大數據及物聯網之營業秘密保護趨勢

楊芝青*
蕭睆文**

壹、前言

Directive（EU）2016/943（歐盟營業秘密保護指令）於2016年頒布，旨在協調全體歐盟國家的營業秘密法，規範會員國針對營業秘密之保護最低之標準。為了追蹤指令之實際落實情況，歐盟智慧財產局委託法律學術單位進行跨國研究，並分別於2018年推出The Baseline of Trade Secrets Litigation in the EU Member States，且在此基礎上於2023年推出歐盟營業秘密訴訟趨勢報告（Trade Secrets Litigation Trends in the EU，下稱2023年歐盟報告）。2023年的報告量化分析，研究期間追蹤逾700則判決觀察到，在案件量和法律論壇方面，歐洲各成員國的營業秘密訴訟往往在國家層面呈現高度本地化的態勢，跨國爭端相對較少。營業秘密爭端的形態往往集中在僱主和（前）員工之間，與第三方企業的爭端相對少見。不正當競爭法仍然常常被用於營業秘密訴訟之輔助。

在歐盟營業秘密保護意識高漲平行的時空背景，隨著電腦運算能力的加速，巨量資料的價值也隨之爆炸式成長，掌握了巨量資料就掌握競爭優勢。「企業現在都知道，收集顧客資料非常重要，也假設公司收集和探勘愈多的顧客資料，就能產生更多見解，提供更好的產品來吸引更多顧客，如此，進入一個贏家全拿的局面」[1]。而早在2017年經濟學人的報導即指出，資料以一種新商品之姿，催生了一個利潤豐厚、快速成長的行業，好比一個世紀前的石油產業。資料巨頭—Alphabet（Google的母公司）、亞馬遜、蘋果、Facebook和微軟—是全球市值最高的五家上市公司，且利潤正在飆升。亞馬遜佔了美國網路消費總額的一半。在2016年，Google和Facebook幾乎佔據了美國數位廣告收入成長的全部。[2]

＊本文作者係執業律師
＊＊本文作者係臺大資訊工程研究所博士候選人
註1：https://www.hbrtaiwan.com/article/19292/capturing-the-real-advantages-of-data
註2：https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

貳、研究動機

在此背景下，與資料巨頭相關的反壟斷疑慮及各國行政調查未曾中斷過。然而本篇將著重於資料巨頭、或者其他資料控制者可能主張更多法律保護的另一個工具，即營業秘密法。在保護智慧財產之同時維持公平競爭秩序，向來是歐盟注重的領域。2023年歐盟報告即指出，「一個關鍵問題是如何以營業秘密法來保護『資料』，尤其是當這些資料是自然發生的語義訊息的抽象記錄（例如，從傳感器收集的資料）。在討論『大數據』與營業秘密之間的關係時，重要的是區分訊息（語義層面上的資料）的概念與其編碼的符號（語法層面上的資料）。這對於物聯網（IoT）應用尤其重要。在這些應用中，如何解釋保密要求，以及如何區分自然存在且對公眾可訪問的訊息與可保護的秘密訊息，都是未來法律發展的關鍵領域。」[3]

學者擔憂道，「借助大數據和智慧財產權（尤其是營業秘密）組合的優勢，物聯網（IoT）公司的商業活動可能對市民產生負面影響，而這些商業活動通常由於技術和法律的保密性，使市民通常對此一無所知。所謂的『技術』保密性源於物聯網演算法的不透明性，尤其是當其具有人工智能功能時。而『法律』保密性則來自營業秘密、商業軟體和契約的組合，這些因素使得物聯網資料實際上維持保密。」[4]、「其他論文主張，至少在原則上，營業秘密保護適用於物聯網（IoT）資料，這些資料主要是由用於資料收集、存檔和進一步加工的自動化過程產生的。因此，它將包括由眾所周知的IoT設備Dash Button和Echo生成和管理的資料。即使歐盟營業秘密保護指令沒有明確提及機器間過程產生的資料，也應該採取廣泛的解釋，將這些資料與其他和更傳統的方式生成的資料

註3：EUIPO, TRADE SECRETS LITIGATION TRENDS IN THE EU 60-61 (2023). A key issue is how 'data' might be protected by trade secret law, particularly when these data are recorded abstractions of naturally occurring semantic information (e.g. data collected from sensors). When discussing the relationship between 'big data' and trade secrets, it is important to distinguish the concept of information (data on the semantic level) from the signs in which it is encoded (data on the syntactic level). This is particularly relevant for Internet of Things (IoT) applications. How the secrecy requirement is interpreted in such applications, and the doctrines for distinguishing between naturally occurring information accessible to the public and protectable secret information, are key areas for monitoring future legal developments）

註4：Guido Noto La Diega and Cristiana Sappa, *The Internet of Things at the intersection of data protection and trade secrets. Non-conventional paths to counter data appropriation and empower consumers*, 3 Revue européenne de droit de la consommation/ European Journal of Consumer Law 419-458 (2020) at 15, available at https:/ssrn.com/abstract=3772700. Leveraging a portfolio of big data and intellectual property rights (especially trade secrets), IoT companies put in place practices that can negatively affect citizens, who are often unaware of them due to a technical and legal secrecy. 'Technical' secrecy results from the opacity of the algorithms that underpin the IoT, especially when AI-enabled. 'Legal' secrecy, in turn, come from a combination of trade secrets, proprietary software and contracts that keep IoT data practices secret

一起納入可保護的對象中。然而，當這些（表面上平凡的）訊息與其他資料相關聯並進行分析時，可能會產生實質價值。在大數據中，包括物聯網資料，當有足夠的平凡訊息被匯集並分析時，這些平凡訊息可以具有經濟價值。這引出了一個問題，即我們是否應該將營業秘密保護擴展到通過匯總最初由人類或人工技術收集的資料而獲得的資料庫。如果這種歷時產生的訊息具有潛在的商業價值，那麼它確實應該受到保護。」[5]。該文作者以消費者的身份請求亞馬遜公司提供其個人資料，然而亞馬遜公司僅提供以機器記錄時間、資料來源名稱（其Alexa產品序號）、國家及軟體版本構成的簡陋資料集，作者因此推論亞馬遜公司不願意提供之原因可能是因為認為消費者與其Alexa機器語音互動之資料，為其寶貴的營業秘密。[6]

組成大型資料匯總的資料在產生時通常是一個原始的無意義組件。因此，它不僅是其他活動的副產品，而且已經成為現實的各個方面轉化為資料的基本“世界記錄的抽象”（“資料化”）的結果。在大多數應用中，它已經成為使任何類型的活動、商品或服務成為可能的基礎設施。資料再經歷挪用和產權化的過程，使人們對大規模資料集的依賴成為全球市場上生存的問題。智慧財產權標準為此作出了貢獻，因為它們構成了個人和社會整體之間為產權努力之關係的基礎，並將其正式化。若推至極端，學者Haggart認為它們打開了通往“新封建制”全球經濟的大門，智慧財產權（和資料）所有者坐鎮頂峰。因此，在今天的“資料化”世界中，智慧財產權出現了新挑戰。如果現實的任何組成部分都是可計算和可轉換為資料的，那麼廣泛的專有體系就是一種可能的未來。如果我們為資料的智慧財產權和類智慧財產權打開了道路，那麼大多數資料元素幾乎都可以變成有資格受到保護的東西[7]。

註5：*Id*. at 18. Other papers have argued that-at least in principle-trade secrets protection applies to IoT data, which are mainly the outcome of automated processes used for the collection, archiving and any further elaboration of data. Therefore, it would cover data produced and managed by the well-known IoT devices Dash Button and Echo. Even if the Trade Secrets Directive does not expressly refer to data resulting from a machine-to-machine process, an extensive interpretation of this text, which includes them in the protectable subject matter together with data generated in other and more traditional ways, has to be followed. However, substantial value may arise from the correlation of such (trivial) information with other data. With big data, including IoT data, trivial information can have economic value when there is enough trivial information that is put together and analysed. This begs the question whether we should extend trade secrets protection also to databases obtained by aggregating data initially gathered by humans or artificial techniques. Should this diachronically created information have a potential commercial value, it would certainly deserve protection

註6：*Id*. at 4.

