

[← 返回列表](#)[← 上一篇](#)[下一篇 →](#)

雲端時代資料保險機制之解析

雲端時代資料保險機制之解析

科技法律研究所
2013年12月05日

壹、前言

資訊時代，資訊應用所帶來的風險幾乎無可迴避，且往往帶來莫大衝擊；尤其在網路應用普及之後，大量資料透過網路傳輸、流通而暴露於資訊安全的風險當中，縱有再有高層級的防護，也無法使資料受損或漏失的風險機率降至零，因此有論者以為，對於無法藉由資訊安全措施加以避免的「殘餘風險」(Residual Risk)，應由「保險機制」予以移轉。本研究特探討本議題，以呼應目前日益進展的保險產品發展趨勢。

此類的保險機制，一般稱為資料保險，專門填補網路應用所造成的風險，諸如網路安全(Network security)之欠缺所造成的損失，或者隱私(Privacy)被害所造成的損失。依據產業觀察者意見，此類保險產品的市場正有逐漸擴張的趨勢，尤其是對於健康照護服務(Health care)以及中小型的業者而言，此類保險對於風險管理服務可以發揮長足的作用，其能夠填補資料被害的通知成本、信用監控以及加強資料防護的成本[1]。

本文以雲端運算應用的興起為背景，觀察相應保險機制的演進及發展；以及其對於產業發展而言，為何被視為不可或缺的配套機制，進一步檢視我國推動資料保險的可行性與條件。

貳、資料保險機制的發展

一、資料保險的種類

用來填補資料受害之損害的保險，一般被稱為「資料保險」，尚可見以「網路保險」或「隱私保險」稱之。與其直接定義何謂「資料保險」，不如分析此保險的涵蓋範圍。此類保險早在十幾年前出現，當時其保險範圍，是填補資料被害所引發的損害賠償責任[2]。

財產保險可分成兩大類型，一類是一般的財產損害，即保險事故發生導致被保險人的財產減損或喪失，承保此類財產損失之保險，即英美法系所稱之「第一方保險」(First-party coverage)。另一類則是責任保險，即保險事故發生導致被保險人應負擔法律上責任或契約上損害賠償責任，承保因被保險人應負擔責任之財產損失，即所稱之「第三方保險」(Third-party coverage)。

在資料應用環境中，因資料受害導致損害大抵可依上述區分。當遭遇網路犯罪的損害、毀壞(Destroys)或是剝奪被保險人對於資料的使用權限，則屬於第一方財產損失。另一方面，當被保險人所保護、監管(Custody)或控制的第三人資料或資訊，遭遇網路犯罪損害、毀壞或竊取時，將使被保險人必須承受對第三方負擔損害賠償責任、並支付相關費用，此屬於第三方財產損失，例如入侵資訊系統而竊取信用卡資訊、受保護的個人資料、及銀行的帳戶號碼，又如妨礙有合法權限的第三人近用系統，以及違反法規所要求而未向第三人通知資料侵害等...[3]。

二、資料受害所致損害是否得請求保險賠償過往有很大爭議

傳統的財產保險，由於未指明承保因資料被害所致損失，往往會在被保險人因資料被害導致財產損失而請求保險賠償時，發生很大的爭議。主要的原因是，傳統的財產保險其設計原則，是以被保險人對於有形財產的「保險利益」作為「保險標的」，並以有形財產受損來估算保險損害，並未考量到資料等無形財產。因此，起因於資料或類似形態的程式、軟體之缺損所致的損害，是否可能在傳統財產的保險範圍內，頗有疑義，且司法實務上的意見相當分歧，茲整理如下。

(一) 有利於被保險人的實務見解

在America Guarantee & Liability Insurance Co. v. Ingram-Micro[4]中，Ingram-Micro因幾分鐘的電力中斷，導致電腦資產與資料的喪失而嚴重影響正常的業務運作，遂依業務中斷保險(Business-interruption insurance)請求保險賠償，但遭受保險公司拒絕，保險公司提起訴訟並宣稱承保範圍未包含電腦與其他資產。地方法院認為，被保險人客製軟體程式的喪失，構成「具體損害」，具體損害不限於電腦迴路的被有形損毀或傷害，也會包含無法近用(Loss of access)、無法使用(Loss of use)以及功能喪失。

