

附件二

新興通訊傳播數位平臺整合與應用之監理

期末報告

中華民國 110 年 12 月

## 目次

壹、緒論.....	2-1
貳、歐盟法制政策研析.....	2-2
一、數位平臺市場競爭.....	2-2
(一) 監管機關之態度與維持競爭之機制.....	2-2
(二) 資料應用對市場競爭之影響.....	2-23
二、數位平臺問責.....	2-31
(一) 安全港免責與平臺監理機制.....	2-31
(二) 強化數位平臺因應網際網路不法內容義務之策略.....	2-42
(三) 資料利用之法制政策.....	2-57
三、歐盟法制政策之啟示.....	2-60
參、英國法制政策研析.....	2-63
一、數位平臺市場競爭.....	2-63
(一) 監管機關之態度與維持競爭之機制.....	2-65
(二) 資料應用對市場競爭之影響.....	2-77
(三) 小結.....	2-85
二、數位平臺問責.....	2-86
(一) 數位平臺監理機制.....	2-86
(二) 網路危害內容處理對策.....	2-95
(三) 數位平臺資料蒐集、利用與保護規範.....	2-111
(四) 小結.....	2-122
三、英國法制政策之啟示.....	2-124
肆、美國法制政策研析.....	2-127
一、數位平臺市場競爭.....	2-127
(一) 監管機關之態度與維持競爭之機制.....	2-127

(二) 資料應用對市場競爭之影響.....	2-146
二、數位平臺問責 .....	2-163
(一) CDA 第 230 條之爭議與修法動態 .....	2-163
(二) FTC 就平臺隱私之問責 .....	2-175
三、美國法制政策之啟示 .....	2-176
伍、結論與建議 .....	2-178
一、各國管制歸納 .....	2-178
(一) 各國思維取向 .....	2-180
(二) 各國數位平臺市場競爭分析 .....	2-181
(三) 各國數位平臺問責分析 .....	2-182
二、我國法制政策建言 .....	2-185
(一) 數位平臺市場競爭部分 .....	2-185
(二) 各國數位平臺問責分析 .....	2-189
陸、參考文獻 .....	2-194

## 圖目次

圖 1：《數位服務法》草案累加義務示意圖 .....	2-38
圖 2：戰略市場地位監理機制架構圖 .....	2-64
圖 3：2009 - 2019 年美國搜尋引擎市場之市占率分布 .....	2-140

## 表目次

表 1：《數位市場法》草案所設之積極與消極義務 .....	2-11
表 2：行銷方法是否須取得個資同意一覽表 .....	2-120
表 3：各國管制歸納.....	2-178

## 壹、緒論

隨著數位經濟快速發展，數位平臺已成為當代民眾生活不可或缺之一部分，無論是社群媒體平臺、網路商店、應用程式商店或共享經濟平臺皆已和我們的食衣住行育樂密不可分。

擁有龐大使用者的大型數位平臺不只扮演著中介者的角色，也透過其整合能力將各式各樣的使用者、應用服務與內容相互串連，藉此蒐集大量的數據與資料。在數位經濟下，一旦大型數位平臺同時兼具極大的規模收益、網路外部性與資料量三項特徵時，即可造就範疇經濟，規模收益亦會隨之增加。隨著大型數位平臺化為無遠弗屆的虛擬公共空間，其競爭能力也將對經濟與社會帶來特殊影響，而有管理之必要。

觀諸近年國際社會對於數位平臺管制之探討，其趨勢主要有二，其一為資料市場之競爭，其二為資料運用之行為；近期亦陸續有對平臺業者問責管制架構為探討，以期數位平臺市場朝向更公平與更開放之方向發展。數位平臺整合與發展已成為近年先進國家在數位發展領域中重視之議題，而如何就此類平臺之管理內容、管理手段與平臺可能帶來之風險為新興應用之監理調和，亦應為我國相關監理機關應探討之課題，以保護數位平臺市場發展之完整性。主要國家經過多年的觀察研析，已經相當理解超大型數位平臺的市場力及影響力，對於超大型數位平臺的管制策略，也逐漸明朗化，我國數位市場也深受跨國超大型數位平臺的影響，對於主要國家的發展亦須持續探究，故本報告將針對歐盟、英國、美國之法制政策進行研析，以供我國監理機關政策擬定之參考。

## 貳、歐盟法制政策研析

觀測近年歐盟對於數位未來之政策走向<sup>1</sup>，可發現執委會積極於數位社會、數位科技、數位經濟等各面向，甚至國際合作推出新的政策，其中針對數位平臺，2019年歐盟便已宣示推動處理，數位單一市場發展，具有正向性的功能，以及建構明確、安全與信任的線上環境規範。以下就競爭與問責之兩大面向進行研析。

### 一、數位平臺市場競爭

#### (一) 監管機關之態度與維持競爭之機制

##### 1. 面對數位平臺之競爭執法挑戰

歐盟曾提出 2014 年至 2019 年歐盟「數位單一市場策略」(Digital Single Market Strategy for Europe)，其戰略建立在三大面向：為歐洲之消費者和事業提供更好的線上近用 (better online access for consumers and businesses across Europe)、為進步的數位網路和創新服務創造合理與公平的競爭環境 (creating the right conditions and a level playing field for advanced digital networks and innovative services)，以及極大化數位經濟之增長潛力 (maximising the growth potential of the Digital Economy)<sup>2</sup>。是為實現建立數位單一市場之目標，歐盟積極為數位時代監理工作進行立法規範。

---

<sup>1</sup> See European Commission, Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/en/policies> (last visited May 05, 2021).

<sup>2</sup> *Communication* from the Commission to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions: A Digital Single Market Strategy for Europe COM(2015) 192 final.

## (1) 數位平臺之特性

面對日益興盛之數位平臺，競爭主管機關也迎來挑戰。競爭法執法中最需處理之兩項關鍵前提要件，即係界定「相關市場」(Relevant market) 與衡量事業之「市場力量」(market power)。而因數位平臺具有雙邊或多邊的特色，對於相關市場之界定，若仍以傳統觀察供給與替代需求之價格變動及事業獲利變動之程度，則無法反映市場彼此連動之現實；對於市場力量之評估，若仍似過往單以事業在系爭產品或服務所在的單一市場中之指標(如市場占有率)衡量市場力量之高低，則將忽略具連動關係市場之競爭誘因影響，故計算所得之市場力量亦恐無法反映真實之市場競爭現狀<sup>3</sup>。

倘若以數位平臺所提供之功能區分，大致可歸納二種態樣：一為「交易平臺」(transaction platform)；二為「非交易平臺」(non-transaction platform)，新興通訊傳播數位平臺大部分為此類之服務平臺。而在說明歐盟對數位平臺之監理態度前，實有必要先行簡述兩種類型之定義，及衡量其競爭程度之方法與困境：

### A. 交易平臺

此類平臺係提供撮合 (matching) 使用者雙方交易之機會，如信用卡或拍賣平臺等，因此較有可能、也較有意願就網路效應之內部化進行協商。故競爭主管機關在確認存在網路效應後，仍需進一步判斷市場中是否有高協商成本或平臺所附加之限制存在，使得買賣雙方無

---

<sup>3</sup> 陳志民，支付系統競爭議題及規範架構之建立，公平交易季刊，第 27 卷第 3 期，頁 7 (2019)。

法透過協商將單邊較高之價格轉嫁至他邊市場，而價格差異之轉嫁程度與此類平臺屬於雙邊市場之可能性成反比<sup>4</sup>。

而由於交易平臺之交易雙方當事人具有「完成交易」之共同互動目的，則「雙邊」即屬平臺服務之必要部分，且彼此具有正向之網路效應，競爭主管機關較適宜以界定單一相關市場來涵蓋雙邊的連動效果，不必再分別對雙邊或多邊市場逐一界定，而可運用「微幅但顯著的非暫時性價格調漲」(small but significant non-transitory increase in price, SSNIP) 市場界定法，對平臺間替代性之高低加以認定<sup>5</sup>。

## B. 非交易平臺

此類平臺作用為引發交易雙方當事人(如瀏覽平臺資訊之消費者或廣告業者)之注意，如提供消費者搜尋及廣告主刊登廣告等。使用者之間並無直接的交易關係，故彼此通常無法得知，或必須承擔相當高之成本才可能知悉他方是否使用平臺。因此，較無法期待此類平臺的使用者之間具有直接協商內部化網路效應(Network Effect)之誘因，競爭主管機關在涉及此類平臺之案件中，只需評估是否存在網路效應、網路效應帶來的為正向(即單邊的使用人數增加會連動他邊的使用人數增加)或負向(即單邊的使用人數增加會造成他邊的使用人數減少)之影響，以及網路效應影響之程度，即可合理認定系爭平臺是否屬於雙邊市場之案件<sup>6</sup>。

對於此類平臺而言，在服務或產品對不同市場之使用人間，有不

---

<sup>4</sup> 同上註，頁 8-9。

<sup>5</sup> 同上註，頁 10-11。

<sup>6</sup> 同上註，頁 8-9。

同程度之替代可能性認定，諸如社群網路平臺、搜尋引擎平臺對消費者面向並不具有替代性，但就廣告主面向即有之，則縱為使用同一平臺，可能因不同邊之使用者對使用目的有不同期待，故平臺業者也未必需要在同一時間內讓多邊使用者得以進行互動才能充分發揮平臺之服務功能，遂對於非交易平臺，較適宜針對不同邊市場個別進行相關市場之界定，亦即，競爭主觀機關應就「每一邊市場」的價格變動對整體利潤（overall profits）之影響加以評估<sup>7</sup>。

而在操作上，在他邊市場價格不變之前提下，如為正向之網路效應，平臺因單邊市場漲價所減少之整體利潤將大於單邊市場本身所減少之利潤，此時 SSNIP 法則所界定之市場範圍，可視為是相關市場之下限（lower bound）；如為負向之網路效應，平臺因單邊市場漲價所減少利潤，或可因他邊市場需求增加而使整體利潤不降反升，此時 SSNIP 法則所界定之市場範圍，可視為是相關市場之上限（upper bound）<sup>8</sup>。

惟當此類平臺出現免費產品或服務時，可能使 SSNIP 法則受到侷限，假設競爭主管機關需判斷「免費」邊與「付費」邊之產品或服務可否納入同一相關市場，此時或可由「付費」邊進行 SSNIP 法則檢測，再觀察「免費」邊之加入程度界定出可能之市場範圍。然而，假設需判斷「免費」邊與「免費」邊之產品或服務可否納入同一相關市場時，SSNIP 法則即有調整必要，對此，有建議改採「微幅但實質且非瞬間之品質降低」（Small but Significant and Non-transitory

---

<sup>7</sup> 同上註，頁 9-10

<sup>8</sup> 同上註。

Decrease of Quality, SSNDQ) 加以評斷，因為該市場之競爭模式可能係產品或服務品質或創新能力等之非價格競爭，從而競爭主管機關可假設獨占者若降低其產品或服務品質（如平臺對隱私權保障之程度）達一定之程度，觀察使用者轉移至其他平臺之情形，將具有替代性之平臺的產品或服務納入相關市場之範疇<sup>9</sup>。

另外，數位平臺亦有多宿特性。數位平臺多宿（multi-homing）是指使用者傾向於利用多個競爭平臺服務之情形，這可自兩種角度加以觀察：

一為商業客戶（business users）端，諸如賣家、生產者、內容創建者、廣告主或酒店經營者等，此類使用者大多數亦會使用多個服務平臺，惟若其所提供的產品或服務之性質，具有獨特性而適合某一特定、專門之平臺（如 eBay 的二手車），則適合平臺單宿。此外，有鑑於為不同且不兼容之應用程式商店（Google Play、Apple APP Store）與開發應用程式之複雜性，超過半數之應用程式開發人員均為單宿（single-home）。另為最終用戶（end users）端<sup>10</sup>，諸如買家、消費者、食客、應用程式用戶等

多宿的特性可能有助於抵消網路效應，及降低大型數位平臺之經濟實力，亦得降低新興市場之參進障礙，進而促進創新之正面競爭效應。

---

<sup>9</sup> 同上註，頁 11-12。

<sup>10</sup> See Egidijus Barcevičius, Dovydas Caturianas, Andrew Leming & Gabija Skardžiūtė, *Multi-homing: Obstacles, Opportunities, Facilitating Factors*, in: EUROPEAN COMMISSION, STUDY ON “SUPPORT TO THE OBSERVATORY FOR THE ONLINE PLATFORM ECONOMY” (Final Report) Analytical paper #7, p.6 (2021).

## (2) 歐盟執委會之執法態度

歐盟執委會再三表示，面對數位平臺的確需要調整，但不會因此修改法規。但面對跨境性質之數位平臺，多頭監理（fragmentation）不利於歐盟數位服務單一市場及數位服務廣大之市場運作，且守門人（gatekeeper）數位平臺未必符合歐盟運作條約（Treaty on the Functioning of the European Union, TFEU）第 102 條所訂之濫用市場優勢地位之獨占者，故而有必要以歐盟層級之法規介入協調。因此，提出下章節討論之草案。

### 2. 《數位市場法》草案

近年來，跨國巨型數位平臺對歐盟的單一數位市場帶來了重大的衝擊性影響，歐盟執委會遂於 2020 年 12 月 15 日公布《數位部門競爭性與公平性市場之規章》草案，簡稱《數位市場法》（Digital Market Act, DMA<sup>11</sup>），以資應對。本草案之性質，在競爭法面向上，類似於美國法上公用事業（public utility）管制、與電信法上公共載具（common carrier）管制的融合形式，當中也包含了傳統反托拉斯法的原則，關注經濟上之失衡情形與不公平之商業行為<sup>12</sup>。

---

<sup>11</sup> Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final.

<sup>12</sup> 即將上任美國「聯邦貿易委員會」（Federal Trade Commission, FTC）委員的「新布蘭迪斯學派」（New Brandeis School）學者 Lina Khan 在其 2017 年的文章當中，即建議透過此種混搭的管制模式對處獨占性線上平臺。 See Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 797-802 (2017). 而其論點與建議與歐盟 DMA 有諸多趨同之處。

## (1) 草案規範架構

《數位市場法》草案分為六大章節，共計 39 條規範。第 1 章（第 1 條至第 2 條）為總則，敘明本法之規範主體、範疇與相關定義，以及針對特定國家內國法所制定之管制調和措施；第 2 章（第 3 條至第 4 條）為針對守門人所制定之規範，如具體定義之量化標準等；第 3 章（第 5 條至第 13 條）係守門人之積極與消極義務規範；第 4 章為（第 14 條至第 17 條）市場調查之程序性規範，諸如執委會的資訊調閱、面談與實地調查權限之規範；第 5 章（第 18 條至第 33 條）程序與執行之規範，諸如執委會資訊要求、現場檢查、採取臨時措施及制定具有拘束力之自願措施，以及對不遵守決定、違規行為或提供不正確、不完整或誤導性之調查資訊等之罰則規範；第 6 章（第 34 條至第 39 條）係其他一般性規範，諸如歐盟法院對罰鍰具有管轄權、本草案之生效與適用時間之規範等。

## (2) 劍指數位守門人

歐盟發現：在現今的數位市場之中，有部分大型數位平臺的服務業者從事濫用市場力之反競爭行為，故為營造歐盟單一數位市場優質之市場環境，以鼓勵創新應用之發展制定《數位市場法》草案作為歐盟單一數位市場的守門人規範，其主要規範目標，在於維護歐盟數位部門，在具有強大市場主導力量的巨型數位平臺業者發展影響下，能確保市場之公平性與競爭性發展，營造更適合創新者與新創公司的業務環境，避免核心平臺服務供應商濫用其市場力量，迫使企業用戶與消費者接受不公平的競爭限制及使用條款。

歐盟認為數位平臺之營業內容可分成兩種類型：核心平臺服務及附屬服務（即平臺之收益管道）。但不代表每個核心平臺服務之服務提供者都出現可競爭性（contestability）和不公平競爭。《數位市場法》草案之主要規管對象，尚須為受歐盟執委會依法指定納管為數位市場之線上守門人的「核心平臺服務」（core platform services）提供者，此類型服務受益於服務本身的網路效應，已具有高度之經濟規模，加之服務種類、型態因涉及多邊市場，對於整體市場已產生高度依賴，故已具備有高度之市場影響力，亦即已成為市場上企業與個人用戶間的守門人，甚至因此產生不利於數位平臺服務產業之市場競爭，亦不利於創新應用服務之推展，以及文化多樣性與媒體多元性等重要價值之維繫，故有必要進一步進行規管。

而《數位市場法》草案中所謂守門人平臺與《數位服務法》草案<sup>13</sup>中僅以使用者人數定義的「非常大型」（very large）平臺有所不同，則必須遵守新義務的「守門人」平臺，其構成要件有三<sup>14</sup>：

➤ **具備強大的經濟地位**：對於歐洲內部市場具有重要之影響力，具體舉例如前三個會計年度，在歐洲經濟區（European Economic Area, EEA）之總營業額達 65 億歐元（約新台幣 2,197 億元）或上一會計年度市值超過 650 億歐元（約新台幣 21,976 億元）之事業。

➤ **具有強大的中介能力**，可使企業觸及大量使用者：具體舉例如於歐盟境內每月向超過 4,500 萬名使用者提供服務。且至

---

<sup>13</sup> 詳後介紹。

<sup>14</sup> DMA, Art. 3.1-3.2.

少為 3 個歐盟會員國提供核心平臺服務。

➤ **目前或未來可擁有長久且穩固不變的市場地位：**意指達三年或三年以上之會計年度均符合上一款條件。

此外，若核心平臺服務符合上開草案所訂之構成要件門檻，應於三個月內通知執委會進行確認，而執委會亦應在收到服務提供者所提交之完整資料後的 60 日內，將符合要件之平臺指定為守門人<sup>15</sup>。

此外，倘若核心平臺服務提供者，提出充分論證其不符合第 1 項之要件，或雖符合第 1 項要件但不符合第 2 項要件，執委會亦得適用同條第 6 項所定之因素及該平臺將來可預見性之發展，透過市場調查對其加以評估，進而考慮是否將其指定為守門人<sup>16</sup>。

亦即，第 6 項賦予執委會可參考：a. 包含營業額 (turnover)、市值 (market capitalisation) 等多寡與核心平臺服務提供者之經營定位情狀；b. 觀察有多少企業用戶可藉由核心平臺服務提供者接觸到終端用戶及其數量；c. 基於網路效應及數據驅動 (data driven) 之優勢所導致之參進障礙，特別是服務提供者近用與蒐集並分析個人資料或非個人資料之能力；d. 服務提供者自規模 (scale) 與範疇 (scope) 效應中獲益情形，包含數據資料；e. 企業用戶或終端用戶套牢情形，以及 f. 其他市場結構性之特徵等因素，進行考量<sup>17</sup>。

因此，守門人平臺包含線上中介服務 (online intermediation services)、線上搜尋引擎 (online search engines)、社群媒體 (online

---

<sup>15</sup> DMA, Art. 3(3)-(4).

<sup>16</sup> DMA, Art. 3(6).

<sup>17</sup> DMA, Art. 3(6), para. 4.

social networking services)、視訊分享平臺 (video-sharing platform services)、非基於號碼之人際通訊服務 (number-independent interpersonal communication services)、操作系統 (operating systems)、雲端服務 (cloud computing services)、廣告服務 (advertising services) 等類型。

具體而言，例如：Facebook、Amazon、Apple、Google、Microsoft、Snapchat、阿里巴巴、字節跳動、Samsung、Booking.com，甚至 Android 或 iOS 之應用程式商店等，預期均屬本草案所欲規範之對象。

而為避免守門人有從事不公平競爭之行為，限縮消費者選擇自由，影響市場競爭秩序，其中《數位市場法》草案第 5 條為指定之守門人平臺無條件均應遵守之事項，第 6 條則是執委會可依照實際情形，額外課予規範對象應負擔之相關義務事項，整體而言，草案設置有多項積極、消極義務，本研究整理如下表。

表 1：《數位市場法》草案所設之積極與消極義務

條號	說明
第 5 條	<ul style="list-style-type: none"> <li>➤ 合併個人資料須徵得使用者同意之義務；</li> <li>➤ 允許企業用戶在平臺之外推廣其商品及服務並與客戶簽約；</li> <li>➤ 不應要求企業用戶使用、提供或共用身分辨識服務；</li> <li>➤ 不得以登入或訂閱其他核心平臺服務作為使用或登入守門人之服務的條件；</li> <li>➤ 不得阻礙或限制企業用戶向任何行政機關</li> </ul>

	<p>提出有關守門人之任何行為相關之問題；</p> <ul style="list-style-type: none"> <li>➤ 當應廣告主或出版人之請求，向其提供廣告服務之相關資訊。</li> </ul>
第 6 條	<ul style="list-style-type: none"> <li>➤ 避免使用企業用戶在平臺活動所生之非公開資料進行競爭；</li> <li>➤ 允許使用者移除任何預先安裝的軟體及 App，並允許安裝第三方軟體；</li> <li>➤ 避免在平臺排名上偏袒自家商品及服務，以與第三方供應商競爭；</li> <li>➤ 向投放廣告的公司提供必要工具及資訊，以利廣告商與發布者獨立驗證由守門人託管的廣告；</li> <li>➤ 促進資料可攜性；</li> <li>➤ 線上搜尋引擎應對免費或付費用戶以公平、合理且無歧視之條件，生成與搜尋相關之排名、查詢、點擊和查看數據，並對構成個資之查詢、點擊和查看數據進行匿名化處理。</li> </ul>
第 7 條	<ul style="list-style-type: none"> <li>➤ 有確保遵守規範而採取因應措施之義務。</li> </ul>
第 8 條	<ul style="list-style-type: none"> <li>➤ 執委會可在例外情況下，由守門人負舉證之責，決定中止其負擔第 5 條和第 6 條所訂的全部或一部之義務。</li> </ul>
第 9 條	<ul style="list-style-type: none"> <li>➤ 執委會可得限於因公共道德、衛生及安全之公共利益而免除全部或一部之義務。</li> </ul>
第 10 條	<ul style="list-style-type: none"> <li>➤ 配合執委會為解決限制競爭或不公平競爭之行為所更新之義務</li> </ul>
第 11 條	<ul style="list-style-type: none"> <li>➤ 不得為阻礙使用者行使連結至平臺以外的企業之選擇權而提供條件或品質較差的核</li> </ul>

	心平臺服務。
第 12 條	➤ 收購計畫的結合申報義務。
第 13 條	➤ 受指定為守門人後，應提交審計之說明，並應至少每年更新 1 次。

資料來源：DMA，本計畫製作

此外，草案並設有相當嚴苛之裁罰機制，具體包含：前一會計年度總營業額 10% 之罰鍰<sup>18</sup>；針對 5 年內遭裁罰 3 次以上之「系統性違法」(systematic non-compliance)，將適用業務分離等結構性矯正措施等<sup>19</sup>。

歐盟對《數位市場法》草案寄予厚望，一向對數位平臺巨擘不假辭色的歐盟執委會競爭事務執行委員 Margrethe Vestager 便曾指出，《數位市場法》草案可能會迫使美國科技巨頭改變其利潤豐厚的商業模式，並確保為較小的競爭對手提供公平的競爭環境。

近期，有歐洲議會議員表示，《數位市場法》草案所針對者應該僅有美國的科技巨頭，即控制 Facebook、Google、Amazon 和 Apple 之市場力。而未免歐盟或亞洲之大型數位科技公司落入適用範疇，其表示：年總營業額之門檻應提高至 100 億歐元(約新台幣 3,381 億元)，上一會計年度市值至少應提高至 1,000 億歐元。從而確實針對那些毫無疑義扮演守門人角色的平臺。此外，其認為歐盟競爭主管機關執法者應該有能力在一個月內指定哪些守門人應遵守規則，而不是草案中

<sup>18</sup> DMA, Art. 26.

<sup>19</sup> DMA, Art. 16.

所擬的三個月期限<sup>20</sup>。

### 3.從個案觀察歐盟競爭執法趨勢

歐盟對於數位平臺之競爭層面，近年來逐漸重視結合所帶來促進競爭或反競爭的影響，尤其是以數據驅動為核心之大型科技公司所為之結合案例類型，像是 2014 年 *FacebookWhatsApp* 案<sup>21</sup>、2016 年 *Microsoft/LinkedIn* 案<sup>22</sup>、2018 年 *Apple/Shazam* 案<sup>23</sup>、2020 年 *Google/Fitbit* 案<sup>24</sup>和 2021 年 *Facebook/Kustomer* 案<sup>25</sup>等，均屬是類。

#### (1) 與 Facebook 有關之結合案

##### A. Facebook 與 WhatsApp 結合案

Facebook 繼 2012 年收購 Instagram 後，2014 年再度宣布以 190 億美元（約新台幣 5,814 億元）收購 WhatsApp，WhatsApp 此後成為 Facebook 完全控制之全資子公司。但仍繼續獨立作業，並保留該品牌名稱。

歐盟擔憂，因 Facebook 為多邊平臺（multisided platform），平臺彼此間會針對使用人數、資料或付費廣告從事競爭，雖 WhatsApp 未蒐集用戶資料，但以資料驅動之結合，未必是著眼於結合當時現存的

---

<sup>20</sup> CPI, EU MP Says Tech Rules Should Target Only Dominant Firms (2021/06/01), [https://www.competitionpolicyinternational.com/eu-mp-says-tech-rules-should-target-only-dominant-firms/?utm\\_source=CPI+Subscribers&utm\\_campaign=99f38a9cf9-EMAIL\\_CAMPAIGN\\_2021\\_06\\_01\\_09\\_24&utm\\_medium=email&utm\\_term=0\\_0ea61134a5-99f38a9cf9-237199592](https://www.competitionpolicyinternational.com/eu-mp-says-tech-rules-should-target-only-dominant-firms/?utm_source=CPI+Subscribers&utm_campaign=99f38a9cf9-EMAIL_CAMPAIGN_2021_06_01_09_24&utm_medium=email&utm_term=0_0ea61134a5-99f38a9cf9-237199592) (last visited June 02, 2021).

<sup>21</sup> *Facebook / WhatsApp*, Case NoCOP/M.7217 (C297 of 04.09.2014).

<sup>22</sup> *Microsoft / LinkedIn*, Case M.8124 (C388 of 21.10.2016).

<sup>23</sup> *Apple / Shazam*, Case M.8788 (C106 of 21.03.2018).

<sup>24</sup> *Google/Fitbit*, Case M.9660 (C210 of 24.06.2020).

<sup>25</sup> *Facebook/Kustomer*, Case M.10262 (C258 of 02.07.2021).

產品或服務市場，而是看中具有競爭價值的資料或取得具競爭價值資料之技術、能力或機會。Facebook 縱未將 WhatsApp 所擁有的用戶資料與資料分析作為商品或服務，惟不排除結合後，Facebook 將透過 WhatsApp 推出廣告服務與蒐集用戶資料，從而改善其定向廣告之正確性，以俾爭取更多的廣告收益<sup>26</sup>，從而導致 WhatsApp 原有的服務品質（隱私權保護、資訊安全等）降低。

執委會對此案<sup>27</sup>區分三個相關市場進行探討：首先，在「消費者通訊服務」市場中，雖 Facebook Messenger 和 WhatsApp 在 EEA 甚至全球均具有顯著市場地位，惟用戶的轉換成本（switching cost）極低，因此極易抵消結合後之 Facebook 利用其優越的市場地位所為之任何嘗試，亦即，若 Facebook 在結合後想以付費方式提供服務或停止創新，則用戶可以輕鬆地轉向會提供免費服務和可提供新功能和更高質量服務的競爭者，故執委會認為本次結合在動態競爭之消費者通訊服務市場中不具有反競爭的影響。

其次，在「社群網路服務」市場中，雖市場上所擔憂透過整合 WhatsApp 將更多的用戶和或功能添加到 Facebook 社群網路服務中，可能有助於增強 Facebook 在社群網路服務潛在市場中的地位。但執委會考量二平臺之整合可能存在重大技術障礙，且需要用戶協助，將有流失用戶的可能性；且基於服務體系結構的差異，啟用跨平臺服務台需要進行實質性的重新設計並編寫代碼等情，加上 Facebook 表示目前並未有整合計畫，執委會認定本結合案對社群網路服務市場並無

---

<sup>26</sup> 陳志民，大數據與市場力濫用行為初探，公平交易季刊，第 26 卷第 3 期，頁 18（2019）。

<sup>27</sup> 同前註 21。

嚴重的反競爭影響。

最後，在「線上廣告服務」市場中，執委會認為 Facebook 從同時擁有二者帳戶的用戶處搜集資料並將其用於 Facebook 的投放廣告上，首先需要更改 WhatsApp 的隱私政策<sup>28</sup>。加上整合二者的用戶個人資料，Facebook 認為目前存在重大的技術障礙，且改變隱私政策對 WhatsApp 的原有用戶而言，有很高的可能性促使其轉向替代的競爭應用程式，從而降低 Facebook 自 WhatsApp 蒐集用戶個人資料的誘因。是以，只有在 Facebook 控制範圍內的資料集中度使其能夠增強其在廣告中的地位時，該交易才會引起競爭擔憂，且執委會認為，本次收購案宣布時，市場上仍有大量參與者與 Facebook 一起收集用戶個人資料<sup>29</sup>，且越來越多平臺重視且願意以個人資料之「隱私權保障」作為非價格競爭（提供免費服務之故）要素，故執委會認定結合的集中度未對線上廣告服務市場帶來反競爭的影響。

不過，雖然歐盟執委會在 2014 年通過 Facebook 與 WhatsApp 的結合案，但於 2017 年執委會卻因本案對 Facebook 祭出罰鍰，理由是基於違反《歐盟結合規章》（EC Merger Regulation<sup>30</sup>）中，提供即時有

---

<sup>28</sup> 有受訪者建議 Facebook 可以提高 WhatsApp 的訂閱費用，從而將 WhatsApp 的用戶切換到 Facebook 以增加 Facebook 用戶數，進而增加 Facebook 的廣告收入和/或相對於廣告市場力量。惟執委會發現 WhatsApp 並不是 Facebook Messenger（更不用說 Facebook 社群網路）的高度替代性競爭對手。無論如何，縱使增加 WhatsApp 的訂閱費，並且用戶果真切換至 Facebook，市場調查表明仍舊有足夠數量的線上廣告服務替代供應商存在。

<sup>29</sup> 諸如 Apple、Amazon、eBay、Microsoft、AOL、Yahoo!、Twitter、IAC、LinkedIn、Adobe 和 Yelp 等公司，總之，網路上這些將會繼續存在之大量的對廣告目的有價值之用戶個人資料，並不在 Facebook 的專有控制範圍之內。惟執委會審酌替代可能性時，將線上廣告市場之服務類型與對象完全不同的 Google、Yahoo!、MSN，甚至是不同的平臺性質的 Apple、Amazon、eBay、Microsoft、AOL 等納入考量，即為有疑。參見邱映曦，競爭法的數位紀元—論數位平臺資訊力對競爭法適用之影響，國立政治大學法律學系博士班博士學位論文，頁 56（2019）。

<sup>30</sup> Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation).

效地審查結合和收購必要之正確資訊的義務，這也是自 2004 年《歐盟結合規章》生效以來，執委會首次根據該規章對提供不正確或誤導性資訊之事業處以罰鍰<sup>31</sup>。

而執委會認為 Facebook 在 3 年前調查結合案之期間提供不正確或誤導性之資訊，是指 Facebook 曾稱，不會對 Facebook 和 WhatsApp 的用戶進行自動匹配，但卻在 2016 年調整 WhatsApp 的隱私政策，允許 WhatsApp 與 Facebook 分享部分用戶的手機號碼，且 2014 年分明已存在自動匹配技術之可能性<sup>32</sup>。

針對此提供不正確或誤導性資訊事件，並不影響結合案之決定，且歐盟得裁罰之最高上限本應為年營業額之 1%（2016 年 Facebook 年營業額之 1% 為 2.48 億歐元，即約新台幣 82 億元），但考量 Facebook 於調查期間合作態度良好且承認疏失，便酌予減輕額度至 1.1 億歐元（約新台幣 36.3 億元）<sup>33</sup>。

## B. Facebook 與 Kustomer 結合案

Facebook 為擴大 WhatsApp 之規模，在 2020 年 12 月宣布以 10 億美元（約新台幣 300 億元）收購名為 kustomer 的新創公司，雖然英國之競爭主管機關－競爭與市場管理局（Competition and Markets Authority, CMA）認為二者結合未對英國之市場帶來反競爭效果，故於 2021 年 9 月 27 日通過此案，惟此收購仍受到世界各國主管機關之

---

<sup>31</sup> European Commission, Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover, Press Release (2017/05/18), [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_17\\_1369](https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369) (last visited June 03, 2021).

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

關注，亦包含美國、歐盟<sup>34</sup>及歐盟會員國之一的德國。

承上案例可知，Facebook 旗下擁有 Messenger、WhatsApp 及 Instagram 三個訊息渠道，為消費者提供社群網路、通訊，以及照片與視訊分享功能之服務。而於 2015 年成立之 Kustomer 則是兜售客戶關係管理（Customer Relationship Management, CRM）支援工具平臺與 AI 客服（即 Kustomer IQ）功能之企業，用以透過電話、電子郵件、簡訊或線上即時通訊軟體提供客服，除能節省大幅人工客服成本外，亦能提供 24 小時線上 AI 客服服務。

而 Facebook 可透過 Kustomer 之 CRM 功能，統一管理旗下各平臺之客戶服務，進而搶攻電子商務市場（如 Facebook、Instagram 所推出之 Shop 功能）之地位，甚至透過 Kustomer 之消費者數據，優化廣告個人化及定向投放之精準度，增強線上廣告市場之競爭優勢，並藉此吸引更多的廣告主於其介面上投放更多的廣告資源，這對幾近 99% 之收入源自於廣告之 Facebook 的重要性，自不待言<sup>35</sup>。

歐盟執委會於 2021 年 6 月收到數會員國請求調查本案市場集中度之聲請，執委會在採取調查之際，初步認為進行價值較低之交易，或許不致使 Facebook 受到反競爭疑慮之審查，惟仍十分擔憂此可能是阻礙競爭之殺手級併購（killer acquisitions），亦即 Facebook 可能一

---

<sup>34</sup> 段智恆，臉書收購案傳喜訊 併 Kustomer 獲英國 CMA 批准，anue 鉅亨網（2021/08/03），<https://news.cnyes.com/news/id/>（最後瀏覽日：2021 年 10 月 20 日）。

<sup>35</sup> 段智恆，臉書「殺手併購」Kustomer 疑壟斷之嫌 歐盟監管機構展開調查，anue 鉅亨網（2021/08/03），<https://news.cnyes.com/news/id/>（最後瀏覽日：2021 年 10 月 20 日）；陳怡伶，強化電商體驗，臉書收購 CRM 新創 Kustomer，TechOrange 科技報橘（2021/09/28），<https://buzzorange.com/techorange/2021/09/28/crm-facebook-startup/>（最後瀏覽日：2021 年 10 月 20 日）。

方面妨害競爭對手使用旗下 Messenger、WhatsApp 及 Instagram，另一方面透過自各該服務所掌握之數據以鞏固其優勢地位，終而扭曲「CRM 軟體供應/克服與支援 CRM 軟體供應」(supply of CRM software/ supply of customer services and support CRM software) 市場及「線上展示廣告服務」(online display advertising services) 市場之競爭，該調查結果則預計於 2021 年 12 月出爐<sup>36</sup>。

### C. 德國對 Facebook 之執法情形

歐盟會員國之一的德國，近年積極對數位平臺之反托拉斯執法。Facebook 創建內部早鳥預警系統，倘若偵測到可能將造成威脅的新創事業，則會以模仿或收購之方式排除潛在競爭，至今 Facebook 已收購包含 WhatsApp、Instagram、Lightbox 等超過 50 家網路社群服務平臺<sup>37</sup>，依據德國競爭主管機關即聯邦卡特爾署 (Bundeskartellamt) 歷經 3 年之 Facebook 數據蒐集式調查，Facebook 在德國擁有每日經常用戶 2,300 萬人次、每月經常用戶 3,200 萬人次，於社群平臺之市占率超過 80%，在相關市場的認定中，因 Google+ 已宣布於 2019 年 4 月關閉其社群網路，而 Snapchat、YouTube、Twitter、LinkedIn 或 Xing 等社群網路平臺因提供消費者之產品或服務之定位不同，因而不在此競爭者之列，遂 Facebook 在德國社群網路平臺市場確實具有優勢支配

---

<sup>36</sup> Facebook/Kustomer, Case M.10262 (C258 of 02.07.2021); European Commission, Mergers: Commission opens in-depth investigation into proposed acquisition of Kustomer by Facebook, Press Release (2021/08/02), [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_4021](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4021) (last visited Oct. 21, 2021).

<sup>37</sup> 陳志宇、巫國豪、余曜成、程致剛、楊東穎、廖祥丞，推動數位經濟發展之通訊傳播匯流政策及法制革新計畫－促進資料自由流通機制及應用趨勢研究計畫，國家通訊傳播委員會委託之計畫成果報告，頁 10 (2019)。

地位<sup>38</sup>。

根據 Facebook 案時之用戶服務契約條款，用戶必須同意 Facebook 在網際網路或智慧手機 APP 等蒐集整併不同來源數據，方得使用其社群網路平臺與服務，因 Facebook 市占率極高，其以個人用戶身分為基礎所衍生之網路效應，對用戶產生套牢（lock-in）效果，使得用戶難以轉換至其他社群網路平臺，亦對其他競爭者產生參進障礙。對此，德國聯邦卡特爾署認為 Facebook 除能透過「Facebook 企業管理平臺工具」逕行處理自身平臺用戶之數據資料，更能蒐集整合旗下 WhatsApp、Instagram 及第三方網站上之服務數據資料，用以招徠廣告主，且對用戶進行目標行銷，已構成「剝削式」濫用市場優勢地位之行為。甚至因不當掌控及處理大量用戶之個人資料，亦有《一般資料保護規章》（Regulation (EU) 2016/679, GDPR<sup>39</sup>）之規定<sup>40</sup>。

故德國聯邦卡特爾署在 2019 年初，依據德國《限制競爭防制法》（Gesetz gegen Wettbewerbsbeschränkung, GWB）第 19a 條決定限制 Facebook 不得將其經營的多種服務中的用戶資料集合整併在一起。德國聯邦卡特爾署要求 Facebook 在 1 年內修改資料處理政策，亦即，若未取得用戶自願同意，數據僅得保留在原有服務當中，不得擅自蒐集整理分析；且若用戶不同意整併蒐集資料，Facebook 亦不得基此拒

---

<sup>38</sup> 許祐寧，德國聯邦卡特爾局限制 Facebook 蒐集整併不同來源的用戶數據以防壟斷，科技法律透析，第 31 卷第 5 期，頁 2（2019）。

<sup>39</sup> GDPR of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

<sup>40</sup> 徐曼慈，德國聯邦卡特爾署決定禁止 Facebook 濫用市場力不當處理用戶資料之行為，公平交易委員會電子報，第 122 期，頁 1-3（2019）。

絕提供社群網路服務；或是在 4 個月內另行提出可行方案<sup>41</sup>。Facebook 已提出訴訟，該案目前仍有待德國法院之最終審理結果出爐。

無獨有偶，2020 年 12 月德國聯邦卡特爾署再度因為登錄 Oculus 之虛擬裝置 Quest 2，只能通過 Facebook 帳號才能使用，進而對其展開是否濫用其市場地位之調查<sup>42</sup>，該案涉及 2021 年 1 月 19 日生效的《GWB 數位化法案》（GWB-Digitalisierungsgesetz）<sup>43</sup>，而 Facebook 所形成之生態系統遍及各個市場，身為數位市場至關重要的平臺，其可能將會是德國聯邦卡特爾署運用新法案事先干預市場競爭之首例<sup>44</sup>。

在繼 Google、Apple 和 Amazon 提起訴訟後，今（2021）年歐盟也可能因對 Facebook 利用其市場力量而加強不公平競爭優勢 Facebook 而展開首次反托拉斯調查<sup>45</sup>，後續發展值得繼續觀察。

## （2）與 Google 有關之結合案

以 2020 年之 Google 與 Fitbit 之結合案<sup>46</sup>為例，Google 透過提供不同的資訊服務，有效蒐集使用者資料（如個人資料、消費習慣、交易紀錄等），且在全球設有 16 個資料中心，以此強大的數據蒐集與分

---

<sup>41</sup> 許祐寧，同前註 38，頁 3-4。

<sup>42</sup> See BBC NEWS, Oculus Facebook account row prompts German competition probe, <https://ec.ltn.com.tw/article/breakingnews/3379638> (last visited May 17, 2021).

<sup>43</sup> 本次修法全稱為「修正限制競爭防制法以建構集中性、主動性與數位化的第 4 代競爭法與其他規定法案」，可參見林家暘，德國 2021 年限制競爭防制法數位化改革分析，臺灣法學雜誌，第 412 期，頁 127-142（2021）。

<sup>44</sup> See Viola C. Didier, Facebook: Bundeskartellamt prüft den neuen § 19a GWB, DER BETRIEB, <https://www.der-betrieb.de/meldungen/facebook-bundeskartellamt-prueft-den-neuen-%C2%A7-19a-gwb/> (last visited June 01, 2021).

<sup>45</sup> See CPI, Facebook May Face New EU Antitrust Probe, <https://www.competitionpolicyinternational.com/facebook-may-face-new-eu-antitrust-probe/> (last visited May 17, 2021).

<sup>46</sup> 同前註 24。

析能力，提供精準的廣告投放<sup>47</sup>，在全球均具有極大的市場競爭優勢。

Fitbit 則是著名的穿戴式裝置公司，在穿戴式裝置市場中，<sup>48</sup>而其所開發之 App 已具備健康指標儀表，可幫助用戶追蹤個人健康趨勢，諸如藉由膚電活動 (electrodermal activity, EDA) 感測器以管理壓力、心電圖 (Electrocardiography, ECG) 分析心房顫動 (Atrial fibrillation, Afib) 跡象、偵測心率變化、呼吸頻率以及血氧飽和度 (SpO2) 等，可串聯用戶之活動、心臟健康、睡眠紀錄等資料。

歐盟擔憂 Google 的線上搜尋和廣告投放服務，將會透過 Fitbit 而建立更加全面的用戶資料蒐集，透過掌握更多的數據以提高潛在競爭對手之參進障礙<sup>49</sup>。

而 Google 於 2021 年 1 月 14 日宣布，以 21 億美元 (約新台幣 578 億元) 完成 Fitbit 之收購，其強調本次結合案始終與裝置有關，而非數據，藉由 Google 所擅長的軟硬體與人工智慧 (AI) 技術高度整合以持續開發對用戶健康有利之新的產品與服務。再三表明 Google 自始承諾將會保護 Fitbit 用戶的隱私與安全，並將與全球監理機關合作，確保 Google 廣告不會利用 Fitbit 用戶之健康數據，且健康數據將與其他 Google 廣告數據分開，亦將繼續允許 Fitbit 用戶自行將第三方

---

<sup>47</sup> 陳志宇等，同前註 37。

<sup>48</sup> 當時根據 Strategy Analytics 市場調查公司於 2019 年所公布之數據來看，Apple 旗下的 Apple Watch 於全球智能手錶市場之市占率為 46% 而名列第一，其次為 Samsung，至於 Fitbit 則為第三。See Neil Mawston, Apple Watch Takes 46% Smartwatch Share in Q2 2019, STRATEGY ANALYTIC, <https://www.strategyanalytics.com/strategy-analytics/blogs/devices/wearables/wearables/2019/08/06/apple-watch-takes-46-smartwatch-share-in-q2-2019> (最後瀏覽日：2021 年 05 月 27 日)。

<sup>49</sup> See European Commission, *Mergers: Commission opens in-depth investigation into the proposed acquisition of Fitbit by Google*, Press Release (2020/08/04), [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_1446](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1446) (last visited June 08, 2021).