註7：Fia, T. Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data. *IIC* 53, 917-949 (2022) at 922.
https://doi.org/10.1007/s40319-022-01204-8. Data that makes up massive digital aggregations is typically a raw meaningless component when it is produced. Therefore, not only is it a by-product

有鑒於前述歐盟2023年報告及學者提出之疑慮，本文檢視歐盟、美國及我國法規、案例，嘗試搜集、分析實務上訴訟之一造主張以營業秘密法保護資料的案例（以及類似案例）？且嘗試探討歐盟學者形容的資料新封建制是否已然呈現？

參、營業秘密法保護框架及各國規定

基於ＷＴＯ與貿易有關智慧財產權協定（TRIPS協定）制定會員國對智慧財產權保護之最低要求，各國對營業秘密之定義遵循相同之原則。TRIPS協定第39條如下：

「自然人及法人應得防止他人未經同意而以違背誠實商業行為的方式，揭露、取得或使用合法處於其控制下之資訊，但該資料須：(a)具有秘密性質，且不論由就其整體或細節之配置及成分之組合視之，該項資料目前仍不為一般處理同類資訊之人所得知悉或取得者；(b)因其秘密性而具有商業價值；且(c)合法控制該資訊之人已依情況採取合理步驟，以保持其祕密性。」[8,9]。歐盟之2016年營業秘密指令[10]、美國統一營業秘密法

of other activities, but it has also become a basic “recorded abstraction of the world” resulting from the transformation of all aspects of reality into data (“datafication”).27 In most applications, it has become an infrastructure that makes any kind of activity, good or service possible.28 Data dependency then goes through processes of data appropriation29 and propertisation, making reliance on massive datasets a matter of survival in global markets. IP standards contribute to this cause, for they form the basis of and formalise the relationship between individuals and social aggregations in their proprietorial endeavours. By taking this to the extreme, Haggart argues that they open the door to a “‘neo-feudal’ global economy, with IP (and data) owners ensconced at the top”.30 Thus, novel challenges for intellectual property ensue in today's “datafied” world. If any component of reality is computable and convertible into data, then a widespread proprietary architecture is a plausible future. If we open the way for IPRs and quasi- IPRs in respect of data, it is striking how most data elements can virtually turn into something eligible for protection

註8：經濟部智慧財產局，與貿易有關之智慧財產權協定第39條（TRIPS§39），https://www.tipo.gov.tw/tw/cp-10-890012-8b516-1.html（最後造訪2023年10月1日）。

註9：WTO, Uruguay Round Agreements: TRIPS, Section 7: protection of undisclosed information Article 39, available at https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm. （Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices (10) so long as such information: (a)is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b)has commercial value because it is secret; and (c)has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.）

註10：Directive (EU) 2016/943, of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their

（Uniform Trade Secret Act）[11]、「2016年營業秘密防衛法」（Defend Trade Secrets Act of 2016）[12]及我國對營業秘密之定義均類似於前述TRIPS規定，容許本文在類似基礎上比較前開國家之案例。

肆、具備營業秘密面向之大數據資料訴訟案例

一、Lyft, Inc. v. City of Seattle, Supreme Court of Washington（190 Wn.2d 769）

Lyft為著名交通網路公司（transportation networking companies），得撮合乘客及司機，該公司之營業範圍均包含華盛頓州西雅圖市，該市交通主管機關之規定其必須定期匯報系統記載之乘客乘車資訊。此外，依照華盛頓州公眾記錄法（Public Records Act），除非法律另有規定，政府應依市民請求公開資訊。在本案中，有市民請求西雅圖市政府提供乘客乘車資訊，Lyft即向地方法院聲請假處分，禁止市政府對該市民提供前開資訊中之上下車之郵政編碼（zip code）。地方法院認定乘

Unlawful Acquisition, Use and Disclosure, 2016 OJ (L 157) 1, 18.「就本指令而言，適用以下定義：(1)“營業秘密”是指滿足以下所有要求的訊息：(A)它是秘密的，因為它作為一個整體或其組成部分的精確配置和組裝，並不為通常處理相關訊息的圈子內的人們所普遍知曉或容易獲得；（二)因為秘密所以具有商業價值；(C)合法控制該訊息的人已根據具體情況採取合理措施對其保密」（For the purposes of this Directive, the following definitions apply: (1) ‘trade secret’ means information which meets all of the following requirements: (a)it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b)it has commercial value because it is secret; (c)it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret）.

註11：美國早期係由各州以不正競爭原則、侵權行為或違約等案例法保護營業秘密。然而因案例法，以及各州自行嘗試立法多有歧義，在產業呼籲下，美國統一州法委員會（The National Conference of Commissioners on Uniform State Laws）為使各州之營業秘密保護有較一致之標準，於1979年制定統一營業秘密法（Uniform Trade Secret Act）之範本，而嗣後各州多參採該範本為立法，斯時聯邦政府並無專門規範營業秘密保護之法律。直至1996年國會始制定經濟間諜法（Espionage Act），訂定違反營業秘密保護刑事責任規定，而國會鑒於營業秘密對美國企業愈益重要，為適應數位時代關於營業秘密民事保護之需要，乃著手研議制定「2016年營業秘密防衛法」（Defend Trade Secrets Act of 2016 DTSA，下稱防衛法）。統一營業秘密法將營業秘密定義為：「訊息，包括公式、模式、彙編、程序、設備、方法、技術或流程（且符合下述要件）：因不為其他可從其揭露或使用中獲得經濟價值的人所普遍知曉且不易透過適當手段確定，進而有實際或潛在的獨立經濟價值；且，是根據情況採取合理努力保守秘密的客體。」（The USTA defines a "trade secret" as: "information, including a formula, pattern, compilation, program, device, method, technique, or process that: Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.）

註12：所有形式和類型的財務、商業、科學、技術、經濟或工程訊息，包括圖案、計劃、彙編、程序裝

客乘車資訊郵遞區號為Lyft之營業秘密，故禁止市政府提供資訊，市政府對此提起上訴。

市政府指摘，地方法院未認定該郵政編碼報告為美國統一營業秘密法定義之彙編。然而上訴法院認為，Lyft郵政編碼報告構成了季度報告中[記錄]的每次Lyft行程的“積累”，故認為郵政編碼報告符合該法定義。[13]

市政府另挑戰郵政編碼記錄的「價值性」要件。市政府主張，Lyft只是使用市政府報告模板提取季度郵政編碼記錄，而在製作這些報告時花費精力或費用極少或甚至於無。然而，上級法院認為，初審法院發現郵政編碼報告作為Lyft收入生成的空間指標以及營銷新產品的戰略指標的價值。法院還發現，Lyft及競爭對手Raiser都有興趣獲取對方的郵政編碼報告，且彼此無法通過適當方式輕易獲取對方之郵政編碼報告。且得作為推出新共乘車和共享產品的潛在路線以及訂閱服務市場的指標。[14]

置、公式、設計、原型、方法、技術、流程、程式、程式或程式碼，無論是有形的還是無形的，以及是否或如何以物理、電子、圖形、照片或書面形式儲存、編譯或記憶，如果(A)其所有者已採取合理措施對該資訊保密；和(B)該資訊具有獨立的經濟價值，無論是實際的還是潛在的，因為該資訊不為其他人所普遍知曉，也無法透過適當的方式輕易查明，而其他人可以從該資訊的揭露或使用中獲得經濟價值。18 U.S. Code § 1839, Definitions. (3)the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A)the owner thereof has taken reasonable measures to keep such information secret; and (B)the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

註13：Lyft, Inc. v. City of Seattle, 190 Wn.2d 769 (Wash. 2d. 2018).

The City contends that the trial court neglected to make concrete findings on the required UTSA elements. RCW 19.108.010(4). First, the City argues that the court failed to specifically find, based on the facts, that the L/R zip code reports constitute a compilation under the UTSA. Opening Br. of Appellant City at 38-39. HN18[ ] Because the UTSA provides no definition for the term “compilation,” we look to its usual and ordinary dictionary definition. Fraternal Order of Eagles, Tenino Aerie No. 564 v. Grand Aerie of Fraternal Order of Eagles, 148 Wn.2d 224, 239, 59 P.3d 655 [*782] (2002). Webster's [***13] defines “compilation” as “something that is a product of the putting together of two or more items: as … an accumulation of many things, elements, or influences.” WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 464 (1981). [**109] ¶17 Lyft argues that its zip code reports constitute an “ ‘accumulation’ of all zip code data for each and every Lyft ride [documented] on the quarterly reports, … contain[ing] the entire universe of zip code data for Lyft for any given quarter.” Resp't Lyft's Answering Br. at 17-18. L/R zip code reports are distinguishable from the discrete reports for which the superior court denied injunctive relief. CP at 266 (Order Granting in Part & Den. in Part Pls.' Mot. for Prelim. Inj. at 3 (Mar. 21, 2016)). The trial court inferred that zip code report queries that extract data equate to an ability to compile information. CP at 2705.