另一案Lambrech & Associates, Inc. v. State Farm Lloyds[5]，保險公司認為電腦病毒感染所造成的損失，非有形損失，因而拒絕保險給付。法院認為，本案之電腦系統以及儲存的資料皆因病毒感染而毀壞、被置換(Replaced)，此種結果，等於電腦系統完全無法接收、發送或回復任何形態的資訊，而完全失去作為電腦系統的效用；因此未接受保險公司的主張。

近期一例為責任保險爭議。Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.[6]中，Retail Venture是DSW鞋子盤商，2005年時它的電腦系統遭駭客入侵，共有百萬筆的客戶資料遭不當下載且許多資料夾也被翻閱過。由於DSW向Nat'l Union購買商業竊盜險，在其承保項目中包括電腦與資金移轉詐欺(Computer & Fund transfer fraud coverage)，DSW遂向保險公司請求保險賠償，主張此次駭客入侵所造成的損失有530萬元之多，但保險公司拒絕給付賠償金。於是DSW對保險公司提起訴訟，地方法院認定保險公司應支付保險賠償，保險公司不服，提起上訴至巡迴法院，巡迴法院認為，條款規定雖是限於該損失是由保險事故「直接造成」(Resulting directly from)，但這不代表該保險事故必須是造成損失的「唯一」(Solely)與「立即」(Immediately)的原因[7]，因此維持地方法院的判決。

（二）有利於保險人的實務見解

在America Online, Inc. v. St. Paul Mercury Insurance Co.中，由於America Online (AOL) 所生產的網路接取軟體AOL 5.0據稱會毀壞用戶的電腦系統，因而被客戶訴訟求償，AOL依責任保險內容，轉而請求保險公司應替其進行訴訟防禦，遭保險公司拒絕。為此，AOL對保險公司提起訴訟，法院遂檢視保險契約中是否載明保險公司有進行訴訟防禦的義務。契約中將情境限於「有形」財產損失，法院解釋，從字義上一般不會認為電腦資料、軟體及系統是「有形」財產，因為有形財產應是指可以觸摸 (Be touched)，但電腦資料、軟體及系統無法被感官感知，因此是無形財產。此外契約中亦有「功能降低除外條款」，意即，不良品或者危險產品所造成的損害非有形，故被排除在承保範圍內。法院據此否認AOL的主張[8]。

三、「新」資料保險產品應運而生

從上述實務案例的觀察，作成不利於被保險人判決結果的法院，是直接認定電腦資料、軟體與系統為無形財產。反之，作成有利於被保險人判決結果的法院，是將「資料」（程式或軟體）與「電腦系統」合為觀之，而認定電腦系統為有形財產，把電腦系統無法發揮正常作用視為具體損害。即使判決結果可能有利於被保險人，但是解釋方式卻較為迂迴，也顯得被保險人相當艱辛。

參、外國資料保險機制之發展實例與推動

雲端運算發展日益普遍日後，可以透過網際網路提供資訊服務（例如儲存空間、應用程式等），「資料」已然不附載在特定或固定的載體（電腦系統）上。因應整體資訊應用形態的轉變，國內外市場上逐漸有相關資料保險產品推出的案例。

一、實例

第一個例子，MSPAlliance是一個資源管理服務業者暨認證聯盟，於2013年4月與保險經紀公司Lockton合作，設計「雲端暨管理服務」保險(Cloud and Managed Services Insurance)，讓其聯盟會員提供資訊服務時得以購買此保險；承保項目包括因網路攻擊、資料滅失或系統故障而導致應負擔損害賠償責任，以及因技術錯誤或無法作用 (Tech Errors & Omissions) 所導致的損害賠償責任，亦包含在內。至於被保險人的資格要求，則限定是聯盟會員，且必須通過Unified Certification Standard (UCS)驗證。事實上，要求被保險人取得一定的驗證，是保險風險管理很重要的一環。

第二個例子，雲端保險服務平台Cloudinsure於2013年2月宣布與保險經紀公司Lockton合作，擬設計適於雲端環境的隱私與安全責任保險方案。其保險產品內容主要在確保雲端服務提供者可履行在契約、或服務水準協議 (Service Level Agreements) 中的承諾，再者也能依據其客戶存放於雲端環境之資料的風險層級，給予金錢防護。

第三個例子，與前兩例不同，是針對一般的資訊服務使用者來設計。保險經紀公司達信 (Marsh) 於2012年6月針對雲端環境的企業使用者，開發新的保險方案CloudProtect。被保險人是採用雲端服務的中小型企業，承保項目包括：因雲端服務中斷所致的營運收入損失 (Loss of income)、因採購新的雲端服務提供者所產生的相關費用支出、因資料轉換至新的雲端服務所產生的相關費用支出。