健康或健身 App 服務與 Fitbit 帳號進行連動<sup>50</sup>。

總言之，Google 對歐盟所承諾有關網路應用程式介面之取用、腕戴式穿戴式裝置之發展，甚至廣告投放技術等，均類似於《數位市場法》草案中賦予守門人之義務。

## （二）資料應用對市場競爭之影響

承上，歐盟一方面加大對市場競爭之監理力度，一方面也深刻體認到經濟活動越來越仰賴數據資料，數據資料可為現有的服務創造顯著的附加價值，並促進嶄新的商業模式。因此，歐盟希望形成讓各種類型數據資料接得以在歐盟自由流通之全面性法律框架，也即讓「資料」流通自由，成為歐洲單一市場所追求之繼人員、貨品、服務和資本後的第五自由<sup>51</sup>。

### 1. 資料自由流通以活絡經濟

#### （1）GDPR 強化個人資料可攜權利

歐盟為保護個人資料，自 1995 年便發布《個人資料保護指令》（Directive 95/46/EC）<sup>52</sup>，然隨著資通訊科技發展，該指令面對網際網

---

<sup>50</sup> See Rick Osterloh, *Google completes Fitbit acquisition, Google: The Keyword*, <https://blog.google/products/devices-services/fitbit-acquisition/> (last visited May 28, 2021). 陳冠榮，Google 完成 Fitbit 收購案，再三強調保護用戶隱私、健康數據不用於廣告，TechNews 科技新報，<https://technews.tw/2021/01/15/google-completes-fitbit-acquisition/>（最後瀏覽日：2021 年 05 月 28 日）。

<sup>51</sup> 吳彥容，簡評歐盟強化資料自由流通之新規則—以非個人資料之流通為中心，經貿法訊，第 245 期，頁 20（2019）。

<sup>52</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.

路等各項應用之迅速崛起變遷已難以為繼，遂幾經討論與修正，於 2016 年通過並發布《一般資料保護規章》(GDPR) 取代《個人資料保護指令》<sup>53</sup>，並自 2018 年 5 月 25 日起施行，GDPR 亦設有行政罰規範，甚至以事業之全球營業額作為計算罰鍰的基礎<sup>54</sup>。

GDPR 之效力及於歐盟各會員國及歐洲經濟區，亦即在此領域內所取得之個人資料，原則上禁止移轉至此領域之外<sup>55</sup>。而所謂「個人」係指包含進入當地市場之事業在當地聘用之員工、從歐盟境外派遣之駐點人員在內之為於歐盟境內的所有人<sup>56</sup>。

GDPR 之規範主體包括政府機關（涉及外交、防衛、警察則不在此限）、地方自治團體、非營利法人，以及營利之事業，且中小或微型事業亦有適用，業者縱使僅透過網際網路為歐盟境內消費者提供產品或服務，而取得或傳輸為於歐盟境內之消費者資訊時，即可能成為適用對象，不必確有在當地設置法人、分公司或派駐人員，但必須在歐盟境內選任代理人，亦即，GDPR 將適用範圍擴及至歐盟以外之地域（extra-territorial applicability），不但所有在歐盟境內之公司處理資料時，須遵循 GDPR 之規範，若於歐盟境外處理歐盟境內之資料時，亦須遵循 GDPR 之規範，以確保達成 GDPR 之實質效力<sup>57</sup>。

GDPR 主要目標，便是冀以制訂統一之數據人權規範，以取回幾乎完全由大型事業（尤其是美國之數位平臺）所獨占之個人資料控制

---

<sup>53</sup> GDPR, Art. 94.

<sup>54</sup> GDPR, Art. 83.

<sup>55</sup> GDPR, Art. 4(1).

<sup>56</sup> 陳志宇等，同前註 37，頁 160-161。

<sup>57</sup> 陳志宇等，同前註 11，頁 160-。

權。而可識別之資料以往係指單純的姓名、性別、電話號碼、住址、身分證字號等，對此 GDPR 擴大保障之個人資料範圍，即係「個人可識別資料」(Personally Identifiable Information, PII) 均屬之，故對其定義係指任何相關於 (identified) 或足資識別 (identifiable) 之自然人，而可識別之自然人則指可以直接或間接地透過識別符號 (identifier)，或經由一個或多個具體的身體、生理、基因、心理、經濟、文化、醫療紀錄或社會身分因素所識別出之特定自然人，而識別符號，可以是姓名、識別號碼、位置資料或線上識別碼等。GDPR 進一步闡釋<sup>58</sup>可追溯特定自然人之線上足跡得線上識別碼，其作用在於自然人可能與其使用之設備、應用程式、工具和協定提供之連線識別碼相關聯，諸如網路協定位址、cookie 識別碼或其他 (如無線射頻識別標記等)，尤其是當伺服器接收具獨特性識別碼與其他資訊結合使用時，可用以創建個人檔案並加以識別特定之個人<sup>59</sup>。

GDPR 所保障之權利重要的有「近用權」(Right to Access)<sup>60</sup>、「被遺忘權」(Right to be forgotten)<sup>61</sup>、「隱私納入設計與設計由隱私出發」(Privacy by Design and by Default)<sup>62</sup>、「資料侵害通知」(Breach Notification)<sup>63</sup>，而歐盟為了讓民眾對自身之個人資料有更大的控制權，在 GDPR 的規範中，也首度明訂「資料可攜權」(Right to Data Portability)<sup>64</sup>，即歐洲民眾在不同服務平臺業者之間，享有自由移轉

---

<sup>58</sup> GDPR, Recital (30).

<sup>59</sup> 張陳弘、莊植寧，新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明，新學林出版股份有限公司，頁 20-21 (2019)。

<sup>60</sup> GDPR, Art. 15.

<sup>61</sup> GDPR, Art. 17.

<sup>62</sup> GDPR, Art. 25.

<sup>63</sup> GDPR, Art. 31.

<sup>64</sup> GDPR, Art. 20.

個人資料的權利。

有關資料可攜權，GDPR 規定當個人資料蒐用之情形屬於 A. 係基於資料主體之同意或係基於履行契約所必要；B. 係以自動化方式為之者時，資料主體有權接收其提供予資料管控者之個人資料；資料管控者需以結構化的、常用的、機器可讀的形式提供，資料主體並有權將之傳輸給其他資料管控者，而不受提供個人資料之管控者的妨礙。在技術許可之情形下，資料主體應有權要求其個人資料得毋需經過資料主體的轉送，而直接由資料管控者處傳輸至其他資料管控者<sup>65</sup>。而為確保或有利執行 GDPR 規定資料可攜權之要求，資料管控者相互間應發展便利於相互資料移轉、交換之相容格式(尤其是電子格式)。對此，Facebook、Google、Microsoft 與 Twitter 於 2018 年跨平臺共同推出「資料傳輸計畫」(Data Transfer Project)，包含「想要使用新服務」、「想要離開現有服務」、「想要備份資料」等三種使用者最適合使用資料傳輸計畫之服務，創建開源資料可攜之平臺，以利所有使用者可在不同服務之間自由的移轉聯絡資訊、健康紀錄、音樂播放清單、相片與影片等內容與資料<sup>66</sup>。而 2019 年又加入 Apple、法國串流音樂服務 Deezer、新興社群平臺 Mastodon 及 Berners-Lee 發起的 Solid 專案<sup>67</sup>，該計畫現有 18 個貢獻組織，迄今加入超過 4.2 萬行程式碼，變更檔案超過 1,500 個，並加入如雲端紀錄和監控等框架功能，以利事

---

<sup>65</sup> 張陳弘、莊植寧，同前註 59，頁 205。

<sup>66</sup> 陳君毅，巨頭聯手！Facebook、Google、微軟要將個人資料所有權還給使用者，數位時代，<https://www.bnext.com.tw/article/49966/the-data-transfer-project> (最後瀏覽日：2021/06/06)。

<sup>67</sup> 林妍臻，蘋果加入 Google、臉書、微軟合推的資料可攜計畫 Data Transfer Project，iThome 電腦報，<https://www.ithome.com.tw/news/132164> (最後瀏覽日：2021/06/06)。

業開發新功能時使用資料傳輸項目<sup>68</sup>。

## (2) 促進非個人資料之資料流通

為了充分釋放數位經濟的好處，歐盟執委會便須確保非個人資料（non-personal data）之自由流通，允許事業或公共行政機關得以在歐盟境內之任何地方儲存與處理數據資料<sup>69</sup>。

然而，為因應號稱史上最嚴格之個資法 GDPR，使得全球事業都不免於受到其效力之震盪，因此，歐盟欲藉由《非個資流通規章》避免歐盟各會員國內之主管機關強制將數據資料在地化的不合理限制，及導致消費者轉換服務提供者（包含雲端儲存）困難等情事，而使中小企業與新創事業能因本規章而更易於開發創新服務，進而提高事業之法律明確性和信任度<sup>70</sup>，故《非個資流通規章》係為補充 GDPR 而制定，二者不存在相互矛盾（no contradictory）之義務。

歐盟於 2018 年 11 月 28 日通過《促進非屬個人資料之資料流通規章》（Regulation (EU) 2018/1807，下簡稱《非個資流通規章》）<sup>71</sup>，藉以促進歐洲單一數位市場之規模經濟發展，本規章於 2019 年 05 月 28 日開始施行。據此，歐盟執委會亦於翌日因應本規章而頒布《歐盟非個人資料自由流通架構規章指引》<sup>72</sup>（下稱《非個資流通指引》），

---

<sup>68</sup> Data Transfer Project, Current State, <https://datatransferproject.dev/updates> (last visited June 06, 2021).

<sup>69</sup> European Commission, Free flow of non-personal data, Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data> (last visited May 20, 2021).

<sup>70</sup> *Id.*

<sup>71</sup> Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

<sup>72</sup> European Commission, Communication from the Commission to the European Parliament and the Council Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM(2019) 250 final.

以釐清本規章與 GDPR 之互動關係<sup>73</sup>。

《非個資流通規章》及《非個資流通指引》之主要重點如下<sup>74</sup>：

#### A. 非個人資料之判斷

非個人資料之定義係以反面定義之方式加以規範，但凡不屬於 GDPR 所規範之個人資料，即屬非個人資料<sup>75</sup>。其主要類型有二，一為「資料自始不會涉及已能識別或足資識別的自然人」，例如在風力發動機上裝設感應裝置，而產生的氣候或機器維護之數據資料；二則為「特定資料最初雖係屬個人資料，惟該資料後來已經去識別化，亦即將該個人資料，經過與假名化不同（pseudonymisation）之適當匿名化（anonymisation）後，除無法判定該資料為屬於某特定人之資料、亦無法透過其他額外資料而判斷為某特定人之資料，然如何判斷個人資料是否已符合適當匿名化，仍應依據個案為個別具體判斷<sup>76</sup>。

#### B. 確保數據資料跨境自由流動

本規章為歐盟之數據資料儲存和處理制定法律框架，減少資料在地化之限制。歐盟各會員國必須將其任何有關資料在地化之限制提交予執委會，然後執委會將對該等限制之合理性進行評估。除非各會員國之法律關於資料在地化的要求符合比例原則，並得依公共安全（如刑事犯罪之調查、偵查和起訴等）或基於現行歐盟法規取得正當性，

---

<sup>73</sup> See European Commission, *Digital Single Market: Commission publishes guidance on free flow of non-personal data*, Press Release (2019/05/29), [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_2749](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2749) (last visited May 29, 2021).

<sup>74</sup> *Id.* 另參吳彥容，同前註 51，頁 20-21。

<sup>75</sup> Guidance 2.1.

<sup>76</sup> *Id.* 另參陳志宇等，同前註 37，頁 174。

否則各會員國應於《非個資流通規章》施行後的 24 個月內廢除與本規章相衝突之資料在地化要求<sup>77</sup>。

而 GDPR 將與《非個資流通規章》共同發揮作用，以促進包含個人與非個人資料之自由流動。然而資料並非可截然二分為純屬個人資料或純屬非個人資料，事實上常見個人與非個人資料混合之情形，在此種「混合型資料集」(mixed datasets) 之情況下，保證個人資料之自由流動的 GDPR 規範將適用於資料集的個人數據部分，而《非個資流通規章》原則將適用於非個人資料部分<sup>78</sup>。

### C. 建立跨境合作程序以確保審查和監控的資料可用性

《非個資流通規章》在交換非個人資料領域為歐盟各會員國之間開拓一般性合作機制之道，消弭各會員國無法對儲存在其管轄領域外之資料執行的顧慮，按照本規章，不論資料在歐盟境內何處進行儲存或處理，若主管機關向資料處理服務之使用者要求閱覽其儲存於其他會員國之資料，卻無法閱覽時，得請求資料儲存第之主管機關提供閱覽該資料之協助<sup>79</sup>，使主管機關能夠取得數據資料以進行審查和監督控制。

---

<sup>77</sup> Regulation (EU) 2018/1807, Art. 4, Art. 33.

<sup>78</sup> Regulation (EU) 2018/1807, Art. 2.2. 僅表示處理有不可分的關聯 (inextricably linked) 之混合型資料集時，不得妨礙 GDPR 之適用 (shall not prejudice the application of Regulation (EU) 2016/679)。

<sup>79</sup> Regulation (EU) 2018/1807, Art. 5, Art. 7.

#### D. 鼓勵制定便於轉換服務提供者之自律行為準則

對於促進資料可攜性，使得消費者更便於轉換服務提供者，《非個資流通規章》採取鼓勵並促進業者自律之方式，列出發展此自律行為準則應考量之重要關鍵層面，且敦促業者須在 2019 年 11 月底之前發展自律行為準則，並於 2020 年 5 月前有效實施，進而促進雲端服務提供者之間的轉換，使得雲端服務市場更加靈活，且歐盟的數據資料服務更加實惠<sup>80</sup>。

#### 2. 資料可攜性有助於促進競爭

歐盟發現數據資料驅動之創新，係為經濟和就業成長之關鍵推動因素，有顯著提高歐盟在全球市場之競爭力的可能性，為使充分利用數據資料經濟，必須使數據資料能夠跨境流動且跨境使用。此種特殊的釋出義務，尚未見於其他國家之規範，然而透過通訊傳播服務所儲存之資料日益增多、數位通訊服務也日益豐富，可想見消費者在不同通訊傳播服務數位平臺間移轉其留存資料之需求只會越來越高，惟在消費者意圖轉換或新增服務提供者時，若無資料可攜之程式設計，則可能因資料量龐雜，造成移轉上之困難，間接限制消費者自由選擇服務與掌控資料之能力與成本，換個角度來看，亦影響平臺彼此之間的競爭效益<sup>81</sup>。

就此，歐盟希望以創設權利之方式，解決轉換平臺之套牢問題。故藉由 GDPR 與《非個資流通規章》攜手一同確保對歐盟數據資料之

---

<sup>80</sup> Regulation (EU) 2018/1807, Art. 6.

<sup>81</sup> 陳志宇等，同前註 37，頁 164-165。

自由移動和可攜性採取全面和一致性之方法，並進一步促進業者間之自律合作關係、鼓勵發展使資料具有可攜性之共同操作模式。而取消資料在地化之限制可以釋放數據資料之全部潛力，除可降低事業因應資料在地化措施之成本，亦得為事業之資料管理與數據分析提供更大的靈活度，作為大幅翻漲 GDP 之重要因素<sup>82</sup>。

## 二、數位平臺問責

### （一）安全港免責與平臺監理機制

歐盟迄今為止，對於數位平臺之責任，仍然仰賴早期《電子商務指令》之規範，尤其是其中關於「責任安全港（safe harbor）」針對不同網路中介者之免責要件。然而該指令在實施二十年之後，由於整體網際網路環境的變化，導致違法內容影響社會等事件層出不窮，故歐盟執委會於前開《數位市場法》草案之同時，併同提出《數位服務法》草案，主要目標即是改革《電子商務指令》之不足，明確化新課予數位平臺的獨立義務。

以下，謹先就《電子商務指令》之內容與檢討耙梳；再接續考察《數位服務法》草案之草擬情形。

#### 1. 《電子商務指令》

歐盟於 2000 年時通過《電子商務指令》（Directive on electronic commerce, 2000/31/EC, ECD），該指令適用於所有資訊社會服務，包

---

<sup>82</sup> European Commission, A framework for the free flow of non-personal data in the EU, [https://ec.europa.eu/commission/presscorner/detail/en/MEMO\\_18\\_4249](https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4249) (last visited June 03, 2021).

括規範網路中介者 (providers of intermediary service) 之設立、法規適用、電子契約和責任等。該指令的主要目標在促進歐盟電子商務的發展，故建構共同之法律框架以拉齊會員國之法律，進而確保會員國間資訊社會服務之自由流動和消費者對線上電子商務之信心<sup>83</sup>。

### (1) 網路中介者定義與免責規範

而資訊社會服務的概念廣泛地涵蓋電商零售、通訊服務、網路搜尋引擎、視聽服務串流等網際網路上之經濟活動。此一規範架構所稱之網路中介者，即指連線 (Mere conduit) 服務提供者、快速存取 (Caching) 服務提供者、資訊儲存 (Hosting) 服務提供者三種服務型態。

➤ **連線服務提供者**：係指提供通訊網路之接取，或在通訊網路中傳輸服務接收者所提供之資訊，此類單純提供傳輸服務者，尚包括基於通訊網路內傳輸之唯一目的，對於所傳輸的資訊為自動、中介及瞬時 (transient) 之儲存，且此一資訊所儲存的時間，並不超過傳輸所需之合理期間 (第 12 條)。

➤ **快速存取服務提供者**：係指在提供通訊網路傳輸服務接受者所提供之資訊時，基於使資訊傳輸更有效率之單一目的，而對資訊所為之自動、中介及暫時之儲存服務 (第 13 條)。

➤ **資訊儲存服務提供者**：係指依使用者要求，而儲存該使

---

<sup>83</sup> See Directorate-General for the Information Society and Media (European Commission), EU Study on the Legal Analysis of a Single Market for the Information Society: New Rules for a New Age? (2014).

用者所提供之資訊之服務提供者（第 14 條）。

為促進網路中介者之發展並降低對其干預，則採功能取向之規範方式，依類型不同而分別設計「通知即行動」(notice and action) 之免責要件<sup>84</sup>，如業者符合規範則賦予侵權責任之豁免權，並若知悉，即可落入安全港之保護範圍。

➤ **連線服務提供者：**服務提供者並未主動啟動傳輸資訊，亦未選擇接受資訊的收訊方，更未挑選或修改所傳輸的資訊，即一般而言，是類服務提供者並未對所傳送或暫時中介儲存之資訊有所知悉、且加以控制，而僅係技術程序範圍內的傳輸，故如服務提供者並未控制或知悉其所傳輸之資訊，則毋庸必須對該資訊負自己責任。

➤ **快速存取服務提供者：**資訊社會服務的提供，係包括於通訊網路中傳輸由服務接收者所提供的資訊時，會員國應確保於以下情形時，服務提供者無須對為了僅讓其他接收者在其要求下，基於使資訊傳輸更有效率之單一目的，而對資訊所為之自動的、中間的與暫行的儲存行為負責：(A) 服務提供者並未修改該資訊；(B) 服務提供者遵守資訊接取的條件；(C) 服務提供者遵守資訊更新的規則，尤其是為產業所廣泛承認與使用的規則而言（或謂「產業標準」industrial standard）；(D) 服務提供者並未干涉，有關合法使用廣泛為產業所承認與使用之科技，以取得資訊使用的資料；(E) 服務提供者確實知悉該資訊之最初傳輸來源，已移

---

<sup>84</sup> 陳人傑，網際網路服務提供者免責規範單一立法模式之探討，智慧財產權月刊，第 71 期，頁 56-60 (2004)。

除於網路之外，或者該資訊已無法接取，或者法院或行政機關命其移除或使之無法接取時，服務提供者應立即移除該資訊，或使之無法接取<sup>85</sup>。

➤ **資訊儲存服務提供者**：資訊社會服務的提供，係包括服務接收者提供資訊的儲存時，會員國應確保在符合以下情形時，服務提供者無須對於因服務接收者之請求而儲存的資訊負責：(a) 服務提供者實際上並未認識不法活動或資訊，並且在有關損害賠償的請求上，並未察覺該不法活動或資訊有顯而易見的事實或狀況；或者(b) 服務提供者在取得此一認識或察覺後，立即移除該資訊，或使該資訊無法接取。首先，如未認識系爭行為或資訊內容係屬違法的話，自不應課予民事或刑事上的故意責任。而在損害賠償的請求上，由於指令要求必須具有「顯而易見該不法活動或資訊的事實或狀況」，因此在解釋上可認為指令已降低服務提供者可能必須負擔之善良管理人注意義務（抽象輕過失責任），而以朝向具體輕過失或重大過失責任的方向設計。再者，對於為服務提供者所「隸屬」(authority) 或「控制」(control) 的使用者，係指此一使用者與服務提供者具有關係企業的關連，而為服務提供者所控制者。此時在責任判斷上，不再將其視為是他人所提供的內容，而是透過從屬事業所從事的自己行為<sup>86</sup>。

需注意者，《電子商務指令》不論第 12 條至第 14 條，均於條文內重申，本指令之規範，並不影響各會員國之法院或行政機關，依據

---

<sup>85</sup> 同上註，頁 58。

<sup>86</sup> 同上註，頁 59-60。

內國法之法律體系要求網路中介者中止或防止侵害行為之可能性。甚至會員國亦可對資訊儲存服務提供者規範符合表現自由原則之移除資訊或使之無法接取的程序（併參引言第 46 點）。

## （2）網路中介者無常規監控義務

《電子商務指令》於第 15 條規定，對於上開網路中介者，會員國不得課予其監控所傳輸或儲存之資訊的一般義務，亦不具尋找象徵不法活動之事實或狀況的一般義務（第 1 項）。不過，同條第 2 項規定，會員國得針對使用者的可疑不法活動或資訊，規定資訊社會服務提供者負有通知主管機關之義務；或者在主管機關的請求下，對於與服務提供者具有儲存協議的使用者，提供其身分資訊。

此一規定最主要的考量，是在於保障人民的秘密通訊自由及隱私權的保護，避免因前揭免責規範，訂有「在認識或確實知悉該活動或資訊違法時，必須移除或使之無法接取」的規定，而讓人誤以為服務提供者負有監控其系統或網路的一般義務。如果在犯罪偵察或被害人進行損害賠償請求確有需要的話，各會員國仍得以其內國法之規定，要求服務提供者必須針對個案配合主管機關，或者提供身分資訊<sup>87</sup>。惟指明使用者不法行為之義務；例外則有該指令前言（Recital）第 47 點及第 48 點之特殊情況，則不限制會員國要求服務提供者依據法律調查或防止非法活動，例如透過法院暫時禁制令，亦即，鬆綁網路中介者的常規監控義務 於特殊情況下或有個別案例時，會員國得要求

---

<sup>87</sup> 同前註。

網路中介者負擔特殊監測義務 (specific monitoring) <sup>88</sup>。

## 2. 《數位服務法》草案

隨著網際網路之服務態樣日益創新，導致資訊社會服務提供者之定義日趨模糊，且各會員國有不同的法律詮釋；加上跨境之網路中介者日漸興起，而各會員國對「通知即行動」(notice and action) 的標準不一，造成法遵上之不確定性<sup>89</sup>。基此，歐盟執委會於 2020 年 12 月 15 日發布《單一市場數位服務暨修正電子商務指令之規章》草案 (Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC)，以下簡稱《數位服務法》草案 (DSA Proposal)。

《數位服務法》草案共分為五大章節，共計 74 條。該草案之規範重點為，首先明確歸責制度的範圍，依照網路中介者之類型，列舉安全港之要件與「通知即行動」義務；其次，探討若網路中介者承諾藉由監控平臺上的資訊合法性，即使該資訊事後被認定為非法，但網路中介者因其努力而可不被歸責，亦即推動自律機制，此一機制亦受到大型平臺的支持<sup>90</sup>。再次，則是設置數位服務協調官 (digital services coordinators) 與設立歐洲數位服務委員會 (European Board for Digital

---

<sup>88</sup> 王牧寰、徐偉群、陳志宇、鄭嘉逸、江耀國、陳人傑、簡陳中、楊東穎、胡家崎、楊儷綺、王艾雲、廖祥丞、田育志，因應數位通訊傳播服務發展之規管趨勢與法制革新研析，國家通訊傳播委員會委託之計畫成果報告，頁 97-98、120 (2021)。

<sup>89</sup> 同前註，頁 121-122。

<sup>90</sup> Aleksandra Kuczerawy, The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?, KU Leuven CiTiP (2018).

Services)，明確監理機構的功能與作用；最後，設有相關罰則規範。

### (1) 網路中介者定義與「通知即行動」規範

《數位服務法》草案基本上沿用《電子商務指令》對於網路中介者之規範定義，依舊區分為連線服務提供者、快速存取服務提供者及資訊儲存服務提供者三類，並依照網路中介者之類型，列舉安全港之要件與「通知即行動」義務，以及其在網路活動中扮演主動或被動的角色，制定更明確的「通知即行動」規範與程序。

### (2) 累加義務模式

《數位服務法》草案雖然沿用《電子商務指令》之將網路中介者的概念，然歐盟認為該等類別有些過時，一方面因為服務與新興科技之發展，使得某些服務提供者對資訊儲存之內容影響加深，導致「中介者」之界線趨於模糊，另一方面《電子商務指令》缺乏必要之盡職調查義務（due diligence obligations），應適當處理線上第三方之內容，以避免不法內容傳散之風險<sup>91</sup>，遂依照類型與規模將服務提供者更加細緻化，並採用累加義務（cumulative obligations）模式，逐級課與額外之義務，加重其所承擔之義務。

---

<sup>91</sup> European Commission, Commission Staff Working Document, Impact Assessment Report, Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, SWD/2020/348 final, at 12.

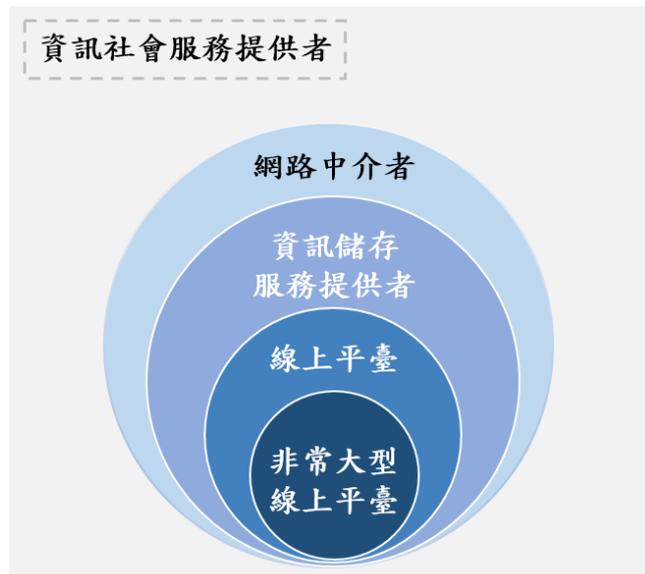


圖 1：《數位服務法》草案累加義務示意圖

資料來源：DSA 草案，本計畫製作

#### A. 網路中介者

依照草案條文所示，網路中介者之定義與《電子商務指令》相同，僅分為「連線服務提供者」、「快速存取服務提供者」，以及「資訊儲存服務提供者」三種態樣<sup>92</sup>。與前述《電子商務指令》第 15 條相同，網路中介者無常規之監控義務<sup>93</sup>，亦可從明文規定網路中介者將不會因其自動地、主動地調查或識別有無違法內容或採取相應之必要行動而喪失安全港免責之保護<sup>94</sup>，歐盟賦予數位平臺更高之期待。

而草案規定網路中介者應負之義務，主要有依照司法或行政機關之命令，採取對抗違法內容與提供資訊之義務；應揭露其於「使用者

<sup>92</sup> DSA, Art. 3-5.

<sup>93</sup> DSA, Art. 7.

<sup>94</sup> DSA, Art. 6.

服務守則」中於其服務上所施加之任何限制；並且，除微型或小型企業外，應至少每年提交 1 次透明度報告<sup>95</sup>等。

### B. 資訊儲存服務提供者

《數位服務法》草案特別針對資訊儲存服務提供者附加兩項額外之義務，一為應建立「通知即取下」機制，二則倘若服務提供者決定移除或阻斷他人接取該資訊，應通知該資訊之提供並說明理由<sup>96</sup>。

### C. 線上平臺

所謂線上平臺（online platform）係指依使用者之要求，將資訊儲存並向公眾傳散之資訊儲存服務提供者（如社群平臺）<sup>97</sup>。

除需符合前開義務外，針對線上平臺再附加額外之義務，主要如：應建立內部申覆機制、訴外爭端解決機制；確保能優先處理認證檢舉人（trusted flaggers）舉報之事項；每 6 個月提供 1 次透明度報告，且內容應包含訴外爭端解決機制及濫用機制防止措施之處理件數、時間與結果，以及揭露平臺使用之自動化措施；尚有揭露並清楚向使用者展示線上廣告主要參數之資訊<sup>98</sup>等。

### D. 非常大型線上平臺

所謂非常大型線上平臺（very large online platform）係指歐盟境內月平均實際接收服務者達 4,500 萬人之線上平臺。至於何業者位在

---

<sup>95</sup> DSA, Art. 8-9, 12-13.

<sup>96</sup> DSA, Art. 14-15.

<sup>97</sup> DSA, Art. 2(h).

<sup>98</sup> DSA, Art. 17-20, 23-24.

非常大型線上平臺之列，歐盟執委會應造冊，並應視情況而隨時更新名冊<sup>99</sup>。

除需符合前開義務外，針對非常大型線上平臺再特別附加額外之義務，主要如：應至少每年進行風險評估 1 次，且應採取合理必要之措施以減輕風險；若非常大型線上平臺有使用資訊推薦系統 (Recommender systems)，應於其平臺介面向其使用者揭露主要參數，讓使用者可選擇或改變其接收之相關訊息；對於線上廣告透明度，應額外將所有投放之廣告彙集和儲存於資料庫，並向公眾揭露，且應自該廣告最後一次播放後保存 1 年；應為每 6 個月提交透明度報告 1 次，除包含線上平臺應提交之資訊外，應再公布且至少每年繳交 1 次經法遵審查之查核報告予數位服務協調官與歐盟執委會；應向數位服務協調官或歐盟執委會，以及研究者提供和分享必要資訊，以協助其監管與評估是否符合本草案之規定<sup>100</sup>等。

最後，歐盟執委會應依職權，於必要時，得邀請相關之非常大型線上平臺、線上平臺、網路中介者或公民團體組織與相關當事人，共同訂定行為準則或危機處置合作<sup>101</sup>。總言之，歐盟預期透過全面性改變對線上服務之監理方式，進而建立安全且具問責機制的線上環境<sup>102</sup>。

---

<sup>99</sup> DSA, Art. 4, 25, 69.

<sup>100</sup> DSA, Art. 26-31, 33.

<sup>101</sup> DSA, Art. 35-37.

<sup>102</sup> 許慈真，歐盟邁向數位單一市場的新里程碑：數位服務法(DSA)與數位市場法(DMA)，北美智權報，第 276 期 (2021/01/06)，

[http://www.naipo.com/Portals/1/web\\_tw/Knowledge\\_Center/Laws/IPNC\\_210106\\_0202.htm](http://www.naipo.com/Portals/1/web_tw/Knowledge_Center/Laws/IPNC_210106_0202.htm) (最後瀏覽日：2021 年 05 月 31 日)。

### (3) 監管單位

《數位服務法》草案新設置由數位服務協調官所組成之「歐洲數位服務委員會」(European Board for Digital Services)，主要功能為向歐盟執委會與數位服務協調官提供本草案規範事項之建議。

為負責《數位服務法》草案相關事務之實施與執行，各會員國應指派一個或數個主管機關，並從中指派數位服務協調官，以獨立、公正、透明且妥速之方式，負責該國境內有關《數位服務法》草案之一切事務，並確保國家層級間之協調。且賦予數位服務協調官擁有對網路中介者之調查權、對網路中介者採取臨時措施、接受網路中介者之承諾、暫時限制用戶接取中介服務等等之權利<sup>103</sup>，以求妥適實行草案所訂定之任務。

此外，歐盟執委會亦屬監理單位之一環，其為歐洲數位服務委員會之主席<sup>104</sup>，並負有其他應盡職之義務，諸如應協助發展與實施自願性之產業標準；若有必要時，亦得依職權邀請相關之非常大型線上平臺、線上平臺、線上中介服務提供者或公民團體組織與相關當事人，共同訂定行為準則或危機處置合作<sup>105</sup>。

### (4) 罰則

《數位服務法》草案對於違反義務者，訂有相應之裁罰規範。首先，針對違反義務之網路中介者，將可處以最高不得超過其年收入或

---

<sup>103</sup> DSA, Art. 38-41.

<sup>104</sup> DSA, Art. 48(3).

<sup>105</sup> DSA, Art. 34-37.

營業額之 6% 之罰鍰<sup>106</sup>。

其次，特別針對非常大型平臺，如認有違反草案規定之義務或未依第 55 條或第 56 條遵循執委會之命令等情事，裁罰最高不得超過其前一個會計年度總營業額之 6%；而若有未能遵守依第 52 條提供資訊之命令、更正不實訊息或提供完整資訊，以及未依第 54 條提供現場查檢（on-site inspections）等情事，將可處以最高不得超過其前一個會計年度總營業額之 1% 之罰鍰，惟自裁決日起算，每日最高不得超過前一會計年度之日平均營業額之 5%<sup>107</sup>。

## （二）強化數位平臺因應網際網路不法內容義務之策略

數位平臺逐漸成為網際網路上大量資訊流通傳遞之主要管道，其中亦乘載諸多不法內容，以往歐盟冀望數位平臺能透過自行建立識別機制，共同合作移除或阻斷接取該等內容，然而，歐盟漸漸針對不同議題採取不同之規範模式。一方面轉向採取強而有力之規範的態度<sup>108</sup>，針對不同「特化型」的線上平臺，以制定其他規章或指令之方式，因應諸如打擊恐怖主義或視訊分享平臺等特別問題<sup>109</sup>，而上開《數位服務法》草案則將作為網路中介服務之普通法，與其他屬特別法之部門硬法（sectoral hard-law）構成「特別—普通法」之適用關係。至於歐盟執委會十分關切的不實訊息、假新聞等內容，《數位服務法》草

---

<sup>106</sup> DSA, Art. 42.

<sup>107</sup> DSA, Art. 59-60.

<sup>108</sup> Steven Musil, EU reportedly ready to act against tech companies over terror content: European Union plans to impose fines over terrorist propaganda, CNET (2018/08/19), <https://www.cnet.com/news/eu-reportedly-ready-to-act-against-tech-companies-over-terror-content/> (last visited June 15, 2021).

<sup>109</sup> Alexandre de Streel, Aleksandra Kuczerawy & Michèle Ledger, Online Platforms and Services, in *Electronic Communications, Audiovisual Services and the Internet: EU Competition Law and Regulation* 152 (Laurent Garzaniti, Matthew O'Regan, Alexandre de Streel & Peggy Valcke ed., 4th ed., 2020).

案並未予直接處理，其於草案前言中提及，該等問題仍將透過發展泛歐之自律性行為準則及由執委會發布指引之軟法方式處理<sup>110</sup>，並不妨礙各會員國自行立法予以規範，且搭配數位平臺自律之相關措施，共同建議安全與可信任之網路環境。總言之，本研究聚焦於較為熱議之議題，分別論述其規範模式。

## 1. 歐盟層級規範特殊樣態之模式

### (1) 打擊線上恐怖主義

歐盟因飽受恐怖主義的威脅，而欲藉由更為嚴格之立法模式打擊恐怖主義，以保護歐盟公民，其發現近年歐洲發生的恐怖攻擊，均與線上恐怖主義內容高度相關，即恐怖組織透過網際網路招募、煽動、宣傳美化、協調與指導恐怖攻擊活動，並號召支持者追隨之，遂歐盟於 2017 年便開始考慮建構打擊線上恐怖主義之框架<sup>111</sup>，直至 2021 年 4 月 29 日通過《打擊線上恐怖主義內容規章》(Regulation (EU) 2021/784)，並自 2022 年 6 月 7 日起執行<sup>112</sup>，預期透過國家間協力打擊恐怖主義，進而建構網際網路安全與言論自由之環境，以保障歐盟公民獲取合法內容與資訊。本規章並不影響《電子商務指令》之適用，其主要規範重點為<sup>113</sup>：

---

<sup>110</sup> DSA, Rec. 68-71.

<sup>111</sup> Directive (EU) 2017/541 of The European Parliament and of The Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

<sup>112</sup> Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

<sup>113</sup> See European Parliament, *New rules adopted for quick and smooth removal of terrorist content online*, Press Releases (2021/04/28), <https://www.europarl.europa.eu/news/en/press-room/20210422IPR02621/new-rules-adopted-for-quick-and-smooth-removal-of-terrorist-content>

➤ **適用主體為資訊儲存服務提供者：**本規章所適用之資訊社會服務提供者，僅限於提供儲存（指將數據保存在實體或虛擬伺服器中）並應用戶要求而提供向公眾傳播之（不論是技術性、自動性或被動性）資訊或資料的服務提供者。故未包含「單純提供連線」、「快速存取」的服務提供者，或其他不涉及儲存之網際網路基礎層設施的服務提供者（如網域名稱系統服務、阻斷服務等）<sup>114</sup>。

➤ **必須在 1 小時內刪除有關恐怖主義內容：**除有不可抗力或事實上不能等客觀合理之技術原因外，原則上資訊儲存服務提供者（如 Facebook、Google 等數位平臺）應有配合主管機關要求移除或阻斷接取恐怖主義內容之命令的義務，且需附理由說明何以移除或阻斷接取該內容。而如數位平臺違反規定未為移除或阻斷接取，則可能面臨高達其全球營業額 4% 之罰鍰<sup>115</sup>。

➤ **排除教育、藝術、研究和新聞內容：**尊重藝術、科學與媒體自由及多元化，用途為教育、新聞、藝術或研究目的，或係為預防或提升恐怖攻擊活動之警覺性所製作的資料，均非本規章所定義之「恐怖主義內容」<sup>116</sup>。

➤ **無監控或過濾內容之一般義務：**維持不課予服務提供者監控其傳輸或儲存之資訊的一般義務，亦不課予其主動查找違反活動之事實或情狀。亦即，只要資訊儲存服務提供者對違反活動

---

[online](#) (last visited June 01, 2021).

<sup>114</sup> Regulation (EU) 2021/784, Art. 1, Rec. 13.

<sup>115</sup> Regulation (EU) 2021/784, Art. 2, 18, Rec. 17-18, 45.

<sup>116</sup> Regulation (EU) 2021/784, Art. 1, Rec. 12.

或資訊無實際了解，且對明顯存在違反活動或資訊之事實或情況並不知悉，便不應對其究責<sup>117</sup>。

另外，資訊儲存服務提供者或主管機關應發布年度透明度報告，加以說明執法情形，執委會亦應於本規章生效之日起三年內進行評估實施之成效等情況<sup>118</sup>。

然而，本規章還是引發國際特赦組織（Amnesty International）、無國界記者組織等非政府組織和人權組織的不安，唯恐本規章有箝制言論自由之疑慮<sup>119</sup>。不過，歐盟認為從源頭移除構成會員國內實施恐怖主義罪刑之網際網路內容，或建構阻斷內容之措施，是打擊網際網路恐怖主義之有效手段，因此賦予資訊儲存服務提供者特殊之社會責任，信任其採取必要、適當和符合比例以保護其服務不被恐怖份子所濫用的矯正措施，這與保護言論和資訊自由並無衝突，甚至為相輔相成之關係<sup>120</sup>。總歸而言，本規章甫通過，仍待後續觀察實際運作狀況。

## （2）規管視訊分享平臺

歐盟於 2007 年通過《視聽媒體服務指令》（Directive 2007/65/EC, Audiovisual Media Services Directive, AVMSD）<sup>121</sup>，其內容管制措施以

---

<sup>117</sup> Regulation (EU) 2021/784, Rec. 23.

<sup>118</sup> Regulation (EU) 2021/784, Art. 7-8, Rec. 31, 48-49.

<sup>119</sup> AFP, EU passes law for quick removal of online “terrorist content”, Deutsche Welle, <https://www.dw.com/en/eu-passes-law-for-quick-removal-of-online-terrorist-content/a-57368591> (last visited June 02, 2021),

<sup>120</sup> Regulation (EU) 2021/784, Art. 5, Rec. 1, 5, 10.

<sup>121</sup> Directive 2007/65/EC of The European Parliament and of The Council of 11 December 2007 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, COM(2005)646. 2010 年修正之《視聽媒體服務指令》（Directive 2010/13/EU）係與《電視無疆界指令》（Directive 89/552/EEC, Television Without Frontiers Directive, TVwF）進行整併，並無更動內容。

「視聽媒體服務」(audiovisual media service, AVMS) 作為規範對象，而視聽媒體服務包括兩大部分<sup>122</sup>：A. 負有編輯責任 (editorial responsibility) 之媒體服務提供者藉由電子通訊網路向公眾提供之主要目的或可分離部分為節目，而其目的係為傳達資訊、娛樂或教育之服務；或 B. 視聽廣告 (audiovisual commercial communication)。

對於負有編輯責任之媒體服務提供者又可區分為兩類，一為「廣播電服務」(television broadcasting or television broadcast)，指以節目時間表為基礎，提供使用者同時收視聽節目之線性 (linear) 視聽媒體服務<sup>123</sup>，亦即所有以「頻道」形式而為提供之視聽媒體服務，皆屬廣播電視；二為「隨選視訊服務」(video on demand, VOD)，則係指以服務提供者編排所選擇之節目為基礎，個別使用者可於任何時間要求提供收視聽節目之非線性 (non-linear) 視聽媒體服務<sup>124</sup>，且此種定義方式不因屬「線上或線下」而有所差異。

然而，歷經十年，隨著新興影音串流服務逐漸普及，對社會影響力大增，歐盟有感視聽媒體服務環境已有巨大轉變，便於 2018 年再次修正，通過《修正視聽媒體服務指令》(Directive (EU) 2018/1808, “Revised AVMSD” )<sup>125</sup>，除針對「歐洲影視作品配額」、「廣告規範之電視廣告與購物頻道特別規範」、「主要事件與新聞短報授權」與「回覆權」仍維持不同程度之管制外，盡量拉齊廣播電服務與隨選視訊服務

---

<sup>122</sup> Revised AVMSD, Art. 1(1)(a).

<sup>123</sup> AVMSD, Art. 1(1)(e).

<sup>124</sup> AVMSD, Art. 1(1)(g).