二、Compulife Software Inc., v. Newman

Compulife建構並維護著一個可供付費訂閱的保費訊息資料庫，名稱為“轉型資料庫（Transformative Database）”，有許多人壽保險公司保費率之最新訊息，得同時比較數十家提供商的費率。其大多數客戶都是保險經紀人，訂閱資料庫以便更輕鬆地向潛在保單購買者提供可靠的成本估算。儘管該資料庫係基於公開訊息，但若無Compulife內部的專門方法和公式，就無法複製它。[15]

註14：¶18 Next, the City argues that the superior court failed to make concrete [***14] findings regarding the effort and expense L/R undertook in extracting quarterly zip code records using the City's reporting template, that neither Lyft nor Rasier met its burden to demonstrate the zip code reports have independent economic value because little or no effort or expense was incurred in producing these reports, and that the real value resides in other L/R data not reported to the City. Opening Br. of Appellant City at 40-42. It notes that "neither [Lyft nor Rasier] attempted to 'quantify in any meaningful way the competitive advantage' the other 'would enjoy' if the information was released." Id. at 42. HN19[ ] Information possesses independent economic value under the UTSA when effort and expense were incurred to develop the information. McCallum v. Allstate Prop. & Cas. Ins. Co., 149 Wn. App. 412, 424, 204 P.3d 944 (2009); Nowogroski Ins., 137 Wn.2d at 438. **The information must not [*783] be readily ascertainable from another source.** Spokane Research & Def. Fund v. City of Spokane, 96 Wn. App. 568, 577-78, 983 P.2d 676 (1999). ¶19 **The trial court found value in the zip code reports as a spatial indicator of L/R revenue generation and as a strategic indicator for marketing new products. CP at 2705. The court also found that both L/R are interested in obtaining the other's zip code reports, though this was hotly debated. Id. The superior court found the zip code reports are not readily ascertainable by competitors [***15] by proper means.** CP at 2717. While it is a close call, the record sufficiently demonstrates the independent economic value of the data reflected by the zip code reports, including as an indicator for potential routes for launching new ride pool and sharing products, and markets for subscription services. Substantial evidence supports the superior court's finding of independent economic value in the zip code reports. ¶20 **Finally, the City argues that every L/R driver accesses company data, even when also driving for the competitor TNC, and thus the zip code data is not a trade secret that is the "subject of efforts that are 190 Wn.2d 769, *781; 418 P.3d 102, **108; 2018 Wash. LEXIS 350, ***11 Page 17 of 26 reasonable under the circumstances to maintain its secrecy." RCW 19.108.010(4)(b); see also Opening Br. of Appellant City at 47. Respondents reply that although the driver may have access to the beginning and ending zip codes for each trip driven, the driver lacks access to other records in the quarterly zip code report. Resp't Rasier LLC's Answering Br. at 28. The superior court found that the respondents L/R do not share the zip code reports between each other because of the perceived competitive disadvantages of doing so.** CP at 2705-06. L/R restrict access to the zip code reports internally within their companies, [***16] with corresponding policies and procedures. CP at 2706. **The limited data drivers have is not the same data L/R protect.** Substantial evidence supports the superior court's finding that L/R make reasonable efforts under the circumstances to maintain the secrecy of the zip code reports. [*784] ¶21 In sum, while the evidence is mixed and the question is not beyond debate, the superior court sustainably concluded that L/R's zip code

Compulife進階的產品是“互聯網引擎”許可證進階客戶可以自己的服務中嵌入Compulife的互聯網報價引擎，其中包括轉換資料庫，並將其與自己創建的其他功能串接。進階客戶更可招攬他人訂閱此集合而成的服務。但進階客戶招攬的對象僅限於Compulife訂閱者，以確保它不會與Compulife競爭潛在的保險代理客戶。Compulife還允許進階客戶向其終端客戶提供其網路報價HTML程式碼，以便終端客戶的網站可以利用進階客戶的服務檢索報價。此組HTML程式碼與Compulife提供給加購網路報價器的PC使用者的HTML程式碼相同。[16]

被告Newman也從事人壽保險報價業務，主要通過網站www.naaip.org。潛在的人壽保險購買者可以在任何NAAIP運行的網站，輸入人口統計訊息以獲取報價，就像他們可以在任何加購網路報價器的PC使用者網站上獲取報價一樣。每個NAAIP運行的網站有一個鏈結，消費者透過此鏈結可向與被告合作的經紀公司購買保險，使被告得以抽佣。[17]

Newman僱傭了一名駭客Natal從Compulife服

---

reports are “trade secrets” within the meaning of the UTSA. For this reason, the UTSA is properly regarded as an applicable “other statute” in this context. See PAWS, 125 Wn.2d at 261-62. Concluding that L/R records contain trade secrets does not end the inquiry, however. As [**110] noted, there is no categorical exemption for trade secrets under the PRA, and we must therefore determine whether L/R are entitled to an injunction to prevent the City from disclosing the records in response to a public records request.

註15：Compulife Software Inc., v. Newman, 959 F.3d 1288 (11 Cir. 2020).
Compulife maintains a database of insurance-premium information called the "Transformative Database" to which it sells access. The Transformative Database is valuable because it contains up-to-date information on many life insurers' premium-rate tables and thus allows for simultaneous comparison of rates from dozens of providers. Most of Compulife's customers are insurance agents who buy access to the database so that they can more easily provide reliable cost estimates to prospective policy purchasers. Although the Transformative Database is based on publicly available information namely, individual insurers' rate tables it can't be replicated without a specialized method and formula known only within Compulife.

註16：the "internet-engine" license permits a licensee to host Compulife's internet-quote engine, which includes the Transformative Database, on its own server and to integrate it with additional features of its own creation. An internet-engine licensee [*1297] can then sell access to "its" product which is an amalgamation of Compulife's internet-quote engine with any accoutrements that the licensee has seen fit to add. Importantly, though, internet-engine licensees can sell access only to Compulife's PC licensees. This arrangement allows an internet-engine licensee to include Compulife's internet-quote engine again, with the Transformative Database as a part of its own product, while simultaneously ensuring that it doesn't compete with Compulife for potential insurance-agent customers. Compulife also permits an internet-engine licensee to provide its web-quoter HTML code to the licensee's customers so that the customers' websites can retrieve quotes from the licensee's server. This is the same copyrighted HTML code that Compulife provides to PC licensees with the web quoter add-on.

註17：Now, to the defendants, who are also in the business of generating life-insurance quotes primarily

務器上“抓取”資料。抓取是一種從網站提取大量資料的技術。駭客使用普通的HTTP命令從服務器請求訊息，類似於服務器的合法客戶端程序在普通過程中可能使用的命令。儘管駭客可以通過將每個命令作為一行代碼輸入然後記錄結果來手動獲取資料，但抓取攻擊的真正威力是通過創建一個可以發出許多請求的機器人（簡稱“機器人”）來實現的。自動且比任何人都快得多。機器人可以從目標服務器請求大量資料（技術上一次一個查詢，但每秒多個查詢），然後立即將返回的訊息記錄在電子資料庫中。[18]

Natal抓取與兩個郵政編碼（一個在紐約，另一個在佛羅里達）相關的所有保險報價資料，總計超過4300萬條報價。如果由人類執行，則需要數千個工時，但機器人只花了四天時間。[19]被告隨後使用抓取的資料作為在自己網站上生成報價的基礎。[20]

through a website, www.naaip.org. Prospective life-insurance purchasers can then obtain quotes on any of these NAAIP-hosted websites by entering demographic information, just as they could on the website of any Compulife PC licensee with a [**7] web quoter add-on. Each NAAIP site includes a link that allows consumers to purchase insurance through One Resource Group, Inc., a brokerage firm with which the defendants have partnered. If a visitor to an NAAIP site uses the link to buy insurance, the defendants receive a part of One Resource's brokerage fees in exchange for the referral.

註18：In the 42 case, Compulife alleges that the defendants hired a hacker, Natal, to "scrape" data from its server. Scraping is a technique for extracting large amounts of data from a website. The concept is simple; a hacker requests information from a server using ordinary HTTP commands similar to those that a legitimate client program of the server might employ in the ordinary course. Although a hacker could obtain the data manually by entering each command as a line of code and then recording the results, the true power of a scraping attack is realized by creating a robot or "bot," for short that can make many requests automatically and much more rapidly than any human could. A bot can request a huge amount of data from the target's server technically one query at a time, but several queries per second and then instantaneously record the returned information in an electronic database. By formulating queries in an orderly fashion and recording the resulting information, the bot can create a copy or at least a partial copy of a database underlying a website.

