大數據應用下個人資料定義的檢討：以我國法院判決爲例

葉志良

摘要

大數據應用技術對資訊經濟、科學發展與商業利益帶來極大貢獻，然而資訊主體經常於不知情下被他人蒐集其各種資料，滋生隱私侵害疑慮，不過隱私保護須與社會其他價值進行權衡，或可透過去識別化作法，以確保資料處理合法性。法律雖對個資有其定義，但是否所有與個人有關之資訊皆屬值得保護之個資，有其疑問。本文透過檢討2014年一則司法判決，探討行動電話用戶之所屬電信業者別是否屬於法律所保護之個資，結論提出不可合理期待之隱私資訊，或經適度去識別化後可供利用之資訊，應可運用於大數據時代資料的探勘與分析，以創造資料經濟之效率，並有利於公共利益與福祉之最大化。

⊙ 關鍵字：巨量資料、大數據、個人資料保護法、個人資料、匿名資料、去識別化、重新識別、號碼可攜服務

⊙ 本文作者葉志良為元智大學資訊傳播學系助理教授。

⊙ 聯絡方式：E-mail：chyeh@saturn.yzu.edu.tw；
電話：03-463-8800 分機2640；通訊處：32003桃園市中壢區遠東路135號 元智大學資訊傳播學系（60915R）

⊙ 收稿日期：2016/04/27　接受日期：2016/08/17

The Adjustment of the Definition of Personal Information in the Age of Big Data: From a Perspective of Court case

Chih-Liang Yeh

Abstract

The technologies of big data applications can help private and public sectors analyze predictive information and thus to develop new services. However, the data subjects are often unware of their personal data collected by others and generates the concerns of privacy invasion. We should weigh the value of the privacy protection among other societal values. The data protection law defines the personal data; however, it is controversial whether all the information related to specific individual deserves the legal protection. This paper attempts to analyze a court case in 2014 to discuss whether the name of mobile carrier belongs to the personal data of such a subscriber. It concludes that the unreasonable expectation of privacy information or the appropriately de-identified information that is available for public use can make use of data mining and analytics in the era of big data and thus create the efficiency of the data economy and is beneficial to the public interest.

⊙ Keywords: Big data, Personal Data Protection Law, personal data, anonymous data, de-identification, re-identification, number portability

⊙ Chih-Liang Yeh is Assistant Professor in the Department of Information Communication, Yuan Ze University..

⊙ E-mail: chyeh@saturn.yzu.edu.tw

壹、前言與問題意識

今日社會民眾透過各式裝置的連網使用、網路購物、雜誌訂閱、商品型錄、問卷填寫、商品保證書回覆等資訊運用進行產品與服務的消費，而政府部門也仰賴電腦與網路透過各式資訊提供公共服務。這些與個人相關的資料，透過大量線上（on-line）與離線（off-line）的活動，不斷地生成、傳遞與利用。根據統計，平均全球每一分鐘即可產出1,700兆bytes（等同36萬片DVD）的資料量，平均每人每天會產出6MB的資料量[1]，資料量的暴增已是目前資訊社會的常態 （Cukier, 2010）。

「資料經濟」（Data Economics）已成爲國際間熱烈討論的議題，資料儼然與物質與能源並列爲重要的經濟資源，其與其他經濟資源最大的差異點，在於資料並不因爲使用而消耗，反而可以不斷的重組而再利用，而且越經使用其價值越高。當大量多元的資料與具備大量、快速與多元（Volume, Velocity, Variety, 3Vs）之大數據資料統計分析應用技術（Big Data Analytics）結合時，可將技術用以尋求各種結構化、非結構化或半結構化的資料間的關聯性，或至各式統計分析應用至科學研發、醫療保健、組織管理、趨勢預測等各領域之產品或服務。

時下熱門的大數據技術，即是透過業者所大量儲存使用者的使用紀錄，例如在智慧手機的脈絡下，包括終端固有ID、位置資訊、APP使用紀錄等，將這些有系統的資料型態透過巨量分析（analytics）與資料探勘（data mining）方式，萃取出有用或可供預測的資訊（Cohen, 2013, p.1920），幫助業者瞭解使用者行爲、進而發展新服務[2]。這種大數據技術爲資訊經濟與智慧創新開創了新的時代，也對科學與商業帶來莫大的利益，同時大數據也影響著國家政策制定的方向，譬如天然資害警報系統、天然資源最佳化以及資訊基礎建設等等。然而，這種資訊洪流下卻也隱含著個人隱私侵害的隱憂，例如資訊主體（或個資主體）在毫無察覺情況下被來自各方的大數據應用服務蒐集其行爲資料，因而產生資料完整性（data integrity）的破壞（Cohen, 2013, p.1925）；倘若處理不善，亦可能造成規範上的衝擊，嚴重者將損害資訊經濟，並箝制創意發展（Tene & Polonetsky, 2012, p. 63）。

由於各式各樣的資訊，包括個人健康紀錄、位置資料、用電資料等，越來越容易被複製且被分享至全球各地，使得維護資訊安全與保障隱私變得越來越困難，同時也

產生資料剖繪（profiling）、特定族群歧視、刻意排除或喪失資料自我控制等負面影響。一般而言，去識別化（de-identification）被視爲利用資料分析技術的同時，也能保護個人隱私，藉以獲取資料利益之利器；不過也有技術專家指出，即便資料已去除個人資料的識別性，但仍可以透過技術將去識別的資料「再識別」（re-identified）。Paul Ohm（2010, p.1731）認爲在大數據時代，資料大量產生後將會被有目的的蒐集與連結，因資料來源的廣泛性使得可供比對的數量大量增加，加上資訊技術的發展與資料辨識能力的大幅提升，使得資料越來越難以保持匿名化狀態，而這種再識別科技的發展將可能摧毀我們對匿名所欲達到隱私權保護的信心。

有鑑於大數據對隱私權帶來極大衝擊以及個人資料保護法（下稱個資法）亦有其保護的界限，本文嘗試重新檢視「個人資料」的定義，並討論因應大數據分析技術影響下，個資的定義應有調整的必要。另外，本文從臺灣臺北地方法院103年度小上字第155號民事判決關於某行動裝置應用程式（app）所引發的個資侵害判決進行討論，該案法院雖認爲app已不法利用他人個人資料而侵害其人格權，但細究個資法所欲保護之眞正意涵，本文認爲除應辨別個人資料所欲保護資訊的範圍外，尚需考量個資法對於資料使用的公益目的，特別是目前將「告知同意原則」作爲發動個資法保護主要依據的今日，將反而成爲限制大數據應用發展的桎梏。本文認爲在大數據應用對資料開發帶來極大價值的趨勢下，現今個人資料保護法制過度偏向個人隱私保護之天平應予調整，對於不可合理期待之隱私資訊，或經適度去識別化後可供利用之資訊，應可運用於大數據時代資力探勘與分析，以創造資料經濟之效率，並有利於公共利益與福祉之最大化。

---

1 European Commission, *Frequently asked questions: Public-Private Partnership (PPP) for Big Data*, Memo IP/14/1129 (Oct. 13, 2014), http://europa.eu/rapid/press-release_MEMO-14-583_en.htm (last visited July. 30, 2015); 目前人類每十分鐘所創造的資料量，大約等同於人類前一萬個世代所產出的資料量 (Goodman, 2015, p.85)；另外，非結構化資料（unstructured data）是各種資料集結的型態，在目前各組織機關所儲存的資料態樣約有超過七成以上皆是非結構化資料，但透過大數據的分析，這類資料倘若轉變成結構化資料，價值將提升許多 (Corken, 2015, p.305).