<sup>125</sup> Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

之管制密度落差。與此同時，更將「不具編輯責任」之「視訊分享平臺」(video sharing platforms, VSP) 納入規管範疇。

所謂編輯責任，指實施節目選擇(selection)及編排(organisation)之有效控制；編排係指廣播電視服務之節目排定次序及時間，或隨選視訊服務之節目片庫呈現順次<sup>126</sup>。故而，唯有同時決定所欲提供之節目、以及決定其提供之先後或順次者，始具編輯責任。此等定義在《修正視聽媒體服務指令》新增視訊分享平臺為管制對象後，更顯重要。因視訊分享平臺係提供使用者供應內容(user-generated content, UGC)服務<sup>127</sup>，亦即節目選擇非由視訊分享平臺之提供者所控制，其僅控制節目之編排，也即僅在陳列、標籤以及排序的方式上，是由服務提供者或演算法決定而已。

而《修正視聽媒體服務指令》針對不屬於視聽媒體服務之特化型線上平臺—視訊分享平臺，原則上就「禁止仇恨性內容」、「兒少身心保護」及「廣告限制之一般性規範」，其內容觸及範圍已與線性或非線性內容並無二致，僅因為視訊分享平臺本身並無編輯責任，也即內容並非視訊分享平臺所提供，因此，對於使用者提供之內容為保障言論自由，既不能事前過濾，故僅能課予視訊分享平臺事後透過內容管制使用條款、內含廣告聲明功能、檢舉機制及說理透明、受理申訴、警語工具、訴外爭端解決機制等方式確保內容管制之目標<sup>128</sup>。

是以，視訊分享平臺服務之義務在於提供適當具體措施，以避免

---

<sup>126</sup> AVMSD, Art. 1(1)(c).

<sup>127</sup> Revised AVMSD, Art. 1(1)(aa).

<sup>128</sup> Revised AVMSD, Art. 28a & 28b. 其中第 28a 條為管轄權規範，有關管制之實質規範僅記載於第 28b 條。

涉及暴力與仇恨性言論、影響兒少身心，或煽惑恐怖攻擊犯罪等之不當視聽商業通訊的內容傳播，包括親子鎖、內容分級、不當內容標記、採取兒少個資保護措施等義務。並保護無障礙之近用權益、彰顯公共利益、保護內容編輯責任者之權益、促進歐洲視聽媒體服務作品彰顯及其內容產製，且應促進共管架構與自律機制，增進媒體素養，且確保視聽媒體服務監理機關的獨立性，以具體維護歐盟視聽服務環境之健全發展<sup>129</sup>。

## 2. 由各會員國自行監理內容之模式：以不實訊息為核心

在 2020 年「歐洲民主行動計畫」(European Democracy Action)<sup>130</sup>中可知，歐盟認為數位平臺對民主選舉和新聞媒體之自由運作，及不實訊息對社會秩序造成之危害負有主要責任，採取敦促數位平臺達成自律協議，並成立專家小組提供執行評估與建議。而法國於 2018 年即通過相關修法措施以表對尤其是選舉方面之不實訊息的重視，且類似於我國國家通訊傳播委員會之獨立機關—「最高視聽委員會」(Conseil supérieur de l'audiovisuel, CSA) 亦衡量數位平臺為對抗不實訊息所採取之措施與成效，出具評估報告，本研究認為法國經驗具參考價值，以下介紹之。

### (1) 歐盟層級

歐盟自 2015 年起即對網際網路不實訊息所帶來之危害採取相關

---

<sup>129</sup> Revised AVMSD, Art. 28b.

<sup>130</sup> European Commission, Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions on the European Democracy Action Plan, COM(2020) 790 final.

措施，諸如成立「假新聞高階專家工作小組」(High Level Expert Group, HLEG) 提出重點因應策略、公布「因應網路不實訊息通報」(Communication on Tackling Online Disinformation: A European Approach) 為行動之關鍵原則達成共識、公布「因應不實訊息之實踐準則」(EU Code of Practice on Disinformation) 供平臺業者自行簽署並定期檢討其是否確實履行義務、公布「因應不實訊息之行動計畫」(Action Plan against Disinformation) 提出四大主軸及十大行動方案以對抗不實訊息等<sup>131</sup>。

歐盟除前述以《數位服務法》草案對數位平臺賦予移除違法內容之義務外，2018 年公告「因應不實訊息之實踐準則」與數位平臺達成自律 (self-regulation) 之共識，採取防止不實訊息之因應措施。諸如 Facebook、Google、Twitter、Mozilla、Microsoft 及 TikTok 等大型數位平臺均已陸續簽署，針對審查廣告投放位置 (scrutiny of AD placements)、區別並揭露政治與議題性廣告之機制 (political advertising and issue-based advertising)、建立標記假帳號、內容農場等誠信服務 (integrity of services)、加強使用者權利 (empowering consumers)，以及持續追蹤不實訊息之議題且共享受隱私保障之相關數據予學術界、事實核查機構和相關團體進行聯合研究及討論會議 (empowering the research community) 等五大面向之承諾<sup>132</sup>。

對此，歐盟委由其轄下組織「歐洲視聽媒體服務管制組織」(European Regulators Group for Audiovisual Media Services, ERGA)

---

<sup>131</sup> 王牧震等，同上註 88，頁 93-96。

<sup>132</sup> 同上註，頁 98-99。

評估承諾簽署業者之執行成效，主要藉由業者所提出的自我評估報告（Self-Assessment Report, SAR）之內容；或業者指定的第三方機構（Third Party Organization, TPO）審查與評估業者的 SAR 後所出具的意見報告，進行審查及評估，並提出改善準則之建議與配套措施<sup>133</sup>。

尤其近年受到 2019 新型冠狀病毒肺炎（下稱 COVID-19）所伴隨而來的不實訊息，歐盟理解到數位平臺（特別是社群媒體平臺）之中的作用越來越大，於是更加要求數位平臺展現更高的透明度，以防堵在 COVID-19 危機中受到不實訊息（disinformation）、錯誤訊息（misinformation）或外國影響戰（foreign influence operations）所構成的社會穩定之威脅<sup>134</sup>。另外，歐盟亦指出 2021 年強化版之「因應不實訊息之實踐準則」將會成為《數位服務法》草案之共同監管（co-regulatory）工具<sup>135</sup>，並呼籲簽署之數位平臺於 2021 年秋季提交相關承諾初稿予執委會<sup>136</sup>，均在在顯見歐盟持續不懈地強力對抗不實訊息。

## （2）歐盟會員國實踐之考察：以法國相應措施為例

### A. 數位平臺應依法院審查命令而配合相關作為

法國近年來受到假新聞影響甚深，總統馬克宏在 2018 年元旦演說時特別提及，希望透過改善法律制度，來「保護虛假新聞中的民主

---

<sup>133</sup> 同上註，頁 99-108。

<sup>134</sup> European Commission, Tackling COVID-19 disinformation - Getting the facts right (JOIN/2020/8 final), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0008> (last visited May 25, 2021).

<sup>135</sup> See European Commission, Code of Practice on Disinformation, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation> (last visited May 27, 2021).

<sup>136</sup> See European Commission, Commission presents guidance to strengthen the Code of Practice on Disinformation, Press Release (2021/05/26), [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_2585](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585) (last visited May 28, 2021).

生活」。在此政策脈絡下，同年即通過《對抗資訊操縱法》(Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information)<sup>137</sup>。

《對抗資訊操縱法》分為 5 大編 (Titre)，共計 20 條。第 1 編是修正《選舉法典》(Code Électoral) 之規範 (第 1 條至第 4 條)；第 2 編是修正 1986 年《通訊自由法》(Liberté de Communication) 之規範 (第 5 條至第 10 條)；第 3 編是規範網路平臺之服務提供者，具有對抗不實訊息之合作義務 (第 11 條至第 15 條)；第 4 編修正《教育法典》，補充媒體識讀教育之規範 (第 16 條至第 19 條)；第 5 編為有關海外行政區 (L'outre-Mer) 之適用規範 (第 20 條)。

而《對抗資訊操縱法》與數位平臺和不實資訊相關部分在於，該法第 1 條修正《選舉法典》多則規範。除了課予超過一定規模之網路社群平臺資訊透明以及配合改善的法律義務外，也同時賦予候選人、政黨及利害關係人，得在重要選舉 (包括國民議會議員及參議員選舉、與歐洲議會議員選舉) 前三個月到投票日止的期間，聲請法院停止不實訊息之散布的權利，且緊急審理法官必須受理案件後之 48 小時內作成裁定<sup>138</sup>。

然而，該法卻引來諸多爭議，多位參議員與國民議會議員質疑其有侵害憲法保障之營業自由、言論及通訊自由，以及罪刑法定主義等

---

<sup>137</sup> 陳洧農，吳秦雯 X 劉定基 X 蘇慧婕 | 當假新聞踩到法律紅線！防治假新聞：立法管制的困難險阻，卓越新聞電子報 (2020 年 02 月 18 日)，<https://www.feja.org.tw/50647> (最後瀏覽日：2021 年 06 月 12 日)。

<sup>138</sup> Code Électoral, Art. L163-1-L163-2.

原則之虞，故向法國憲法委員會聲請釋憲<sup>139</sup>。

憲法委員會針對聲請人所提之事由進行審查後，認定該法在聲請人提及之條文中皆屬合憲。首先，在營業自由方面，憲法委員會解釋，由於課與網路平臺服務提供者之義務僅限於選舉期間，且僅及於規模達一定門檻之服務提供者；尚且，該義務內容僅係要求揭露相關資訊，此係一種讓公民更瞭解選舉活動宣傳或廣告之範圍與對價的手段，從而有助於選舉辯論越辯越明。基此，鑑於所追求之整體利益、課與網路平臺服務提供者義務之有限性，系爭條款並未過度限制營業自由<sup>140</sup>。

其次，聲請人主張，該法係以不必要之方式侵害言論自由。同時，由於法官難以在 48 小時內做出裁決，因此該法之緊急審理程序有可能會被濫用，反而用以改變尚未進行之投票真實性。對此，憲法委員會則解釋，立法者制定特定期間之緊急審理程序，而可訴請停止散布可能破壞選舉真實性之不實訊息，係為了防止公民在行使投票權時被公眾網際網路通訊服務上大量傳播之是類資訊誤導或操縱，故其目的乃為確保選舉辯論的明確性及投票真實性原則。此外，憲法委員會認為，上述緊急審理程序可能會產生停止散布某些資訊內容之效果，因此，為求最大程度保障言論及通訊自由，僅有在指控或指責明顯不實或扭曲，始有理由採取暫停措施；同樣地，其變更投票真實性之風險，也必須符合「明顯」之要素<sup>141</sup>。

綜上，憲法委員會裁決，只要符合前開合憲性限縮解釋所施加之

---

<sup>139</sup> *Décision n° 2018-773 DC du 20 décembre 2018 (Loi relative à la lutte contre la manipulation de l'information)*.

<sup>140</sup> *Id.* at para. 3-10.

<sup>141</sup> *Id.* at para. 11-23.

限制，系爭規範並無不必要、不適當不合比例地侵害言論及通訊自由；同時，也未侵害辯護權、公平審判權、正當司法程序等權利，該法當屬合憲<sup>142</sup>，也成為法國境內對數位平臺課與強制義務之法源依據。

## B. 最高視聽委員會發布數位平臺自律評估報告

根據《對抗資訊操縱法》第三編有關數位平臺之合作義務中，第 11 條規範「單月內使用者數量超過 500 萬」之網路平臺服務提供者必須建置檢舉回報機制及對抗不實訊息之相關措施，並向法國最高視聽委員會（CSA）提出打擊不實訊息所採取對策之年度報告<sup>143</sup>，而 CSA 則在 2020 年 7 月做成「2019 年打擊數位平臺不實評估報告」（*Lutte contre la diffusion de fausses informations sur les plateformes en ligne - Bilan de l'application et de l'effectivité des mesures mises en oeuvres par les opérateurs en 2019*）<sup>144</sup>。

此報告包含 11 家服務提供者所提交的資料、共涉及 16 項服務，如第三方提供的內容、商品、線上評分與推薦服務和多方聯繫服務，以及內容、商品或服務之交易或分享等<sup>145</sup>，並針對各家平臺所採行的措施進行歸納及適用性分析，同時考量平臺經營活動和商業模式的多樣性，如點閱人數和營業額的差異，再給予效果評估與建議。

從評估報告中可知，CSA 主要衡量數位平臺對抗不實假訊息的

---

<sup>142</sup> *Id.* at para. 25-26.

<sup>143</sup> CSA, *Lutte contre les infox: le CSA publie son premier bilan* (2020/07/30), <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Lutte-contre-les-inox-le-CSA-publie-son-premier-bilan> (last visited June 12, 2021).

<sup>144</sup> CSA, *LUTTE CONTRE LA DIFFUSION DE FAUSSES INFORMATIONS SUR LES PLATEFORMES EN LIGNE - BILAN DE L'APPLICATION ET DE L'EFFECTIVITÉ DES MESURES MISES EN OEUVRES PAR LES OPÉRATEURS EN 2019* (2020).

<sup>145</sup> *Id.* at 4.

措施之面向、並給予建議之事項有以下六點：

➤ **引發社會紛擾或左右選情之不實訊息的檢舉回報機制**

大部份的網路業者都採用 CSA 所提供的檢舉回報機制之建議，但檢舉工具的效率取決於使用者在操作上的便利性，因為各家平臺設置的操作模式各有不同，常使得檢舉程序變得繁瑣，且各家平臺提供的查核程序、人力配置與對不實訊息處理方式之相關資料仍相當缺乏。因此 CSA 建議業者簡化相關檢舉程序、提供更多有價值且詳盡的統計數據，並在「事實查核」上建立審查的標準規範和參考來源，鼓勵平臺建立與事實核查機構之間的合作夥伴關係，甚至建立可公開使用的非機密參考資料庫，一方面幫助平臺集中資源，另一方面也可以讓用戶和社會大眾對資訊進行檢視<sup>146</sup>。

➤ **演算法之透明度**

CSA 希望平臺能提供更多可理解且具解釋性的資訊，諸如用以編輯、選擇和分類內容之原則，以及演算法運作之標準和數據資料。雖然有部分平臺之商業模式奠基於演算法的性能，但 CSA 認為特別是內容審查方面之演算法的運用不斷增加，提升透明度之目的並非揭露其業務模式，故平臺仍有必要提供相關資料，進而有利於 CSA 或用戶了解其營運之原則和目標<sup>147</sup>。

➤ **加強出版業者、新聞機構和視聽媒體服務之內容**

各家平臺所使用之查核機制及推廣內容之方式往往有所不同，如

---

<sup>146</sup> *Id.* at 21-32.

<sup>147</sup> *Id.* at 33-39.

大多數之平臺利用視覺標誌以識別可信資訊，有部分平臺讓用戶取得有關消息來源的進一步資訊，還有部分平臺透過演算法來提高或降低資訊的能見度。因此，CSA 鼓勵平臺向用戶提供消息來源之組織名稱和標籤，並提供有關加強「出版業者、新聞機構和視聽媒體服務」（Entreprises et agences de presse et services de communication audiovisuelle, EAP-SCA）所驗證之資訊內容與事實查核之作法，透過透明化「可信」及「權威」之消息來源的分類標準，進而有助於用戶對資訊之認知<sup>148</sup>。

#### ➤ 打擊大規模散布不實訊息之帳戶

數位平臺可對藉由人工或自動方式所檢測出之大規模散布不實訊息之帳戶，採取包含刪除內容、暫時或永久封鎖帳號等因應措施，惟平臺多係「間接」透過打擊網路詐欺或其他行為（如寄發垃圾郵件、煽動仇恨、暴力或色情等內容）以處置大規模散布不實訊息之帳戶，即通常平臺處理帳戶之機制均與帳戶本身無關，且用戶不一定知悉建立「大量轉傳」不實訊息之帳戶的後果。因此，CSA 要求平臺必須提供大規模散布不實訊息帳戶之偵測方式與詳細處理程序，以及這些帳戶所產生的廣告收入資訊，並讓用戶知悉平臺處理此類帳號的措施<sup>149</sup>。

#### ➤ 告知使用者關於贊助或廣告內容之資訊

因數位平臺之商業營收大多主要來自於廣告，包含傳統廣告與受大眾矚目議題有關之贊助、促銷資訊。CSA 鼓勵數位平臺持續為此類

---

<sup>148</sup> *Id.* at 40-48.

<sup>149</sup> *Id.* at 49-57.

內容引入清晰且直接可觸及的標籤，讓用戶容易看到，並提供有關廣告主身分的具體細節，像是提供用戶透明度工具（User transparency tools）和賦予消費者權力的工具，幫助用戶了解其成為投放目標的原因，以及如何設置其廣告偏好工具。此外，為避免出現廣告主可能被一些平臺封殺，而其他平臺卻不封殺的情況，建議平臺之間建立對話窗口，使他們能夠針對有關日常熱門議題的訊息內容得採取更加一致的作法，期待平臺能夠瞭解這些機制對打擊不實訊息的重要性，並能在贊助內容的能見度之透明化措施方面付出努力<sup>150</sup>。

### ➤ 發展更多提升媒體與資訊素養之措施與工具

鑑於公民對資訊來源應有選擇權，當務之急係為數位平臺用戶提供了解網路資訊供給來源之細節、潛在影響與風險之協助與支持。儘管某些平臺已有舉辦相關培育課程，但仍在少數。因此，CSA 建議平臺針對所有用戶開設多面向之媒體與資訊素養（Education aux médias et à l'information, EMI）教育課程；鼓勵平臺與教育界公認之機構和主要利益相關者（公共機構、協會等）建立長期夥伴關係；鼓勵平臺評估其行動對用戶行為的影響；建議平臺與世界研究機構建立協議，以實現數據共享和透明化<sup>151</sup>。整體而言，CSA 肯認數位平臺為對抗網際網路上傳播不實訊息所付出之巨大且不間斷之努力，但在確認訊息內容之真偽實屬不易與平衡言論自由之保障仍需要持續改進目前之因應措施，賦予平臺透過強化識別與檢舉不實訊息機制、處理不實程序之透明化、揭露演算法之功能與效果，並加強與第三方事實查核組

---

<sup>150</sup> *Id.* at 58-65.

<sup>151</sup> *Id.* at 66-69.

織建立合作夥伴關係的期許，希望得以更加有效之對抗不實訊息<sup>152</sup>。

### (三) 資料利用之法制政策

#### 1. 平臺利用資料說明之機制

通訊傳播產業可說是數位時代下最主要的資料流通管道，而數位平臺更是透過蒐集資料並加以分析，提升資料價值以作為重要之競爭利器。

#### 2. 平臺服務條款透明度

##### (1) 《線上中介服務規章》之義務規範

根據歐盟之調查顯示，數位平臺於數位經濟之推動與發展方面，實功不可沒。超過 100 萬家企業透過數位平臺為提供產品或服務，為歐盟市場帶來創新發展之生機，特別是作為歐盟經濟中流砥柱的中小企業 (Small and Medium Enterprise, SME)，其中超過 50% 的企業用戶藉由數位平臺從事跨境商業活動<sup>153</sup>。

然而「平臺對商家」(Platform-to-Business, P2B) 的營運模式存在某些結構性之問題，故在經營的過程中，有近半數 (46%) 的企業用戶曾遇到問題，更有 20% 經常遇到問題；甚至以重度用戶 (指自數位平臺獲利之營業額超過 50%) 角度來看，多達 75% 曾遭遇問題，甚

---

<sup>152</sup> *Id.* at 72.

<sup>153</sup> European Commission, Online Platforms: New European Rules to Improve Fairness of Online Platforms Trading Practices, available at: <https://platformobservatory.eu/app/uploads/2019/05/OnlinePlatformsFactsheet.pdf>. (last visited May. 20)

至更加頻繁地遇到問題的企業用戶也占 32% 的比例<sup>154</sup>。

此外，線上搜尋引擎之服務亦對企業用戶有所影響，像是前 5 個搜尋結果的點擊率高達 88%，而排名第 10 序位之後的搜尋結果僅存 1.11% 的點擊機率。整體而言，有 66%<sup>155</sup>

總歸而言，對於線上中介服務與線上搜索引擎，所衍生的問題均會帶來營業損失，甚至對數位經濟缺乏信任，甚至引發消費者選擇產品或服務之價格與品質減少之風險<sup>156</sup>。

因此，歐盟於 2019 年 6 月通過《促進線上中介服務之企業用戶的公平性與透明性規章》(Regulation (EU) 2019/1150, OIS Regulation, 下簡稱《線上中介服務規章》)<sup>157</sup>，與其後之《數位市場法》草案類似，秉持一貫取締不公平競爭之行為的理念，為線上平臺與線上搜尋引擎提供明確的法遵規範。

而《線上中介服務規章》所規範對象包含所有（約 7,000 個）在歐盟境內營運之數位平臺，上至科技巨擘，下至規模雖小但對企業用戶具重要議價能力的新創公司（small start-up）皆在本規章所囊括的範圍之內。惟本規章實則係為保障相對較無議價能力之中小型企業而設，故藉由本規章，中小型企業可獲益於下列規範事項<sup>158</sup>：

➤ **禁止特定不公平行為**：條款與條件需以易於取得且以簡

---

<sup>154</sup> *Id.*

<sup>155</sup> *Id.*

<sup>156</sup> *Id.*

<sup>157</sup> Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

<sup>158</sup> European Commission, Digital Single Market: EU negotiators agree to set up new European rules to improve fairness of online platforms' trading practices, Press Release (2019/02/14), [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_1168](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168) (last visited June 07, 2021).

明易懂之文字表明，而當條款與條件有所變更時，線上中介服務提供者需在 15 天之前通知，以便企業用戶得即時調整業務，且業務調整之複雜度增加，應伴隨延長通知期間，否則該變更無效；線上中介服務提供者不得在無明確理由或未提供申訴可能性之情況下，暫停或終止企業用戶之帳戶，如係誤為暫停，應立即回復<sup>159</sup>。

➤ **提高線上平臺之透明度：**線上中介服務提供者與線上搜尋引擎服務提供者需以淺明論述揭露其排序商品或服務的主要參數，以供企業用戶理解機制運作方式。由於某些線上中介服務提供者不僅提供平臺服務促進交易進行，更在該平臺中身兼賣家之角色，是為避免不公平競爭，則強制該線上中介服務提供者全面揭露說明基於經濟、商業或法律之考量下任何可能對自家產品給予差別待遇之原因。此外，該等線上中介服務提供者還需揭露所蒐集之資料及使用方式，尤其是與其他企業合作夥伴共享之資料。當涉及個人資料時，則有 GDPR 之適用<sup>160</sup>。

➤ **增設爭端解決機制：**線上中介服務提供者應建立內部申訴處理系統以對企業用戶提供適當協助。線上中介服務提供者應提供調解之協助，以協助企業用戶進行訴外紛爭解決爭議，有效節省時間與金錢之成本<sup>161</sup>。

➤ **執行與監理機制：**商業公會能對違反規則之線上中介服

---

<sup>159</sup> OIS Regulation, Art. 3-4.

<sup>160</sup> OIS Regulation, Art. 5-10.

<sup>161</sup> OIS Regulation, Art.11-13.

務提供者提出告訴，以降低企業用戶對平臺報復行為的恐懼，並降低個別企業用戶之訴訟成本<sup>162</sup>。

《線上中介服務規章》已於通過及公布後的 12 個月後（即 2020 年 6 月）正式施行<sup>163</sup>，且執委會須進行審查評估<sup>164</sup>，並設立專門的線上平臺觀測站（Online Platform Observatory）<sup>165</sup>，以監控市場的變化，並確保新規則有效施行。

## （2）個人資料存取規範

歐盟規定個人資料之蒐集、處理和利用，必須先取得當事人之同意，要求事業企業必須強化同意書的條件，以簡明易懂之文字說明，且必須和其他事項內容有區隔，可以更容易獲得當事人之了解和同意。包含撤銷個資使用同意書，亦不要使用充滿法律術語和難以理解的文字，且需容易撤銷。

再者，GDPR 也賦予歐洲民眾可以選擇「不共用資料」的權利，即歐洲民眾可以拒絕企業共同行銷<sup>166</sup>。

## 三、歐盟法制政策之啟示

歐盟認知到數位平臺，尤其近年受到美國大型跨境數位平臺（尤其是通訊傳播服務數位平臺）之競爭，為了保護歐盟境內中小型企業

---

<sup>162</sup> OIS Regulation, Art.14-15.

<sup>163</sup> OIS Regulation, Art. 19.

<sup>164</sup> OIS Regulation, Art. 16-18.

<sup>165</sup> See European Commission, EU Observatory on the Online Platform Economy, Shaping Europe's digital future, <https://digital-strategy.ec.europa.eu/en/policies/eu-observatory-online-platform-economy> (last visited June 08, 2021).

<sup>166</sup> 黃彥棻，快速入門，專家解讀 GDPR 十大重點，iThome 電腦報，<https://www.ithome.com.tw/news/116876>（最後瀏覽日：2021 年 06 月 04 日）。

與消費者，歐盟一步步有規劃的透過脈絡清晰的資料利用規範，在個人資料利用層面，將控制權完整回歸至資料主體；在非個資利用層面，透過資料主體參與、自主控制資料流通，特別是新增資料可攜權，且鼓勵業者自律，進而打破資料被大型跨境數位平臺事業所獨占之情形。具體作為則是設法與既有的《一般資料保護規章》(GDPR)、《電子商務指令》(ECD)、《線上中介服務規章》(OIS)，以及競爭法 (TFEU Art. 101-102 等) 之規範架構下進行調和，積極藉由歐盟層級 (規章) 之立法模式，為全歐洲建構數位單一經濟市場之公平、有效競爭及隱私保護之環境，進而提升整體之經濟活絡發展。

在市場競爭面向，因具守門人地位之核心平臺服務常見高度垂直整合情形，進而把持數據資料與經濟脈動，遂以《數位市場法》草案對符合一定營業額者之服務提供者課予應為或不應為之義務，惟仍樂見其創新，只是不得以不公平之方式對待企業用戶及消費者，有違者除罰鍰外，甚至可對其祭出結構調整之矯正措施。此外，《數位市場法》草案並不影響原有之競爭法效用，尤其對於大型數位科技平臺之結合案件，歐盟執委會憂心其藉由殺手級併購而造成相關市場競爭之損害，仍持續以競爭法進行調查或嘗試予以罰鍰等制裁手段，期以維持歐洲市場的公平競爭。

而在平臺問責面向，則著重處理線上違法內容，以《數位服務法》草案作為普通法，站在《電子商務指令》之網路中介者之基礎上，再依照類型與規模區分為四種服務提供者之態樣，採取累加義務模式，逐級負擔額外增加之義務，並強調透明度、揭露服務條款或資訊，及配合司法與行政機關之命令等，尚有因應網路數位跨境特性而設計數位服務協調官、歐洲數位服務委員會等，進行整體 EEA 之協調整合；

另外搭配部門硬法，針對特定議題或特化型之數位平臺，以特別法體例課予相關義務之規範，期以建構安全之網際網路空間，進而達到保障數位服務消費者之目的。

綜上所述，歐盟近年轉而以較為積極、事先干預的態度監理數位平臺，雖一方面維持數位平臺自律之呼籲；但一方面也透過對違反規範或不作為之服務提供者設有鉅額之罰則規範，加大法律之力度而加重數位平臺之義務負擔。而包含《數位服務法》草案與《數位市場法》草案在內之包裹式草案（The Digital Services Act package）已列為優先法案，然目前尚在歐洲議會組成聯席委員會進行審查及歐盟部長理事會進行辯論階段，後續立法動態仍值持續觀測。

## 參、英國法制政策研析

### 一、數位平臺市場競爭

英國現行的競爭法主管機關為競爭與市場管理局（Competition and Markets Authority, CMA），其前身為競爭委員會（Competition Commission, CC）與公平交易局（Office of Fair Trading, OFT），兩者並於 2013 年完成整併。此外，除了維繫產業市場競爭秩序的競爭法之外，英國並針對特定產業訂有對應之產業主管法規，以本研究所欲探討之數位平臺服務市場而言，即同時涉及通訊管理局（Office of Communications, Ofcom）以及資訊委員辦公室（Information Commissioner's Office, ICO）之主管權責，亦即網路有害內容之處理，以及個人資料、隱私保護與處理之議題。

數位平臺服務所涉及的爭議在於，受惠於其服務本身的網路與規模效應，使其影響力擴及雙邊或多邊市場，也因此衍生大型數位平臺業者之市場力量是否可能過度延伸，而不利於整體市場的公平、有效競爭；其次，平臺經營者可能因掌握大數據，得以進一步透過演算法、人工智慧等技術，進行更為精準之商業廣告投放、行銷，使得新進業者難以與之抗衡，或因此間接構成市場進入障礙，而衍生限制競爭或不公平競爭之爭議。

此外，近年大型數位平臺業者也經常透過併購途徑，以消弭潛在競爭風險，並藉此構築產品/服務生態系，以鞏固其競爭優勢，卻也衍生市場力過度延伸，引發反競爭行為之疑慮。面對前述之情形，使得 CMA 開始關注具有具有「戰略市場地位」(strategic market status, SMS) 之大型數位平臺服務，並著手研議對應之解決辦法。

作為對應之解決策略，CMA 自 2020 年 3 月起，即透過數位市場工作小組（Digital task force）與 Ofcom 及 ICO 進行合作，研議建置支持數位市場競爭之監理機制，而根據 CMA 於 2020 年 12 月所發布之「支持數位市場的競爭監管機制-數位市場工作小組之政策建議」（A new pro-competition regime for digital markets : Advice of the Digital Markets Taskforce），英國預計於 2021 年於 CMA 成立數位市場部門（Digital Market Unit, DMU），以專責處理網路平臺服務衍生之競爭議題，並規劃針對具有戰略地位之數位平臺業者建置對應之監理機制，而此一監理機制則係有賴執行準則（Code of conduct）、競爭性干預措施（Pro-competitive interventions）與具戰略市場地位業者之結合規範（SMS merger rule），以下將分別簡要進行介紹：

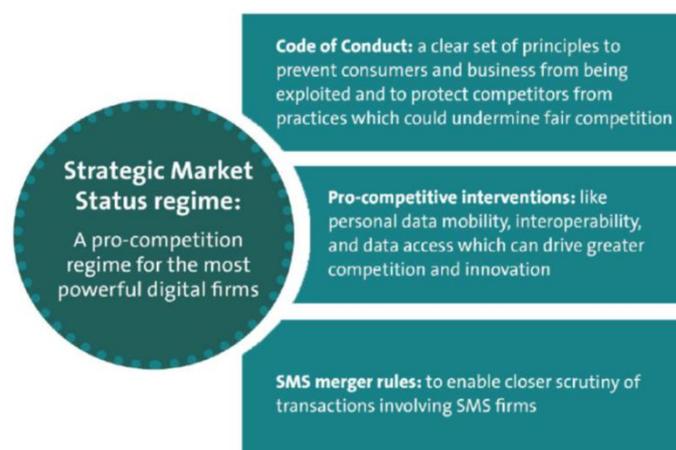


圖 2：戰略市場地位監理機制架構圖

資料來源：CMA

## (一) 監管機關之態度與維持競爭之機制

### 1. 數位市場部門之角色

按 CMA 之規劃，為完善大型數位平臺服務之監理工作，並促進市場競爭與多元創新等目標，政府將採納 2019 年「解鎖數位競爭」(Unlocking digital competition) 報告(下簡稱 Furman 報告)之建議<sup>167</sup>，建立數位市場部門，以解決既有組織專業能力與行政執行能量不足之處，並完發揮三大具體功能：第一，為指定具戰略市場地位之企業，應制訂執行準則；其二，應持續推動個人資料之流動性與開放資料之共同標準；其三，應透過資料開放促進市場競爭。

而依據數位市場工作小組於 2020 年 11 月所發佈之「新型態數位市場競爭監理機制政策建議」(A new pro-competition regime for digital markets- Advice of the Digital Markets Taskforce) 報告<sup>168</sup>，DMU 的設立、運作則將基於以下五大準則<sup>169</sup>：

➤ **證據導向且有效 (Evidence driven and effective)**：考量數位平臺服務之態樣十分多元，難以制訂一體適用之制度，故為使監理機制可有效運作，相關的市場地位評估、指定之制度設計皆應以證據為基礎，以快速反應並有效預防對市場競爭所帶來之

---

<sup>167</sup> Digital Competition Expert Panel, Unlocking digital competition, Mar. 2019, available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/785547/unlocking\\_digital\\_competition\\_furman\\_review\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf) (last visited May. 11, 2021).

<sup>168</sup> CMA, A new pro-competition regime for digital markets- Advice of the Digital Markets Taskforce, Dec 2020, available at [https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital\\_Taskforce\\_-\\_Advice.pdf](https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital_Taskforce_-_Advice.pdf) (last visited May. 11, 2021).

<sup>169</sup> *Id* at 4.

損害。

➤ **精準且合乎比例原則 (Proportionate and targeted)**：相關的規範手段與目標之間需合乎比例性，以解決問題並降低潛在之政策風險。

➤ **開放、透明與可問責性 (Open, transparent and accountable)**：有關規範之運作需基於開放、透明之原則，並妥善諮詢利害關係人之意見，明確說明政策決定之原因，監理單位必須為此負責。

➤ **兼具主動與前瞻性 (Proactive and forward-looking)**：DMU 之角色係聚焦於預防、避免整體市場效益之減損，而非僅只是針對特定反競爭行為、個案進行事後 (*ex post*) 管制，故有必要進行積極評估，以有效控管風險。

➤ **一致性 (Coherent)**：DMU 之組織營運、規劃，應與既有政府部門之組織架構、功能與運作實務達成一致性，尤其應透過數位監理合作論壇 (Digital Regulation Cooperation Forum, DRCF) 進行跨機關合作，以妥善協調相關工作之進行。

在具體的職能上，數位工作小組則建議：應賦予 DMU 資料調閱之權限，得以發動調查，並指定具「戰略市場地位」之特定業者作成處分，而具體之行政處理流程如下<sup>170</sup>：

---

<sup>170</sup> *Id.* at B30.

- 先期調查與證據蒐集。
- 發布啟動指定具戰略市場地位業者之通知。
- 與業者進行諮詢，提供其陳述意見之機會。
- 發布最終決定、處分。

## 2. 戰略市場地位企業之評估標準、指定程序

### (1) 評估標準

為評估數位平臺服務之市場地位，實有必要釐清企業之產品/服務之特定市場行為 (activity) 是否具有重要且根深蒂固之市場力，故應評估該產品/服務之替代程度，是否具有高度之不可替代性，或使用者轉移、使用其他服務時是否有成本過高之情形，進而構成市場參進或者擴張規模之障礙，導致整體市場創新、競爭能力下滑，而有損公共利益，有進一步管制之必要性。

依據數位市場工作小組之建議<sup>171</sup>，應賦予 DMU 指定企業是否具有具戰略市場地位之權力，而具體考量或有以下 5 點<sup>172</sup>：

#### A. 企業大小/規模

該企業之產品/服務，是否以達重要之市場規模，具體指標應包含財務與非財務指標，前者如企業營收、市值等統計資料；後者如使用

---

<sup>171</sup> CMA, Appendix B: The SMS regime: designating SMS firms, available at [https://assets.publishing.service.gov.uk/media/5fce72c58fa8f54d564aefda/Appendix\\_B\\_-\\_The\\_SMS\\_regime\\_-\\_designating\\_SMS\\_firms.pdf](https://assets.publishing.service.gov.uk/media/5fce72c58fa8f54d564aefda/Appendix_B_-_The_SMS_regime_-_designating_SMS_firms.pdf) (last visited May. 11, 2021).

<sup>172</sup> *Id* at B14-B18.

者數量、產品使用時間，以及促成交易之總體價值等指標。舉例而言，如特定產品/服務已擁有相當之市占率，擁有龐大之用戶數量時，或可認定其已擁有相當之市場力量。

B. 該企業所從事之商業行為，是否為連結消費者的  
重要通路

企業所提供之產品/服務是否以成為連結消費者的重要通路（gateway），具體實例如 Amazon 公司的電商平臺所提供之服務，係媒合產品製造商與消費者之重要中介者，故可視該平臺為重要之通路，扮演關鍵之市場機能、角色。

C. 該企業從事之特定行為，是否可促使企業擴張、  
保護其市場力

該企業所提供之產品/服務是否有助於其延伸市場力至其他市場，並進一步鞏固、強化其所既有之市場力量、地位。舉例而言，例如當社群媒體服務兼營網路廣告、電子商務等服務時，受惠其服務之網路效應，其擁有龐大之使用者規模，故可能導致其市場力延伸至周邊市場，並藉此構築更為完整之產品／服務生態系，同時鞏固其核心服務之市場領先地位。

D. 該企業是否可以透過制訂其產品／服務生態系之  
運作規則，進一步影響更大範圍之市場參與者

該企業所提供之產品／服務是否有助於其延伸市場力至其他市

場，並進一步鞏固、強化其所既有之市場力量、地位。舉例而言，當社群媒體服務兼營網路廣告、電子商務等服務時，受惠其服務之網路效應，其擁有龐大之使用者規模，故可能導致其市場力延伸至周邊市場，並藉此構築更為完整之產品／服務生態系，同時鞏固其核心服務之市場領先地位。

E. 該產品/服務所為之商業行為，已為市場帶來更廣

泛之社會、文化之影響

由於搜尋引擎與社群媒體等服務涉及新聞內容與資訊的傳遞、擴散，故可能涉及言論自由保障之範疇，故其營運實際上擁有高度之政治、文化影響力。

## (2) 數位市場工作小組之建議

承繼前述對於指定具戰略市場地位之業者之主要考量，數位市場工作小組亦建議 DMU 應制訂對應市場地位測試、評估指南，指南內容並應以下三點：其一，該公司之年度營收；其二，該公司所從事商業行為之本質；最後，並應考量是否有其他部門監理單位更適合介入、處理所涉及之競爭規範。

有關營收標準之設計，應以英國境內之年度營收為主要標準，全球營收為輔，故其規劃為英國境內年度營收超過 10 億英鎊，同時需特別關注年度營收超過 25 億英鎊之業者，應具有相當之市場地位。然而，數位市場工作小組亦指出，不建議將年度營收直接列為法定標準，請該標準應不定期進行滾動修正，以保留一定之彈性，有效處理

市場的潛在問題<sup>173</sup>。

其次，DMU 應妥善定義其管轄範圍，DMU 之任務應聚焦於數位產品/服務所衍生之數位行為，且具體之監理對象為平臺、線上平臺服務，其相關市場之部門則含括網路電商平臺、APP 商店、社群媒體平臺、網頁瀏覽器、線上搜尋引擎、操作系統及雲端運算服務等態樣<sup>174</sup>。

### (3) 指定流程與救濟途徑

具體而言，若有企業遭到 DMU 指定具有戰略市場地位時，此一指定處分之效力為 5 年，並將附帶矯正措施。

### 3. 執行準則

承上，CMA 亦將擬定市場調查、市場力評估、處分、救濟等程序之執行準則。而根據數位市場工作小組之建議，其認為準則之建立應以以下三大目標為基礎進行規劃。首先，需符合公平交易（fair trading）原則，使用者需受到公平、無差別歧視之對待，並與具戰略市場地位業者於合理之商業模式下進行交易，以解決數位平臺業者所為之剝削行為；其次，需遵守開放選擇（open choices）原則，使用者可以自由、無障礙之選擇由具戰略市場地位之業者，或其他企業所提供之同質性服務；最後之目標則為信任與透明度（trust and transparency），DMU 應確保具戰略市場地位之企業將提供使用者充分之資訊，以利使用者做出正確決定。

---

<sup>173</sup> *Id* at B23.

<sup>174</sup> *Id* at B24.

而為確保 DMU 可以承擔前述之監理工作，數位市場工作小組建議應賦予 DMU 調查權，若經 6 個月之調查期間，認定有違法事實時即可發出違法通知，敘明違法事由外，並提供業者意見陳述之機會<sup>175</sup>，以決定是否做出相應之處分，課予業者負擔矯正措施之義務，或處以對應之罰鍰<sup>176</sup>。

#### 4. 競爭性干預措施<sup>177</sup>

有關競爭性干預措施 (pro-competitive intervention, PCI) 之態樣，整理羅列如下：

##### (1) 與資料相關之干預措施<sup>178</sup>

考量「資料」已是數位平臺運作不可或缺之重要元素，故數位市場工作小組建議，DMU 應有權實施與資料相關之競爭干預措施 (data-related interventions)，以降低大型數位平臺所構築之市場參進障礙，並降低消費者轉換服務之成本，同時強化使用者對於其個人資料的控制能力，以有效促進市場競爭與創新發展，並兼顧資料與隱私權保護。

##### A. 消費者控制矯正措施

消費者控制矯正措施 (consumer control remedies) 係促使消費者得以更為妥善管控其個人資料，具體舉例如可透過控管企業對於個資

---

<sup>175</sup> *Id* at C41.

<sup>176</sup> *Id* at C47.

<sup>177</sup> CMA, Appendix D: The SMS regime: The pro-competition interventions, available at [https://assets.publishing.service.gov.uk/media/5fce70118fa8f54d58640c7f/Appendix\\_D\\_-\\_The\\_pro-competition\\_interventions\\_.pdf](https://assets.publishing.service.gov.uk/media/5fce70118fa8f54d58640c7f/Appendix_D_-_The_pro-competition_interventions_.pdf) (last visited May. 11, 2021).

<sup>178</sup> *Id* at D8-D9.

蒐集、使用、分享與促進資料可攜等使用條款之訂定情形，以完善相關資料之保護措施。

### B. 資料接取矯正措施

資料接取矯正措施 (data access remedies) 係授權第三方單位可取得由具戰略市場地位業者所蒐用之資料，以供市場新進業者用以發展創新服務，降低因關鍵資料所構築而成的市場參進障礙。

### C. 資料孤島矯正措施

資料孤島矯正措施 (data silo remedies) 係管理具戰略市場地位之業者間的資料使用分享機制，以避免因不同企業使用不同之資料格式，導致資料無法流通、共同使用。

## (2) 互通與共同標準

互通 (interoperability) 與共同標準可要求不同系統、裝置採取開放、標準化之格式，以具體實踐資料可攜權，並可強化不同系統間的相容性，使不同系統間得以進行合作。

## (3) 消費者選擇權利與預設干預

有鑑於部分硬體裝置所預先安裝之軟體，對於消費者使用與否之決定具有關鍵影響力，消費者選擇權利與預設干預 (defaults intervention) 除可能鞏固特定業者之市場地位外，並間接導致新興服務在市場競爭上居於劣勢，因此，此一措施乃是限制系統不得有預先安裝之行為，或應提供消費者自由選擇之權利，由其自主決定是否進

行安裝。

(4) 產品／服務接取需遵守公平、合理與無差別待遇原則之義務<sup>179</sup>

此一措施係授權 DMU 進行規範，要求企業提供之服務應基於公平、合理且無差別待遇之原則。具體舉例如基礎設施、服務應基於此一原則提供接取。

(5) 分離矯正措施<sup>180</sup>

在分離矯正措施 (separation remedies) 的部分，一般而言可以採取營運分離與所有權分離兩類之矯正措施，簡述如下：

➤ **營運分離矯正措施 (Operational separation remedies)：**

係要求企業內部不同功能之部門分別獨立進行營運，惟仍受同一企業所控制，同時由監理機關進行持續性監測。

➤ **所有權分離矯正措施 (Ownership separation remedies)：**

係禁止單一公司透過所有權控制其旗下不同部門之營運，是相對於營運分離措施強度更高之干預措施。

惟根據數位市場工作小組之建議，其僅建議授權 DMU 可實施營運分離矯正措施之權限，而不建議得以實施所有權分離措施。主要考量在於，所有權分離乃是極為侵入性之干預措施，故此一權限仍保留予競爭法主管機關 CMA 所負責，若其認為有必要採取結構分離措施，

---

<sup>179</sup> *Id* at D15.

<sup>180</sup> *Id* at D18.

