東海大學法律研究所

碩士論文

指導教授 范姜真媺 博士

隱私權政策現況與展望

-以美國為中心

The Current Status and Future Prospects of Privacy Policy-Focusing on The United States

研究生：邱智偉

中華民國 108 年 1 月

東海大學
TUNGHAI UNIVERSITY
1955

碩士學位考試委員會審定書

東海大學法律學研究所

碩士班研究生 邱智偉 君所提之論文：

隱私權政策現況與展望-以美國為中心

經本委員會審查並舉行口試，認為符合碩士學位標準。

考試委員簽名處

劉定基

108 年 1 月 16 日

東海大學
TUNGHAI UNIVERSITY
1955

摘要

電子商務與網路科技的高度發展下，企業經營者為藉助網路科技拓展商務，利用網站消費者和使用者個人資料乃現代電子商務經營不可或缺之一環。然企業和消費者雙方資力不對等，如何有效保障個人資料屬各國政府面臨之難題。歐盟於 1995 年制定個人資料保護指令，目的在於因應資料電腦化時代的來臨。然 1995 年的指令到網路高度發展的時代已經不敷使用，因應而生的則是 2016 年一般性個人資料保護規則，個人資料保護規則不但補足指令的不足之處，更擴大保護範圍，對世界個人資料保護有深遠的影響。

有別於歐盟，美國並無全面性個人資料保護，為了保障美國本土個人資料，美國開始發展隱私權政策，透過美國政治和經濟的影響力，世界各國企業也紛紛效仿美國制定隱私權政策。然美國隱私權政策係因美國無全面性個人資料保護法為保障個人資料所發展而出，相對於我國已有個人資料保護法時，隱私權政策在我國法律效力為何？實質得關注，因私人企業大量使用隱私權政策作為保護個人資料的準則，若我國可以透過隱私權政策補足個人資料保護法之不足處，並結合消費者保護法和公平交易法，對於個人資料保護應能更加完善。

關鍵字：個人資料保護 隱私權政策 消費者保護法

目錄

第一章 緒論 1
第一節 研究動機與研究目的 1
第二節 研究範圍 1
第三節 研究方法 2
第一項 比較法分析法 2
第二項 文獻案例分析法 2
第四節 研究架構 2
第二章 個人資料保護各國立法介紹 3
第一節 歐盟個人資料保護 3
第一項 OECD 八大原則 3
第二項 歐盟 1995 年個人資料保護指令 6
第三項 歐盟 2016 年個人資料保護規則 8
第二節 美國個人資料保護 19
第一項 1974 年隱私權法案(The Privacy Act) 20
第二項 1999 年金融服務現代法(Financial Services Modernization Act) 22
第三項 消費者隱私保護草案(Consumer Privacy Bill of Rights Act) 23
第三節 我國個人資料保護法 27
第一項 個人資料保護憲法上基礎 27
第二項 我國立法沿革 29
第三項 2015 年新修正個資法要點 30
第三章 隱私權政策與個人資料保護法 34
第一節 隱私權政策 34
第一項 隱私權政策發展背景 34
第二項 美國隱私權政策執行概述 36
第二節 隱私權政策美國法上效力 38
第一項 隱私權政策契約說 39

第二項 隱私權政策非契約說.....42
第三項 小結.....48
第三節 歐盟對美國隱私權政策影響.....49
第一項 歐盟限制個人資料傳輸.....49
第二項 美國安全港協議(Safe Harbor Principles).....53
第三項 隱私盾(Privacy Shield).....55
第四項 小結.....57
第四章 隱私權政策在我國之法律適用.....60
第一節 公平交易法第二十五條與隱私權政策適用關係.....60
第一項 第 25 條構成要件與適用範圍.....60
第二項 實務執行.....63
第三項 小結.....66
第二節 隱私權政策和消費者保護法適用關係.....68
第一項 網路電子契約成立要件.....69
第二項 隱私權政策和定型化契約.....72
第三項 小結.....86
第三節 我國司法實務判決.....87
第一項 台北地方法院 102 年度北小字第 2182 號民事判決.....87
第二項 台北地方法院 97 年度北小字第 313 號民事判決.....91
第五章 結論與建議.....94
第一節 結論.....94
第二節 建議.....94
第一項 建立有效機制.....95
第二項 隱私權政策在台灣發展方向.....96
第三項 成立權責機關.....98
參考資料.....100

東海大學
TUNGHAI UNIVERSITY
1955

第一章 緒論

第一節 研究動機與研究目的

現今社會商業決策或行銷，資訊之利用乃不可或缺之一環，因此企業據有強烈動機蒐集個人資料，而在網路科技高度發展的現今社會，一但企業濫用其蒐集之個人資料所造成之傷害和後果都會比過去無網路時代嚴重許多。為保障個人資料，我國於 2010 年立法通過個人資料保護法。而其中第七條規範，公務機關和非公務機關個人資料之蒐集、處理和利用時，除法律有特別規定外，必須告知當事人並取得當事人同意。目前非公務機關告知當事人蒐集其個人資料常用方式為隱私權政策。隱私權政策(Privacy Policy)，係為公司對於個人資料保護陳述或者聲明，具體內容為企業如何蒐集當事人個人資料，以及其利用目的和蒐集後如何保存和保障個人資料之安全。

隱私權政策最早起源於美國，而後逐漸受到個國私人企業廣泛運用。私人企業利用隱私權政策作為蒐集、處理和利用個人資料的準則，然隱私權政策其法律性質為何？效力為何？在我國實務上探討甚少，目前實務判決僅有 7 篇判決有簡短論述，學說上討論亦屬少數，因此形成民間企業大量使用隱私權政策，但隱私權政策法律效力上卻不明確的現況。隱私權政策現況問題諸如有隱私權政策是否為契約？當事人應如何同意方據有效力？企業為反隱私權政策時，當事人如何進行救濟？政府機關或司法單位如何進行監管？上述問題如不加以釐清可能會造成私人企業在保障個人資料上產生漏洞，故實有討論空間。本文將就歐盟、美國和台灣隱私權政策執行現況和相關法規進行探討，用以釐清隱私權政策可能產生的問題，並嘗試提出解決之道。

第二節 研究範圍

本文之研究範圍僅針對我國、歐盟和美國與個資相關之法規、學說、

案例及實務見解做研究探討。

第三節 研究方法

本文主要以比較法、文獻分析與案例分析式探討研究。

第一項 比較法分析法

蒐集我國、美國與歐盟有關個資法之規定，將三者整理之後比較三個地區之差別與優缺點，藉以發現問題並提出討論，以做為我國個資法研究之參考。

第二項 文獻案例分析法

藉由文獻分析法蒐集台灣、美國和歐盟相關專書、學術論文、期刊、官方文獻資料等，並佐以網路上取得之官方組織、私人組織之公開文獻，豐富文章之內容後，加以統整分析。

第四節 研究架構

本文以美國、歐盟和我國個人資料法制、實務及學說關於隱私權政策之見解為中心，共分為五章：

第一章為緒論說明本文撰寫動機、目的、研究範圍、方法及架構。

第二章為各國個人資料保護相關法制、實務及學說，以及我國新修正個人資料保護法之問題與研究。

第三章為介紹美國關於隱私權政策的由來和隱私權政策在美國法律效力，以及歐盟對於美國隱私權政策的影響。

第四章透過公平交易法、消費者保護法、和法院實務判決，分別探討隱私權政策在我國法制下，性質和法律效力，以及政府可能扮演的角色。

第五章檢討我國法制對於隱私權政策規範不周的部分，以及提出相關可改進的建議。

第二章 個人資料保護各國立法介紹

第一節 歐盟個人資料保護

經濟合作暨發展組織(Organization for Economic Co-operation and Develop-ment,OECD 下稱 OECD)於 1980 年針對個人資料保護提出了綱要(The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)[1]，其中綱要的八大原則影響歐洲各國對於個人資料保護的法規制定和發展。而後歐盟於 1993 年成立後，更依據該八大原則制定 1995 年個人資料保護指令(Data Protection Directive, 95/46/EC)，故 OECD 八大原則對於歐盟個人資料保護的立法具有相當深遠的影響。以下本論文就個人資料保護之外國或國際組織相關法規作一介紹。

第一項 OECD 八大原則

OECD 於 1960 年代後期有鑒於電腦的使用率不斷的上升，尤其在自動化處理訊息部分，對於資料保護形成新型態的威脅，故在 1971 年的會議中提出兩份報告，一份為數位資訊與隱私權保護的問題(Digital information and the privacy problem)，該份報告提出了電腦使用率的上升對於資訊隱私權所帶來的問題，並於附件中附上了由 1970 年德國郝森邦(Hessen)所立的資訊保護法(Data Protection)提供給會員國參考[2]。於 1974 年針對於自動化處理訊息，與資訊跨國流動進行第一次在會議中進行討論。後於 1977 年針對於跨境資料傳輸與隱私權保護(Symposium on Transborder Data Flows and the Protection of Privacy)召開了一次重要的會議，受該會議結論影響，1980 年 OECD 針對於隱私權和個人資料保護提出隱私權保護綱要，該綱要包含八個基本原則適用各

[1] 參范姜真媺，他律與自律之共構個人資料保護法制-以日本有關民間法制為主，東吳法律學報第二十一卷第一期，2009 年 7 月，頁 166。

[2] OECD, 30 YEARS AFTER: THE IMPACT OF THE OECD PRIVACY GUIDELINES,2010,at 1。

國家的(national application)隱私權保護和因應國際傳輸(international application)的四大原則，提醒各會員國對於隱私權和個人資料保護的重要性，並希冀統一會員國對於隱私權和個人資料保護的歧異，進而保障各會員國人民之隱私權。[3]

OECD 提出的隱私權綱要雖不具有法律拘束性，惟揭示之八大基本原則對各國制定個人資料保護法之影響非常深遠，具有高度參考價值。

以下介紹 OECD 八大原則：[4]

1、資料的限制收集原則(Collection Limitation)：

個人資料的蒐集應有所限制，必須以公平、公正和合適的方法為之，且蒐集資料應徵得被蒐集人的同意或者應使被蒐集者知悉。

2、資料內容原則(Data Quality Principle)

個人資料的保存必須遵循其利用目的，且在利用目的之下必須確保個人資料的完整、正確性和最新性。

3、目的特定原則(Purpose Specification Principle)

蒐集資料的目的之不確定不可以晚於蒐集資料之時，後資料之利用不可以違背當初的蒐集目的，若蒐集的目的有所改變亦應有明確的規範。

4、利用限制原則(Use Limitation Principle)

非經過個人同意或者法律規定外，個人資料不得揭露、提供或者以其他方式利用於當初蒐集的目的之外。

[3] Id.at 2。

[4] OECD, THIRTY YEARS AFTER THE OECD PRIVACY GUIDELINES, 2011, at 21。

5、安全保護原則(Security Safeguards Principle)

個人資料需經過合理和妥善的安全保護，以避免造成其遺失、非法存取、銷毀、使用、竄改或者不當之揭露等安全上的風險。

6、公開原則(Openness Principle)

個人資料之蒐集、實施和政策應該有一個通用的公開政策。對於個人資料的存在、種類以及利用的目的、資料控制者的身分和住居所，應該建立一套簡易的查詢系統。

7、個人參加原則(Individual Participation Principle)

對於個人資料被蒐集者有下列之權利

(a)、個人資料主體得向資料管理者直接確認其是否擁有相關個人資料或者其他可得確認之方法。

(b)、對於查詢確認個人資料，資料控制者應該以當事人最容易理解的形式提供，在合理的時間內、少許的收費和合理的查詢方式。

(c)、若資料控制者拒絕個人資料主體依照第(1)和(2)之規定，查詢確認其個人資料時，應說明拒絕之理由，且對於拒絕理由個人資料主體可以提出異議。

(d)、個人資料主體得對其個人資料提出異議，若異議成立個人資料主體必須刪除、校正、修改與補充

8、責任原則(Accountability Principle)

資料控制者有責任遵守上述原則以及遵循上述原則完成必要管理措施。

上述隱私保護綱要對個人隱私權和個人資料自主權的保護，要求資訊控制者(擁有者)必須盡到告知和保護義務，並且讓個人資料主體有知悉其資訊受到蒐集，進而有權利確認、修改和監督其被蒐集之個人資料。1980 年提出的隱私權綱要為公務機關和非公務機關在蒐集個人隱私權和資料保護劃出了一條明確且可遵守的界線。

第二項 歐盟 1995 年個人資料保護指令

OECD 提出隱私權綱要如同前述並沒有法律上拘束效力，僅是給予會員國對於個人資料蒐集和跨國流動提供一般性準則。1993 年歐盟成立後，各會員國經濟合作交流頻繁，且電腦普及率越來越高。為了保障歐盟境內人民個人資料，歐盟於 1995 年訂立具有指標性個人資料保護指令(Data Protection Directive,95/46/EC)。指令提出重要個人資料保護原則，該原則分為兩大部分為資料控制者之義務及資料當事人權利[5]。

一、資料管理者義務

(一)資料品質原則[6]

個人資料保護指令明確要求各會員國在制定國內個人資料保護法時，蒐集目的應有正當理由，個人資料處理、利用不應違反當初蒐集目的，禁止目的外利用，並在個人資料當事人允許方式下進行保存。資料管理者應隨時更新正確資訊。

(二)資料處理合法原則[7]

個人資料必須符合特定目的下才能構被處理、利用，其中包括個人明確同

[5] 李仁淼，個人資料保護的理念與實踐，南區就業服務中心講習，2007 年 7 月，頁 8。
[6] Data Protection Directive 95/46/EC Article 6
[7] Data Protection Directive 95/46/EC Article 7

意、為履行契約所需要、為符合法定義務、為保護個人之重大利益、為維護公益或為合法之利益。

(三)敏感資料處理原則[8]

指令將種族、血統、政治傾向、宗教信仰、哲學信仰、工會會員資格、健康、性生活以及犯罪紀錄列為敏感性個資，只有在特定例外下方能蒐集、處理和利用。因敏感性個資涉及重大個人隱私權，應以保護為原則，蒐集、處理和利用為例外。

(四)告知當事人原則[9]

資料管理者在蒐集資料時應該告知資料當事人其蒐集目的、蒐集人的姓名或者住居地，蒐集後處理、利用的目的範圍，以及告知其蒐集資料編輯而成的檔案存放位置，供資料主體查詢更新。

二、資料當事人權利

(一)近用權

資料管理者應該給予資料當事人訪問查詢其資料。

(二)刪除權

資料管理者應該給予資料主體得糾正、更新或刪除不正確的資料。若資料曾給予第三方，當資料經過糾正、更新或刪除時，除告知是不可能或不符合比例原則，否則應該告知第三方。

(三)異議權

[8] Data Protection Directive 95/46/EC Article 8
[9] Data Protection Directive 95/46/EC Article10,18-21

當事人對於資料處理不符合特定目得反對資料管理者處理其資料；資料管理者將資料傳輸給第三人，資料當事人得反對該傳遞。

總結來說1995年個人資料保護指令依據OECD八大原則制定出一套完整個人資料保護，其制定內容深遠的影響世界各國個人資料保護法制。

第三項 歐盟2016年個人資料保護規則

OECD提出八大原則後，歐盟隨即著手訂立個人資料保護指令並在1995年公布，要求各會員國需在三年內針對上述指令國內法化，惟1995年個人資料保護指令訂立之時網際網路尚不發達，隨著近十年個人電腦、智慧型手機、電子終端器和感應設施等高科技產品的問世，以及網路的普及和社群網站興起，個人隨時可以透過其隨身電子終端裝置收發個人資料，而網路科技公司可以透過搜尋引擎，快速的蒐集個人資料並建置資料庫，再透過巨量數據(Big Data)的運算，分析個人的生活消費習慣、健康狀況、信用，將其集結成檔案(Profiling)，藉此探知商品潛在客群進行更直接的行銷(Direct Marketing)。

上述新型態之個資蒐集或利用已非1995年之個人資料保護指令所能規範，對個人資料保護已然不足。故而歐盟開始指令之修正，並在2012年提出了個人資料保護規則草案(2012 EU Proposal for General Data Protection Regulation)，目的除了使個人資料保護能符合於現今的時代之需求，亦也希望整合統一歐盟各會員國對個人資料保護法有較一致之程度，故本次修正將個人資料保護規範拉高到規則(Regulation)[10]層級。該草案經過個會員國四年的討論和意見整合，最終於2016年通過成為正式的個人資料保護規則(General Data Protection Regulation, GDPR)，已於2018年5月正式於歐盟境內實施。個人資料保護規則的訂立施行，有劃時代的意義，建構了資訊科技時代個資保護新

[10] 指令在歐盟的法律規範上只有要求各會員國需要達到的明定的目標但不要求各會員國達到目標的方法；規則有別於指令是直接適用於各會員國政府，權利義務直接歸屬於會員國國民。

的原則，實值得參考和借鏡。

個人資料保護規則(下稱 GDPR)更明確化了個人資料蒐集處理的要件保護之對象、範圍，亦加強當事人之權利，增加資料管理者和其受託者的義務。希望有效的釐清和解決在指令時代下的問題。本文以下就 GDPR 訂立修正分為四大部分進行說明。

一、確立個人資料保護規範對象和地域範圍

(一)規範的對象

歐盟 GDPR 將規範對象分為規範客體和適用主體這兩部分，其中規範客體依據 GDPR 係指「全部或部分以自動化方式蒐集、處理或利用的個人資料」，而非屬於自動化蒐集、處理、利用個人資料的部分以「構成檔案系統（filing system）一部分，或『為』構成檔案系統一部分而蒐集、處理或利用的個人資料」始有適用。[11]其因係避免打擊範圍過大，故對於非屬自動化蒐集、處理、利用個人資料且散在未構成檔案系統者，不適用本規則。而所謂檔案系統依據 GDRP 第 4 條第 6 款的定義為「可以特定條件存取的結構化個人資料集合，不論是集中、分散或以其他功能或地理因素散佈者」[12]，據此學者普遍認為若是個人資料屬於非自動化蒐集，且又為過於分散之紙本資料，如果無法用一般檢索可以得知時，該資料並不適用本規則。[13]

本次 GDPR 的修訂值得注意的是對於規範對象「為自然人、法人，公務機關構或其他組織(natural or legal person, public authority, agency or other body)[14]，並不以特定組織為規範對象。對於一般自然人的規範，於指令

[11] GDPR Article 2。
[12] GDPR Article 4。
[13] 參范姜真媺、劉定基、李寧修，「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告(編號：1050224)，行政院法務部，2017 年 3 月，頁 8。
[14] GDPR Article 4(7)&(8)。

時代一般自然人已經納入規範範圍，然因在於電子網路普遍發達的時代，一般人透過網路蒐尋即可獲得大量個人資料，再將資料予以儲存處理、利用，故將一般人納入規範而不是用組織型態作為規範主體，目的在於更周全的保護個人資料並免形成保護漏洞。指令對於自然人蒐集、處理、利用個人資料規定「純供個人或家庭活動」則不在規範的範圍內。但現今社群網路發達的年代所謂「純供個人或家庭活動」已經難以區分，據此歐盟在本次 GDPR 在草案本有增加「未獲得任何利益（without any gainful interest)」的要件，試圖限縮該例外之規定。惟「未獲任何利益」之條件最終還是被刪除。而歐盟在一讀通過的草案對於自然人純供個人或家庭活動若是屬於「公開」該個人或家庭活動之資料則是增加了「可合理預期僅得由數量有限之人存取」，目的是希望限縮該個人資料被他人存取的範圍，亦有督促一般人應該更重視維護自身隱私權，並且在使用社群軟體時應該積極利用隱私權功能維護自身和他人權益。然最終 GDPR 訂立後並未增加任何要件，而是在其立法理由加以宣示「個人或家庭活動」仍不得與職業或商業活動有關[15]。總結來說對於自然人的規範，GDPR 希望可以藉由增加要件來確保一般人在公開自己個人資料時，若其中又牽涉到他人個人資料時能夠注意並保護他人之隱私。不過由於區分的困難且為避免干涉人民的自由最終並未增加任何要件。

(二)規範的地域

個人資料保護指令對於規範的地域規定只有在歐盟境內設有設備(諸如電腦機房、資料儲存機房等)情形下方有適用該指令[16]，如此規定已經無法適應全球網路化下個資蒐集、處理或利用無國界的時代。為了應付此一狀況 GDPR 於規則第 3 條第 1 項 a 款規定「只要在歐盟境內提供商品或服務即受規範，無論當事

[15] GDPR Recital (18)。

[16] 參劉定基，雲端運算與個人資料保護–以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心，東海大學法學研究第 43 期，2014 年 8 月，頁 11-14。

人是否有付費。」b 款「在歐盟境內的行為進行監控。」[17]將過去指令採用之屬地主義，修正為只要對於歐盟境內人提供服務或商品，而蒐集個人資料，即便歐盟境內沒有任何廠房設備或者設立分公司子公司都有規則之適用。b 款所謂的監控，係指資料管理者或者受託者利用網路或者其他電子科技設備，對歐盟境內之人進行「追蹤」蒐集其個人資料，包括上網習慣、生活習性…等，而解釋上對於後面的剖析亦或者是大數據上的分析都應該包含在 b 款的規範內。

二、個人資料的定義之修正

在指令時代個人資料定義未趨完整明白，尤其在社群網路快速發展的現今，個人資料的定義需要有新的要件來定義以清楚界定其範圍，故本次規則針對個人資料定義增加了部分要件。

(一)明確化個人資料定義

所謂個人資料原指令之定義為「任何有關一個已識別或足資識別自然人的資料」[18]。此定義對於現今社群網路時代形成模糊地帶之存在，故規則增加新的個資定義「一個可以識別符號，例如：姓名、識別號碼、位置資料、線上識別碼或經由其他一項或多項身體、生理、基因、精神、經濟、文化或社會身分特徵，直接或間接識別特定自然人」。其中位置資料根據修正理由認為應該包含網路協定位置（internet protocol addresses,ip），小型文字檔案識別碼(cookies identifier)或其他識別碼。[19]

一般大眾在使用電腦設備或者智慧型手機連上網際網路時，必須先向網路提供業者取得一組 IP[20]，並利用該 IP 和終端機取得網路數據，在上網瀏覽網頁

[17] GDPR Article 3。
[18] Data Protection Directive 95/46/EC Article 2。
[19] 參范姜真媺、劉定基、李寧修，同前註 13，頁 12。
[20] 一般稱為 IP 地址，兩台電腦為了能夠在網際網路上相互傳遞訊息和溝通並且辨識彼此據此在連上網際網路之時會先給予一個代碼編號，類似電話號碼一樣。

或者影片…等任何指令行為都會有紀錄留存在電腦內或者是瀏覽器提供者的終端機內，此稱之為 cookie[21]。IP 位置和 cookies 紀錄是否為個人資料過去多有爭議，而本次修正直接將其定義為位置資料，屬個人資料。網路提供業者或者瀏覽器提供業者針對上述資料進行蒐集、處理、利用應受規則之適用，此要件之增加大幅提升網路隱私權之保障。

(二)去連結化和不可回復性

資料管理者或委託者於個人資料蒐集後，為了方便利用，均會將其進行處理後並儲存，為保障當事人個人資料安全，一般會使用電腦軟體將其匿名化去連結化，避免駭客入侵電腦時，一次性的取走資料庫所有的個人資料。如此之保護個人資料手段和方法，在指令上並未規範，而 GDPR 則新增保護要件，要求資料管理者和受託者於保存資料時應該符合當時科技水準避免資料外洩，其條文為「在不使用額外資料的情形下，無法將個人資料歸屬於特定個人的資料處理或利用方式；但該額外資料必須分別保管，並採取技術及組織上的措施，以避免個人資料被歸屬於一個已識別或足資識別的自然人」[22]，針對去連結化在規則第 25 條、第 32 條及第 40 條都有不同層次的規範，GDPR 希望透一連串的規範來達到以去連結化方式保障個人資料的安全[23]。

GDPR 針對於去連結化有明確層次性的規範，但對於去連結化後的個人資料，能否再進行回復，GDPR 則未有明確的規範，僅在立法理由上，針對於已經去連結化的資料，若已經達到無任何可能回復的情形下，則不適用 GDPR 的規定，故 GDPR 鼓勵資料管理者或者受託者盡量使用不可回復個人資料之意。

總結來說 GDPR 針對於資料管理者或者受託者課予相當高程度的規範，依利

[21] 指某些瀏覽器或者網站公司為了辨識用戶在網頁什麼執行指令而記錄在用戶終端機上的資料。
[22] GDPR Article 4(5)。
[23] 參范姜真媺、劉定基、李寧修，同前註 13，頁 14。

用層次化的規定，要求資料管理者或受託人需盡力保護其蒐集之資料，並針對已經去連結化之個人資料亦盡可能不將其在回復。透過事前的規範(去連結化)和事後個鼓勵(不可回復的個人資料不受到 GDPR 的規範)來保障個人資料的安全，降低其隱私權上的風險。

三、增加管理者資料處理和告知義務

(一)、資料管理者處理義務

個人資料從蒐集開始直到處理、利用為止，每一個步驟都有其被規範的之要件，GDPR 對此分為兩大部分規定:

1.一般資料

一般的個人資料處理要件，其中最重要的即是當事人同意，係以當事人接受告知後在自由意願下允許被蒐集、處理和利用，而 GDPR 則將上述該規定增加了「明確或清楚、積極的行為之要件。」據此學者認為此要件的增加，明確的否定以默示的同意做為同意的要件。GDRP 的同意不以書面為必要，只需要有明確的表達，不問以口頭或者電子表單都可以認定為同意之方式。若當事人對於該同意有爭執，原則上資料管理者或者受託者負舉證責任。當事人得隨時隨地的撤回該同意，同意一經撤回除非有其他法定要件，否則資料管理者或者受託人應該立即停止使用該個人資料。