註19：Natal used this scraping technique to [**12] create a partial copy of Compulife's Transformative Database, extracting all the insurance-quote data pertaining to two zip codes one in New York and another in Florida.3 That means the bot requested [*1300] and saved all premium estimates for every possible combination of demographic data within those two zip codes, totaling more than 43 million quotes. Doing so naturally required hundreds of thousands of queries and would have required thousands of man-hours if performed by humans but it took the bot only four days. The HTML commands used in the scraping attack included variables and parameters essentially words (or for that matter any string of characters) used to designate and store values from Compulife's copyrighted HTML code. For example, the parameter "BirthMonth" in Compulife's code stores a number between one and twelve, corresponding to a prospective purchaser's birth month.)

註20：Compulife alleges that the defendants then used the scraped data as the basis for generating

法院認為Compulife若依據佛羅里達統一營業秘密法（FUTSA），必須證明(1)它擁有營業秘密，並且(2)該秘密被不當取用。佛羅里達州法律將營業秘密定義為具下述屬性的訊息：(a)[d]產生獨立的經濟價值…不為其他可從其披露或使用中獲得經濟價值的人所普遍知悉，也不易通過適當手段查明；(b)[i]是在當時情況下採取合理努力保守秘密的對象。[21] 地方法院法官認定Compulife的轉型資料庫屬於營業秘密，這一裁決並沒有明顯錯誤，而且無論如何，上訴時似乎未受到質疑。因此，上訴審法院直接討論不當取用的問題。[22]

依照佛羅里達州法律，一方透過取得、揭露或使用的方式可能構成不當取用另一方的營業秘密。Compulife指控被告透過取得和使用方式進行挪用，而當一個人獲得營業秘密並且「知道或有理由知道該營業秘密是透過不正當手段獲得的」時，他就透過獲取而盜用了該營業秘密。如果一個人「未經明示或默示同意」使用秘密，並且存在以下任一情況，則該人透過使用盜用秘密：1.以不正當手段知悉營業秘密的；或者2.在揭露或使用時，知道或有理由知道她或他對營業秘密的了解是：A.來自或透過使用不正當手段獲得的人；B.在產生保密義務或限制其使用的情況下獲得的；或者C.來自或透過對尋求救濟的人負有保密或限制其使用的義務的人；或者3.在她或他的職位發生重大變化之前，知道或有理由知道這是商業秘密，並且該資訊是透過意外或錯誤獲得的。[23]

---

quotes on their own websites. The defendants don't disagree, except to claim that they didn't know the source of the scraped data but, rather, innocently purchased the data from a third party. Moses Newman testified, however, that he watched Natal collect the requested data in a manner consistent with a scraping attack. David Rutstein also testified that when the defendants instructed Natal to obtain insurance-quote information, they fully intended for her to "extract[ ] data" from an existing website.

註21：And now for something completely different trade-secret law. HN30[ ] To prove a claim under the Florida Uniform Trade Secrets Act (FUTSA), Compulife "must demonstrate that (1)it possessed a trade secret and (2) the secret was misappropriated." Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1297 (11th Cir. 2018) (quotation and quotation [*1311] marks omitted).13 Florida law defines a trade secret as information... that: (a)[d]erives independent economic value... from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) [i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

註22：Fla. Stat. §688.002(4). "[W]hether something is a trade secret is a question typically 'resolved by a fact finder after full presentation of evidence from each side.'" Yellowfin Yachts, 898 F.3d at 1298-99 (quoting Lear Siegler, Inc. v. Ark-Ell Springs, Inc., 569 F.2d 286, 288-89 (5th Cir. 1978)). The magistrate judge found that Compulife's Transformative Database was a trade secret, a finding that is not clearly erroneous and that, in any event, doesn't seem to be contested on appeal. We can therefore move straight to the question of misappropriation.

註23：HN31[ ] One party can misappropriate another's trade secret by either acquisition, disclosure, or use. See Fla. Stat. §688.002(2). Compulife alleges misappropriation [**38] both by acquisition and by use but not by improper disclosure. A person misappropriates a trade secret by acquisition

FUTSA中使用的“不正當手段”被定義為包括“盜竊、賄賂、虛假陳述、違反或誘導違反保密義務，或通過電子或其他方式進行間諜活動”。方法。”在更一般的營業秘密法中，“盜竊、竊聽，甚至空中偵察”可以構成不正當手段，但“獨立發明、意外洩露或……逆向工程”則不能。法院並引用E. I. Du Pont de Nemours & Co. v. Christopher, 431 F.2d 1012, 1014（5th Cir. 1970）案件（駁回以下論點：“盜用營業秘密必須存在非法侵入或其他非法行為，才構成不法行為”），認為即使行為本身不違法，也可能是“不當”的。[24]

如果抓取攻擊構成“不正當手段”，則很難逃脫以下結論：被告(1)使用了他們通過不正當手段獲取的營業秘密，抑或(2)使用他們從他們知道或有理由知道以不正當方式獲得該知識的人那裡獲得的營業秘密。被告承認僱傭了駭客並觀察她採取與抓取攻擊一致的行動。[25]

地方法院認定轉型資料庫是營業秘密，但認為因為個別報價是向公眾公開的，因此

---

when he acquires it and "knows or has reason to know that the trade secret was acquired by improper means." Id.§688.002(2)(a). A person misappropriates a secret by use if he uses it "without express or implied consent" and either:

1.Used improper means to acquire knowledge of the trade secret; or

2.At the time of disclosure or use, knew or had reason to know that her or his knowledge of the trade secret was:

a.Derived from or through a person who had utilized improper means to acquire it;

b.Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

c.Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

3.Before a material change of her or his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake. Id. §688.002(2)(b).

註24：The concept of "improper means" which under FUTSA may apply in both the acquisition and use contexts is significant here, so we should pause to unpack it. HN32[ ] As used in FUTSA, "[i]mproper means" is defined [**39] to include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." Id. §688.002(1). In the law of trade secrets more generally, "theft, [*1312] wiretapping, or even aerial reconnaissance" can constitute improper means, but "independent invention, accidental disclosure, or . . . reverse engineering" cannot. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476, 94 S. Ct. 1879, 40 L. Ed. 2d 315 (1974).14 Actions may be "improper" for trade-secret purposes even if not independently unlawful. See E. I. Du Pont de Nemours & Co. v. Christopher, 431 F.2d 1012, 1014 (5th Cir. 1970) (rejecting the argument "that for an appropriation of trade secrets to be wrongful there must be a trespass, other illegal conduct, or breach of a confidential relationship"). Moreover, the inadequacy of measures taken by the trade-secret owner to protect the secret cannot alone render a means of acquisition proper. So long as the precautions taken were reasonable, it doesn't matter that the defendant found a way to circumvent them. Indeed, even if the trade-secret owner took no measures to protect its secret from a certain type of reconnaissance, that method may still constitute improper means.

註25：If the scraping attack constituted "improper means" a question that the magistrate judge also

“不構成營業秘密”，故所有指控不當取用這些報價的主張都必然失敗。[26]然而上訴法院認為，即使承認個別報價本身無權作為營業秘密受到保護，但這本身並不能解決整個資料庫實際上是否被盜用的問題。即使單獨報價不是營業秘密，獲取足夠的單獨報價在某些時候也必定相當於不當取用潛在的秘密。否則，法律明確規定的“彙編”營業秘密保護就沒有實質內容。法院並引用Penalty Kick Mgmt., 318 F.3d at 1292-1293見解作為作證（“未經授權的使用無需擴展到營業秘密的每個方面或特徵；使用營業秘密的任何實質性部分都足以使行為者承擔責任。”。[27]上級法院認為地方法院設定之議題即取用的內容是否受到單獨保護是錯誤的；真正關鍵的問題應該是：(1)被告獲取的資料塊是否足夠

failed to address it would be difficult to escape the conclusion that the defendants either (1)used a trade secret of which they had improperly acquired knowledge or (2)used a trade secret of which they had acquired knowledge from a person whom they knew or had reason to know had improperly acquired the knowledge. See Fla. Stat. §688.002(2)(b)(1), (2)(a). [**44] The defendants admitted both to hiring the hacker and to observing her take actions consistent with a scraping attack. It's hard to see how the defendants didn't at least "have reason to know" that Natal had acquired knowledge of a trade secret for them by improper means if, indeed, the scraping attack amounted to improper means. The magistrate judge's failure to consider this possibility must also be rectified on remand.

註26：Transformative Database couldn't have been misappropriated by acquisition in the 42 case because the individual quotes that Natal scraped were freely available to the public. True, the quotes' public availability is important to the first prong of trade-secret misappropriation the initial determination whether a protectable secret exists. HN36[ ] Public availability creates a vulnerability, which if unreasonable could be inconsistent with the reasonable precautions requisite to trade-secret protection. See Fla. Stat.§688.002(4)(b). But here the magistrate judge found that the Transformative [**45] Database was a trade secret; he gave judgment for the defendants because he believed that the public availability of the quotes precluded a finding of misappropriation. The magistrate judge reasoned that all "claims in the 42 case, alleging misappropriation of these quotes, necessarily fail" simply because the individual quotes were available to the public and thus did "not constitute trade secrets." Compulife Software, 2018 U.S. Dist. LEXIS 41111, at *45.