2 例如以近期爆紅的Netflix可知，業者透過歸納閱聽人收視行爲，不僅可了解閱聽人喜好，亦可選擇製作多數閱聽人喜好之內容，使內容產製的投資準確率提高，進而提高業者的投資報酬率。參見〈Netflix是如何用大數據捧紅「紙牌屋」的〉，INSIDE，2013/02/26，http://www.inside.com.tw/2013/02/26/netflix-big-data-houseof-card（最後瀏覽日：2016/7/25）。

貳、個人資料之定義及其保護界限

一、大數據革命與服務應用變革

在大數據巨大商業利益的驅使下，企業將以最大程度蒐集、處理、利用個人資料作爲提升其產業競爭力的重要手段，使得傳統個資法上的「知情同意」、「目的限定」、「資料蒐集最小化」等原則遭受嚴峻的挑戰。尤其是在資料處理喪失原有的「情境脈絡」（context）（Nissenbaum, 2010; The White House, 2014）情況下，由於資料主體本身對於個資遭他人蒐集後進行何種方式的利用往往不知情，且大數據資料分析所建構、追求的個性化服務，亦對資料主體的隱私造成莫大威脅。

不管是美國或是歐盟，對於大數據所帶來的積極或潛在利益或商機，大都是樂觀其成或積極追求，且認爲大數據各種應用應該要注意資訊隱私、個人資料保護，甚至是其他基本人權的保護。然而這些國家或地區，有共識也有分歧的地方，諸如隱私威脅程度的評估有些許不同，相對應要採取保護的手段也有所不同（Schwartz & Solove, 2014; Tsesis, 2014; Ybarra, 2011）。不過各國大多同意，大數據應用發展前提是，至少要注意資訊隱私與個資保護問題，藉以取得民眾的信賴。

大數據革命的根本在於使用者的覺醒（users' awareness）。以大數據相關應用分析來說，其提供我們對於所有事物更多的認知，也讓我們對未來能有所預測，並解決問題。舉例來說，研究人員曾分析超過68萬名波士頓居民的在該市各個基地站台之通訊紀錄，匿名追蹤每個人的通勤內容，包括各個起訖地點，並產生一幅過去從未出現、極爲細緻的市區交通型態之地圖，並揭露市區街道過去隱藏的使用型態（Wang et al., 2012）。

藉由擴張國家安全當中「情境察覺」（situational awareness）之概念（Salmon et at., 2009），大數據被稱爲是對抗恐怖攻擊的萬靈藥。根據美國國土安全法第515條所定義的「過去隱藏型態」（previously hidden pattern）[3]，其要求國家營運中心（National Operations Center, NOC）「向聯邦政府提供情境察覺以及一種共通的營運情境…並確保對政府決策者得以獲取關鍵之恐攻及與防災有關資訊。」[4]

但國家安全相關單位如何確認並逮捕恐怖攻擊之行爲人[5]？只要讓政府機關得以

事先取得各種後設資料（metadata），他們就可以根據可識別資訊（identifier）建立資料庫，例如電話號碼。倘若制度或規範上允許調查者得以調閱電腦內部在攻擊之前的資料並喚起情境察覺，透過大數據分析就可以確認誰是恐怖攻擊之嫌犯。

政府機關透過各種大數據應用，在2013年波士頓馬拉松爆炸案中展現出相當不錯的犯罪偵查效果，例如執法單位調閱波士頓基地站台的通訊紀錄，交互查證所有街道錄影資料、目擊照片，並且爲了確認嫌犯，讓執法者使用各種工具得以接觸到Twitter自2010年以來在波士頓市發送有關「炸彈」（bomb）字眼的後設資料（Konkel, 2013）。這種方法極可能找到隱藏型態，讓資料分析者得以結合其他資料以確認該攻擊事件是否會發生。一旦任一嫌犯的電話能被鎖定、確認，大數據分析即可確認恐怖攻擊的嫌疑團體。

然而，當許多人知道大數據可能對個人隱私造成侵害時，眾人開始關注隱私權的問題，但這些問題通常超越隱私權本身的概念。每個人都擔心自己的私密資訊被揭露給第三人知悉，但是大數據應用本身具有法定或營業上的機密，因此在衡量大數據預測與其對人們所帶來之影響，我們欠缺必要的透明性。另外一項值得擔心的是，目前大數據應用較傾向有利於政府或機關組織更勝於個人，然而大數據所帶來的巨大利益確實來自於個人本身的貢獻[6]。

二、大數據應用下個人資料保護制度及其界限

大數據應用本質上係追求資料開發的價值最大化，而個人資料保護的最終目的在於保障個人對於個人資料的自主控制，這兩者價值各異，實無須放置於同一天平上衡

---

3 Homeland Security Act of 2002, Pub. L. No. 107-296, § 515, 116 Stat. 2135 (*amended by* Department of Homeland Security Appropriation Act, Pub. L. No. 109-295, 120 Stat. 1355, 1409 (2006)) (codified at 6 U.S.C. § 321d(b)(1)-(2)(2012)).

4 "[P]rovide *situational awareness* and a common operating picture for the entire Federal Government…and [to] ensure that critical terrorism and disaster-related information reaches government decision-makers." Homeland Security Act of 2002, § 515, 6 U.S.C. § 321d(b)(1)-(2)(2012) (emphasis added). 該法將「情境察覺」定義爲："information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decisionmaking." Id. § 321d(a).

5 在波士頓馬拉松爆炸案發生不到24小時，經過美國聯邦調查局（FBI）抽絲剝繭，已彙整多達24TB的資料指向嫌犯者是誰（Konkel, 2013）。

6 網路文化有句名言：「如果商家爲你提供免費服務，那你就不是他們的客戶，而是他們的產品。」("If you're not paying for it, you're not the customer; you're the product being sold.")（Zittrain, 2012）。

量其輕重（Richards & King, 2014, p.409）；然倘若這兩者價值間產生交錯時，孰輕孰重仍應按法益衡量方式，或可調整既有框架（如大數據應用採取Privacy by Design概念、個資法調整其規範定義或範圍等）尋求利益最大化之解。歐盟的基本人權憲章（The Charter of Fundamental Rights of the European Union）明確指出隱私權與個人資料保護的重要性[7]，該憲章第7條規定，任何人皆須尊重他人私人生活、家庭活動與個人通訊；第8條規定，任何人皆有權利享有關於其個人的資料受到法律之保護。傳統上，隱私權著重在私人與私密事項上，對於公共場合則不予以保護。但在1967年美國聯邦最高法院在Katz案建立了「合理的隱私期待」（reasonable expectation of privacy）判斷標準，指當特定個人如主觀上具有隱私權的實質期待，同時該隱私期待在客觀上須被社會一般大眾認爲是合理的[8]，才享有隱私權的保護。

上述歐盟與美國皆承認個人資料保護屬於憲法上所保障的基本權利，但隱私權與個人資料之保護則必須與社會其他利益，包括國家安全、公共衛生、政府執法、環境保護、經濟效益，甚至言論自由，進行利益權衡，非屬絕對性的權利，而大數據所展現的社會利益，同樣也必須與其所對個人隱私造成侵害之風險進行權衡。

以美國而言，過去四十多年來，個人資料創新利用以及資訊隱私之間的緊張關係已被一系列廣義的「公平資訊實踐原則」（Fair Information Practice or Fair Information Practice Principles; FIP or FIPPs）所涵蓋[9]。直到1980年經濟合作與發展組織（OECD）制定「隱私權保護與個人資料跨境傳輸指導原則」（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）後，隱私權與個資保護逐步落實到各國的法律體制上（OECD, 1980）。美國白宮於2012年2月公布一項由商務部所提供關於FIPPs原則的報告（The White House, 2012），將個人管控（individual control）、透明性（transparency）、尊重情境脈絡（respect for context）、安全性（security）、接觸與正確性（access and accurate）、重點蒐集（focused collection）與課責性

---

7 Charter of Fundamental Rights of the European Union, *OJ* C 364/10, 18.12.2000, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