除了上述的要件外，歐盟工作小組(Working party)[24]特別重視同意的自由性，尤其現今經濟活動常大量蒐集個人資料以為利用者，多是為企業法人或者是政府部門，相對一般民眾係處於弱勢地位，往往拒絕自己的個人資料時，企

[24] 歐盟個人資料保護工作小組係依據歐盟個人資料保護指令第 29 條所成立，目的在於統一解釋個人資料保護指令，並且統一各會員國對於個人資料保護之意見。該小組會不定期針對個人資料保護提供意見，解答民眾或企業的問題。http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (最後瀏覽日：2018 年 03 月 26 日)

業法人或者政府部門則拒絕提供相關之商品服務。歐盟工作小組認為這樣不對等的關係下，同意應屬有瑕疵，不過最終在 GDRP 並沒有修訂相關的規定；學者認為這個問題的解決已在立法理由的內涵中具體呈現。故雖沒有正式條文規定，但從其立法理由中還是可以推知在不對等關係下的「同意」，應該無法認為合法蒐集、處理和利用[25]。

總結來說，GDPR 針對於「同意」個人資料被蒐集、處理和利用部分增加了要件，避免當事人的個人資料被蒐集和濫用，尤其是現今個人資料保護的意識抬頭，企業法人或者政府部門為了避免觸法，往往利用不對等的關係或者概括同意，來取得使用當事人個人資料的同意，如此對於個人資料自主權明顯造成侵害，GDPR 依立法理由揭示「瑕疵同意」的內涵實在值得贊同。

2.特種資料(special categories of personal data)

特種資料有別於一般個人資料係，指個人之醫療紀錄、政治傾向、宗教信仰、性傾向…等較私密且敏感之資料。針對於特種資料原在指令中即與一般個人資料蒐集、處理、利用區分而有特別規定，而 GDPR 亦延續這樣的規範。特種資料處理僅在符合 GDPR 第 9 條第 2 項之規範下才能進行處理，其要件仍為當事人同意、法規命令下允許資料管理者或者受託人處理、公益原則(諸如醫療、為保護當事人所必要…等)、司法審判上所需要、當事人已經為完整公開[26]。而針對於當事人同意部分，若法令規範明確排除當事人同意並禁止處理時，該同意不能構成處理個人資料之要件。至於法令規範也必須符合手段與目的關聯，並非恣意立法即可。總結來說 GDPR 特種資料處理所要求之要件較嚴格，希冀透過事前的規範來保護特種個人資料，以防止特種資料遭受到不正當的濫用[27]。

[25] 參范姜真媺、劉定基、李寧修，同前註 13，頁 15-22。
[26] GDPR Article 9(2)。
[27] 參范姜真媺、劉定基、李寧修，同前註 13，頁 22-27。

(二)、資料管理者告知義務

1.告知義務

資料管理者在進行蒐集、處理和利用個人資料時，須告知資料當事人，告知方法並沒有限制，但應以清楚明瞭的方式和淺顯易懂的文字，且若資料當事人對於資料管理者擁有其個人資料，得要求資料管理者提供給予檢視，但對於資料當事人明顯且無理由的濫權請求時，資料管理者得收取合理費用或者拒絕之[28]。

其次，資料管理者若是間接蒐集資料當事人個人資料，GDPR 亦設有特別規定，間接資料蒐集者仍必須告知資料當事人，資料蒐集者名稱、聯絡方式、資料當事人可行使之權利、蒐集目的、資料管理者是否會向第三人傳遞等資訊。

至於間接蒐集者應何時告知資料當事人，原指令並沒有明確規定，而 GDPR 則明確規範[29]，資料管理者於第一次取得個人資料第一個月內須告知，至遲須於第一次利用時應告知；若要向第三人揭露則須於向第三人揭露前告知。

惟考量告知成本、使用目的和公共利益，在符合 GDRP 第 14 條第 5 項[30]以下之規定，例外得不告知資料當事人：

(a)當事人已經知悉相關資訊；

(b)提供資料不具可能性（impossible）或將涉及不成比例的努力，特別是基於公益目的的檔案保存、科學或歷史研究目的或統計目的，或提供基本告知事項將嚴重影響資料蒐集、處理或利用目的的達成；

(c)資料管理者係基於歐盟或會員國法律取得相關資料，且對資料當事人的

[28] GDPR Article 12。
[29] GDPR Article 13。
[30] GDPR Article 14。

合法利益有適當保障；

(d)基於歐盟或會員國法律所課予之職業上保密義務

2.個人資料外洩告知義務

資料管理者所擁有個人資料因故外洩，原指令中並沒有明確規範，而GDPR針對於個人資料外洩規範[31]，資料管理者必須在事件發生後72小時內告知監督機關，告知資料外洩損害範圍(諸如外洩資料種類、大概受影響人數等)以及補救方式，且告知內容包含聯絡窗口和資料保護專員聯絡方式。對於資料當事人，則應該立即告知，須告知損害情形、補救方式並留下聯絡方式，告知方法也必須使用簡單明瞭的方法和淺顯易懂的文字。

資料管理者有例外情事時[32]得不告知資料當事人，例如，外洩之個人資料已有採取適當之保密措施，他人無法從外洩資料得知資料內容；資料管理者事後採取措施不會導致當事人個人自由或者權力受損；告知付出和受損情形不成比例，此時資料管理者可以選擇以公告方式或其他類似之方式告知。

對上述之情形，監督機關掌握最後審查權力[33]，當資料外洩時監督機關認為有必要告知當事人時，或認為資料管理者不符合例外情事，則得命資料管理者告知當事人以確保資料當事人權益不會遭受到損失。

3.個人資料評估(data protection impact assessment)

資料管理者在針對特別類型之資料進行蒐集、處理和利用，尤其是使用新興科技之資料管理者，應對該個人資料保護進行風險上評估，所謂特種資料諸如大眾場所監視器監控。大規模的蒐集、處理和利用特種個人資料；大量蒐集

31 GDPR Article 33(1)。
32 GDPR Article 34(3)。
33 參范姜真媺、劉定基、李寧修，同前註13，頁34-40。

自然人的活動數據(lifelog)，進行個人剖析等，此類資料因影響人權甚劇，故在蒐集前應該對於保護風險進行評估，以利保障人權。至於評估方法以下所述規範為標準[34]

(a)對預計進行的蒐集、處理或利用活動及其目的的為系統性描述。

(b)蒐集、處理或利用活動所達成目的之必要性與比例性的評估。

(c)對於當事人自由與權利造成風險之評估。

(d)回應風險所預計採取的措施，包括保護措施、安全措施，以及考量資料當事人與其他關係人權利與合法利益，確保個人資料保護與符合本規則要求所採取的機制。

四、當事人權利

GDPR 的當事人權利除指令上原有之接觸權、更正權、刪除權和反對權外，本次 GDPR 更將被遺忘權的內涵入加入第 17 條，確立資料當事人之被遺忘權。

(一)近用權：GDPR 第 15 條規範當事人有隨時請求查詢自己資料權力，有別於指令的規定 GDPR 更進一步規定，如果資料傳遞至第三國或者國際組織，當事人有權知道其保護資料的安全措施為何？以及其他相關的權利(諸如刪除權、更正權)的教示資訊。

(二)更正權：GDPR 第 16 條規定當事人有權利針對不正確的資訊予以更正，除非符合例外之規定，例如學術、歷史研究或者公益之目的。與指令的規定比較，並沒有太大之差別。

(三)刪除權：當事人對於個人資料的不正確、不完整或者違反個人資料保

[34] GDPR Article 35。

護指令之利用時，當事人得主張刪除權，該權利在指令上原即有明確規定，不過當時網際網路並不發達且沒有社群網路和智慧型手機。因此指令的規範無法因應現在網際網路發達之下保護個資之所需。

本次 GDRP 的訂立，將刪除權作大幅度的調整，部分主因來自於 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González 案[35]。所謂被遺忘的權利，係指在數位化的時代，人們對於已在網路上流傳之資料應該有不再被揭露被世人遺忘的權利，性質上屬於資訊自主權一環，但學者認為[36]，被遺忘的權利，其用詞雖然醒目易懂，但是確不能夠精準表達該權利的主要內涵。本次 GDRP 刪除被遺忘的權利修正為「刪除權(the right to erasure)」，將舊有的刪除權進行更細緻的規定。

其主要內容規定在 GDRP 第 17 條，將舊有的刪除權加入停止擴散權；當事人對於資料資料蒐集者於符合下列要件者有權利請求刪除(a)就原蒐集資料目的和處理目的已經無保留必要者。(b)對於該個人資料之蒐集係依據第 6 條(1)(a)之同意，或超過其所同意之保存期限或處理個人資料之法律依據已不存在者；(c)資料當事人依第 19 條，對資料管理人基於第 6 條為保護其重大利益或公共利益遂行其業務而有必要處理其個資之行為，提出異議者；(d)違反本規則處理個資者。但為了避免請求刪除權被濫用，造成當事人能藉由刪除不利於自己的資料而編造自己的歷史，本條 3 則設有例外規定，(a)為表現自由之實現；(b)在公共衛生領域為公共利益之理由；(c)為歷史上、統計上及科學研究上之目

[35] 本案係由 2011 年西班牙一名叫做 Mario Costeja González 的人告上法院要求當地報章刪除一篇 16 年前有關他陷入財政危機、物業因沒繳稅而被拍賣的報道。Mario Costeja González 雖已還清了債務，但這篇報道的內容、關鍵詞及他的名字仍可以在 Google 中搜索。Mario Costeja González 認為事件有損他的名聲，希望透過法律保護個人隱私。最初西班牙法院以言論自由駁回 Mario Costeja González 的請求，但在 2014 年歐盟法院認為 Google 確實有侵害 Mario Costeja González 的基本權利故有權要求刪除該項報導。

[36] 參范姜真媺，網路時代個人資料保護之強化-被遺忘之權利主張，興大法學第 19 期，2016 年 5 月，頁 68。

的；(d)依歐盟法規或會員國法律，有保有當事人個人資料義務者。且該加盟國法律為符合公共利益之目的，尊重個人資料保護權利本質，又與所追求之目的間符合比例原則；(e)因當事人對資料正確性有異議或為證據目的而應保留者，或為違法處理個資，因當事人對資料刪除提出異議，並請求以限制使用該當資料為替代手段時，得將該個人資料保留但不得近用及處理[37]。

綜上，保護規則第 17 條將原指令上之刪除權加入了停止擴散權，形成新的請求刪除權，藉此來落實被遺忘權利。然多數學者認為，請求刪除權最大的挑戰，乃在資料當事人主張刪除請求權時和其他利益(諸如言論自由、資訊自由等)產生衝突時，應該如何權衡和取捨[38]。

(四)異議權

GDRP 第 21 條賦予資料當事人異議權，GDRP 的異議權和指令原規定並無太大差異。而對於資料當事人如何行使異議權，GDRP 之規範較為完整，資料當事人只要利用明確的、可理解的形式，表達其異議，除非符合例外情形(諸如基於法令規定、公益上目的或處理上之正當性等)，資料管理者都應該立即停止利用個人資料。

上述為 GDPR 規範個人資料保護之內容，屬於統一性立法，交由行政機關執行，並不區分線上(online)和一般消費者，亦無對各個部門進行不同的規範，僅有細部執行規定授權給予行政機關作調整，與美國的立法截然不同。歐盟作為世界第一大經濟體系，因個人資料係為重要人力資源，個人資料保護制度的發展與走向對世界之影響自然不容忽視。

第二節 美國個人資料保護

[37] 參范姜真媺，同前註 36，頁 69。
[38] 參范姜真媺、劉定基、李寧修，同前註 13，頁 31。

有別於歐盟個人資料保護的立法模式，美國對於個人資料保護的立法模式係採「市場機制」,「政府管制」則為輔助。此係因美國貫徹資本主義之傳統，認為市場本身的機制，有如一個看不見的手，當市場充分運作下所有的供需都會達成平衡，若政府有太多的干涉將會使得市場失去平衡，因此政府應該只是輔助的角色而不是主導的角色。而歐洲經過第二次大戰，納粹德國利用個人資料鎖定特定種族或者團體進行人權得迫害，在這歷史教訓下歐洲各國深深明瞭個人資料保護政府立場的重要性，故造就了兩大經濟體對於個人資料保護完全迥異的立法態度。

美國所謂市場機制為主軸的規範模式，一般而言為信任市場交易機制故不做特別的管制，必要時再輔以產業自訂的自律規範，但若有特定領域濫用消費者的個人資料問題嚴重，造成個人隱私權保護的危機，政府則會針對該特定領域制定適用該領域的特別法，學者稱這種立法模式為「部門」[39]式立法，用來補足對隱私權保障不足之部分。有關公部門領域的法案以 1974 年隱私權法最為重要。以下本文將就 1974 年隱私權法、金融服務現代法以及在科技網路時代和消費者息息相關的消費者隱私草案進行介紹。

第一項 1974 年隱私權法案(The Privacy Act)

1970 年代，大型電腦由於儲存資料和程式應用的方便性，美國政府機關開始大量使用電腦處理各種事物。當時美國眾議院對於電腦儲存資料的便利性，考慮成立一個由聯邦管控的電腦資料銀行，以便利政府應用人民的個人資料，這樣的考量引起大多數人民的疑慮，而掀起大規模的抵制[40]。基於民眾的疑慮，在 1973 年美國衛生教育與福利委員會(The Health Education and

[39] 參翁清坤，論個人資料保護標準之全球化，東吳法律學報第 22 卷第 1 期，2010 年 3 月，頁 21-22。

[40] 參陳起行，資訊隱私權法理探討-以美國法為中心，政大法學評論第 64 期，2000 年 12 月，頁 322。

Welfare Committee,HEW)提出一份有關於電腦和隱私權相關報告(Computers and the Rights ofCitizens)，內容提及政府掌握個人資料越來越多，卻無準則和規範來約束，因此HEW建議政府應該管控自動化個人資料蒐集系統，並且提出了五大原則，(1)存在於系統中的個人資料不應該是高度的機密[41]。(2)個人資料當事人得查詢他們存在於政府的個人資料以及查詢被什麼人使用過[42]。(3)個人資料當事人應該能夠防止其個人資料被為目的外利用[43]。(4)資料當事人能更改其錯誤的個人資料[44]。(5)資料管理者應該預防個人資料被濫用[45]。而該份報告最終促成了1974年隱私權法的通過[46]。

1974年隱私權法規範對象主體為政府機構(agency)[47]，並不涉及私人，目的在於防止政府濫用個人資料侵害人權。保護的客體為個人記錄(record)，條文所稱記錄包含教育、財務交易、病史、犯罪或工作經歷，並且包含名字或足資識別數字、符號或其他識別特定的個人身份，例如手指或聲紋或照片[48]。隱私權法僅賦予政府機構在符合法規範下得以保持(maintain)[49]個人記錄。受到HEW報告所影響，隱私權法亦有目的限制使用原則[50]，資料保有機構不得為目的外利用和傳遞給予第三人，僅有在例外情形下能為目的外利用，其例外情形為[51](1)統計上目的時，得為目的外利用。(2)為保護美國總統時，各機構首長得訂立規則解除目的外利用之限制。另外若向第三人傳遞資料，除非經過當事人同

41 No personal-data record-keeping systems whose very existence issecret.
42 An individual must have access to records about him and how they are used.
43 Individuals must be able to prevent information collected for one purpose to be used for another purpose.
44 Individuals must be able to correct or amend their records.
45 Organizations must take reasonable precautions to prevent misuse
46 Lieutenant Colonel Evan M. Stone, The Invasion of Privacy Act: The Disclosure of My Information in Your Government File, 19 WIDENER L. REV. 345, 352 (2013)
47 5 U.S. Code § 552a(a)(1)
48 5 U.S. Code § 552a(a)(4)
49 maintain 包含對於資料的蒐集、維護、使用和傳遞而言，5 U.S. Code § 552a(a)(3)
50 5 U.S. Code § 552a(e)(1)
51 5 U.S. Code § 552a(k)

意或該資料經過加密無法直接識別當事人，方可例外向第三人揭露資訊[52]。

而隱私權法為保障資料當事人則賦予兩項權利：

(一)近用權[53]

個人資料當事人得請求閱覽自己存於政府機構中的個人資料，而政府機構對於當事人請求，應該允許並在當事人自己選擇的人陪同下，觀看閱覽其存於政府機構的個人資料，並可以授權陪同人員讓其和當事人討論什麼資料可以複印一份給予當事人。

(二)更正權[54]

個人資料當事人得向政府機構請求更正不正確、不相關、不正當或者不完整之個人資料，政府機構於收到請求10日內必須做出更正。惟若有相關規定得拒絕當事人該項請求時，政府機構得依該規定拒絕當事人更正之請求且附上理由，而當事人則得針對該拒絕要求審議救濟之。

第二項 1999年金融服務現代法(Financial Services Modernization Act)

金融服務現代法又稱為格雷姆-里奇-比利雷法(Gramm Leach Bliley Act,GLBA)，該法的訂立是因為當時大多數的金融銀行業均不遵守隱私權法，將消費者或者客戶非公開個人資料賣給予電話行銷業者，讓電話行銷業者得直接對民眾進行電話廣告，金融銀行業甚至配合電話行銷業者只要消費者口頭同意契約，在未經消費者同意下直接從其銀行戶頭進行扣款。據此美國民眾大聲疾呼要求有關當局應該立法管控這樣的亂象，該法經過激烈的討論後最終通過限

[52] 5 U.S. Code § 552a(b)
[53] 5 U.S. Code § 552a(d)(1)
[54] 5 U.S. Code § 552a(d)(2)

制金融銀行業使用消費者的非公開資料。

GLBA 規範對象為金融機構，金融機構係指該只要該機構有從事具有金融本質(Financial in nature)的主要、附隨(Incidental)或輔助(Complementary)業務就屬於該法規範之對象，採取實質認定而非形式上認定[55]。在隱私部分保護的客體則是消費者非公開的個人資料，其中包括：該資料是由消費者提供給金融機構、消費者在金融機構任何交易過程的資料或者由金融機構提供消費者服務所產生的資料、金融機構以其他方式取得消費者的資料[56]。

非公開個人資料原則上限制傳輸給予第三人，若金融機構要將非公開資料向第三人揭露，則必須履行告知義務方能夠向第三人揭露，而告知義務之內涵為[57](1)金融機構必須在消費者關係存續中，每年以書面告知客戶該金融機構隱私權政策。(2)讓消費者有選擇退出(opt-out)的權利。(3)對於接受資訊之第三人要再利用該資訊傳遞於他人時，仍必須符合上述兩項規定方得為之[58]。

GLBA 確立了金融機構對於消費者個人資料保護的架構，不過其採取選擇退出的方式遭受到很大的批評，主要原因在於銀行的告知並非所有消費者均能夠清楚明瞭，雖然法規上規定隱私權政策之告知須清楚明瞭，但每個消費者理解程度並不盡相同，隱私權政策所使用之文字是否能夠讓所有的消費者明瞭即有疑慮的，據此學者們認為若要讓消費者和企業站在平等的立場去決定其個人資料是否要向第三人揭露，選擇加入(opt-in)應該是比較好的方式。總結而言 GBLA 訂立雖有不足之處，但卻也成為開啟消費者個人資料保護的先驅。

第三項 消費者隱私保護草案(Consumer Privacy Bill of

[55] GLBA sec 103 (a)(1)
[56] GLBA sec 509(1)(A)
[57] GLBA sec 503(a)
[58] 參於知慶，論客戶資料在金融控股公司於共同行銷時應有之保護，國立臺北大學法學系研究所，碩士論文，2005 年 6 月，頁 82-83。

Rights Act)

消費者隱私權保護草案最早在 2012 年由歐巴馬政府發佈提出，目的在於彌補現行隱私權保護規範的不足。歐巴馬政府一直致力促進各種科技發展，且在人民對於此發展有疑慮時，適時的給與政策上的解釋或立法；正因為歐巴馬政府重視科技產業發展，其政府施政所面臨的問題大多都和網路隱私權有關，例如大數據、開放政府、雲端科技等新興科技發展，都無法擺脫、降低大多民眾對於網路隱私權的疑慮。為了保障人民的網路隱私權，歐巴馬政府於 2012 年提出該草案，而該草案勾勒出建構保護消費者隱私權的標準，其標準如下：

1.個人資料控制(Individual Control)：消費者對於企業組織蒐集什麼資料?以及如何使用?有權利可以行使和控制。

2.透明度(Transparency)：消費者有權利可以簡單的理解企業組織如何保障其資料隱私之安全。

3.查詢、閱覽權(Respect for Context)[59]：消費者有權利可以知道企業組織蒐集、使用以及揭露個人資料之方法是否符合當初提供資料之目的。

4.資料安全性(Security)：消費者有權利要求企業組織保障其資料之安全和負責任的處理。

5.資料接觸與正確性(Access and Accuracy)：消費者有權利簡單的接觸使用他們的個人資料，企業組織有責任維護資料的正確性。

6.特定目的蒐集(Focused Collection)：消費者有權利要求企業組織在合

[59] Context 在 2015 年白宮新版的白皮書有明確的定義為，資料蒐集者在處理資料之情況，而該情況的判斷標準有資料蒐集者和資料提供者的聯繫，其歷史對話或者客觀情況，蒐集資料者是否之道提供者的隱私偏好等情形判斷，簡單的來說資料蒐集者蒐集資訊應該符合特定目的，而特定目的的判斷需要透過各種客觀狀況、主觀互動和契約來判斷。

理的限度內蒐集和保存他們的資料。

7.相關法律責任(Accountability)：消費者有權利要求企業組織使用適當的方法處理他們的個人資料，並且符合消費者隱私權法案的規範[60]。

2012 年的消費者隱私權法案源自於 2010 年美國商務部網際網路政策任務推動小組(Department of Commerce Internet Policy Task Force)的一份商業隱私與物聯網經濟報告：一個平衡的政策架構(Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework)。這份報告提出了業界、學者對於現行法規下，對消費者網路個人資料保障的不足，以及模糊規範致業界容易觸法的問題。因此歐巴馬政府在 2012 年提出上開白皮書，目的在於補充現行法規不足外，更希望可以建構一個網路隱私權保障的框架。該份草案明確表達透過該法幫助企業決定當履行(可能包含處理、利用、保存)個人資料政策時，什麼是消費者沒有爭議的，什麼是消費者覺得受到侵犯的。並且提高美國在全球的競爭力，進而成為世界的先驅，領導世界確立網路個人隱私與物聯網平衡法規的架構。2012 報告並指出為什麼美國可以達成上述目標的四個原因

1.依據美國的公平資訊實踐原則，消費者隱私權利法案可以保障個人的權利，並統一企業對於個人資料的義務，非常適用於蓬勃發展的網路時代。

2.為考量多方利益所制定出具有執行力的施行辦法，詳細說明在特定環境下，消費者隱私權利法案的標準。

3.聯邦貿易委員會利用其權限來禁止不公平或詐欺的行為，以執行消費者資料隱私權利的相關法令。

[60] The White House,Big Data:Seizing Opportunities,Preserving Values, 2014.05, at 19-20

4.透過美國與其他國家對消費者隱私權保護執行經驗的交流、藉由各國的現行法規和強制的合作，皆能有效的減少資訊流通的阻礙[61]。

2012 的草案提出希望可以確立一個保護消費者隱私可行的架構，但本法案最終並未通過，而消費者隱私仍然有迫切保護的需要，白宮於 2015 年再度提出新版本的消費者隱私權保障草案，該草案大體上架構和 2012 年的相似，其不同之處在於該草案明確的定出每一個章節，每一個用詞的定義，以及美國聯邦貿易委員會(Federal Trade Commission,FTC)民事裁罰最高只能加總為 2500 萬美金。簡言之，2015 年的版本有別於 2012 年只提出概念性的規範，而更進一步提出細項的規定。

值得一提的是在 2012 年的草案中之安全港原則，目標在於平衡聯邦與地方洲的法律適用問題，但是具體上要如何實現，草案中僅有框架。而 2015 年則確定安全港原則的運作方式為許可制度，亦即受規範者對於消費者個人資料之處理利用，均須遵照本法案，且有義務說明如何實踐保護消費者個人資料，以符合上述的 7 大原則[62]，另提出隱私權政策向 FTC 申請許可，其經過 FTC 核准許可後，只要完全遵守該許可的守則，則地方洲政府不應對於受規範主體給予以裁罰[63]。從 2015 年草案的安全港原則可以了解，目前美國頃向民間團體企業先自行訂立範，再將規範的原則交由 FTC 做審核。不過本草案比較可惜的並未對國外傳輸定出規範，因網路並無國界，歐盟針對於國際傳輸有在 GDPR 加以規範[64]，但是美國並未針對這塊進行規範。綜上所知，美國政策傾向由民間團體先規草擬可行的守則，再由 FCT 做出許可，F 政府仍不打算強行介入規範，以保障商業自由。

---

61 The White House,Consumer Data Privacy In a Networked World:A Framework for Protecting Privacy And Promoting Innovation In the GlobalDigital Economy, 2012.02, at 7

62 Administraion Discussion Draft:Consumer Privacy Bill of Rights Act of 2015,2015.02, at17

63 Id

64 General Data Protection Regulation,Article 45.2(b)

本草案的提出一直在國會討論中，2016 年川普政府上台後，對於該草案並不感興趣，故該草案並無任何進展，直到 2018 年 GDPR 實施後，為了避免商業交易法律上問題，川普政府目前傾向提出新的消費者線上隱私權保障草案。