註27：That is incorrect. Even granting that individual quotes themselves are not entitled to protection as trade secrets, the magistrate judge failed to consider the important possibility that so much of the Transformative Database was taken in a bit-by-bit fashion that a protected portion of the trade secret was acquired. The magistrate judge was correct to conclude that the scraped quotes were not individually protectable trade secrets because each is readily available to the public but that doesn't in and of itself resolve the question whether, in effect, the database as a whole was misappropriated. Even if quotes aren't trade secrets, taking enough of them must amount to misappropriation of the underlying secret at some point. Otherwise, there would be no substance to trade-secret protections [**46] for "compilations," which the law clearly provides. See HN37[ ] Fla. Stat. § 688.002(4) ("'Trade secret' means information, including a... compilation."); Unistar Corp. v. Child, 415 So. 2d 733, 734 (Fla. Dist. Ct. App. 1982) (holding that a "distillation of"

大，足以構成對轉型資料庫本身的侵占，以及(2)他們使用的手段是否不當。[28]

三、AirFacts, Inc. v. De Amezaga

AirFacts公司的主要產品是TicketGuard，這是一款用於分析航空公司和旅行社的機票價格的審計軟體，以確保機票以適當的價格出售。TicketGuard的算法將機票價格與佣金、稅費和航空業規則（例如航空公司關稅出版公司（“ATPCO”）收集的規則）進行比較。AirFacts員工通過將機票資料輸入TicketGuard來執行自動審核，並記錄門票的正確價格。如果該價格與機票銷售價格不同，AirFacts會向出售機票的航空公司或旅行社發出借項通知單，並由接受審核的航空公司或旅行社處理退款流程。AirFacts還審核航空公司和旅行社的機票退款，但不為其處理機票退款本身。Diego de Amezaga於2008年至2015年間在AirFacts擔任該公司程式開發主管。

離職大約一個月後，de Amezaga使用他的AirFacts員工憑證遠端登錄並下載了兩個流程圖，顯示源自ATPCO及其票價規則系統的票價規則（“流程圖”）。該流程圖係de Amezaga在AirFacts花費約四個月的時間所創，顯示規則、相關處理訊息和“來自（他的）腦袋的東西”，以使AirFacts員工更系統、更輕鬆地審核票證。下載流程圖後，他將之作為工作履歷提交給一家旅行社。AirFacts指控de Amezaga將流程圖發送給旅行社盜用了AirFacts的營業秘密。

依據MUTSA，AirFacts必須證明(1)它擁有營業秘密，並且(2)被告取得該秘密及(3)被告知悉或應知悉該秘密係透過不當手段獲得。[29]MUTSA將營業秘密定義為訊息，包括公式、模式、彙編、程序、設備、方法、技

publicly available information was a protectable trade secret). And total, stem-to-stern appropriation is unnecessary to establish liability; appropriation of a "substantial portion" is sufficient. Cf. Penalty Kick Mgmt., 318 F.3d at 1292-1293 ("The unauthorized use need not extend to every aspect or feature of the trade secret; use of any substantial portion of the secret is sufficient to subject the actor to liability." (quoting Restatement (Third) of Unfair Competition § 40 cmt. c (1995)).

註28：The magistrate judge treated the wrong question as decisive namely, whether the quotes taken were individually protectable. He left undecided the truly determinative questions: (1)whether the block of data that the defendants took was large enough to constitute appropriation of the Transformative Database itself, and (2)whether the means they employed were improper. Having found that the Transformative Database was protectable generally, the magistrate judge was not free simply to observe that the portions taken were not individually protectable trade secrets.

註29：AirFacts, Inc. v. De Amezaga, 909 F.3d 84 (4th Cir. 2018).

We now turn to AirFacts' Maryland trade secrets claims. HN6[ ] "To prove misappropriation of [***1819] a trade secret [under the MUTSA], a plaintiff must show (1)that it possessed a valid trade secret, (2)that the defendant acquired its trade secret, and (3)that the defendant knew or should have known that the trade secret was acquired by improper means." Trandes Corp. v. Guy F. Atkinson Co., 996 F.2d 655, 660 (4th Cir. 1993) (citing Md. Code Com. Law §11-1201(c)(1)).

術或流程，其：(1)由於其他人不為公眾所知，無法透過適當手段輕易確定，而其他人可以從其揭露或使用中獲得經濟價值，從而獲得實際或潛在的獨立經濟價值；和(2)是在當時情況下採取合理努力保守秘密的標的。[30]在MUTSA編纂之前，馬裡蘭州應用了重述中基於因素的「營業秘密」定義，該定義在MUTSA分析中仍然有用。根據重述，營業秘密可以透過以下方式識別：(1)此資料在其業務以外的知曉程度；(2)其業務所涉及的僱員及其他人知曉的程度；(3)採取保密措施的程度；(4)該資訊對他和他的競爭對手的價值；(5)開發該資訊所花費的金額、精力或金錢；(6)他人正確取得或複製該資訊的難易度。[31]

地區法院認為流程圖不是營業秘密，因為它們只是ATPCO訊息的“概述”。但上訴法院不同意地方法院的意見，認為營業秘密既可以從保密中獲得獨立的經濟價值（至少第三方不易查明），又可以採取合理的努力來維持其保密性。儘管任何訂閱的人都可以訪問ATPCO資料，但de Amezaga先生花了幾個月的時間按特定分組對其進行彙編，並應用他的ATPCO專業知識以有用的格式顯示彙編的訊息，因此構成營業秘密。

四、HiQ Labs., Inc. v. LinkedIn[32]

LinkedIn是一家超過5億會員註冊的專業社群網站。會員發布履歷和職位列表，並與其他會員建立專業「聯繫」。根據用戶協議，會員擁有他們提交或發佈到LinkedIn的內容，並僅授予LinkedIn非獨佔許可「使用、複製、修改、分發、發布和處理」該資訊。會員可以指定其個人資料的哪些部分對公眾（即對LinkedIn會員和非會員）可見，哪些部分只有聯絡人或聯絡人之聯絡人可見。

HiQ是一家資料分析公司，它使用自動化機器人抓取LinkedIn用戶在設定公開之資訊，包括姓名、職位、工作經歷和技能，並用這些資訊以及專有的預測演算法提供“人員分析”報告給商業客戶，可用於識別最有可能

註30：information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1)Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (2)Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

註31：Md. Code Com. Law §11-1201(e). Before the MUTSA was codified, Maryland applied the Restatement's factor-based definition of "trade secret," which remains useful in a MUTSA analysis. Trandes, 996 F.2d at 661. Under the Restatement, HN8[ ] a trade secret can be identified by:
(1)the extent to which the information is known outside of his business; (2)the extent to which it is known by employees and others involved in his business; (3)the extent of measures taken by him to guard the secrecy of the information; (4)the value of the information to him and to his competitors; (5)the amount or effort or money expended by him in developing the information; (6)the ease or difficulty with which the information could be properly acquired or duplicated by others.
Restatement (First) of Torts §757 cmt. b.

註32：HiQ Labs., Inc. v. LinkedIn, 938 F.3d 985 (9th Cir. 2019).

