美國提出個人資料安全及外洩通報法草案

華盛頓特區於今〈2010〉年8月5日由阿肯薩州及維及尼亞州參議院議員Pryor及John Rockefeller所倡議之「個人資料安全及外洩通報法」〈Data Security and Breach Notification Act of 2010〉，其旨趣，在於統一美國各州不同個資外洩通報法，並嘗試為消費者個人資料之安全及隱私設定全國性的標準。

Pryor法案曾於2007年提出，惟當時未能通過，其立法緣由係為處理美國各州、聯邦及國際間政府對個資安全與日俱增之重視。其規範內容，在要求處理及儲存消費者私人資訊，諸如「社會安全碼」〈social security numbers〉之企業，一旦發生資料外洩事件，需對國家提出通報，如該事件對消費者產生現實的「身分盜竊」〈identity theft〉或「帳戶詐欺」〈account fraud〉風險，則應於發現個資外洩六十日內通知受影響之消費者。

Pryor法案之適用對象甚廣，故有認為，該法一旦通過，其將成為繼美國金融服務法〈the Gramm-Leach-Bliley Act，簡稱GLBA〉後的模範法典，其適用對象包括受GLBA規範之金融機構及任何個人〈any individual〉、合夥〈partnership〉、公司〈corporation〉、信託〈trust〉、工地產產業〈estate〉、合作社〈cooperative〉、協會〈association〉、維持或傳送「敏感的會計資訊」或「敏感的個人資訊」之業主〈entity that maintains or communicates “sensitive account information” or “sensitive personal information”〉，但並不包括任何政府辦事處或其他聯邦、州政府單位、地方政府〈any agency or other unit of the federal,state, or local government〉或任何其下所再劃分之單位〈any subdivision thereof〉。

惟此一倡議中之資料安全立法不論法令遵循或執行皆有一定難度，因該法雖要求對超出「損害門檻」之資料外洩需對消費者通報，但對「損害門檻」並無明確定義。此外，受影響之企業似無實行適當風險評估之誘因，除需耗費大量成本評估外洩事件是否超過損害門檻外，尚需面臨企業名譽受損與客戶不滿之損失，在個資外洩要素風險指導原則付之闕如之情形下，企業恐無法客觀地評估自身個資外洩之風險。故有建議，解決之道，應明定損害門檻，並聘請外部專家或使用市場新工具，訂定客觀的指導原則，使企業在處理個資外洩問題時能減輕混亂及鼓勵評估結果的一致性並縮短風險評估的時間。

就資訊安全部分，此法案揭櫫於其通過一年內，美國商務、科學及交通委員會〈Committee on Commerce, Science, and Transportation〉應頒布規定，要求擁有或處理含有個人資料或契約之企業，必須建立並執行蒐集、使用、出售，及其他傳播、維持個人資訊之資訊安全政策，以達保護個人資料之目的。

相關連結

- 美國聯邦法案提案動態
- 個人資料安全及外洩通報法提案介紹

孫嘉欣 編譯整理

上稿時間：2010年12月27日

資料來源：

個人資料安全及外洩通報法提案介紹，http://www.willkie.com/files/tbls29Publications%5CFileUpload5686%5C3459%5CThe-Data-Security-Act-of-2010.pdf，最後瀏覽日201
0年12月17日
美國聯邦法案提案動態，http://www.govtrack.us/congress/bill.xpd?bill=s111-3742，最後瀏覽日：2010年12月17日

推薦文章