二、政府的參與及投入推動

美國的國家技術標準局 (Institute of Standards and Technology, NIST) 在規劃新網路時代藍圖時，把持續促進資料「保險」 (Cyber Insurance)，列為關鍵的一角。從這個角度而言，保險不僅具有轉移風險與填補損害的功能，更具有正面積極的意義，可作為新興技術發展的後盾。對於NIST這樣的主張，美國保險人協會 (American Insurance Association) 也予以呼應，認為針對網路應用環境而持續開發各種保險產品，是勢在必行的方向。

（一）政策推導

美國證券交易委員會指引 (2011年)，建議公司若為因應資安風險而購買保險產品，應列入資訊揭露範圍。此被認為是間接鼓勵企業購買相關保險產品的具體措施之一。

（二）政府機關作為被保險人購買資料保險之例

美國有以政府機關名義購買資料相關保險之例，蒙大拿 (Montana State Government) 購買「網路資料安全保險」 (Cyber/Data Information Security Insurance)，為期一年 (2012年7月1日至2013年7月1日)，保險項目包括：資訊安全責任 (每次事故保險賠償上限200萬美元)、行政罰款 (每次事故保險賠償上限200萬美元)、損害通知支出 (每次事故保險賠償上限100萬美元)、網站媒體披露支出 (每次事故保險賠償上限200萬美元)、每次保險事故發生以200萬美元為總保險賠償限額。此案之保險業者為Beazley，保險經紀人為Alliant Insurance Services。值得特別注意的是，保險項目當中包含損害通知支出，此是呼應了美國相關法令要求業者必須於獲悉資安事件時踐行通知相關的資料主體。

資安事故的確實可能使政府機關蒙受莫大損失，美國南卡羅萊納州稅務局 (South Carolina Department of Revenue) 2012年發生攻擊事件，州政府花費約2000萬美元收拾殘局，其中1200萬美元用來作為市民身份被竊後的信用活動監控，其他則用來發送被害通知、安強化措施、及建立數位鑑識團隊、資安顧問。

肆、結論－我國推動相關資料保險機制可行性之總合評析

現階段我國相關保險市場的現況，為因應我國個人資料保護法的通過與正式實施，也有推出資料相關保險產品，目標客群為企業，以幫助企業因應個人資料可能產生對他人的損害賠償責任、及填補其他附帶損害為主要訴求。至於，針對業者 (被保險人) 因提供資訊服務過程中的資料被害、毀損滅失所導致營業損失 (營運中斷、負擔契約上損害賠償責任) 之損害填補，似尚未有相關保險產品推出。考其原因，是保險業者對於此種因無形財產 (資料) 所導致損害的保險賠償模式，尚未累積足夠的經驗，也缺乏相關精算數據的掌握，因而不敢貿然承作，另一方面，保險業者本身也擔憂無足夠資力因應大規模的保險事故。

對此現象，我國主責資訊服務產業推動的有關政府部門，也思及政府投入參與資料保險機制，例如推動以機關為被保險人而購買相關的資料保險，藉以活絡資料保險市場；此種構想，在法律層面並無疑義，此乃保險賠償與國家賠償機制雖有各自目的，但未有衝突[9]。然而，實際操作上，必須考量政府機關資訊系統是否能通過保險業者的保險風險查核、是否有足夠的預算足以支付保險費用、以及決策單位是否能有效與資訊業務單位溝通以評估購買此類保險的需求...等諸多問題。

事實上，我國相關資料保險市場要邁向成熟發展，尚待多方努力，除保險業者本身規劃並提出合適的保險產品之外，參酌國外經驗，保



險經紀公司也能扮演一定角色，可針對客戶需求量身訂作風險評鑑、研提最符合的保險方案，並藉客戶共同需求而匯聚保險風險共同團體。政府所扮演之角色，除直接以政策推導之外，尚能在若干條件齊備之後實際參與保險機制，其後續方向值得關注。

[1]Collin J. Hite, Top lawyers on trends and key strategies for the upcoming year the ever-changing scope of insurance law, Aspatore Feb. 2013.

[2]<http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover> (last visited at Oct. 24, 2013)

[3]Jack Montgomery, Cybercrime losses and insurance for property damage and third-party claims, Maine Bar Journal, Summer 2012, p. 159.