雖消費者隱私權保護草案最終沒有立法，但不難發現在科技快速發展的時代，過去領域式、部門式立法很容易造成緩不濟急保護不周的困境，因此美國對於消費者個人資料保護似乎有越來越趨向訂立專法，解決目前法規林立的現象[65]。

第三節 我國個人資料保護法

第一項 個人資料保護憲法上基礎

隱私權在我國憲法並未明文規定，而是經由歷年大法官解釋逐漸形成的概念，最後將其納為憲法第 22 條概括基本人權，其中最重要的解釋文有大法官釋字第 293 號、釋字第 585 號和釋字第 603 號，而 603 號的解釋提出了「資訊自決權」更是直接影響了我國個人資料保護的發展，本文將就這三號大法官解釋說明並探討我國個人資料保護憲法上的基礎。

一、司法院大法官第 293 號解釋

我國對於隱私權一詞最早出現在釋字 293 號理由書上，大法官解釋認為銀行法上要求銀行對於客戶交易往來資料進行保密屬於一種隱私權上的表現，銀行不應任意公開客戶之交易往來資料[66]。同時，陳瑞堂、張承韜、劉鐵錚三位

---

[65] Are US insurers ready for a national GDPR-style privacy law?，https://www.insurancebusinessmag.com/us/news/breaking-news/are-us-insurers-ready-for-a-national-gdprstyle-privacy-law-116809.aspx (最後瀏覽日：2018 年 11 月 25 日)

[66] 參釋字第 293 號理由書節錄：銀行法第四十八條第二項規定「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密」，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。

大法官的不同意見書亦也表達認為，銀行法要求銀行遵守的義務是保障人民隱私權的具體表現，該隱私權是屬於人格權的一種。而人格權本身為憲法所保障，因此保障人格權不受侵害，為人民應享有之基本權利，從而推論出隱私權亦受憲法所保障[67]。從上述大法官解釋理由書和不同意見書即可以明瞭大法官承認隱私權為我國憲法上的一種基本人權，但其具體範圍和權利之要件未有明確的揭示。

二、司法院大法官第 585 號解釋

隱私權於釋字 293 號解釋後，確認為人民基本權，但是其憲法基礎為何，釋字 293 號並未表明，直到了釋字 585 號方對隱私權做出完整解釋，釋字 585 號認為基於「人性尊嚴」、「個人主體性之維護」及「人格的發展完整」，人們應該享有其生活秘密空間有不受他人干擾之權利，此即為隱私權，且應受憲法第 22 條所保障。解釋理由書以上述三點理由認為隱私權雖非憲法明文所列舉之權利，但仍為概括基本人權之一而受到憲法保障。多數學者亦贊同此見解，學者通說認為憲法第 22 條為概括基本權，而憲法未列舉之權利要受憲法第 22 條所保障其基本要件應為(1)權利本質上需與國民主權、人性尊嚴或一般人格權保障息息相關。(2)權利保障需求上必須具備有普遍性。(3)從立憲者角度而言，該種權利若不予保障將有違自由民主憲政秩序與價值觀者[68]。而解釋理由書提出三點理由，確切的吻合憲法第 22 條保障基本人權之標準。

---

[67] 參陳瑞堂、張承韜、劉鐵錚不同意見書節錄：我國銀行法第四十八條第二項明定：「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密」。此項法律所規定保守銀行秘密之隱私權亦為人格權之一種，依民法第十八條第一項規定：「人格權受侵害時，得請求法院除去其侵害。」憲法對此雖無直接保障之規定，但依憲法第二十二條規定：「凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障。」第二十三條復明定「以上各條列舉之自由權利，除為防止妨礙他人自由，避免緊急危難，維持社會秩序或增進公共利益所必要者外，不得以法律限制之」。保護人格權不受侵害，為現代法治國家人民應享之權利，無妨害社會秩序、公共利益之可言，故此項權利自亦為憲法所保障，非有必要情形不得以法律限制之。

[68] 參李震山，多元、寬容與人權保障—以憲法未列舉權之保障為中心，元照出版社第 2 版，2007 年 9 月，頁 11。

三、司法院大法官第 603 號解釋

釋字 603 號背景係當時內政部在戶籍法第 8 條第 2 項和第 2 項增設，國民請領身分證時，應按捺指紋方得請領。此規定目的為「確認個人身分」、「辨識迷失民眾、路倒病患、失智老人及無名屍體」，並可防止身分證冒用。惟此一目的是否有為重大公益而限制人民基本權之必要？學者認有疑義，故由立法院立委向司法院大法官申請釋憲。

釋字 603 號解釋文則將隱私權的內涵作更進一步詳細的解釋，認為隱私權的內涵包含資訊隱私權和資訊自決權。所謂資訊隱私權係美國法上之用語，因個人資料具有私密性，本質上和隱私權保障密不可分，因此學者認為隱私有包含個人資料部分則為資訊隱私權，受到隱私權的保障[69]。資訊自決權則係針對於上述資訊隱私的部分，個人資料當事人有自主之權利決定是否要揭露？向誰揭露？揭露的方法、時間為何等。學者指出釋字 603 號明確了隱私權的內涵，將隱私權分為消極不讓人侵入干擾之權利和積極決定自我選擇之權利[70]。釋字 603 號對於資訊隱私權和資訊自決權，確實開創個人資料保護新的里程碑。

第二項 我國立法沿革

我國在現行個人資料保護法施行之前，定有電腦處理個人資料法保護法，該法於 1995 年 8 月 11 日公佈後至 2010 年 4 月 27 日，由個人資料保護法取代之。個人資料保護法於 2010 年 5 月 26 日正式公布，全文 56 條，並於 2012 年 10 月 1 日施行，其中第 6 條和 54 條考量到爭議性和社會衝擊性較大，並未施行，至 2015 年再次進行修正後，於 2016 年 3 月 15 日施行。個資法雖在我國已修法施行，然因科技時代的快速演變，大數據、開放資料、互聯網…等新形態

[69] 參李震山，政府資訊公開法與資訊隱私權保障，研考雙月刊第 31 卷 3 期，2007 年 6 月，頁 50-60。

[70] 參李震山，人性尊嚴及人權保障，元照出版第 4 版，2011 年 10 月，頁 207 以下。

個資蒐集、處理或利用行為不斷發展，現行個資法事實上仍有不足之處。

第三項 2015 年新修正個資法要點

一、個人病歷之保護

本次個資法修正，將原先特種資料隻種類中增加了病歷，並在蒐集、處理和利用等增加如下隻法定要件。

(一)、擴大安全維護之範圍

舊法第 27 條即有對於安全性維護的一般性規定，並授權給中央目的事業主管機關可以制定個人資料安全維護計畫，部分個人資料安全維護計畫即有規範個資之蒐集事前或事後都必需要有安全維護，故國發會個人資料保護專案辦公室認為第 6 條修正應為宣示性規定[71]。

(二)、增加去識別化要件

原第 6 條第 4 款僅有要求須經過一定程序後方能蒐集、處理、利用，新法明確要求對於特種資料之蒐集、處理或利用需經過去識別化，以保護資料主體人格權。

(三)、增加蒐集之法定要件

舊法對於資料管理者蒐集特種資料並沒有當事人同意之選項，惟依照大法官釋字 603 號解釋為尊重當事人對個人資料自主權，故增列當事人同意之規定。

[71] 參國發會個人資料保護專案辦公室，有關個人資料保護法第 6 條第 1 項但書第 2 款及第 5 款所定「事前或事後有適當安全維護措施」屬法定要件抑或注意規定？，
https://pipa.ndc.gov.tw/News_Content.aspx?n=7D3602579D2BF23F&sms=2F28806F8A42AE16&s=C92BC3676043F359 (最後瀏覽日：2019 年 01 月 22 日)

二、蒐集、處理和利用之法定要件之修正

(一)、蒐集之同意修正

舊法下資料當事人同意資料蒐集者蒐集其個人資料需用書面同意，其立法之用意在於希冀透過要式方法讓資料當事者獲得充足的說明或者更充分的思考，惟均須書面同意，在便利性上有不足，據此新法將刪減書面同意，僅要求個人資料蒐集者有充分的說明後，當事人明確同意即可。嗣後雙方針對於同亦有爭議之時，舉證責任則在於資料蒐集者一方。

(二)、非公務機關安全措施蒐集前之要求

舊法第 27 條對於非公務機關蒐集或處理資料時，必須採取一定安全措施，並在施行細則第 18 條明訂，安全措施應該如何實施。而本次修法第 19 條第 2 款新增，雙方在簽訂契約蒐集或處理個人資料時應已採取適當安全措施，從條文文義上看起來似乎將安全措施提前到蒐集資料以前就必須有一定安全措施之建置，有學者認為業者安全措施建置在第 27 條已經有明訂，第 19 條又重複訂立意義上並不明確[72]。本文以為新法增訂本款要件目的應該是希冀規範企業管理者在依契約蒐集個人資料之前，就已經採取完整的安全措施，而並非等到蒐集之後在加以保護，故仍有其修正上的意義。

(三)、免除當事人權益無侵害權益之要件增加

舊法下只有公務機關有本款適用，非公務機關並沒有該條款適用，而法務部修法說明舉例：如公司要求員工填寫緊急聯絡人時，因填寫人非當事人涉及蒐集第三人資料，此時只能以文件告知第三人同意徒增作業流程，故增設本款

[72] 參蘇柏毓，104 年個人資料保護修正簡評，科技法律透析，第 28 卷第 4 期，2016 年 4 月，第 13-17 頁。

[73]。

（四）、目的外利用要件修正

新法將公務機關目的外利用修正部分要件，對於公益條款增加「所必要」重申第 5 條必要性原則，而學術或者統計條款部分後段增加「經」蒐集者依其揭露方式無從識別特定之當事人。該要件修正法務部並沒有特別說明，從法務部過去函令解釋上看來法務部認為個人資料經過資料提供人處理後或資料蒐集者依其揭露方式已無從事別特定個人時，該資料則不屬於個資法保護之資料[74]。據此本款加上「經」應該係指資料管理者將蒐集之資料去識別化後就得為目的外利用。故學者認為法務這樣的修法並不妥適，可能會增加個人資料被濫用之風險[75]。

本次修法亦將非公務機關目的外利用大幅放寬，個資法第 20 條新增了第七款「有利於當事人」，並修正公益條款要件和學術統計條款要件。將公務機關和非公務機關目的外利用要件調整幾乎一模一樣。這樣的調整沒有考量非公務機關安全措施保護之能力，以及兩者之間本質上的不同，並不妥適。

（五）、免除告知義務的擴大

新法第 8 條將第 4 款告知將妨礙第三人重大利益，改成為告知妨礙「公共利益」，法務部說明認為提升為公共利益，比較能夠符合公益性，惟符合何種公益並沒有多加解釋。新法第 8 條新增第六款，資料管理者蒐集個人資料，只要非基於營利目的或者不會對當事人不利，則可免除告知義務，修正理由認為，為了避免增加蒐集成本，故只要目的不是用來營利，或者蒐集對當事人並沒有不利時，免除告知義務是比較符合社會運作成本。惟本款之新增，其目的只是

[73] 參法務部個人資料保護專區，http://pipa.moj.gov.tw/mp.asp?mp=1 (最後瀏覽日：2018 年 3 月 13 日)
[74] 參法務部法律字第 10103106010 號，中華民國 101 年 7 月 30 號。
[75] 參蘇柏毓，同前註 72，頁 13-17。

為了避免增加蒐集者的成本，卻未考量到資料被過度蒐集和浮濫使用之風險，並不妥適。

三、部分刑事責任之免除

新法修正第 41 條，資料管理者若非基於營利部分觸犯個資法者，原則上並不構成刑事犯罪；惟本條亦將部分告訴乃論之罪，全部轉換為非告訴乃論之罪，目的在於擴大法院處罰之範圍。這樣的修正是否可以有效嚇阻個人資料被不當蒐集、處理和利用仍有待觀察實務的運作。

第三章 隱私權政策與個人資料保護法

美國現行法並無針對個人資料保護有專法保護而係散見於各領域，分別立法保護，對於網路消費者個人資料保護目前並無法律上規範。而隨著網路科技進步，線上隱私權保障越來越受到重視，然美國政府並不打算利用強制力介入管理線上隱私權，希望企業自主規律保障消費者線上隱私權，因此隱私權政策便是在此背景被提出，做為保障企業對消費者個人資料蒐集、處理和利用之規範。本文下就隱私權政策發展經過、法律上效力以及歐盟對美國個人資料保護影響提出相關問題與討論。

第一節 隱私權政策

第一項 隱私權政策發展背景

隨著網路科技高度的發展，人們使用網路從桌上型電腦有線網路轉向隨時隨地都可以上網的無線網路，網路的使用幾乎成為每個人每天生活上所必須之行動。網站提供者多要求使用者必須先行註冊基本資料方提供後續服務，且在提供之時，均會存取記錄使用人之利用記錄，故網站服務提供者每天都大量的蒐集、處理和利用個人資料，對個人網路資訊隱私權有很大的威脅。

除了當事人自己提供給網站蒐集的個人資料外，網站可以透過各種網路科技運用，蒐集追蹤個人上網資訊，其範圍包含個人消費紀錄、上網記錄、信用交易紀錄等，透過收集、整理、分析後得以歸納出當事人一定之喜好，用於直接行銷。有鑑於此，美國社會注意到了網路隱私權的重要性，人民開始大聲呼籲政府主管機關和民間企業應該要注重網路個人資料隱私權，並且要求提出一

個可供解決問題的辦法[76]，網站上隱私權政策就在這樣的時代背景下被提出。

在探討隱私權政策之前，應該先了解美國對於電子商務發展與政府態度，美國政府對於網站隱私權關注始自於1997年柯林頓政府所提出「全球電子商業綱要(A Framework For Global Electronic Eommerce)」報告[77]，該報告討論出了五大原則和九大議題，其五大基本原則包括有：

1.私人企業應居領導地位：網際網路應該發展成自由導向的市場，不應該由政府任意介入，且政府應該鼓勵業者自律。

2.政府應避免對電子商業做不必要的限制：政府應該讓消費者可以自由的在網路世界裡活動買賣從事商業行為，政府應該避免制定不必要的法律規範。

3.政府參與市場目的在創造一個可預測的、最小化的、持續的及簡單的商業法律環境：政府介入電子商務發展是必要的，惟政府的介入，是為了確保一個公平競爭的環境，且避免有詐欺事情產生，促進爭議之解決，而避免以強硬之手段達到上述目的。

4.政府應該肯認網際網路的獨特性：網際網路的發展迅速來自於它向外分散的性質，現存的法律對於網際網路的管理並不合適，政府應該重新審視，必要時制定新的法律。

5.網際網路上電子商業的推動應該以全球為基礎：網際網路是全球的市場，買家賣家可能存在地球的任一地方，故制定法律應該是一致性且可預測，方能增加消費者信心。

而九大議題中第五議題則提出了網路隱私權的重要性，認為網路隱私的保

[76] Hetcher Steven, The FTC as Internet Norm Entrepreneur, VANDERBILT UNIVERSITY LAW SCHOOL PUBLIC LAW AND LEGAL THEORY RESEARCH PAPER SERIES, 53 Vand. L. Rev. 2041(2000),2041-2061

[77] 參戴豪君、常天榮、張雅雯，美國全球電子商業綱要與我國因應之道，資訊法律透析，1997年12月，頁18。

護可以讓消費者更願意進行電子商業行為，政府應該鼓勵民間企業訂出一套可解決爭議之方法。

從 1997 年的報告顯示，美國政府傾向由企業自律訂出一套規範，政府只做最後監管，並不任意干涉。於是 1990 年代末期各大網站開始著手制定自己的隱私權政策，但比例並不高。為了提高企業制定隱私權政策之意願，1998 年 FTC 警告民間企業，若其不制訂屬於自己的隱私權政策，將向國會建議訂立專法管制，這樣的警告起了很大的作用。加之，美國在 1998 年制定兒童線上隱私保障法(Children's Online Privacy Protection Act of. 1998,COPPA)，針對網站若要蒐集 13 歲以下兒童的個人資料，應先提供書面告知父母，其將蒐集兒童的資料，爭取父母同意。若未取得父母同意搜集兒童資料，FTC 會以違反聯邦貿易委員會法第五條，不公平或者詐欺商業行為進行處罰。

該法案通過後，美國民間企業為了避免更多相類似的法案通過，幾乎所有的網站都開始制定隱私權政策。美國學者 Steven Hetcher 在其研究報告[78]指出 1998 年兒童線上隱私保障法制定後，從 1998 年網站制定隱私權政策是 14%，到 2000 年隱私權政策制定有 88%來觀察，FTC 所釋出的警告是相當有效的。

第二項 美國隱私權政策執行概述

一、公平資訊實踐原則(Fair Information Practice Principles,FIPPs)

FTC 於 1998 年向國會提出網路隱私權報告，該報告指出對於個人資料之蒐集以及利用應該符合五大原則方能稱之為公平[79]。五大原則為：

[78] Hetcher Steven, super note76。

[79] Federal Trade Commission , Privacy Online: A Report to Congress,1998,

(一)告知原則(notice/awareness)

FTC 明確指出資料蒐集者應該告知資訊當事人，蒐集何種資訊、資訊的存放位置和標籤，資訊接觸者和潛在接觸者，以及如果拒絕被蒐集的後果。

告知方式應該是張貼在網站明顯位置，並且隨時隨地可以讓資訊當事人查閱，其文字應為淺顯易懂。

(二)選擇原則(choice/consent)

當資訊管理人已經為目的外利用，或欲揭露給第三人，必須讓當事人有選擇退出的權利。

(三)近用原則(access/participation)

資訊當事人得隨時隨地存取自己的個人資料，若有不正確資訊當事人也能要求進行修正甚至刪除個人資料。

(四)安全原則(integrity/security)

資料管理者應該確保資料的完整性和安全性，避免因不正當存取導致資料的滅失或者缺損，必要時應該用去識別化保存該個人資料。

(五)執行原則(Enforcement/Redress)

人們普遍認為應該有一個機制來保護隱私權，若無任何機制則公平資訊實踐原則只是建議而非規範性不具有約束力，而 FTC 認為業者自律可以當作隱私權保護的核心，政府機關在針對業者違反自律時應負之民事或者刑事責任進行立法即可。

---

https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf
(最後瀏覽日：2018 年 04 月 24 日)

二、美國企業自律現狀

FTC 於 1998 年向國會建議報告，對於美國國內企業自律推動有很大的幫助，雖美國國會最終並未對於電子商務進行立法，但各大企業為了避免政府的手伸進電子商務世界，紛紛成立隱私保護聯盟或者第三方認證標章，表明自己已進行保障消費者的個人資料隱私權[80]。其中比較有名的組織有 The Online Privacy Alliance(OPA)和 The Network Advertising Initiative(NAI)，第三方認證標章有 BBBonline 和 TRUSTe[81]。以 NAI 為例，該組織會針對加入組織企業成員發佈網路隱私權保障原則，要求成員訂立隱私權政策，並且讓 TRUSTe 擔任第三方監督者，由 TRUSTe 定期發佈監督結果以供組織成員改進[82]。

美國企業針對消費者的個人資料蒐集、處理和利用，透過發佈隱私權政策來施行並輔以第三方認證來進行監督，若有明確違反隱私權政策涉及到民事或者刑事法律時，則由 FTC 以其為不公平或者詐欺交易，進行裁罰，成為美國保障網路個人資料的最佳手段。

第二節 隱私權政策美國法上效力

美國法上明確規範蒐集個人資料須以隱私權政策告知個資當事人者，有(1)兒童線上隱私保護法(Children’s Online Privacy Protection Act of 1998,COPPA)(2)電子化政府法(E-Government Act of 2002,EGA)(3)金融服務現代法(Gramm Leach Bliley Act,GLBA)(4)健康保險可攜性暨責任法(Health

[80] Dennis D. Hirsch,The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?, Seattle University Law Review, Vol. 34, No. 2, (2011),439-480。

[81] TRUSTe 是 1997 年由電子先鋒基金會(Electronic Frontier Foundation)商業網路聯會(Commerce Net Consortium)所成立，針對於網路隱私權保障 Truste 發佈一系列準則，只要該企業遵守其發佈準則即可向其申請認證，而該認證組織於 2008 年從非營利組織轉為營利組織，積極的輔導其客戶保障網路隱私權，也針對於消費者投訴努力改變認證的標準。

[82] NAI 於 2008 年因為和 Truste 執法有認知上的差異，最終將執法權回歸於組織內部，學者 Hirsch 批評認為這樣的監管並非理想。

Insurance Portability and Accountability Act of 1996,HIPAA)。其中兒童線上隱私保護法和電子化政府法係直接規定適用於網路；金融服務現代法和健康保險可攜性暨責任法並非僅有規範網路而係虛擬實體一併適用，故學者稱前者為直接規範之聯邦立法；後者為間接規範之聯邦立法[83]。除了上述聯邦法外，美國洲法有加州線上隱私權保障法（California Online Privacy Protection Act of 2003)、加州產業與專業法（California's Business and Professions Code)、2002 年南卡羅來納州之家庭隱私保護法（Family Privacy ProtectionProtection Act)、2008 年康乃狄克州一般法(General Statutes)等，上述洲法乃補充聯邦法的不足，但整體而言美國並沒有專法明定隱私權政策的法律效力，故隱私權政策其法律上效力有兩說，第一說為隱私權政策為契約，就契約成立要件，以及適用法律進行相關討論。第二說則為隱私權政策非為契約，其法律適用上以 FTC 執法為主，學者稱為 FTC 隱私權法律體系（The Privacy Common Law of the FTC)。[84]下就兩者差異進行相關問題探討。

第一項 隱私權政策契約說

隱私權政策其定位為何？在美國學說上一直有極大的爭議，最早在 1999 年 Scott Killingsworth 在其 Minding Your Own Business: Privacy Policies in Principle and in Practice 文章中表達隱私權政策可以當作契約執行，只要企業明確的將條款告知到使用者，使用者接受後即可認定雙方成立契約。然隱私權政策為契約目前在美國實務上屬於少數說，主要原因在於認定契約成立要件有其困難性，一般而言契約之成立以雙方意思表示一致，無論是明示或者默示，雙方意思合致則契約成立，美國常見契約成立原則

[83] 參翁清坤，網路上隱私權政策之效力：以美國法為中心，台大法學論叢第 45 卷第 1 期，2016 年 03 月，頁 174。
[84] 參翁清坤，同前註 83，頁 178。

為「告知與同意」(notice and consent)原則[85]。但瀏覽各大網站，隱私權政策都是放在網站下方或者是網頁較不起眼之邊角，透過超連結到另一個網頁才能夠閱讀完整之條款，這樣的設計是否有達到公平資訊實踐原則中的「告知」實有疑義。縱使認為有達到告知而構成要約，消費者是否有表達承諾所示條款亦難證明，故隱私權政策是否能成立契約關鍵在於「告知」與「同意」。

在探討隱私權政策是否為契約之前，必須先理解電子商務契約的運作原理。電子商務契約一般都以網路包裹契約(web-wrap contract)[86]之形式表現，所謂網路包裹契約係指網站或者電子商務平台經營者和利用滑鼠點選使用者締結契約[87]。其表現方式有

一、點擊包裹契約(click-wrap agreement)：點擊包裹契約又稱點擊拘束契約，使用者在瀏覽網站、使用軟體程式亦或者填寫個資成為會員會時先彈跳出視窗表明契約條款後，讓消費者點擊「同意」之後方能繼續使用網站。有些網站甚至會設計消費者必須將條款拉到最底下後方能點擊同意。點擊包裹契約在美國法上並無太大爭議，主要在於它有明確告知的設計，消費者也必須點擊同意才能使用後續服務。美國法院認為上述點擊包裹契約進行方式，足以認定達成契約法定構成要件[88]。

二、瀏覽包裹契約(browse-wrap agreement)：瀏覽包裹契約又稱瀏覽拘束契約，使用者在使用網站或者下載安裝軟體，並不會有任何界面或者視窗彈出要求當事人閱讀相關條款。而是將契約條款放在網頁任一處，讓使用者點擊方能看到完整條款。故瀏覽包裹契約嚴格上來說並未達到契約所要求的「告知」

---

85 The United States President's Council of Advisors on Science and Technology(2014),Big Data and Privacy:A Technological Perspective 36,The White House,May 1.

