國便一致同意提供更加嚴格的資保隱私保護。

須注意的是，如果今日是較小的國家需要較高的保護時（如希臘、葡萄牙），幾乎是不可能透過歐盟對他國產生壓力。正是因為這些強大國家利益的集中，以其廣大的市場為後盾，有可能推動歐盟保護個人資訊隱私的指令向前一步。亦即，就是因為德、法兩國政治性地利用市場力量，才能使得在歐盟內的資料保護標準向上提昇[12]。

3.對抗歐盟以外第三國的鬆散資料隱私管制

在全球化的影響下，只靠歐洲內部各國的合作，可能仍無法達到其境內居民資料的保護，因此，除了對歐盟會員國的約束外，獲得多數會員國同意的歐盟指令的第二十五條，亦賦予歐盟執委會（European Commission）得決定禁止所有資料傳送至第三國的權力。其標準為該第三國是否採取適當層級保護（an adequate level of protection）措施以確保個人資料的隱私。如果經該委員會認為措施不足時（not deemed “ adequate ”），則可以禁止所有的資料傳送至該國。然「適當」（adequate）此一概念並未在歐盟指令加以定義，而是視個案方式加以認定。

雖說個案認定，但是對於是國家保護措施是否適當，但其評估仍有下列的原則可供參酌：

(1)資料的處理必須限於一定的目的

(2)該目的須要使相關的個人知曉

(3)個人必須有接近及拒絕其處理該資料的權利

(4)個人必須有可獲得的程序機制來有效執行此保護措施

(5)第三國資料接收者不得將該資訊傳送至不符合「適當層級保護」的其他國家

[12] See Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in Ratcheting Up of U.S. Privacy Standards, Yale J. Int’l L, winter, 2000, pp11-12.

換句話說，只有該國資料處理的規範符合歐盟「適當」的標準者，方才得列於「安全名單」（white list）上，從而可避免可能禁止所有個人資料傳送的禁令[13]。

（二）歐盟指令的內容

相較於美國多依賴私人市場的運作過程來保護個人資料，歐盟採取較多的立法方法來保障資料隱私。值得注意的是歐盟指令廣泛含蓋了私領域的活動，並且創造了在企業進行蒐集及使用個人資料前（ex ante）、後(ex post)的控制。以下將就其重要的保護措施加以簡介。

1. 打擊面為全方位

除了某些例外情形（如公眾安全或刑事法律規定），凡是取得、蒐集個人資料的手段－不限於商業活動或使用－均為歐盟指令所涵括，為其第一個特色。

2. 歐盟指令要求進行蒐集個人資料事前（ex ante）的控制

歐盟要求資料的控制者（data controller），告知（inform）資料主體（data subject）其身分，蒐集其資料的目的，以及其他必要的資訊以確保公平的資料蒐集程序。另外，只能基於特定的目的擁有及使用該項資料，所以企業不得基於上開目的蒐集不必要的資訊。

此外，歐盟指令特別要求在第一次以直接的交易目的將個人資料給與第三人前，該個人須被告知。並且明白地給與該個人拒絕無償取得或使用的權利。資料的控制者或是其代表必須明白地告知該人買受該資料的第三人身分或其種類，否則其同意將被視為無效。

另外，關於敏感資訊（sensitive information）的蒐集，各會員國均必須嚴格禁止，或是經予個人選擇的權利，於其選擇進入（opt in）後，方得為之。換言之，敏感資料的蒐集原則上是不予准許，只有在給予該個人選擇 opt in 的選擇後，才得為之。敏感資訊的範圍包括所有可揭露個人種族、少數民族的血統、政治意見、宗教或哲學信仰、工會成員以及與健康、或性生活相關的資料。又，凡基於自動而未經本人同意所蒐集的資料（如個人信用價值或工作）而做成的任何明顯影響個人的決定，歐盟指令承認個人有權利去挑戰該決定。

[13] See 前註，pp.21-22.