[4]Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299 (D. Ariz., April 19, 2000).

[5]Lambrech & Associates, Inc. v. State Farm Lloyds, 119 S.W.3d 16, 25 (Tex. App. 2003).

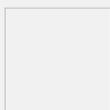
[6]Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 691 F.3d 821 (6th Cir. 2012).

[7]Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 691 F.3d 821 (6th Cir. 2012), p.13.

[8]America Online, Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459 - Dist. Court, ED Virginia 2002, P.461-462.

[9]請參考96年法務部法律字第0960003420號函。

本文為「經濟部產業技術司科技專案成果」



張乃文
主任 編譯整理

上稿時間：2013年12月

文章標籤



📄 推薦文章

👁 你 可 能 還 會 想 看

歐盟EDPB認為防範Cookie疲勞應確保資訊透明及簡化

歐盟資料保護委員會（European Data Protection Board, EDPB）於2023年12月13日回覆歐盟執行委員會（European Commission, EC）有關Cookie協議原則草案（Cookie Draft Pledge Principles）之諮詢。該草案旨在處理「Cookie疲勞」（Cookie fatigue）所造成的隱私權保護不周全之處。在電子通訊隱私指令（ePrivacy Directive）以及GDPR規範下，由於現行同意機制複雜，造成用戶對Cookie感到疲勞，進而放棄主張隱私偏好。為了避免「Cookie疲勞」，EDPB提出以下原則和建議，大致可以分為三點：一、簡化Cookie不必要的資訊 1.基本運作所需之Cookie（essential cookies）無需用戶同意，故不..

英國倫理機構針對海量資料（big data）之使用展開公眾諮詢調查

納菲爾德生物倫理理事會（Nuffield Council on Bioethics）成立於1991年，是一家英國的獨立慈善機構，致力於考察在生物與醫學領域新近研究發展中所可能牽涉的各項倫理議題。由該理事會所發表的報告極具影響力，往往成為官方在政策決策時之依據。有鑑於近年big data與個人生物和健康資料的分析使用，在生物醫學研究中引起廣泛的爭議討論，此間雖然不乏學者論理著述，但對社會層面的實質影響卻較少實證調查研究。Nuffield Council on Bioethics於日前發布一項為期三個月（2013/10/17~2014/01/10）的生物暨健康資料之連結使用公眾諮詢調查計畫（The linking and use of biological and..

美國聯邦通訊委員會修改廣播電視業者對於兒童觀看電視的保護義務

美國聯邦通訊委員會（The Federal Communications Commission /FCC）在2006年9月，修改並解釋2004年一項課與廣播電視業者對兒童觀看電視保護義務之指令。在2004年提出的指令中對廣播電視業者有許多規定，包括：電視業者被要求提供兒童適當比例基準之核心（core）教育及資訊節目，並於該類型節目中全程播放中標示E/I的符號；允許在節目中出現網站網址，但限制兒童節目中顯示非與節目相關以及有商業目的之網站網址；原兒童節目之

美國國防部5G戰略

因應5G通訊技術快速發展與關鍵應用逐漸普及之趨勢，美國國防部於2020年5月2日由部長批准「國防部5G戰略」(Department of Defense 5G Strategy, 以下簡稱5G戰略)；同月發布之公開版(unclassified)5G戰略，為美國軍方第一份公开发布的5G戰略性指導文件，主要內容包含指出國防部面對5G帶來的挑戰、設定5G技術發展目標、擬定5G發展行動計畫(lines of effort)等，以確保美國在軍事與經濟上的優勢地位。5G戰略指出，5G技術對於維持美國軍事與經濟優勢至關重要，為關鍵戰略性科技(critical strategic technology)。5G技術為產業與軍事帶來重大變革的契機，同時也帶來對資通安..

最 多 人 閱 讀

- 二次創作影片是否侵害著作權-以谷阿莫二次創作影片為例
- 美國聯邦法院有關Defend Trade Secrets Act的晚近見解與趨勢
- 何謂「監理沙盒」？
- 何謂專利權的「權利耗盡」原則？

▶ 隱私權聲明

▶ 徵才訊息

▶ 網站導覽

▶ 聯絡我們

▶ 資策會

▶ 相關連結

財團法人資訊工業策進會 統一編號：05076416

Copyright © 2016 STLI,III. All Rights Reserved.