被挖走的員工。另一個分析是技能映射器，總結了員工的整體技能。

然而，LinkedIn發布了一款新產品Talent Insights，該產品可分析其用戶資料，為企業提供類似HiQ之分析。約莫於此同時，LinkedIn向hiQ發出警告函，聲稱hiQ違反了用戶協議，並要求hiQ停止從LinkedIn伺服器存取和複製資料，並稱其有違反《電腦詐欺和濫用法》（“CFAA”）、《數位千禧年版權法》（“DMCA”）、《加州刑法典》§502(c)和加州普通法的侵入法，並指出其已「實施技術措施，透過偵測、監控和阻止抓取活動的系統，阻止hiQ造訪並協助其他人造訪LinkedIn網站」。

HiQ則要求LinkedIn承認hiQ訪問LinkedIn公共頁面的權利，並聲請法院核發禁制令，確認LinkedIn不能合法援引CFAA、DMCA、加州刑法典第502(c)條或美國普通法禁止其造訪公共頁面。地方法院批准了hiQ的聲請，令LinkedIn撤回其停止函，消除hiQ存取公共資料的任何現有技術障礙，並避免採取任何法律或技術措施來阻止hiQ存取公共資料。LinkedIn則提出上訴。

法院核發禁制令的標準，係原告必須證明有本案勝訴可能性，且在欠缺暫時救濟的情況下，可能會遭受不可挽回的傷害，依平衡理論應對他作成有利認定，並且核發禁制令符合公共利益。而上級法院審查之標準，係地方法院是否有濫用裁量權。而對相關因素的評估或權衡，若有“不合邏輯、難以置信或沒有記錄支持”的情形，則屬於濫用裁量權。

關於HiQ若欠缺暫時救濟，其營運將受不可挽回的傷害，此點上級法院同意地方法院的認定。在審酌橫平理論上，LinkedIn稱，即便使用者將履歷設為公開，也不代表同意第三方以任何方式及理由利用該資訊，且舉出該平台的「請勿廣播」（即使用者履歷更新資訊將不推播給聯絡人）功能廣受歡迎為佐證，此功能使得員工得避免僱主知悉其在搜尋新職缺。然而，LinkedIn本身之獵頭服務允許獵頭公司在使用者所不知悉的情況下追蹤使用者的動態更新，以便在最佳時機接觸該使用者，公開履歷的使用者對自身隱私之期待恐怕不高。權衡此低度隱私期待利益（或者領英禁止HiQ抓取履歷的利益）及HiQ繼續營業之利益，要以後者為重要。對於領英禁止他人搭便車的論點，上級法院則回覆，因為使用者對其履歷保有所有權，LinkedIn對於使用者提供之資料欠缺受法律保護之財產利益（LinkedIn has no protected property interest in the data contributed by its users, as the users retain ownership over their profiles.）。就公共利益的斟酌，上級法院同意地方法院的觀點，若允許LinkedIn自由裁量誰可以收集和使用資料而這些資料不屬於該公司所有，該公司以其他方式公開提供給公眾，且公司自己收集及使用－可能會造成資訊壟斷，從而損害公共利益。

五、豬豬快租案

公平交易法第25條規定：「除本法另有規定者外，事業亦不得為其他足以影響交易秩序之欺罔或顯失公平之行為。」同法第42條規定：「主管機關對於違反第21條、第23條至第25條規定之事業，得限期令停止、改正

其行為或採取必要更正措施，並得處新臺幣5萬元以上2,500萬元以下罰鍰，屆期仍不停止、改正其行為或未採取必要更正措施者，得繼續限期令停止、改正其行為或採取必要更正措施，並按次處新臺幣10萬元以上5,000萬元以下罰鍰，至停止、改正其行為或採取必要更正措施為止」。又公平交易法第25條所稱「顯失公平」，係指以顯然有失公平之方法從事競爭或營業交易者。顯失公平之行為包括以損害競爭對手為目的之阻礙競爭、榨取他人努力成果、不當招攬顧客、不當利用相對市場優勢地位、利用資訊不對稱之行為及妨礙消費者行使合法權益等類型，而抄襲他人投入相當努力建置之網站資料，混充為自身網站或資料庫內容，藉以增加自身交易機會，即為常見「榨取他人努力成果」類型之一。

豬豬快租以爬蟲技術擷取591房屋網、樂屋網及信義好好租之出租物件資訊，將部分欄位資料充作自身豬豬快租App之內容，將出租物件資訊提供給使用者，其中以擷取自591房屋網的數量最多。豬豬快租App以廣告版位提供給廣告媒合服務業者使用，並獲取廣告費用之分潤。

公平會認為，豬豬快租逕自擷取並使用591房屋網出租物件資訊，作為自身App之內容，並以此招攬使用者下載、付費購買租屋雷達服務、銷售廣告版位等商業交易行為，賺取付費服務項目及廣告分潤之行為，核屬「抄襲他人投入相當努力建置之網站資料，混充為自身網站或資料庫之內容，藉以增加自身交易機會」之榨取他人努力成果。

公平會說明，經營者首先必須吸引足夠數量之房東及房客加入同一個平台，才能提升租屋網站之價值。豬豬快租將原本造訪591房屋網欲檢索出租物件之房客，自身App而瓜分591房屋網所投入之努力，也會因為平台兩邊間接網路效應，降低591房屋網對於房東之價值。此外，591房屋網之網頁也有廣告版位，而網站廣告版位的價值取決於造訪網站的網路流量，而591房屋網之網路流量遭到豬豬快租瓜分，有減損591房屋網出租物件刊登客源及其廣告版位商業價值之虞。本案豬豬快租所為係足以影響交易秩序之顯失公平行為。

經營591房屋網之數字科技公司另行依公平法向豬豬快租請求停止侵害及損害賠償，智慧財產及商業法院107年度民公訴字第8號判決認定「被告豬豬科技有限公司應將本院於民國108年8月30日107年度民公訴字第8號中間判決附表二所示攝影著作，自「豬豬快租」手機AP移除；又應移除「豬豬快租」手機App所設定搜尋、存取、點選、連結原告「591房屋交易網」網路平台及「591房屋交易」手機App之內建瀏覽介面及物件資訊，且不得再以任何網路平台或手機App介面形式提供搜尋、點選、連結及存取原告之前開物件資訊，並不得於「豬豬快租」手機App頁面呈現擷取自原告「591房屋交易網」網路平台及「591房屋交易」手機App之物件圖片及詳細物件資料。」，而該獲二審法院維持（智慧財產及商業法院109年度民公上字第2號民事判決），該案目前上訴最高法院審理中。

六、住通搜尋系統案

住通搜尋系統係不動產專門搜尋系統。只要鍵入不動產地段或地址、價格、屋齡或坪

數面積，就會搜尋並例出各家房仲業者相同條件的不動產，其盈利模式為收費會員制。房仲業者台灣房屋對住通搜尋系統提起民事訴訟，主張該公司違反公平法。本件各審級雙方勝敗互見。智慧財產及商業法院104年度民公上字第2號民事判決認定：「上訴人（台灣房屋）所屬網站上之不動產租售資料，或因上訴人信譽卓著，屋主自願提供房屋租賃資料，或上訴人投入大量人力、物力、時間，以長期建立之商譽，由眾多仲介經紀人、業務員探訪、招攬客源，並實際確認不動產之地點、面積、屋齡、使用及產權情形後，再由行政人員分類、整理、彙總、建檔等，歷經周折、繁複之程序，始登載於該等事業之網站上，惟被上訴人就上開物件之招攬或重要資訊未作任何之努力與付出，復未徵得上訴人之同意，即擅自以連結之方式連結至上訴人之網站，大量擴充為己身網站內容，使上訴人之網站功能遭到取代，且極易誤導不知情使用者，誤認其與上訴人有合作關係。被上訴人（住通搜尋系統）榨取上訴人網站所登載之不動產租售資料，擴充為己身網站之資料，以達自身經濟目的之行為，核屬榨取他人之努力成果，足以影響價格、品質、服務等效能競爭本質為中心之交易秩序，並對其他遵守公平競爭本質之競爭者而言，構成顯失公平，而具商業競爭倫理之非難性，業已違反修正前公平法第24條及現行公平法第25條之規定。」因而判處住通搜尋系統應賠償台灣房屋新台幣三十萬元。

然而最高法院108年度台上字第1240號民事判決推翻前揭智慧財產法院判決，認定：「上訴人（台灣房屋）為房屋仲介業者，提供房屋買賣居間服務以收取報酬；被上訴人（住通搜尋系統）建置之系爭系統，係提供房地產出售資訊搜尋整合平台，採付費會員制，使用者設定一定之搜尋條件（包括物件地址、價格坪數、房屋形態、樓層建築形式、房仲品牌等），進行搜索比對後，提供符合設定條件之各大房屋仲介業者官方網站之不動產銷售資料等事實，為兩造所不爭。本件經原審及第一審當庭操作系爭系統，顯示輸入搜尋條件後，所得符合條件之物件，可點選連結至刊登該物件資訊之房屋仲介公司網站，堪認被上訴人抗辯系爭系統顯示之物件地址，係依上訴人公開網站提供之物件資訊，以電腦進行綜合比對後所得之結果，並未侵入使用上訴人內部物件資料等語，為可採信。又被上訴人係提供房屋物件資訊整合之服務，以向會員收費方式收益，上訴人則為房屋仲介服務業，以與房屋買賣雙方簽立仲介合約、收取成交之佣金收益，且有專屬經紀人，可見被上訴人與上訴人從事之服務內容明顯不同，難認為同業而有妨礙上訴人所營房屋仲介業務自由競爭之情形。再者，系爭系統僅係單純提供房屋資訊蒐集、整合及連結之功能，並未直接顯示物件之詳細資訊，亦無從事仲介服務，且搜尋結果設置連結回房屋仲介公司網站，而未有何積極欺瞞或消極隱匿重要交易資訊致引人錯誤之欺罔行為。此外，系爭系統係利用自行開發之電腦軟體，未限制使用對象，將社會大眾皆可搜尋所得之公開資料，進行整合為更有利消費者使用之資訊，亦難認有不當榨取他人努力成果而有顯失公平之情事。」