8 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

9 FIPPs是一系列國際上所認可的實踐原則，強調個人的資訊隱私極爲重要，因爲這些原則提供了許多國家在隱私權與個人資料保護上制定其內國法提供了許政策指引（Gellman, 2015）；但也有學者提出反對見解（Cate, 2006）。

（accountability）等七項原則納入隱私權與個資保護體系。而大數據各項應用的出現卻尖銳地挑戰著其中幾項基本原則，例如：保護架構之範疇（強調可辨識之個人資料）、資料蒐集最小化原則（重點蒐集）、知情同意（包括個人管控與尊重情境脈絡），以及個人利用權利（接觸與正確性）[10]。

爲使數據（資料）正向利用與個人隱私保護有所平衡，政策制定者必須在隱私權的基本概念下，重新審視包括可識別之個人資訊（Personally Identifiable Information, PII）、當事人同意與使用目的限制[11]，以及資料最小蒐集等原則（Schwartz & Solove, 2011; Sloan & Warner, 2014; Tene & Polonetsky, 2013）。

三、個人資料之定義、種類與識別性

各國法律對於個人資料的定義各有不同：歐盟資料保護指令指的是個人資料能用以辨識（identify）特定自然人或具備辨識可能性之任何資料[12]；在美國指的是能夠區別（distinguish）特定個人身分或連結（link）到特定個人之資料（McCallister et al., 2010）；在德國聯邦個人資料保護法則是指任何有關於該個人之資訊或已識別或可識別之個人（即資料主體）的實質情形[13]。

根據上述歐盟資料保護指令的規定，可識別之個人（identifiable person）是指某一個人透過身分證號碼或一項以上之專屬於其個人身分之因素，包括其個人之身體、精神、心理、經濟、文化或社會地位，可直接或間接被他人所識別[14]。根據2016年新

---

10 FTC Commissioner Julie Brill（2012）曾說：「大數據對隱私的衝擊，正需要我們投入一些嶄新且深入的思考。」

11 「其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。」（釋字第603號解釋參照）其中從釋字603號解釋可得知，憲法並未將資訊隱私權絕對化，但必須遵守該解釋所強調應以法律明定其蒐集之目的，其蒐集應與重大公益目的之達成具有密切之必要性與關聯性，並應明文禁止法定目的外之使用。

12 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, Art. 2(a) (“personal data shall mean any information relating to an identified or identifiable natural person.”)

13 Sec. 3(1) of German Federal Data Protection Act (“…any information concerning the personal or material circumstances of an identified or identifiable individual (data subject)”)。聯邦個人資料保護法（Bundesdatenschutzgesetz, BDSG）於2003年1月14日公告（BGBl. I S. 66），2009年8月14日曾修正過（BGBl. I S. 2814），最近一次修正爲2015年2月25日（BGBl. I S. 162），http://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D'bgbl115s0162.pdf'%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s0162.pdf%27%5D__1467279844276。

頒布的歐盟一般個人資料保護規則（EU General Data Protection Regulation）的第4條規定[15]，個人資料是指已識別或可識別該自然人（或稱資料主體，data subject）的任何資訊，而所謂可識別之自然人，是指透過參酌姓名、身分證號碼、位置資料、線上識別資訊，或其他一項以上之專屬於其個人身分之身體、精神、基因、心理、經濟、文化或社會身分，而可直接或間接識別之自然人。

我國個人資料保護法第2條第1款規定，個人資料係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料[16]。其中「得以間接方式識別」係指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人（個人資料保護法施行細則第3條參照）。

由於個資法保護的個資必須是具有特定個人的識別性，原則上資料管理人或其他人必須盡一切方法（take account of all the means）以該資料爲依據或線索以識別出、連結到或確認該個人之所在，倘若是單純的中獎號碼，因無從識別特定個人，即非爲個資。當該資料主體已不再可被識別，該來源不明資料即不適用於個資法之保護[17]。

關於以「間接方式」識別特定個人，參考歐洲理事會No. R (90) 19之建議案[18]，倘若必須以不合理的時間、成本或人力始能識別該個人，則該個人尚不得被認爲是「可識別」（identifiable）[19]。另根據日本個人資料保護法規定，個人資料係指可藉由姓

---

14 Article 2(a) of Directive 95/46/EC (“an identifiable person is one who can be identified, *directly or indirectly*, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”)

15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural personals 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), Official Journal of the European Union, L119/1, 4 May 2016, Art. 4(1) (“…an identifiable natural person is one who can be identified, *directly or indirectly*, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”).

16 個人資料保護法於2010年5月26日修正公布，於2012年10月施行（除第6、54條除外）；2015年12月30日部分條文修正，於2016年3月15日施行（前述第6、54條也施行）。

17 Recital (26) of Directive 95/46/EC; recital (26) of General Data Protection Regulation.

18 Council of Europe, Recommendation No. R (90)19 of the Committee of Ministers to Member States concerning the protection of 1personal data used for payment and other related operations, adopted 13.9.1990.

名、出生年月日或其他可描述該個人之資料，或有些資料雖未直接指名道姓，但一經揭露仍足以識別爲某一特定人，而且該資料容易與其他資料爲對照、組合，而藉此識別出特定個人者[20]。

由於國際間並未對於個人資料的定義與判斷標準給予統一、清楚的規定，按前述歐盟資料保護指令與新頒布的一般個人資料保護規則在定義個人資料上，僅給予較爲抽象的判斷標準，在解釋上有很大的彈性空間，藉以因應未來技術發展所面臨的情形；而我國的個資法採取列舉式的方式規定個資的定義，但仍未解決其定義模糊性的問題，而這種極爲不確定的界定方式使得實務操作上存在著極大的困擾。

綜整以上各國對於個資的定義，本文約略整理出以下三種個資類型：已識別之個人資料、可直接識別之個人資料，以及可間接識別之個人資料（如表1）。

表1：個人資料的類型

類　　型	說　　明
已識別之個人資料（*Identified* personal information）	屬於特定自然人的資料而已被識別。例如：某人在網路上揭露其個人的健康紀錄。
可直接識別之個人資料（*Directly identifiable* personal information）	對於無法辨識之資料進行蒐集、處理與利用，而可進一步識別出特定之自然人。例如：蒐集到姓名、住址等聯絡資訊而可識別出特定自然人。
可間接識別之個人資料（*Indirectly identifiable* personal information）	對於無法辨識之資料進行蒐集、處理與利用，但尚不足以識別出之特定自然人，而需要更進一步的訊息以識別該特定自然人。例如：蒐集到不知名之人的地址，但仍需要進一步的資訊(例如性別或姓名)作為識別的資訊。

19 ***Id*. Appendix to Recommendation, 1.2.**

20 **個人情報の保護に する法律，平成十五年五月三十日法律第五十七 （May 30, 2003）， http://www.japaneselawtranslation.go.jp/law/detail/?id=130&vm=04&re=02. (“第二 この法律において「個人情報」とは、生存する個人に する情報であって、 該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。”)**

四、資訊隱私之可合理期待性

隱私權概念可從1890年由美國律師Samuel Warren和Louis Brandeis二人共同於哈佛法學評論（*Harvard Law Review*）所發表之「The Right to Privacy」論文作爲濫觴，該文主張應被承認的隱私權乃在保護個人生活不受干擾、獨處的權利（right to be let alone），亦即個人有不可侵害的人格，對其思想、情緒和感受等自身事務之公開、揭露，具有決定的權利。但這種隱私權並非絕對，仍應受公共利益及本人同意之限制（Warren & Brandeis, 1890）。我國個資法之立法目的也呼應這樣的規範方向，除保障個人隱私與資訊自主權外，更有其施行之公共利益價值。