86 參王至德，電子商務交易平台提供者之民事法律責任，國立高雄大學法律系研究所碩士論文，2010 年，頁 50。

87 參王碧瑩，線上電腦軟體按鍵契約與消費者保護法之探討，中原大學財經法律研究所碩士論文，2008 年，頁 41。

88 參翁清坤，同前註 83，頁 180-183。

和「同意」，惟美國實務認為在下列例外情形得承認瀏覽包裹契約有達成契約成立要件。

(一)使用者持續利用網頁

美國實務上認為，瀏覽包裹契約條款雖然以超連結方式呈現，只要使用者或消費者可以知悉(或者推定知悉)契約條款的存在，則例外可以構成「告知」，且若使用者或消費者持續進入網頁頁面進行使用，則得推定消費者或使用者有「默示同意」，契約成立[89]。甚至有美國法院認為消費者有時係直接透過使用產品訂立契約而非閱讀條款後訂立契約[90]。

(二)超連結文字較其他文字明顯，使用者仍繼續使用網頁

美國實務上認為，網頁的超連結若在使用者或消費者切換網頁過程中不斷的出現在所有的網頁中，並且該超連結文字相較於其他網頁文字明顯，使用者仍繼續使用該網頁時，應可以推斷使用者或消費者有接受到「通知」，並且繼續的使用有「默示的同意」存在，契約仍得成立[91]。

美國實務認為瀏覽包裹契約成立要基礎件在於「默示同意」的存在[92]，法院認為瀏覽包裹契約成立要檢驗三大步驟，第一契約條款是否有被充分告知使用者或者費者，第二消費者或使用者「同意」的給予是否有符合契約公平。最後契約條款有無違反法律的規定，例如選擇準據法、管轄權的決定或者仲裁條款的約定…等[93]。

綜上所述隱私權政策若要認定為，契約必須該條款有明確告知網站使用者

[89] Ticketmaster Corp. v. Tickets.com, Inc., 2003 WL 21406289, at *2.
[90] Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 981 (E.D. Cal. 2000).
[91] Hubbert v. Dell Corp., 835 N.E.2d 113 (Ill. App. Ct. 2005)
[92] 參翁清坤，同前註 83，頁 185。
[93] Ian Rambarran & Robert Hunt, Are Browse-Wrap Agreements All They Are Wrapped Up to Be?bepress Legal Series,2006, bepress Legal Series.Working Paper 1885.

或者個人資料當事人，而隱私權政策的同意方式若為點擊包裹契約，則較容易符合契約成立要件[94]；若隱私權政策係以瀏覽包裹契約方式呈現，因同意方式不如點擊包裹契約明確，此時契約成立必須符合上述美國法院要求的三大條件，方能以默示同意之方式成立。

第二項 隱私權政策非契約說

美國實務上將隱私權政策認定為契約事實上為少數，因隱私權政策為FTC主力推行之政策，目的用來解決網路個人資料被企業蒐集、處理和利用等問題。根據美國學者調查，隱私權政策過去執行十幾年間，幾乎沒有任何有意義的司法判決。故美國學者認為FTC對於隱私權政策影響力極為強大，甚至主導整個隱私權政策的發展，因此學者將FTC執法過程稱為FTC隱私權法律體系(The Privacy Common Law of the FTC)，並進行相關研究與探討其法律上效力[95]。

一、隱私權政策無適用契約法

一般認為隱私權政策無法以契約方式執行主要原因在於(1)、當事人無法明確證明自己的損失並進行索賠[96]。(2)、美國部分法院認為隱私權政策只是一般公司廣義政策的陳述，不能當作契約執行[97]。(3)、現行隱私權政

---

94 參翁清坤，同前註83，頁183-184。

95 Daniel J. &Hartzog, Woodrow, The FTC and the New Common Law of Privacy (August 15, 2013). 114 Columbia Law Review 583 (2014); GWU Legal Studies Research Paper No. 2013-120;

96 例如SmithvTrusted Universal Standards in Elec.Transactions，Inc.，No. 09-4567（RBK / KMW），2010 WL 1799456，於* 10（D.N.J.，2010年5月4日）（認為原告原則上可以根據隱私政策違約行為提起合同違約索賠，但由於原告未聲稱違約導致的任何損害賠償，因此授予被告的駁回動議）; Cherny訴移民銀行，604 F. Supp。 2d 605,609（S.D.N.Y. 2009）（裁定原告在收到垃圾郵件後被告在違反隱私政策的情況下披露其電子郵件地址未能產生可追償的損害賠償）;關於JetBlue Airways Corp.隱私Litig。，379 F. Supp。 2d 299,325-27（E.D.N.Y. 2005年）（由於原告沒有宣稱因違反而造成的任何損害，因此授予被告的駁回動議）; In re Am.Airlines，Inc.Privacy Litig。，370 F. Supp。 2d 552,567（N.D.Tex。2005）（以未能聲稱損害賠償為理由駁回原告的違約索賠）

97 Daniel J. Solove & Woodrow Hartzog,super note 95

策告知模式無法達成法定充份告知要件，且在瀏覽包裹模式下無法有效表達出使用者的同意[98]。(4)、隱私權政策的條款若有顯失公平或者違反程序規定，會導致條款無效[99]。

隱私權政策其條款之顯示看起來雖然像契約，但在實務處理，並無法以契約方式執行[100]，雖有學者認為可以改善隱私權政策顯示方式或者改變隱私權政策的模型，不過要徹底的讓隱私權政策符合契約規範要件還有一段努力的空間。由於美國法院普遍認為隱私權政策非為契約僅是公司一般政策性陳述，因此若企業違反隱私權政策時，一般民眾並無法依契約法規定主張權利。為解決這項困境美國實務上最終發展出FTC對隱私權政策的運作模式。

二、FTC對於隱私權政策的運作模式

(一)概述

FTC成立於1914年，最初目標在於確保商業環境的公平競爭，國會通過聯邦貿易委員會法(federal trade commission act)，後FTC成為反托拉斯最重要的組織機構。聯邦貿易委員會法第5條規範「不公平或欺罔行為或慣例」，解釋上應為可能誤導理性消費者致受損害之重要陳述、省略或慣例，和導致或可能導致消費者未能合理避免之重大損害、及該重大損害大於對於消費者或競爭所產生之對應的利益[101]。第5條成為FTC禁止商業不公平交易或詐欺最大的武器。

1995年在國會的督促下，FTC開始參與消費者隱私權上的問題，FTC對於

98 Ian Rambarran & Robert Hunt,super note 93
99 參翁清坤，同前註83，頁201-207。
100 Thomas B. Norton, The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model, 27 Fordham Intell. Prop. Media & Ent. L.J. 181(2016)
101 參翁清坤，同註83，頁213。

美國境內商業市場都抱持同一態度，企業應該自律，政府機關僅做最後的監督，國會立法係最後手段而非必要。秉持這樣信念 FTC 對於消費者隱私權保障係要求企業機關應訂立隱私權政策，而 FTC 確保隱私權政策的合理性和可信任性[102]。

FTC 由五位委員組織經由總統任命，參議院同意，其中一人總統任命為主席，任期為七年，除有違法和怠忽職守外，原則上不得隨意解職。FTC 掌握有調查、執法和訴訟權利，一般接獲消費者投訴 FTC 會先經調查，調查中如果確定被投訴的企業明顯違反法律，FTC 會決定給予行政處罰或者進行司法追訴[103]。企業接獲 FTC 的指控可以選擇在行政或司法追訴前，向 FTC 提交協議命令(consent order)的協議來解決 FTC 所提出的投訴。協議命令是美國法上常用的手段，目的在節省訴訟時間以及訴訟所帶來龐大的金錢和商譽的損失。協議命令在聯邦和州法效力細節上雖有所不同，但大致上並無太大的差異，均是雙方同意下自願提出協議，通常和法院命令具有相同效力，其中一方不遵守可以申請法院強制執行[104]。故 FTC 對於企業違反聯邦貿易委員法進行追訴，企業可以隨時向 FTC 提交協議命令，FTC 經審查後會公告三十天，讓大眾提供意見，若無任何疑義，雙方則會達成和解(Settlements)。公司大多選擇以和解結束和 FTC 的爭議，還有一個原因在於美國法院大多都會基於尊重，而採信行政機關調查報告，因此在企業在司法訴訟中並未有太大的勝訴機會，相較於司法訴訟企業大多都會選擇和 FTC 和解以解決兩者間的紛爭[105]。

FTC 的協議命令通常包含行政罰金、糾正企業活動或者禁止未來可能違法活動、以及 FTC 會要求企業持續進行報告和保留紀錄，甚至對於客戶隱私的維

---

102 Daniel J. Solove & Woodrow Hartzog,super note 95,at559-600

103 參 About the FTC，https://www.ftc.gov/about-ftc (最後瀏覽日：2018 年 04 月 28 日)

104 參 What is a consent order? The legal jargon free guide，https://amicable.io/what-is-a-consent-order/ (最後瀏覽日：2018 年 04 月 28 日)

105 Daniel J. Solove & Woodrow Hartzog,super note 95,at601

護，須於固定年份間交由第三分進行認證，用以證明企業已經達到協議命令保護隱私的要求。例如 FTC 和 PayPal 旗下的 Venom 的和解，就要求 Venom[106]必須向其用戶揭露隱私規則，並保障客戶金融訊息的隱私性、安全性和完整性，Venom 必須在十年間每兩年都經由第三方認證，其是否有達成協議命令的承諾[107]。最後 FTC 附註未來 Venom 每次違反其承諾則開罰 41,484 美金。

(二)FTC 針對於企業協議命令項目：

(1)禁止不當的行為(Prohibitions on Wrongful Activities)：協議命令的核心在於禁止不法的活動，企業對於現行的商業活動若被 FTC 宣告不法，企業除了須修正現行做法外，未來也不能再從事相關行為。例如被指控隱私權政策設計沒有充分告知當事人，未來公司不能使用相同設計。

(2)罰款或者其他金錢處罰(Fines and Other Monetary Penalties)：FTC 針對違法者會給予 1000 美金到 3500 萬美金的罰款、凍結資產或要求企業將不法所得退還給消費者。

(3)告知消費者和補救(Consumer Notification and Remediation)：FTC 會要求企業必須告知消費者其違反何種承諾，並且給予適當的補救措施。

(4)刪除數據或者不使用該數據(Deleting Data or Refraining from Using It)：FTC 會要求企業刪除用非法手段(wrongfully collected)或者利用引誘(inducement)所方式蒐集，個人資料。消費者即使有明確同意企業蒐集資訊，FTC 仍會令其刪除或禁止使用該資料。

---

[106] Venom 為 PalPal 旗下的一個行動支付服務，該服務宣稱使用者帳戶受到銀行級別的保護，並且保障使用者交易隱私性，但經過調查 Venom 並未達到其承諾，故 FTC 對 PalPay 進行追訴。

[107] 參 PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act，https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information (最後瀏覽日：2018 年 04 月 28 日)

(5)對不法的隱私權政策進行修正(Making Changes in Privacy Policies)：FTC 會要求企業修改不合法的隱私權政策，並且重新告知資訊當事人，若企業沒有完整的隱私權政策，FTC 會要求擬定新的隱私權政策。

(6)建立完整的全面性計畫(Establishing Comprehensive Programs)：FTC 會要求企業須建置一套完整的資訊隱私權保障計畫，計畫內容包含風險評估、訪問者的流量規模和可以達到的安全水準評估、人員教育訓練和安全責任…等[108]。計畫需要用書面方式呈現，甚至 FTC 要求企業該計畫需通過第三方評估其可行性[109]。

(7)獨立的專業人士評估(Assessments by Independent Professionals)：對違反規定的企業，FTC 會要求需要給獨立的專業人士評估，通常評估期為兩年，如果不同意這項要求，企業必須負擔可能違反協議命令的風險。Google 就會同意將其計畫交給第三方專業人員進行完整評估。

(8)紀錄保存和遵守定期報告(Recordkeeping and Compliance Reports)：FTC 會要求公司應該保存一定年限的紀錄以供檢查，並且針對後續進行之改進，亦應定期提交報告給予 FTC 以確定企業確實有遵守當初的協議。

(9)重大變更的告知(Notification of Material Changes Affecting Compliance)：針對於企業主體如果有重大變更可能影響當初使用者個人資料時，應該告知當事人。例如企業因為併購，將併入另一公司時，對於其保有個人資料當事人應該盡到告知義務[110]。

FTC 針對於違反隱私權政策企業所做成的協議命令大致上都有上述九項內

[108] In re Facebook, Inc., FTC File No. 092 3184, No. C-4365, at 5 (F.T.C. Nov. 29, 2011) (consent order); see also FTC v. EMC Mortg., No. 4:08-cv- 338, at 11 (E.D. Tex. Sept. 9, 2009) (decision & order)

[109] Google 在 2012 年便被要求開發新的管理方法解決消費者現有的隱私權風險，並且該計畫需要風險評估、培訓人員以及專人負責，計畫也需經過第三方定期評估和提交報告。

[110] Daniel J. Solove & Woodrow Hartzog,super note 95,at614-619

容，雖然每個公司不一定相同，但第一項和第二項以及第六項幾乎都會出現在協議命令上。有學者[111]認為從 FTC 發佈的協議命令來看可以認為 FTC 已自成一個法制體系，這個體系和一般普通法並無二致。

(三)違反隱私權政策之三大類型

(1)詐欺：一般係指公司違反自己的承諾、透過欺騙和引誘之方式讓消費者提供個人資料[112]、沒有適當或者充分的告知消費者，以及安全維護不夠確實，導致破壞當初隱私權政策的承諾[113]。

(2)不公平：有追朔更改[114]、利用間諜軟體取得個人資料、不正確的使用個人資料、不公平的設計[115]以及不公平的安全管理方式者，FTC 均認為屬違反不公平。

(3)違反安全港協定：歐盟於 1995 年發佈個人資料保護指令，限制歐盟境內公司將個人資料傳輸給第三國，為了符合該指令之規範，美國和歐盟於 2000 年簽定安全港協議，美國公司必要加入安全港機制才能夠接收歐盟傳遞之資料；而要加入安全港公司必須自我證明，其個人資料保護符合歐盟 7 大原則，並且向商務部提出保證。比較常見的做法是公司先取得第三方認證標章，例如

111 Daniel J. Solove & Woodrow Hartzog,super note 95,at583

112 在 FTC v Hill 案，FTC 指控 Hill 提供虛假的連結和宣稱，要求使用者提供個人資料給予該公司，這樣的釣魚網站便符合一般性欺騙。參閱 Complaint for Permanent Injunction and Other Equitable Relief at 10–11, FTCv. Hill, No. 03-5537 (S.D. Tex. Mar. 22, 2004)

113 PayPle 即為破壞當初和消費者約定安全性之承諾。參 The FTC settles with Venmo over a series of privacy and security violations，https://techcrunch.com/2018/02/27/the-ftc-settles-with-venmo-over-a-series-of-privacy-and-security-violations/ (最後瀏覽日：2018 年 04 月 28 日)

114 追朔更改通常指消費者同意隱私權政策後，公司變更隱私權政策確沒有告知消費者，並且實踐新的隱私權政策使消費者產生損害而言。參 In re Gateway Learning Corp., 138 F.T.C. 443, 470 (2004) [hereinafter Gateway Decision & Order] (decision & order) (agreeing to pay $4,608 to U.S. Treasury as disgorgement)

115 不公平的設計一般指軟體程式設計上無法讓消費者自由選擇使用或者移除而言。參 Complaint at 4, In re Sony BMG Music Entm't, FTC File No. 062 3019, No. C- 4195 (F.T.C. June 28, 2007) [hereinafter Sony BMG Complaint].

TRUSTe，然後申請加入安全港協議[116]。

美國企業加入安全港協議後就可以在其網頁宣告，而企業一旦違反當初安全港上對於個人資料保護的承諾，就會被 FTC 認定為詐欺而遭到追訴[117]。

FTC 認定企業違反隱私權政策標準程序為：(1)調查。(2)確認違法後進行追訴。(3)企業提協議命令希望和 FTC 達成和解。(4)協議命令經協議並公告，若無人反對或有公眾表達意見，經參考修改後和企業達成和解。(5)根據協議命令定期檢驗，一旦發現違反協議命令則依據協議命令進行處罰[118]。學者 Daniel J. Solove & Woodrow Hartzog 把上述這套模式稱作為 FTC 法律體系，並認為這樣的法律處理方式跟普通法應為一樣[119]。

第三項 小結

綜上得知 FTC 事實上為主導隱私權政策的機關，但是亦有學者[120]認為 FTC 的執行是沒有威脅力、軟弱的，因 FTC 僅能對於賦予其管轄權限之聯邦貿易委員會法或其他法律之違反事件而加以執，且由於 FTC 欠缺能自行制定隱私法令之權限，因此不受上開賦予 FTC 管轄權限之法律拘束之業者倘欠缺隱私權政策時，則將無權對之加以執行[121]。因此有些企業考量到風險和成本，可能會以移除隱私權政策方式來規避 FTC 的監管。

FTC 對於企業違反安全港協議，在 2009 年開始執行了一連串的行動，針對

---

116 安全港協議在 2015 年遭到歐盟法院判決違法，目前美國和歐盟採取新協議為隱私盾(privacy shield)。

117 Daniel J. Solove & Woodrow Hartzog,super note 95,at620

118 同意命令的罰款通常都一案一罰，所以原本根據聯邦貿易委員法最高罰款上限為 3500 萬美金但如果根據同意命令進行處罰下最高上限可以被突破，因此同意命令也成為 FTC 最好的處罰利器。

119 Daniel J. Solove & Woodrow Hartzog,super note 95,at676

120 James P. Nehf, discussing “FTC’s inadequacy and toothlessness in ensuring privacy protection,Recognizing the Societal Value in Information Privacy, 78 Wash. L. Rev. 1, 58 (2003)

121 翁清坤，同前註 83，頁 213。

於宣稱有符合安全港協議但違反其承諾的企業進行調查和追訴，該行為成功的迫使許多跨國企業修定個人資料保護原則以符合 FTC 的要求，如學者 Daniel J. Solove & Woodrow Hartzog[122]即表示 FTC 的行動迫使企業更遵守隱私權政策。然亦有學者如 Florencia Marotta-Wurgler and Daniel Svirsky[123]抽樣調查 2010 年到 2013 年和 2014 年到 2015 年間宣稱遵守安全港協議，以及對於個人資料安全保護技術的描述…等項目裡發現，FTC 的行動前和行動後並沒有太大的影響，FTC 的行動迫使企業用更含糊的標準來描述隱私權政策，以規避 FTC 的調查和處罰。最終學者 Florencia Marotta-Wurgler and Daniel Svirsky 結論認為 FTC 的安全港行動並沒有使企業更加遵守線上隱私權保護。

從 Florencia Marotta-Wurgler and Daniel Svirsky 文章，及調查數據中可以得知，FTC 雖然大力推行隱私權政策來保障使用者網路個人資料安全，但事實上並沒有發揮太大的效力，故美國政府若要保障人民線上個人資料，仍然需要建立全國性專法方能達到保護的目的。

第三節 歐盟對美國隱私權政策影響

第一項 歐盟限制個人資料傳輸

歐盟於 1995 年訂立個人資料保護指令，明確規定歐盟境內企業或公部門蒐集個人資料不應將該資料傳輸給第三國[124]，除非第三國有完整個人資料保護規範，完整個人資料保護規範包含需要有專責機關、專法以及個人資料保護安全相關機制…等。保護是否完善應由歐盟工作小組(Working Party)認定[125]。於

[122] Daniel J. Solove & Woodrow Hartzog,super note 95,at680

[123] Florencia Marotta-Wurgler and Daniel Svirsky,Do FTC Privacy Enforcement Actions Matter? Compliance Before and After US-EU Safe Harbor Agreement Actions https://www.ethz.ch/content/dam/ethz/special-interest/gess/law-n-economics/professor-for-intellectual-property-dam/Documents/wl-series-innovation/Marotta-Wurgler_1.pdf

[124] Data Protection Directive 95/46/EC Article 25

[125] Data Protection Directive 95/46/EC Article 29、30

2016 年新訂 GDPR 第 45 條有更加嚴苛之規定，新法並設立獨立監督有權對於跨境傳輸第三國是否符合法規範進行調查，甚至要求停止傳輸，加上第二章所述 GDPR 將適用地域擴大，因此 GDPR 的適用範圍和跨境傳輸的限制，強力影響美國企業對於個人資料蒐集、處理和利用。

例如 FaceBook 為了規避 GDPR 的規範，將用戶條款主體從愛爾蘭改變至美國[126]，並且停止和第三方數據[127]的合作關係，以避免觸犯 GDPR[128]。類似的情形如 YouTube[129]停止了和第三方數據合作的關係、Instagram[130]開放使用者可以打包個人數據給予自己的 mail…等。

GDPR 對於跨境傳輸事由學者[131]分為三點具備適足性認定，即符合 GDPR 第 45 條規定。具備適當防護。例外條款。下就境外傳輸規定分別介紹。

一、具備適足性認定

(一)個人資料保護規則第 45 條規範

1、個人資料移轉給第三國或國際組織，皆須經委員會判斷該第三國、領土

126 參為規避歐盟史上最嚴個資保護法，Facebook 將為 15 億用戶服務條款變更主體至美國，https://technews.tw/2018/04/24/facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law/ (最後瀏覽日：2018 年 04 月 29 日)

127 第三方數據所指係網路平台或手機應用程式等，例如許多網路平台入會方式可以用 FB 直接登入，不須另外填寫會員資料。

128 參防患未然！Facebook 停止與第三方數據公司合作，https://tw.news.yahoo.com/%E9%98%B2%E6%82%A3%E6%9C%AA%E7%84%B6-facebook%E5%81%9C%E6%AD%A2%E8%88%87%E7%AC%AC%E4%B8%89%E6%96%B9%E6%95%B8%E6%93%9A%E5%85%AC%E5%8F%B8%E5%90%88%E4%BD%9C-112005642.html (最後瀏覽日：2018 年 04 月 29 日)

129 參 YouTube 於 5 月停止支持第三方廣告服務，將啟用 GDPR 政策，http://www.ifuun.com/a2018041612102032/ (最後瀏覽日：2018 年 04 月 29 日)

130 參史上最嚴個資保護法下月上路，Facebook 家族如何打這場仗？，http://technews.tw/2018/04/26/instagram-data-download-tool-export-privacy-gdpr-compliance/ (最後瀏覽日：2018 年 04 月 29 日)

131 參林玫君，簡介歐盟一般資料保護規則(GDPR)之跨境傳輸例外條款，經貿法訊第 233 期，2018 年 5 月 25 日，頁 45-46。

或國際組織，是否具有充足的保護水準。這種移轉不需要任何特別授權[132]。

2、在評估保護水平是否足夠時，委員會應特別考慮到下列要素：

（a）法律，關於人權和基本自由的相關法規，包括公私部門關於公共安全、國防、國家安全和刑法以及政府當局存取個人資料之規定，以及對此類法規、資料保護規則、專業規則和安全措施之執行，包括在該國或國際組織中向其他第三國或國際組織移轉個人資料的法規、案例法，以及對被移轉的個人資料之資料主體，是否具備有效而可實施的主體權利，和行政與司法救濟[133]。

（b）第三國須具備一個或多個有效且獨立運作的主管機關，或有國際組織負責確保資料保護規則之執行，其須包括充分的執行權力，以協助和指導資料管理者行使其權力，並與會員國的主管機關合作[134]。

（c）有關該第三國或國際組織作出的國際承諾或具有法律約束力的公約或文書，以及其參與其他多邊或區域體系所產生的，特別是有關個人資料保護的義務[135]。

3、獨立主管機關

資料保護規則第 45.2 條 b 款要求第三國設立個資保護的獨立主管機關，究其原因，蓋個資保護機關若為一般行政機關而非一獨立機關，則與其他機關在階層上為同等，難以拘束他機關對個資的使用或保護。

個資為重要資源，影響人民權益重大，故不該有任何政治或經濟利益的干涉或介入，否則將無法維護個人資料保護法的基本原則，此機關須有代表各領域不同意見之人進入，故須為合議制機關，不得是獨任制機關，才能真正發揮

132 GDPR Article 45.1
133 GDPR Article 45.2(a)
134 GDPR Article 45.2(b)
135 GDPR Article 45.2(c)

個資保護機關的功能。

(二)適足性規定

上述歐盟個人資料保護規則第 45 條即明示了歐盟適足性定義，其中該條第 45.2 條 a 款列舉了委員會應審查之範圍，包括第三國之法規，關於人權及基本自由、私人企業或政府當局存取個人資料之相關立法、法規執行與救濟途徑。此外，資料保護規則第 45.2 條 b 款則要求第三國須具有有效且獨立運作的主管機關，以協助及指導資料保護規則之執行。第 45.2 條 c 款則要求檢視該第三國是否符合國際標準及其所簽訂之其他現行有效之多邊或區域體系中保護個人資料的條款之規定。

又，由於適足保護水準基本上沿用資料保護指令的判斷標準，故對於如何認定資料保護水準是否適足，乃是以資料之性質、資料處理之目的與期間、資料來源國及跨境傳輸之目的國、第三國現行有效之一般及特別法律規定、以及該第三國所採之專門法規與安全措施，並以個案方式綜合判斷該第三國或國際組織是否達到充足保護水準。

二、具備適當防護

資料接收國若經歐盟執委會認定其不具備 GDPR 第 45 條所稱之適足性，此時依 GDPR 第 46 條，資料接收方必須提供適當防護措施，方能接收歐盟境內個人資料，學說[136]依法條將其分為四種，(1)標準資料保護條款(standard data protection clauses)，資料控制者與處理者間簽訂歐盟執委會公布之標準資料保護條款。(2)企業拘束規則(binding corporate rules)，適用同一集團企業或合作進行經濟活動的不同集團內企業，且經主管機關核准的企業拘束。(3)行為守則(codes of conduct)，歐盟資料控制者或處理者採行行為準則，搭配第

[136] 參林玫君，同前註 131，頁 45。

三國之資料控制者或處理者具法律效力且可執行。(4)取得特定認證(certification)，歐盟資料控制者或處理者經過認證，搭配第三國之資料控制者或處理者具法律效力且可執行[137]。

三、例外條款

GDPR 第 49 條規定，當境外傳輸無法適用第 45 條和第 46 條情形時，仍允許部分例外情形，其為(1)當事人同意。(2)其他必要措施，例如公共利益、因執行契約所必要等。

第二項 美國安全港協議(Safe Harbor Principles)

歐盟法規限制境內公、私部門向第三國傳輸個人資料，故美國企業為了避免雙方貿易受損，由美國商務部和歐盟執委會進行談判，於 2000 年談定安全港協議，美國希冀其企業透過加入安全港協議，得不受歐盟個人資料保護指令拘束[138]。