伍、比較與討論

一、以法院案件而言，學者針對公司執營業秘密為理由行資料壟斷之實之憂慮似尚未在訴訟案中發生

承前述，歐盟學者擔憂，因為現實的任何組成部分大多是可計算和可轉換為資料的，而海量資料已漸經成為使任何類型的活動、商品或服務成為可能的基礎設施，若此等資料受營業秘密法保護，那麼廣泛的資料專有體系就是一種可能的，則全球經濟可能轉為“新封建制”，由智慧財產權（和資料）所有者坐鎮頂峰。

學者擔憂我們生存的世界將被量化，而資料的控制者因為得主張資料營業秘密之緣故，得進而宰制全世界的重要經濟活動。本文觀察歐盟、美國及我國之相關案例，並依照個案重要特性整理如下：

案件	最原始資料來源	最原始資料來源是否含個資[33]	最原始資料來源是否對外公佈	原告是否對資料加工[34]	資料庫資料是否對外開放	是否為營業秘密
Lyft	會員行為	是	否	否	否	是
Compulife	人壽公司保費	否	是	是	是	是
Airfacts	職業公會守則	否	是	是	否	是
HiQ Labs	會員提供資訊	是	是	否	是	否
豬豬快租	會員提供資訊	否	是	否	是	未主張[35]
住通搜尋	會員提供資訊	否	是	否	是	未主張[36]

本文發現美國的案例較多，且在Lyft及Compulife的案件中確實某種程度展現資料控制者自原始資料來源（可能是對外公開的產業訊息、或者消費者行為或提供之內容）搜集資料集結成資料庫後，主張資料應受營業秘密保護。我國的案例部分，則因為資料控制者之商業模型需將資料廣為人知，似因評估不符營業秘密法保護要件而皆未主張之。本文未查得歐盟國家相關案例。

然而，訴訟案例不多並不代表歐盟學者擔

註33：原始資料是否涉及個資，涉及資料之「所有權」歸屬於個人還是資料控制者；個資之範圍在各國容有差異，例如cookie在我國法下並非個資，惟在歐盟「一般資料保護規則」（General Data Protection Regulation, GDPR）下則是個資。

註34：在資訊領域，常見對搜集而來之原始資料予以加工，其主要的原因主要有三者，一來避免侵害原始內容著作權之疑慮，二來有機會對加工後的內容主張權利（作為排除第三者未得同意直接取用的理由），三來避免客戶直接找原始來源合作而遭跳過。

註35：公平會及法院均認為，豬豬快租構成榨取他人努力成果，顯失公平，違反公平法。

註36：法院不認為兩造為同業，而有妨礙房屋仲介業務自由競爭之情形，住處通未違反公平法。

憂並不存在。相反地，更可能的原因係資料控制者實際上不揭露資料，外人也無從得知，則即毋庸透過法律手段主張營業秘密保護。

二、《資料法》（Data Act）若訂定落實，未來歐盟極可能成為何種資料得構成營業秘密的風口浪尖

歐盟執委會發布的新聞指出，由於物聯網技術的不斷推出以及感測器產生的大量資料，資料控制者事實上可以獨占互聯產品產生的資料，如果不解決這一問題，《資料法》中規定的權利，即資料存取及可攜性將受到阻礙。[37]

（一）《資料法》與營業秘密相關之段落

在本文撰寫時，《資料法》目前仍在草案階段，已經過歐盟執委會提出，目前由歐洲議會（European Parliament）部長理事會（Council of the European Union）一讀，未來有機會成為歐盟法規範，故值得吾人注意。《資料法》第2條該法規制的對象為：(a)歐盟市場上產品的製造商和相關服務的供應商以及此類產品或服務的使用者；(b)向歐盟資料接收者提供資料的資料持有者；(c)歐盟內可取得資料的資料接收者；(d)公共部門機構和聯盟機構、機關或機構，在為執行公共利益而執行的任務特別需要數據的情況下，要求數據持有者提供數據，以及提供這些數據的數據持有者響應此類請求；(e)向歐盟客戶提供此類服務的資料處理服務提供者。

本文將《資料法》處理營業秘密之相關條文臚列如下：

草案前言第28點指出，使用者應可以自由地將資料用於任何合法目的。這包括將**使用者根據本條例行使權利而收到的資料提供給提供可能與資料持有者提供的服務競爭的售後服務的第三方，或指示資料持有者這樣做**。資料持有者應確保提供給第三方的資料與資料持有者本身能夠或有權透過使用產品或存取而存取的資料一樣準確、完整、可靠、相關且最新。相關服務。**處理資料時應尊重任何營業秘密或智慧財產權**。重要的是要保持對產品的投資動機，這些產品的功能是基於產品內建感測器資料的使用。因此，該法規的目的應理解為促進新的創新產品或相關服務的開發，刺激售後市場的創新，同時也刺激利用資料開發全新的服務，包括基於各種資料的服務。產品或相關服務。同時，**其目的是避免損害對獲取資料的產品類型的投資激勵，例如利用資料開發競爭產品**。[38]

草案第4條規範使用者存取和使用因使用產

註37：European Commission, Data Act-Questions and Answers, 28 June 2023, available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114 (last visited October 1, 2023).

註38：Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN (last visited October 1, 2023).

品或相關服務而產生的資料的權利，「1.當使用者無法從產品直接存取資料時，資料持有者應及時、免費並在適用的情況下持續向使用者提供其使用產品或相關服務所產生的資料並且是即時的。在技術可行的情況下，這應基於透過電子方式提出的簡單請求來完成。2.資料持有者不得要求使用者提供超出第1款規定的驗證使用者性質所需的任何資訊。資料持有者不得保留任何有關使用者存取所請求資料的資訊，除非對於正確執行使用者的存取請求以及資料基礎設施的安全和維護而言是必要的。**3.只有在採取所有具體必要措施保護營業秘密（尤其是對第三方而言）的情況下，才可揭露營業秘密。資料持有者和使用者可以商定採取措施保護共享資料的機密性，特別是與第三方相關的機密性。4.使用者不得使用根據第1款所述請求所獲得的資料來開發與資料來源產品競爭的產品。**」[39]

草案第5條規範與第三方共享資料的權利，其中第8項規定「營業秘密僅在為實現使用者與第三方約定的目的所必需，且第三方已採取資料持有者與第三方約定的所有具體必要措施的情況下，始得向第三方揭露。一方保守營業秘密的機密性。在這種情況下，資料

The user should be free to use the data for any lawful purpose. This includes providing the data the user has received exercising the right under this Regulation to a third party offering an aftermarket service that may be in competition with a service provided by the data holder, or to instruct the data holder to do so. The data holder should ensure that the data made available to the third party is as accurate, complete, reliable, relevant and up-to-date as the data the data holder itself may be able or entitled to access from the use of the product or related service. Any trade secrets or intellectual property rights should be respected in handling the data. It is important to preserve incentives to invest in products with functionalities based on the use of data from sensors built into that product. The aim of this Regulation should accordingly be understood as to foster the development of new, innovative products or related services, stimulate innovation on aftermarkets, but also stimulate the development of entirely novel services making use of the data, including based on data from a variety of products or related services. At the same time, it aims to avoid undermining the investment incentives for the type of product from which the data are obtained, for instance, by the use of data to develop a competing product.

註39：1.Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.

2.The data holder shall not require the user to provide any information beyond what is necessary to verify the quality as a user pursuant to paragraph 1. The data holder shall not keep any information on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure.

3.Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.