1967年美國聯邦最高法院在*Katz v. US*.一案將隱私權保障係以「人」爲核心，從原本僅限於有形之物品擴大至無形的資通訊，將原本僅限於私人處所擴大至個人在公共場所中之行爲，另外奠定了「合理的隱私期待」（reasonable expectation of privacy）判斷標準：人民在主觀上必須先有「隱私期待」，再進一步判斷此一主觀的期待於客觀上是否可被認爲是合理的。其中主觀要件的判斷，關鍵在於反面角度觀察個人是否已「自願」放棄隱私利益，藉以判斷其主觀上是否仍具有隱私期待，通常這種判斷是建立在隱私主體的「同意」與否。至於主觀的隱私期待在客觀上是否「合理」之判斷，則必須綜合參考時間與空間等相對因素，不同時代、地域、社會、科技發展與社會認知等，皆會有不同的判斷結果（林錦鴻，2007，p.70-71）。

爲因應大數據應用的發展，個資法的實施有必要考量是否符合整體社會的利益最大化，並兼顧公共福祉損害之最小化。特別是那些不具備有合理隱私期待性之隱私標的，舉例來說：

（一）無法協助識別該個人之零散、片段之資訊。例如使用「性別」作爲識別特定個人的資料集，該資料在個資法上可被認爲屬於間接識別之個資；然而，單以這項資料將難以識別特定個人，因爲以性別所劃分出來的範圍過廣。倘若所蒐集其他與性別結合之資料藉以識別特定個人，則所需花費的時間、金錢與人力難以估算。相對來說，即便該資料會可能對個人造成損害，其程度尚屬輕微，因此法院對此等可能構成「間接識別」的資訊應採取較爲限縮的解釋。由於該資料或資料集並不會對資料主體造成人格權的損害，因此並不屬於個資法之個資。

（二）該資訊係包含於其他資訊當中而成爲已知之公開資訊。一般而言，在一定範圍內資料種類越多，越容易識別出特定個人；然而，部分資料種類並無法限縮識別特定個人的範圍，例如：我國身分證統一編號包括一個開頭英文字母與接連的九個數字，其中英文字母代表出生地，A表示台北市，而F表示新北市，而第一個數字代表性別，1代表男性，2代表女性。因此，身分證統一編號本身代表三種資料集，包括出生地、性別與身分證統一編號本身。然而，身分證上所隱含的資訊（出生地與性別）其實無法作爲識別特定個人的資訊，因爲資料主體的隱私權期待顯然不合理（因皆是法定資訊）。同樣的例子也適用於住家地址、郵遞區號與網路服務的IP位址。

（三）該資訊本身並不會對個人造成損害。此指資訊主體在「主觀上」認爲該資訊未經其許可而遭他人蒐集、處理、利用將會對其造成損害，然而此一主觀的期待於客觀上並不被大多數人認爲是合理的。例如某台北市民A進入台北市立兒童新樂園而出示自己所擁有的「悠遊卡」，但A不欲讓他人知悉其「擁有」悠遊卡此項資訊，並認爲園方未經其許可而蒐集其「擁有」悠遊卡此項資訊而進行其他利用。但絕大多數的人皆認爲利用自身「悠遊卡」進入兒童新樂園是極爲正常的事情，也不認爲會對個人造成損害。

基於上述分析，特別是不具備有合理期待性之隱私資訊，或是經適度去識別化之後可加以公開而利用之資訊，應可運用於大數據時代資料的探勘與分析，以創造數據經濟之效率，並有利於公共利益與福祉之最大化。

參、臺灣臺北地方法院103年度小上字第155號民事判決介紹

自2002年起，所有電信業者皆受主管機關—國家通訊傳播委員會（通傳會）之要求，必須對其用戶提供號碼可攜服務（number portability service, NP），所有電信業者因此共同建立「號碼可攜集中式資料庫管理中心」（Centralized Number Portability Database, CNPDB）並以此資料庫管理號碼可攜服務，這項服務包括固網服務與行動服務。號碼可攜服務，係指用戶移轉至其他電信業者卻不用變更其原始的電話號碼。根據通傳會之統計，從行動電話號碼可攜服務自2005年開始提供以來至2016年3月爲

21 通傳會，號碼可攜服務統計（截至2016年6月爲止），http://www.ncc.gov.tw/chinese/files/16070/電話號碼可攜服務.pdf

止，已有超過4,000萬筆行動電話號碼移轉至其他業者的紀錄[21]（下表2）。

年份	行動攜碼生效數	固網攜碼生效數	總生效數
2005	93,858	94	93,952
2006	511,358	516	511,874
2007	2,080,264	1,093	2,081,357
2008	3,318,003	3,946	3,321,949
2009	3,220,594	8,109	3,228,703
2010	3,072,746	6,629	3,079,375
2011	3,068,243	5,102	3,073,345
2012	3,452,627	6,177	3,458,804
2013	3,457,314	4,756	3,462,070
2014	6,197,019	3,250	6,200,269
2015	8,302,682	2,823	8,305,505
2016.1	622,259	163	622,422
2016.2	652,330	225	652,555
2016.3	652,405	197	652,602
2016.4	656,475	224	656,699
2016.5	690,722	276	690,998
2016.6	628,250	236	628,486
總計	42,432,541	43,816	42,476,357

表1：號碼可攜服務生效案件數（包括行網與固網）

資料來源：通傳會（2016.7）

透過大數據技術之應用，號碼可攜服務集中式資料庫（CNPDB）是查詢用戶轉換率（churn rate）與消費者偏好等行爲分析的極佳資料來源。2012年一家行動電話公司提供一項行動應用服務（app）名爲「M+ Messenger」，其允許使用者得以知悉其手機通訊錄中之電話號碼所屬之行動電話業者別，藉以確認通訊錄中的朋友是否屬

於網內（intra-network）以享有較爲便宜的通話費率。然而，該app被某消費者告上法院，認爲該app違法蒐集並使用其個人資料，並請求因其隱私權受侵害之損害賠償。

一、事實與爭點

「T」行動電話公司開發通訊應用程式「M+ Messenger」（下稱M+），並以其關係企業「K」子公司名義推廣，而T與K爲本案之共同被告。任何行動用戶皆可在其智慧型手機上安裝此app，當開啓該app後，該軟體會依據手機中通訊錄所儲存之電話號碼，經由母公司T向CNPDB查詢該電話號碼所屬之電信業者後，接著在M+ 聯絡簿中顯示出手機原儲存之通訊錄內容，包括姓名及電話號碼，並標示出該電話號碼所屬之「電信業者別」。

原告原本爲行動電話公司「C」之用戶，後來攜碼至行動電話公司「F」，其後某日原告在友人的智慧型手機中發現M+ 介面顯示自己的行動電話業者別爲F公司，原告認爲M+ 的功能會揭露自己的行動電話公司別之資訊提供他人所知悉，認爲這屬於不法蒐集個資之行爲，因而以違反個資法第29條規定向臺北地方法院起訴，並向T與K公司請求損害賠償。

本案爭點有二：（一）個人所使用之手機電話號碼，其所屬之電信業者別是否爲個資法規範下之個人資料？（二）若是，利用號碼可攜集中式資料庫查詢後所獲得「電信業者別」之資訊，是否逾越蒐集特定目的之必要範圍而與公共利益無關，而非屬合理關聯之利用？

本案第一審（即原審）法院見解認爲，在原告手機上顯示之電信業者別資訊，屬於可得間接識別之個人資料，被告不法蒐集、利用其個人資料而侵害其權利，原告依個資法第29條、第28條及共同侵權行爲之規定，請求被告連帶賠償新台幣500元，判賠獲准（臺灣臺北地方法院103年度北小字第1360號小額民事判決）。本案被告不服，經上訴至臺北地方法院合議庭。上訴審（即本審）法院亦認爲電信業者別爲個資法所保護之個資，原告因個資遭不法侵害請求精神上損害賠償，從情理上來看並不違背。最後本審法院仍維持原審法院的見解，本案至此確定。以下分別說明原審與上訴審法院之判決理由。

二、原審法院判決理由

（一）電話號碼屬於個資法保護的個資

原審法院認爲，電話號碼資料屬於個人聯絡方式，本身雖只是一串數字組合，卻無法從中直接識別特定個人，不過該電話號碼一旦與其他個人資料，如姓名、身分證統一編號、特徵，或其他社會活動資料進行相互比對、組合、連結及勾稽等作爲，即可以間接方式識別該特定人，應該屬於個資法所保護之個資。