一、安全港協議運作方式[139]

加入安全港協議之機構完全係基於自願性質，參加之機構必須公開宣示完全接受安全港之七項規範原則，每年以書面資料向商務部自我證明其確實遵循告知、選擇、取出、執行等原則，並陳述依附於隱私港原則之公開隱私政策聲明（published privacy policy statement），商務部將隨時更新參加組織名

137 參歐盟一般資料保護規，https://www.roc-taiwan.org/uploads/sites/124/2018/05/%E6%AD%90%E7%9B%9F%E4%B8%80%E8%88%AC%E8%B3%87%E6%96%99%E4%BF%9D%E8%AD%B7%E8%A6%8F%E7%AB%A0GDPR%E7%B0%A1%E4%BB%8B2.pdf (最後瀏覽：2018 年 10 月 29 日)

138 參行政院司法行政廳，個人資料保護法之研究，司法研究年報第 29 輯行政類第一篇，2012 年 12 月，頁 67-69。

139 參謝巧君，美國與歐盟安全港架構協議(The Safe Harbor Framework)，科技法律透析第 14 卷第 10 期，2002 年 10 月，頁 46-62。

單，並將參加機構名單及機構之自我證明信函內容公布。

為確保安全港之品質，機構可選擇(1)加入附屬於安全港之自我規範隱私計畫（self-regulatory privacy program）；(2)各自發展一套符合安全港之個別隱私規範；(3)表明係依據任何足以保護個人隱私之法律(statutory)、法規(regulatory)、行政命令(administrative)或其他判決(other body of law or rules)行事[140]。

二、安全港原則規定內容

美國商務部與歐盟執委會共同協商出安全港之原則，因其目的係為促進美國與歐盟間之貿易往來，故在徵求一般大眾及民間企業的意見後，納入非公務機關的自我認證與自我評估，以及公務機關之監督與干預的規定，構成歐盟2000/520/EC 決議附件 I 之安全港原則，其內容分為七大原則(1)告知(Notice)、(2)選擇(Choice)、(3)轉送(Transfers to Third Parties)、(4)近用(Access)、(5)安全(Security)、(6)資料完整(Data integrity)、(7)執行(Enforcement)。[141]。七大原則和歐盟指令並無不同，甚至可以說安全港原則是參考歐盟指令所制定。

三、安全港協議無效

歐盟法院在 2015 年 10 月 6 日做成，依據歐盟 2000/520/EC 決議制定的安全港協議，不具合法性之認定，因歐盟資料保護指令規定僅得將歐盟之個人資料傳輸至對個人資料有相當保護水準之第三國，歐盟執委會並作成 2000/520/EC 決議，以具體實施，法院認為如歐盟執委會欲實施 2000/520/EC

[140] 參什麼是安全港架構(Safe Harbor Framework)？，http://jackforsec.blogspot.tw/2011/05/q-safe-harbor-framework.html (最後瀏覽日：2018 年 04 月 30 日)

[141]參各國隱私法規與個資保護要求簡介，http://www.netadmin.com.tw/article_content.aspx?sn=1303110005&jump=2 (最後瀏覽日：2018 年 04 月 30 日)

決議應充分說明特定第三國國內法或者國際性承諾，已足確保歐盟法律要求之保障，易言之，歐盟執委會必須確定美國和歐盟執委會安全港協議，具有足夠之規範保障歐盟境內人民個人資料。然歐盟執委會並無法明確說明美國是否能確保歐盟傳輸個人資料安全，故 2000/520/EC 決議第 1 條違反個人資料保護指令。

且因 2000/520/EC 決議第 3 條第 1 項第 1 款之規定已事實上排除了歐盟會員國國內資料保護主管機關，得獨立檢視個人資料主體的基本權利以及其自由權是否有受到侵害的權力，使得該主管機關無法確保個人資料保護指令第 25 條的規定得到遵守。

綜上所述，歐盟法院認為 2000/520/EC 決議第 1 條和第 3 條第 1 項第 1 款，違反個人資料保護指，故 2000/520/EC 決議應為無效[142]。

第三項 隱私盾(Privacy Shield)

由於安全港原則的失效，美國商務部重新和歐盟執委會進行談判，事實上自 2009 年開始 FTC 每年都執行安全港行動，發現多數大型跨國企業都違反其隱私權政策和安全港宣告，歐盟法院的裁判正好給美國一個重新檢視消費者個人資料保護的問題，歐巴馬政府更希望透過立法來管理消費者個人資料，然如前所述消費者隱私草案提出至今並無任何進展[143]，而 2016 年川普政府對於科技法律並不感興趣，因此沒有意願針對現上消費者個人資料提出任合法案。故美國商務部和歐盟於 2016 年 10 月達成隱私盾協議[144]，隱私盾協議和安全港協議框

142 參林其樺，安全港判決後歐美個人資料國際傳輸趨勢觀察，科技法律透析第 28 卷第 2 期，2016 年 2 月，頁 23-26。

143 參 Reforming the U.S. Approach to Data Protection and Privacy，https://www.cfr.org/report/reforming-us-approach-data-protection (最後瀏覽日：2018 年 04 月 29 日)

144 參 Privacy Shield，https://www.privacyshield.gov/welcome (最後瀏覽日：2018 年 04 月 30 日)

架並無不同，其差別在於(1)歐盟允許個人資料傳輸到美國和儲存但美國政府必須保證不進行大規模的檢查和監控。(2)美國政府必須設立專員和專門機構處理歐盟個人資料相關問題。(3)美國必須接受歐盟人民投訴，而政府或企業須於一定時間內回覆。(4)歐盟法院可以對美國進行強制仲裁[145]。

歐盟工作小組針對於隱私盾在 2017 年發表評論，認為(1)相較於安全港協議隱私盾協議進步不少。(2)企業需要更明確的要求符合規定。(3)資料當事人應該被告知其受到隱私盾保護。(4)個人資料應該視為重要人力資源加以保護。(5)美國機構應該應該定期檢閱和調查企業合法性。最後歐盟認為美國應該立即解決的問題有(1)任命一名獨立監督員。(2)恢復隱私和公民自由監督委員會(Privacy and Civil Liberties Oversight Board, PCLOB)運作，任命新的委員。而這兩項任命應該在 GDPR 實施前為之[146]。雖歐盟工作小組提出改善建議，然川普政府並不打算理會，因此 GDPR 正式施行後，美國仍沒有改善工作小組所提出之缺失，直到 2018 年 6 月 12 日歐洲議會中公民自由，司法和內政委員會(Committee on Civil Liberties, Justice and Home Affairs)通過一項決議，決議內容為美國政府如果不於 2018 年 9 月 1 號改善缺失，議會將考慮暫停隱私盾之運作[147]。這項決議讓美國政府為了避免貿易上的問題最終妥協歐洲議會的決定。

目前川普政府已經任命一名監察員，以及三名 PCLOB 委員恢復 PCLOB 之運作，在 2018 年 10 月 19 日歐盟和美國針對隱私盾執行問題進行第二次討論，發

[145] 參 U.S., EU Reach Deal on New Data-Transfer Framework ，https://www.wsj.com/articles/u-s-eu-reach-deal-on-new-data-transfer-framework-1454429818 (最後瀏覽日：2018 年 04 月 30 日)

[146] 參 EU – U.S. Privacy Shield – First annual Joint Review， https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782 (最後瀏覽日：2018 年 04 月 30 日)

[147] 參 EU-US Privacy Shield data exchange deal: US must comply by 1 September, say MEPs ，http://www.europarl.europa.eu/news/en/press-room/20180611IPR05527/eu-us-privacy-shield-data-exchange-deal-us-must-comply-by-1-september-say-meps (最後瀏覽日：2018 年 12 月 05 日)

表共同聯合聲明，文中提到歐盟將會繼續和美國密切合作，確保隱私盾能夠發揮應有之作用[148]。

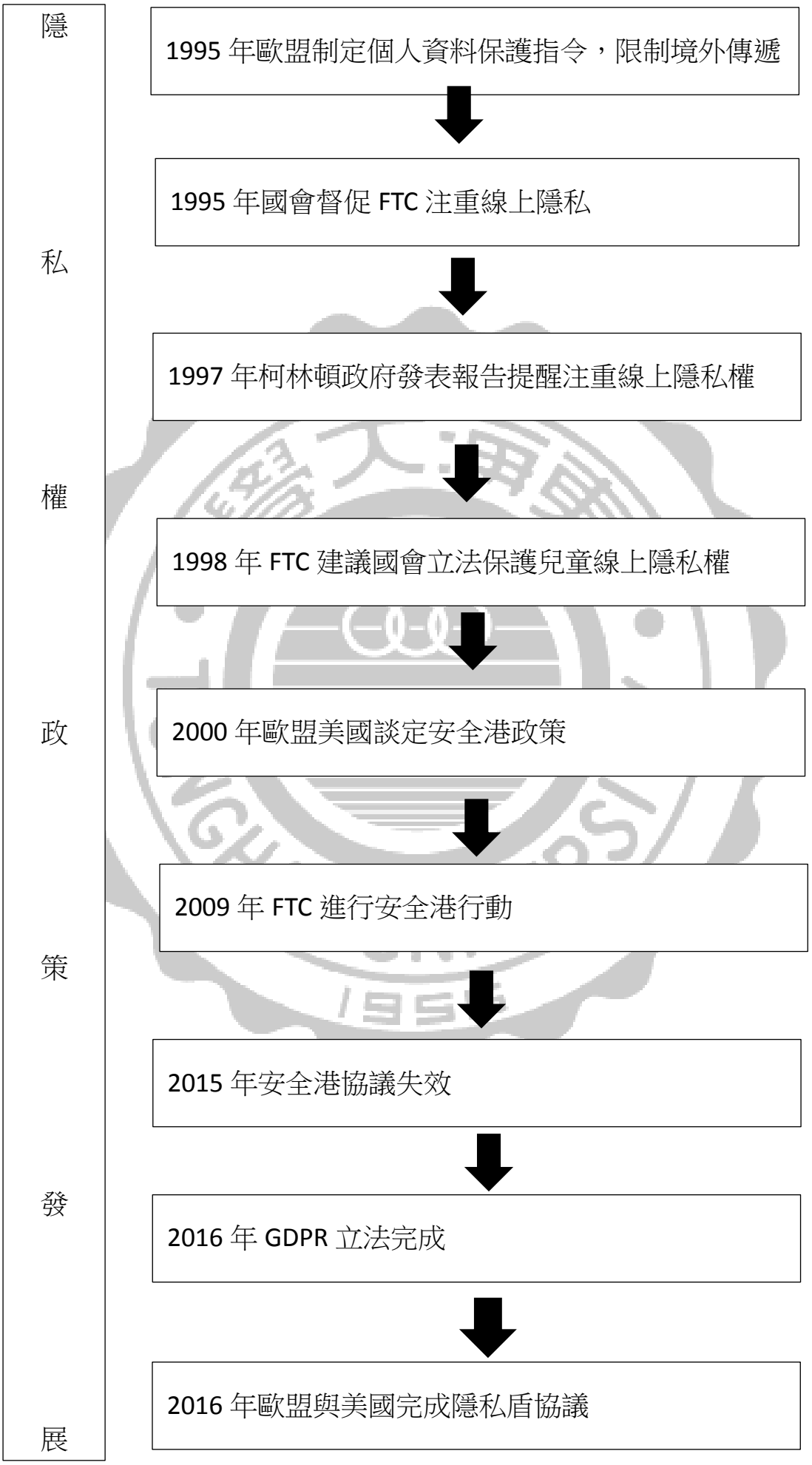
隱私盾協議目前為美國和歐盟暫時解決跨境傳輸問題的暫時方案，因隱私盾協議是否會為歐盟法院所接受目前仍在未定之天，而且據媒體報導歐盟還是認為隱私盾保護不夠周密[149]，無法達到 GDPR 的要求，歐盟法院可能無法接受隱私盾協議。故本文還是認為美國對於線上隱私權保障仍應有統一性專法來應對 GDPR 的規範較為適當。

第四項 小結

隱私權政策發展和歐盟個人資料保護跨境傳輸息息相關，大致可以統整如下圖

[148] 參 Joint Press Statement from Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross on the Second Annual EU-U.S. Privacy Shield Review，http://europa.eu/rapid/press-release_STATEMENT-18-6157_en.htm (最後瀏覽日 2018 年 12 月 05 日)

[149] 參 Privacy Shield under pressure as lawyers back MEPs' call for suspension，https://www.theregister.co.uk/2018/07/16/privacy_shield_under_pressure_as_lawyers_back_meps_call_for_suspension/ (最後瀏覽日：2018 年 12 月 05 日)


隱私權政策發展
1995 年歐盟制定個人資料保護指令，限制境外傳遞
1995 年國會督促 FTC 注重線上隱私
1997 年柯林頓政府發表報告提醒注重線上隱私權
1998 年 FTC 建議國會立法保護兒童線上隱私權
2000 年歐盟美國談定安全港政策
2009 年 FTC 進行安全港行動
2015 年安全港協議失效
2016 年 GDPR 立法完成
2016 年歐盟與美國完成隱私盾協議

綜上所述本文認為隱私權政策的加速發展來自於歐盟個人資料保護指令，為了能夠應付歐盟限制跨境傳輸以及保障美國電子商業市場自由，隱私權政策的加速發展係為了能讓美國不立專法下，利用隱私權政策和安全港協議達成歐盟跨境傳輸之目的。自美國實務上觀之，加入安全港協議必須要有個人資料保護自我監管機制，該自我監管計畫，美國企業均在隱私權政策中作出宣告，利用宣告的隱私權政策取得第三方認證和美國商務部認證後，該企業方能接收來自歐盟的個人資料。

本文認為隱私盾協議從歐盟工作小組所披漏之文件和外電媒體新聞報導觀之，該協議有很大的可能再次受到歐盟法院宣告違法無效。因從 GDPR 對境外傳輸的規範和歐盟工作小組所提出的原則可以推知歐盟仍希望歐盟境內個人資料傳遞至第三國時，該第三國法律體系係完善且有專責單位和獨立委員會，最重要在於政府不能任意干涉和監控[150]。從 2016 隱私盾協議至今美國仍未達到歐盟所期望，隱私盾再次被宣告無效的機率相當高。美國希冀企業透過宣告隱私權政策，加入隱私盾協議達到 GDPR 要求之規範恐怕有相當難度。美國是否會走向全面立法或者如同學者提出共同監管模式[151]，延續現行隱私權政策的，仍要看歐盟對 GDPR 執法的力道和態度。

[150] 安全港之所以爆發爭議最終導致無效係起因於美國 CIA 幹員史諾登披露美國利用網路大量監控人民線上隱私活動並輔以大數據分析找出淺在可能的恐怖份子。該案件一經披露後，引起全球嘩然認為美國企業助長美國政府侵害人權。

[151] Dennis D. Hirsch, super note 80

第四章 隱私權政策在我國之法律適用

第一節 公平交易法第二十五條與隱私權政策適用關係

如前述在美國消費者個人資料保護係美國公平交易委員會透過隱私權政策和聯邦貿易委員會法第 5 條中的「不公平或欺罔行為或慣例」規範保障；反觀我國公平交易法第 25 條亦有同之規範，惟我國公平交易法是否可以和美國法上作同一解釋發揮相同效力，實有必要探討與釐清，故本文以下就我國公平交易法第 25 條進行相關問題討論。

第一項 第 25 條構成要件與適用範圍

一、第 25 條適用範圍

(一)限制競爭和不公平競爭概括規定

公平交易法(下稱公平法)第 25 條性質為何？早期學說和實務見解容有爭議，有論者認為該條應僅為「不公平競爭」之概括規定，因從其章節編排觀之，本條置於不公平競爭章節中，故應僅有不公平競爭章節適用。而通說則認為本條為規定應為「限制競爭」和「不公平競爭」概括條款，因從比較法上觀察，其與德國不當競爭防止法(Gesetz gegen den unlauteren Wettbewerb, UWG)第 3 條和美國聯邦貿易委員法第 5 條相類似，而德國法和美國法並未區分兩者，且一個事業競爭行為必須同時通過限制競爭和不公平競爭檢視，才能被認定為合法競爭行為，兩者之間息息相關，實無必要將概括條款作出區分[152]。公平會最終採納通說之意見，在「公平交易委員會對於公平交易法第 25 條案件之處理原則」第二點明定，本條為限制競爭和不公平競爭之補遺性質概括條款，具有創造性補充性，若有其他條款可以引用時，則不需要援引本條。

[152] 參張麗卿，公平交易法第 24 條之法理分析與實務運用，公平交易季刊第 15 卷第 4 期，2007 年 10 月，頁 49。

(二)保護主體

公平法第 25 條保護對象是否包括消費者？學者認為從比較法上觀察，美國和德國並沒有明顯排除消費者，且美國更是以消費者利益為立足點，運用聯邦貿易委員法第 5 條對企業進行裁罰。我國公平法第 1 條亦表明本法訂立目的在於保障消費者利益，故本條保護對象應包含消費者[153]。

惟學者認為本條雖包含消費者，但並非單一事件的個別消費者，而係保護整體消費者。從公平會針對第 25 條案件處理原則觀之可知，侵害消費者利益須以該事件已「足以影響交易秩序」為要件，若只是單一消費糾紛，則消費者應依民法或者消費者保護法請求救濟，而非適用公平法[154]。

二、構成要件

(一)禁止欺罔

欺罔用語屬於公平法專用，與常見民法和刑法上的詐欺不同。民刑法上詐欺係以行為人施用詐術致被害人陷於錯誤，因此處分財產，產生財產上的損失。公平法欺罔則係指以欺瞞、誤導或隱匿重要交易資訊方式致引人產生認知上的錯誤，進而從事交易行為。所謂重要交易資訊系指足以能夠影響交易決定的資訊，引人產生認知上的錯誤，該錯誤判斷標準需以一般社會大眾客觀上均有可能受騙為判斷基準，並非以個別消費者作為認定標準。

公平法保護為一般社會消費大眾的公共法益並非個人法益，學者[155]認為公平法所保護並非個人財產上的損失，而是消費大眾的交易安全，故行為人只要有欺罔行為並足以影響一般社會交易秩序，不需要以造成個別交易相對人財產

153 參公平交易法第 1 條：「為維護交易秩序與消費者利益，確保自由與公平競爭，促進經濟之安定與繁榮，特制定本法。」
154 參公平交易委員會對於公平交易法第 25 條案件之處理原則第 2 點
155 參劉孔中、薛景文，仿冒表徵及欺罔或顯失公平行為之執法檢討與展望，公平交易季刊第 21 卷第 1 期，2013 年 1 月，頁 88。

上損失即構成本條要件。

(二)顯失公平

顯失公平一詞為不確定法律概念用語，因此如何解釋顯失公平，學說上認為雖然公平法第 25 條顯失公平一詞，和美國聯邦貿易委員法第 5 條中「不公平」一詞類似，但不能作相同解釋，因美國法規範係以「商業上或者影響商業上」作為認定標準，和我國法以「足以影響交易秩序」認定上不同，故解釋上仍應回歸我國法體系作解釋。又有學說見解認為顯失公平一詞屬於民法上用語，為誠信原則之一環，據此應該從民法上誠信原則作解釋較為妥當[156]。所謂誠信原則係指在具體的權利義務之關係，依正義公平之方法，確定並實現權利之內容，避免一方當事人犧牲他方利益以圖利自己，而應以權利人及義務人雙方利益為衡量依據，並應考察權利義務之社會上作用，於具體事實妥善運用之方法[157]。

顯失公平具體要件與操作模式有：

1、不公平行為必需造成消費者實質損害。實質損害包含財產、生命、健康…等權利上損害，且損害不以現時結果為限，包含將來可能發生的危害。

2、損害必須大於對消費者所提供的利益。消費者的損害必須考量到業者的成本和利益，例如，提供消費者完整的產品設計圖雖然可以提高消費者的判斷和決定，但若提供將會造成廠商智慧財產的外流以及製造成本提高時，廠商不提供完整設計圖則不屬於消費者的損害。亦即消費者的損害是眾多因素考量下權衡的結果，並非絕對以消費者利益為考量[158]。

3、消費者必須已盡到合理注意而仍無法避免損害。消費者於消費時需冷靜

156 參張麗卿，同前註 152，頁 63。
157 參王澤鑑，民法總則，三民書局，增訂版，2009 年 9 月三刷，頁 597。
158 參公平會公處字第 107033 號處分書，公處字第 106062 號處分書

思考與理性判斷，善盡應有之注意義務，若仍受到損害，主管機關才有介入之必要，以避免過度干涉自由市場機制。

實務上[159]公平會認為顯失公平有兩點考量，第一：從交易過程中檢視，若交易人明顯利用其優勢地位壓抑妨害消費者思考，或訂立不平等條款，則會構成顯失公平。第二：從市場效能判斷，若市場效能明顯受到一方掌控，而失去自由市場應有之作用，對於其他競爭者或消費者而言則屬於顯失公平。

第二項 實務執行

一、欺罔之態樣

公平會針對目前交易市場上出現的欺罔態樣分為三類型(1)冒充或依附有信賴力之主體，(2)未涉及廣告不實之促銷手段，(3)隱匿重要交易資訊，其中和個人資料保護有相關者為隱匿重要交易資訊。

隱匿重要交易資訊係指交易雙方如有一方刻意隱瞞重大交易資訊，引起另一方判斷錯誤，藉此牟取不當利益或者損害他人利益，致使影響市場交易秩序。故積極隱匿或消極不告知重要交易資訊，均屬本條處罰對象。

常見的案件有企業經營者隱匿其真實蒐集、利用和處理個人資料之目的，利用欺罔之手段取得消費者，再將消費者個資作為他用。具體裁罰案件為A廠商為賣淨水設備之公司，利用參加抽獎之方式取得消費者個人資料，謊稱消費者中獎，並且到府進行安裝，因淨水設備每家廠牌規格並不相同，致使消費者若安裝A廠商淨水設備，日後濾心以及相關消耗品之更換均只能向A廠商採購，又A廠商宣稱機器完全免費，但需支付獎品10%的安裝費用，A廠商宣稱該產品有32,500元之價值，消費者需支付3,250元安裝費用，事實上產品價值不如A廠商宣稱如此高價，根據公平會調查該機器市價不到3,250元，故A廠商

[159] 參張麗卿，同前駐152，頁65

利用欺罔之方式取得消費者資訊，又利用資訊不對等和優勢市場地位進行行銷，明顯對消費者不公平，構成公平法第 25 條要件，依法裁罰[160]。

二、顯失公平之態樣

只要企業商業行為若明顯造成不公平競爭，公平會便會介入調查並且進行裁罰，常見態樣有(1)不符商業競爭倫理的不公平競爭行為，(2)不符合社會倫理手段從事交易行為，(3)濫用市場優勢地位。其中涉及個資保護者為濫用市場優勢地位。

濫用市場優勢地位係指企業經營者利用商業優勢地位妨礙消費者或者其他企業經營者行使其權利或其他不當之行為，常見態樣有

(一)利用資訊不對稱之行為：交易人居於市場優勢地位，並未對交易相對人充分揭露市場資訊，影響交易交對人是否交易之決定或造成交易相對人權益上損害。常見案例有業者並未對加盟者充分揭露事業經營現況、權利金以及相關費用和其他重要交易資訊[161]。

(二)妨礙消費者行使合法權益：重大交易若交易之一方處於市場弱勢，應有充分審理契約之權利，若不當限制合理審約權利則構成本條濫用市場地位之要件。常見案例有建設公司要求購屋者需付訂金才給予審約，公平會認為預售屋之交易較其他消費性商品，具有「價值高」之特性，由於預售屋尚未具體成形且未辦理產權登記，購屋人於簽訂買賣契約書時，就所購房屋事先可取得之資訊相當有限，建築開發業者(即建商)無疑為資訊優勢之一方，故於預售屋交易過程中，建築開發業者應提供充分、完整之資訊以供購屋人評估是否作成交易，以衡平雙方之締約地位。倘建築開發業者先收取定金或一定費用，再提供

[160] 參公處字第 103117 號，相同案件有公處字第 107042 號；公處字第 105105 號；公處字第 106070 號等，上述案件全部都是淨水公司利用同樣的手法，騙取消費者個資後，再加以濫用。
[161] 參公平會公處字第 091100 號處分書，公處字第 107018 號。

契約審閱，及至購屋人對契約內容有所異議，建築開發業者不能接受或甚至堅持依既定內容簽約，否則沒收定金，則該定金之收取將陷購屋人於弱勢之不利地位而顯失公平，致影響購屋人作成交易之決定，同時對契約書供購屋人自由審閱之同業形成不公平競爭。故濫用市場地位不當限制消費者權利屬於顯失公平態樣之一，構成本條處罰要件[162]。

(三)利用定型化契約之不當行為：此類案件，交易人與交易相對人間其契約不利條款已經充分完全揭露，且並無不當限制當是人審約之條件，惟其中一方藉由其優勢地位要求另一方必須遵守對其不利之條款否則將拒絕交易，亦即交易之一方沒有議約能力，只能完全接受優勢之一方提出所有議約條件。常見案件有銀行憑藉優勢地位要求貸款者遵守不確定性概括條款，貸款者多為一般民眾，和銀行為明顯不對等關係，而不確定性概括條款有多種解釋之可能性，容易導致貸款人負擔不確定義務，是以銀行金融業者利用不確定概括條款片面約束貸款者，明確違反誠實信用原則，構成本條顯失公平態樣[163]；銀行利用定型化契約要求貸款人接受加速條款，所謂加速條款係指銀行於契約簽訂，若嗣後發現貸款人有信用不良之情形，銀行可以停止或減少授信金額之給付，或縮短授信期限。加速條款之約定攸關借款人期限利益，倘金融業者於定型化契約約定概括條款作為債信不足事由，因其文義內涵抽象，且金融業者相對於貸款人具有市場相對優勢地位，縱係透過個別議定或事前告知方式為之，金融業者透過片面解釋或適用系爭概括約款，仍將使交易相對人隨時陷於義務不明確之狀態，銀行利用優勢地位要求貸款人接受加速條款，構成本條顯失公平之要件[164]。