作為營業秘密的性質以及保密措施資料應明訂於持有者與第三方之間的協議中。」[40]

草案第6條資料持有者提供資料接收者資料的條件，其中第2項規定「第三方不得(e)使用其收到的資料來開發與所存取資料的來源產品競爭的產品，或為此目的與其他第三方共享資料。」[41]

草案第8條資料持有者提供資料接收者資料的條件，其中第6項規定「除非歐盟法律（包括本條例第6條）或實施歐盟法律的國家立法另有規定外，（義務人）不因具備向資料接收者提供資料的義務，而有義務揭露歐盟營業秘密保護指令定義下之營業秘密。」[42]

草案引發企業對於揭露營業秘密之疑慮，在西門子及SAP向歐盟執委會主席的聯合聲明中稱該法案：「它不僅要求與用戶共享資料，還要求與第三方共享資料，包括核心技術和設計資料，從而有可能損害歐洲的競爭力。實際上，這可能意味著歐盟公司將不得不向第三國競爭對手披露資料，特別是那些不在歐洲運營且《資料法》的保障措施將無效的公司」，歐盟執委會對此回應《資料法》將不變更歐盟營業秘密保護指令或各國營業秘密之保護，然而重要的是不得以營業秘密做為拒絕提供資料的藉口。[43]

（二）《資料法》操作面問題探討

1.草案的前言第28點稱：使用者根據本條例行使權利而收到的資料提供給提供可能與資料持有者提供的服務競爭的售後服務的第三方，或指示資料持有者這樣做，相對的，第2條第6項規定第三方不得(e)使用其收到的資料來開發與所存取資料的來源產品競爭的產品，或為此目的與其他第三方共享資料。

乍看，草案的前言跟第2條第6項(e)款似乎產生衝突，究竟使用者是否能從資料持有者處索取資料，提供給售後服務第三方（該第三方與資料持有者處於競爭關係）？前言對此是肯定的，而第

註40：8 Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret. In such a case, the nature of the data as trade secrets and the measures for preserving the confidentiality shall be specified in the agreement between the data holder and the third party.

註41：The third party shall not: (e)use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose;

註42：6. Unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.

註43：Foo Yun Chee, EU draft Data Act puts trade secrets at risk, Siemens, SAP say, May 9, 2023 https://www.reuters.com/technology/siemens-sap-say-eu-draft-data-act-puts-trade-secrets-risk-2023-05-07/ (last visited September 27, 2023).

2條第6項(e)款似乎是否定的。然而，若將第2條第6項(e)款解讀為從零到一開發競品，或許使用者得對售後服務第三方得提供資料的界限在於，該售後服務第三方本身已經與資料持有者處於競爭關係時可以提供資料，若還未處於競爭關係則不可以。然而資訊之應用千變萬化，是否為競品往往不易界定。舉前述住處搜尋系統案為例，智慧財產法院認為住處搜尋系統與台灣房屋有競爭關係，最高法院卻認為台灣房屋為房屋仲介服務業，以與房屋買賣雙方簽立仲介合約、收取成交之佣金收益，且有專屬經紀人，兩者服務內容明顯不同而無競爭關係。

草案之預想情境應該是資料持有者之商品或服務及售後服務分屬二個市場，欲透過資料可攜性規範，讓消費者在選擇資料持有者之商品或服務後，在售後市場亦得自由選擇廠商。然而售後服務是否僅限於維修，或也包含在此基礎上提供加值服務、開外掛？以及，縱使是純粹進行維修售後服務的廠商，有朝一日，是否有可能被競爭對手收購？是否應全盤禁止此類收購或注資，或者在內部設立防火牆為已足？

2.《資料法》第4條3項稱，只有在採取所有具體必要措施保護營業秘密（尤其是對第三方而言）的情況下，才可揭露營業秘密。資料持有者和使用者可以商定採取措施保護共享資料的機密性，特別是與第三方相關的機密性。

然而資料持有者與使用者間處於一對多數的情形，難以期待資料持有者與使用者個別磋商共享資料之機密性，個別磋商之法遵成本將相當可觀。此外，消費者群眾如此龐大且智識落差甚大，縱使在形式上讓消費者透過點擊（click-through）同意保密協議，究竟有多少比例會實際看過、或讀懂保密協議細部內容並遵守之？而在技術層面，有什麼機制可以讓他們攜資料去供維修，又不會營業秘密外洩？目前尚較難想象。

3.如同歐盟執委會強調「重要的是不得以營業秘密做為拒絕提供資料的藉口」（參本文第28頁），由於營業秘密三要件解釋上具有相當之彈性，歐盟學者已呼籲：「《資料法》草案應在前言中澄清：個別、原始或未處理的資料不得作為營業秘密受到保護，並且《資料法》之適用範圍應包含推斷和派生資料以及多個使用者的聚合資料集」[44]，以試圖將原始資料排除於營業秘密保護範疇之外。此類討論，恰正呼應了前述學者懷疑Amazon係基於營業秘密而拒絕提供資料（參本文第3頁），以及Lyft案上下車之郵政編碼被美國二個審級之法院均認定為營業秘

註44：Aplin, T., Radauer, A., Bader, M.A. et al. The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis. IIC 54, 826-858 (2023) at 854. https://doi.org/10.1007/s40319-023-01325-8.

密（參本文第7頁）之正反意見。

4.營業秘密成立的條件在僅有少數人知悉的基礎上，如果某一資料越來越多人知道，例如坐擁近10億台裝置銷售成績之Alexa[45]，假設使用者均要求亞馬遜提供資料給使用者自身及其指定的維修公司，即便假設全體均簽保密協定並且嚴格遵循之，有無可能就資料當中之共通部分（去除使用者個別之資料）因量變而質變，使得逾全世界人口10%已知之資料共通部分不是營業秘密了？

陸、結論

以今日之資訊技術與運算能力而言，現實的任何組成部分大多是可計算和可轉換為資料的，而海量資料已漸經成為使任何類型的活動、商品或服務成為可能的基礎設施，前述歐盟學者擔憂，若此等資料受營業秘密法保護，則全球經濟可能轉為“新封建制”。本文梳理歐盟、美國及我國之相關案例，認為目前雖然沒有諸多資料相關營業秘密訴訟，然而此原因係基於資料控制者透過技術上之保密措施達成，而此“新封建制”確是現在進行式。

舉例而言，熱門人工智慧工具ChatGPT是OpenAI公司的產品。OpenAI在2019年轉型為營利事業OpenAI LP[46]，有OpenAI Inc.作為無限責任合夥人（general partner）控制，微軟作為有限責任合夥人（limited partner），微軟是OpenAI最大的投資者，與OpenAI簽有專屬商業夥伴合約，能利用OpenAI未向外界發表的特殊服務，將使用者所擁有的資料如email、對話記錄、Word、PowerPoint文件做為訓練資料，搭配其大型語言模型，來協助產出更符合個別使用者的專屬AI助理。這項服務已整合至Microsoft 365 Copilot、Bing Chat Enterprise中。而這些使用者資料，並不會返遺回OpenAI去訓練其大型語言模型。[47]ChatGPT透過世界各地超過一億人使用者的回饋，訓練增強其人工智慧模型，而將此資料提供給微軟，但微軟並無回饋資訊之義務。其他巨頭，例如谷歌、臉書、亞馬遜及特斯拉亦當然無將資料

註45：國家實驗研究院科技政策與資訊中心，科技產業研究室，Alexa在生成式AI加持下，成為通往智慧家庭的最後一哩路？2023年9月26日，https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=20034&fbclid=IwAR3vlZyAY7yT2l-dPaizobNSJgMz35CBKtIRMMnJ-LlcxUzGqGU_wxFMpmw_aem_AbiIQPmRH-1Bi-i4N6B_8v3ynXhzdezrnG9ywALZC4v2APQ6I0Z8DZIc6RvfQm3Q4y0（最後造訪：2023年10月1日）。

註46：David Coldewey, *OpenAI shifts from nonprofit to 'capped-profit' to attract capital*, March 12, 2019, https://techcrunch.com/2019/03/11/openai-shifts-from-nonprofit-to-capped-profit-to-attract-capital/ (last visited October 1, 2023).

註47：Microsoft, Data, Privacy, and Security for Microsoft 365 Copilot, September 27, 2023, https://learn.microsoft.com/en-us/microsoft-365-copilot/microsoft-365-copilot-privacy (last visited October 1, 2023).

回饋或公開之義務。

當今技術資訊發展之智慧財產權保護主要建立在二大對立的模型上，一是期使技術擁有者將技術公開而予以特定年限壟斷保護之專利，二者是千年來最傳統之技術保護方式，即技術予以祖傳秘方、獨門暗器保密不傳外人。當前資訊產業領域隱約呈現百年前專利制度實施以前，各工匠以秘密方式保護其技術而各陣營壁壘分明的態勢。本文提出以下二點方向供思考：

大數據資料是否應由類似專利制度，以一定年限給予專屬權利之方式予以保護作為公開之條件，而何等誘因足夠促使資料控制者願意公開？

營業秘密保護之法律效果相當嚴重（如我國有刑事處罰），個別、原始或未處理的資料或許應一概不得作為營業秘密受到保護，如個案有嚴重違反商業倫理之情形應循公平交易法救濟而使得罪刑相當？

可以預期未來若《資料法》草案通過落實，原本深藏於各陣營之海量數據被依法要求提出，而在大數據當中之何種成分構成營業秘密、何種成分為不受保護之資料，將在各種案例情境中被反覆辯論。