美國網路安全相關法規與立法政策走向之概覽

美國網路安全相關法規與立法政策走向之概覽

科技法律研究所
法律研究員 沈怡伶
104年08月11日

網路安全（cyber security）是近年來相當夯的流行語，而在這個萬物聯網時代，往後數十年對於網路安全的關注勢必不會減退熱度。在美國，因層出不窮的網路攻擊和資料外洩事件讓政府機關不勝其擾，也讓許多企業產生實質上經濟損失和商譽受損，隨之而來的是聯邦和州政府主管機關的關切目光，除了透過政策和行政規管之外，國會也開始制訂新法或對現行法規進行修法，補入對於網路安全維護之要求，以下本文將簡介美國現行法規範之要點及目前最新法案。

壹、美國聯邦政府相關網路安全規範、標準及措施

一、金融業相關管制規範

對金融機構的管制依據為「金融服務業現代化法/格雷姆-里奇-比利雷法（Gramm-Leach Bliley Act, GLBA ）」，該法要求金融機構必須建置適當的程序保護客戶的個人財務資訊，維護客戶個人資料的機密性、完整性和安全性，避免遭受任何可遇見的威脅或騷擾，以及避免任何未經授權的近用行為導致損害或對客戶造成不便利[1]。

另外美國證券交易委員會（Security and Exchange Commission, SEC）下設法令遵循檢查與調查室（SEC Office of Compliance Inspections and Examinations, OCIE），在2014年發布全國檢查風險警示（National Exam Program Risk Alert），命名為「OCIE 網路安全芻議（OCIE Cybersecurity Initiative）」，用來評估證券交易商和投資顧問對網路安全維護的準備以及曾遭遇過的資安威脅種類和經驗；而金融監管局（Financial Industry Regulatory Authority ,FINRA）也在2014年實施「掃蕩計畫（sweep program）」，金融監管局就其主管的特定企業會寄發的檢查通知書，要求回答有關於企業網路安全的相應準備措施[2]。

二、支付卡產業資料安全標準（Payment Card Industry Data Security Standard, PCI DSS）

該標準是由支付卡產業標準協會由五家國際信用卡組織聯合訂定的安全認證標準，雖不具法律位階，但因其公信力，美國企業都會自律遵循的規範，保護支付卡的資料安全。該標準關注於組織應該要開發和維護資訊系統和應用程式，並追蹤和監督網路資源和持卡者的個人資料，並發展出一個強健的支付卡數據安全流程，包括預防、偵測及適當回應資安事故的方式[3]。

三、醫療健康資訊相關管制規範

「健康保險可攜式及責任法（Health Insurance Portability and Accountability Act of 1996, HIPPA）」是最先開始要求所有電子化的受保護醫療照護資料在創建、接收、維護和傳輸時，需受有基本的保護措施和機密性之法規[4]；爾後，「經濟與臨床健康資訊科技法(Health Information Technology for Economic and Clinical Health Act, HITECH)」則將HIPPA適用主體擴及所有處理受保護醫療照護資訊的個人和機構，並強化資訊傳輸時的安全性和效率性規定[5]。

貳、立法焦點新況：網路安全及網路威脅資訊共享

美國政府對網路安全非常看重，因其對國家經濟和國家安全都有巨大的影響力，不過美國總統歐巴馬曾明白表示美國對於資訊及通信基礎建設的防護措施尚未到位，也尚未建立數位關鍵基礎建設的全方位發展策略；透過盤點與檢視，美國政府的網路空間政策（Cyberspace Policy）方向之一，是建立網路安全合作夥伴關係，包括各級政府間的水平合作及公、私部門間的上下合作網絡，共同研發尖端技術因應數位式帶的網路安全威脅[6]。

針對網路威脅資訊分享方式，美國國會一直持續的研擬相關法案，希望能在妥適保護公民隱私和公民自由的前提下，建立資訊分享管道，2015年3月美國參議院提出754號法案「網路安全資訊分享法2015（Cybersecurity Information Sharing Act of 2015, CISA）」[7]，試圖將CISA作為國防授權法（National Defense Authorization Act，NDAA）修正案之一部，但卻未獲得足夠通過票數[8]。CISA係由美國情報局（Director of National Intelligence）、國土安全部(Department of Homeland Security)、國防部（Department of Defense）和司法部（Department of Justice）共同定之，計十條，目的之一是希望透過法律授權讓聯邦政府機關能即時的將機密性或非機密性網路威脅指標分享與私人實體（個人或企業）[9]、非聯邦政府機關單位、州政府、原住民政府和當地政府，以阻止或減輕網路攻擊帶來的負面衝擊；其二，允許私人實體得為網路安全之目的，在一定要件下監控自己或他人的資訊系統，以運作相關的網路安全防御措施，並分享資訊給聯邦各級政府。CISA亦設計了監督機制，和隱私及公民自由保護條款，避免變相創造一個撒網過廣的監控計畫[10]。CISA法案雖未通過，但參議院並未放棄，欲以該法案的基礎框架進行修正，修正重點為訂定資料外洩事件通報標準並擴大隱私權之保護，預計於同年8月底國會休會期前再次提出修正版本進行表決[11]。

現行法案重點在資訊共享並授權私人實體監控自己或他人之資訊系統，而主要分享標的為「網路威脅指標（cyber threat indicator）[12]及「防禦措施（defensive measure）」[13]。網路威脅指標係指有必要描述或鑒別之：