上述三種態樣公平會並無針對違反個資裁罰之案件，但值得令我們注意者

[162] 參公平會公處字第 103088 號處分書，公處字第 103034 號處分書，公處字第 103036 號處分書。
[163] 參公平會公處字第 096143 號處分書。
[164] 參公平會公處字第 096060 號處分書。

是隱私權政策屬於契約之一環，若企業濫用市場地位制定不合理之隱私權政策，例如電信業者利用綑綁同意，過剩的蒐集個人資料當事人，若不同意則拒絕服務，如同上述銀行業者利用優勢地位要求當事人同意「加速條款」一樣，本文認為公平會得用「顯失公平」為行政裁罰。

第三項 小結

在台灣企業若違反其隱私權政策是否可以用公平法第 25 條，欺罔(如企業宣稱其所蒐集消費者個資受到高等級資安防護，並且派有專員維護和員工定時接受保護個資之教育訓練，事實上並沒有上述情事)或顯失公平(如企業濫用市場地位，蒐集超過其服務所需之個資，消費者無任何議約能力，拒絕企業過度蒐集)處罰企業？本文採肯定見解，理由如下

一、消費者為公平法保護對象，公平法雖不像消費者保護法有明定消費者適用定義，惟從學者意見和公平會處分書觀察，只要企業商業行為足以影響市場交易秩序，消費者即得為保護對象。

二、從公平會統計報表和公平會處分書觀察，消費者個人資料保護為公平會業務範圍。

表二：公平會歷年案件統計表

處分案件統計－按違法行為別分

單位：件

年月別	處分件數	違反公平交易法						
		限制競爭行為	獨占行為	結合行為	聯合行為	約定轉售價格行為	其他	不公平競爭行為
總計	**4,610**	**508**	**16**	**63**	**210**	**77**	**154**	**3,261**
81-90年	1,792	207	3	25	80	25	82	1,368
91年	218	17	4	1	9	1	3	145
92年	187	23	-	1	10	2	10	133
93年	135	13	-	4	5	-	4	82
94年	141	15	1	-	10	2	2	84
95年	175	19	-	3	9	3	4	139
96年	184	15	-	4	7	3	1	137
97年	169	15	-	4	9	-	2	118
98年	183	18	1	4	8	3	2	147
99年	155	12	-	1	6	-	5	119
100年	272	19	-	1	8	1	10	180
101年	203	28	-	1	18	4	6	129
102年	214	29	3	6	7	10	3	132
103年	150	27	2	5	6	8	6	95
104年	144	24	1	2	12	7	2	82
105年	140	11	-	1	4	3	4	96
106年	116	13	1	-	1	3	8	61
107年1-5月	32	3	-	-	1	2	-	14
1月	9	-	-	-	-	-	-	5
2月	2	-	-	-	-	-	-	1
3月	5	-	-	-	-	-	-	4
4月	4	-	-	-	-	-	-	2
5月	12	3	-	-	1	2	-	2

年月別	違反公平交易法							違反多層次傳銷管理法行為	違反個資法行為
	虛偽不實或引人錯誤廣告行為	仿冒他人商品或服務表徵行為	不當贈品贈獎行為	損害他人營業信譽行為	欺罔或顯失公平行為	非法多層次傳銷行為	其他		
總計	**2,146**	**34**	**1**	**20**	**1,143**	**625**	**117**	**147**	**-**
81-90年	794	24	-	11	575	172	75	-	-
91年	60	1	-	-	85	55	1	-	-
92年	46	2	-	-	88	31	5	-	-
93年	48	2	-	1	32	38	4	-	-
94年	62	2	-	-	26	39	3	-	-
95年	95	-	-	2	47	18	-	-	-
96年	88	1	-	-	50	29	6	-	-
97年	93	1	-	-	28	32	4	-	-
98年	120	1	-	4	28	18	1	-	-
99年	89	-	-	-	32	22	2	-	-
100年	151	-	-	-	35	69	6	-	-
101年	110	-	-	1	20	46	2	-	-
102年	108	-	-	1	25	51	3	-	-
103年	74	-	-	-	26	5	1	23	-
104年	73	-	1	-	9	-	-	38	-
105年	77	-	-	-	20	-	-	33	-
106年	46	-	-	-	15	-	4	38	-
107年1-5月	12	-	-	-	2	-	-	15	-
1月	5	-	-	-	-	-	-	4	-
2月	1	-	-	-	-	-	-	1	-
3月	3	-	-	-	1	-	-	1	-
4月	1	-	-	-	1	-	-	2	-
5月	2	-	-	-	-	-	-	7	-

圖表來源：公平會

公平會歷年案件統計報表，明顯可以看到個人資料保護是列在統計項目內，雖目前沒有事業主體因單純違反個資被裁罰，但公平會針對事業主體用欺

罔方式取得個人資，再利用個人資料行銷產品則有裁罰紀錄，因此可以得知利用欺罔之手段取得個人資料加以利用，為構成第 25 條欺罔之情形，公平會可以介入進行裁罰。

三、從法律文義上解釋，公平法並沒有排除消費者個人資料保護之適用。我國法和美國法不同，美國未定立全面的個人資料保護法，為採部門式立法，故美國 FTC 透過隱私權政策和聯邦貿易委員法保障消費者個人資料。台灣制定有個資法，個人資料保護法律適用上應該優先適用個資法，惟從公平法第 45 條和第 46 條規定上觀察，公平法沒有明顯排除個資法之適用，亦即當事業主體用欺罔或者不公平方式蒐集個人資料或為目的外使用，足以影響市場交易秩序情況下，公平會應可依公平法第 25 條針對企業進行處罰。

本文認為基於上述三點理由，事業主體如違反其隱私權政策，而其違反行為明顯影響到市場交易秩序，公平會應可以用公平法第 25 條介入調查並且處罰事業主體。

第二節 隱私權政策和消費者保護法適用關係

本文認為企業違反隱私權政策且足以影響市場交易秩序，消費者得依公平法第 25 條主張權利。若隱私權政策之違反未影響市場交易秩序，消費者無法依公平法主張權利時，消費得否依照消費者保護法(下稱消保法)主張權利？

隱私權政策是否適用消保法關鍵在於隱私權政策是否能成立為契約。又隱私權政策於實務上運用大多都是網路電商，因此隱私權政策若能成立契約大多應為網路電子契約。網路電子契約和傳統民法契約並不相同，法律適用上和一般契約法並不一致，故網路電子契約較常討問之問題為契約成立之要件，以及消保法定型化契約適用條款的問題。本文下就契約成立以及定型化契約條款，

與隱私權政策在消保法適用關係上進行討論。

第一項 網路電子契約成立要件

網路電子契約成立要件為當事人、標的以及意思表示，而其和傳統民法契約不同處在於意思表示的方式和表示方式的法律性質，本文為避免討論範圍過大，故僅針對隱私權政策相關範圍進行討論，其中包含

一、網路意思表示方式

民法意思表示分為有相對人和無相對人，其中有相對人的意思表示民法第94條和第95條第1項規定，將其分為對話和非對話，前者表意人能和相對人即時為交換意思，如打電話、面對面口頭溝通；後者指表意人與相對人依間接方式交換意思方式，如電報、電郵、書信等。兩者判斷基準以是否能夠直接對話溝通為基準。又區分兩者間差異的實益，在於意思表示生效之時點，對話的意思表示生效以對方了解其意思表示時；非對話的意思表示生效則為通知達到相對人時。無相對人的意思表示生效時點法並無明文規定，學者認為生效時點應為意思表示的當下即生其效力[165]。

網路意思表示究竟為有相對人或無相對人？對話或非對話？應就具體個案探討之。例如電子商務網站若設有即時線上服務部門，能夠針對客戶問題直接進行回答，此時網路意思表示應該定義為對話且有相對人；若電子商務網站僅有刊登特定資訊給與大眾閱覽，並無即時交換意思表示，從上述判斷認為應係有相對人且非對話。故隱私權政策若僅有刊登在網頁上，且無即時交談時，該隱私權政策應為有相對人且非對話之意思表示。

意思表示生效相關問題，2001年電子簽章法立法，針對於電子文件生效時點有明確規定，依據電子簽章法第7條第2項規定：「電子文件以下列時間為其

[165] 參王澤鑑，同前註157，頁370-376

收文時間。但當事人另有約定或行政機關另有公告者，從其約定或公告。一、如收文者已指定收受電子文件之資訊系統者，以電子文件進入該資訊系統之時間為收文時間；電子文件如送至非收文者指定之資訊系統者，以收文者取出電子文件之時間為收文時間。二、收文者未指定收受電子文件之資訊系統者，以電子文件進入收文者資訊系統之時間為收文時間。」所謂電子文件依照電子簽章法第 2 條第 1 款規定，為指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。如 e-mail、Line 對話訊息等。因此電子簽章法確立了網路意思表示生效時點的問題。

二、網路刊登隱私權政策法律性質

契約之成立除了表意人意思表示外，尚須相對人作出承諾，而要約與承諾相互一致時，則契約成立。然網路電子契約意思表示方式有別於傳統民法表示方式，一般常見型態為企業主或者廠商將其商品放在網頁上供人參考，消費者於瀏覽網站後，依據網路操作界面指示下成立訂單並支付款項，業者依據消費者購買商品出貨給予消費者，並收取貨物價金，完成交易。此種交易模式最常引發的爭議在於網頁上陳列商品並且標訂商品價金其法律性質上為何？如果廠商標錯價格是否能夠撤銷契約，還是必須依約出貨？台灣過去最有名的案子為戴爾電腦標錯價案，從該案延伸出的學說有兩說

(一)要約說

依據民法第 154 條第 2 項規定，貨物標訂賣價陳列者，視為要約。依此銷售者已在網頁標明商品之外觀、規格、型號以及售價，消費者可以直接確定其想要商品後向銷售者表示其購買意願並下訂單，此種表意內容及型態因已符合

呈現契約必要之點，故因視為要約[166]。實務法院判決認為只要刊登訊息「達到確定」程度，諸如標明型號名稱、原價、線上折扣、線上折後價等，此時刊登訊息已完整呈現物品資訊，則該刊登訊息為要約非要約之引誘[167]。

(二)要約之引誘說

民法第 154 條第 2 項但書規定，價目表之寄送，不視為要約。但書之規定為要約之引誘，引誘特定或不特定人向業者要約，要約引誘本身不發生法律上的效果[168]。網頁商品只有商品售價以及相關介紹，消費者看不到具體商品，本質上和商品價目表寄送相似，故應認為網頁應屬於要約之引誘，非要約[169]。網路商店業者，並非實體店業者，交易模式和一般實體店不相同，消費者在網頁下訂單後，業者仍須透過一般管道寄送貨物，此與一般價目表寄送並無不同，故應認為網路上標價出售商品應為要約之引誘[170]。法院實務上判決認為，網路網頁上張貼商品資訊並販賣商品，如果認為該資訊屬於要約，可能會使業者意外締結超過其履約能力之契約，而需負擔債務不履行之責任。故網路刊登商品資訊應為要約引誘[171]。

上述兩說爭論不休，最終主管機關經濟部為了解決網路標錯價格糾紛，於 2010 年公布零售業等網路交易定型化契約應記載及不得記載事項，其中第 5 點第 2 項明確規定業者必須依照合約出貨，但賦予業者可以收到訂單兩天內附正當理由拒絕契約成立，又同法再於 2016 年修正，刪除第 2 項規定，賦予業者最終有確認契約成立權利，其修正目的一樣是從企業違約風險和交易安全為出發

166 參林誠二，網路購物之錯誤標價衍生之法律問題，月旦法學教室第 86 期，2009 年 12 月，頁 10-11。
167 參台北地方法院 99 年度簡消上字第 1 號
168 參王澤鑑，債法原理，三民書局，2009 年 9 月，頁 174。
169 參李淑如，網路購物標價錯誤之法律解析，台灣法學雜誌第 135 期，2009 年 9 月，頁 135。
170 參陳自強，契約之成立與生效(三版)，元照出版，2014 年，頁 72。
171 參台北地方法院 98 年度北消簡字第 13 號判決

點，至此網路張貼販售資訊，應可以認定為要約之引誘，而非要約。

綜上述網路刊登資訊法律性質從上述學者文獻、法院判決和主管機關的規範可以推知，如果是企業將販售物品資訊張貼在網路平台，並且有可能產生大量違約風險和市場交易安全，則該資訊定義為要約引誘，依循此理由，本文認為得自反面解釋推知，若企業張貼契約條款不涉及大量違約風險和交易安全時，其條款應該可定義為要約，亦即消費者或使用者在獲得充分告知並同意後，即成立契約。例如企業要求網站使用者填寫個人資料加入會員，其於會員條款中所告知的隱私權政策，經使用者同意後，隱私權政策則應成為雙方成立契約之一部分，未來企業若有違反其隱私權政策，使用者得依此向企業求償。

三、小結

網路電子契約成立要件原則上為當事人、標的以及意思表示，而意思表示的方式會影響到意思表示生效之時點，由於本文將討論限縮於和隱私權相關之範圍，故從現今大多網路電商宣告的隱私權政策上看來都是只有靜態的宣告，因此靜態隱私權政策應屬於有相對人且非對話，其意思表示得依電子簽章法第 7 條第 2 項之規定生效。而隱私權政策應無法產生網路電商有締結超過其履行能力之契約，因而發生大量違約的風險，故隱私權政策應為要約，只要當事人有明確同意即構成契約。

第二項 隱私權政策和定型化契約

電子商務於 21 世紀初期隨著網路的普及開始活絡，改變人們購物習慣，為了因應電子商務所造成的影響，我國於 2001 年訂立電子商務消費者保護綱領，目的是為了保障交易安全、消費者隱私權、避免網路詐欺以及跨國交易等相關消費者權利[172]。綱領訂立後兩年於 2003 年我國針對網路交易正式將其納入消保

[172] 參行政院消費者保護委員會電子上物消費者保護綱領，
https://www.cpc.ey.gov.tw/cp.aspx?n=97E610626B9F499E (最後瀏覽日：2018 年 10 月 28 日)

法規範之範圍。依據消保法第二條第十款規定，將網際網路交易納入郵購買賣之一部份，並於 2015 年再次修法將郵購買賣修訂為通訊交易。

電子商務納入消保法規範，其影響範圍在於契約若屬於定型化契約，將受到主管機關公告「定型化契約應記載及不應記載」之事項拘束，企業違反主管機關公告之事項，則可能導致契約部分條款失其效力。又隱私權政策通常為企業事先擬定，若隱私權政策成為契約則應為定型化契約，自受到上述主管機關之公告所規範，故本文下就隱私權政策為契約要件、定型化契約應記載及不應記載事項以及個資法交互應用之問題提出探討。

一、定型化契約應記載及不應記載事項

(一)立法背景

在高度經濟發展的商業社會裡，企業經營者為了追求高利潤，降低經營風險，經常利用是先擬制的契約內容再向消費者進行締約，消費者完全沒有磋商契約內容之餘地，此種契約條款稱為定型化契約[173]。企業大量使用定型化契約其理由有(1)效率，比起向個別消費者進行磋商後再成立契約，定型化契約可以快速有效的和大量的消費者完成契約之締結。(2)風險規避，企業可以依預先定好契約條款規避其商業風險。(3)補充民法債篇有名契約不足，避免不必要的糾紛和訟累[174]。

惟大量使用定型化契約造成企業濫用契約自由，利用定型化契約條款制定許多對消費者不利之內容，或將風險轉嫁給消費者，而消費者因無足夠資力對抗，因此只能選擇簽約或不簽約，完全沒有磋商之餘地造成不公平之交易。政府為保障消費者避免企業濫用定型化契約逃避契約法上責任，於 1992 年立法之

173 參消費者保護法第 2 條第 7 款

174 參尤重道，定型化契約之概念與法律效果暨實務見解分析，消費者保護研究第 17 期，行政院消費者保護委員會，2011 年 12 月，頁 156。

初即訂立消保法第 17 條，授權給予中央主管機關可以根據其主管相關產業，公告定型化契約應記載及不應記載之事項，業者若違反主管機關公告之事項，相關契約條款無效。為補充法規的完善，消保法施行細則第 15 條第 2 項，針對主管機關公告內容，即使於該當企業定型化契約條款上未予記載，公告之條款仍構成契約之內容，亦即主管機關定型化契約條款一經公告，即構成企業和消費者締約內容之一部分[175]。

中央主管機關可以依實際需要選擇特定產業，公告其定型化契約應記載及不應記載事項，學者有贊成意見亦有反對意見，贊成意見認為行政機關依法介入定型化契約之制定，有效導正不公平，不合理之定型化契約條款[176]。且讓行政機關有監督之權責，得有效預防企業濫用定型化契約條款[177]。反對意見則認為立法者既然無權越俎代庖於法律上明定應記載及不應記載之事項，行政機關又如何利用法規命令代替企業制定契約條款[178]；應記載及不應記載事項事涉契約內容形成自由，主管機關應該謹慎為之，不應因具體個案引起的問題，即任意公告相關行業應記載及不應記載之事項[179]。

(二)應記載及不應記載事項合憲性

應記載及不應記載之事項為行政機關透過公告之方式干預契約自由，為國家行政之作用，被限制者為企業之營業和締約自由。然這樣的限制多數學者[180]認為應符合不足禁止之要求。所謂不足禁止係指憲法課予國家採取某種措施保

175 參舊消費者保護法施行細則第 15 條第 2 項：「中央主管機關公告應記載之事項，雖未記載於定型化契約，仍構成契約之內容。」現行施行細則第 2 項已經刪除。

176 參黃明楊，保險消費權益之探討，消費者保護研究第 12 輯，行政院消費者保護委員會，2006 年 12 月，頁 46-47。

177 參楊淑文，新型契約與消費者保護法，元照出版，第 2 版 1 刷，2006 年 4 月，頁 86。

178 參蔡宗珍，消費者保護或父權宰制？，台灣法學雜誌第 239 期，2014 年 1 月 1 號，頁 27-31。

179 參胡華泰，消費者定型化契約條款之行政規制，消費者保護研究第 17 期，行政院消費者保護委員會，2011 年 12 月，頁 146。

180 參胡博硯、張佑齊，論消費者保護法的行政監督與基本權保障，國會月刊第 44 卷第 1 期，2016 年 1 月，頁 57

障人民之基本權[181]。而在於現今，經濟活動主體已非個人與個人，是個人與企業的交易。由於企業與個人間經濟能力的懸殊，所掌握的資源也有差異，因此產生地位上的不對等。雖定型化契約具有提高交易效率、合理分配商品風險與補充法律規範不足的功能。然兩造經濟地位的不平乃是事實，在資本主義下，若企業對於某商品具有獨占地位，則根本無須與消費者妥協，消費者根本上處於完全劣勢地位。因此若從保障消費者權益避免過度受到企業侵害權益上觀之，國家確實有介入企業與消費者間之必要[182]。

(三)應記載及不應記載事項公告法律性質

又應記載事項及不應記載事項法律性質為何？學說容有爭議

1.一般處分說：此說認為企業與消費者締結契約時受到主管機關公告拘束，必須遵守主管機關公告應記載及不應記載之事項，否則契約部分條款會歸於無效，因此主管機關之公告部分對外直接發生法律效果，且相對人可得特定，符合一般處分之性質[183]。

2.法規命令說：法務部於95年發佈函示認為：消保法第17條之規定其目的係為導正不當之交易習慣及維護消費者正當之權益，且消保法第17條授權給行政機關公告特定行業契約之應記載或不應記載之事項，該特定行業之定型化契約若有違反者，其條款無效，故該項公告係對多數不特定人民，就一般事項所作抽象之對外發生法律效果，屬實質意義之法規命令[184]。法院判決則認定：消保法既賦與中央主管機關得公告定型化契約應記載及不應記載事項之權限，該公告即係行政機關基於法律授權，對多數不特定人民，就一般事項所作抽象

181 參大法官解釋728號湯德宗大法官協同意見書，2015年3月，頁4-5
182 參胡博硯、張佑齊，同前註180，頁58。
183 參尤重道，同前註174，頁169。
184 參法務部95年9月21日法律字第950035512號函。

之對外發生法律效果之規定，具有行政程序法第 150 條第 1 項法規命令之性質[185]；故實務意見認為應記載及不應記載之事項為法規命令。

(四)2015 年消保法修法

除了上述法律性質爭議外，消保法施行細則第 15 條第 2 項規定，「中央主管機關公告應記載之事項，雖未記載於定型化契約，仍構成契約之內容。」，該施行細則是否逾越母法授權亦有爭議，學者認為施行細則第 15 條第 2 項規定等於政府利用法規命令代替人民訂立契約，嚴重影響私法自治精神，且施行細則並非法律，應無權干涉或限制人民基本權利，故消保法施行細則第 15 條第 2 項應屬違憲[186]。為解決施行細則授權爭議，消保法 2015 年修法中將原施行細則的規定修訂進消保法第 17 條內，修法理由明確表示，為授權行政機關有法律依據公告應記載及不應記載事項，將原消保法施行細則第 15 條第 2 項內容修訂進消保法第 17 條促使主關機關公告程序更加明確[187]。故目前應記載及不應記載公告事項，法律性質應為法規命令，且企業若有違反其條款，其契約該當條款為無效外，特定定型化契約所訂條款若該當企業之契約並未記載時，該條款仍成為契約之一部分。

2015 年修法為了更完備主管機關對於定型化契約條款的公告，且避免主管機關濫權恣意公告定型化契約條款，增修消保法第 17 條第 2 項和第 3 項[188]，將主管機關應公告之範圍明確化，立法理由亦表示第 2 項和第 3 項之範圍，主管機關無須全部公告，得依現實情況調整其公告之範圍與項目。

二、隱私權政策如何符合消保法定型化契約條款

185 參最高法院 105 年度台上字第 266 號判決。
186 參蔡宗珍，同前註 178，頁 28。
187 參行政院消費者保護委員會，https://www.cpc.ey.gov.tw/News_Content.aspx?n=3840722B002ADEAB&s=C24DA92907D96559 (最後瀏覽日：2018 年 10 月 28 日)。
188 參行政院消費者保護委員會，同前註 187。

隱私權政策是否符合消保法之規範，必須從契約性質、構成要件以及個資法規定進行相關討論。

(一)定型化契約條款要件

定型化契約條款若要具有法律效力，學說和實務見解認為應符合以下標準

1.定型化契約條款應給予消費者一定時間審閱：依消保法第 11 條之 1 第 1 項規定，企業經營者與消費者訂立定型化契約前應給予消費者有 30 天以內之合理期間，供消費者審閱全部定型化條款內容，所謂合理期間應就商品內容和交易性質而定，並非一定為 30 日[189]。學者認為[190]本條係法律規定之合理機會審閱定型化契約條款，所謂合理機會應考慮交易相對人之屬性、交易之慣例、定型化契約條款提供之時期、地點、方式、以及定型化契約條款之字體、用語、印刷方式等因素作綜合判斷。

2.定型化契約條款應明示或公告：舊消保法第 13 條規定，「定型化契約條款未經紀載於定型化契約中者，企業經營者應向消費者明示其內容；明示其內容顯有困難者，應以顯著之方式，公告其內容，並經消費者同意受其拘束者，該條款則成為契約內容。」亦即消費者對於契約條款內容必須明確的知道，並經同意後才生效力。新修正消保法第 13 條將「定型化契約條款未經紀載於定型化契約中者」刪除，修法理由認為，定型化契約條款不論是否記載於定型化契約中，企業經營者均應向消費者明示或公告其內容，並經消費者同意，該條款始構成契約之內容。課予企業較重之告知義務目的在於保障消費者權益，避免因雙方資力過於懸殊，當發生消費糾紛時消費者無從舉證。

3.異常條款之排除：消保法第 14 條「定型化契約條款未經記載於定型化契約中，而依正常情形顯非消費者所得預見者，該條款不構成契約之內容。」學

189 參行政院消費者保護委員會 93.03.01 消保法字第 930000500 號函參照。
190 參翁清坤，同前註 83，頁 219。

說稱本條規定為異常條款之排除，所謂異常條款指，定型化契約條款雖已載於契約，惟其規範之事項，為一般人無法用其經驗法則所預知者，該條款對消費者即構成突襲，使消費者承擔不可預知之責任[191]。

另外定型化契約條款雖載明契約，但其字體細微或印刷不清、記載於契約背面等，任何讓消費者難以注意或辨識閱讀者，亦構成異常條款，學者更進一步認為異常條款之構成，應綜合考量除了外在難以注意和辨識外，若條款使用之文字超越消費者之知識程度者，亦屬異常條款。

4. 符合主管機關公告應記載或不應記載之事項：消保法第 17 條修正後，法律正式授權予主管機關公告定型化契約條款應記載及不應記載之事項，即使企業經營者未將該當條款載明於契約，依法主管機關之公告者，仍構成契約之一部分。