（二）電信業者別是個人電話號碼之附屬資料，亦是個人資料

原審法院認爲，電話號碼所屬之電信業者別，乃個人電話號碼之附屬資料，判決理由指出：「……其係得與前述其他個人資料如姓名、身分證統一編號等資料相互比對、組合、連結及勾稽後，據以作爲間接識別特定個人之社會活動資料之一，亦屬於個資法所保護之聯絡方法之個人資料。」原審法院認爲，倘若可以讓任何人皆得以蒐集、處理、利用自然人電話號碼所屬電信業者別之資料，並藉由拼湊、比對、組合、連結其他當事人之社會活動資料，將可能間接識別出特定之自然人，會使當事人陷於遭不當窺探、侵擾或行銷之危險中，這已然違反個人資料保護法的立法意旨。

（三）M+ 軟體之運作需蒐集、傳輸個資至第三人手機，未經個資當事人同意，屬於不法利用當事人個資

原審法院認爲，原告雖提供其電話電碼予其友人，但並無證據證明原告亦曾提供其電信業者別名稱，被告既明知利用該軟體程式所傳輸電話號碼之電信業者別名稱予第三人，判決理由指出：「……將與該手機聯絡簿中所載之其他個人資料相互組合、連結而得以間接識別該特定自然人，自有不當揭露、利用該自然人個人資料之認識，而故意不法侵害其人格權。」

（四）57016查詢網內網外專線並未與用戶其他個資結合，不具識別性

通傳會雖曾要求電信業者提供「57016」專線，讓消費者可以自行查詢電話號碼之電信業者別，不過原審法院認爲，這只是單純提供消費者對於利用號碼可攜服務後該用戶號碼屬於網內或網外的查詢服務，判決理由指出：「……並未與該自然人用戶其他個人資料相結合或連結情形，不具識別性，而與該軟體之上揭利用個人資料有別，二者尚有不同。」

（五）被告將CNPDB中原告個資中之電信業者別資料傳輸與第三人，已逾越蒐集特定目的之必要範圍，而屬不法利用原告之個資而侵害其人格權

CNPDB是各電信業者共同依照「號碼可攜服務管理辦法」，爲通報、查詢、更新、交換，因轉換至其他電信事業，仍保留原使用電話號碼之用戶個人資料正確性之相互通報、協調、測試及查核、管理必要之特定目的而蒐集[22]，被告將CNPDB中原告之個人資料檔案，有關電話號碼之電信業者別資料，透過M+ 軟體傳輸給其他第三人，判決理由指出：「……被告雖辯稱係提供其他第三人判別網內或網外，以節省其電話費用等情，但已逾越上開蒐集特定目的之必要範圍，亦與公共利益無關，且難謂係有合理關連之利用，自屬不法利用原告之個人資料而侵害其人格權。」

三、本審法院判決理由

本審法院維持原審法院的見解，主要是認爲電話號碼所屬之電信業者別爲個人電

22 號碼可攜服務管理辦法第31條第1項：「全體固網經營者及行動經營者應共同監督集中式資料庫之建置、維運與管理，並辦理下列事項：一、共同成立集中式資料庫管理委員會（以下簡稱委員會），並訂定委員會組織及運作規定。二、訂定集中式資料庫管理者（以下簡稱管理者）、固網經營者及行動經營者間攜碼用戶移轉作業之協調方式及測試方法。三、訂定管理者與固網經營者及行動經營者間之通報作業方式。四、訂定管理者接獲第二十二條所定通報後之集中式資料庫更新時限、固網經營者及行動經營者接獲管理者通報後之攜碼用戶資料庫更新時限。五、訂定管理者應定期提供攜碼用戶資料供固網經營者及行動經營者檢視攜碼用戶資料庫資料正確性與固網經營者及行動經營者攜碼用戶資料更新之途徑及作業方式。六、訂定集中式資料庫與各經營者攜碼用戶資料庫間之介面規格、攜碼用戶資料交換之格式與程序及攜碼用戶資料交換之測試方法。七、訂定管理者應辦理事項及其服務品質標準。八、訂定對管理者監督機制。九、訂定管理者之評選標準及評選程序等相關事項。十、依評選標準及評選程序，選出單一管理者。十一、訂定委託管理契約。十二、訂定前後任管理者應交接事宜及監督機制。十三、訂定管理者出缺時之應變計畫。」

話號碼之附屬資料，得與其他個人資料相互比對、組合、連結及勾稽後，作爲間接識別特定個人之社會活動資料之一，屬於個資法所保護之個資。當此個資被認定爲法律所保護之客體時，其判決結果即可被預期。本審法院判決之其他理由，如下所述。

（一）57016係單純供查詢是否爲網內或網外，無須揭露特定之電信業者別通傳會要求業者提供「57016」專線，提供行動電話用戶查詢特定門號係網內或網外號碼，藉以判斷其通話可能適用網內或網外費率等情。本審法院認爲：「……足見如欲達到使用戶得以辨別欲撥打之電話是否係網內號碼以節省資費之目的，僅需提供特定行動電話號碼係屬網內或網外之資訊即足，無須揭露特定之電信業者別。」因此，本審法院認定被告未經原告書面同意，竟將CNPDB中原告之個人資料檔案有關電話號碼之電信業者別，傳輸予其他第三人，與通傳會要求電信業者提供之57016專線係單純供消費者查詢是否網內或網外有所不同，已然違反個資法對於蒐集個資必須符合特定目的之必要範圍之規定。

（二）被告指摘原審法院職權行使不當及防禦方法皆不可採

被告認爲原審法院指稱M+ 將不具識別性之行動電話電信業者別傳送予第三人，是屬於不當揭露當事人個人資料之行爲，在論理上有邏輯上的謬誤。不過本審法院認爲，倘若要指摘原審法院認定事實、取捨證據之職權行使爲不當，應具體說明原審判決就此部分有哪裡是不適用法規或適用法規不當之情形，並提出符合哪些法律之規定（例如民事訴訟法第469 條所列各款之事實），被告因未能具體說明原審法院職權行使不當，難以採納。另被告雖提出英文、日文之網頁資料，主張美國、日本均可公開查詢電話號碼之電信業者別，故行動電話之電信業者別非屬個人資料等等說詞，但經查被告於原審法院並未提出該防禦方法及證據資料，也未說明原審有何違背法令致其未能提出之情形，按規定被告不得於二審程序中提出本項防禦方法（民事訴訟法第436條之28）。

（三）原告因個資遭不法侵害請求精神上損害賠償，從情理上來看並不違背個資屬於隱私權之一部分，個資遭不法利用，衡諸常情，被害人精神上是會受到一定程度的痛苦，由於這種精神上的痛苦屬於抽象概念，難以期待被害人會提出具體的證據證明其所受到的精神痛苦程度爲何。原告於原審訴訟程序中已敘明被告T公司私自將自CNPDB查得之原告攜碼轉換電信公司資料，提供予被告K公司經營之M+軟體使用，

侵犯原告的個人資訊隱私權，依個資法第28條第3項規定請求上訴人連帶賠償5百元；原審法院審酌被告任意利用該個人資料，使他人得以藉此拼湊、比對、組合、連結其他原告之社會活動資料，將使原告陷於遭到不當窺探、侵擾或行銷之危險，依照個資法規定判命上訴人賠償5百元，而這個結果屬於原審法院依自由心證所為判斷，從情理上來看並不違背。