一、惡意偵察，包括為蒐集與網路安全威脅[14]或安全漏洞之技術資訊，而利用異常態樣的通信模式。

二、能破解安全控制或利用安全漏洞的方法。

三、安全漏洞。包括能指出安全漏洞存在的異常活動。

四、使用戶合法使用資訊系統或儲存、處理、傳輸資訊時，不知情地使安全控制失效或利用安全漏洞的方法。

五、惡意網路命令和控制。

六、引發實際或潛在的危險，包括因特定網路安全威脅使資訊外洩。

七、其他任何具網路安全威脅性質者，且揭露並不違法其他法律者。

八、任何結合上開措施之行動。

防禦措施（Defensive measure）則指一個行動、裝置、程序、簽名、技術或其他方式應用於資訊系統或透過該資訊系統進行儲存、處理或傳輸之資訊，能防禦、阻止或減緩已知或懷疑的網路安全威脅或安全漏洞。但不包括私人實體自行/經聯邦機關或其他實體授權同意，破壞、使其無法使用或實質傷害資訊系統或資訊系統內之資訊的相關措施。

就資訊共享部分，法案第3條及第5條分別明定聯邦機關分享機密性網路威脅指標給私人實體、以及私人實體分享網路威脅指標和防禦措施給聯邦政府機關之管道。前者指定司法部應會同國土安全部、國家情報委員會及國防部訂定相關辦法，；後者相關辦法由司法部訂定，讓聯邦機關依法接收來自私人實體的指標和防禦措施，不論是電子郵件、電子媒體、內部網路格式、或資訊系統間的即時性和自動化程序等各種形式之資訊，且需定期檢視對隱私與公民自由的保護狀況，限制接受、保留、使用、傳播個人或可識別化個人之資訊。

美國各級政府機關得經私人實體同意後，得利用所接收的網路威脅指標，用以預防、調查或起訴下列違法行為：即將發生而可能造成死亡、重大人身傷害、重大經濟危害的威脅，威脅包括恐怖攻擊、大規模殺傷性武器；涉及嚴重暴力犯罪、詐欺、身份竊盜、間諜活動、通敵罪及竊取商業機密罪。另針對監控資訊系統部分，法案第4條授權私人實體得為網路安全目的監控自己或他人所有之資訊系統及資訊系統中儲存、處理或傳輸之資訊，並應用相關防禦措施來保護權利及資產，若屬其他私人實體或聯邦機關之資訊系統，需取得其他私人實體或聯邦機關之授權及代表人之書面同意。

參、小結

網路威脅的態樣隨著經濟活動發展和科技技術不斷變化和演進，故在擬訂應對措施時，須納入「適應性（adaptation）」概念，適應性指需要具體討論如何分配實質上的物質資源和經濟上資源，來保護組織內最有價值的智慧財產權和客戶資訊；提供成員和利害關係人相關資訊，讓他們關注網路威脅並能實踐可行的安全措施[15]。

就美國在訂定網路安全相關政策及規範之走向來看，充分及即時的資訊互享流通方能產出完善且強健的安全防護政策，惟其中牽涉到國家機密資訊、私部門智慧財產權和商業機密以及個人隱私和自由權利之保護議題。是以，從眾議院到參議院陸續所提出各版本的網路威脅資訊共享草案，均受有恐將產生大規模監控美國公民計畫之爭議，故至今尚未成功通過任一法案。惟資訊共享所帶來之正面效益和影響並未被否定，而究竟如何建構健全且可靠之機制，尚待各方團體與立法機關進行充分的溝同及討論，協同打造能安心活動之網路虛擬空間。

[1] Gramm Leach Bliley Act, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Aug.11, 2015).

[2]Paul Ferrillo, Weil, Gotshal & Manges LLP, *Cyber Security and Cyber Governance :Federal Regulation and Oversight*, http://corpgov.law.harvard.edu/2014/09/10/cyber-security-and-cyber-governance-federal-regulation-and-oversight-today-and-tomorrow/ (last visited Aug.11, 2015).

[3] PCI DSS, PCI Security Standard Council, https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0 (last visited Aug.11, 2015).

[4] Health Information Privacy, HHS.gov, http://www.hhs.gov/ocr/privacy/ (last visited Aug.11, 2015).

[5] Health IT Legislation, Health IT.gov, http://healthit.gov/policy-researchers-implementers/health-it-legislation (last visited Aug.11, 2015).

[6] Cybersecurity Laws& Regulations, Homeland Security, https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (last visited Aug.11, 2015).

[7] https://www.congress.gov/bill/114th-congress/senate-bill/754

[8] Text:754-114th Congress, Congress. Gov, http://www.natlawreview.com/article/senate-fails-to-include-cybersecurity-legislation-part-national-defense-authorizatio (last visited Aug.11, 2015).

[9] Sec.2(15).

[10] S.754- Cybersecurity Information Sharing Act of 2015 Summary, Congress. Gov, https://www.congress.gov/bill/114th-congress/senate-bill/754 (last visited Aug.11, 2015).

[11] Amy Davenport, *Senate is likely to consider cybersecurity legislation before August recess*, Capita; Thinking Blog, July.27, 2015, http://www.capitalthinkingblog.com/2015/07/senate-is-likely-to-consider-cybersecurity-legislation-before-august-recess/ (last visited Aug.11, 2015).

[12] Sec.2(6).

[13] Sec.2(7).

[14] 網路安全威脅（cybersecurity threat）指「不受憲法修正案第一條保護之行為、未經授權而利用資訊系統造成資訊系統或使資訊系統中儲存、處理或傳輸之資訊的安全性、可用性、機敏性或完整性之不利影響，但不包括任何僅違犯消費者條款或服務/消費者許可協議之行為」，參 Sec.2(5)。

[15]Paul et al., *supra* note 2, at 2.

上稿時間：2015年09月

推薦文章