上述為構成定型化契約之合法要件，故隱私權政策內容必需要符合上述規定之要件。

(二)隱私權政策是否能以默示同意而構成定型化契約條款

隨著科技的發展，電子商務契約不斷推陳出新，其中較有爭議的契約種類為包裹契約，包裹契約在本文第三章有提及，分別為點擊包裹契約以及瀏覽包裹契約，前者有明確提供使用者或消費者審約和同意的權力；後者則無。對於瀏覽包裹契約成立要件，著重在於「默示的同意」，亦即使用者和消費者在有審查契約的可能下，其嗣後仍繼續使用服務或者消費商品者，美國實務上方認為使用者和消費者後續行為符合默示同意要件。

我國實務上網路企業經營者亦大量使用瀏覽契約，然我國學術和法院實務

191 參楊淑文，定型化契約之管制與契約自由-德國與我國法制發展之比較分析，政大法學評論第 132 期，頁 195。

卻甚少討論瀏覽契約成立要件，大多學者都引用美國實務見解加以討論

1. 無效說：此說認為美國實務上並未有統一意見，大多的瀏覽契約均為無效居多，據此為保障公平正義，應認為瀏覽契約無效[192]。

2. 條件說：此說和美國實務意見相同，學者認為瀏覽契約的條款為要約，使用者和消費者必須有意識到該條款的存在，或者有審閱該條款的可能，且使用者或消費者仍繼續使用，則成立默示同意的契約，其餘應該為無效[193]。

3. 類推適用說：此說認為我國在商品郵購和電訪買賣上已經有充分判決和學術討論，據此不需要再為電子商務創立新的法律概念，因電子商務隨著科技的進步變化太快，不如以舊有的框架套入電子商務契約加以類推適用[194]。

本文認為，採無效說較為適當。因條件說同意要件並不明確，且對使用者和消費者保障不足，有其弊端故條件說並不能採；而類推適用說，適用範圍太過廣泛，並不符合快速變遷的網路電子契約形式，無效說相較於其他兩說對消費者和使用者保障較佳，且具有明確操作之標準，故本文贊同無效說之意見。

承上述隱私權政策若以瀏覽包裹契約形式呈現者，有論者[195]認為在符合默示同意要件下，應得成立定型化契約條款，然亦有學者[196]認為默示同意對個人資料保障並不周到，故隱私權政策若以瀏覽包裹契約方式呈現應無法成立契約。置於個資法第 7 條雖有推定同意之規定，然推定同意應解釋上當事人尚須有積極提供個資之行為，方能成立推定同意。又國家發展委員會個人資料保護專案辦公室於 2018 年 12 月 18 日針對個資法第 7 條推定同意作出明確解釋認為

192 參楊智傑，資訊法，五南書局，2017 年 1 月，頁 302。
193 參陳曉慧；呂佩芳，數位內容之授權與交易機制，經濟部智慧財產局，2008 年 3 月，頁 25-27。
194 參許慈儀，電子商務世紀與契約締結之變革司法新聲第 125 期，2018 年 1 月，頁 66-67。
195 參翁清坤，同前註 83，頁 231-236。
196 參劉定基，析論個人資料保護法上「當事人同意」的概念，月旦法學雜誌第 218 期，2013 年 7 月，頁 153。

「推定同意」之方式取得個人資料，除應盡告知義務且明確告知外，尚須符合「當事人未表示拒絕」及「當事人已提供其個人資料」兩項要件，始得為之[197]。故本文認為默示同意應不能構成個資法上「同意」，因此隱私權政策若以瀏覽包裹契約形式呈現，該隱私權政策應無法成立契約。

三、現行公告應記載及不應記載事項和個資相關部分

消保法第 17 條授權主管機關得選擇特定行業，公告應記載及不應記載事項，目前行政院針對定型化契約應記載及不應記載事項公告，從 1998 年 6 月 17 日起至 2018 年 10 月 8 號止已有 83 筆，又從 2012 年 9 月 21 日個資法施行開始至今，行政院公告應記載及不應記載事項共有 44 筆[198]，對於個人資料保護，有明定應記載於定型化契約條款的共有 18 筆[199]，而行政院現行公告應記載及不應記載事項大致上可分為三種(1)完全沒有記載個人資料保護(2)公告上僅要求契約必須載明企業會遵守個資法(3)針對部分個資保護簡單記載要求是項。

197 參國家發展委員會個人資料保護專案辦公室，推定同意取得同意之方式，https://www.ndc.gov.tw/Content_List.aspx?n=726A44EA5D724473 (最後瀏覽日：2019 年 01 月 20 日)

198 44 筆包含個人網路銀行業務服務定型化契約；預售停車位買賣定型化契約；藝文展覽票券定型化契約；成屋買賣定型化契約；零售業販售福袋定型化契約；兒童課後照顧服務中心定型化契約；電子票證定型化契約；電影片禮券定型化契約；國內線航空乘客運送定型化契約；市區汽車客運業旅客運送定型化契約；公路汽車客運業旅客運送定型化契約；自由氣球乘客載運定型化契約；洗衣定型化契約；骨灰(骸)存放單位使用權買賣定型化契約；生前殯葬服務定型化契約(自用型)；生前殯葬服務定型化契約(家用型)；海外留學契約；信用卡定型化契約；第三方支付服務定型化契約；消費性無擔保貸款定型化契約；預售屋買賣定型化契；零售業等商品(服務)禮券定型化契約；菸酒商品禮券定型化契約；個人購車貸款定型化契約；個人購屋貸款定型化契約；金融機構保管箱出租定型化契約應記載事項；小客車租賃定型化契約；餐飲業等商品(服務)禮券定型化契約；移民服務定型化契約；國內固定航線載客船舶乘客運送定型化契約；房屋租賃定型化契約；國內旅遊定型化契約；國外旅遊定型化契約；零售業等網路交易定型化契約；個別旅客訂房定型化契約；自行車租賃定型化契約；即時通訊軟體服務定型化契約；以通訊交易方式訂定之食品或餐飲服務定型化契約；短期補習班補習服務契約；短期補習班補習服務契約；家用液化石油氣供氣定型化契約；藝文表演票券定型化契約；鐵路旅客運送定型化契約；遊覽車租賃定型化契約；網路連線遊戲服務定型化契約

199 兒童課後照顧服務中心定型化契約；洗衣定型化契約；生前殯葬服務定型化契約(自用型)；海外留學契約；第三方支付服務定型化契約；消費性無擔保貸款定型化契約；個人購車貸款定型化契約；個人購屋貸款定型化契約；移民服務定型化契約；國內旅遊定型化契約；國外旅遊定型化契約；零售業等網路交易；個別旅客訂房定型化契約；即時通訊軟體服務定型化契約；以通訊交易方式訂定之食品或餐飲服務定型化契約；短期補習班補習服務契約；家用液化石油氣供氣定型化契約；網路連線遊戲服務定型化契約；

本文下就部分應記載及不應記載事項要求記載個資保護之內容和個資法要求告知內容進行相關比較。

(一)即時通訊軟體服務定型化契約應記載及不得記載事項

現行行政院公告即時通訊軟體服務定型化契約應記載及不得記載事項其應記載部分為 9 條，不應記載部分為 8 條，和個人資料保護具有關聯性為應記載部分第 1 條企業經營者資訊、第 3 條消費者帳號申請及使用、第 4 條安全維護責任；不應記載部分則為第 2 條個人資料權利之行使和第 3 條目的外之個人資料利用。上述條文內容和個資法比較為

應記載事項	個人資料保護法
第 1 條：企業經營者之名稱、代表人、網址、營業所所在地地址、電話、電子郵件信箱、客服聯絡方式。	第 8 條第 1 項第 1 款：公務機關或非公務機關名稱。
第 3 條第 2 款：消費者配合登錄本服務及個人資料確認之方式。	第 8 條第 1 項第 5 款：當事人依第三條規定得行使之權利及方式。其行使權利部分應為第 3 條第 1 款：查詢或請求閱覽。
第 3 條第 4 款：約定消費者刪除帳號，本服務之使用權即消滅者，企業經營者應於消費者主動刪除帳號同時，提供刪除確認及警示機制。	第 8 條第 1 項第 5 款：當事人依第三條規定得行使之權利及方式。其行使權利部分應為第 3 條第 5 款：請求刪除。
第 3 條第 5 款：約定消費者一定	第 11 條第 3 項：個人資料蒐集之特定

期間未使用本服務，即得刪除其帳號者，企業經營者除應事先以官網約款提醒文字促使注意外，關於其刪除應以官網公告、簡訊、電子郵件或推播等方式通知消費者，並於一定期間(至少十五日)經過後消費者仍未使用本服務時，始得刪除其帳號並終止提供本服務。	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。
第 4 條第 1 款：消費者遭他人不法冒用帳號之通知方式；企業經營者確認消費者帳號被冒用後應立即停止該帳號使用。除因法令規定或有正當事由外，於通知消費者申請更換密碼後，應回復該帳號使用。	第 12 條：公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。
第 4 條第 3 款：企業經營者應維護其系統符合當時科技或專業水準可合理期待之安全性，防止不法入侵、取得、竄改、毀損消費者使用本服務之相關紀錄或個人資料；對於系統遭不法入侵或破壞，應採取合理措施後儘速予以回復，並對於消費者所受損害負賠償責任。	第 27 條：非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

不應記載事項	個人資料保護法
第 2 條：不得約定消費者預先拋棄或限制下列個人資料權利之行使：(一)查詢或請求閱覽。(二)請求製給複製本。(三)請求補充或更正。(四)請求停止蒐集、處理或利用。(五)請求刪除。	第 3 條：當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：一、查詢或請求閱覽。二、請求製給複製本。三、請求補充或更正。四、請求停止蒐集、處理或利用。五、請求刪除。
第 3 條：不得於法律規定外，約定對消費者個人資料為契約目的必要範圍外之利用。	第 5 條、第 19 條和第 20 條

從上述比較表上可以理解雖即時通訊軟體服務定型化契約應記載及不得記載事項主管機關有要求企業必須將個資保護納入企業和消費者之定型化契約，然而規範範圍仍嫌不足，比如個資法第 8 條有 6 款告知事項，並沒有全部納入規範只有部分納入規範。即便主管機關公告事項並沒有完整將個資法之規定納入，但仍可發現部分條文的規範相較於個資法是比較詳細。

(二)國內旅遊定型化契約應記載及不得記載事項

現行國內旅遊定型化契約應記載及不得記載事項其應記載部份共有 31 條，不應記載部分為 9 條。和個人資料保護相關者為應記載第 1 條旅行社之名稱和第 29 條個人資料之保護，其比較如下

應記載之事項	個人資料保護

第 1 條第 1 項：應記載旅客之姓名、電話、住(居)所及旅行業之公司名稱、註冊編號、負責人姓名、電話及營業所。	第 8 條第 1 項第 1 款：公務機關或非公務機關名稱。
第 29 條第 1 項：旅行業因履行本契約之需要，於代辦證件、安排交通工具、住宿、餐飲、遊覽及其所附隨服務之目的內，旅客同意旅行業得依法規規定蒐集、處理、傳輸及利用其個人資料。	第 8 條第 1 項第 2 款：蒐集之目的。 第 8 條第 1 項第 4 款：個人資料利用之期間、地區、對象及方式。
第 29 條第 2 項：前項旅客之個人資料旅行業負有保密義務，非經旅客書面同意或依法規規定，不得將其個人資料提供予第三人。	第 27 條：非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
第 29 條第 3 項：第一項旅客個人資料蒐集之特定目的消失或旅遊終了時，旅行業應主動或依旅客之請求，刪除、停止處理或利用旅客個人資料。但因執行職務或業務所必須或經旅客書面同意，不在此限。	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。
第 29 條第 4 項：旅行業發現第	第 27 條：非公務機關保有個人

一項旅客個人資料遭竊取、竄改、毀損、滅失或洩漏時，應即向主管機關通報，並立即查明發生原因及責任歸屬，且依實際狀況採取必要措施。	資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
第 29 條第 5 項：前項情形，旅行業應以書面、簡訊或其他適當方式通知旅客，使其可得知悉各該事實及旅行業已採取之處理措施、客服電話窗口等資訊。	第 12 條：公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

上述條文比較，可以發現國內旅遊定型化契約應記載及不得記載事項相較於即時通訊軟體服務定型化契約應記載及不得記載事項是比較完整，但仍有許多不足之處，比如收集資料種類規屬為何消費者如何使用個資法第 3 條規範之權利等。

(三)零售業等網路交易定型化契約應記載及不得記載事項

現行零售業等網路交易定型化契約應記載及不得記載事項其應記載部分共有 14 條，不應記載部分為 9 條。和個資保護相關應記載部分為第 1 條和第 11 條，不應記載部分則為第 1 條和第 2 條。主管機關要求記載內容相當簡略，其中應記載第 1 條契約必須表明企業名稱，第 11 條則為契約必須遵照個資法；不應記載部分第 1 條為契約不得記載消費者放棄個資法第 3 條之權利，第 2 條為契約不得記載消費者同意企業主個人資料目的外利用。

(四)實務現況

從零售業等網路交易定型化契約應記載及不得記載事項即可發現，現行實

務很多應記載及不應記載事項幾乎都是簡單記載甚至不記載，故可知實務上主管機關對於契約是否要明確記載個人資料保護並無太多要求，除已經公告被要求必須載明於契約之產業外，業者得依照其產業特性，自由宣告個人資料保護之條款或者隱私權政策，若業者未將個人資料保護載明於契約中，或業者雖有宣告隱私權政策，但因隱私權政策未能符合默示同意購成契約一部分者，消費者應仍能依個資法請求保障。

如此實務上作法，有其優點和缺點，優點在於避免法律疊床架屋產生適用上的困難；缺點在於企業經營者一旦有侵害個人資料事情發生，消費者求償管道有限。本文認為主管機關應善用消保法賦與之權利保障個人資料安全，因消保法第 17 條第 2 項明定主管機關公告應記載及不應記載事項法律效力，如主管機關能針對大量蒐集個人資料相關產業作出相關公告，企業經營者即使未載明契約或另外利用網站公告其隱私權政策，但該公告因未能構成消費者默示同意無法成立契約，此時依消保法第 17 條第 2 項之規定，主管機關仍得依法認定有關個人資料保護應記載及不應記載事項公告構成契約內容之一部分，讓消費者仍得依契約權利向企業經營者請求損害賠償。

第三項 小結

網路電子契約成立和一般民法契約成立差別，在於意思表示方式以及其發生效力之時間，從上述第一項結論可以得知企業經營者公告隱私權政策其法律效力應為要約，因隱私權政策不涉及企業大量違約風險和交易安全，企業對於公告之隱私權政策並未保有最終決定全，隱私權政策公告，經消費者或使用者同意即成為契約一部分，企業經營者必須遵守其所公告隱私權政策，若隱私權政策嗣後有修改則必須再行告知消費者或使用者，並取得其同意。

消費者或使用者之同意，依新修正個資法規定，並不限書面同意，然因默示同意無法構成個資法上的同意，故隱私權政策若以瀏覽包裹契約方式呈現應

不合法，企業應放棄使用，改用較明確點擊同意契約，取得消費者同意。又隱私權政策亦須遵守消保法定型化契約條款規範，諸如定型化契約條款必須給予消費者一定時間審閱、條款應明示或公告、無異常條款、遵守主管機關應記載及不應記載事項公告等。故隱私權政策須符合定型化契約成立之規範，方有消保法規定之適用，若隱私權政策無法構成契約之一部，此時關於個人資料保護，消費者僅能依個資法和民法侵權行為，向企業經營者請求損害賠償。

第三節 我國司法實務判決

我國司法實務對於隱私權政策判決相當的少，依司法院法學資料檢索裁判書查詢系統，輸入隱私權政策，查詢各級法院判決顯示出只有 7 筆，其中智慧財產法院 2 筆、台北地方法院 4 筆、新竹地方法院 1 筆，而企業明確涉及個資違反遭消費者起訴共有 2 筆。另外 5 筆，智慧財產法院有 2 筆，所爭訴者為隱私權政策內容是否為著作權所保護，與個資法明顯無關。而台北地方法院 106 年度訴字第 140 號民事判決爭訟標的者為保證契約清償債務問題，內容雖有提及隱私權政策，但本案爭訟重點非個人資料保護，故法院對此並無任何判斷論說。又台北地方法院 102 年度小上字第 81 號民事裁定，雖有提及隱私權政策，惟該案件訴訟內容為妨礙名譽和個人資料保護無關。而新竹地方法院 100 年度訴字第 487 號民事判決，爭訟內容為公然侮辱之侵權行為賠償，與個人資料保護無涉。

故法院判決有關個人資料保護引述到隱私權政策者並加以論斷者，有台北地方法院 102 年度北小字第 2182 號民事判決、台北地方法院 97 年度北小字第 313 號民事判決；本文下就兩篇判決作評析。

第一項 台北地方法院 102 年度北小字第 2182 號民事判決

一、爭訟事實

原告主張：原告曾於被告網站上(TAAZE 讀冊生活)購書，但未料購書資料遭外洩公開，且並且未經當事人同意即公開大頭貼照片，未合理使用本人大頭貼照片，且為行銷需要，在網頁上刊登表示原告也推薦及收藏這些書，但實際上原告並未推薦也未收藏這些書，使原告名譽受損，嚴重不法侵害其名譽及隱私。原告提出相關網頁資訊和被告公司隱私權政策以作為佐證。

被告之抗辯：蒐集原告資料均來自於原告於臉書公開資料，並且在原告入會購書、使用「冊格子」服務及提出公司隱私權政策，以及服務條款，被告知悉上述條款並「同意」後方能入會使用該功能，據此被告並無違反任何法律侵害原告權利。

二、法院判斷

法院判斷「參照冊格子資料使用政策內容觀之，其上即載明會連結到個人臉書上，並在個人臉書上所公開之姓名、大頭貼照及封面相片均係一律可公開取得的資訊，有上開使用政策附卷可參。原告於加入上開應用程式前，既已同意使用政策並使用之，且得知有連結到臉書功能，足認原告於事前已得知使用冊格子虛擬書櫃功能將屬公開資訊且未事先設定權限，足認原告已同意公開上開訂書之個人資料，且同意蒐集、處理、利用上開大頭貼照片，及於冊格子中虛擬書櫃收藏內容，被告應尚無違反個人資料保護法……原告提供之網頁列印資料觀之，其內容僅係指買了格雷的五十道陰影這本書的人也買了哪些書本，有該網頁附卷可參，被告稱推薦功能僅係享收藏之內容，並非係指原告亦購買了上開網頁所列書籍，況縱格雷的 50 道陰影該書籍本身，實為合法、公開上市之書刊，縱原告買入該書，亦難認有何使原告在社會上之評價受到貶損之情，客觀上原告並無任何損害。而隱私權之保護目的在於避免個人於其私人生活事務領域所享不受不法干擾，免於未經同意之知悉、公開妨害或侵犯，而原告既使用上開網路服務，同意被告蒐集、處理、利用上開大頭貼照片及於冊格子中

虛擬書櫃收藏內容，甚難認原告有保護其私領域之意欲，是原告稱被告不法侵害其隱私權及個資外洩云云，應屬無理由，且原告復未能就其受有何等損害舉證以實其說，此主張即難憑採。」

法院意見依下列兩點認為被告並未違反個資法而判決原告敗訴

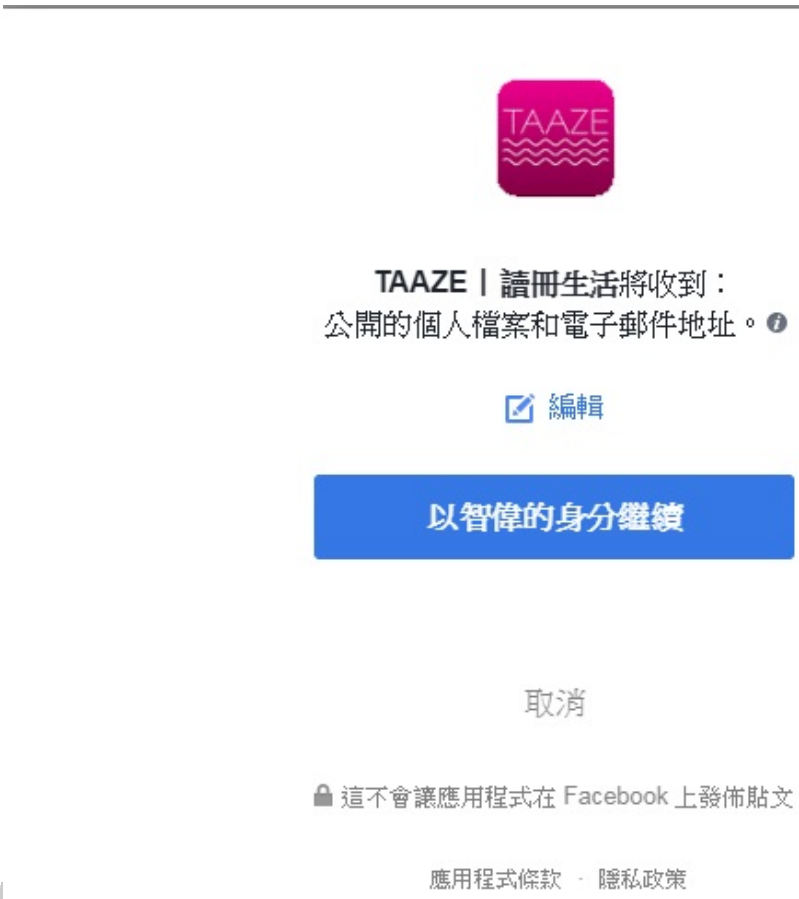
(一)被告利用原告姓名、照片等相關資訊，屬於原告臉書所公開之資料，且原告於入會時即被告知網路書商會蒐集、處理和利用其所公開資料，原告也明確表示同意。

(三)公開原告在冊格子收藏何書業經原告同意，故難認有保護原告其網路藏書內容為何隱私之必要，據此法院判斷原告隱私權並未遭受到侵害判決駁回原告之訴。

三、評析

被告為一網路書商，透過網頁販賣書、二手書和電子書，欲使用其服務必須先加入會員，加入會員有三種方式，其中為方便讀者，被告允許得以個人臉書帳號加入會員，只要點選連結並同意即可直接入會，不須另外提供其他個人資料，其入會方式見下方圖片

點選 FB 快速登入後會出現下圖



點選以身分繼續後，及加入該網站會員，並且可以使用其網頁所有功能。從上圖得以明瞭網路書商業者會收到臉書上所公開之個人檔案和電子郵件地址，個人檔案則包括，臉書大頭貼，臉書上登記的名子…等。

其隱私權政策係在網頁右下角，以較小字體和超聯結呈現，點選後會連結到該網頁隱私權政策，業者隱私權政策包含個人資料蒐集、處理和利用，明確標明業者蒐集目的、蒐集個人資料類別、使用項目、使用地區、使用期間和消費者對個人資料之權利等。蒐集和利用項目則明確表示用在(1)行銷業務。(2)對消費者、客戶管理與服務。 (3)統計與研究分析。(4) 網路購物及其他電子商務服務及與調查。故業者確實有向消費者表明蒐集個資以及如何處理和利用。

雖書商隱私權政策完整且告知消費者後獲得消費者同意，然該隱私權政策

列於不起眼之網頁角落，消費者若未點選超連結，將不知書商如何蒐集、處理和利用個人資料，故該告知是否有效？法院並無深入討論，僅單純認為消費者同意入會，即代表消費者同意書商得對其個人資料有蒐集、處理和利用之權利，因此，此判決上似有不足之處。

其次行政院對於網路交易有公告零售業等網路交易定型化契約之應記載及不得記載事項，該公告對於個人資料保護有要求業者應記載及不應記載事項，法院並未探討書商是否符合行政院公告事項，或該隱私權政策是否符合定型化契約成立條款，實為可惜。

再者從書商隱私權政策上觀之，書商於隱私權政策中「您的隱私就是我們的隱私」明確表達對於消費者購物紀錄、逛遊記錄都是個人隱私，書商不會隨意透露，惟書商另一冊格子服務功能卻可以讓外人看到個人藏書記錄，似乎明顯違反隱私權政策的承諾。事實上從入會資訊和隱私權政策，消費者並無法明確、有效了解冊格子會將藏書資訊公開，必須消費者自行進入冊格子 Q&A 網頁才會知悉，又該資訊會遭受公開之事於入會前無從知悉，明顯違反隱私權政策，法院卻以消費者入會時即明瞭使用政策並同意，故書商並未違反個人資料保護法，故判決關於此點有瑕疵。

最後本文認為書商隱私權政策入會時並明顯顯示，入會後亦難以找尋，因此書商未善盡告知義務，隱私權政策應不成立契約。無法依消保法和民法請求損害賠償。然未充分告知消費者並取得其同意即蒐集、處理和利用消費者個人資料，書商違反個資法第 19 條和第 20 條規定，消費者得依個資法第 29 條向書商請求損害賠償。

第二項 台北地方法院 97 年度北小字第 313 號民事判決

一、爭訴事實

原告主張：原告主張其在博客來網路書店購買商品，於交易完成後一個月，有自稱博客來客服人員打電給他，聲稱當時付款選擇勾選到分期付款，需要持金融卡到 ATM 解除分期付款，否則將會持續扣款，由於對方對原告個資相當清楚，原告不疑有他致使其遭到詐騙，損失存款金額，原告認為博客來在其隱私權政策上，明確揭示將會保障個人資料，然博客來並未善盡資料保護責任，致使個人資料外洩，造成其財務上損失，依民法第 184 條、第 188 條、第 191 條之 1 規定請求博客來負賠償之責。