四、本判決之簡評

本判決主要圍繞在「個人資料定義」與「蒐集與利用之目的」兩項爭點，因此本文根據上述原審與本審法院的判決理由，簡短提出以下兩點評論：

（一）電信業者別資料應不包含於個資法之規範範圍內

本案原告提供其電話號碼予其友人，其友人將該資料登錄於智慧型手機之通訊錄中，經由系爭軟體M+自CNPDB蒐集該電話號碼所對應之電信業者別資料後，再顯示於其友人手機的M+軟體介面上。單純操作目前個資法對於個人資料的定義，該「電話號碼」以及「電信業者別」等資訊，係屬於可識別其特定個人之資訊，自屬於個人資料，並無疑義；然而，是否所有與個人有關之資訊皆屬值得保護之個資？原告對於其友人而言，顯為「已識別」之特定個人，就此觀之，似無須再探究電信業者別資料是否足以「間接識別」特定個人，而應檢討的是，本件原告對於其電話號碼之電信業者別有無任何資訊隱私之合理期待。

由於電話號碼係由通傳會核配予各電信業者，早期尚未實施電話號碼可攜服務，民眾可由電話號碼前四碼而輕易判斷所屬之電信業者別（例如0932是中華電信、0935

---

23 例如遠傳電信提供之查詢網內外門號：**http://www.fetnet.net/cs/Satellite/eCare/QryNetType**。其實，當攜碼用戶移入後，移入業者亦會預設一個月的攜碼移入「答鈴告知」，其告知內容即為電信業者別，但業者通常告知用戶可以隨時取消或轉換其他來電答鈴（**RBT**）。

24 原審判決認為「被告既明知利用系爭軟體程式所傳輸電話號碼之電信業者別名稱與第三人，將與該手機連絡簿中所載之其他個人資料如姓名、出生年月日、聯絡方式（電話號碼）、職業、住址、特徵、社會活動資料等相互組合、連結而得以間接識別該特定自然人，自有不當揭露、利用該自然人個人資料之認識。」若在手機連絡簿中已載有電話號碼、姓名、出生日期等資料，倘若還需結合電信業者別資料方能間接識別特定人，從經驗法則推論，殊難想像。參見徐仕瑋（**2014，137**）。

是台灣大、0936是遠傳），因此在已知電話號碼的情形下，當事人對於電話號碼所屬之電信業者別，自無所謂有合理的隱私期待。

在實施號碼可攜服務後，通傳會雖有要求電信業者設立「57016」專線以供消費者查詢特定電話號碼與自己電話號碼之間屬於網內或網外關係，但其實各行動業者之網頁也能提供相同且更爲簡便的查詢服務[23]；或用戶亦可自行申請通話明細，亦能知悉所撥打之電話號碼屬於網內或網外。因此，原告縱然對電話號碼所屬之電信業者別有主觀上的隱私期待，然而電話號碼所屬之電信業者別資訊卻可輕易透過上述各種方式查詢可知，尚難認爲原告之隱私期待爲合理。

單純電信業者別資訊，實難以直接辨別出特定個人，但是否可以間接識別出特定個人？由於電信業者別資訊的顯示僅讓消費者得知受話對方是屬於「網內」或「網外」藉以節省電信資費支出，並無涉及窺視、干擾或刺探個人生活問題，並不會對個人隱私造成傷害（邱忠義，2014，p.102）。實則，法院若能以認同「電話號碼應較電信業者別更具有隱私期待」爲前提，則當顯示在原告友人手機通訊錄中之電話號碼係由原告所提供，而原告提供自己電話號碼予他人時，在形式意義上也同時將電信業者別之資訊讓其友人知悉，換言之，已知他人電話號碼後再蒐集其所屬之電信業者別，識別範圍不因資料增加而縮小，因此電信業者別資料在本案對於識別特定個人毫無實質助益[24]，本文認爲電信業者別資料屬於不具備有合理期待性之隱私資訊，並無特別值得保護之必要，適度公開讓一般大眾或業者合理知悉、利用，反而對公共利益有所助益。

（二）個資法過度重視隱私權保障而輕於資訊流通利用之傾向應予調整

本案之原審與上訴審法院皆認爲電信業者別屬於個資法所應保護之個人資料，因此認定M+利用各電信業者所共同建置之CNPDB顯示出電信業者別名稱，已逾越蒐集特定目的之必要範圍，與公共利益無關，且難謂係有合理關連之利用。以M+業者來說，本案爭議的「事後」解方，或可考量先取得使用者同意，若有不同意者，則以屏蔽或不顯示電信業者別之方式作爲解套；然而本文認爲，在個資法保護體系仍偏重於隱私權保障之際，該判決雖在法律論理與邏輯上有其依據，但在經驗法則與法情感上

恐對資訊流通，甚至對當前大數據應用造成極大之負面影響。

肆、個人資料定義應予調整

我國個資法對個人資料有清楚的定義，只要得以直接或間接方式識別該個人（自然人）之資料，即屬之。但這種偏向靜態、列舉式的定義，極易引發爭議。我國個資法施行細則第17條規定：「……資料經過處理後或依其揭露方式無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人。」似乎是指將個人資料隱匿起來即屬於無從識別該個人之資料；但同時施行細則第3條則規定：「……間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。」這兩規定似乎互爲矛盾，究竟資料經過處理後，是屬於「無從識別」抑或「可被間接方式識別」，這兩者之間從個資法的靜態定義上來看，並未清楚釐清。

傳統個人資料與非個人資料的「二分法」，其標準是「識別之可能」，只要可加以識別，無論直接或間接，皆適用個資法；反之，若無法被識別，即無需適用個資法。在此大前提下，透過大數據應用技術而大量儲存或分析個人資料，按原則只要將可識別個人的資訊去除，或使該個人資訊無法被識別，該項資料即非屬於個人資料之範疇。然而資料比對的技術日新月異，尤其是目前再識別技術極容易將去識別之資料（unidentified data）再回復爲可識別之資料（identifiable data），或者透過資料比對、連結、組合等方式將原先分散、無法識別之個別資料轉變爲可識別之資料。由於資料控制者對於先前已去識別之資料或無法識別之資料已不受個資法保護，而得以對該資料進行利用，但該資料倘若嗣後可能回復爲可識別之資料，特別是這種「再識別行爲」資料主體經常無法察覺，這使得傳統個資法中「二分法」主要針對資料本身靜態描述，亦即是否可直接或間接識別特定個人的定義是否仍然可行，值得存疑。

個資定義「二分法」所產生的模糊空間，在大數據應用下可能帶來無法預測的衝擊（Chung, 2014, p. 418）。學者Schwartz與Solove嘗試發展出其他資料類型藉以突破過去二分法的迷思，但他們也認爲隱私保障若無一合理邊界，資料保護的限制將不復存在（Schwartz & Solove, 2011, p. 1866）。他們認爲可採納識別風險程度的高低來

決定保護程度的高低，亦即：識別風險高者其保護程度較高、識別風險低者其保護程度較低；另外，他們也指出資料種類也影響資料的利用，例如一般性資料經過大數據分析之後，所得出來的資料卻是敏感性資料，這結果將對現今個資法造成巨大的衝擊（Schwartz & Solove, 2011, p. 1877-79）。

目前我國個資的定義強調資料對於個人「識別可能與否」，但對於資料的「關聯性」或「連結性」，亦即資料是關於哪個特定個人（linked or linkable to an individual），卻著墨甚少。此類資料本身無獨特性，僅可能知曉「關於何人」或「歸屬何人」，此時資料並非足以「區分」資料主體之識別要素，而是作爲充實其既有之個人剖繪（enrich existing profiles of individuals）之要素，藉以增強資料之累積效應（WP 216, 2014, p.4）。也因此，能相互連結的資料量愈多，可識別出特定個人的可能性也愈高，即知曉其屬於何人並建構、充實其個人剖繪的機率就愈高。故判斷一筆資料是否構成個人資料，必須在具體情境脈絡中進行個案權衡（case by case analysis）而無法跳脫情境作抽象、靜態的考量（Schwartz & Solove, 2011）。

因此，本文認爲在大數據應用之下，傳統以靜態、列舉式的個資定義有必要加以調整，特別可以從「去識別化」、「資料最小蒐集原則」、「去識別後再識別的議題」，以及「從設計著手保護隱私的架構設計」進行討論。以下分別說明之。