3. 歐盟指令要求進行蒐集個人資料事後（ex post）的控制

歐盟承認個人有權利監控並挑戰於蒐集個人資料的使用。歐盟指令保證個人有下列幾個永久的權利：

(1)具有免費、不受限制以及迅速接近被蒐集的個人資料的權利。
(2)具有獲得有關其資料的備份的權利。
(3)具有更正其資料的權利。
(4)具有確認其蒐集資料的目的及接收資料之第三人的身分權。

因此，個人得以追蹤那個第三人持有有關他的資訊，確認該第三人如何使用此項資訊以及禁止不符合資訊控制者第一次告知的使用。

4. 歐盟指令賦予個人重要的執行權利

歐盟指令要求會員國給資料隱私受侵害者司法補償。個人也可挑戰資料的正確性、蒐集程序、以及阻止其資料的擴散。為了有效執行，歐盟指令亦規定會員國必須指派一獨立的公家機關負責監控。監督機關具有下列的權力：

(1)調查蒐集資料程序運作的權力
(2)於該資料蒐集程序運作前遞送意見的權力
(3)阻止、抹去或破壞資料的權力
(4)對於蒐集資訊程序發出暫使或具有決定性的禁令的權力
(5)進行訴訟以對抗侵害者的權力
此外，根據各個會員國的法律，亦有可能有罰款或監禁等民事或刑事的制裁[14]。

（三） 歐盟指令對美國產生影響力的原因

1.歐洲各國結盟成一整體強化國際地位，擁有足以對抗美國的政治影響力

在歐洲各國成立歐盟後，美國逐漸將其視為與歐洲各獨立國家相同的一個政治實體，所以近年來也逐漸增加與歐盟間的會議和協議。這也可以由美國和歐盟

[14] See 註 11，pp14-17。

於一九九五年十二月成立了新跨大西洋會議（New Transatlantic Agenda）可以得到證明。而正因為歐洲各國將貿易協議的權力授權給歐盟機構，使得歐洲各國能夠以整體、單一且強有力的方式在國際中發聲，強化了歐盟在國際貿易協議的地位。

美國是世界上相當具有影響力的國家，但是，正因為歐洲各國將有關傳送資料保護事件的協議權移轉給歐盟執委會（European Commission），而能一致地對外發聲，無形中也增強了歐盟各國本身的自治權以及影響力。歐盟權力集中化後，使得歐盟要求嚴格管制跨大西洋資料傳遞（transatlantic data transfers）的想法更能獲得落實。在歐盟成立以前，雖然歐洲有不少國家立法對於資料權送至美國加以嚴格限制，但是對於這種限制資料傳送至國外的規定，實際上要執行甚為困難。然而，這一切都在歐盟指令生效之後有了不一樣的情形。美國開始認真地對歐盟指令做出回應，嘗試與歐盟的官員協調一個解決方案。同時，美國的企業為了避免受到歐盟管制的衝擊，也對歐盟指令作出回應，加強了其內部資料隱私保護。

歐盟會員國在主權集中與行動一致後，藉由擴大資料傳送禁令的影響以及如果美國報復此一禁令的結果，歐盟會員國增強了其與美國談判的力量。若沒有此一與美國相當地位的力量，美國很可能會藉由威脅報復的手段，用其壓倒性的政、經實力來打擊各個獨立的會員國。可是在歐盟成立後，美國節制了許多。主要的原因是歐盟反報復的威脅（the threat of counter-retaliation）是足以與美國匹敵的一股力量。因此，歐盟會員國以有效影響其談判權力的方式重置了主權，並因此增加－與美國相較－其獨立自治的地位[15]。