被告之抗辯：被告主張原告並無證據證明被告有洩漏個人資料保護，故法院應駁回其訴。

二、法院判斷

法院採信被告所言，認為原告不能舉出被告洩漏個資之證據，故判決被告敗訴。

三、評析

原告於訴訟中有主張博客來違反隱私權政策，對於客戶資訊未善加保護，法院並未針對這部分予以論述，僅單純以原告證據不足判決原告敗訴，實有論證上之瑕疵。

依民事訴訟法第 277 條但書規定，法院認為兩造雙方資力不對等時，得依職權降低或轉移舉證責任，原告和博客來明顯資力不對等，且博客來於隱私權政策中明確闡明會以合理技術保護個人資料，保護個人資料屬契約之一部分。當原告主張博客來有保護不周之事，法院應檢視隱私權政策條款是否符合定型化契約條款規範，再依民事訴訟法規定倒置舉證責任，命博客來提出其已善盡保護之證據，而非單純以原告舉證不足駁回其訴[200]。

[200] 相同案例台北地方法院 104 年度北小字第 2548 號民事判決，原告一樣主張網路電商洩漏個資導致其遭受詐騙，法院依然以原告證據不足駁回其訴。目前因個資外洩導致被害人遭受詐騙，被害人依個資法請求成功案例僅有台北地方法院 106 年度北小字第 2161 號民事判決，本件判決能請求成功主要在於被告華信航空承認其個資外洩，故華信航空若不承認其個資外洩，依目前法院見解仍會以原告未能舉證而判決敗訴。

上述兩篇判決為司法院判決檢索系統能查詢到隱私權政策和個資保護有關之判決，從判決內容可以得知，目前法院對於隱私權政策並無太多要件上或法律意見上之論述。學者[201]認為我國對個人資料保護是採專法管理，並非如同美國用部門式立法，民間企業用隱私政策管理，故法院審理案件時，即使當事人有提出隱私權政策之主張，法院仍以個人資料保護法進行審理裁判。

[201] 參翁清坤，同前註 83，頁 236。

第五章 結論與建議

第一節 結論

電子商務與網路科技的發展，企業經營者為藉助網路科技拓展商務，利用網站消費者和使用者個人資料乃現代電子商務經營不可或缺之一環。惟雙方資力不對等，如何有效保障消費者和使用者個人資料屬各國政府面臨之難題。

隱私權政策係企業經營者對於個人資料蒐集、處理和利用之書面聲明或陳述。隱私權政策常見於美國企業，其發展過程應係受到歐盟個人資料保護指令所影響，因歐盟資料保護指令對於境外傳輸有嚴格之規定，然美國卻沒有一套完整保障個人資料之法規。而美國私人企業為了確保個人資料自主權、避免貿易上觸犯法規和美國政府過度干預，最終發展出隱私權政策用以達到上述之目的。具體操作為企業須先宣告隱私權政策，且經過第三方認證合格，加入美國和歐盟關於個人資料保護之協議(目前協議為隱私盾)，方得蒐集、處理和利用歐盟人民之個人資料。

隱私權政策在美國有其必要性，理由在於美國為部門式立法，並無統一聯邦法規範個人資料保護，故透過隱私權政策來確保符合歐盟之規定以及保障國內人民之個人資料。然我國從 2010 制定個資法，2012 年正式施行個資法，一直以來都有專法保障個人資料。因此隱私權政策雖在我國私人企業盛行，惟法律實務上卻未受到重視，不論是行政部門的裁處或司法部門的審判，對於隱私權政策均未有深入討論，因主管機關和法院均認為個人資料保護交由個資法統一管制即可，無須另外透過隱私權政策保障。這樣的認定是否代表隱私權政策在台灣完全無用武之地？本文持否定之看法，本文認為隱私權政策的發展有助於補充個資法的不足之處，只要利用得當將會有效提升私人企業對個人資料的保障。故隱私權政策在台灣仍有發展之空間與必要。

第二節 建議

隱私權政策在我國法律實務上未受到重視其原因有(1)我國過度重視對個資之保護。(2)隱私權政策法律性質不明確。(3)主管機關未善用隱私權政策來管理和監督私人企業。故本文就隱私權政策提出以下建議。

第一項 建立有效機制

網路電子契約成立與一般契約成立不同，電子契約型態會隨著科技發展不斷的改變，目前常見的電子契約種類為點擊包裹契約與瀏覽包裹契約。其中點擊包裹契約，消費者會接受到明顯告知，於彈跳出視窗中點選「我同意」後方能繼續使用該網站服務或程式；有別於點擊包裹契約，瀏覽包裹契約並無任何彈跳視窗或明顯的選項讓消費者或使用者點擊，因此無從得知企業經營者是否有取得同意。

基於營運成本考量多數網路企業經營者都使用瀏覽包裹契約呈現其隱私權政策，然因瀏覽包裹契約沒有明確的機制取得消費者的同意，故對於契約之成立常產生爭議。尤其現行使用瀏覽包裹契約之網站，其隱私權政策幾乎都放在不明顯之處，消費者可能無法得知網站聲明或陳述之內容為何？對於個人資料保護有明顯不周之處。

依個資法第 7 條規定，蒐集、處理和利用他人個人資料，必須告知當事人後取得當事人允許之意思表示，故隱私權政策是否能發揮其功效，關鍵在於利用合理方式告知於消費者，並取得其同意。

為了有效發揮隱私權政策之功能，網站對於隱私權政策聲明或陳述必須公告在明顯可見之地方，利用彈跳視窗告知消費者閱讀或引導消費者至公告網頁，若消費者或使用者有留下 e-mail，亦可發送電子檔案到電子信箱，透過上述方式方能符合法所規範的告知。而消費者獲得合理告知後，其同意方式在個資法 2015 年修法後已經不以書面為限，有學者認為消費者只要持續使用網站服務或沒有積極要求網站禁止蒐集、處理和利用個資時，應可視為消費者默示同

意，實務上[202]認為個資法第 7 條推定同意必須是消費者積極行為方能符合本條規範，因此為保障個人資料，消費者消極無任何行為不能表示其同意企業經營者蒐集資料，默示同意不符法所規範。

為杜絕企業經營者浮濫蒐集個人資料以及保障消費者權益，企業經營者仍需要建立一套符合法規同意機制，而瀏覽包裹契約同意方式並不明確，對消費者保障不周，應禁止廠商使用這種類的契約以避免上述之弊端。

最後隱私權政策可以補充個資法不足之處，為企業提供具體操作方式以保障消費者個人資料，和避免觸犯相關法規，有其存在之必要性。為能夠發揮隱私權政策之功能，避免其淪為具文，企業應依照上述之規範，建立有效之機制讓消費者知悉和取得其同意。

第二項 隱私權政策在台灣發展方向

隱私權政策在台灣發展應該有兩種方向，一是隱私權政策為契約，透過消保法加以規範和保護消費者。二是隱私權政策非為契約，為一般公司政策性陳述，目的在補足法規範上的不足。本文下就兩種方向提出分析與討論。

一、隱私權政策為契約

隱私權政策若要成為契約首先公司必須建立第一項所說有效機制，明確告知消費者隱私權政策，並且獲得同意成為契約之一環。而企業經營者因經營策略上考量通常會採預先擬制之定型化契約。因此如何保障消費者個人資料，則成為隱私權政策發展上的重點。

為了避免企業濫用定型化契約，消保法授予主管機關得公告行政命令，將定型化契約應記載及不應記載事項公告周知，用以監督與規範定型化契約。利用應記載及不應記載事項管控定型化契約，雖有違反契約形成自由之嫌，然卻能有效避免企業利用資力不對等之優勢，而侵害消費相關權利。

依消保法第 17 條規範，企業一旦違反主管機關所公告之事項，其應記載之

[202] 參國家發展委員會個人資料保護專案辦公室，同前註 197。

事項未記載者，法律效果令其構成契約內容之一部分，不應記載者，法律效果為無效。消保法第 17 條第 3 項、第 4 項規範，讓主管機關具有強而有力的武器以管控定型化契約，然現行狀況主管機關對於個人資料保護所發佈的公告甚少，以現行公告應記載及不應記載事項觀察，有要求業者必須記載保護個資者甚少。顯見主管機關對於這部分並不重視。

本文認為，新修正消保法賦予主管機關得利用應記載及不應記載事項管控定型化契約，因此主管機關對於消費者個人資料保護得邀請相關領域學者和廠商進行研討，共同討論出合適隱私權政策，並將其公告，將隱私權政策成為應記載及不應記載之一部分，藉此保障消費者個人資料。

二、隱私權政策非為契約

隱私權政策非為契約，僅是一般公司陳述或聲明時，美國實務上透過 FTC 利用聯邦貿易委員會法第 5 條規範「不公平或欺罔行為或慣例」來進行相關裁罰，我國雖有相似條文和機關，但由於我國有個資法，因此主管機關和法院遇到個資問題時，大多還是以個資法來處理相關問題。

我國有個資法是否代表隱私權政策非為契約時即無討論之必要？本文認為並非如此，因個資法僅能制定原則性條文，至於細項內容仍必須交由其他方式來達成法律規範的要求，以個人資料安全為例，個資法第 27 條第 2 項和第 3 項要求中央目的事業主管機關可以制定個人資料安全維護計畫，保障個資安全。因此目前主管機關針對於敏感性產業都有制定安全為護計畫及處理辦法來保證個人資料安全，例如旅遊業除了國內旅遊定型化契約應記載及不得記載事項外，針對個資保護還有旅行業個人資料檔案安全維護計畫及處理辦法，該辦法第 3 條明定個人資訊安全應如何維護，其內容包含要求業者必須配置專門處理人員、對個人資料安全定期評估、通報機制、人員教育訓練等。然安全維護計畫及處理辦法僅能夠針對該產業作原則性規定，至於具體實現內容仍須由企業主自行制定相關之規則。

因此隱私權政策的好處在於可以讓企業自行制定符合企業之個資保護。主管機關則可透過隱私權政策進行相關監管。簡言之，隱私權政策相較於法規直接規範可以更有彈性更符合企業需求。

三、隱私權政策為契約和非契約兩者間利與弊

隱私權政策為契約的優點在於主管機關可以透過現行消保法之規範，直接介入企業與消費者之間，透過定型化契約的應記載及不應記載事項來保障消費者權益；缺點在於破壞契約自由且直接透過法規命令制定契約內容可能會過於僵化不一定符合企業需求。

隱私權政策非為契約的優點在於立法者僅需要制定原則性規定，剩下交由主管機關和企業彈性運用其內容，進而達到個人資料保障；缺點則為若企業不願制定隱私權政策時，主管機關只能回到個資法進行監督和管理。

最後本文認為隱私權政策為契約或非為契約有其利弊，但整體而言隱私權政策不論法律性質為何？都可以補充現在法規之不足，本文站在保護消費者的立場上，仍會傾向透過消保法應記載及不應記載事項保障個人資料安全。

第三項 成立權責機關

我國個人資料保護法並未有設定專責機關，而係將權責交由中央目的事業主管機關或直轄市、縣政府等管理[203]，因此容易產生標準不一或者執行公權力上的困難。有鑒於此，行政院於2018年5月在國發會下成立個人資料保護專案辦公室，該辦公室目前有兩大方針，第一整合因應GDPR相關事宜，與向歐盟申請適足性認定工作。第二配合檢討個人資料保護法，協調整合並加強各部會落實執行個資法之一致性[204]。從該聲明可以明瞭專案辦公室目的在於協調各主管機關，並且針對法規範上的疑義作出統一的解釋，實際法律執行全仍然屬於各目的事業主管機關。

---

[203] 參個人資料保護法第 22、24、25 條。

[204] 參個人資料保護辦公室 https://www.ndc.gov.tw/Content_List.aspx?n=726A44EA5D724473 (最後瀏覽日：2018 年 12 月 11 日)。

個人資料的流動是快速且龐大，在公務機關往往涉及跨部會合作和流動，在非公務機關，企業間個資的交流、委託、處理和利用亦是趨勢。因如成立專責機關有助益達成[205]：

(1)、有效的整合跨部會個資的交流及合理利用。

(2)、獨立自主的運作，不受傳統行政架構拘束，更能有效的監督公務機關和非公務機關。

(3)、確立統一符合法的規範以及標準明確的執行準則。

除了上述整合和執行外，在隱私權政策部分，獨立的權責機關，即可整合各部會主關機關，讓其邀請專家學者，針對其主管個資之領域發佈其領域所需隱私權政策，並且公告成為應記載及不應記載事項，讓隱私權政策發揮更大的效用。

然現行專案辦公室現行只有整合統一解釋權利並沒有直接執行的權利，有別於歐美國家個人資料權責機關。而成立完整獨立權責機關為世界趨勢，故本文為仍建議我國應成立獨立權責機關方能完整保障國民個人資料。

[205] 參司法院大法官解釋 613 號。

參考文獻

中文文獻：

專書：

1、王澤鑑，民法總則，三民書局，增訂版，2009 年 9 月三刷，頁 597。

2、王澤鑑，債法原理，三民書局，2009 年 9 月，頁 174

3、李震山，多元、寬容與人權保障—以憲法未列舉權之保障為中心，元照出版社第 2 版，2007 年 9 月，頁 11。

4、李震山，人性尊嚴及人權保障，元照出版第 4 版，2011 年 10 月，頁 207 以下。

5、范姜真媺、劉定基、李寧修，「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告(編號：1050224)，行政院法務部，2017 年 3 月，頁 8。

6、陳自強，契約之成立與生效(三版)，元照出版，2014 年，頁 72

7、陳曉慧；呂佩芳，數位內容之授權與交易機制，經濟部智慧財產局，2008 年 3 月，頁 25-27。

8、楊淑文，新型契約與消費者保護法，元照出版，第 2 版 1 刷，2006 年 4 月，頁 86。

9、楊智傑，資訊法，五南書局，2017 年 1 月，頁 302。

期刊：

1、尤重道，定型化契約之概念與法律效果暨實務見解分析，消費者保護研究第 17 期，行政院消費者保護委員會，2011 年 12 月，頁 156。

2、李震山，政府資訊公開法與資訊隱私權保障，研考雙月刊第 31 卷 3 期，2007 年 6 月，頁 50-60。

3、李淑如，網路購物標價錯誤之法律解析，台灣法學雜誌第 135 期，2009 年 9 月，頁 135。

4、林玫君，簡介歐盟一般資料保護規則(GDPR)之跨境傳輸例外條款，經貿法訊第 233 期，2018 年 5 月 25 日，頁 45-46。

5、林其樺，安全港判決後歐美個人資料國際傳輸趨勢觀察，科技法律透析第 28 卷第 2 期，2016 年 2 月，頁 23-26。

6、林誠二，網路購物之錯誤標價衍生之法律問題，月旦法學教室第 86 期，2009 年 12 月，頁 10-11。

7、林庭宇，論我國法下非消費性定型化契約，萬國法律第 205 期，2016 年 2 月，頁 43-45。

8、胡華泰，消費者定型化契約條款之行政規制，消費者保護研究第 17 期，行政院消費者保護委員會，2011 年 12 月，頁 146。

9、胡博硯、張佑齊，論消費者保護法的行政監督與基本權保障，國會月刊第 44 卷第 1 期，2016 年 1 月，頁 57

10、翁清坤，論個人資料保護標準之全球化，東吳法律學報第 22 卷第 1 期，2010 年 3 月，頁 21-22。

11、翁清坤，網路上隱私權政策之效力：以美國法為中心，台大法學論叢第 45 卷第 1 期，2016 年 03 月，頁 174。

12、范姜真媺，他律與自律之共構個人資料保護法制-以日本有關民間法制為主，東吳法律學報第二十一卷第一期，2009 年 7 月，頁 166。

13、范姜真媺，網路時代個人資料保護之強化-被遺忘之權利主張，興大法學第 19 期，2016 年 5 月，頁 68。

14、陳起行，資訊隱私權法理探討-以美國法為中心，政大法學評論第 64 期，2000 年 12 月，頁 322。

15、許慈儀，電子商務世紀與契約締結之變革司法新聲第 125 期，2018 年 1

月，頁 66-67。

16、張麗卿，公平交易法第 24 條之法理分析與實務運用，公平交易季刊第 15 卷第 4 期，2007 年 10 月，頁 49。

17、黃明楊，保險消費權益之探討，消費者保護研究第 12 輯，行政院消費者保護委員會，2006 年 12 月，頁 46-47。

18、楊淑文，定型化契約之管制與契約自由-德國與我國法制發展之比較分析，政大法學評論第 132 期，頁 200-202。

19、詹森林，最高法院與定型化契約之發展-民法第 247 條之 1 裁判研究，政大法學評論第 94 期，2006 年 12 月，頁 103-104。

20、劉定基，析論個人資料保護法上「當事人同意」的概念，月旦法學雜誌第 218 期，2013 年 7 月，頁 153。

21、劉定基，雲端運算與個人資料保護－以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心，東海大學法學研究第 43 期，2014 年 8 月，頁 11-14。

22、劉孔中、薛景文，仿冒表徵及欺罔或顯失公平行為之執法檢討與展望，公平交易季刊第 21 卷第 1 期，2013 年 1 月，頁 88。

23、蔡宗珍，消費者保護或父權宰制？，台灣法學雜誌第 239 期，2014 年 1 月 1 號，頁 27-31。

24、戴豪君、常天榮、張雅雯，美國全球電子商業綱要與我國因應之道，資訊法律透析，1997 年 12 月，頁 18。

25、謝巧君，美國與歐盟安全港架構協議(The Safe Harbor Framework)，科技法律透析第 14 卷第 10 期，2002 年 10 月，頁 46-62。

26、蘇柏毓，104 年個人資料保護修正簡評，科技法律透析，第 28 卷第 4 期，2016 年 4 月，第 13-17 頁。

學位論文：

1、王至德，電子商務交易平台提供者之民事法律責任，國立高雄大學法律系研究所碩士論文，2010 年，頁 50。

2、王碧瑩，線上電腦軟體按鍵契約與消費者保護法之探討，中原大學財經法律研究所碩士論文，2008 年，頁 41。

3、於知慶，論客戶資料在金融控股公司於共同行銷時應有之保護，國立臺北大學法學系研究所，碩士論文，2005 年 6 月，頁 82-83。

英文文獻：

期刊：

1、Dennis D. Hirsch,The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?, Seattle University Law Review, Vol. 34, No. 2, (2011),439-480

2、Daniel J. and Hartzog, Woodrow, The FTC and the New Common Law of Privacy (August 15, 2013). 114 Columbia Law Review 583 (2014); GWU Legal Studies Research Paper No. 2013-120;

3、Florencia Marotta-Wurgler and Daniel Svirsky,Do FTC Privacy Enforcement Actions Matter? Compliance Before and After US-EU Safe Harbor Agreement Actions

4、Hetcher Steven, The FTC as Internet Norm Entrepreneur, VANDERBILT UNIVERSITY LAW SCHOOL PUBLIC LAW AND LEGAL THEORY RESEARCH PAPER SERIES,53 Vand. L. Rev. 2041(2000),2041-2061

5、Ian Rambarran & Robert Hunt, Are Browse-Wrap Agreements All They Are Wrapped Up to Be?bepress Legal Series,(2006), bepress Legal Series.Working Paper 1885.

6、James P. Nehf, discussing “FTC’s inadequacy and toothlessness in ensuring privacy protection,Recognizing the Societal Value in Information Privacy, 78 Wash. L. Rev. 1, 58 (2003)

7、James P. Nehf, discussing “FTC’s inadequacy and toothlessness in ensuring privacy protection,Recognizing the Societal Value in Information Privacy, 78 Wash. L. Rev. 1, 58 (2003)

8、Lieutenant Colonel Evan M. Stone, The Invasion of Privacy Act: The Disclosure of My Information in Your Government File, 19 WIDENER L. REV. 345, 352 (2013)

9、Thomas B. Norton, The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model, 27 Fordham Intell. Prop. Media & Ent. L.J. 181(2016)

官方文獻：

1、Administraion Discussion Draft:Consumer Privacy Bill of Rights Act of 2015,2015.02, at17

2、Complaint at 4, In re Sony BMG Music Entm’t, FTC File No. 062 3019, No. C-4195 (F.T.C. June 28, 2007) [hereinafter Sony BMG Complaint].

3、ln re Facebook, Inc., FTC File No. 092 3184, No. C-4365, at 5 (F.T.C. Nov. 29, 2011) (consent order); see also FTC v. EMC Mortg., No. 4:08-cv- 338, at 11 (E.D. Tex. Sept. 9, 2009) (decision & order)

4、ln re Gateway Learning Corp., 138 F.T.C. 443, 470 (2004) [hereinafter Gateway Decision & Order] (decision & order) (agreeing to pay $4,608 to U.S. Treasury as disgorgement)

5、The White House,Big Data:Seizing Opportunities,Preserving Values, 2014.05,

at 19-20

6、The White House,Consumer Data Privacy In a Networked World:A Framework for Protecting Privacy And Promoting Innovation In the GlobalDigital Economy, 2012.02, at 7

7、The United States President's Council of Advisors on Science and Technology(2014),Big Data and Privacy:A Technological Perspective 36,The White House,May 1

判決解釋：

1、Hubbert v. Dell Corp., 835 N.E.2d 113 (Ill. App. Ct. 2005)

2、Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 981 (E.D. Cal. 2000)

3、Ticketmaster Corp. v. Tickets.com, Inc., 2003 WL 21406289, at *2.

4、司法院大法官第 293 號解釋

5、司法院大法官第 585 號解釋

6、司法院大法官第 603 號解釋

7、台北地方法院 97 年度北小字第 313 號民事判決

8、台北地方法院 99 年度簡消上字第 1 號

9、台北地方法院 98 年度北消簡字第 13 號判決

10、台北地方法院 102 年度北小字第 2182 號民事判決

11、台北地方法院 104 年度北小字第 2548 號

12、台北地方法院 106 年度北小字第 2161 號民事判決

網路資料：

1、Are US insurers ready for a national GDPR-style privacy law?，https://www.insurancebusinessmag.com/us/news/breaking-news/are-us-insurers-ready-for-a-national-gdprstyle-privacy-law-116809.aspx

2、法務部個人資料保護專區，http://pipa.moj.gov.tw/mp.asp?mp=1

3、Federal Trade Commission , Privacy Online: A Report to Congress,1998, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

4、About the FTC，https://www.ftc.gov/about-ftc

5、What is a consent order? The legal jargon free guide，https://amicable.io/what-is-a-consent-order/

6、PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act，https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information

7、The FTC settles with Venmo over a series of privacy and security violations，https://techcrunch.com/2018/02/27/the-ftc-settles-with-venmo-over-a-series-of-privacy-and-security-violations/

8、為規避歐盟史上最嚴個資保護法，Facebook 將為 15 億用戶服務條款變更主體至美國，https://technews.tw/2018/04/24/facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law/

9、參防患未然！Facebook 停止與第三方數據公司合作，https://tw.news.yahoo.com/%E9%98%B2%E6%82%A3%E6%9C%AA%E7%84%B6-facebook%E5%81%9C%E6%AD%A2%E8%88%87%E7%AC%AC%E4%B8%89%E6%96%B9%E6%95%B8%E6%93%9A%E5%85%AC%E5%8F%B8%E5%90%88%E4%BD%9C-112005642.html

10、YouTube 於 5 月停止支持第三方廣告服務，將啟用 GDPR 政策，http://www.ifuun.com/a2018041612102032/

11、史上最嚴個資保護法下月上路，Facebook 家族如何打這場仗？，http://technews.tw/2018/04/26/instagram-data-download-tool-export-privacy-gdpr-compliance/

12、歐盟一般資料保護規，https://www.roc-taiwan.org/uploads/sites/124/2018/05/%E6%AD%90%E7%9B%9F%E4%B8%80%E8%88%AC%E8%B3%87%E6%96%99%E4%BF%9D%E8%AD%B7%E8%A6%8F%E7%AB%A0GDPR%E7%B0%A1%E4%BB%8B2.pdf

13、什麼是安全港架構(Safe Harbor Framework)？，http://jackforsec.blogspot.tw/2011/05/q-safe-harbor-framework.html

14、各國隱私法規與個資保護要求簡介，http://www.netadmin.com.tw/article_content.aspx?sn=1303110005&jump=2

15、Reforming the U.S. Approach to Data Protection and Privacy，https://www.cfr.org/report/reforming-us-approach-data-protection

16、Privacy Shield，https://www.privacyshield.gov/welcome

17、U.S., EU Reach Deal on New Data-Transfer Framework ，https://www.wsj.com/articles/u-s-eu-reach-deal-on-new-data-transfer-framework-1454429818

18、EU -.S. Privacy Shield - First annual Joint Review， https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

19、EU-US Privacy Shield data exchange deal: US must comply by 1 September, say MEPs ，http://www.europarl.europa.eu/news/en/press-room/20180611IPR05527/eu-us-privacy-shield-data-exchange-deal-us-must-comply-by-1-september-say-meps

20、Joint Press Statement from Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross on the Second Annual EU-U.S.

Privacy Shield Review，http://europa.eu/rapid/press-release_STATEMENT-18-6157_en.htm（

21、Privacy Shield under pressure as lawyers back MEPs' call for suspension，

https://www.theregister.co.uk/2018/07/16/privacy_shield_under_pressure_as_lawyers_back_meps_call_for_suspension/

22、行政院消費者保護委員會電子上物消費者保護綱領，

https://www.cpc.ey.gov.tw/cp.aspx?n=97E610626B9F499E

23、行政院消費者保護委員會，

https://www.cpc.ey.gov.tw/News_Content.aspx?n=3840722B002ADEAB&s=C24DA92907D96559

24、國家發展委員會個人資料保護專案辦公室，推定同意取得同意之方式，

https://www.ndc.gov.tw/Content_List.aspx?n=726A44EA5D724473