一、去識別化

根據歐盟資料保護指令（Directive 95/46/EC）規定，個人資料的去識別化是指對個人資料進行移除足夠的識別因子之處理，使得資料管理者或他人無從透過合理方式識別特定個人之操作[25]。我國個資法第9條、第16條、第19條及第20條皆有所謂「資料經過提供者處理後或依其揭露方式無從識別特定當事人」，係指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人（個資法施行細則第17條參照），此乃我國個資法對於去識別化的明文規定。

---

25 Recital 26 of Directive 95/46/EC, at 33 (“in such way that the data subject is no longer identifiable”).

26 美國FTC（2009）在一項研究報告指出，不具識別性資料相互結合後，可能得出具識別之個資。

傳統上對個資進行去識別化的方式，不外乎有匿名化（anonymization）、加密（encryption）與轉換代碼（key-coding），被視爲是允許企業得以利用資料分析技術並同時保護個人隱私。例如Google透過移除連結（de-link）將個資中的特殊識別因子（identifiable factors），亦即直接辨識之資料，將盡可能移除指向某一特定主體之資料集片段的「連接性」，讓資料盡量分散，使其變爲足夠小的片段，讓搜尋到完整資料的可能性大幅降低（WP 216, 2014）。然而這種操作在實務上卻有相當高的難度，也經常讓一般使用者或個資主體誤認以下幾種情形，例如：將個資加密等同於去識別化、將單純移除直接辨識之資料即視同去識別化、資料的去識別化是永久性、匿名資料之利用可安心無憂、不具識別性資料相互結合仍等於不具識別性資料[26]等，以至於個資主體經常忽略了個資風險的存在。

由於匿名資料經常會被再識別而將該資料指向特定個人，因此去識別化資料其實只是一種暫時的狀態，且經常引起個人隱私的顧慮。當然，或可將所有資料視爲可識別的個人資料而受到法律規範；然而學者Ohm（2010）認爲這種將可識別之個人資訊（PII）定義擴大解釋，難免會讓使用資料的業者放棄去識別化的作爲，反而增加隱私與資料安全的風險；更進一步的風險是，隨著擴張PII的解釋將使得隱私保護架構顯得難以執行。尤其，匿名資料通常伴隨著可能會被再識別的風險，因而對於PII的保護架構中將產生不確定性。我們無法確切得知某一資料會眞的與特定個人有所關連，因此各種資料集盡可能越多不確定性，越可能確保其匿名性。

這種基於標示個人是否可被識別之「可識別」與「無法識別」的二分法，其實無助於保障個人隱私，而且不可避免會導致「去識別」與「再識別」的無效率競賽。對於PII的定義，應考量風險高低、故意與否以及再識別的潛在結果（Schwartz & Solove, 2011; Tene, 2011），以及資料本身是否因變質或遺失所造成完整性、正確性以及價值性的問題，並與其他社會利益相互衡量。

在大數據時代下，企業不應將重心集中在如何使去識別化做到「完美無缺」的程度，而是在承認去識別化的不完善性與風險性的基礎上，重視如何將資料隱私風險掌控在合理且可接受的範圍內。判斷去識別化的有效性，實際上是對風險本身的評估（WP 216, 2014, p.6），更正確來說，是將個資的生命週期（從隱私權政策、風險評估、去識別化操作、重新識別評鑑等）都納進來，才是所謂的去識別化（林其樺，

2015）。法律學者Tene與 Polonetsky（2012）倡議可採取美國聯邦貿易委員會（FTC, 2012）一項研究報告「在快速變化的時代中為保障消費者隱私對企業與決策者提出建議」（*Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Business and Policymakers*）指出，可比對資料再識別本身在統計學上的可能性，並搭配企業對於不進行再識別的合法承諾以及契約義務[27]，以達到眞正的防制效果（Tene & Polonetsky, 2013, p. 259）。因此本文認同上述兩位學者的看法，認為應將基於資料安全與課責性原則所採取的去識別化方法視為一種保護措施（protective measure），而不是作為大數據謎題的解方。企業藉由盡可能將個資去識別化，同時不放棄對資料進行有益利用，或許是值得讓大數據對於資料進行蒐集與利用最有智慧的做法。

個資去識別化的處理方法很多，但必須考量許多因素（例如去識別化之目的、資訊欄位、所要串接的資料是否可能連結導致重新識別等）才能決定。對於個人資料去識別化，在技術上可建立一套驗證標準規範，以供企業遵循。我國行政院已指示經濟部標準檢驗局進行驗證標準規範之研訂，目前國際上並無個資去識別化驗證標準及驗證作法可資遵循，現階段則採用我國與國際標準（ISO）調和之國家標準（CNS），分別於2014年6月公告「資訊技術—安全技術—隱私權框架」國家標準CNS29100，以及於2015年6月公告「資訊技術—安全技術—部分匿名及部分去除連結鑑別之要求事項」國家標準CNS29191，可作為我國現階段推動開放政府資料或大數據之個人資料去識別化驗證標準[28]（標準檢驗局，2016）。由於國家標準並無強制性，各機關或企業可視需要程度在評估驗證導入與否。

二、資料最小蒐集原則

資料最小蒐集原則一直是隱私法制中相當重要的原則（OECD, 1980），可透過許多不同方式執行，包括對於個資的蒐集、使用、揭露、保留、識別性、敏感性以及近用加以限制，如此可協助保護兩項與隱私有關的風險。第一是儲存資料量越多，越可能成為資料竊賊的攻擊目標，包括組織內與組織外，並對消費者帶來潛在傷害；第

28 另參酌相關國際規範，經濟部標準檢驗局研訂「個人資料去識別化過程驗證要求及控制措施」，其中控制措施參考ISO29101等相關規範之控制措施，而執行之作業程序，則參考工研院、資策會或學界之經驗與相關技術文件。

二，倘若企業蒐集並保留大量資料，則利用資料本身將會增加風險，悖離消費者對於隱私的合理期待（FTC, 2015, p. iv）。因此企業必須刪除那些基於特定目的所蒐集到卻不再利用的資料，且對於可識別之個人資料的保留行爲必須執行較爲限制的政策。

在大數據時代，資料最小蒐集原則似乎難以做爲保護隱私權的做法，因爲大數據商業模式基本上就是盡可能在更長的時間內蒐集更多的資料，特別是集中在資料的二次利用（secondary use），今日企業透過各種管道，包括網路、行動裝置、感應器、影音、電子郵件以及社交網路等工具，蒐集並保留個人資料，而蒐集資料的企業直接從個人或第三人蒐集資料，並且從私人、半公開（例如臉書）或公開（例如選民名冊）資料來源擷取資料。資料最小蒐集原則已然不適用在現今商業市場型態，而應該用另一種方式來闡釋：當企業有必要對資料進行去識別時，應要求企業必須在合乎保障個人隱私與社會利益之下，執行合理的安全措施，並限制資料的使用（Tene & Polonetsky, 2013, p. 260）。

三、去識別後再識別的議題

按前分析，個人資料與匿名資料之判斷有賴相關的情境脈絡，不能作抽象界定，在特定情境下有效的去識別化資料，可能因情境變化而重新變成個人資料，此爲去識別化後再識別的議題。由於匿名資料隨時可能因被再識別而落入個資法的適用範圍，因此在鑑別去識別化的有效性上，其實就是對去識別化進行風險評估。首應考慮匿名資料之使用目的，或資料接收者有無利用個資之動機。由於企業對匿名資料的二次利用通常不同於資料初始之處理目的，因此從目的角度切入去識別化是否充分以及是否合乎「善意不知情」，可成爲較爲有效的判斷方式（劉定基，2012，pp. 50-51）。