將任命獨立之審查小組，以評估是否有實施分拆 (divestiture) 措施之必要性<sup>181</sup>。

## 5. 戰略市場地位企業結合規範<sup>182</sup>

### (1) 現行制度介析

有關英國企業結合管制之規範，主要係由競爭與市場管理局 (Competition and Markets Authority, CMA) 所負責，CMA 並針對企業結合之規範訂定有相關實務指引，諸如《管轄權與程序指引》(Mergers: Guidance on the CMA's jurisdiction and procedure)<sup>183</sup>、《結合評估指引》(Merger Assessment Guidelines)<sup>184</sup>。而以英國之現行規範而言，企業間的結合係採取自願通報，而非強制性規範，CMA 僅有權進行調查，且其管轄權僅有在結合案達到相關標準，或因涉及重大公共利益時，可主動進行審查。

有關前述啟動調查之標準，主要係「營業額評估」(turnover test) 與「市占率評估」(share of supply)。前者之規範，主要是針對試圖併購具有一定市場地位之目標之結合案，故其門檻為被收購標的於英國

---

<sup>181</sup> *Id* at D20.

<sup>182</sup> CMA, Appendix F: The SMS regime: a distinct merger control regime for firms with SMS, available at [https://assets.publishing.service.gov.uk/media/5fce706ee90e07562d20986f/Appendix\\_F\\_-\\_The\\_SMS\\_regime\\_-\\_a\\_distinct\\_merger\\_control\\_regime\\_for\\_firms\\_with\\_SMS\\_-\\_web\\_-\\_pdf](https://assets.publishing.service.gov.uk/media/5fce706ee90e07562d20986f/Appendix_F_-_The_SMS_regime_-_a_distinct_merger_control_regime_for_firms_with_SMS_-_web_-_pdf) (last visited May. 11, 2021).

<sup>183</sup> CMA, Mergers: Guidance on the CMA's jurisdiction and procedure, available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/987640/Guidance\\_on\\_the\\_CMA\\_s\\_jurisdiction\\_and\\_procedure\\_2020.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987640/Guidance_on_the_CMA_s_jurisdiction_and_procedure_2020.pdf) (last visited May. 11, 2021).

<sup>184</sup> CMA, Merger Assessment Guidelines, available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/986475/MAGs\\_for\\_publication\\_2021\\_-\\_pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986475/MAGs_for_publication_2021_-_pdf) (last visited May. 11, 2021).

境內之年營業額至少為 7000 萬英鎊；其次，有關市占率測試之部分，係當兩公司結合後之於英國之市場占有率將達 25%<sup>185</sup>。在完成調查後，CMA 可以禁止企業之結合，或透過設定附款之條件限制，以維繫市場公平、有效之競爭環境。

然而，英國既有之規範卻難以因應目前大型數位平臺業者所頻繁進行之併購行為，主要原因在於此類業者多採取垂直或多角化結合之方式，以擴張、建置其產品/服務生態系，以鞏固其核心產品/服務之市場地位，卻因相關企業之結合多涉及不同之產銷階段，結合雙方既不是相互競爭者，也並非另一方投入要素的供給者，其所涉及之產品/服務彼此間為互補關係，或無關連性，故相對於水平結合之競爭疑慮較低<sup>186</sup>，故英國政府多仍採取許可之態度。然而，問題在於，此類型的交易往往可能涉及下列潛在之競爭問題<sup>187</sup>：

- 被併購之企業，於未來可能發展成併購方企業之直接競爭者，故併購行為等同提前消弭潛在之市場競爭。
- 被併購企業擁有可支援併購方企業競爭對手進入市場或擴張規模之重要資產，而可以維繫其市場領先地位。
- 併購方可能於結合後採取閉鎖（foreclosure）策略，以強化或擴張其既有之市場力量。

面對前述之困境，CMA 目前在結合案評估、審查上多採取「實質減少競爭檢定」（SLC），亦即結合案是否應予禁止，係取決於其實

---

<sup>185</sup> CMA, *supra* note 182, F6-F7.

<sup>186</sup> 胡祖舜，競爭法之經濟分析，頁 382，元照，2021。

<sup>187</sup> *Id.* at F7-F8.

質上是否將減少市場競爭，亦即《歐盟結合規章》(EC Merger regulation)<sup>188</sup>第 2 條第 3 款<sup>189</sup>所言之「尤其於產生或增強事業優勢地位而嚴重妨害共同市場，或相當一部份區域內有效競爭並受到顯著損害之結合案，應宣告與共同市場不相容」。

經 CMA 調查後，若經其評估認定可能導致英國任一產品/服務市場內部競爭的顯著減少，可以採取結構矯正、行為矯正等措施。前者含括禁止結合，或要求企業進行所有權分離 (divestiture)，以維持或恢復市場的競爭狀態，後者具體如智慧財產權補救措施 (IP remedies)、支持措施 (Enabling measures) 與結果控制 (Controlling outcomes) 措施等態樣<sup>190</sup>。

## (2) 未來規劃

依照數位市場工作小組之建議，英國目前仍傾向將具戰略市場地位之數位平臺業者所涉及之結合案交由 CMA 進行處理，惟課予俱戰略市場地位之業者額外之通知義務，要求有關業者之結合需進行事前通知，且需待主管機關同意後方能生效<sup>191</sup>。

---

<sup>188</sup> Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (EC Merger Regulation).

<sup>189</sup> EC Merger Regulation, Art. 2.

<sup>190</sup> CMA, Merger remedies, p.14-16. available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/764372/Merger\\_remedies\\_guidance.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/764372/Merger_remedies_guidance.pdf) (last visited May. 11, 2021).

<sup>191</sup> *Id* at F23.

## (二) 資料應用對市場競爭之影響

### 1. 資料保護法制發展現況

英國個人資料保護主管機關為資訊委員辦公室 (Information Commissioner's Office, ICO)，英國雖於 2016 年透過公民投票決定將退出歐盟，並於 2020 年始完備相關脫歐程序，惟依據《2018 年脫歐法》(European Union (Withdrawal) Act 2018) 第 3 條第 1 項，過去曾適用之歐盟直接立法，於脫歐後仍為英國內國法之一部分，故歐盟 GDPR 將繼續於英國適用，而為消除 GDPR 與英國內國法間之落差，英國於 2018 年通過現代化之資料保護架構，並建立與 GDPR 一致的個人資料保護標準。

此外，受到脫歐政策之影響，由於英國將不再具有歐盟成員國之身分，故仍需取得歐盟 GDPR 之適足性認證 (adequacy decision)，以處理脫歐後，英國與歐盟間個資保護法制落差與銜接之問題。而為因應此一問題，英國已於 2020 年 12 月的最後過渡期 (Transition period) 與歐盟達成貿易與合作協議 (Trade and Cooperation Agreement, TCA)<sup>192</sup>，自 2021 年 1 月 1 日起為期 4 個月的「過渡期」中，英國將不被視為第三國，此一協議並將自動延長六個月，除非英國或歐盟單方面反對，且英國應於此一期間完成相關法制銜接工作。

基此，歐盟執委會於 2021 年 2 月 19 日通過基於 GDPR 與《執

---

<sup>192</sup> Document 22021A0430(01), Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part.

法指令》(Law Enforcement Directive, LED)<sup>193</sup>所撰擬之《資料適足性認證草案》(Draft Data Adequacy Decisions)，該草案目前正由歐盟個資保護委員會(European Data Protection Board, EDPB)與歐盟成員國代表所組成之委員會進行審查<sup>194</sup>。

待草案正式通過，英國即取得歐盟個資保護之適足性認證，允許個人資料從歐盟(European Union, EU)和歐洲經濟區(European Economic Area, EEA)繼續自由轉移至英國；若未通過，自EEA移轉個人資料至英國之行為仍須遵守GDPR之規範。

## 2. 資料可攜相關規範

所謂資料可攜權係指個人有權利取得其提供與資料蒐用者之資料，且該資料需以結構化、常用且機器可讀之形式提供，並有權要求資料蒐用者可傳輸其資料予其他資料蒐用者。以下則分別就歐盟GDPR與英國資訊委員辦公室發布之《GDPR指引》<sup>195</sup>，進行介紹：

### (1) GDPR

#### A. 行使要求與方式

依據GDPR第20條第1項之規定，當個資蒐用屬於下列情形

---

<sup>193</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

<sup>194</sup> ICO, Data protection at the end of the transition period, available at <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/> (last visited June 05, 2021).

<sup>195</sup> ICO, Guide to the General Data Protection Regulation(GDPR), available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> (last visited June 5, 2021).

時，資料主體有權接收其提供給資料管控者之個資；管控者需以結構化、常用且機器可讀之形式進行提供，資料主體並有權將之傳輸予其他管控者，而不受提供個資管控者的妨礙：

- 個資蒐用係基於資料主體之同意，或基於履行契約之必要。
- 個資蒐用係以自動化方式進行者。

依照同條第 2 項之規範，在技術許可之前提下，資料主體應有權要求其個資無須經過資料主體之轉送，而由資料控管者直接傳輸至其他資料控管者。

## B. 行使限制

依據 GDPR 第 20 條第 3 之規定，資料可攜權之行使，不應妨礙同法第 17 條<sup>196</sup>刪除權之行使；且資料可攜權不適用於當資料管控者蒐用資料之行為乃是基於公益，行使公權力或執行職務所必要之行為。此外，依據同條第 4 項之規定，資料可攜權之行使不應對他人自由權利造成不當之影響。

### (2) 資訊委員辦公室之 GDPR 指引

資料可攜權之目的在於允許不同之系統可以共享資料、資源，而為於英國實踐資料可攜權，ICO 並公布有相關指引。以下將針對該指引有關資料可攜權所訂定之規範進行介紹：

---

<sup>196</sup> GDPR, Art. 17.

## A. 資料範圍

有關資料可攜權可請求之範圍，具體而言可包括以下 3 種態樣<sup>197</sup>：

- 網頁瀏覽或關鍵字搜尋之記錄。
- 交通與定位資料。
- 由智慧型電表、穿戴式裝置等連網裝置所處理之原始資料。

除前述之態樣外，有關基於使用者所提供之個人資料所進行額外處理、加工之資料並不在資料可攜權之請求範圍之內。

## B. 匿名資訊與假名資訊

有關資料可攜權可請求之範圍，僅限定於個人資料，且不適用於已完全匿名（anonymous）之個人資料，惟可透過特定技術回溯、連結個人之假名資料（pseudonymous）仍為資料可攜權之涵蓋範圍<sup>198</sup>。

## C. 資料格式

依據 GDPR 前言第 68 點<sup>199</sup>，應鼓勵資料蒐用者開發可互通之格式，以實現資料可攜性。資料可攜權之目的在於允許不同之系統可以共享資料、資源，而為於英國實踐資料可攜權，ICO 並公布有相關指引<sup>200</sup>。在該指引中，ICO 考量部分產業部門有其特殊格式之需求，故

---

<sup>197</sup> ICO, *supra* note 195, at 130.

<sup>198</sup> *Id.* at 133.

<sup>199</sup> GDPR, Rec. 68.

<sup>200</sup> ICO, *supra* note 195, at 133-134.

若企業使用之格式符合結構化、常用且為機器可讀之形式，其仍符合資料可攜權所要求之規範。

資料格式除應符合前述之基本原則外，英國 GDPR 雖未要求企業內部需採用開放格式，但若使用之格式導致資料主體無法進用相關資料時，仍須進行附加處理，使相關資料符合資料保護法制所要求之格式規範。

此外，若企業所屬之產業部門並未使用特定共通格式，該指引則建議企業使用 CSV、XML 與 JSON 等易於使用，且符合資料可攜權規範之格式設計<sup>201</sup>。

### 3. 資料可攜、分享實務規範

依據《2018 年資料保護法》第 121 條<sup>202</sup>，ICO 針對資料分享訂定有《資料分享實務準則》(Data sharing code of practice)<sup>203</sup>，要求個人、企業與組織得以透過公平、安全且透明之方式分享個人資料，並於符合資料保護之法律規範之前提下，執行相關法律遵循工作<sup>204</sup>。

#### (1) 規範主體

本準則主要之適用對象，係指歐盟《一般資料保護規則》以及英國《2018 年資料保護法》定義下之資料管控者，特別是所謂的資料保護長(Data protection officer, DPO)，亦即擁有決定個人資料蒐用目的、

---

<sup>201</sup> *Id.*

<sup>202</sup> Data Protection Act 2018, Sec. 121.

<sup>203</sup> ICO, Data sharing code of practice, available at <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/> (last visited June 5, 2021).

<sup>204</sup> *Id.* at 48.

方式權限之對象。換言之，此一準則之訂定係為規範資料管控者間的資料分享行為。

而所謂數據分享行為之定義，於本準則係指透過傳輸、散佈或其他可行之方式揭露個人資料，可能之行為態樣如下：

- 透過任何方式向第三方單位提供個人資料。
- 作為數據分享的共同參與者，基於資料分享協議接收個人資料。
- 個人資料的雙向傳輸行為。
- 透過 IT 系統授予第三方單位訪問個人資料之權限。

## (2) 規範模式

具體而言，資料共享行為須遵守《2018 年資料保護法》之規範，除涉及重大公共利益之特殊情境下可取得豁免外，應取得個人資料主體之同意，且資料主體得以拒絕、撤回許可，且分享行為僅得以就其蒐用目的、蒐用期間內進行使用，同時應採取適當之技術、措施避免資料遺失、破壞，以維繫個人資料主體之權益。

除此之外，為協助實施者執行相關法遵作業，本準則亦針對資料分享協議訂定有基本原則與注意事項，並設計有資料分享檢核表，以協助實施者踐行相關準備工作與程序，妥善保護個資主體之資料安全。本研究並將於以下進行說明：

## A. 個人資料保護、隱私規範

根據《2018年資料保護法》之規範，個人資料的蒐集與利用均須取得資料主體之同意，故當共享資料涉及敏感性個資，且可能對於個人帶來重大影響，資料管控者應進一步進行溝通，並主動發布隱私通知（privacy notice）<sup>205</sup>，以完備相關通知程序。然而，若基於犯罪預防、偵察，或為逮捕、起訴嫌犯，以及稅捐稽徵等目的時，資料共享無須取得當事人之同意，以避免情資外洩而影響檢警行動之執行。

另外，因資料分享僅得以於其蒐用目的、蒐用期間內進行合理使用，並須採取適當技術、措施以避免資料遺失、破壞，同時確保資料持續更新，故為協助業者落實有關之法遵作業，ICO除針對系統性與一次性資料共享訂定有工作檢核表（Data sharing checklists）<sup>206</sup>，並要求業者具體考量共享資料之目的，將與哪些組織進行資料共享，以及共享行為可能導致之風險，以制訂合宜之資料分享計畫，以及資料共享協議。

## B. 資料安全性之確保

根據《2018年資料保護法》之規範，資料管控者應採取適當之技術與組織措施，以確保資料共享行為之安全性。基此，資料管控者應綜合考量資料之機敏性及參與組織之複雜程度，以及安全性漏洞可能導致組織營運、聲譽受損等影響下，建立合理之物理隔絕系統與技術

---

<sup>205</sup> *Id* at 18.

<sup>206</sup> *Id* at 48.

防護措施。

有關前者的部份，具體舉例如應建置有完善之訪客管理系統，且筆記型電腦、隨身碟等儲存裝置應存放於安全之環境；後者之部份，應要求該組織建置資料安全管理系統，確保資料之接取過程應歷經妥善之加密程序，以有效降低整體資料損毀、外洩之風險。除此之外，資料分享實務準則亦建議從事相關行為之組織應簽署資料共享協議，以確保個資分享過程得以順利進行。

### C. 資料共享協議

依據《資料分享實務準則》，ICO 建議在進行分享數據前應進行資料保護影響評估（Data protection impact assessment, DPIA），並簽訂數據分享協議，以確保符合相關法制規範，並保障資料主體之權利，若有嚴重違反資料保護規範之行為，最高將可處以 1,750 萬英鎊，或該公司全球年營業額 4% 之罰鍰<sup>207</sup>。

### D. 個人權利

為確保資料主體之權利，《資料分享實務準則》除指明資料分享行為須取得資料主體之同意外，並有權得知其個資使用用途，並得以於個資使用導致其重大損害時撤銷授權，個資管控者並應於接受請求之 21 天內進行回覆，以落實資料主體之權益保障。

---

<sup>207</sup> *Id* at 12.

### (三) 小結

針對近年數位平臺服務蓬勃發展所帶來的市場競爭議題，英國政府提出之對應措施主要係於競爭與市場管理局之組織架構下，成立專責之數位市場部門，並針對具戰略市場地位之數位平臺業者訂定對應之監理機制。

首先，其考量在於，大型數位平臺業者受惠於網路效應而有龐大之經濟規模，且逐步透過垂直、多角化結合行為擴張其市場影響力，存在有從事反競爭行為之疑慮；其次，面對前述之疑慮，英國既有監理架構在制度設計與專業行政能量之培育，均面臨難以因應、負荷之困境。綜合前述之考量，同時為避免過度干預市場自由競爭、發展，故英國係採取事前管制措施，透過具體之評估方法，指定具有戰略市場地位之業者，並課予其對應之管制義務，或實施對應之矯正措施，以有效維繫、建置適宜競爭之市場環境。

而有關影響數位平臺服務最為關鍵之投入要素「資料」，英國之主管機關為資訊委員辦公室（Information Commissioner's Office, ICO），而雖英國已正式脫歐，惟透過《2018年歐盟（退出）法》之規範，歐盟《一般資料保護規則》將繼續於英國適用，與《2018年資料保護法》共同構築英國之資料保護規範體系。

其中，有關資料可攜之規範，英國之制度係與歐盟接軌，亦即同樣須遵守《一般資料保護規則》，故個人有權取得其提供與資料蒐用者之資料，且該資料須以結構化、常用且機器可讀之形式進行提供。而有關英國針對資料可攜權之具體實踐，ICO制訂有《資料分享實務準則》（Data sharing code of practice），協助從事資料分享行為之組織

進行法遵工作，資料管控者除須建置、完善資訊安全管理體系外，並應確實取得個人資料主體之同意，同時與合作組織簽署資料共享協議，於確保個人資料主體全一之前提下，最大化個人資料之使用效益。

## 二、數位平臺問責

### （一）數位平臺監理機制

隨著資通訊科技快速演進，使得數位平臺服務與周邊衍生之服務生態系蓬勃發展，而鑑於此類服務之市場規模與社經影響力的持續擴張，也進一步帶動世界各國監理機關與公民社會對於社群媒體、搜尋服務的關注，並試圖課予業者進一步的法定義務，以避免使用者受到網路危害內容之影響，並促使數位平臺服務可接受外部監督，以解決此類型服務過往欠缺民主課責性不足之缺陷。

而有關英國數位平臺服務的規管法制，在英國脫歐前，數位平臺服務之主要規範係集中於歐盟《電子商務指令》以及英國內國法《2002年電子商務管制法》（Electronic Commerce Regulations 2002）。

而雖英國已正式退出歐盟，但由於前述兩者具有類似之規範架構，故適用上並未衍生其他疑義。《2002年電子商務管制法》之規範架構，旨在規範中介服務提供者之責任，並將作為資訊服務媒介的網際網路服務提供者（Internet Service Provider, ISP）區分為三種型態，包括連線服務提供者、快速存取服務提供者、資訊儲存服務提供者等三者，並設置有安全港免責規範。

## 1. 納管基準與規範

《2002年電子商務管制法》第2條<sup>208</sup>，該法之規範主體為「資訊社會服務」，而該服務之具體要件有以下三點：(1) 通常為付費提供；(2) 遠距提供 (at a distance)；(3) 以電子設備處理與儲存資料 (含數位壓縮)，具體而言涵蓋電商平臺、通訊服務、網路搜尋引擎、視聽服務串流等服務之態樣。

## 2. 責任安全港規範

有關中介服務提供者責任的規範，係《2002年電子商務管制法》的重心，亦即服務提供者的責任安全港規範，服務提供者於符合特定條件下，可免除傳輸或儲存由第三人提供之違法資訊的法律責任。以下則分就不同態樣服務之免則規範進行介紹：

### (1) 連線服務提供者

依據《2002年電子商務管制法》第17條之第1項之規定<sup>209</sup>，連線服務為資訊社會服務的一種類型，而包含對於在通信網路中傳輸服務接受者所提供的資訊，或提供通信網路的接取者，符合以下要件時，其資訊傳輸行為不須負擔損害、金錢賠償，以及刑事處分之責任：

---

<sup>208</sup> The Electronic Commerce (EC Directive) Regulations 2002 § 2.

<sup>209</sup> The Electronic Commerce (EC Directive) Regulations 2002 § 17(1).

- A. 未發起傳輸行為。
- B. 未選擇傳輸之接收者。
- C. 未選擇或修正所傳輸之資訊。

另外，依據同條第 2 項<sup>210</sup>之規範，連線服務之要件尚包含以下內容：係基於通信網路內傳輸之唯一目的，對於所傳輸的資訊為自動化、中介性質與暫時性的儲存，且資訊儲存時間並未超過傳輸所須之合理期間。

## (2) 快速存取服務提供者

依據《2002 年電子商務管制法》第 18 條之規定<sup>211</sup>，快速存取服務為資訊社會服務的一種類型，包含通訊網路中傳輸由服務提供者提供資訊時，若遇有以下情形時，服務提供者無須對為了僅讓其他接收者在其要求下，基於使資訊傳輸更有效率之單一目的，而對資訊所為之自動化、中介性質與暫時性的儲存行為負擔損害、金錢賠償，以及刑事處分之責任：

---

<sup>210</sup> The Electronic Commerce (EC Directive) Regulations 2002 § 17(2).

<sup>211</sup> The Electronic Commerce (EC Directive) Regulations 2002 § 18.

- A. 服務提供者並未修改該資訊。
- B. 服務提供者遵守資訊接取之條件。
- C. 服務提供者遵守資訊更新之規範，尤其是由產業所廣泛承認、使用之規範。
- D. 服務提供者並未干涉，有關合法使用廣泛為產業所承認、使用之技術，以取得資訊使用的資料。
- E. 服務提供者確實知悉該資訊之原始來源，並已針對該資訊進行移除或使之無法接取，或法院、行政機關命其移除或使之無法接取時。

### (3) 資訊儲存服務提供者

依據《2002年電子商務管制法》第19條<sup>212</sup>，資訊儲存服務為資訊社會服務的一種類型，提供資訊儲存之服務，而在符合以下情形時，服務提供者無須為其儲存行為負擔損害、金錢賠償，以及刑事處分之責任：

- A. 服務提供者實際上並未認識不法活動或資訊，且在有關損害賠償的請求上，並未察覺該行為或資

---

<sup>212</sup> The Electronic Commerce (EC Directive) Regulations 2002, sec 19.

訊有明顯違法之事實與情況，或於察覺違法適時後，立即採取資訊移除與禁止接取措施。

B. 資訊之接收者並非基於儲存服務提供者的授權、控制下從事相關行為。

綜上，《2002年電子商務管制法》對於連線、快速存取與儲存服務等不同之服務態樣所訂定之責任安全港規範，而為掌握有關規範落實之情形，以下將簡要介紹數則英國判決先例，透過實務見解之補充，以瞭解安全港規範於英國實踐之情形。

### 3. 法院對 ISP 角色認定及作為義務之見解

在普通法層面，法院在下列判例裡揭示 ISP 與出版人的角色差異：

#### (1) 2001 年 *Godfrey v. Demon Internet Ltd.* 案

法院於此案<sup>213</sup>針對 ISP 是否應視為出版人表示其見解。此案涉及網路誹謗，被告為一 ISP 業者，在此案中被視為內容儲存(content host)服務提供者。然法院認為被告之角色可類推適用 19 世紀案件，類似書商與包裹運送人的角色，不能因為被告不知悉系爭內容即可否認其出版行為；法院認定被告在一定日期知悉系爭文字後卻未將之移除，而判決其敗訴。

---

<sup>213</sup> *Godfrey v Demon Internet Service* [2001] QB 201.

## (2) 2006 年 *Bunt v. Tilley* 案

此案<sup>214</sup>為英國第一個區分單純連線服務提供者與出版人差異的案例，原告控告在網路上發表誹謗言論的發文者與三家 ISP 業者，主張三家 ISP 業者為二次出版人 (secondary publisher)，應負連帶責任。法院駁回原告此部分主張，認為 ISP 僅為被動的溝通工具，且 ISP 並未知悉出版系爭文字的出版經過，不應該將 ISP 視為二次出版人。

其後，法院更進一步地肯認資訊儲存服務提供者如 Google，其僅為被動傳輸工具的角色：

## (3) 2009 年 *Metropolitan International Schools* 案

此案<sup>215</sup>關於在 Google 上搜尋所獲得涉及個人的誹謗言論，Google 是否應負責任之爭點上，法院採取 *Bunt v Tilley* 案見解，認為 Google 只是被動的角色和傳輸工具，搜尋結果並非 Google 有意為之的輸出內容，不構成二次出版人。法院認為此為科技上的侷限，Google 無法避免此類不法言論出現，且縱使出現此類不法言論，並不必然表示 Google 是有意挑選該搜尋結果，因而 Google 得受安全港免責機制之保護。

最後，更透過兩例涉及 Google 旗下之平臺（即 Blogger.com）之案件，進一步探討網路中介者作為義務的判斷標準，其爭點為：若部落格主在 Blogger.com 發表不法言論時，Google 在收到原告通知後

---

<sup>214</sup> *Bunt v Tilley* [2007] 1 WLR 1243.

<sup>215</sup> *Metropolitan International Schools Ltd v Designtechnica Corp and Google* [2009] EWHC 1765 (QB).

是否有作為義務？

#### (4) 2011 年 *Davison v Habeeb & Ors* 案

在此案<sup>216</sup>中，法院認為部落格網站之格主自有能力可以移除系爭言論，且 Google 收到來自原告與部落格格主兩方的矛盾資訊，無從判斷資訊真偽，因而無須有所作為。

#### (5) 2013 年 *Tamiz v Google* 案

初審法院<sup>217</sup>與上訴法院於此案<sup>218</sup>採取不同見解。初審法院採 *Davison v Habeeb & Ors* 案之見解，認為 Google 只是「一個塗滿塗鴉的牆面之擁有者」，沒有任何義務採取主動的措施，亦不須負擔任何不作為之責任；上訴法院卻認為 Google 在收到原告通知後應有作為義務，否則無安全港免責機制之適用，惟因系爭言論不構成誹謗，故上訴法院遂駁回上訴；此案亦揭示了單純的申訴通報不等同於「通知」，要求平臺取下系爭言論前須有足夠證據支撐。

### 4. 網路著作權保護層面 ISP 作為義務

2009 年 6 月，英國商業、創新及技能部 (Department for Business Innovation and Skills, BIS) 與英國 DCMS 發布「數位英國報告」(Digital Britain Report)<sup>219</sup>，揭示在全球邁向數位知識經濟的時代下，英國所

---

<sup>216</sup> *Davison v Habeeb & Ors* [2011] EWHC 3031 (QB).

<sup>217</sup> *Tamiz v Google Inc Google UK Ltd* [2012] EWHC 449 (QB).

<sup>218</sup> *Tamiz v Google Inc* [2013] EWCA Civ 68.

<sup>219</sup> Department for Culture, Media and Sport & Department for Business, Innovation and Skills, *Digital Britain: Final Report* (2009), available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228844/7650.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf) (last visited June 5, 2021).

欲採取之相關對策。該報告建議應立法要求 ISP 業者承擔「初步義務 (initial obligations)」，使其依著作權人所送查證資料，對被指控涉有侵害著作權行為之訂戶，提出警告通知，並對於再犯者建立「黑名單」，必要時在法院裁定下，將侵害者資料提供給著作權人<sup>220</sup>。

2010 年 4 月 9 日，英國政府即根據「數位英國報告」內之政策目標，國會通過《2010 年數位經濟法》(Digital Economy Act 2010, DEA 2010)，以進一步解決線上著作權侵權之問題。DEA 2010 包含 11 個議題與 48 項條文，其中第二項議題(第 3 條至第 18 條)可分成兩個部分，第 3 條至第 16 條主要是討論 ISP 對網路侵害著作權之責任，第 17 條及第 18 條則是由法院命令 ISP 業者封鎖具侵權行為之網站。此法欲課予平臺業者建立監控機制即所謂的「逐級回應」(graduated response scheme) 或俗稱的「三振機制」(three-strikes policies)，以打擊網路上侵害著作權之不法行為。

然 DEA 2010 立法後，引發相當爭議，英國 ISP 業者包含 BT 遂針對 DEA 2010 提起司法審查訴訟，其中一項主張即認為 DEA 2010 所要求之常態性作為義務違反歐盟《電子商務指令》第 15 條之規範，已逾越常規監控之禁止<sup>221</sup>。惟英國高等法院駁回業者之主張，認為儘管此法案將賦予平臺業者一定作為義務，業者在打擊網路上著作權侵害的角色仍為被動的，此義務並非監控，負擔監控此類不法行為之角

---

<sup>220</sup> 章忠信，英國「數位經濟法案」(The Digital Economy Act) 有關網路服務業者責任條款評析，檢察新論，第 10 期，頁 55 (2011)。

<sup>221</sup> *British Telecommunications Plc & Anor, R (on the application of) v. The Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin).

色仍為著作權人<sup>222</sup>。

而由於 Ofcom 所提出的管制規章，於諸如執行成本負擔等問題受到極大反彈，英國國內便一直處於多方協商狀態。隨後於 2014 年，各大 ISP 業者與著作權利人取得共識，將改以寄發教育性電子郵件通知涉侵權人、以及投入資源支持喚起公民意識等活動，取代 2010 年數位經濟法的逐級回應措施。最後，英國於 2015 年通過《2015 年去管制法》(Deregulation Act 2015)，其中第 56 條，即刪除 2010 年第 17 條與第 18 條關於逐級回應措施之條文。換言之，英國的逐級回應制度實未真正施行<sup>223</sup>。

## 5. 既有監理制度下的困境

責任安全港此一制度之發動條件，係於服務提供者得知有違法活動或資訊的存在時，立即採取有效手段使之無法被接取。然而，藉由前開判決之內容可得知，由於法律並未規範何者屬於「違法活動」，同樣也未定義「得知」，而導致責任安全港與通知取下義務等制度之實施帶來一定程度之不確定性，亦難以回應社群媒體時代下，大量違法或不利使用者身心健康之有害內容於網際網路環境快速傳播下，所引發之負面影響<sup>224</sup>。

然而，前述之規範已難以因應快速變遷的網際網路環境，亦未能

---

<sup>222</sup> *Id.* at 115-116.

<sup>223</sup> 王牧寰，封鎖境外網站之研究—以英國網路中介者之「限制智財侵權特別責任」為例—，2016 年資訊社會年會暨研討會（2016 年 11 月）。

<sup>224</sup> 王牧寰、徐偉群、陳志宇、鄭嘉逸、江耀國、陳人傑、簡陳中、楊東穎、胡家崎、楊儷綺、田育志，《因應數位通訊傳播服務發展之規管趨勢與法制革新研析》，頁 121，國家通訊傳播委員會委託之計畫成果報告（2020）。

處理網路危害內容對於社會大眾日趨嚴重的負面影響。因此，英國政府除於 2019 年 4 月提出「網路危害白皮書」(Online Harms White Paper)，提出部分政策建議外，並於 2020 年 2 月公告，將由 Ofcom 擔任網路內容之獨立監管機關，以積極處理涉及恐怖主義、兒童性剝削與虐待 (child sexual exploitation and abuse, CSEA) 的內容。

而基於前述之籌備工作，DCMS 於 2021 年 5 月 12 日提出《線上安全法》草案，旨在透過課予網際網路服務 (internet service) 提供者處理網路危害內容之義務，並授權 Ofcom 可針對違法內容進行調查<sup>225</sup>，並可針對違法之業者裁處 1,800 萬英鎊，或 10% 全球營業額之罰鍰<sup>226</sup>，或經法院聲請、核可後採取各種「商業中斷措施」(business disruption measures) 之權限<sup>227</sup>，以營造安全、友善之網際網路使用環境，本研究將於其後進行介紹。

## (二) 網路危害內容處理對策

### 1. 網路危害白皮書

根據英國數位文化媒體暨體育部 (Department for Digital, Culture, Media & Sport, DCMS) 與內政部 (Home Office) 於 2019 年 4 月 8 日發表之「網路危害白皮書」(Online Harms White Paper)<sup>228</sup>，當時之修

---

<sup>225</sup> Draft Online Safety Bill, § 75.

<sup>226</sup> Draft Online Safety Bill, §§ 85(3), 90.

<sup>227</sup> Draft Online Safety Bill, §§ 91, 92, 93, 94.

<sup>228</sup> Secretary of State for Digital, Culture, Media & Sport (DCMS) & Secretary of State for Home Department (HD), *Online Harms White Paper* (2019), available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/973939/Online\\_Harms\\_White\\_Paper\\_V2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf).

法方向之架構與建議如下：

- 建議成立專責主管機構
- 要求網路業者強化其申訴管道，包括符合監理機關所要求之申訴格式，若業者不處理申訴，消費者將能透過獨立的第三方申訴管道進行申訴。
- 業者應採取適度和積極主動的措施，使使用者瞭解他們收到的資訊的性質和可靠性，並盡量減少誤導性和有害虛假資訊的傳播，並增加可信和多元的新聞內容。
- 監理機關應制定相關的守則供業者參考，例如業者應對故意隱匿其身分以傳播虛假信息之用戶，所可以採取的步驟；如何使用戶看不到經事實查核後發現有所爭議的內容；避免同溫層效應，使用戶可以觸及多元的資訊觀點等。
- 業者必須確保其內容排序的演算法不會導致極端和不可靠的內容頻繁出現。

而在網路危害白皮書公告後，英國政府進行了廣泛的公眾意見諮詢，並分別於 2020 年 2 月與 12 月公告了公眾意見諮詢的政府初步與完整回應報告<sup>229</sup>，並於 2020 年 2 月宣布，將指定 Ofcom 為主管機構，以營造更為安全的網路環境，支持快速發展的數位產業部門。而在歷經為期一年之立法工作規劃、籌備後，最終於 2021 年 5 月提出《線

---

<sup>229</sup> Secretary of State for DCMS & Secretary of State for HD, Online Harms White Paper: Full Government Response to the consultation (2020), available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/944310/Online\\_Harms\\_White\\_Paper\\_Full\\_Government\\_Response\\_to\\_the\\_consultation\\_CP\\_354\\_CCS01\\_CCS1220695430-001\\_V2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS01_CCS1220695430-001_V2.pdf) (last visited June 5, 2021).

上安全法》(Online Safety Bill) 草案<sup>230</sup>，以完備英國網路內容治理之法制體系。

## 2. 《線上安全法》草案

草案著眼於 Facebook、YouTube 等社群媒體、視訊分享平臺等使用者對使用者服務，以及 Google、Bing 等搜尋服務類型之影響力日益增加，故基於不同之服務型態、使用者數量與功能，以及傳播影響力之差異，課予業者寬嚴不同的法定義務；其次，為避免服務提供者未能落實相關法遵工作，草案授權 Ofcom 可進行調查，以及針對違法業者採取「商業中斷措施」，以及科以罰鍰等措施之權限，以積極處理網路違法、有害內容，並藉此有效降低違法內容的呈現時間與傳播能力，達成充分預防網路違法內容快速傳播之立法目的。

而《線上安全法》草案 (Draft Online Safety Bill) 之立法目的主要有兩大部分，首先，配合本次草案之訂定，修訂或刪除英國國內法之相關規範。第一部分，係因指定 Ofcom 為線上危害內容之獨立監理機關，故有必要修正《2003 年通訊法》(Communications Act 2003)，配合其職權範圍、功能擴張，進行對應之修正，並賦予法源依據；第二部分，由於本次草案將視訊分享平臺納入管理，故配合刪除《2003 年通訊法》4B 專章有關視訊分享平臺 (Video sharing platforms, VSPs) 之規範<sup>231</sup>；第三部分，由於草案已針對違法內容與涉及兒少性剝削、暴利之網路危害內容訂定相關規範，故配合刪除《2017 年數位經濟

---

<sup>230</sup> Draft Online Safety Bill (2021), available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/985033/Draft\\_Online\\_Safety\\_Bill\\_Bookmarked.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf) (last visited June 5, 2021).

<sup>231</sup> Communications Act 2003, Part 4B.

法》(Digital Economy Act 2017) 有關網路色情之相關規範<sup>232</sup>。

其次，草案基於不同網際網路服務型態、使用者數量與功能之差異，所具有相異之傳播影響力，區別「搜尋服務」(search service) 與「使用者對使用者服務」(user-to-user service) 兩類服務並納入管理，同時課予其寬嚴不等的法定義務，並授與 Ofcom 相關權限，以有效落實草案營造安全、友善之網路環境此一立法目的。

以下則針對《線上安全法》草案(以下簡稱草案)之具體規範進行說明：

### (1) 納管基準與範疇

根據草案第 3 條第 2 項<sup>233</sup>，《線上安全法》納管之服務主要有兩大態樣，即「使用者對使用者服務」、「搜尋服務」兩大類型，且該服務須於英國境內具有龐大之使用者數量，或英國為該服務的重點市場，或唯一之市場，以下則進一步說明前述服務之具體定義：

#### A. 搜尋服務

有關搜尋服務之定義，依據草案第 137 條第 2 項<sup>234</sup>，搜尋服務係指提供搜尋多個網站或資料庫之服務或功能的網際網路服務，亦即本法所稱之「2A 類服務」<sup>235</sup>。舉例而言，如 Google、Bing 等搜尋引擎

---

<sup>232</sup> Digital Economy Act 2017, Part 3; § 103.

<sup>233</sup> Draft Online Safety Bill § 3(2).

<sup>234</sup> Draft Online Safety Bill § 137(2).

<sup>235</sup> Draft Online Safety Bill § 59, schedule 4. 根據本草案草案第 59 條，本法所納管之業者將進一步區分為類別 1、類別 2A、類別 2B 等三類，並規範有寬嚴不等之義務，其具體區別之標準則訂定於附表 4，內閣大臣將於綜合考量不同服務之使用者數量、服務功能、性質等因素後，訂定此一區別標準。

屬之。

此外，根據同條第 7 項<sup>236</sup>，針對前述服務類型，該法於附表 1<sup>237</sup>訂有豁免條款，將特定服務型態排除於草案之納管範圍之內。因此，簡訊、多媒體簡訊、一對一即時語音服務、企業內部服務、功能限定服務、公共服務等服務態樣不在本法之監管範疇之下。

## B. 使用者對使用者服務

有關使用者對使用者服務之定義則規範於第 2 條<sup>238</sup>，係指提供該服務使用者所生產之內容（user generated content, UGC），或提供該服務使用者上傳或分享 UGC，並供該服務其他使用者接觸之網際網路服務。舉例而言，如 Facebook、YouTube 等社群媒體或視訊分享平臺服務屬之。

除此之外，「使用者對使用者服務」又再依使用者數量規模及內容傳播風險，區分為管制密度較高的「1 類服務」與管制密度較低的「2B 類服務」<sup>239</sup>，兩者除皆須負擔與前述「搜尋服務」相同的義務外，「1 類服務」尚須額外負擔特別義務，本研究將於其後進行說明。

而為達成本草案之立法目的，草案亦針對納管業者課有登記、報備、提交透明度報告，以及繳納行政規費、執行風險評估等義務，以協助主管機關 Ofcom 掌握產業實態，並協助業者執行相關法遵作業。

---

<sup>236</sup> Draft Online Safety Bill § 3(7).

<sup>237</sup> Draft Online Safety Bill, schedule 1.

<sup>238</sup> Draft Online Safety Bill § 2.

<sup>239</sup> Draft Online Safety Bill § 59, schedule 4.

## (2) 數位平臺業者應負擔之一般性義務

### A. 登記義務

根據草案第 59 條第 1 項<sup>240</sup>，Ofcom 應針對受本法監管之服務建置登記制度，服務提供者於登記時須載明服務名稱，並說明所提供服務之商業型態與營運模式等內容。

針對受本草案規管服務之納管標準，則規範於附表 4<sup>241</sup>，Ofcom 將將基於服務之使用者數量與功能，基於該服務可能造成之風險進行通盤研究，並就「類別 1」、「類別 2A」、「類別 2B」等服務之納管標準分別提出政策建議，以作為內閣大臣訂定前述標準之參考依據。

### B. 繳交透明度報告

根據草案第 49 條第 1 項<sup>242</sup>，受本草案納管之服務提供者，負有每年提交、公布透明度報告之義務，服務提供者並應於指定期限內進行繳交。此一義務之目的，旨在協助使用者瞭解服務提供者為提供安全網路環境所採取之措施，並提供 Ofcom 監理工作推動所需之資料，以建立企業、政府與公民社會間的監督、互信關係。

此外，依據草案第 50 條第 1 項<sup>243</sup>，Ofcom 應就透明度報告撰寫發布相關指引，以協助業者撰寫透明度報告，完備相關法令遵循之工作。

---

<sup>240</sup> Draft Online Safety Bill § 59(1).

<sup>241</sup> Draft Online Safety Bill, schedule 4, § 4.

<sup>242</sup> Draft Online Safety Bill § 49(1).

<sup>243</sup> Draft Online Safety Bill § 50(1).

### C. 繳納行政規費

根據草案第 51 條<sup>244</sup>，當服務提供者之全球營收，或已達指定標準時，除應主動通知 Ofcom 外，並須遵循草案第 52 條之規範<sup>245</sup>，繳交當年度之行政規費。

而有關前述全球營收標準門檻之訂定程序，內閣大臣將提供 Ofcom 研提標準之指引<sup>246</sup>，由 Ofcom 就有關資料進行研究、擬定後，經內閣大臣核准後公布<sup>247</sup>，並定期檢視相關標準之訂定是否合宜，以決定是否進行修正<sup>248</sup>。

### D. 風險評估

根據草案之規範，納管之服務提供者負有針對違法內容，以及兒少可能接觸之服務內容進行風險評估之義務，並確保相關風險評估措施將持續更新，並應於服務之營運與設計將發生重大改變時，執行進一步違法內容風險評估<sup>249</sup>。

具體而言，風險評估應基於該服務所掌握之使用者數量、規模，以及服務所具備之功能，妥適考量其使用者接觸恐怖主義、兒少性剝削與暴力等內容之風險、有關內容快速、廣泛傳播的難易程度，以及該服務對於個人、兒少族群產生傷害之性質與嚴重程度，以釐清使用

---

<sup>244</sup> Draft Online Safety Bill § 51.

<sup>245</sup> Draft Online Safety Bill § 52.

<sup>246</sup> Draft Online Safety Bill § 54(1).

<sup>247</sup> Draft Online Safety Bill § 53(1)(3).

<sup>248</sup> Draft Online Safety Bill § 53(5).

<sup>249</sup> Draft Online Safety Bill §§ 7(1)(2)(3), 19(1)(2).

者可能接觸網路危害內容之風險等級。

另外，針對使用者對使用者服務，草案基於傳播風險之高低進一步區別為類別 1 與類別 2B 之業者，而類別 1 之業者須額外負擔執行成人風險評估之義務。而為便利業者執行內容風險評估作業，依據草案第 62 條第 1 項，Ofcom 應針對風險評估制訂實務指引，以協助服務提供者完備相關法令遵循工作。

### (3) 網路危害內容處理機制

本草案旨在營造英國友善、安全之網際網路環境，是以草案之核心在於建構社群網站、視訊平臺與搜尋引擎等服務對於違法、危害內容之處理機制，並賦予 Ofcom 相關權限，以有效落實本法之相關規範。

以下將先行說明「網路危害內容」之定義，並簡要介紹此類行內容之檢舉與處理機制：

#### A. 網路危害內容之定義

##### (A) 違法內容

有關違法內容之定義，根據草案第 41 條第 2 項至第 5 項<sup>250</sup>，有關違法內容之定義，係指由受監管服務所提供之特定文字、影像與音訊內容，已涉及犯罪、犯罪相關行為，或散播內容之行為已構成相關犯罪<sup>251</sup>。

---

<sup>250</sup> Draft Online Safety Bill § 41(2)(3).