2.歐洲廣大市場的吸引力

美國商業的發展須要擴展、開發外國市場。而歐洲廣大內部市場，一直是美國商業眾垂涎的一座寶山。因為歐洲居民的生活水準高，較為富裕，消費能力強，但同時也對於個人資訊隱私的保護有較一般開發中國家更高水準的要求。因此，為了能夠開發歐洲的市場，使得美國不得不考慮其不適當的資料隱私保護規範，而順應歐盟的資料隱私的法律。同樣的挑戰若是由一個不能吸引美國投資或貿易的國家，或是由經濟規模較小而極易受到美國報復的威脅的國家提出，可能其影響力就微乎其微[16]。因此，除了上述的政治影響力外，歐洲廣大的市場也是另一個其足以影響美國的原因。

[15] See 同註 11，pp40-42。
[16] See 同註 11，pp82。

（四）美國資料隱私保護受歐盟指令影響後的轉變

美國政府對於個人資訊隱私保護，分裂為兩派。一派為仍支持以市場為主的方式，亦即以自我管治（self-regulation）方式來達成保護的目的，此派以商務部（Department of Commerce）為主。另一方面，聯邦貿易委員會（FTC）則主張採取積極的方式、促使立法的方式來擴大資料隱私的保護，例如 FTC 成功地促使國會就兒童線上資料隱私保護在一九九八年秋季完成立法。關於 FTC 的部分，前以論及，不再贅述。

為了在與歐盟協調時能有效捍衛、保護美國的商業利益，商務部也同樣地促使各企業增強其自我管治的程序，否則，商務部所倡導的以自我管治來保護隱私的方式將失去其可信度。為了向歐盟證明得以商業自我管制確保隱私保護，以及能讓美國商業能不受歐盟資料傳送規定的限制，商務部於一九九八年十一月，即歐盟指令生效後的一個月，起草了一份安全港原則（Safe Harbor Principles）。在與國內的工商業界及密集地對外與歐盟相關權責機構協調後，於一九九九年四月十九日正式公布了修正後的安全港原則。歐盟則在二〇〇〇年七月二十七日，正式認定「安全港原則」對歐盟之資料傳輸將可提供適當之保護。茲將其主要內容說明如下：

(1)通知（Notice）：機構必須通知（notify）消費者有關收錄及使用個人資訊之目的，並提供消費者有關請求（inquiries）或抱怨管道之資訊，及對第三者揭露個人資訊之型式、機構賦予第三者使用及揭露個人資訊之選擇（choices）及方式（means）等之資訊。

(2)選擇（Choice）：機構必須提供消費者有關個人資料不對第三者公開揭露，或不用於其他用途（非原始資料蒐集目的）之選擇機會（opt out choice）；對於敏感性資料（sensitive information），當機構擬將資料對第三者揭露或另有用途時，須獲得消費者本人肯定或明確（affirmative or explicit）之同意（opt in choice）。

(3)轉送（Onward Transfer）：當機構擬將消費者所提供之個人資料對第三者揭露時，須遵循上述「通知」及「選擇」原則。當第三者為機構之任務代理人（an agent），且符合安全港原則或歐盟隱私保護水準，則機構可將消費者之個人資料傳送給該第三者。或者機構可要求第三者與其訂定書面協議（written agreement），確保第三者對個人隱私保護與安全港原則具相同之基本水準。

(4)取出（Access）：消費者必須有合理之管道更正、修改或刪除不正確之個人資料，惟倘提供消費者取出資料之負擔或費用不符合風險及隱私之比例原則，機構

得拒絕提供消費者「取出」之權利。

(5)安全（Security）：機構必須採取合理審慎之保護措施，以避免個人資料之遺失、遭濫用（misuse），無授權之情況下取得個人資料、遭公開揭露、毀壞（alternation and destruction）。

(6)資料完整（Data Integrity）；機構必須採取合理之步驟，保持資料之正確、完全、更新。

(7)執行（Enforcement）：為了符合安全港原則，機構必須：（Ａ）提供獨立之申訴機制（recourse mechanisms），依據相關法律或私人部門訂定之規範，處理消費者申訴案件之調查、解決及損害補償；（Ｂ）提供消費者對公司於安全港原則下之承諾執行之查驗程序；（Ｃ）倘因不符合安全港規範而產生問題，組織須負解決問題之義務。制裁必須相當審慎嚴格（rigorous），一旦因不符合規範而遭安全港組織清單除名者，將永遠無法再度列名於安全港組織清單中[17]。

安全港原則為美國與歐盟間隱私保護之橋樑，可確保歐盟境內民眾之個人資料可獲得適當之保護。這個原則表面上無意去影響美國的法律，但是值得注意的是，如果任何公司採用了安全港原則，但是卻不遵守的話，就會使自己限入挑戰FTC「在商業上使用不公正或欺瞞手段或策略」規定的胡同中。依據聯邦交易委員會法案（the Federal Trade Commission Act），違反安全港原則之公司，將被聯邦交易委員會視可起訴之詐欺行為（deceptive and actionable），起訴對象可包括宣稱依循安全港原則之自律業者組織，聯邦政府可處以每日一萬一千美元之最高罰緩。相反地，如果該公司並未採用隱私保護政策，FTC 就無介入的管轄權。所以，雖然不強迫美國公司採納這些原則，但是大多數的大型企業為了避免在資料傳送上與歐盟的規定牴觸，多會去遵守。一旦遵守，即不能有違背的行為，否則可能會受到 FTC 的制裁，因此，吾人可說基本上「安全港原則」形成了美國保護資料隱私的基本規定[18]。

（五）　小結

由上面的討論我們可以得知，歐盟指令的內容與美國安全港原則的內容雷同，這是歐盟利用其市場及政治上的力量，迫使美國在網路的管制上由原先的完

---

[17] See 註 11，pp.56-60。譯文係引自 http://www.trade.gov.tw/impt_issue/impt_6/ec-rept03-3.htm，搜尋日期，2001/6/19。

[18] See 註 11，pp.61-63 及 http://www.trade.gov.tw/impt_issue/impt_6/ec-rept03-3.htm，搜尋日期，2001/6/19。

全「自我管制」，轉向成為由政府介入引導的模式的一個成功案例。雖然「安全港原則」畢竟僅是一個原則，不具有強制約束力，與歐盟指令具有強制約束力有所不同。但是，由於美國公司希望能深入歐洲市場之故，多半會選擇遵守此一原則。然一但採用了安全港原則，即不得為違反，否則即屬以不正或欺瞞手段進行商業活動，將遭受 FTC 的制裁。是以，實際運作的結果，與歐盟指令所欲達成的目的接近，因此，歐盟指令可謂成功地影響美國國內的個人資料保護政策。

肆、 結論

網路資料隱私保護的問題應如何加以解決，眾說紛云。大體而言，有透過自我管制及政府訂立法律加以規範。前者以美國為例，後者則是以歐盟為代表。美國之所以採取以自我管制為基調的保護方式，實源自於立國以來的傳統，亦即，不認為一個大有為的政府（big government）是一個有利於人民、經濟體制運作的好的政府，反而認為一個有限政府（limited government）才是較佳的選擇。在此一概念下，凡屬於市場機制可以自我解決的，政府便應儘量不插手干預、不加以管制。然而由本文的分析，不難得知，在網路資料隱私的保護上，若欲介由完全的自我管制則達成該目標之日將遙遙無期。在歐盟指令通過以後，美國被迫就正視網路資料隱私保護的問題，再加以國內許多隱私保護運動人士的鼓吹，終於使其由原先自我管制的方向，轉型為由政府引導的自治模式。雖然美國並沒有對於網路隱私保護加以立法，但是在實際的運作上有 FTC 的監控、大型網站等內部壓力以及歐盟指令外部壓力的影響，使得資料隱私的保護較以往的情形躍進許多。未來，期許全球的網站不只是「尊重」個人隱私而已，而是更能落實「遵守」網路隱私保護的規定，使每一個網路使用者都能無憂無慮地使用網際網路，而不用擔心非法的個人資料蒐集。