<sup>251</sup> Draft Online Safety Bill § 41(4). 另依據該條第 4 項，違法內容之具體態樣如下：A. 為涉及恐

而此處之犯罪，蓋指三種類型之犯罪，即涉及恐怖主義者、涉及兒少性剝削與暴力者，以及「優先違法內容」(priority illegal content)。所謂優先違法內容，係指其他經主管內閣首長經第 44 條評估特定違法內容之盛行率 (prevalence)、造成個人或社會傷害之風險程度、傷害之嚴重程度等後指定者<sup>252</sup>。

然而，前述所指之相關犯罪行為，並未包含涉及侵害智慧財產權之犯罪、不安全與不合格之商品，以及由非適格之服務提供者所提供之服務，前述之犯罪行為將回歸各行為之作用法進行管理<sup>253</sup>。

## (B) 危害內容

### I、有害兒少內容

有關有害兒少身心健康、發展內容之定義，除須為本法納管服務所提供之內容外，並須為本法或相關法制所指定之有害兒少內容<sup>254</sup>；除此之外，若服務提供者認為該內容之「本質」(nature)或傳播方式」(dissemination)將為兒少族群之生理或心理帶來直接/間接之嚴重影響時<sup>255</sup>，具體如導致身體層面的損傷、心理層面的焦慮、恐懼，或長期感到沮喪、壓力等症狀<sup>256</sup>；或已構成針對特定使用者之霸凌、恐嚇行為時<sup>257</sup>，均為本法之納管對象。

---

怖主義或相關犯罪行為之違法內容。B. 為涉及兒少性剝削與暴力等犯罪行為之違法內容。C. 為涉及內閣大臣所指定之犯罪行為態樣之違法內容。D. 非涉及前述犯罪行為之違法內容，且受害者或預期之受害者為單一或複數之個人。

<sup>252</sup> Draft Online Safety Bill § 44(1).

<sup>253</sup> Draft Online Safety Bill § 41(6).

<sup>254</sup> Draft Online Safety Bill § 45(2), § 45(2)(ii).

<sup>255</sup> Draft Online Safety Bill § 45(3),(5)

<sup>256</sup> DCMS, Online Safety Bill: Explanatory Notes (May 12, 2021), at para. 236, available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/985031/Explanatory\\_Notes\\_Accessible.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985031/Explanatory_Notes_Accessible.pdf) (last visited July 30, 2021).

<sup>257</sup> *Id.* at para. 275.

## II、有害成人內容

有關有害兒少身心健康、發展內容之定義，依據草案第 46 條之規範，除須為本法納管服務所提供之內容外，並須為本法所規範之有害成人之內容<sup>258</sup>；除此之外，若服務提供者認為該內容之「本質」（nature）或傳播方式」（dissemination）將為兒少族群之生理或心理帶來直接/間接之嚴重影響時<sup>259</sup>，將為本法所規範之對象。

### B. 網路危害內容之管理

有關網路危害內容之處理機制上，本草案除課予納管業者網路危害內容管理義務外，Ofcom 並可於業者未履行相關義務時發布技術警告通知，並於業者仍未改善時處以罰鍰，並視情形發布限制服務令或限制接取令，以避免網路危害內容持續進行擴散。以下則分就前述機制之內容進行說明：

#### （A）違法內容之安全管理

根據草案之規劃，「使用者對使用者服務」與「搜尋服務」均被課予處理違法內容之義務，服務提供者須將其服務上呈現優先排序之違法內容，進行最少化呈現（minimise the presence），以降低其呈現時間與傳播能力，減輕、有效管理相關內容對個人造成傷害之風險<sup>260</sup>。

此外，草案依據服務之類型，另課有不同之義務，如使用者對使用者服務須於其服務移除已確認、將確認以及可能為違法之內容<sup>261</sup>；

---

<sup>258</sup> Draft Online Safety Bill § 47.

<sup>259</sup> Draft Online Safety Bill § 46(3), (5).

<sup>260</sup> Draft Online Safety Bill § 9(3), § 21.

<sup>261</sup> Draft Online Safety Bill § 9(3).

搜尋服務則須公開說明該服務為保護個人免受網路違法內容，所實施之政策、程序規範，並確保法規範與實務執行之一致性<sup>262</sup>。

## (B) 有害兒少內容之安全管理

### I、兒少族群服務使用評估

根據草案第 26 條第 1 項之規範<sup>263</sup>，受本法所納管之服務提供者應進行評估，以釐清該服務或該服務之一部分是否可能由兒少族群所接觸、使用；其次，若兒少族群得以使用該服務，則應進一步釐清是否有大量兒少使用者使用該服務，以及該服務是否可能吸引大量兒少使用者<sup>264</sup>，以作為落實草案第 10 條、第 26 條有關有害兒少內容安全管理相關規範之依據。

此外，為協助納管之服務提供者執行評估工作，Ofcom 將發布相關指引<sup>265</sup>，服務提供者除獲得例外許可，應於 3 個月內完成相關評估工作，以有效保障兒少族群之權益<sup>266</sup>。

### II、有害兒少內容安全管理

根據草案第 10 條第 2 項<sup>267</sup>，使用者對使用者服務提供者須針對經草案第 7 條風險評估認定之有害兒少內容<sup>268</sup>，依據不同年齡層分別進行風險管理，避免使兒少族群易於接觸有關內容，以減輕危害內容對於不同年齡之兒少族群所帶來的負面影響。

---

<sup>262</sup> Draft Online Safety Bill § 21(4)(5).

<sup>263</sup> Draft Online Safety Bill § 26(1).

<sup>264</sup> Draft Online Safety Bill § 26(4).

<sup>265</sup> Draft Online Safety Bill § 28.

<sup>266</sup> Draft Online Safety Bill § 27(1).

<sup>267</sup> Draft Online Safety Bill § 10(2)(3).

<sup>268</sup> Draft Online Safety Bill § 7.

在搜尋服務的部分，依據草案第 22 條<sup>269</sup>，服務提供者須應採取相應之系統、措施，於所有年齡層之兒少族群於使用搜尋服務時，盡可能降低兒少族群因搜尋結果所帶來之風險<sup>270</sup>，並應公開說明為處理有害兒少內容，該服務所採取之營運政策與措施<sup>271</sup>，以有效降低、管理對兒少族群所帶來之負面影響、傷害之風險<sup>272</sup>。

然而，若服務提供者未能確實遵守、執行前開規範與義務時，草案亦訂定有技術警告通知、限制服務令與限制接取令等規範，以下將進一步介紹。

### (C) 保障具民主政治重要性之內容

根據草案第 13 條第 2 項<sup>273</sup>，「1 類服務」之服務提供者應採相關措施，以落實民主政治體制運作下的言論自由保障。而有關此一內容類型之定義，根據同條第 6 項<sup>274</sup>，係指由新聞媒體於本草案納管之服務所發布之內容，且內容發布之主要目的係為促進英國民主政治環境下的議題研討、辯論。

因此，服務提供者應就相關內容是否下架、是否限制使用者接觸，以及是否針對使用者生產、上傳與分享等行為採取限制措施等環節訂定辦法，並採取相關措施，以確保政治言論之多元性，且相關措施之用語、設計須清晰易懂並具一致性<sup>275</sup>。

---

<sup>269</sup> Draft Online Safety Bill § 22.

<sup>270</sup> Draft Online Safety Bill § 22(3).

<sup>271</sup> Draft Online Safety Bill § 22(4).

<sup>272</sup> Draft Online Safety Bill § 22(2).

<sup>273</sup> Draft Online Safety Bill § 13(2).

<sup>274</sup> Draft Online Safety Bill § 13(6).

<sup>275</sup> Draft Online Safety Bill § 13(4)(5).

#### (D) 保障新聞自由<sup>276</sup>

為保障民主社會下的新聞自由，避免無正當事由而下架、限制媒體所生產、上傳與分享之內容，而不利於民主政治之發展，故草案於草案第 14 條訂定有規範，課予「1 類服務」之服務提供者義務，業者應訂定相關措施，於決定是否將內容下架，或是否對使用者接取內容之權限做出限制時，充分考量有關措施是否有違言論自由保障<sup>277</sup>。

而言論自由保障之基礎，即在於有關內容之管理模式，故為協助服務提供者便利管理其服務上之新聞內容，草案之規範亦要求服務提供者應於其服務使用條款說明，該服務如何辨識、認定新聞內容，其進行內容下架、限制等決策時將如何顧及新聞自由之保障，以及該服務在處理新聞內容檢舉時所採取之政策與措施<sup>278</sup>。

最後，由於實務上仍有實施新聞內容下架、限制接取等措施之可能性，故為保障新聞自由，草案另課予服務提供者義務，應提供新聞、新聞內容創作者完善之申訴管道<sup>279</sup>。而若有關檢舉、申訴成立時，應儘速於其服務上復原以下架之新聞內容，或撤銷原對於使用者所採取之限制<sup>280</sup>。

---

<sup>276</sup> 根據草案第 40 條第 1 項，所謂「公認之新聞出版業者」之定義如下：A. 英國廣播公司(British Broadcasting Corporation, BBC)。B. 威爾斯語公共電視台(Sianel Pedwar Cymru, S4C)。C. 依據《1990 廣電法》(Broadcasting Act 1990) 或《1996 年廣電法》(Broadcasting Act 1996) 領有執照，並依該執照之授權發布新聞內容之業者。D. 新聞發布者之營運措施需符合以下要件：(A) 所發布之新聞內容係由不同人所創作，且新聞發布者對內容負有編輯、控制之權限。(B) 不論是否基於營利目的，其營運係以發布相關新聞內容為主。(C) 其營運受標準作業手冊所拘束。(D) 為處理使用者檢舉，設置有對應之政策與措施。(E) 在英國境內有經註冊之辦公室或其他聯絡地址。(F) 服務提供者對於其所發布之內容負有法定責任。(G) 服務提供者需公告其營運相關資訊，包含服務名稱、聯絡方式與註冊編號等。

<sup>277</sup> Draft Online Safety Bill § 14(2).

<sup>278</sup> Draft Online Safety Bill § 14(6).

<sup>279</sup> Draft Online Safety Bill § 14(3)(4).

<sup>280</sup> Draft Online Safety Bill § 14(5).

### (E) 有害成人內容安全管理

根據草案第 11 條第 2 項，「1 類服務」之服務提供者應於其服務使用條款中載明，其如何處理其服務上優先呈現的成人有害內容，以及其他方經風險評估界定為有害成人之內容。

除此之外，根據同條第 3 項<sup>281</sup>，服務提供者須於服務使用條款中載明內容如何對成人產生負面、危害影響，且服務使用條款內容之用語須清晰易懂且具一致性。

### C. 技術警告通知

依據草案第 63 條第 2 項<sup>282</sup>，若 Ofcom 基於合理之事由，認為受本法所監管之服務未能遵守草案第 9 條有關違法內容安全管理之規範<sup>283</sup>，證據並證明該服務確實涉及恐怖主義與兒少性剝削與暴力內容之傳播，且該內容持續存在於該服務之上時，Ofcom 可發布技術警告通知（technology warning notice），要求業者進行改善。

該通知之效力自送達日起，至多可延續 36 個月<sup>284</sup>，而若業者未能遵守前述通知所要求遵循之內容，Ofcom 最高將可課以 1,800 萬英鎊或相當其全球營業額 10% 之罰鍰<sup>285</sup>。

---

<sup>281</sup> Draft Online Safety Bill § 11(3).

<sup>282</sup> Draft Online Safety Bill § 63(2).

<sup>283</sup> Draft Online Safety Bill § 9.

<sup>284</sup> Draft Online Safety Bill § 66(2).

<sup>285</sup> Draft Online Safety Bill §§ 85(3), 90.

#### D. 限制服務令

受監管之服務，若未能遵守本草案之規範與課予之義務<sup>286</sup>，或未能遵守 Ofcom 所發布之技術警告通知，且該狀況為延續性時，Ofcom 可向法院申請限制服務令（service restriction order），法院將將審酌相關事由，決定是否發出限制服務令，要求提供輔助服務之提供者（如網路金流、廣告服務），中斷提供予違法服務營運所需之服務。

此外，若受監管服務未能遵守本草案之規範與技術警告通知之要求，以致於可能為英國民眾帶來立即性之重大風險時，Ofcom 可向法院申請臨時限制服務令，以避免限制服務令之申請未能及時處理有關事件惡化所帶來之負面影響<sup>287</sup>。

#### E. 限制接取令

當前述之限制服務令與臨時限制服務令均已失效，或未能有效防止重大傷害時。Ofcom 可依據草案第 93 條<sup>288</sup>，向法院申請限制接取令（access restriction orders），法院並將審酌申請事由後，決定是否針對提供違法業者接取設施（access facility）服務之業者（如網路接取服務事業）進行限制，以防止英國使用者使用該服務。

---

<sup>286</sup> Draft Online Safety Bill § 82. 具體而言，當發生有以下情形 2 項時，即構成申請申請限制服務令之事由： a.受監管之服務未能遵守 Ofcom 所施加之確認處分，且該狀況為延續性的。b.服務提供者尚未繳納罰鍰。c.服務提供者可能不遵守前述之確認處分。d.因服務提供者不履行法定義務時，可能為個人帶來損害風險，以致於不適合發出臨時執法通知與確認處分，或等待確認處份之發布。

<sup>287</sup> Draft Online Safety Bill § 82(3).

<sup>288</sup> Draft Online Safety Bill § 93.

#### (4) 救濟機制

##### A. 服務登記

依據草案第 59 條，受本法所監管之服務提供者均應向 Ofcom 辦理登記，而若服務提供者對於其被納入本法之監理範疇，或對於 Ofcom 認定應持續納管之行政決定不服，可依據草案第 104 條 向上級法院提起救濟<sup>289</sup>。

##### B. 有關技術警告通知之救濟

依據草案之規範，Ofcom 可於業者違反草案相關規範時發布技術警告通知<sup>290</sup>，要求業者進行限期改正，違者得連續進行處分並科以罰鍰。此一機制之設計係為確保納管業者遵守相關規範，惟若業者對相關處分之決定不服時，可依據草案第 105 條<sup>291</sup>，向上級法院提起救濟。

##### C. 越級申訴

根據草案之規範，若使用者對於納管之服務有以下情形時，可依據草案第 106 條<sup>292</sup>，向 Ofcom 提起申訴，而具體之態樣如下：

- 為服務使用者、會員，或社會特定群體帶來嚴重危害。
- 嚴重影響使用者、會員，或特定社會群體之言論自由權

---

<sup>289</sup> Draft Online Safety Bill § 104(1)(2).

<sup>290</sup> Draft Online Safety Bill §§ 63, 64, 65, 67.

<sup>291</sup> Draft Online Safety Bill § 105.

<sup>292</sup> Draft Online Safety Bill § 106(1).

利造成嚴重侵害、影響。

- 導致使用者、會員，或特定社會群體之隱私受到侵害。
- 對於使用者、會員，或特定社會群體帶來嚴重不利之影響。

而為有效處理相關申訴作業，以維護使用者與受影響者之權利，依據草案第 108 條<sup>293</sup>，Ofcom 將針對越級申訴訂定相關之實務指引，以利相關申訴作業之進行。

### （三）數位平臺資料蒐集、利用與保護規範

#### 1. 一般性合法原則

根據英國《2018 年資料保護法》（Data Protection Act 2018），個人資料蒐用行為應遵守一般性合法原則之要求，並具體規範於第 34 條至第 40 條，以下則簡要進行介紹：

#### （1）合法性、公平原則

依照《2018 年資料保護法》第 34 條第 1 項<sup>294</sup>，任何基於法律目的所從事之個人資料蒐用行為，均應合法且合乎公平性。蒐用合法性之要求，依同條第 2 項之規定，資料蒐用應取得資料主體之同意，或該蒐用行為權責單位執行工作之必需。

---

<sup>293</sup> Draft Online Safety Bill § 108.

<sup>294</sup> Data Protection Act 2018, Sec. 34.

## (2) 目的明確、合法

依照《2018年資料保護法》第35條第1項<sup>295</sup>，個人資料應在特定的，明確與合法之目的下被蒐集，且不得以與前述目的不相符之方式進行利用。然而，依照同條第3項，仍有例外適用之規範，亦即當有其他法律授權之前提下，蒐用資料可作其他目的之使用，惟該資料之利用確實合乎必要性與比例原則之規範。

## (3) 最少化蒐用

依照《2018年資料保護法》第37條<sup>296</sup>，在達成任何法律所授權之個人資料蒐用之目的時，應為適切、相關且有限度之使用，且不得逾越該蒐用行為之使用目的。

## (4) 正確性

依照《2018年資料保護法》第38條<sup>297</sup>，個人資料的蒐用應確保正確性，並於必要時隨時更新，請需採取合理程序，以確保不正確之個人資料已即時進行修正或刪除。

## (5) 最短化儲存時間要求

依照《2018年資料保護法》第39條第1項<sup>298</sup>，個人資料的保存時間不應超過基於蒐用目的所需之時間。此外，依據同條第2項，企

---

<sup>295</sup> Data Protection Act 2018, Sec. 35.

<sup>296</sup> Data Protection Act 2018, Sec. 37.

<sup>297</sup> Data Protection Act 2018, Sec. 37.

<sup>298</sup> Data Protection Act 2018, Sec. 39.

業應建立合適之時間限制，以提供定期審視、注意資料儲存是否合乎儲存限制。

## (6) 資料安全性

依照《2018年資料保護法》第40條<sup>299</sup>，基於任何法律授權目的的個資蒐用行為，均應確保於適當且安全之方式下進行處理，透過適當的技術或組織措施進行防範，以避免個資受到未經授權或非法之措施所導致之意外損失、損害。

## 2. 資料管控者與資料處理者之義務

### (1) 個資安全性義務

#### A. 安全性要求

➤ 依照《2018年資料保護法》第66條<sup>300</sup>，所有資料管控與蒐用者均應實施適當之科技化與組織性措施，以確保風險控管於適當之安全等級。另外，在自動化資料處理的部分，所有資料管控者與蒐用者亦應評估風險，並實施以下指定措施：

- 應避免對於連線之系統有未經授權之資料處理或干預。
- 應建立明確之資料處理細節規範。
- 應確保任何連線、處理資料之系統得以正常運作，且於

---

<sup>299</sup> Data Protection Act 2018, Sec. 40.

<sup>300</sup> Data Protection Act 2018, Sec. 66.

連線中斷時可以進行修復。

➤ 應確保個人資料不致因連線系統損壞、故障而有損害之情形。

#### B. 個資破壞之通報、通知義務

依照《2018年資料保護法》第67條第1項與第2項<sup>301</sup>，當資料控管者知悉有個資破壞事件時，應儘速或於72小時內通知主管機關，除非該事件對於個人自由與權利僅有低度侵害可能性之事件；而依據同條第3項與第4項，若資料管控者未於72小時內完成通報，應敘明延遲通報之事由。此外，依同法第68條<sup>302</sup>，於對於個人自由與權利有高度侵害風險之事件時，亦應通知資料主體，且不可無故延遲通報。此兩者之應通報之內容如下：

➤ 說明個資破壞事件之內容，涵蓋洩露個資之種類、資料主體與記錄之約略數量。

➤ 資料保護長（Data protection officer）之或其他聯繫窗口之姓名、聯絡資訊。

➤ 說明個資破壞事故可能導致之結果。

➤ 說明針對個資破壞事件所採取之處理措施，以降低可能

---

<sup>301</sup> Data Protection Act 2018, Sec. 67.

<sup>302</sup> Data Protection Act 2018, Sec. 68.

之不利影響。

## (2) 法遵義務

### A. 設置資料保護長

依照《2018年資料保護法》第69條<sup>303</sup>，資料管控者需任命一名資料保護長，除非該單位為法院或其他需行使司法權之機構，且該名資料保護長需擁有資料保護法與實務之專業能力。

依據《2018年資料保護法》第70條<sup>304</sup>，資料管控者應提供資料保護長就其執行所需之必要資源、得進用個資與蒐用操作，並維持其專業知識。

### B. 妥善保存蒐用記錄之義務

依照《2018年資料保護法》第61條<sup>305</sup>，資料管控者應對其負責之資料蒐用記錄負擔保存義務。依該條第2項之規定，保存記錄應包括以下事項：

---

<sup>303</sup> Data Protection Act 2018, Sec. 69.

<sup>304</sup> Data Protection Act 2018, Sec. 70

<sup>305</sup> Data Protection Act 2018, Sec. 61.

- 資料管控者之姓名與聯絡方式。
- 共同資料管控者之姓名與聯絡方式。
- 資料保護長之姓名與聯絡方式。
- 資料蒐用目的。
- 個資已被揭露或將要揭露之接收者的類型。
- 資料主體與個人資料類別之描述。
- 詳細說明使用分析之情形。
- 說明將個資移轉至第三國或國際組織之類別。
- 應指明資料處理之法源基礎為何。
- 如果可能，應設想刪除不同類別資料之時限。
- 如果可能，應針對本法第 66 條所言之技術、組織性安全措施進行簡要敘述。

有關資料蒐用者之保存義務，則係規範於第 4 項，以下具體說明之：

- 參與資料蒐用行為之個資料蒐用者之姓名與聯絡方式。
- 資料管控者之姓名與聯絡方式。
- 資料保護長之姓名與聯絡方式。
- 蒐用行為類別。
- 說明明顯由資料管控者指示，將資料移轉至第三國或國際組織之行為，包含第三國或國際組織之身分。
- 如果可能，應針對本法第 66 條所言之技術、組織性安全措施進行簡要敘述。

### C. 資料保護影響評估與事前諮詢義務

依照《2018 年資料保護法》第 64 條<sup>306</sup>，針對可能導致侵害個人權利與自由的高風險蒐用行為，資料管控者應優先進行處理、執行資料保護影響評估（Data protection impact assessment, DPIA）。具體評估事項則應涵蓋以下項目：

- 對於預期資料蒐用處理過程的一般性描述。
- 對於資料主體之權利與自由所造成之之風險影響評估。
- 為應對前項風險所設置之措施。
- 應確保個人資料安全與法律遵循之保護、安全措施。

另外，依照《2018 年資料保護法》第 65 條<sup>307</sup>，資料管控者應向

---

<sup>306</sup> Data Protection Act 2018, Sec. 64.

<sup>307</sup> Data Protection Act 2018, Sec. 65.

監理機關進行事前諮商 (Prior consultation)，並提供依第 64 條所進行之資料保護影響評估，以及主管機關所要求之相關資料，主管機關並應於六週內提出對應之建議，期間最多可延長至 1 個月，並通知資料管控與資料蒐用者，並敘明延長之事由。

### (3) 提升法遵之制度

依據《2018 年資料保護法》第 63 條<sup>308</sup>，資料管控者與資料蒐用者應與主管機關進行合作。

### 3. 數位平臺廣告、行銷之資料保護、隱私規範

GDPR 最為重要的部分係業者需要完善資料與隱私保護規範，以符合課責原則 (accountability)，故依據《2018 年資料保護法》第 122 條<sup>309</sup>，ICO 應對直銷 (direct marketing) 訂定實務準則，亦即就宣傳理想、目標之廣告商品與服務訂定相關規範，以協助業者進行相關法遵作業。為此，ICO 已提出《直銷實務準則》(Direct marketing code of practice) 草案<sup>310</sup>，並於 2020 年 4 月完成公眾諮詢程序，惟具體之正式公告與生效期程尚不明朗，仍有待進一步觀測。

#### (1) 規範主體

《直銷實務準則》之適用對象，係針對透過個人資料對特定個人，或於更為廣泛之範圍進行行銷、廣告或任何基於產品、服務、目標與

---

<sup>308</sup> Data Protection Act 2018, Sec. 63.

<sup>309</sup> Data Protection Act 2018, Sec. 122.

<sup>310</sup> ICO, Direct marketing code of practice Draft code for consultation, available at <https://ico.org.uk/media/for-organisations/documents/2021/2619043/direct-marketing-code-draft-guidance-122020.pdf> (last visited June 5, 2021).

理念進行行銷、推廣之行為。以下則羅列納管行為之態樣<sup>311</sup>：

- 針對商品/服務所進行之商業行銷行為。
- 慈善機構或第三部門所進行之募款或宣傳行為。
- 政黨所進行之募款或宣傳行為。
- 政府與公共單位所進行之政令、服務宣導。
- 以個人資料進行諸如購買、銷售、剖析或充實等直銷之行為。

而本研究主要研究之類型，則係透過電話、傳真、電子郵件、簡訊，以及透過電子通訊網路所傳遞之訊息所進行之行銷行為。

## (2) 規範模式

《直銷實務準則》之規範目的，係為協助業者落實歐盟《一般資料保護規則》、英國《2018年資料保護法》與《隱私暨電子通訊規則》（Privacy and Electronic Communication Regulations, PECR）等規範之要求，以避免行銷、推廣過程衍生侵害個人資料之爭議。具體而言，ICO將要求業者進行資料保護影響評估，並於違反有關規範時透過發布警告、譴責（reprimands）、強制執行與行政罰鍰等政策工具進行因應，並可於發生嚴重個資侵害事件時，處以2000萬英鎊或4%全球營業額<sup>312</sup>。

---

<sup>311</sup> *Id* at 7.

<sup>312</sup> *Id* at 11.

以下則分就行銷服務所涉及之法遵作業規範進行說明：

#### A. 合法性基礎

一般而言，透過使用個人資料從事直銷行為的合法性基礎主要有二。其一，須取得當事人同意；其二，則是行為本身具有合法利益，其資料使用目的與必要性間須取得平衡，亦即須經過合法利益評估（legitimate interests assessment, LIA）。

而根據《隱私暨電子通訊規則》之規範，以下將進一步說明各類型行銷方法是否須依法取得個資主體之同意：

表 2：行銷方法是否須取得個資同意一覽表

行銷方法	是否須取得同意
撥打電話予拒接電話服務所登記之電話號碼	是
撥打電話予曾拒接者	是
撥打拒接電話服務未登記或未曾拒接之電話號碼	否
自動撥打電話	是
電子郵件/文字/APP 服務/數位平臺訊息服務 （於資料蒐集目的內使用）	否
電子郵件/文字/APP 服務/數位平臺訊息服務 （於資料蒐集目的外使用）	是
向企業遞送電子郵件、文字訊息	否

傳統郵件	否
------	---

資料來源：ICO<sup>313</sup>，本計畫製作

### B. 資料保護影響評估

根據歐盟《一般資料保護規則》第 35 條<sup>314</sup>，當涉及具有顯著效果之系統性分析，或處理大規模之特殊類別與刑事犯罪資料，以及大規模系統性監控公共區域時，須執行資料保護影響評估；此外，英國《2018 年資料保護法》第 64 條亦設有相似之規範<sup>315</sup>，要求資料管控者於可能導致個人權利與自由處於高風險狀態時，應執行資料保護影響評估。

而為預防直銷行為所導致之相關風險，ICO 羅列有以下行為態樣，應列為評估之重要事項<sup>316</sup>：

- 大規模分析。
- 透過資料配對執行之直銷行為。
- 隱形措施（invisible process），如資料仲介、第三方線上追蹤、線上廣告、重複使用公開資料等服務。
- 追蹤個人地理位置與行為，如線上廣告、網站與跨裝置

<sup>313</sup> *Id* at 30-31.

<sup>314</sup> GDPR, Art 35.

<sup>315</sup> Data Protection Act 2018, sec 64.

<sup>316</sup> ICO, *supra* note 310 at 28.

追蹤、電話追蹤、財產分析、忠誠度計畫等服務。

➤ 針對兒童與弱勢者進行之行銷與分析行為。

此一制度的主要目的，係為確保從事行銷、宣傳之組織建置有完善之個人資料保護系統、措施，確保，並協助企業、政府部門與非營利組織釐清其個資保護風險，並透過 ICO 審查機制之運作，以確保資料安全體系之完整性。

### C.數位平臺線上行銷、廣告規範

數位平臺服務之行銷、廣告服務有別於傳統行銷服務之型態，可透過追蹤使用者數位足跡，進行精準之廣告投放，具體包含社群網站、視訊分享服務、隨選視訊服務、線上遊戲等服務之類型。而面對前述之新興服務監管之挑戰，ICO 於《直銷實務準則》草案中指出，一旦行銷行為涉及個人資料之蒐集與利用時，即須遵守《2018 年資料保護法》與《隱私暨電子通訊規則》之規範。

而在前述之規範下，數位平臺服務若藉由第一方或第三方記錄（Cookie）蒐集使用者之數位行為、足跡；或透過追蹤軟體與應用程式，以及其他方式接取個人裝置以取得、儲存個人資料時，均應獲得資料主體之同意，相關服務並應完成個人資料保護影響評估，以有效降低個資外洩、遺失與損毀等風險。

#### （四）小結

英國作為前歐盟會員國成員之一，其在打擊數位通訊傳播的不法內容時，採取之措施與原則皆遵守歐盟規範，法院判決也多採納歐盟

法院見解，而在具體的監理措施上，英國目前已指定通訊管理局為獨立監管機關，並於 2021 年 5 月提出《線上安全法》之草案。草案基於網際網路服務之型態、使用者數量與功能等差異的基礎上，將現代社會最具傳播影響力之「搜尋服務」與「使用者對使用者服務」兩類服務納入監理範疇，並課予其寬嚴不等之法定義務。

《線上安全法》草案納管之服務提供者除所須負擔之共同義務，須向 Ofcom 進行登記、報備，按年度繳交透明度報告，並於營收達一定水平時繳交行政規費外，尚須針對其服務進行內容風險評估，並建置違法與有害內容之管理機制，以及使用者完整之申訴、處理管道。而其中，並課予使用者規模與傳播影響力較大之使用者對使用者服務（1 類服務）額外之法定義務，須進一步針對有害成人內容進行管理，並針對具民主重要性，以及新聞機構所發布之新聞內容訂定管理辦法，以實踐言論自由與新聞自由之保障。此外，為有效落實草案之相關規範，草案亦授權 Ofcom 可針對個案進行調查、發布技術警告通知要求業者限期改善，並可針對違法業者裁處 1,800 萬英鎊或相當其全球營業額 10% 之罰鍰等權限。

然而，若前述措施未能有效發揮功能時，Ofcom 將可採取以下措施：其一，可向法院聲請「限制服務限制令」，要求線上金流、廣告等輔助服務之業者中斷提供予違法服務營運所需之服務；其二，可向法院聲請「接取限制接取令」，限制使用者可用以可接取違法服務之接取設施進行限制，以防止英國使用者繼續使用該服務，藉此有效維繫安全之網路環境。綜整而言，英國對於網路內容係採取較高密度之管制模式，除課予業者處理違法、有害內容等諸多義務外，並授權主管機關可經法院核發令狀後，採取前述之阻斷措施，以阻止相關內容之

迅速擴散，並藉此營造合宜、友善之網際網路環境。

其次，有關數位平臺服務於執行業務所進行之個人資料蒐集行為，則須遵守歐盟《一般資料保護規則》與英國《2018 年資料保護法》，須遵守一般性合法原則之拘束，且資料管控者與資料處理者亦須擔負相關義務，如須保全個人資料之安全性，並於個資破壞時通知資料主體，且須任命資料保護長，並完善個人資料保護相關之法令遵循工作。

而有關數位平臺服務從事廣告投放、行銷等行為，ICO 目前已制訂《直銷實務準則》之草案，當資料分享與行銷、廣告行為涉及個人資料蒐用時，除應執行資料保護影響評估外，亦應取得個人資料主體之同意，並完善資料儲存、使用之系統、措施之安全性，惟此一草案尚未完成立法程序，仍有必要持續進行觀測。

### 三、英國法制政策之啟示

在數位平臺所涉及的競爭議題上，英國政府的對應措施係成立專責之數位市場部門，並針對具戰略市場地位之數位平臺業者訂定對應之監理機制，故在綜合考量數位平臺可能對於市場產生之反競爭效果，以及既有組織能量不足及法制規範難以因應之現況下，預計針對具有戰略市場地位之數位平臺業者採取事前管制措施，透過具體之評估方法，指定具有戰略市場地位之業者，並課予其對應之管制義務，或實施對應之矯正措施，以有效維繫、建置適宜競爭之市場環境。

在數位平臺服務業者問責的議題上，英國目前已指定通訊管理局為獨立之監管機關，並於 2021 年 5 月提出《線上安全法》之草案。

草案基於網際網路服務之型態、使用者數量與功能等差異的基礎上，將現代社會最具傳播影響力之「搜尋服務」與「使用者對使用者服務」兩類服務納入監理範疇，並課予其寬嚴不等之法定義務，除須向 Ofcom 進行登記、報備，按年度繳交透明度報告，並於營收達一定水平時繳交行政規費外，尚須針對其服務進行內容風險評估，並建置違法與有害內容之管理機制，以及使用者完整之申訴、處理管道。此外，為有效落實草案之相關規範，草案亦授權 Ofcom 可針對個案進行調查、發布技術警告通知要求業者限期改善，並可針對違法業者裁處 1,800 萬英鎊或相當其全球營業額 10% 之罰鍰等權限。

然而，若前述措施未能有效發揮功能時，Ofcom 將可採取以下措施：其一，可向法院聲請「限制服務限制令」，要求線上金流、廣告等輔助服務之業者中斷提供予違法服務營運所需之服務；其二，可向法院聲請「接取限制接取令」，限制使用者可用以可接取違法服務之接取設施進行限制，以防止英國使用者繼續使用該服務，藉此有效維繫安全之網際網路環境。

而有關個人資料保護規範，除應遵守英國國內法《2018 年資料保護法》外，基於脫歐法案之規範，英國於脫歐後仍須遵守歐盟《一般資料保護規則》之規範，故數位平臺業者除須於蒐用個資時遵守個資蒐用原則外，當其作為資料管控者與資料處理者時，亦須擔負相關義務，如保全個人資料之安全性，並於個資破壞時通知資料主體，且須任命資料保護長，並完善個人資料保護之法令遵循工作。

最後，有關數位平臺業者對於資料可攜權的具體實踐，以及廣告投放、行銷行為之規範上，ICO 依據《2018 年資料保護法》之規範，

分別訂定有《資料分享實務準則》與《直銷實務準則》，而根據前述準則之規範，當資料分享與行銷、廣告行為涉及個人資料蒐用時，除應執行資料保護影響評估外，亦應取得個人資料主體之同意，並完善資料儲存、使用之系統、措施之安全性。除此之外，為確保資料分享行為之安全性，資料管控者並應與資料共享之組織簽訂資料共享協議，以確保符合相關法制規範，並保障資料主體之權利。

## 肆、美國法制政策研析

### 一、數位平臺市場競爭

#### (一) 監管機關之態度與維持競爭之機制

##### 1. 監管單位對數位平臺之執法傾向與困境

作為全球四大網路產業巨頭 Google、Amazon、Facebook 與 Apple 的發源地，美國的國家整體經濟政策向來以降低政府干預、鼓勵市場機制作為推動產業的價值核心，這樣的政策導向往往也可見於監管機關放任式 (laissez-faire) 與輕度管制 (light-touch) 之規管態度。由於網路資通訊等新創產業往往涉及發展中的新興科技或破壞式創新的商業模式，無法納入現行的規管架構，是故就經濟發展而言，當美國政府願意透過輕量管制的政策型態提供此類產業較多的彈性與發展空間時，便能為經濟的創新動能注入活水，進而創造大量的財政稅收與工作機會，並吸引國外高科技人才移入，藉由經濟、科技的發展放大美國在國際社會上的影響力。

挾著產業對全球經濟輸出的優勢，加上較為寬鬆、輕量的市場規管態度，美國透過反托拉斯法調查數位平臺市場競爭的速度便顯得較世界各國政府為緩。然而，隨著數位平臺持續擴張自身業務領域，開始成為數位經濟時代下與個人生活密不可分的主宰者，科技巨頭身兼市場「競爭者」與「守門人」的雙重身分也帶來濫用市場力的誘因，形成了平臺鞏固其獨占地位的隱憂。面對這樣的趨勢，各界也開始注意到監理機關執法態度與傳統競爭法見解所形成的困境。

以 Amazon 為例，新布蘭迪斯學派（New Brandeis School）<sup>317</sup>學者 Lina M. Khan 在 2017 年時便為文指出，當前美國主流的競爭法理論受芝加哥學派（Chicago School）<sup>318</sup>影響甚深，往往是以價格和短期的「消費者福祉」作為最主要的關注對象，然而，這種論述非但誤解了立法者制訂反托拉斯法的初衷，其重「結果」而不關心「過程」、重「計算」而不關心「結構」的理論框架也勢將導致生產者與整體市場的健康程度遭到輕忽，同時更難以因應新興數位平臺對市場競爭帶來的巨大衝擊<sup>319</sup>。

Khan 以事業橫跨零售、物流、支付、信貸、拍賣、出版、影視內容製作、雲端服務等無數領域的 Amazon 為例，指出：這家企業巨頭之所以能成長至當前的地位，最主要的理由便是其採取了無懼虧損、只追求增長與市場支配的激進商業策略，一方面藉由掠奪性定價（predatory pricing）吸引大量用戶，一方面則積極進行跨行業的垂直結合<sup>320</sup>。

以 2005 年上線的 Amazon Prime 會員計畫為例，消費者只需繳交 79 美元的費用便能享受無限制的快速配送服務，以及電子書、線上影音串流等豐富功能。根據估計，每位 Prime 會員會為 Amazon 造成每年至少 11 美元的虧損，但相對地，會員們的消費行為也會因平臺而

---

<sup>317</sup> 新布蘭迪斯學派一名源自最高法院大法官 Louis Dembitz Brandeis，該學派主張：大型企業是否具有獨占地位，應從市場結構與競爭過程加以觀察，而非僅關注價格與結果，「市場看不見的手」是各方勢力的總和，因此必須透過立法與競爭政策予以調節市場，無法靜待市場自行達到均衡狀態。

<sup>318</sup> 芝加哥學派的發源地為美國芝加哥大學（University of Chicago），該學派使用實證經濟學（positive economics）之論證方式，立場偏向信賴市場機制，主張自由放任、減少政府干預，加上治學嚴謹，在學界具有相當大的影響力。

<sup>319</sup> See generally Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710(2017).

<sup>320</sup> *Id.* at 746-747.

改變：當會員們對 Amazon 服務的依賴度越高、在 Amazon 的消費越來越頻繁，他們對其他平臺的使用率自然也會隨之降低。另一方面，Amazon 以低於成本價銷售電子書的模式也使其在 2009 年達到了電子書市場 90% 以上的占有率。透過綁定專屬的電子閱讀器 Kindle，Amazon 不只提高了消費者轉換至其他電子書平臺的成本，更能利用閱讀器蒐集的個人資料為每位消費者量身訂製推薦內容與未來的購買方案，進一步提高用戶的黏著度。這些數位產品固有的特性都在在顯示了，電子商務平臺對數位產品採取虧本售價的模式，往往能比採用相同策略的實體產品獲得更高的回饋，然而傳統的競爭法理論卻秉持「企業重視利潤」的前提，將掠奪性定價視為業者的「不理性」策略，並從價格的角度切入認為消費者的福祉幾乎不會因此受到影響；法院也往往假定採用此一策略的企業會在日後透過同一商品的漲價彌補虧損，而忽略 Amazon 這樣橫跨多個市場的大型平臺可以透過不同產品定價的交互補貼彌平整體虧損，甚至可基於自身的平臺身分，直接向出版商收取商品陳列等服務費用<sup>321</sup>。

與此同時，Amazon 更透過與現有企業的垂直結合持續擴張事業版圖，最終將自身化為網際網路上的某種「基礎設施」。這意味著市場上的新參進者不只難以複製它的商業模式，這些競爭者往往也會是依賴 Amazon 的客戶：與 Amazon 競爭銷售額的零售商可能會使用它的線上商城與物流服務；與 Amazon 競爭內容製作的媒體企業也可能會使用它的雲端服務，或是在它的串流平臺上架節目，這樣的利益衝突自然給了 Amazon 為自家產品提供優勢地位、形成不公平競爭的誘

---

<sup>321</sup> *Id.* at 747-753, 756-768.

因。Khan 強調：現行競爭法上的分析方法假定「理性」的企業會採取將對手逐出市場的策略，但 Amazon 的商業模式其實更加高明：它將自己的線上商務變得無可取代，即便在競爭過程中也能一同享受競爭者業務帶來的好處，甚至還能利用自身服務提供者的身分蒐集、分析競爭者的資訊，進一步提升自身產品的相對優勢、擴張自身在市場上的支配地位<sup>322</sup>。

簡言之，Amazon 多年來的策略正是以一種符合競爭法的安全路線持續走向通往獨占的康莊大道，其「不理性」策略為的是要持續擴張自身的支配地位，甚至成為有能力控制競爭者的「網路關鍵設施」。有鑑於此，Khan 呼籲重新審視當代的法律框架，將焦點轉向企業結構與市場的動態競爭，並提出了兩種以資應對的模式：其一，改革傳統競爭法之見解，尤其應對數位平臺採用掠奪性定價的判定適用新的推定基準、重新審視垂直結合帶來的利益衝突與不公平競爭；其二，接受大型數位平臺具有自然獨占性質的事實，將其與電力、天然氣、鐵路、電話等公用事業相類比，引入公共載具（common carrier）的思維進行監理<sup>323</sup>。

除了以 Khan 為首的學術分析外，美國各界的倡議團體及政治人物亦開始呼籲政府加強對此類大型科技巨頭的監管，使政府近來逐漸重視此一議題，並針對巨型科技企業近年來採取的發展策略與市場作為、甚或是對國內數位市場競爭狀與消費者權益帶來的影響，展開積極的調查與司法上的因應行動。而隨著政權交替，這股趨勢從新任總

---

<sup>322</sup> *Id.* at 802-805

<sup>323</sup> *Id.* at 790-802

統拜登的人事任命意向也可窺一二。2021 年 3 月，台裔學者吳修銘（Tim Wu）受邀加入白宮國家經濟委員會（National Economic Council），出任總統的科技與競爭政策特別助理<sup>324</sup>；同年 6 月，總統拜登更於參議院通過 FTC 委員的人事任命案後，正式任命 Lina M. Khan 出任 FTC 主席<sup>325</sup>。兩位新布蘭迪斯學派的代表性人物先後獲得當前行政團隊的重用，無疑也代表著美國的競爭法論述將開始轉變，大型數位平臺的管理思維即將邁向新的時代。

## 2. 眾議院發布「數位市場競爭調查」報告

2020 年 7 月 29 日，美國眾議院司法委員會下轄之「反托拉斯、商業及行政法小組委員會」（Subcommittee on Antitrust, Commercial and Administrative Law，下簡稱「反托拉斯小組」）召開線上聽證會，傳喚時任 Google、Apple、Amazon 及 Facebook 之執行長，要求四位負責人分別就其企業可能涉及的獨占行為進行答詢。

這場聽證會觸及的議題包括：Google 是否濫用其在市場上具有主導地位的搜尋引擎業務監控新進的挑戰者？Apple 在其 App Store 市場上是否對特定的應用程式開發者有所偏頗？Amazon 是否濫用第三方賣家的數據，以圖利自有品牌之商品<sup>326</sup>？Facebook 收購 Instagram、WhatsApp 一案是否有減損市場競爭之疑慮？雖然會中就四大科技公

---

<sup>324</sup> Cecilia Kang, *A Leading Critic Of Big Tech Will Join The White House*, THE NEW YORK TIMES (2021/3/5), available at <https://www.nytimes.com/2021/03/05/technology/tim-wu-white-house.html> (last visited May. 26, 2020).

<sup>325</sup> Federal Trade Commission, *Lina M. Khan Sworn in as Chair of the FTC* (2021/6/15), available at <https://www.ftc.gov/news-events/press-releases/2021/06/lina-m-khan-sworn-chair-ftc> (last visited October. 26, 2021).

<sup>326</sup> See David Uberti, *Tech Antitrust Hearing Puts Big Data On Hot Seat*, THE WALL STREET JOURNAL (2020/07/29), available at <https://www.wsj.com/articles/tech-antitrust-hearing-puts-big-data-on-hot-seat-11596067130> (last visited May. 13, 2021).

司掌握、利用使用者數據之界線再度提出了質問，但民主、共和兩黨眾議員所著重的面向仍有所不同：民主黨人認為現行的競爭法制度似乎難以有效地管理科技巨頭，故呼籲對法制展開變革；共和黨人關注的焦點則是社群媒體在平臺上對保守言論的審查<sup>327</sup>。

同年 10 月 6 日，反托拉斯小組進一步提出了「數位市場下之競爭調查」(Investigation of Competition in Digital Markets) 報告<sup>328</sup>，對前述四大科技企業可能涉及之限制競爭行為展開了調查，並探討現行法制之設計與行政機關之執法程度是否足以因應優勢企業挾其市場力對數位市場帶來的隱憂，進而提出詳盡的改革建議。

該報告認為，Amazon、Apple、Facebook 與 Google 在當代的社會、經濟環境中已經躋身為通訊、資訊、商品與服務交流的基礎架構。截至 2020 年 9 月為止，四大平臺的市值總和已經超過 5 兆美元，占 S&P 100 指數的 3 分之 1 以上；隨著當代社會的工作、商業與通訊方式逐漸轉移至線上傳輸，這些企業提供的服務也將與人類的經濟、生活更加密不可分。但另一方面，在過去十年來，數位經濟市場卻逐漸出現了獨占化的傾向，無論社群網路、網路搜尋引擎、網路廣告等市場皆係呈現一至兩家企業寡占的局面。上述四家企業不只佔據了資源分配的關鍵渠道、獲得了中介者的地位，甚至進一步濫用其優勢平臺

---

<sup>327</sup> See Ryan Tracy, *After Big Tech Hearing, Congress Takes Aim But From Different Directions*, THE WALL STREET JOURNAL, 2020/07/30, available at <https://www.wsj.com/articles/after-big-tech-hearing-congress-takes-aim-but-from-different-directions-11596149053?mod=searchresults&page=4&pos=3> (last visited May. 13, 2021).

<sup>328</sup> See generally INVESTIGATION OF COMPETITION IN DIGITAL MARKETS: MAJORITY STAFF REPORT AND RECOMMENDATIONS, Subcommittee on Antitrust, Commercial and Administrative Law, House Committee on the Judiciary (2020) [hereinafter Majority Staff Report], available at [https://judiciary.house.gov/uploadedfiles/competition\\_in\\_digital\\_markets.pdf](https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf) (presenting antitrust and regulatory reform recommendations).

的守門人力量，支配了整個數位經濟市場的運作。而當其他參進者只能透過守門人的力量與消費者、市場進行接觸時，自須接受各種可能帶來重大經濟損害的妥協與要求，付出此等「交易成本」換取獲利的機會<sup>329</sup>。

該報告進一步指出，四大企業顯著且具有持續性的市場力量係肇因於諸多因素，其一即為優勢平臺的大規模併購策略。在過去十年來，Amazon、Apple、Facebook 與 Google 已併購了數以百計的企業，以此吸收新創或可能構成潛在威脅的競爭者，甚或透過「殺手併購」（killer acquisition）完全抹消市場上既存的特定產品，藉此維持自身的主導力量。但在多數情況下，反托拉斯法的監管機關卻從未要求四大企業提出進一步的資料與文件，以審查該結合案之通過是否有削減競爭或促進獨占的疑慮——以 Facebook 為例，在其歷來近 100 件的事業結合案中，聯邦貿易委員會（Federal Trade Commission, FTC）僅對 2012 年收購 Instagram 一案展開過大規模的審查<sup>330</sup>。

透過一連串的聽證與調查，反托拉斯小組也發現，在網路效應（network effect）的強烈影響下，當前的數位市場上往往呈現出優勢平臺只與自家產品競爭的獨占傾向，四大企業對市場的支配不只減損消費者的選擇、侵蝕創新與美國經濟的挑戰者精神，更削弱媒體的自由與多樣性、侵害了美國民眾的隱私<sup>331</sup>，故該份報告分別就「重新建構數位市場之競爭」、「強化反托拉斯法之規範」，以及「強化反托拉

---

<sup>329</sup> *Id.* at 10-11.

<sup>330</sup> *Id.*

<sup>331</sup> *Id.* at 12.

斯法之執行」三大方向提出了具體的建議。分述如下：

(1) 重新建構數位市場之競爭

➤ **透過結構性拆分、限制經營領域減少利益衝突<sup>332</sup>**：由於優勢平臺除了在數位市場上扮演中介者之外，亦整合了多樣化的業務，與其他必須仰賴優勢平臺生存的事業在其跨足的經營領域相互競爭，其身兼中介者與競爭者的雙重身分自然形成了利益衝突。優勢平臺可能在提供其他事業營運及上架管道的同時，不當蒐集及運用該第三方事業在平臺上經營所產生的數據，藉以偵測甚至消滅競爭對手；亦可能運用其市場上優勢地位作為談判籌碼，迫使其他經營領域之事業遵從其要求，或運用其多元經營之整合能力綁定商品、服務，進而鎖定使用者、隔絕與其他業者競爭之機會。除此之外，優勢平臺也可透過優於競爭對手而獲取之利潤補貼參進其他市場所需之成本，藉此擴大自身的經營領域。為解決利益衝突的問題，報告中建議可透過結構性拆分，禁止優勢平臺與依賴平臺基礎設施營生之第三方事業競爭，並防止其利用補貼參進其他市場；並可限制其業務經營領域，藉此控制其事業版圖之擴增。

➤ **實施禁止歧視、偏惠及自我偏惠之規定<sup>333</sup>**：由於優勢平臺就自身之商品、服務享有特權（例如 Google 在搜尋結果的呈現上給予自身產品優先排序），且往往會給予事業夥伴較優惠之

---

<sup>332</sup> *Id.* at 378-381.

<sup>333</sup> *Id.* at 382-383.

待遇，其自我偏好或差別待遇的行為具有在市場上擇定贏家的效果，導致其他透過優勢平臺連結至市場的第三方事業面臨不公平的競爭，甚至被迫將資源轉移至購買廣告或其他附加性服務的成本上，新創事業亦可能因此障礙而難或創投公司的青睞。為了解決這個問題，報告建議應設立反歧視之規定，要求優勢平臺對其他事業提供與平臺本身相當之服務條款、價格及連結條件，藉此確保線上市場的公平競爭與創新。

➤ **透過互通性(interoperability)與開放接取(open access)促進競爭**<sup>334</sup>：礙於網路效果、轉換成本等固有的特性，數位市場對於單一優勢事業的發展較為有利，而不利於新事業之參進，這種特徵在社群網站的市場上尤其明顯：例如 Facebook 與其他社群網站之間並不具有互通性，導致用戶欲轉移至其他平臺時必須付出相當高的轉換成本，對原本平臺的黏著度也因此提昇。故本報告建議：應允許其他社群網站平臺與優勢平臺相互連結、提昇資料之互通性與可攜性，並提供消費者及事業簡易之方式，將原本提供予優勢平臺之照片、個人檔案或其他數據轉移至其他平臺，藉此減少競爭者之參進障礙及消費者之轉換成本。

➤ **於結合審查運用推定以降低市場力**<sup>335</sup>：為了避免優勢平臺以併購鞏固其地位、消除潛在之競爭者，本報告認為，在當前無法確定競爭法主管機關就數位市場之結合案件是否具備適當分析工具、藉以判定有無競爭疑慮的情況下，應改變對優勢平臺

---

<sup>334</sup> *Id.* at 384-386.

<sup>335</sup> *Id.* at 387-388.

併購之推定。未來當主管機關審查優勢平臺之事業結合案時，除非參與結合之事業可證明此結合有利於公共利益，且該利益無法透過事業自身之內部成長及擴張實現，否則皆應推定該結案案具有限制競爭性。此外，本報告亦主張優勢平臺之結合案件不應適用現行結合門檻制度，所有優勢平臺之結合案件皆應申報，且無審查時間之限制。

➤ **為自由、多元之媒體建構公平的環境**<sup>336</sup>：自由、多元，尤其是在地化的媒體乃健全民主社會的基礎，但隨著優勢平臺竄起、掌控數位市場上的廣告與關鍵通訊領域，各種可信新聞來源的可得性卻也出現了顯著的減少。據此，本報告建議透過立法手段為新聞業者提供量身訂做的暫時性「安全港」，賦予其集體和優勢平臺議價而排除反托拉斯法適用之免責權。

➤ **禁止濫用優勢地位並要求正當程序**<sup>337</sup>：作為數位市場上的守門人，優勢平臺往往會濫用其市場力，自仰賴其運作之第三方事業及用戶手中獲取大量資料，藉此連結更多客戶及市場，甚或是強迫其他事業或個人接受其所制定之契約條款、單方面無預警地將第三方事業或個人自平臺上除名，但相較之下，依賴優勢平臺之第三方事業或個人卻不具與其對等的談判能力，本報告遂建議，應禁止優勢平臺制定限制競爭之契約條款，並對依賴平臺

---

<sup>336</sup> *Id.* at 388-389.

<sup>337</sup> *Id.* at 389-390.

之個別用戶及事業提供正當程序之保障。

## (2) 強化反托拉斯法之規範<sup>338</sup>

報告指出：雖然美國國會自 1890 年起便先後制定《休曼法》(Sherman Act)、《克雷頓法》(Clayton Act) 等法律，1936 年開始又有《羅賓森－帕特曼法》(Robinson-Patman Act)、《賽勒－凱弗維爾法》(Celler-Kefauver Act)、《哈特－史考特－羅迪諾法》(Hart-Scott-Rodino Act) 等反托拉斯法的陸續問世，但這些法規的力量卻因為司法權的行使而大幅削弱，導致聯邦的反托拉斯執法者及個別原告難以針對限制競爭行為及結合案主張其立場，進而獲得法院的支持。是故，本報告建議國會應重新聲明制定反托拉斯法之初衷及目標，並透過立法手段制定「明線法則」(Bright-Line Rule)，當參與結合事業的其中一方具有高度市場力時，即應在市場結構性之推定上依《克雷頓法》禁止其結合。

## (3) 強化反托拉斯法之執行<sup>339</sup>

針對反托拉斯法當前的執行狀況，本報告也分別就國會監督、機關執法、私部門與個人執法等不同面向提出相應的建議。

就國會監督方面，報告建議國會應恢復過去對反托拉斯法及執法之監督機制，並持續進行市場調查及立法活動；機關執法部分，報告則建議增加主管機關之預算，FTC 也應依其職權定期蒐集市場資料，

---

<sup>338</sup> *Id.* at 391-399.

<sup>339</sup> *Id.* at 399-405.

就各產業之市場結構及競爭情形提出報告；反托拉斯執法機關之透明性及公眾對機關之問責應當增強，宜要求機關審查結合案時徵求及回應公眾意見，並對外公開機關執法決定；執法機關及受審查事業之間的人員流動也須訂定更嚴格的旋轉門條款，以防不公正情事發生。

針對私部門與個人執法，報告則建議排除當前由法院所創設、對於「反托拉斯損害」(antitrust injury)及「反托拉斯當事人適格」(antitrust standing)的認定標準，透過消除訴訟程序之障礙、降低法院對於抗辯所要求之標準，使私部門與個人更有機會在司法程序中反映事業的獨占行為。

### 3. 相關司法訴訟

隨著眾議院反托拉斯小組發布「數位市場下之競爭調查」報告，主責市場公平競爭與消費者保護的聯邦反托拉斯主管機關也開始採取積極的應對措施，聯邦司法部 (Department of Justice, DOJ) 與聯邦貿易委員會 (FTC) 皆針對報告中論及的各大優勢平臺展開調查，分別對相關的反競爭行為採取了司法行動。而除了行政部門針對優勢平臺提起之反托拉斯訴訟，私人企業之間——尤其是平臺業者與程式開發商之間的訴訟，同樣也在數位市場競爭的議題上帶來了諸多討論。相關訴訟介紹如下：

#### (1) DOJ 訴 Google 案<sup>340</sup>

2020 年 10 月 20 日，DOJ 率先就 Google 鞏固搜尋引擎、線上

---

<sup>340</sup> DOJ, *Justice Department Sues Monopolist Google For Violating Antitrust Laws* Department Files

廣告市場獨占地位而為之限制競爭行為，向美國哥倫比亞特區地方法院（U.S. District Court for the District of Columbia）提起訴訟。

DOJ 指出，當前美國市場上僅有 Google、Bing、Yahoo!，以及 DuckDuckGo 四家通用搜尋引擎的供應者，而 Google 不只在過去十幾年來始終居於市場上遙遙領先的主導地位，其市場占有率更是穩定地逐年上升，直至近期已高達近 90%。對新參進者而言，通用搜尋引擎服務的創造、維持與成長需面臨巨額資本、複雜科技與規模等諸多顯著的障礙，而其中，搜尋引擎的規模更是與使用者的搜尋體驗息息相關，當前市場參進者為了參與競爭所需的規模亦遠勝以往，但 Google 採取的各種反競爭行為卻有效地削弱了對手提昇自身規模的能力，這些因素都在在顯示了 Google 在美國搜尋引擎市場上的獨占力。

---

*Complaint Against Google to Restore Competition in Search and Search Advertising Markets* (October, 2020), available at <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws> (last visited May. 10, 2021).

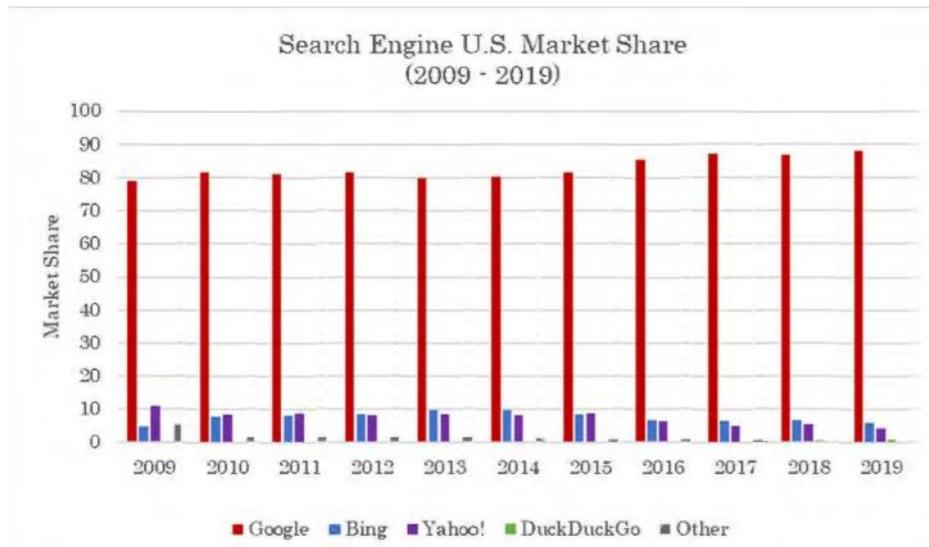


圖 3：2009 - 2019 年美國搜尋引擎市場之市占率分布

資料來源：DOJ 之起訴書<sup>341</sup>。

DOJ 在起訴書中主張，Google 用以在搜尋引擎及搜尋廣告市場上排除競爭者的違法手段包括：利用排他性的合約，禁止行動裝置預先安裝任何競爭對手提供的搜尋引擎服務，甚或是強制在行動裝置中安裝自己的搜尋引擎服務，使其無法基於使用者的偏好被刪除；與 Apple 簽署長期合約，在其廣受歡迎的 Safari 瀏覽器及其他搜尋工具中，將 Google 設定為預設且具有實質排他性的搜尋引擎。整體而言，Google 透過自身享有的獨占利潤，在各種裝置、瀏覽器與其他搜尋存取點為自己的搜尋引擎服務購買優惠待遇，最終形成了獨占自我強化的循環。DOJ 遂認為，Google 的諸多反競爭行為不只對消費者的搜尋品質帶來隱私、資料保護與資料利用等層面上的損害、限縮了消費者的選擇，更減損了新創企業研發與參與競爭的能力，應透過司法訴訟

<sup>341</sup> *U.S. v. Google LLC*, Case 1:20-cv-03010 (Oct. 20, 2020) [hereinafter DOJ Google Complaint], available at <https://www.justice.gov/atr/case-document/file/1329131/download>.

要求其終止此等反競爭行為，並為美國數位經濟的消費者、廣告商與關聯企業重建競爭秩序。

## (2) *FTC 與 46 州訴 Facebook 案*<sup>342</sup>

2020 年 12 月 9 日，FTC 亦與 46 州就 Facebook 併購 WhatsApp、Instagram 等潛在競爭對手、藉此維持社群網站獨占地位之長年違法行為，向美國哥倫比亞特區地方法院提起集體訴訟。

FTC 主張，Facebook 作為世上最有優勢的個人社群軟體服務提供者，在市場上享有獨占力，卻透過系統性的策略消滅各種潛在威脅、企圖維持其獨占地位。首先，當消費者的社群軟體使用習慣開始轉移至手機與相片分享、使得 Instagram 的市占率迅速成長時，Facebook 便以 10 億美元的價格於 2012 年收購此一競爭者。而當 Facebook 意識到手機通訊軟體的龍頭 WhatsApp 可能透過新增功能或推出獨立 app 進軍社群軟體時，亦採取了收購而非競爭的相同策略，以 190 億美元的價格於 2014 年將 WhatsApp 納入自己旗下。其次，在過去多年來，Facebook 陸續透過平臺互連權限對第三方的軟體開發商施以各種反競爭行為，例如限制開發具有競爭性之程式功能、禁止宣傳或連結至其他社群軟體服務等，以此作為允許開發商使用關鍵應用程式介面（application programming interface, API）的條件，甚或是透過關閉 API 的存取權阻斷其他社群服務、行動通訊等相類競爭對手的競爭威脅。

---

<sup>342</sup> FTC, *FTC Sues Facebook for Illegal Monopolization* (December, 2020), available at <https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization> (last visited May. 10, 2021).

舉例而言，2013 年時 Twitter 曾推出一款名為 Vine 的 app 供使用者拍攝並分享短片，但 Facebook 的回應措施卻是將 API 關閉，使 Vine 無法透過 Facebook 存取使用者的好友名單。據此，FTC 認定 Facebook 濫用自身的市場獨占力，其各種反競爭之併購行為與商業措施已傷害市場競爭秩序、減損消費者就社群服務之選擇，並剝奪了廣告商透過市場競爭獲利的機會，需透過司法程序終止。

然而，2021 年 6 月 28 日時，哥倫比亞特區地方法院法官 James Boesberg 以本案欠缺證據為由駁回訴訟，並指出原告 FTC 有責任透過清楚、大量的資料佐證 Facebook 現已控制 60% 的個人社群網路服務市場，但 FTC 在訴狀中並未詳細定義所謂個人社群網路服務的確切範圍，也欠缺證明 Facebook 收購 Instagram、WhatsApp 涉及獨占的證據力<sup>343</sup>。法官並給予原告修改訴狀、補充證據的 30 日期限。

在重新提出的補充訴狀中，FTC 針對社群軟體的用戶使用時間、每日活躍用戶數、每月活躍用戶數等指標提出了相關的統計數據，並指出 Facebook 自 2012 年開始便一直是人們使用時間最長、市占率也最高的一款社交類 app。而與此同時，市面上雖然存在著 TikTok、Twitter、YouTube 等其他公司，但這些平臺所提供的服務並不是被用來與家人或朋友進行互動，因此它們在「個人社群網站」這個市場上並沒有辦法形成 Facebook 的替代。FTC 並強調，面對消費者使用重心逐漸轉移至手機的浪潮，Facebook 其實欠缺商業上的敏銳度與相關

---

<sup>343</sup> The Verge, *Federal Court Dismisses FTC's Bid to Unwind Instagram from Facebook* (June 28, 2021), available at <https://www.theverge.com/2021/6/28/22554476/ftc-facebook-instagram-antitrust-case-whatsapp-federal-court> (last visited August. 31, 2021).

的科技技術，因此在與新參進者競爭失利後，便違法地使用將對手納入旗下或將其消滅的策略，一方面在競爭者坐大前就將其收購，一方面則依靠自身的用戶流量優勢與第三方的程式開發商簽訂排他性協議、阻斷其對潛在對手的服務，FTC 並將這種策略取名為「買或埋葬」（Buy-or-Bury）。隨著 FTC 於 8 月 19 日再次提起訴訟<sup>344</sup>，本案的後續結果仍有待追蹤。

### (3) *Epic Games* 訴 *Apple* 案<sup>345</sup>

本案的原告 Epic Games 是一間遊戲開發商，其作品《要塞英雄》（Fortnite）受到了全球廣大玩家的熱烈歡迎，並且在蘋果的 App Store 與 Google 的 Google Play 平臺皆有上架。2020 年 8 月 13 日時，《要塞英雄》在 iOS 與 Android 版的更新檔中皆增加了「Epic Direct Payment」系統，使玩家在遊戲內使用程式內付費功能時將會被引導至 Epic Games 自家的金流，藉此繞過平臺的付費抽成機制，這款遊戲遂因違反開發商協議遭到兩大平臺的下架，Epic Games 也為此在同一天內向蘋果與 Google 提起訴訟，指控兩大平臺濫用其市場力量。

在 Epic Games 起訴蘋果一案的初審判決中，北加州地區法院（United States District Court for the Northern District of California）法官 Yvonne Gonzalez Rogers 針對蘋果是否構成壟斷的爭議做出了定奪。

---

<sup>344</sup> FTC, *FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate*, available at <https://www.ftc.gov/news-events/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush> (last visited August. 31, 2021).

<sup>345</sup> *Epic Games, Inc. v. Apple Inc.*, 20-cv-05640-YGR, available at <https://cand.uscourts.gov/cases-e-filing/cases-of-interest/epic-games-inc-v-apple-inc/> (last visited October. 21, 2021).

針對本案相關產品的認定，法官並未採取兩造的對立主張，而是認為行動遊戲市場係一具有獨立性的子市場，與電腦遊戲市場、家用主機遊戲市場、雲端串流遊戲市場及非遊戲 iOS App 市場具區隔性，且 App Store 為雙邊交易市場，本案之相關產品應為數位行動遊戲交易（digital mobile game transaction）。至於市場地理範圍的判定，法官則採信蘋果的主張，採用全世界一致、包含中國的全球市場。透過蘋果內部的商業數據，法官計算出其在數位行動遊戲交易市場上的市占率自 2015 年的 52.9% 逐步攀升至 2020 年的 57.6%。而按照過往的判例，市占率雖非唯一指標，但構成壟斷的企業通常會達到 65% 至 75% 的市占率。

另一方面，Epic Games 主張蘋果的作業系統 iOS 為主市場（foremarket），並以此延伸出散布 iOS app 的 App Store 與應用程式內購買（In-App Purchase，IAP）兩個售後市場（aftermarkets），彼此之間的關係類似刮鬍刀與替換式刀片，但法官根據 2008 年美國聯邦第九巡迴上訴法院的 *Newcal Industries v. Ikon Office Solution* 判例<sup>346</sup>，指出了單一品牌的售後市場是否構成壟斷的四個判斷標準，包括：一、售後市場係完全由主市場發展而來。二、壟斷行為僅發生在售後市場。三、該品牌的市場力來自與消費者之間的關係，其在售後市場的市場力並非來自主市場的契約授權。四、售後市場的反競爭行為未能被準確地傳遞到主市場的競爭之中。

法官分析，App Store 與 IAP 這兩個售後市場確實能滿足該案判準的前三個條件；但針對第四個條件，Epic Games 並沒有辦法證明消

---

<sup>346</sup> *Newcal Industries, Inc. v. IKON Office Solution*, 513 F.3d 1038

費者是否對 App Store 為 iOS 平台唯一的 app 來源毫不知情，且法官認為，iOS 多年來皆以其封閉性聞名，並與具有開放性的 Android 平臺相互競爭，消費者照理應對此知情。

綜上所述，本案判決認定蘋果並未在數位行動遊戲交易市場上構成壟斷。然而另一方面，法官在判決宣布的同時又發布了永久禁制令，要求蘋果未來不得再禁止開發商於程式內告知消費者 IAP 以外的付費管道，並於 90 天後生效，這起訴訟的結果也因此遭外界評為「兩造皆輸」<sup>347</sup>。

#### 4. 總統拜登發布「促進美國經濟競爭」命令

隨著當前進行中的各大反托拉斯訴訟引起全球關注，2021 年 7 月 9 日，美國總統拜登也發布「促進美國經濟競爭」行政命令 (Executive Order on Promoting Competition in the American Economy)<sup>348</sup>，正式宣示了行政團隊未來的整體政策路線規劃。

該命令開宗明義指出進一步強調豐沛的市場競爭是美國經濟領先全球之關鍵，政府有義務積極作為、導正後疫情時代的健全市場。而就具體措施而言，該命令所觸及之領域橫跨農業、電信業、資訊業、金融業與醫療健保業，除為行政機關設立整合性的行動方針與跨機關之協調機制，確立白宮競爭委員會所扮演之角色，更敦促各主管機關

---

<sup>347</sup> The Verge, Apple and Epic Both Lost Today, available at <https://www.theverge.com/2021/9/10/22667769/apple-epic-lost-lawsuit-verdict-ruling> (last visited October. 21, 2021).

<sup>348</sup> The White House, Executive Order on Promoting Competition in the American Economy (July 9, 2021), available at <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/> (last visited August.19, 2021).

積極落實反托拉斯法、促進市場競爭。

其中，與數位平臺相關之政策方向包括：FTC 應針對不公平之資料蒐集與資料監控，以及網路市場之不公平競爭進行立法，也應更公平、積極地行使反托拉斯法所賦予之職權，挑戰過往政府放任的事業結合案，並重新審視現行之垂直、水平事業結合規範。命令中更強調，科技巨頭收購潛在競爭者、藉以扼殺競爭威脅的「殺手併購」在過往時常受到監理機關的放任，甚至不曾受到實質的結合審查，未來監理機關的執法方向將會採取更加嚴格的審查基準，並特別關注大型網路平臺的結合與限制競爭行為。

## （二）資料應用對市場競爭之影響

### 1. 美國聯邦層級之個人資料保護與資料流通

由於美國向來將個人資料保護與隱私權視為消費者權益保障之一環，若從聯邦層級觀之，美國並未透過法規對資料之跨境自由流通進行限制或禁止；即便在 1996 年《電信法》(Telecommunications Act of 1996) 裡，也僅設立了相當狹隘的資料隱私條款<sup>349</sup>，因此整體而言，美國的立法趨勢係傾向支持資料自由流通不受限制、反對「資料貿易保護主義」(Data Protectionism) 的立場<sup>350</sup>，並透過業者自律維持市場運作，輔以聯邦貿易委員會 (Federal Trade Commission, FTC) 提供的行業規範與第三方程序等部門式立法進行監督。

---

<sup>349</sup> 47 U.S.C. § 222。

<sup>350</sup> Information Technology and Innovation Foundation [ITIF], *International Data Flows: Promoting Digital Trade in the 21st Century* (2015), available at [http://www2.itif.org/2015-atkinson-international-data-flows.pdf?\\_ga=1.242200450.1428966053.1450714332](http://www2.itif.org/2015-atkinson-international-data-flows.pdf?_ga=1.242200450.1428966053.1450714332) (last visited May. 2, 2021).

面對近年蓬勃發展的數位經濟與相應而生的資料流通議題，美國總統行政辦公室（Executive Office of the President）曾在2014年5月發布《大數據：掌握機遇，確保價值》（Big Data: Seizing Opportunities, Preserving Values）白皮書<sup>351</sup>，藉此傳達行政部門對於大數據潛藏價值的高度重視，進而就大數據之分析、儲存、加密、網路安全、運算能力、人才等項目展開重大投資。但另一方面，白皮書對於數據蒐集、處理與共享所面臨的嚴峻挑戰也有所意識，無論是公民與消費者權利的保障、或是商業利益和隱私權之間的平衡，亦是行政部門相當關切的議題。

針對資料的利用與流通，白皮書中特別針對以下各點提出了觀察與建議<sup>352</sup>：

➤ **資料服務業之透明度**：業者應主動提高其服務之透明度，使消費者更加清楚地瞭解其所提供之資料與該服務之業務有何關聯。無論是第三方的資料蒐集者、資料服務業、網路廣告和信貸行業，皆應在企業自身的網站上明確揭示其資料處理政策，向消費者提供控制資料蒐集與利用的方法，並使消費者能自主選擇退出某些商業用途。

➤ **大數據與差別待遇**：當前透過大數據進行的資料分析已逐漸擴及健康、教育、就業、信用等領域的諸多服務，但其用於自動化決策的技術卻缺乏透明度。針對此種技術結合在自動化決

---

<sup>351</sup> White House, *Big Data: Seizing Opportunities, Preserving Values* (May 2014), [https://www.whitehouse.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf).

<sup>352</sup> *Id.* at 58-68.

策過程中產生的差別待遇問題，必須有能力加以檢測與糾正。

➤ **大數據分析與資料共享作為強化網路安全之手段：**若能提高網路威脅資料的共享程度，大數據將能成為一種強化網路安全與保護關鍵基礎設施研究的手段。在現行的網路安全機制下，網路威脅資訊的分享與受害資訊的即時通報皆是有助於公私部門預先分析、應對威脅的重要因素，若能透過大數據分析加以識別不正常的網路活動模式，便有可能在早期預警網路威脅的發生。就此而言，公私部門之間的資料共享將會是預警技術仰賴的關鍵。

➤ **資料作為公共資源：**政府資料作為一種國家資源，應廣泛向公眾開放、藉此提高政府效率，並在推動經濟與社會利益的同時確保個人隱私、商業機密與國家安全。政府應開放、公布其大型數據集，並確保所有機構能最大限度地利用聯邦數據工具 Data. Gov 與資料庫。透過大數據的幫助，公共服務的品質、新政策的擬定，以及各級政府使用納稅人資金的效率皆有可能獲得提昇。

2016 年 5 月，美國總統行政辦公室則發布《大數據：演算法系統、機遇與公民權利報告》(Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights)，進一步從信用、勞雇、高等教育、刑事司法等不同角度切入，研析近年來大數據在不同領域的利用狀況，以探討其帶來的機遇與挑戰。舉例而言<sup>353</sup>：

---

<sup>353</sup> White House, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, at 11-21 (May 2016), available at [https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016\\_0504\\_data\\_discrimination.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf) (last visited May. 12, 2021).

➤ **大數據與信用**：對渴望在經濟上躋身中產階級的受薪勞動者而言，與銀行放款條件息息相關的信用評等乃是相當重要的一項因素，但根據消費者金融保護局（Consumer Financial Protection Bureau, CFPB）的研究，全美卻有約莫 11% 的消費者處於「信用隱形」(credit invisible) 的狀態，因演算法缺乏其與時俱進的還款、繳費紀錄，而無從產生信用評等。統計資料更顯示，在信用隱形者中，不只非裔與拉丁裔（15%）較白人（9%）占更高的比例，這種現象也明顯與低收入族群（30%）有高度相關。為了解決信用隱形的現象，報告中提供的解決方式是建立一套從複數來源汲取分析資料的新式評等系統，透過結合電話帳單、公開資料、教育背景、稅務紀錄等大量資料，甚至是手機定位、社群網站上的資訊、網路購物服務的消費偏好、瀏覽個人金融網站時滑鼠滾動的速度等非傳統資料，為當事人提供更加量身訂作、經濟上合理的信用評等。但相對地，這套系統也可能導致偏見、歧視被惡化或掩蓋，甚至使消費者更難對資料的可信度與評等的合理性提出質疑，故其透明性、消費者對資料蒐集的知悉權與對資料正確性的申訴權將至關重要。

➤ **大數據與勞雇**：隨著美國企業開始仰賴網路媒合服務進行人才招聘，用以從大量投遞資料中篩選出適當人選的演算法也應運而生。但由於演算法終究是人為產物、也可能構築於有缺陷的資料，其運作自然也有可能繼承各種人為判斷時帶有缺陷的評估與推定，有延續偏見的可能，因此報告中呼籲：企業應採用以資料為導向的方法，尋找傳統教育、職場經驗篩選方式中可能遺漏的潛在受雇者，並以機器學習客觀分析現有員工能力、經驗與

其職場成就之關聯性，藉此為未來受雇者應具備的特質建立一套可依循的模式。倘若能以公平、道德與機遇作為核心的設計要件，一個規模龐大的資料系統便有助於對抗傳統人力招募過程中造成歧視的內、外在偏見。

很顯然地，面對近年興起的大數據與演算法，如何透過一套客觀運行的評定機制消弭其隱含的偏見，並在快速變遷的技術環境中建立監督的機制，是美國行政部門在資料流通議題上持續努力與關切的方向。

## 2.FTC 執法面向

如前所述，美國在聯邦層級對於資料流通的處理是採取反對資料貿易保護主義的立法趨勢，並以 FTC 提供的部門式立法進行市場自律的監督。作為 1970 年代起美國個人資料保護的主要執法機關<sup>354</sup>，FTC 的職權係自其原始執掌的消費者權益保護衍生而來，並致力在保障消費者隱私、安全的同時，兼顧促進創新與競爭。根據 2018 年 FTC 就消費者隱私及資料自由流通政策向美國國家電信暨資訊管理局（National Telecommunications and Information Administration, NTIA）提出的回應，其將歷年來經手的個人資料案例歸納為至少四種類型的損害態樣<sup>355</sup>，包括：

---

<sup>354</sup> FTC, *Protecting Consumer Privacy and Security*, available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security> (last visited May. 12, 2021).

<sup>355</sup> FTC, *Comment to the National Telecommunications & Information Administration on Developing the Administration's Approach to Consumer Privacy*, No. 180821780-8780-01, at 8-9 (Nov. 9, 2018), available at [https://www.ftc.gov/system/files/documents/advocacy\\_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400\\_ftc\\_comment\\_to\\_ntia\\_112018.pdf](https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf) (last visited May. 12, 2021).

➤ **財務損害 (Financial Injury)**：主要指金錢或財產受到的損害，例如詐欺、身分偽造，也包含因個人資料遭外洩、盜用而衍生，對時間、機會成本所生之損害。

➤ **人身損害 (Physical Injury)**：包含對個人健康或人身安全的威脅，例如受跟踪或騷擾的風險。

➤ **名譽損害 (Reputation Injury)**：因私密資訊或事務遭不當揭露，進而形成對個人名譽的可能損害。例如醫療或病歷資料的外洩，個人行蹤記錄的外洩等。

➤ **惡性侵擾 (Unwanted Intrusion)**：即個人日常生活遭到不當的打擾，大體而言可區分為兩種類型。其一是個人居住或私密活動的場所遭到入侵，例如家庭網路攝影機的資料外洩；其二則為引發反感的商業性侵擾，例如推銷、騷擾電話、垃圾郵件等。

但 FTC 也在報告中強調：即便資料的不當利用可能對大眾帶來風險，不可否認的是，資料的利用本身仍然具有推動創新及競爭的效用，可在數位經濟時代下增進消費者福祉，為個人節省時間及金錢成本、挖掘商機、推動創新服務，進而為社會、環境帶來廣大的利益。舉例而言，若能對資料進行妥適的利用，銀行或可主動辨識客戶是否遭受詐欺、各式各樣的行銷服務能更加對消費者的需求量身訂作、感測裝置可以讓人類的生活環境更添舒適。資料的利用或許會造成危害，也可能成為防制危害的手段。

據此，FTC 從防止不公平、遏止詐欺與反競爭行為等消費者保護的角度切入，進一步提出了四項依循的政策原則：「安全」、「透明」、

「控制」，以及「執法」<sup>356</sup>。

➤ 安全 (security)：針對資料安全領域，FTC 在過往已處理了超過 60 起企業未依循合理安全措施之指標案件，並在判斷案例主採用之資料安全措施有欠妥適、或是揭露之安全資訊有誤導性的情況下進行裁處。

➤ 透明 (transparency)：作為 FTC 長期依循的隱私政策指標之一，透明的重點在於該「如何」(how) 及「何時」(when) 向消費者提供有關資料蒐集之重要資訊，並且透過消費者可理解、對其有意義的方式進行資料利用。許多隱私條款對消費者不是內容過於繁雜導致難以閱讀，就是內容過於簡略導致欠缺透明度，但其仍然構成了主管機關向業者問責的依據，該條款是否有被揭露、以及是否有確實被業者達成，皆是 FTC 作成處分時的判斷依據。

➤ 控制 (control)：控制的重點在於賦予消費者對資料蒐集與利用的掌控。但若消費者完全拒絕資料的蒐集與利用，對於當代數位經濟的發展仍會帶來不利，故 FTC 盼能在消費者權益保障與商業利益之間達成平衡。FTC 並指出，資料控制的程度是否妥適，需將消費者偏好、整體脈絡（包括風險）與形式皆納入判斷。例如在資料利用符合業務性質或企業與消費者之關係、或是受到法規授權或要求的情況下，當事人的同意可能就非必要；反之，在資料蒐集與利用可能對個人帶來極高的風險或損害，例

---

<sup>356</sup> *Id.* at 12-18.

如資料具有高度敏感性的情況下，當事人的同意便會相應地具有重要性。另外，FTC 也強調，當企業提供消費者同意的選擇時，也應考量當事人之真意，設計出可使其確切同意的機制。

➤ 執法 (enforce)：藉由自身的執法權力，FTC 的主要打擊對象在於消費者資料遭不當利用、企業未妥善保管敏感個人資料的案件，但其在報告中也指出自身的執法仍存在著某些侷限。其一，包括非營利組織在內的對象並不屬於 FTC 的管轄範圍，但此類組織的行為對於資料安全仍有相當的影響力；其二，FTC 所依循的隱私保護及資料安全法規本身也存在著固有的限制，例如《兒童線上隱私保護法》(Children's Online Privacy Protection Act, COPPA) 僅規範網路上以兒童為對象的資料蒐集，對於網路之外或非以兒童為對象的資料蒐集行為卻無法著力；《健康保險可攜性及責任法》(Health Insurance Portability and Accountability Act, HIPAA) 的管制對象則為醫生、保險公司與醫院，而不適用於直接從消費者蒐集資料的健康應用程式、網站、資料仲介業者或廣告網路。故 FTC 也在報告中呼籲，若其就資料隱私之執法權力可獲提昇，將有助於獲得與其職權需求相應的資源。

### 3. 美國的資料跨境傳輸協議

相較於境內傾向市場自律的資料保護政策與立法態度，美國對於資料跨境傳輸與個資保護規範的努力則主要體現在「貿易無障礙」的追求上，故其歷來簽署之資料跨境傳輸協議也多以貿易與商業考量、解決國與國之間的概念落差為導向。以個人資料保護規範較為週延的歐盟為例，美國歷來便曾與其簽訂過「安全港協議」(Safe Harbor)、

「隱私盾協議」(Privacy Shield) 等資料跨境傳輸協議。

### (1) 美國－歐盟之安全港框架協議

由於歐盟將資料隱私視為人權保障之一環，與美國隱私保護的方向有所不同，為了解決兩地之間的法規落差及資料流通困境，歐盟執委會(European Commission)與美國商務部(Department of Commerce, DOC)於2000年簽署了全球第一份規範資料跨境傳輸的國際協議——「安全港協議」<sup>357</sup>，透過符合歐盟指令規範之合理國際傳輸方式，以促進歐美貿易往來為前提，允許雙方之企業與個人流通「個人可識別資料」(Personally Identifiable Information, PII)<sup>358</sup>，並且基於美國應尊重歐盟隱私保護標準之核心精神，建立折衷處理兩國間隱私相關程序措施的框架。

安全港協議建立的七大原則係「告知」(Notice)、「選擇」(Choice)、「傳輸」(Onward Transfer)、「安全」(Security)、「資料真實性」(Data Integrity)、「存取」(Access)，以及「執行」(Enforcement)，其具體內涵分別為：

- 「告知」原則：機構(organizations)應向資料當事人告知個資蒐集與利用之目的，提供當事人相關意見聯絡或申訴管道之資訊，或向第三方揭露資訊之第三方型態。此外，提供資料之

---

<sup>357</sup> Commission Decision 2000/520/EC pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

<sup>358</sup> DOC, *U.S.-EU Safe Harbor Framework A Guide to Self-Certification* (2009), available at [https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1650&context=key\\_workplace](https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1650&context=key_workplace) (last visited May. 12, 2021).

當事人對於自身資料應擁有一定程度之主導權，包括限制利用與揭露欄位、選項、方法等。當機構向資料當事人要求提供資料或於之後實際運用時、每次進行目的外使用、傳輸前處理，或第一次向第三方揭露資料時，機構應主動向資料當事人履行告知義務<sup>359</sup>。

➤ 「選擇」原則：資料當事人對於是否將其個人資料揭露予第三方有選擇權。當有目的外使用或授權目的時，機構應事先取得資料當事人之同意。此外，當資料被歸為敏感性資料時，亦須依循前揭規定，並提供資料當事人肯定且明確、表示是否加入（opt in）之選擇<sup>360</sup>。

➤ 「傳輸」原則：機構將資料揭露給第三方之際，必須遵守「通知及選擇原則」（Notice and Choice Principles）<sup>361</sup>。

➤ 「安全」原則：機構對於個人資料的蒐集、處理、利用或傳輸，應採取合理之預防措施，並應保護個人資料，避免其遺失、濫用、未經授權存取、外洩、竄改或遭到破壞<sup>362</sup>。

➤ 「資料真實性」原則：對於所管理的個人資料，機構有義務採取合理的方式與步驟，確保在特定目的範圍內，進行個人資料之蒐集、處理、利用，並應維持資料內容之真實性、正確性、

---

<sup>359</sup> Commission Decision 2000/520/EC, Ann. I, Notice.

<sup>360</sup> Commission Decision 2000/520/EC, Ann. I, Choice.

<sup>361</sup> Commission Decision 2000/520/EC, Ann. I, Onward Transfer.

<sup>362</sup> Commission Decision 2000/520/EC, Ann. I, Security.

完整性及最新性<sup>363</sup>。

➤ 「存取」原則：個人資料為機構持有之資料主體，原則上具有存取其資料之權利。且當資料有錯誤狀況時，應進行更正、修改或刪除<sup>364</sup>。

➤ 「執行」原則：機構應訂定相關規範，以確保安全港原則之遵循；規範中也應明定違反之效果，及至生損害時之救濟方式<sup>365</sup>。

總結來說，歐盟與美國之間的個人資料跨境傳輸重點在於機構自律。機構的自我認證與自我評估應為法所允許，其遵循隱私保護之方式需符合安全港隱私原則之要求，並向美國商務部提出自我認證之申請、公布安全港隱私政策，並揭露自身將如何遵循隱私原則。

雖然安全港協議旨在弭平歐盟與美國之間的概念鴻溝與規範落差，透過內容明確、具有可操作性之原則促進兩地基於資料跨境傳輸的經濟貿易合作與互動，甚至填補了國際上有關跨境傳輸資料保護的規範空白，但隨著 2013 年美國爆發史諾登(Edward Joseph Snowden)洩密事件，歐美雙方關係產生劇烈動盪，安全港協議也在 2015 年 10 月因未能充分保障歐盟民眾隱私而遭歐盟法院(European Court of Justice, ECJ)的 Schrems I 判決宣告無效<sup>366</sup>。在此之後，歐盟各會員國可自行訂立與美國企業使用的國民隱私資料規定，並要求美國企業

---

<sup>363</sup> Commission Decision 2000/520/EC, Ann. I, Data Integrity.

<sup>364</sup> Commission Decision 2000/520/EC, Ann. I, Access.

<sup>365</sup> Commission Decision 2000/520/EC, Ann. I, Enforcement.

<sup>366</sup> C-362/14, *Maximilian Schrems v Data Protection Commissioner*. 29 October 2015.

必須將個資存取於境內，甚至可禁止將個資跨境傳回美國<sup>367</sup>，歐盟各會員國也紛紛對資料保護法規展開了修法工作，導致美國境內企業遭受劇烈的衝擊。

## (2) 美國－歐盟之隱私盾框架協議

根據歐盟執委會之研究，歐美資料流通之阻礙恐造成歐盟整體國民生產總值（Gross National Product，GNP）下降 0.8% 至 1.3%<sup>368</sup>；美國的商務意見也曾指出，歐美安全港協議一旦失效，將帶給歐美數位經濟負面衝擊<sup>369</sup>。有鑑於此，當安全港協議於 2015 年 10 月遭歐盟法院宣告無效後，美國旋即就政治、法律與技術等層面之問題解決再次與歐盟展開協商，最終於 2016 年 2 月達成美國境內伺服器處理歐盟人民個人資料之處理規範——「隱私盾協議」，藉此作為取代安全港協議的資料跨境流通新框架。而為了提昇對歐盟民眾個資安全的保障，該協定更承諾遵循歐盟規章，使之准許歐盟個資存放於美國的資料中心<sup>370</sup>。

按隱私盾協議之內容，美國以書面承諾其官方機構保護國安之行動，將受到明確的監管機制規範，亦不會對歐洲國民實施無差別的大規模監控；只要歐盟消費者提出申訴，該保管個資之美國企業即有義務配合強制仲裁，美國政府亦須設置專責人員協助調查，並於每年召

---

<sup>367</sup> See Mark Scott, *Data Transfer Pact Between U.S. and Europe Is Ruled Invalid*, Oct. 6, 2015, THE NEW YORK TIMES, available at

<https://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html>

(last visited May. 13, 2021).

<sup>368</sup> See generally Yann Padova, *The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?*, 6 INT'L DATA PRIVACY L. 139 (2016).

<sup>369</sup> *Id.* at 140.

<sup>370</sup> See Shona McCusker, *The EU-US Privacy Shield: The Antidote To The Transatlantic Data Transfer Headache? Headache?*, 37 BUSINESS LAW REVIEW 84, 84-85 (2016).

開一次歐盟與美國聯邦貿易委員會的聯合評估<sup>371</sup>。

然而，當年曾在 *Schrems I* 一案挑戰安全港協定、導致其被歐盟法院判決無效的奧地利原告 Maximilian Schrems 又再次起訴，主張 Facebook 設立於愛爾蘭之子公司透過標準契約條款（standard contractual clause, SCC）將使用者個人資料傳輸回美國母公司，由於此一機制僅能約束契約雙方，無從拘束國家，Schrems 認為歐盟的資料主體將無法因此獲得妥適的保障<sup>372</sup>，愛爾蘭高等法院遂於 2018 年 5 月 4 日將本案提交至歐盟法院，請求一併檢視隱私盾協議與 SCC 之有效性。

就結論而言，歐盟法院在 *Schrems II* 一案的判決中肯定了 SCC 的有效性，另一方面卻也宣告美國與歐盟簽訂之隱私盾協議無效<sup>373</sup>，而歐盟法院作成如此結論的理由係依據以下兩點：其一，美國的情報監控法規就個人資料監控之實施違反比例原則與必要性原則，例如其《外國情報監視法》（Foreign Intelligence Surveillance Act, FISA）第 702 條便允許國安局獲取電子形式儲存之數據，藉此蒐集美國境外非美國人的外國情報；其二，雖然美國政府實施個人資料監控時須遵守隱私盾協議的要求，但歐盟的資料主體卻並未被賦予救濟權，無法在

---

<sup>371</sup> See Natalia Drozdiak & Sam Schechner & John D. McKinnon, *U.S., EU Reach Deal on New Data Transfer Framework*, THE WALL STREET JOURNAL, Feb. 2, 2016, available at <https://www.wsj.com/articles/u-s-eu-reach-deal-on-new-data-transfer-framework-1454429818> (last visited May 12, 2021).

<sup>372</sup> Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – Data Protection Commissioner v Facebook Ireland Limited, Maximilian Schrems (Case C-311/18), available at <https://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=583421> (last visited May 20, 2021).

<sup>373</sup> Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, 16 July 2020.

權益遭受侵害時透過訴訟保障自身的權益，有鑑於此，隱私盾協議的架構無從為歐盟公民提供充分的保障，亦不符歐盟的隱私規範要求。

由於 *Schrems II* 判決並未提供任何的寬限期，導致超過 5,300 家適用隱私盾的企業受到巨大衝擊，美國商務部長隨即發表新聞稿，表示對該判決的結果感到「相當失望」<sup>374</sup>，但仍會持續與歐盟執委會及資料保護委員會就此議題展開研究與協商；美國商務部<sup>375</sup>與歐盟料保護委員會<sup>376</sup>後續也相繼在網站上發布常見問答集，為協議失效後的利害關係人提供有關應對措施的指引。直至 2021 年 3 月，歐盟執委會司法執行委員（Commissioner for Justice）與美國商務部長進一步發表了聯合聲明，表示將繼續歐盟與美國之間的隱私盾協議改革談判，使新一代的協議內容符合歐盟法院在 *Schrems II* 判決中提出之要求<sup>377</sup>。

2021 年 6 月 4 日，歐盟執委會進一步通過了兩份新版標準契約條款，其一針對將個人資料跨境傳輸至第三國接收者之情形<sup>378</sup>，其二則規範資料控制者將個人資料跨境傳輸至第三國之資料處理者之情

---

<sup>374</sup> U.S. EMBASSY IN LUXEMBOURG, *U.S. Secretary Of Commerce Wilbur Ross Statement On Schrems II Ruling And The Importance of EU-U.S. Data Flows*, available at <https://lu.usembassy.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/> (last visited 2021/5/21).

<sup>375</sup> PRIVACY SHIELD FRAMEWORK, FAQs – EU-U.S. Privacy Shield Program Update, available at <https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update> (last visited 2021/5/21).

<sup>376</sup> EUROPEAN DATA PROTECTION BOARD, *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*, available at [https://edpb.europa.eu/sites/default/files/files/file1/20200724\\_edpb\\_faqoncjeuc31118\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf) (last visited 2021/5/21).

<sup>377</sup> EUROPEAN COMMISSION, *Intensifying Negotiations On Transatlantic Data Privacy Flows: A Joint Press Statement By European Commissioner For Justice Didier Reynders And U.S. Secretary Of Commerce Gina Raimondo*, available at [https://ec.europa.eu/commission/presscorner/detail/en/statement\\_21\\_1443](https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443) (last visited 2021/5/21).

<sup>378</sup> Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance).

形<sup>379</sup>。為符合 GDPR 與 *Schrems II* 判決之見解，新版的標準契約條款涵蓋了多種類型的個人資料傳輸型態，並以模組化的設計建立契約範本，允許複數締約方加入使用，對複雜的個人資料處理型態提供更多彈性；除此之外，新版的標準契約條款亦要求資料控制者於資料傳輸前進行實質的影響評估，確保個人資料之接受者是否能完善資料保護之義務，且應於監理機關要求時提供相關影響評估報告。新版標準契約條款預計於公布後 3 個月正式實施，即便是未在歐盟設立據點但受 GDPR 規範之資料控制者與資料處理者，亦應適用；使用舊版條款之企業則享有 18 個月的轉換期，其全面實施後，勢將對歐盟的隱私保護與資料跨境傳輸帶來深遠影響。

#### 4. 資料法制革新之嘗試

雖然美國缺乏聯邦層級的資料流通法制，並在立法上傾向支持資料自由流通不設限的立場，但隨著科技日新月異、數位經濟蓬勃發展，個人隱私保護的意識也開始高漲，使得資料隱私逐漸被視為基本權的一環。在歐盟嚴格的《一般資料保護規則》(GDPR) 影響下，不只多數企業開始採取相應的法規遵循措施，美國境內無論在州立法、甚至聯邦立法的層級也受到啟發，相繼出現保護資料隱私的立法聲浪。

在當前這股美國資料法制革新的浪潮中，最值得關注者乃 2020 年 1 月 1 日正式生效施行的《加州消費者隱私法》(California

---

<sup>379</sup> Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Text with EEA relevance).

Consumer Privacy Act, CCPA )<sup>380</sup>。由於該法設計之嚴謹可與歐盟 GDPR 比肩，也導致加州既有的隱私權規範產生了相應的變化。

顧名思義，CCPA 所保護的主體為加州的消費者，即居住在加州的自然人，且其範圍不只包括所有非暫時性居留於加州之人，也及於暫離加州但居籍仍在加州之住民。針對資料的刪除、存取與分享，CCPA 賦予消費者的權利可概分為以下類型：其一，針對企業經營者蒐集個人資料時有無明確告知蒐集範圍、分享對象、蒐集來源、蒐集目的、要求資料揭露、製作資料複本確認之用等事項，消費者享有知悉權 (Right to Know)。其二，給予消費者拒絕企業經營者利用、分享或銷售個人資料的退出權 (Right to Opt out)。其三，當企業因未妥善保護其所蒐集之個人資料而造成損害時，消費者可主張賠償請求權<sup>381</sup>。CCPA 甚至賦予了消費者「主觀權利要求」(Subject Rights Request, SRR)，使任何的加州消費者都可依法就其權利提出，而受要求之企業經營者對於每次要求皆須在 45 天內處理，且其處理不得有差別待遇。

另一方面，按 CCPA 之規定，企業經營者對於被蒐集個人資料的類別、來源別、蒐集或出售個人資料的營業或商業目的、共享消費者個資的第三方類別、具體個資內容等事項皆有揭露義務。如未遵循此規範，加州總檢察長可對每次違規進行最高 7,500 美元的裁處；加上當事人擁有損害賠償請求權，消費者自身也能為單獨或集體訴訟，藉

---

<sup>380</sup> *The California Privacy Rights and Enforcement Act of 2020* (2019), available at <https://oag.ca.gov/system/files/initiatives/pdfs/19-0019%20%28Consumer%20Privacy%20-%20Version%202%29.pdf> (last visited May. 21, 2021).

<sup>381</sup> CALIFORNIANS FOR CONSUMER PRIVACY, *Executive Summary*, available at <https://www.caprivacy.org/cpra-exec-summary/> (last visited May. 21, 2021).

此請求損害賠償、申請禁制令或其他救濟。

在正式施行的第一年裡，CCPA 光是在集體訴訟部份就已促成了至少 73 起由聯邦法院審理的案件<sup>382</sup>；2021 年第一季的訴訟則多與企業經營者未提供合理安全程序、導致用戶資料遺失或遭受勒索攻擊有關<sup>383</sup>。雖然針對資料外洩事件的處理，CCPA 並不會對年度總收入低於 2,500 萬美元、用戶個資處理與蒐集數不超過 5 萬筆，且年收入 50% 並非源自加州居民個資的商業行為生效，然若企業經營者侵害該法賦予消費者的權利，面臨的裁處將比歐盟的 GDPR 更為嚴厲。因此儘管 CCPA 的規範內容與 GDPR 類似，對企業經營者的法規遵循而言，其恐將帶來更加沈重的負擔。更遑論加州作為全美人口最多、經濟體量最龐大的城市，CCPA 的施行成效無疑會是一大指標，未來也將影響各州的資料保護政策與立法趨勢。

除了已在加州施行的 CCPA，美國的聯邦立法層級也不乏重新思考資料法制的呼籲，眾議員 Suzan DelBene 於 2021 年 4 月提出的《資訊透明與個人資料控制法》（Information Transparency & Personal Data Control Act）草案即為一例<sup>384</sup>。該草案內容效法 GDPR 之精神，針對個人資料控制者（controller）、處理者（processor）與第三方之蒐集、傳輸、儲存、販售、分享等行為進行規範，明確定義敏感性個人

---

<sup>382</sup> THE NATIONAL LAW REVIEW, *With All This Talk About The CCPA Litigation Risk, How Many CCPA Class Actions Actually Got Filed In 2020?*, available at <https://www.natlawreview.com/article/all-talk-about-ccpa-litigation-risk-how-many-ccpa-class-actions-actually-got-filed> (last visited May. 21, 2021).

<sup>383</sup> THE NATIONAL LAW REVIEW, *2021 CCPA Q1 Litigation Report: 35+ Cases Filed, Unsurprising Trend of Data Event Class Actions*, available at <https://www.natlawreview.com/article/2021-ccpa-q1-litigation-report-35-cases-filed-unsurprising-trend-data-event-class> (last visited May. 21, 2021).

<sup>384</sup> GovTrack.us, *H.R. 1816: Information Transparency & Personal Data Control Act*, available at <https://www.govtrack.us/congress/bills/117/hr1816> (last visited May. 21, 2021).

資料，以強化個人資料之自主控制，並授權 FTC 為主管機關，其立法動態也值得觀察。

## 二、數位平臺問責

隨著數位經濟蓬勃發展，各種新興服務逐漸滲透人們的日常生活與社交活動，Facebook、Twitter 等新興數位傳播平臺也為言論市場帶來了巨大的改變。面對掌握龐大數據、影響力甚至可與政府機關比肩的數位平臺，其監督與問責自然也成了當代法制政策亟需關注的焦點。就此而言，美國長年來針對 1996 年《通訊端正法》（Communication Decency Act of 1996，下稱 CDA）第 230 條<sup>385</sup>存廢與修正之討論，以及近年來逐漸受到重視的有關 FTC 對於平臺隱私責任之執法，皆是值得吾人追蹤的議題。

### （一）CDA 第 230 條之爭議與修法動態

#### 1. 規範概述

自 1990 年代網際網路服務萌芽之初，網路中介業者是否應就第三人侵權內容負法律責任的爭議便從未止息。根據 1995 年紐約州最高法院在 *Stratton Oakmont v Prodigy Service* 此一指標性判決中的見解<sup>386</sup>，當電子佈告欄（Bulletin Board System, BBS）之經營者對於論壇上張貼之內容有板主、過濾系統等審查控制能力，卻未善盡管理義務時，應就使用者發表之誹謗言論負「出版人」責任。但該判決在實際

---

<sup>385</sup> 47 U.S.C. § 230(c).

<sup>386</sup> *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N. Y. Sup. Ct. 1995).

上卻造成了網路平臺服務提供者進退維谷的困境——若積極管理平臺內容，恐將構成出版人責任而需為第三方發表的言論負責；若完全放任平臺自行運作，則又可能導致用戶處於不當內容充斥的使用環境。在前述判決的影響下，為了促進網際網路蓬勃發展，1996 年通過的 CDA 第 230 條遂為平臺業者創設了「善良撒馬利亞人」(Good Samaritan) 的免責規定，若其刪除或限制對特定內容的訪問，即可不必對第三人的侵權內容承擔民事責任，以此作為網路平臺的「安全港」(Safe Harbor) 條款，並鼓勵網路服務提供者主動採取合理的措施，為使用者清除不法內容、維護良好的網路空間。

從 CDA 第 230 條的基本結構觀之，此一責任安全港條款的規範內容可分為以下兩部分：

### (1) 適用主體

按 CDA 第 230 條(c)(1)規定：「互動式電腦服務之提供者或使用者，就其他資訊內容提供者所提供之資訊，不應被視為出版人及發表人」<sup>387</sup>。

此處所謂的「互動式電腦服務」(Interactive Computer Service)，係指：「提供或讓多數使用者電腦得以連結至同一電腦伺服器之任何資訊服務、系統、或接取軟體，具體而言包括提供網際網路接取的系統或服務，以及由圖書館或教育機構所經營的這類系統或提供的服務」<sup>388</sup>，故適用 CDA 第 230 條的典型網路中介者，包括社群平臺如 BBS

---

<sup>387</sup> 47 U.S.C. § 230(c) (1). No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

<sup>388</sup> 47 U.S.C. § 230(f) (2). The term “interactive computer service” means any information service,

討論版、Facebook、Twitter 等，也包括資訊中介平臺如租屋媒合網站、電子商務平臺等。

## (2) 免責條件

根據 CDA 第 230 條(c)(2)規定：互動式電腦服務提供者或使用者，無需因下列原因負責。包括：針對服務提供者或使用者認為猥褻、邪惡、淫亂、過度暴力、騷擾性或其他令人不快之內容，無論該內容是否受到憲法保護，為了限制其接觸或取得而基於善意 (good faith)、自願 (voluntarily) 採取之任何行為；或任何採取科技方法以限制接取上述內容之行為。

## (3) 競合規範

根據 CDA 第 230 條(e)所設立之排除規範：本法不妨礙聯邦層級之刑事法規、著作權法規、州法、包括 1986 年《電子通訊隱私法》(Electronic Communications Privacy Act) 在內之通訊隱私法規、以及以性剝削為目的之人口販運 (sex trafficking) 相關法規之適用。

## (4) 司法實務對於免責範圍之見解

自從 CDA 第 230 條在 1996 年立法通過後，網路中介者應適用的具體免責界線便屢屢受到廣泛的討論與挑戰。舉例而言，在 1997 年的 *Zeran v American Online* 一案中，初審法院便認定，CDA 第 230 條

---

system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

不只免除了網路平臺作為「出版人」之責任，亦同時免除其「散布者」之責<sup>389</sup>，聯邦第四巡迴上訴法院亦維持其判決<sup>390</sup>，使本案正式推翻先前 *Stratton Oakmont v Prodigy Service* 的見解，為網路言論的責任判斷立下了新的標竿。然而另一方面，針對網路中介者是否應依被害人請求而主動移除相關侵權內容的爭點，*Zeran* 案雖指出網路中介者可自行決定之，但在 2003 年的 *Doe v GTE* 案中，聯邦第七巡迴上訴法院卻採取了不同的見解<sup>391</sup>，認為當網路中介者未採行任何限制或移除的措施時，縱其符合 CDA 第 230 條所規範之主體定義，被害人仍得就網路中介者散布第三人侵權言論之行為向其請求賠償<sup>392</sup>。

在歷來涉及 CDA 第 230 條的指標性案件中，2012 年的 *Force v Facebook* 案<sup>393</sup>除了係以新興社群平臺為被告，更論及平臺使用演算法篩選、排序之手段是否將影響其身分判斷與安全港適用的議題，法院在判決中採取的立場值得注意。

本案原告為哈瑪斯(Hamas)襲擊以色列時的多名受害者及家屬，其指控 Facebook 未能取締其平臺上的恐怖分子帳號，亦無法有效防堵恐怖主義的宣傳內容，成為恐怖分子的幫兇，此舉已違反美國《反恐法》(Anti-Terrorism Act)之規定，應為恐怖分子在社群平臺上的宣傳內容負責。有鑑於過往判決中，互動式電腦服務提供者經常援引 CDA 第 230 條主張免責，本案原告遂採取不同主張，未強調 Facebook

---

<sup>389</sup> *Zeran v. America Online, Inc.*, 958 F.Supp. 1124 (E.D. Va. 1997).

<sup>390</sup> *Kenneth M. Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997).

<sup>391</sup> *Doe v. GTE, Corp.*, 347 F.3d 655 (7th Cir. 2003).

<sup>392</sup> 郭戎晉，網路言論傳播中介者責任與其免責規範之研究—以美國通訊端正法實務發展為中心，科技法律透析，第 23 卷第 4 期，頁 42 (2011)。

<sup>393</sup> *Force v. Facebook, Inc.*, No. 18-397 (2d Cir 2019).

管理平臺內容的責任，而是著眼於 Facebook 的推播及媒合服務（“networking” and “brokering” links and communications），認為這項功能係依據個人資料的數據分析，將特定內容推播給其他喜好相似之用戶，這種基於演算法的自動化媒合功能應使 Facebook 被視為內容的「創造者」（developer）。換言之，原告主張，平臺上恐怖分子交流及散布的內容，應被視為 Facebook「自己」發表的內容，而非「第三方」資訊內容提供者之內容，平臺應就此負責。

然而按一審判決，Facebook 所使用的演算法僅為一種中立的工具，且 Facebook 本身也受到其使用者政策的束縛，針對何人可使用平臺、可在平臺發表什麼言論，Facebook 並不具有自行決策的空間，是故按 CDA 第 230 條規定，Facebook 不必為平臺上第三方的言論負責。上訴法院亦同意 Facebook 使用演算法來顯示及媒合用戶提供的內容，屬於 CDA 第 230 條所欲保護之態樣，因此視為「非出版人」，全然不必為第三方資訊服務提供者的內容負責，原告因此敗訴。

## 2. 新時代下對網路中介者作為的新期待

由於 CDA 第 230 條的免責規範係訂於網際網路發展之初，旨在鼓勵美國的網路中介者主動維護良好網路空間、避免法律的約束阻礙產業新創，但其簡短的條文設計卻使得司法實務往往傾向擴張解釋，導致網路中介者的免責判斷越趨寬鬆。加上當前的社會已邁入網路服務高度普及化的時代，社群平臺成為人們重要的言論發表與討論空間，若繼續維持過往放任私人企業自主管理網路言論、缺乏問責機制的模式，恐將導致私人企業恣意決定言論審查之標準，影響民主實踐。是故，近年來也有越來越多針對網路中介者免責條款的呼籲與修法倡議

興起，冀望在新時代的科技環境下重新審視社會對於網路中介者的作為期待，審慎評估 CDA 第 230 條可能的修正方向。

### (1) 政府作為

為了保障言論自由，防止 Twitter、Facebook、Instagram 及 YouTube 等科技公司濫用內容審查權限，影響大眾對於公共事件的解釋，美國總統川普（Donald Trump）在 2020 年 5 月 28 日簽署了「防止網路審查行政命令」（Executive Order on Preventing Online Censorship）<sup>394</sup>，欲以此防止社群平臺基於偏頗的政治立場選擇性地刪除言論。

根據「防止網路審查行政命令」，若社群平臺直接編輯或修改使用者貼文內容，將被排適用 CDA 第 230 條的免責保護；若平臺不公平地封鎖或刪除使用者貼文，聯邦通訊委員會（Federal Communications Commission, FCC）則有權立案審查，釐清平臺是否存在與其服務條款相背的行為與動機，或是未提供使用者合理解釋說明等狀況。必要時，FCC 可決定平臺能否受到 CDA 第 230 條的免責保護。除此之外，該命令也要求檢視政府投放的廣告是否遭到社群平臺不當限制；FTC 應密切注意社群平臺是否有任何不公平、詐欺，或反競爭且影響商業運作之行為，必要時可課與其法令遵循義務；白宮也必須建立投訴管道，以便民眾檢舉與平臺有關的偏見及不當對待。

雖然「防止網路審查行政命令」針對當前具有莫大言論影響力的社群平臺進行問責，並責成政府介入監管，但外界普遍認定此一命令

---

<sup>394</sup> The White House, Executive Order on Preventing Online Censorship (May 28, 2020), available at <https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/> (last visited May. 22, 2021).

的制定係肇因於川普個人與 Twitter 之間的糾紛。由於 Twitter 在同年 5 月 26 日曾基於事實查核機制將川普發布的兩則推文內容標註警語，並附上與其言論相左的報導連結供讀者參考，故輿論多將川普事後簽署「防止網路審查行政命令」的舉動視為一種報復性的措施<sup>395</sup>。除此之外，該行政命令本身亦有違反憲法的爭議，故民權團體「民主與科技中心」(The Center for Democracy & Technology) 已於同年 6 月 2 日向法院提起訴訟，主張其違反憲法第一增修條文之禁止政府干預言論自由<sup>396</sup>。

但另一方面，「防止網路審查行政命令」的頒布也再度讓社群平臺問責的議題受到高度的討論與關注，美國司法部遂於同年 6 月針對 CDA 第 230 條的施行狀況提出檢討與建議。司法部在報告中指出，基於時空環境的重大改變，當前多數的網路平臺已成為大型科技公司，不再是過往需要受到高度保障的小型新創事業，故 CDA 第 230 條賦予網路中介者的免責有立法修正之必要，應在制度上提供更加有力的鼓勵措施，敦促網路中介者處理其服務上的不法內容，並促進創新與言論自由<sup>397</sup>。

司法部的建議方向包括：

- 鑑於司法實務對 CDA 第 230 條多採擴大解釋，實有必

---

<sup>395</sup> BBC, *Trump Signs Executive Order Targeting Twitter After Fact-Checking Row*, BBC NEWS (2020/05/29), available at <https://www.bbc.com/news/technology-52843986> (last visited May. 25, 2021).

<sup>396</sup> Geneva Internet Platform, *Trump's Executive Order Challenged In Court*, GIP Digital Watch (2020/06/02), available at <https://dig.watch/updates/trumps-executive-order-challenged-court> (last visited May. 26, 2021).

<sup>397</sup> U.S. DEPARTMENT OF JUSTICE, *Section 230-Nurturing Innovation or Fostering Unaccountability?* (June 2020), available at <https://www.justice.gov/file/1286331/download> (last visited May. 26, 2021).

要修法限縮範圍。在構成要件的設計上，惡意進行非法活動之網路中介者、以及刻意忽視非法活動之網路中介者應屬於排除免責之態樣。條文也宜明文規定網路中介者取下法院判決違法之內容，並增設非法內容之標註機制。

➤ 恐怖主義、兒童性虐待、人口走私、網路跟蹤等重大權益侵害之處理應優先於 CDA 第 230 條，此類案件宜排除網路中介者之免責，使其盡相關義務與責任。另外，若網路中介者實質知悉 (actual knowledge) 不法情事卻未採取任何行動，該侵權事件也不宜賦予網路中介者免責權，但對於誹謗等相類之言論侵權應列為例外，以免網路中介者陷入責任困境。

➤ 網路中介者不應豁免來自聯邦政府的刑事或民事執行。

➤ 網路中介者刪除、編輯內容、或對使用者進行任何限制時，應符合其服務條款，亦應向使用者提出合理的解釋。司法部並建議將服務條款的揭露與遵循程度列入 CDA 第 230 條的「善意」要件；且為了進行監督，宜課與大型網路平臺提交透明度報告之義務，揭露其移除有害內容之數據，以評估其是否有差別待遇等。

## (2) 各界立法倡議

隨著「防止網路審查行政命令」與司法部發布的檢討建議成為討論焦點，其他政府機關與參、眾兩院也開始就 CDA 第 230 條未來的走向展開熱烈的討論及公眾諮詢，意圖透過法制架構的調整維護自由且健全的網路言論環境。各界意見整理如下：

## A. NTIA 之法規制定請願書

2020 年 7 月 27 日，美國商務部下轄之「國家電信暨資訊管理局」（National Telecommunications and Information Administration, NTIA）提出了「NTIA 法規制定請願書」（Petition for Rulemaking of the National Telecommunications and Information Administration），建請 FCC 明確界定 CDA 第 230 條之規範<sup>398</sup>。NTIA 在請願書中建議之內包括：

- 按法制架構，FCC 對於 CDA 第 230 條具有管轄權，應負主管機關之責任，賦予該條文正確的解釋或修法。
- FCC 應重新導正 CDA 第 230 條之解釋正確性。首先，第 230 條(c)(1)賦予網路中介者的免責之範圍並不包括網路中介者自己之言論，若網路中介者在推播或顯示內容的過程中添加自己的決定或評論，或是進行言論限制及移除使用者帳號之決定，將構成網路中介者自身之言論，需承擔出版人或發表人之責。其次，CDA 第 230 條(c)(2)所規範的免責要件過於模糊，諸如「其他令人不快的內容」、「善意」等，皆需由 FCC 明確定義之。
- 據 *Fair Housing Council v Roomates.com* 一案的法院見解，網路中介者若超出被動傳輸資訊之範圍，對違法行為產生實質貢獻，亦須承擔責任。因此，建議明文將「對他人言論附加修改、變更、加入不同比較觀點、評論或編輯者」視為「資訊服務提供

---

<sup>398</sup> NTIA, *NITA Petition For Rulemaking To Clarify Provisions Of Section 230 Of The Communications Act* (May. 27, 2021), available at <https://www.ntia.gov/fcc-filing/2020/ntia-petition-rulemaking-clarify-provisions-section-230-communications-act> (last visited Oct. 26, 2020).

者」，必須為言論內容承擔責任。

➤ 建議立法要求提供市場零售服務之網路中介者，應公開揭露其內容管理機制，以及對內容審核、促銷及顯示之政策，藉此保護消費者。

NTIA 的法規制定請願書也吸引了消費者科技協會（Consumer Technology Association, CTA）<sup>399</sup>、新創科技社群 Engine<sup>400</sup>、法制政策智庫 Tech Freedom<sup>401</sup> 等相關團體的公開回應。其中，三者在各自的回應中皆指出：美國的網路生態仍是由數以千計的小型或新創公司所組成，其需仰賴 CDA 的免責保護，才能避免涉入龐大的訴訟案件。CDA 不單是網際網路發展初期協助創新的工具，更是整個網路生態運作的基石，若只關注大型科技公司的發展恐會對現狀產生錯誤的評估；Tech Freedom 更強調，一旦 CDA 第 230 條遭到廢止，小型的網路中介者將因訴訟資源有限而容易被擊垮，導致掌握專業人才、擁有較完整法遵能力的大型網路中介者獲得優勢，反而不利市場競爭。除此之外，川普總統要求介入指導網路中介者對網路內容的管理，相當於政府間接進行言論審查，恐違反憲法保障言論自由的精神。

---

<sup>399</sup> Comments of Consumer Technology Association (Sep. 02, 2020), available at <https://www.wiley.law/assets/html/documents/Comments%20of%20CTA%20RM-11862.pdf> (last visited May. 26, 2021).

<sup>400</sup> In the matter of the National Telecommunications & Information Administration's Petition to Clarify Provisions of Section 230 of the Communications Act of 1934, as Amended, Comment of Engine, RM No. 11862 (Sep. 02, 2020), available at <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5f500e261e00bf5988ac1ee8/1599082023193/Engine+comments+RM-11862.pdf> (last visited May. 26, 2020).

<sup>401</sup> TECHFREEDOM, *NTIA's FCC Petition to Reinterpret Section 230 Is a Constitutional Non-Starter* (2020/07/27), available at <https://techfreedom.org/ntias-fcc-petition-to-reinterpret-section-230-is-a-constitutional-non-starter/> (last visited May. 26, 2021).

## B. FCC 之公眾諮詢

在 NTIA 提出請願書後，FCC 主席 Ajit Pai 於同年 8 月 3 日公開表示將邀請公眾就 CDA 第 230 條的調整方向自由表達意見，以利綜合評估<sup>402</sup>。截至同年 9 月 21 日為止，FCC 的公共平臺總計收到了至少 19,689 份多以個人名義提交之意見回復<sup>403</sup>。其中，多數回應肯定 CDA 第 230 條創造網路空間的言論自由，並表達對川普總統「防止網路審查行政命令」之不滿，希望 FCC 不會屈於政治壓力而變更既有規範。

## C. 近期之立法倡議

隨著社群平臺的問責成為各界討論的焦點，CDA 第 230 條的存廢議題不只成為美國 2020 年總統大選期間的政見指標之一，也在參、眾兩院醞釀出數量相當可觀的修法提案。惟共和黨及民主黨陣營對於 CDA 第 230 條及網路平臺責任之討論方向意見紛陳，整體呈現出百家爭鳴的膠著狀態。

在共和黨部分，除了前述由總統川普公布之「防止網路審查行政命令」外，參議員 Marco Rubio 也公開表達了對 CDA 第 230 條改革的支持。Rubio 認為，當 Twitter 等科技公司決定扮演近似出版人的「編輯」角色、對貼文加註查核時，即不該繼續享有安全港的免責保

---

<sup>402</sup> FCC, *Chairman Pai On Seeking Public Comment On NTIA's Sec. 230 Petition* (Aug. 03, 2020), available at <https://www.fcc.gov/document/chairman-pai-seeking-public-comment-ntias-sec-230-petition> (last visited May. 26, 2021).

<sup>403</sup> Docket RM-11862 Section 230 of the Communications Act of 1934 (Jul. 29, 2020), available at [https://www.fcc.gov/ecfs/search/filings?proceedings\\_name=RM-11862&sort=date\\_disseminated,DESC](https://www.fcc.gov/ecfs/search/filings?proceedings_name=RM-11862&sort=date_disseminated,DESC) (last visited May. 26, 2021).

護，應該同樣受出版相關法律的約束<sup>404</sup>；Rubio 並與 Kelly Loeffler、Kevin Cramer、Josh Hawley 三位同黨議員於 2020 年 6 月 9 日聯名向 FCC 主席 Ajit Pai 發表公開信，呼籲參考總統的行政命令，重新思考網路中介者免責保護之合宜性<sup>405</sup>。

民主黨方面，新任總統拜登（Joe Biden）曾在競選期間表示應全面廢除 CDA 第 230 條，讓科技公司及社群平臺經營者為網路上的內容亂象承擔責任<sup>406</sup>。而隨著政權在拜登勝選後交替，除了新任商務部長 Gina Raimondo 公開表示支持網路平臺問責，將持續推動 CDA 第 230 條的修法工作外<sup>407</sup>，白宮近來也延攬反網路壟斷立場鮮明的台裔學者吳修銘加入國家經濟委員會，擔任總統的科技與競爭政策特別助理，似可窺見行政部門對此議題所持的立場。

立法部門方面，目前眾議院較受矚目的法案為共和黨眾議員 Ted Budd 提出的《將 230 條免責對象限縮於善良撒馬利亞人》草案（Limiting Section 230 Immunity to Good Samaritans Act）。該草案主張保留 CDA 第 230(c)(2)的民事免責條款，同時為(c)(1)的適用主體增列但書，要求內容提供者（edge provider）必須制定並遵守符合本法要求之明文服務條款，包括：明列與限制內容接取有關之政策供使用者

---

<sup>404</sup> 怪獸對決：川普與社群網路龍頭們的「通訊端正法」戰爭？，轉角國際 udn Global，2020 年 5 月 29 日，[https://global.udn.com/global\\_vision/story/8662/4599574](https://global.udn.com/global_vision/story/8662/4599574)（最後瀏覽日：2021 年 5 月 26 日）。

<sup>405</sup> 詳見：<https://www.rubio.senate.gov/public/cache/files/c204fc9b-360e-4846-9db7-c9eba0600b18/F8EDFBD5B590665E44E91E240D1F473C.20.06.09--fcc-pai-230-letter-signatures.pdf>（最後瀏覽日：2021 年 5 月 26 日）。

<sup>406</sup> Casey Newton, *Everything You Need To Know About Section 230*, THE VERGE (2020/05/28), available at <https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation> (last visited May. 26, 2020).

<sup>407</sup> Makena Kelly, *Biden'S Commerce Nominee Backs Changes To Section 230*, THE VERGE(2021/1/26), available at <https://www.theverge.com/2021/1/26/22250746/biden-gina-raimondo-commerce-secretary-section-230> (last visited May. 26, 2020).

知悉、承諾將秉持善意營運……等，才可適用本條規定。該草案也預計修正第 230 條(f)之名詞定義，將前述的「內容提供者」定為境內或全球使用者超過 3,000 萬、年度全球營收達 15 億美元之互動式電腦服務提供者<sup>408</sup>。

除此之外，尚有共和黨眾議員 Louie Gohmert Jr.提出、主張將 CDA 第 230 條完全廢止之《終止網路審查法》(Abandoning Online Censorship Act)草案<sup>409</sup>，以及共和黨眾議員 Jim Banks<sup>410</sup>、民主黨眾議員 Tom Malinowski<sup>411</sup>等人所提出，文本仍有待公佈之諸多提案，皆是本研究後續將持續追蹤研究之對象。

## (二) FTC 就平臺隱私之問責

FTC 為美國線上隱私的最高主管機關，然而其執法卻極為慎重保守，大多數場合，僅針對涉及隱私脈絡的不實廣告方向為之。要之，FTC 仍是以「消費者保護」之原則進行線上隱私之相關執法，且相當程度採取自由市場之「合理選擇理論」，也即廠商之服務所有優劣，而消費者能在其中進行選擇。基此，FTC 的執法著重於資訊公開，也即，在資訊公開的基礎上，推定業者與消費者在使用約款與隱私政策上具有合意<sup>412</sup>。

---

<sup>408</sup> H.R. 277: Limiting Section 230 Immunity to Good Samaritans Act, *available at* <https://www.govtrack.us/congress/bills/117/hr277/text> (last visited May. 1, 2020).

<sup>409</sup> H.R. 874: AOC Act, <https://www.govtrack.us/congress/bills/117/hr874/text> (last visited May. 1, 2020).

<sup>410</sup> H.R. 2000: Stop Shielding Culpable Platforms Act, *available at* <https://www.govtrack.us/congress/bills/117/hr2000/text> (last visited May. 1, 2020).

<sup>411</sup> H.R. 2154: Protecting Americans from Dangerous Algorithms Act, *available at* <https://www.govtrack.us/congress/bills/117/hr2154/text> (last visited May. 1, 2020).

<sup>412</sup> クリス・フーフナグル (Chris Jay Hoofnagle) 著，宮下紘、板倉陽一郎、河井理穂子、國見真理子、成原慧、前田恵美譯，アメリカプライバシー法：連邦取引委員会の法と政策，頁

然而，美國公民社會與消費者團體對此則多所批評，認為隱私問題已非單純的消費者自由選擇問題。因此 FTC 亦於 2012 年以「安全、隱私始於設計」(private by design, PBD) 之概念為核心，公布「快速變動時代下的消費隱私保護：給企業與政府決策者的建議」報告 (Protecting Consumer Privacy in An Era of Rapid Change: Recommendations for Business and Policymakers<sup>413</sup>)，認為基於企業就資料安全以及資料蒐集的合理限制，其實質隱私保護，應包括妥善保存、刪除及確保資料之正確性，並將之歸納為執法規範之一部；同時提醒企業與政府應意識數位時代下消費隱私保護可能帶來的衝擊，並提出解決方案。其中，以買賣、編輯整理和販售與個人高度相關的資料作為產品與服務之業者，為 FTC 特別關注的產業之一<sup>414</sup>，而 Facebook、Google 等數位平臺所營利的資料經銷轉售與平臺仲介模式，則為主要關切的對象<sup>415</sup>。

### 三、美國法制政策之啟示

綜上所述，相較於極度重視個人資料隱私保護、消費者權益與數位平臺問責的歐盟，美國作為政治、經濟領域上享有輸出優勢的世界強權，不只在傳統上缺乏聯邦層級之個人資料保護與資料流通架構，對於數位經濟市場亦採取寬鬆、放任的規管態度；加上 CDA 第 230

---

71-72，勁草書房（2018）。

<sup>413</sup> See generally FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS (2012), <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

<sup>414</sup> 許慧瑩、葉志良，資料經濟趨勢下美國對於資料仲介業規制之研究，科技法學評論，13 卷 2 期，頁 112（2016）。

<sup>415</sup> フーナナグル。前掲註 412，頁 61-71。

條為數位平臺就第三人發表言論的責任提供了極大的保障，這些因素都在在賦予了新創產業極大的優勢，使得 Google、Apple、Facebook、Amazon 等企業得以誕生，並成為主宰全球數位市場的科技巨頭。

但隨著優勢數位平臺危害市場競爭、致生消費者權益損害的問題日益嚴重，各界對於反托拉斯法強勢介入、增強平臺問責的呼籲也為美國政府的監管態度帶來了新的改變。繼 2020 年眾議院反托拉斯小組發布「數位市場競爭調查」報告後，DOJ、FTC 等主責機關開始對企業巨頭的反競爭行為採取積極的司法行動；CDA 第 230 條的固有問題更是隨著 2020 年總統大選期間川普與 Twitter 之間的糾紛再次成為各界關注的話題，促成了百家爭鳴的立法倡議。而隨著政權交替，總統拜登在 FTC 主席、科技與競爭政策特別助理等人事的任命上表現出強烈的立場，甚至簽署「促進美國經濟競爭」行政命令、敦促行政機關積極落實反托拉斯法，當前美國對數位平臺監理之立場明顯已進入關鍵的政策轉變期，其未來之發展值得持續關注。

## 伍、結論與建議

### 一、各國管制歸納

表 3：各國管制歸納

		歐盟	英國	美國	我國
市場競爭	現行法規範	歐盟運作條約中之一般競爭法	競爭法、2002 年企業法等競爭法體系	休曼法、克雷頓法等反托拉斯法體系	公平交易法
	當前困境	<ul style="list-style-type: none"> <li>● 殺手級併購及跨產業獨占</li> <li>● 守門人數位平臺不見得構成顯著市場力量</li> </ul>	<ul style="list-style-type: none"> <li>● 殺手級併購及跨產業獨占</li> <li>● 競爭法主管機關 CMA 專業能力與行政執行能量不足</li> </ul>	<ul style="list-style-type: none"> <li>● 殺手級併購及跨產業獨占</li> <li>● 仰賴理論及大量司法判決形成見解，但實務上卻造成執法機關執法限制</li> </ul>	欠缺數位平臺精確之調查與實證研究
	改革方向	<ul style="list-style-type: none"> <li>● 2019 年制定線上中介服務規章</li> <li>● 2020 年提出數位市場法草案</li> </ul>	<ul style="list-style-type: none"> <li>● CMA 內成立數位市場部門 (DMU)</li> <li>● 擬立法授予權限</li> </ul>	<ul style="list-style-type: none"> <li>● 總統發布促進美國經濟競爭命令</li> <li>● 倡議立法，排除不合理之法律及司法判例</li> <li>● 透過訴訟強化執法</li> </ul>	<ul style="list-style-type: none"> <li>● 成立數位發展部</li> <li>● 公平會成立數位平臺產業調查小組</li> </ul>
	擬主管機關	歐盟執委會	新設 DMU (CMA 數位市場部門)	維持 FTC/DOJ	新設之數發部擬不涉管制，組織法草案分工尚未定案
	擬規管對象	<ul style="list-style-type: none"> <li>● 線上中介服務 (P2B 業者)</li> <li>● 核心平臺服務：線上中介服務、線上搜尋引擎、社群媒體、視訊分享平臺、非基於號碼之人際通訊服務、操作系統、雲端服務、核心平臺廣告服務</li> </ul>	戰略市場地位 (SMS) 企業	GAFAM 科技巨擘	未明 (僅及於數位平臺)
	擬規管措施	<ul style="list-style-type: none"> <li>● 類似公用事業管制</li> <li>● 非歧視、中立及</li> </ul>	<ul style="list-style-type: none"> <li>● 資料干預：消費者控制、資料接取、資料孤島矯</li> </ul>	<ul style="list-style-type: none"> <li>● 修法調整反拖司損害及當事人適格性</li> </ul>	未明

		透明性、市場力控制	正 ● 互通與共同標準 ● 消費者選擇權利與預設干預 ● 公平合理無歧視 ● 結構拆分	● 結構性拆分 ● 禁止歧視 ● 互通性與開放接取 ● 結合審查運用推定 ● 禁止濫用優勢地位並要求正當程序	
平臺問責	現行法規範	電子商務指令	2002 年電子商務管制法、2017 年數位經濟法(線上色情內容)	CDA 230	無(僅著作權法設有責任安全港)
	當前困境	● 已 20 年未調整規範，無法對應當前環境 ● 線上平臺多行自律，欠缺問責及監督	● 線上違法或有害內容層出不窮 ● 發展與歐盟不同之策略	● 規範過於寬鬆 ● 仰賴司法形成標準 ● 平臺多行自律，欠缺問責及監督	● 欠缺網際網路內容基礎規範 ● 數位平臺違法內容激增與對言論之限制等問題已大量出現
	改革方向	2020 年提出數位服務法草案	2021 年提出線上安全法草案	立修法倡議百家爭鳴	草擬數位通訊傳播服務法草案
	擬主管機關	● 歐盟執委會(歐盟層級執法) ● 新設數位服務協調官(會員國執法) ● 新設歐洲數位服務委員會(協調)	● 部會：DCMS 及主管內閣大臣 ● 監理機關：Ofcom	擬維持 FCC	NCC
	擬規管對象	網路中介者：連線服務、快取服務、資訊儲存服務、線上平臺、非常大型線上平臺	● 使用者對使用者(U2U)服務 ● 搜尋服務	或調整互動式電腦服務之定義	尚未確定(數位平臺)
	擬規管措施	● 鼓勵自願性執法採累加義務： ● 透明度報告、揭露重要參數及管制透明 ● 建立內部異議及訴外爭端解決機制 ● 風險評估報告及	針對違法內容及有害兒童內容、有害成人內容 ● 登記制 ● 透明性報告 ● 風險評估 ● 降階措施等 ● 確保民主辯論及新聞自由	或調整互動式電腦服務之免責範圍、或課予其義務	參考歐盟數位服務法草案模式

		外部稽核	<ul style="list-style-type: none"> <li>● 服務限制令</li> <li>● 限制接取令</li> </ul>		
--	--	------	--	--	--

資料來源：本計畫製作

### （一）各國思維取向

隨著數位經濟快速發展，數位平臺與人們的日常生活逐漸形成密不可分的關係，全球先進國家不只開始意識到數位平臺背後隱藏的風險，相應的監理思維也在多方討論中逐漸清晰。

觀諸近年來國際社會之討論，資料市場之競爭、資料運用之行為，以及平臺問責之架構設計皆係和數位平臺管制息息相關之核心議題。其中，歐盟為了因應跨境數位平臺對境內市場帶來的衝擊，除了積極調和既有規範，致力建構歐洲數位單一經濟市場之公平、有效競爭及隱私保護環境，更於 2020 年 12 月提出《數位市場法》草案及累加義務模式的《數位服務法》草案，以較為積極、事先干預的態度監理數位平臺；英國政府則計畫成立專責之數位市場部門，針對具戰略市場地位之數位平臺業者訂定對應之監理機制，並擬定《線上安全法》草案，賦予監理機構相應之執法權力。

相較之下，美國作為政治、經濟上享有輸出優勢的世界強權，不只缺乏聯邦層級之個人資料保護與資料流通架構，對於數位經濟市場向來亦採取寬鬆、放任的規管態度。但隨著優勢平臺危害市場競爭的弊病日益嚴重，各界對於反托拉斯法介入、增強平臺問責的呼籲也為美國政府的監管態度帶來了新的轉變，無論是眾議院反托拉斯小組之「數位市場競爭調查」報告，DOJ、FTC 等主責機關開始對企業巨頭的反競爭行為採取積極的司法行動、甚或是新任總統拜登近期簽署的

行政命令皆可見一斑。

儘管各國政經背景與法律文化有別，歐盟、英國、美國三地之監理思維仍有趨同之傾向。究其原因，乃各國政府已確切意識到大型跨境數位平臺對市場競爭、消費者權益所帶來之潛在危害。作為借鏡，我國亦應積極就隱私保護、線上違法內容處理及數位服務市場競爭等面向進行法制整備、促進平臺問責，使數位經濟之發展兼顧人權保障。

## （二）各國數位平臺市場競爭分析

細言之，在數位平臺之市場競爭方面，由於涉及跨國大型平臺於多年策略下、且多角化經營脈絡下的經濟性管制，各國的競爭法皆不免捉襟見肘。因此除美國致力於調整現有反托拉斯法的侷限，歐英的一致改革方向，大抵皆為於一般競爭法外，另定可以降低競爭法主管機關證明責任，且授權明確矯正措施之類產業部門法規範。

例如歐盟的「線上中介服務規章-數位市場法草案」體制，即獨立於一般競爭法外，建立類似於公用事業及公共載具之管制模式，課予「抓大放小」的義務。尤其在數位市場法草案中，以「具備強大的經濟地位」、「具有強大的中介能力，可使企業觸及大量使用者」、「目前或未來可擁有長久且穩固不變的市場地位」為原則標準；例外考量含營業額、市值、企業藉由平臺服務接觸到終端用戶數量、基於網路效應及數據驅動之優勢所導致之參進障礙、自規模與範疇經濟中之獲益、企業用戶或終端用戶套牢、其他市場結構性之特徵等因素，加以認定核心平臺服務提供者。加諸英國擬新設「具戰略市場地位業者」之標準，為考量企業大小或規模、該企業商業行為是否為連結消費者之重要通路、企業行為是否使企業擴張或保護其市場力、企業是否

可以透過制定其產品或服務生態系之運作規則，影響更大範圍之市場參與者、產品或服務是否更廣泛影響社會與文化，顯見此兩種標準已與傳統競爭法相異其趣。

在手段上，歐盟、英國及美國則是共同地朝向產業規管邁進，也即課予事前（*ex ante*）的一般性義務，而非單純採取傳統競爭法的事後管制策略。要之，此類手段大抵可分為「非歧視原則型」、「平臺中立之透明性型」及「防止市場力過大型」三種。「非歧視原則型」大抵包括禁止獨家交易、差別待遇、搭售等傳統公平合理無歧視（FRND）的管制原則，此部分與一般競爭法有原理上的親和性。「平臺中立之透明性型」則包括允許第三方之 App、程式商店及作業系統 OS 等互通性、服務使用條款及廣告價格透明性、資料可攜、資料平等接取，大抵將數位平臺改造成一具有「中立性」（*neutrality*）的事業，以提供其他競爭者或鄰接市場參與者公平接取其服務與所取得之資料。最後，在「防止市場力過大型」上，則包括新型態的結合控制方法（如美國冀希透過單一市場力推定禁止垂直整合）、結構拆分、個資防火牆、禁止使用競爭者資料與之競爭、禁止不得爭訟約款等，一方面防止線上平臺之規模與優勢持續擴張，同時也防制其透過獨占性或寡占性服務進行榨取性濫用，對個人或企業使用者獲取不當之利益。

### （三）各國數位平臺問責分析

而在數位平臺之問責方面，各國主要關切者為線上平臺對於違法內容的處置。線上違法內容之管制並非新興議題，但過往於 Web 1.0 時代，由於頻寬及網站數量有限，各國可以透過「資訊源」也即散布違法內容之行為人加以處罰、或查扣其伺服器。而在 Web 2.0 時代，

隨頻寬提升，互動式服務紛紛出現，執法手段已難以透過逐一清查行為人的方式，而該類的互動式服務也並非違法內容的「直接提供者」，因此各國開始轉向針對有效的網路「控制點」(control point) 著手，從民事責任上論以共同責任、或是立法要求其負擔一定的違法內容取締責任(尤其針對著作侵權)；但更大程度地，是鼓勵其進行有效的自律，將違法內容移除。但到了 Web 3.0 時代，巨量的資料和使用者全天候聯網，互動式平臺即便增自律，也無法對應爆炸性成長的內容了，因此便開始採用以演算法為基礎之過濾軟體及人工智慧等自動化機制辨識並移除違法內容，但同時也引發了不精準、平臺偏好等對於言論自由的戕害疑慮，故本研究所研究的歐盟、英國、美國近期的法制政策皆係針對平臺責任與自律失控所進行的反思與回應。

除了美國的法制改革方向仍在持續議論、迷惘之外，歐英已經相當明確未來的監理方向。首先，在規管對象上，其大抵皆針對特別容易引起社會傷害的數位平臺加以規管，歐盟雖然維持過往的網路中介者定義，但為了強化義務課予的精確性，增加了「線上平臺」與「大型線上平臺」之定義，課予「抓大放小」的義務形式；英國亦同樣，針對使用者對使用者(U2U)服務及搜尋服務，也課予了相應的義務，是為脫歐後第一個將與歐盟走向顯著差異化的通訊傳播法制草案。

其次，在課予義務上，可以發現每年提出透明性報告，以及針對整體服務有關違法內容之傳散或受資訊操縱的可能性的風險評估，已經是全球共通標準的管制措施；同時，為了確保移除或是下架內容免於打擊錯誤而戕害言論自由，也都課予相應業者提供內部異議、外部訴外爭端解決機制或越級申訴等機制。

不過，課予義務也即手段的選擇上，歐英還是有一些差異。其一，英國採取了所有受管制業者都應向主管機關登記的制度；歐盟則是僅要求業者向公眾揭露資訊。

其二，英國在其線上安全法草案中明定違法內容及有害內容之定義，關於違法內容也即規管密度最高者，雖然聚焦在恐怖主義、與兒童性剝削及暴力犯罪，但英國仍開闢一條授權主管機關評估並公告其他應適用該法犯罪類型之途徑，此將會影響法律明確性，可能會形成業者的立法遊說阻力，以及立法後的合憲性挑戰<sup>416</sup>。再者，針對有害兒少內容即管制密度中等者，及有害成人內容即管制密度最低者，則採取抽象的定義方式描述，同樣凸顯了不確定性。反之，歐盟採取最聰明的做法—由其他法律（包括歐盟法及內國法）另定違法內容。不過此舉雖然便宜，但所有民刑事、行政法上的違法內容都將納入定義，將會產生打擊範圍過廣的疑慮；尚且，違法內容對社會傷害的影響亦有程度之別，不加以分類而全部採用相同義務程序與措施，是否適宜，仍有值得斟酌之處。

其三，英國擬常時課予受管制業者採取降低違法內容觸達使用者的措施，如降階等，僅在罰鍰等手段無法擔保業者改正時，由主管機關先向法院聲請切斷金流或輔助服務之「服務限制令」，而當「服務限制令」亦無法達成目的時，主管機關始採取最後手段性之向法院聲請「接取限制令」，也即阻斷接取特定內容。而英國欲創設之「服務限制令」及「接取限制令」，早於 2017 年數位經濟法對處線上色情內容

---

<sup>416</sup> See e.g. Jack Fenwick, *Twitter says Online Safety Bill needs more clarity*, Oct. 23, 2021, BBC NEWS SERVICES, <https://www.bbc.com/news/uk-politics-59010723> (last visited Nov. 1, 2021).

之規範中，即有相似的手段，此次草案本即整合此相關規定，有其脈絡背景。而歐盟則將「資訊阻斷令」全部委由各會員國規範，並未限制任何要件；僅是於草案中明定其效力擴及所有「具有關連」之聯繫因素個案，因此業者應遵守之範圍亦相應擴張。

最後，英國擬針對確保民主辯論及新聞自由之內容，要求業者應訂定特別之服務使用條款，是其針對新聞做為特定內容所設之獨特規範。

## 二、我國法制政策建言

反觀我國，無論在數位平臺之市場競爭或違法內容等之問責上，都顯著落後於歐美英各國。

### （一）數位平臺市場競爭部分

#### 1. 監理機關

首先在數位平臺之市場競爭方面，目前我國目前尚欠缺數位平臺相關市場競爭問題之精確調查與實證研究，是當前最大的問題。雖然數位平臺之機制與運作原理，其商業模式及優勢，由於數位平臺的跨國性，使得各國主管機關這方面的研究與調查皆相去不遠；但對於數位平臺於一國內結合、差別待遇、甚或對消費者之榨取性濫用等實踐情形，卻是有所不同。因此，當務之急，應儘速就我國進行地毯式之本土調查，研析數位平臺之參進與擴張對相鄰產業鏈、甚或整體產業是否已然集中等影響。

然而，我國目前僅公平交易委員會（下簡稱「公平會」）成立任務

小組<sup>417</sup>，將針對數位平臺產業進行通盤調查<sup>418</sup>，此固然是好的開始；然公平會之調查取向可以想見，應是採取傳統競爭法理論或法規詮釋之思維，能否針對競爭法所無法應對之領域、甚至其他機關應採取的行動加以分析，不無疑問。

本研究對此深感焦慮，尤其，我國立法院近期聚焦審議數位發展部（下簡稱「數發部」）組織法草案，預計將成立數位產業的火車頭部會。但若細究於立法院聯席委員會所審查完竣之數發部組織法草案，涉及數位平臺產業之職權，僅第二條第一款規定該部將掌理「國家數位發展政策之規劃、協調、推動、審議與法規之擬訂及執行」，以及第四款「數位經濟相關產業之輔導、獎勵及管理」寥寥數語<sup>419</sup>。

另一方面，配合組改修正之國家通訊傳播委員會（下簡稱「通傳會」）組織法修正草案，於審查完竣之版本第三條，則於第一款規定其未來之執掌包括「通訊傳播監理及網際網路傳播政策之訂定、法令之訂定、擬訂、修正、廢止及執行」，其立法說明修正為：「網際網路服務快速發展下，建立多方利害關係人參與、自律、他律之機制；並協調各部會依其權責處理非法內容機制。」則顯然僅關注於非法內容領域，未提及數位平臺之市場競爭或經濟性管制層面<sup>420</sup>。

---

<sup>417</sup> 李雅雯、高嘉和，公平會立案前哨 數位平台產業調查啟動，自由時報，2021/07/02，<https://ec.ltn.com.tw/article/paper/1458194>（最終瀏覽日：2021/11/1）。

<sup>418</sup> 李雅雯，數位平台與新聞媒體議價 公平會：行政院跨部會討論中，2021/10/04，自由時報，<https://ec.ltn.com.tw/article/breakingnews/3692414>（最終瀏覽日：2021/11/1）。

<sup>419</sup> 立法院，審查會通過條文、行政院函請審議「數位發展部組織法草案」、委員劉世芳等 20 人擬具「數位發展部組織法草案」、委員吳怡玳等 17 人擬具「數位發展委員會組織法草案」、民眾黨黨團擬具「數位發展部組織法草案」、委員謝衣鳳等 16 人擬具「數位發展部組織法草案」條文對照表，[https://lis.ly.gov.tw/lygazettec/mtcdoc?DN100350:1104300795\\_0\\_1](https://lis.ly.gov.tw/lygazettec/mtcdoc?DN100350:1104300795_0_1)。

<sup>420</sup> 立法院，審查會通過條文、行政院函請審議「國家通訊傳播委員會組織法第三條、第九條及第十四條條文修正草案」、委員陳素月等 19 人擬具「國家通訊傳播委員會組織法第三條、第九

此處引起的第一個疑問是，網際網路傳播與數位發展、或數位經濟相關產業的關係；其次，才是數位平臺的市場競爭及經濟性管制權責誰屬的問題。本研究認為，確實數位平臺的市場競爭及經濟性管制，在各國都有競爭法主管機關之參與、甚至發起，但誠如英國所承認，傳統競爭法主管機關的專業與能量都有所不足，因此 CMA 內部也新設 DMU；而雖然歐盟數位市場法草案依然由歐盟執委會主管，但該法涉及諸多服務活動的常態性監管，就算不若 GDPR 新設全新的監管機構，執委會勢必亦將調整內部的事權劃分，甚至創設新內部部門。

基此，本研究建議，無論未來數位平臺的市場競爭及經濟性管制要由那個部會或獨立委員會主責，現行想像中的「數發部-通傳會-公平會」體制並無法適切回應產業與環境監理需求。也即，即便日後循美國方案，制定競爭法體系中的新法、並由競爭法主管機關執法，公平會當前的職能也必須進一步調整；更遑論是項工作要移撥、或由數發部以「數位經濟相關產業之...管理」從頭拾起承擔。甚至，不同機關間要採取更複雜、更擅所長的雙元或多元管制，諸如由數發部負責跨部會協調及管制決策，公平會專責競爭分析，而通傳會負責線上平臺產業特定議題的調查等<sup>421</sup>。

## 2. 規範主體與管制措施

至於具體規範主體與管制措施上，本研究認為仍有待公平會提出

---

條及第十四條條文修正草案」、委員許智傑等 18 人擬具「國家通訊傳播委員會組織法第十四條條文修正草案」、現行條文條文對照表，  
[https://lis.ly.gov.tw/lygazettec/mtdoc?DN100350:1104300793\\_0\\_1](https://lis.ly.gov.tw/lygazettec/mtdoc?DN100350:1104300793_0_1)。

<sup>421</sup> 廖正義，電信業結合管制之研究：以電信法與競爭法的雙元管制為中心，國立交通大學管理學院碩士在職專班科技法律組碩士論文，頁 32-35（2010）。

產業調查報告後，再行思考；尤其，歐英美各國目前也僅止於立修法倡議或提出草案的階段，相關要件仍不明確。

細究之，於規範主體的立法策略分析上，本研究認為歐英模式較為釜底抽薪而可參採。因其不管是歐盟模式的透過新設「線上中介服務」或「核心平臺服務」定義，抑或英國模式之新設「戰略市場地位」定義，雖然或多或少皆有運用競爭法之科學界定方法，但實則已將受管制事業視為公用事業或公共載具，其常態性的監理並課予諸多事前管制的一般性義務，說明此二模式本質已為「產業管制法」，已與傳統的競爭法大異其趣，則將事權交由專為此設計的產業監理機關主責，較為妥適；尚且，為配合常態性監理、以及諸多事前管制義務之行政能量，產業監理機關也比競爭法主管機關也更為適合<sup>422</sup>。

繼而，在監理手段的立法策略分析上，本研究接續歐英美三國之比較分析，認為干預密度從高至低可分類為「非歧視原則型」、「平臺中立之透明性型」及「防止市場力過大型」三種，雖然皆可為參考，但於規劃上，仍有兩點值得注意：其一，英美手段上兼採結構性拆分，此一處分的干預程度非常大，且結構性分離涉及到非常精密的產權切割作業，監管成本與誤判風險都非常高，需要極高的行政能量投入。其二，由於數位平臺的商業模式也涉及大量的資料蒐集、處理與利用，因此管制手段上也多有資料干預措施，如使用服務即開始蒐集資料時的限制手段、開放資料接取，以及互通與資料可攜制度之建立等，需要和個資或資料主責機關相互配合與共同執法。而由此觀之，也都間

---

<sup>422</sup> 廖賢洲，*Verizon v Trinko* 案看電信市場之管制與競爭，公平交易季刊，第 13 卷第 3 期，頁 165 (2005)。

接證立了現行公平會不適合做為主要監理機關，而應由數發部加以統籌的觀點。

## （二）各國數位平臺問責分析

在數位平臺有關違法內容等之平臺問責之建議上，前開通傳會組織法修正草案審查會版第三條中，除第一款載明「通訊傳播監理及網際網路傳播政策之訂定、法令之訂定、擬訂、修正、廢止及執行」外；尚有第五款「通訊傳播傳輸及網際網路內容分級制度及其他法律規定事項之規範」之設，則關於違法內容之監理應由通傳會主責，應無疑義。

則針對數位平臺的違法內容監理，本研究考察前開歐英美之法制政策取向後，提出以下建議：

### 1. 逐步調適我國法制因應

從已著手法制化的歐英比較觀之，歐盟立法模式的重點乃在於明確法制化數位平臺於「內容調控」(content moderation) 的應盡義務，也即，歐盟執委會至少在目前還不會介入數位平臺對於其所傳輸或儲存內容是否為違法內容之審查或判斷，僅要求要將其無論肯否決定之理由告知通知者、使用者、甚至公布於公開資料庫上供大眾及研究者檢視。

英國立法模式則是揉合了 2017 年數位經濟法的嘗試，將原本針對網路色情內容的管制統合進此次草案中，也即針對不同種類的違法內容，明確要求降階或建立法官保留的移除管道。

本研究建議此兩國的策略都值得參採，畢竟歐盟數位服務法草案是經濟聯盟的立法，重點在於調和各會員國的國內法，很大程度保留給各會員國內國法決定；但英國脫歐後，必須自行建立內國法之完整的制度與配套。

但無論是歐盟數位服務法草案、或英國線上安全法草案，其背後理路即所欲解決的問題雖相對明確，但皆為目前世界上針對線上違法內容進行全面性平臺問責法制化之區域，草案本身非常具實驗性質，我國應持續觀測其發展，而不是貿然引進。

尤其，本研究認為，規範跨國線上平臺之平臺問責制度，應參考歐盟或美國之大型經濟體之立法例，就最大限度進行「法規調和」或「管制對接」(regulatory alignment)，除不增加跨國大型平臺之法遵成本外，最重要者，則是促其遵守我國法規，以避免 2011 年台北市法規會依消費者保護法裁處 Google，而引發「Google Android Market」付費服務全面退出台灣之類似事件。

## 2. 應從網際網路基礎規範加以建立，並調和相關規範

相較於歐盟數位服務法草案做為調和性質之規章，我國目前除著作權法外，尚無一般違法內容之安全港機制，因此若要參考數位服務法草案，實為一「蛙跳」的大膽策略。

也即，歐盟數位服務法草案仍以電子商務指令及資訊社會服務 (information society service, ISS) 相關法制為基礎，我國早先版本的「電子通訊傳播法」或「數位通訊傳播法」兩草案其本質皆係欲建立網際網路基礎規範，卻未竟全功；今若將重點「數位通訊傳播服務法」

僅置於數位平臺，則恐怕有如重心不穩的高樓，在業者法遵上或主管機關的有權機關解釋上都可能寸步難行。故本研究建議今「數位通訊傳播服務法」以數位平臺為核心固然重要，但仍應相當程度揉合類似於電子商務指令（即英國於 2002 年內國法化之 2002 年電子商務管制法）之規定，以資整全。

再者，除美國原本即採一般違法內容與著作權法的安全港「分散式立法模式」外；英國的法制設計也採取比較複雜的體例，也即在責任安全港部分，英國仍然不區分違法內容種類，統一適用 2002 年電子商務管制法，但線上安全法草案所指之違法內容類型，則明確已將侵害智慧財產權犯罪排除，亦即主管機關無法將智慧財產相關犯罪之違法內容納入「優先違法內容」的範疇中。

基此，我國的立法也必須處理與著作權法的競合關係。考量降低業者法遵成本，本研究建議應採取歐盟式的一致化規範。

### 3.仿照英國建立永久禁制令制度，並強化政府透明治理

我國目前亦無獨立之永久禁制令之設，本研究建議可參採英國罰鍰、「服務限制令」及「接取限制令」三層式的逐級回應（graduated response）體系，也即若行政罰無法達成管制目的時，首先先向法院聲請阻斷金流或雲端等輔助服務的禁制令；仍無法達成管制目的時，最終手段再向法院聲請阻斷特定內容之禁制令。

於我國，具體而言，可參考家庭暴力防治法中家事保護令之規定，設計向法院聲請核發「資訊阻斷令」之立法模式；惟考量到往後相類案件可能會大增，本研究建議司法院也應於各地方法院增設「數位專

庭」，以資因應並加速審理。

此外，歐盟數位服務法草案第 8 條有關介接各會員國法院或行政機關移除或阻斷違法內容之命令規範，也值得參考。該規範之重點在於要求法院或行政機關必須於移除或阻斷之裁判書或處分書記載相關必要記載事項，包括必要性理由、救濟手段等，甚至亦必須公開於公眾可接取的資料庫，以資開放政府及透明治理理念。

#### 4. 違法內容定義除介接他法外，應加以分類

在「違法內容」之定義上，應採取歐盟數位服務法草案中未明定，而介接他法。

此外，也應積極參考英國線上安全法草案中對於違法內容「事實上」(*de facto*) 加以分級之做法。要之，最嚴重者為構成恐怖主義、兒少性剝削及暴力，及授權主管機關評估而公告的涉刑事犯罪內容；次者則是有害兒少內容，此亦算是放諸四海皆準的違法內容類型；最輕微者係有害成人內容，只要求受管制業者納入風險評估中而已。

此外，英國針對新聞內容也採取了較於優遇的保障策略，以促進民主辯論並確保新聞自由。

由此觀之，英國相較於歐盟，在違法內容的範圍內上，選擇了避免打擊過廣的策略；同時也積極性地保障了新聞自由，值得參考。

#### 5. 建立「普通-特別法」之法制架構

最後，以及課予義務的清單上，應採取歐盟數位服務法草案與其他規章及指令之「普通-特別法」兩層架構。也即數位通訊傳播服務法

草案，可做為「總則性法律」為最低度之共通規範；具有特殊考量性質者，則應明定於個別作用法，如《兒童及少年福利與權益保障法》第 46 條，有關有害兒少身心內容由目的事業主管機關通知網際網路平臺提供者，即須先行移除之規定，因不透過法院而較為簡易，可優先於「總則性法律」適用。

數位平臺之管制策略已是當前各國監理機關無法迴避之重要議題。相較於監理思維逐漸明朗化的世界主要國家，我國在數位時代所面臨的數位平臺競爭與資料利用議題，可說是處於相對弱勢的地位。面對科技巨頭挾其跨國市場影響力之壓境，即使我國之通訊傳播業者也不易抗衡，監理機關實有必要掌握現今主要國家之法制動態，思考我國在此領域應採取之治理思維。

本報告針對歐盟、英國、美國所進行之法制政策研析，盼能為我國監理機關後續之政策擬定提供相當之參考與指引。

## 陸、參考文獻

1. 王牧寰、徐偉群、陳志宇、鄭嘉逸、江耀國、陳人傑、簡陳中、楊東穎、胡家崎、楊儷綺、王艾雲、廖祥丞、田育志，因應數位通訊傳播服務發展之規管趨勢與法制革新研析，國家通訊傳播委員會委託之計畫成果報告(2021)。
2. 王牧寰，封鎖境外網站之研究—以英國網路中介者之「限制智財侵權特別責任」為例—，2016年資訊社會年會暨研討會(2016年11月)。
3. 吳彥容，簡評歐盟強化資料自由流通之新規則—以非個人資料之流通為中心，經貿法訊，第245期，頁19-22(2019)。
4. 林家暘，德國2021年限制競爭防制法數位化改革分析，臺灣法學雜誌，第412期，頁127-142(2021)。
5. 邱映曦，競爭法的數位紀元—論數位平臺資訊力對競爭法適用之影響，國立政治大學法律學系博士班博士學位論文(2019)。
6. 徐曼慈，德國聯邦卡特爾署決定禁止Facebook濫用市場力不當處理用戶資料之行為，公平交易委員會電子報，第122期，頁1-3(2019)。
7. 胡祖舜，競爭法之經濟分析，元照出版，2021。
8. 陳人傑，網際網路服務提供者免責規範單一立法模式之探討，智慧財產權月刊，第71期，頁54-81(2004)。
9. 陳志宇、巫國豪、余曜成、程致剛、楊東穎、廖祥丞，推動數位經濟發展之通訊傳播匯流政策及法制革新計畫—促進資料自由流通機制及應用趨勢研究計畫，國家通訊傳播委員會委託之計畫成果報告(2019)。
10. 陳志民，大數據與市場力濫用行為初探，公平交易季刊，第26卷第3期，頁1-33(2019)。
11. 陳志民，支付系統競爭議題及規範架構之建立，公平交易季刊，第27卷第3期，頁1-40(2019)。

12. 許祐寧，德國聯邦卡特爾局限制 Facebook 蒐集整併不同來源的用戶數據以防壟斷，科技法律透析，第 31 卷第 5 期，頁 2-4 (2019)。
13. 張陳弘、莊植寧，新時代之個人資料保護法制：歐盟 GDPR 與臺灣個人資料保護法的比較說明，新學林出版股份有限公司 (2019)。
14. 章忠信，英國「數位經濟法案」(The Digital Economy Act) 有關網路服務業者責任條款評析，檢察新論，第 10 期 (2011)。
15. 郭戎晉，網路言論傳播中介者責任與其免責規範之研究—以美國通訊端正法實務發展為中心，科技法律透析，第 23 卷第 4 期，頁 42 (2011)。
16. BBC, Trump Signs Executive Order Targeting Twitter After Fact-Checking Row, BBC NEWS (2020/05/29), available at <https://www.bbc.com/news/technology-52843986> (last visited May. 25, 2021).
17. BIG DATA : SEIZING OPPORTUNITIES, PRESERVING VALUES, Executive Office of the President (May, 2014), available at [https://obamawhitehouse.archives.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf) (last visited May. 9, 2021).
18. BIG DATA: A REPORT ON ALGORITHMIC SYSTEMS, OPPORTUNITY, AND CIVIL RIGHTS, Executive Office of the President (May, 2016), available at [https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016\\_05\\_04\\_data\\_discrimination.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_05_04_data_discrimination.pdf) (last visited May. 12, 2021).
19. CALIFORNIANS FOR CONSUMER PRIVACY, Executive Summary, available at <https://www.caprivacy.org/cpra-exec-summary/> (last visited May. 21, 2021).
20. Casey Newton, Everything You Need To Know About Section 230, THE VERGE (2020/05/28), available at <https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation> (last visited May. 26, 2020).
21. Cecilia Kang, A Leading Critic Of Big Tech Will Join The White House, THE

- NEW YORK TIMES (2021/3/5), available at <https://www.nytimes.com/2021/03/05/technology/tim-wu-white-house.html> (last visited May. 26, 2020).
22. CMA, A new pro-competition regime for digital markets- Advice of the Digital Markets Taskforce, Dec 2020, available at [https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital\\_Taskforce\\_-\\_Advice.pdf](https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital_Taskforce_-_Advice.pdf) (last visited May. 11, 2021)
23. CMA, Appendix B: The SMS regime: designating SMS firms, available at [https://assets.publishing.service.gov.uk/media/5fce72c58fa8f54d564aefda/Appendix\\_B\\_-\\_The\\_SMS\\_regime\\_-\\_designating\\_SMS\\_firms.pdf](https://assets.publishing.service.gov.uk/media/5fce72c58fa8f54d564aefda/Appendix_B_-_The_SMS_regime_-_designating_SMS_firms.pdf) (last visited May. 11, 2021)
24. CMA, Appendix C: The SMS regime: the code of conduct, available at [https://assets.publishing.service.gov.uk/media/5fce73098fa8f54d608789eb/Appendix\\_C\\_-\\_The\\_code\\_of\\_conduct\\_.pdf](https://assets.publishing.service.gov.uk/media/5fce73098fa8f54d608789eb/Appendix_C_-_The_code_of_conduct_.pdf) (last visited May. 11, 2021)
25. CMA, Appendix D: The SMS regime: The pro-competition interventions, available at [https://assets.publishing.service.gov.uk/media/5fce70118fa8f54d58640c7f/Appendix\\_D\\_-\\_The\\_pro-competition\\_interventions\\_.pdf](https://assets.publishing.service.gov.uk/media/5fce70118fa8f54d58640c7f/Appendix_D_-_The_pro-competition_interventions_.pdf) (last visited May. 11, 2021).
26. Comments of Consumer Technology Association (Sep. 02, 2020), available at <https://www.wiley.law/assets/htmldocuments/Comments%20of%20CTA%20RM-11862.pdf> (last visited May. 26, 2021).
27. COURT OF JUSTICE OF THE EUROPEAN UNION, Maximillian Schrems v. Data Protection Commissioner, Case C 362/14 (2015), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN> (last visited May. 13, 2021).
28. COURT OF JUSTICE OF THE EUROPEAN UNION, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18 (2020), available at <https://eur-lex.europa.eu/legal->

[content/en/TXT/?uri=CELEX:62018CJ0311](https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response) (last visited 2021/5/21).

29. David Uberti, *Tech Antitrust Hearing Puts Big Data On Hot Seat*, THE WALL STREET JOURNAL (2020/07/29), available at <https://www.wsj.com/articles/tech-antitrust-hearing-puts-big-data-on-hot-seat-11596067130> (last visited May. 13, 2021).
30. DCMS & Home Office, Online Harms White Paper: Full Government Response to the consultation, available at <https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response> last visited June 5,2021 )
31. DCMS & Home Office, Online Harms White Paper: Full Government Response to the consultation: Annex A, available at <https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response> ( last visited June 5,2021 )
32. Department for Culture, Media and Sport & Department for Business, Innovation and Skills, Digital Britain: Final Report (2009), available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228844/7650.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf) (last visited Feb. 6, 2020).
33. Department of Justice, Justice Department Sues Monopolist Google For Violating Antitrust Laws Department Files Complaint Against Google to Restore Competition in Search and Search Advertising Markets (October, 2020), available at <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws> (last visited May. 10, 2021).
34. Digital Competition Expert Panel, Unlocking digital competition, Mar. 2019, available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/785547/unlocking\\_digital\\_competition\\_furman\\_review\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf) (last visited May. 11, 2021)

35. Digital Economy Act 2010, available at [http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga\\_20100024\\_en.pdf](http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf) (last visited Feb. 6, 2018).
36. DIRECTORATE-GENERAL FOR THE INFORMATION SOCIETY AND MEDIA (EUROPEAN COMMISSION), EU STUDY ON THE LEGAL ANALYSIS OF A SINGLE MARKET FOR THE INFORMATION SOCIETY: NEW RULES FOR A NEW AGE? (2014).
37. Docket RM-11862 Section 230 of the Communications Act of 1934 (Jul. 29, 2020), available at [https://www.fcc.gov/ecfs/search/filings?proceedings\\_name=RM-11862&sort=date\\_disseminated,DESC](https://www.fcc.gov/ecfs/search/filings?proceedings_name=RM-11862&sort=date_disseminated,DESC) (last visited May. 26, 2021).
38. Egidijus Barcevičius, Dovydas Caturianas, Andrew Leming & Gabija Skardžiūtė, Multi-homing: obstacles, opportunities, facilitating factors, in: EUROPEAN COMMISSION, STUDY ON “SUPPORT TO THE OBSERVATORY FOR THE ONLINE PLATFORM ECONOMY” (Final Report) Analytical paper #7 (2021).
39. EUROPEAN DATA PROTECTION BOARD, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, available at [https://edpb.europa.eu/sites/default/files/files/file1/20200724\\_edpb\\_faqoncjeuc31118\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf) (last visited 2021/5/21).
40. EUROPEAN COMMISSION, Intensifying Negotiations On Transatlantic Data Privacy Flows: A Joint Press Statement By European Commissioner For Justice Didier Reynders And U.S. Secretary Of Commerce Gina Raimondo, available at [https://ec.europa.eu/commission/presscorner/detail/en/statement\\_21\\_1443](https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443) (last visited 2021/5/21).
41. FCC, Chairman Pai On Seeking Public Comment On NTIA's Sec. 230 Petition (Aug. 03, 2020), available at <https://www.fcc.gov/document/chairman-pai-seeking-public-comment-ntias-sec-230-petition> (last visited May. 26, 2021).
42. Federal Trade Commission, FTC Sues Facebook for Illegal Monopolization

- (December, 2020), available at <https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization> (last visited May. 10, 2021).
43. Federal Trade Commission, Protecting Consumer Privacy and Security, available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security> (last visited May. 12, 2021).
44. Fed. Trade Comm'n, Comment to the National Telecommunications & Information Administration on Developing the Administration's Approach to Consumer Privacy, No. 180821780-8780-01, (Nov. 9, 2018), available at [https://www.ftc.gov/system/files/documents/advocacy\\_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400\\_ftc\\_comment\\_to\\_ntia\\_112018.pdf](https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf) (last visited May. 12, 2021).
45. Geneva Internet Platform, Trump's Executive Order Challenged In Court, GIP Digital Watch (2020/06/02), available at <https://dig.watch/updates/trumps-executive-order-challenged-court> (last visited May. 26, 2021).
46. GOV.UK, Draft Online Safety Bill, available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/985033/Draft\\_Online\\_Safety\\_Bill\\_Bookmarked.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf) ( last visited June 5,2021 )
47. GOV.UK, Online Harms White Paper, available at <https://www.gov.uk/government/consultations/online-harms-white-paper> ( last visited June 5,2021 ) .
48. GovTrack.us, H.R. 1816: Information Transparency & Personal Data Control Act, available at <https://www.govtrack.us/congress/bills/117/hr1816> (last visited May. 21, 2021).
49. Home office, Interim Code of Practice on Online Child Sexual Exploitation and Abuse, available at <https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-online-child-sexual->

- [exploitation-and-abuse-accessible-version](#) ( last visited June 5,2021 )
50. Home office, Interim Code of Practice on Terrorist Content and Activity Online , available at <https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-terrorist-content-and-activity-online-accessible-version> ( last visited June 5,2021 )
  51. ICO, Data protection at the end of the transition period, available at <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/> (last visited June 05.2021)
  52. ICO, Data sharing code of practice, available at <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/> (last visited 2 June)
  53. ICO, Direct marketing code of practice Draft code for consultation, available at <https://ico.org.uk/media/for-organisations/documents/2021/2619043/direct-marketing-code-draft-guidance-122020.pdf> ( last visited June 5,2021 )
  54. ICO, Guide to the General Data Protection Regulation(GDPR), available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> ( last visited June 5,2021 )
  55. In the matter of the National Telecommunications & Information Administration’s Petition to Clarify Provisions of Section 230 of the Communications Act of 1934, as Amended, Comment of Engine, RM No. 11862 (Sep. 02, 2020), available at <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5f500e261e00bf5988ac1ee8/1599082023193/Engine+comments+RM-11862.pdf> (last visited May. 26, 2020).
  56. INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION[ITIF], International Data Flows : Promoting Digital Trade in the 21st Century (2015), available at [http://www2.itif.org/2015-atkinsoninternational-data-flows.pdf?\\_ga=2.211889044.144194272.1569468529-1177970121.1569468529](http://www2.itif.org/2015-atkinsoninternational-data-flows.pdf?_ga=2.211889044.144194272.1569468529-1177970121.1569468529) (last visited May. 2, 2021).
  57. INGE GRAEG, EU COMPETITION LAW, DATA PROTECTION AND

ONLINE PLATFORMS: DATA AS ESSENTIAL FACILITY (Kluwer Law International B.V., UK, 2016).

58. INVESTIGATION OF COMPETITION IN DIGITAL MARKETS: MAJORITY STAFF REPORTS AND RECOMMENDATIONS, available at [https://judiciary.house.gov/uploadedfiles/competition\\_in\\_digital\\_markets.pdf?utm\\_campaign=4493-519](https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519) (last visited May. 9, 2021).
59. Justice Department's Google complaint filed, available at: <https://www.justice.gov/opa/press-release/file/1328941/download> (last visited May. 10, 2021).
60. Lina M. Khan, Amazon's Antitrust Paradox, 126 YALE LAW JOURNAL 710 (2019).
61. Makena Kelly, Biden'S Commerce Nominee Backs Changes To Section 230, THE VERGE(2021/1/26), available at <https://www.theverge.com/2021/1/26/22250746/biden-gina-raimondo-commerce-secretary-section-230> (last visited May. 26, 2020).
62. Mark Scott, Data Transfer Pact Between U.S. and Europe Is Ruled Invalid , Oct.6, 2015, THE NEW YORK TIMES, available at <https://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html> (last visited May. 13, 2021).
63. Natalia Drozdiak & Sam Schechner & John D. McKinnon, U.S., EU Reach Deal on New Data Transfer Framework , THE WALL STREET JOURNAL, Feb. 2, 2016, available at <https://www.wsj.com/articles/u-s-eu-reach-deal-on-new-data-transfer-framework-1454429818> (last visited May. 12, 2021).
64. NTIA, NITA Petition For Rulemaking To Clarify Provisions Of Section 230 Of The Communications Act (May. 27, 2021), available at <https://www.ntia.gov/fcc-filing/2020/ntia-petition-rulemaking-clarify-provisions-section-230-communications-act> (last visited Oct. 26, 2020).
65. OFFICIAL JOURNAL OF THE EUROPEAN COMMUNITIES, Pursuant To Directive 95/46/EC Of The European Parliament And Of The Council On The

Adequacy Of The Protection Provided By The Safe Harbour Privacy Principles And Related Frequently Asked Questions Issued By The US Department Of Commerce (2000/520/EC) (2000), under the heading 'Notice', available at <https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32000D0520&from=en> (last visited May. 12, 2021).

66. Peter Carey, *Data Protection: A Practical Guide to UK and EU Law* Fifth edition, Oxford, 2018.
67. PRIVACY SHIELD FRAMEWORK, FAQs – EU-U.S. Privacy Shield Program Update, available at <https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update> (last visited 2021/5/21).
68. Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18), available at <https://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=583421> (last visited May 20, 2021).
69. Ryan Tracy, *After Big Tech Hearing, Congress Takes Aim But From Different Directions*, THE WALL STREET JOURNAL, 2020/07/30, available at <https://www.wsj.com/articles/after-big-tech-hearing-congress-takes-aim-but-from-different-directions-11596149053?mod=searchresults&page=4&pos=3> (last visited May. 13, 2021).
70. Shona McCusker, *The EU-US Privacy Shield: The Antidote To The Transatlantic Data Transfer Headache? Headache?*, 37 Business Law Review 84, 84-85 (2016).
71. TECHFREEDOM, *NTIA's FCC Petition to Reinterpret Section 230 Is a Constitutional Non-Starter* (2020/07/27), available at <https://techfreedom.org/ntias-fcc-petition-to-reinterpret-section-230-is-a-constitutional-non-starter/> (last visited May. 26, 2021).
72. *The California Privacy Rights and Enforcement Act of 2020* (2019), available at <https://oag.ca.gov/system/files/initiatives/pdfs/19->

- [0019%20%28Consumer%20Privacy%20-%20Version%202%29.pdf](#) (last visited May. 21, 2021).
73. THE COMMISSION OF THE EUROPEAN COMMUNITIES, 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (2000), available at <https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML> (last visited May. 12, 2021).
74. THE NATIONAL LAW REVIEW, With All This Talk About The CCPA Litigation Risk, How Many CCPA Class Actions Actually Got Filed In 2020?, available at <https://www.natlawreview.com/article/all-talk-about-ccpa-litigation-risk-how-many-ccpa-class-actions-actually-got-filed> (last visited May. 21, 2021).
75. THE NATIONAL LAW REVIEW, 2021 CCPA Q1 Litigation Report: 35+ Cases Filed, Unsurprising Trend of Data Event Class Actions, available at <https://www.natlawreview.com/article/2021-ccpa-q1-litigation-report-35-cases-filed-unsurprising-trend-data-event-class> (last visited May. 21, 2021).
76. The White House, Executive Order on Preventing Online Censorship (May 28, 2020), available at <https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/> (last visited May. 22, 2021).
77. U.S. DEPARTMENT OF JUSTICE, Section 230-Nurturing Innovation or Fostering Unaccountability? (June 2020), available at <https://www.justice.gov/file/1286331/download> (last visited May. 26, 2021).
78. U.S. DEPARTMENT OF COMMERCE, U.S.-EU Safe Harbor Framework A Guide to Self-Certification(2009), available at [https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1650&context=key\\_workplace](https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1650&context=key_workplace) (last visited May. 12, 2021).
79. U.S. EMBASSY IN LUXEMBOURG, U.S. Secretary Of Commerce Wilbur Ross Statement On Schrems II Ruling And The Importance of EU-U.S. Data Flows,

available at <https://lu.usembassy.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/> (last visited 2021/5/21).

80. Yann Padova, The Safe Harbour Is Invalid What Tools Remain For Data Transfers And What Comes Next?, *International Data Privacy Law*, Volume 6, Issue 2, 139-161 (2016).
81. クリス・フーフナグル (Chris Jay Hoofnagle) 著，宮下紘、板倉陽一郎、河井理穂子、國見真理子、成原慧、前田恵美譯，アメリカプライバシー法：連邦取引委員会の法と政策，頁 71-72，勁草書房（2018）。