另外，進行去識別化處理前的原始個人資料是否留存一事，對去識別化有效性判斷甚爲重要。歐盟個資保護小組指出，無論對個資處理者還是接受者而言，若不刪除原始資料，無論資料經何種程度之處理，皆排除構成匿名資料之可能（WP 216, 2014, p. 20）。

---

29 一個數列集合可用數學方式寫成：{2, 4, 6……}。

舉例來說，數學的集合是指具有某種特定性質的事物的總體，而這些數字可類比爲「間接識別」的資料。例如數字2、4、6分別爲不同之數，但當這三個數字放在一起，則形成一個集合[29]。倘若條件吻合的話，我們可以在該集合中添增更多的數字；我們也可以比較不同的集合，並且在其他的集合中取出相同的因子。當資料蒐集得越多，相同因子彼此間的交互作用就變得越低。以個人資料來說，當各個間接識別的資料交互作用之後只能形成單一型態時，該個人就會被識別。本文前述之歐盟與日本的個資法強調間接識別之個人資料，應有適當的限制。因此當間接識別資料（或資料集）對於識別特定個人太過於困難，抑或該資料根本無法協助識別以至於不構成合理的隱私期待。本文認爲，這類資料或資料集在我國個資法的適用上也應有所限制。

四、從設計著手保護隱私的架構設計

其實大眾經常希望在隱私保障的前提下也能享有資訊流通的便利，特別在今日大數據分析下各種資料顯然賦予了更多的應用價值，資料主體也希望資料利用者能恪守各項隱私保護規範；然而，大數據應用雖經常以「去識別化」作爲阻卻個資法適用的理由[30]，也作爲資料留存（retention）及處理等各項環節中提供有效的隱私保障、降低資料在儲存及傳輸等環節中的外洩風險，但如前述分析，去識別化資料通常只是一種暫時狀態，如何減少個人對於隱私侵害的顧慮，單純的課與法定作爲義務（諸如蒐集告知義務[31]、取得當事人書面同意[32]、應當事人請求更正資料[33]、資料外洩後處置查明之告知[34]等）並無助於上述目的達成，實應針對個資去識別化後，課與企業對於資料

30 個資法施行細則（2016.3.2）第17條有去識別化之規定，「無從識別特定當事人」是指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者，則回歸母法第二條關於個人資料之定義，去識別化之資料並非屬於個人資料。

31 個資法第8、9條。

32 個資法第15、16、19、20條。

33 個資法第11條。

34 個資法第12條。

再識別的不作爲承諾，而這項不作爲承諾，應可具體落實在「資料使用前」或本文所討論之應用程式之「下載安裝前」的隱私權政策設計上。

作爲隱私權保障的工具不僅只有法律而已，本文前述的「公平資訊實踐原則」（FIPPs）所營造出的業者自律（self-regulation），以及技術本身因應服務的發展而透過系統或制度的設計將隱私權保護納入組織運作上的「預設模式」（default mode）（Willis, 2014），將更能務實而有效地達成隱私保護之目的。按我國個資法施行細則第12條之「個資安全維護義務」來看，資料控制者如何在一開始整體設計時將隱私「包含」在內，此涉及所謂「從設計著手保護隱私」（或稱隱私架構設計，Privacy by Design, PbD）概念，有學者指出在大數據時代下，採納此概念有其必要而且實際（realistic）（Cavoukian & Jonas, 2012）。

歐盟網路與資訊安全機構（European Union Agency for Network and Information Security, ENISA）於2014年12月公告一項「設計階段納入隱私與資料保護」報告指出，隱私保護的制度設計其實可以導入技術手段，並採納許多隱私設計策略與隱私保護技巧，包括：資料最小化、個資隱藏、個資分離、個資集結、通知、控制、執行與個資利用公告（隱私權政策）等八種隱私設計策略；以及包括驗證、資格顯示、安全保密私人通訊、秘密通訊、資料庫隱私、統計揭露控制之隱私技術、保護隱私之資料探勘、私人資訊檢索、儲存隱私，以及維護隱私之運算等十種隱私技巧（ENISA, 2014）。英國通訊管制機關Ofcom也於2015年2月提出一項「促進物聯網的投資與創新」報告（*Promoting Investment and Innovation in the Internet of Things*），建議在隱私保障上應採納隱私架構設計概念（Ofcom, 2015）。

伍、個資定義的再檢討—代結論

本文分析了大數據應用在商業利益驅使下對於人類文明的進步有著關鍵性的作用，但大數據本身卻對於人們所熟知的隱私保障制度，特別是「知情同意」、「目的限定」以及「資料最小蒐集原則」等基礎原則皆產生顛覆性的衝擊；而當資料在喪失原有情境脈絡下，資料利用者藉由「去識別化」取得資料利用的正當性，同時資料主

體也喪失對個資的主導性；更令一般人難以置信的是，資料再識別技術愈來愈進步，透過大數據分析，可將零散、非結構化資料拼湊出特定個人的具體特徵。

職是之故，原有以「識別可能與否」作爲個人資料定義的二分法，如要將此二分法硬套於大數據各種有利社會大眾的應用面向，將凸顯出個資法悖離現實的窘況，同時恐將引發眾人對於資料利用中性價值的非理性責難。因此，透過檢討2014年一則司法判決，探討行動電話用戶之所屬電信業者別資訊是否屬於法律所保護之個資，從個資的定義、識別性以及資訊隱私之可合理期待性綜合分析，本文認爲並非所有與個人有關之資訊皆屬值得法律保護之個資，特別是不可合理期待的隱私資訊，或經適度去識別化後可供利用的資訊，應可運用於大數據時代資料的探勘與分析，因此，傳統以靜態、列舉式的個資定義實有必要加以檢討。

雖然去識別化並不足以提供可靠的隱私保障，甚或被認爲資料去識別與保留資料價值兩者間已然水火不容，不過本文認爲不能因去識別化存在某種程度之風險而因噎廢食，正因個資法所欲保障之價值同時包括隱私權保障與促進個資之合理利用，且資料價值開發與隱私保障並非平行線關係，掌握合理的隱私設計架構確可達到二者雙贏，而去識別化正是實現雙贏的利器。在大數據時代下，重點已非是否要將資料去識別化，而是如何實現有效的去識別化。

行政院爲解決各機關推動開放資料時所面臨部分資料無法進一步開放的情形，分別於2014年與2015年公告兩項國家標準，讓政府機關得以落實個資法「無法識別特定當事人」的匿名和去識別化的標準（黃彥棻，2015）。在去識別化的實務上，政府確實已看到問題所在。但至於是否將CNS入法則有待商榷，畢竟個資去識別化之目的在於資訊的利用，CNS標準建立係鼓勵業者自發性地進行去識別化，且過程中有較爲清楚的依據，但並非以CNS作爲合乎個資法規定之唯一依據。畢竟有關個人資料，基於具體個案情形得爲特定目的外利用之範圍相當廣泛（個資法第16條及第20條第1項但書各款規定），例如法律明文規定、爲增進公共利益等。這類個資爲特定目的外之利用，包含適度提供個資給其他機關，俾協助其執行法定職務；在個案適用及認定上不宜過度偏廢、因噎廢食，遽而停止一切個資之利用行爲，否則將不符合個資法第1條所定「促進個人資料之合理利用」之立法目的（法務部103.11.17法律字第10303513040號函）。

本文認爲，去識別化並不僅僅作爲合法利用個資的理由，尚可作爲資料留存及處理等各項環節中提供有效的隱私保障、降低資料在儲存及傳輸等環節中的外洩風險，特別是資料再識別可能性隨技術進步而增加時，課與資料使用者再識別不作爲義務有其論理與實務上之價值，例如在「資料使用前」或應用程式「下載安裝前」，將不作爲義務植於隱私權政策內容中，作爲資料使用者的責任，亦即前述所討論之「隱私架構設計」（privacy by design）。

當然，大數據應用對於法規範所產生的巨變，難以本文僅就個資定義的檢討而將所有問題處理完畢，例如告知同意原則之適用，即是相當棘手的問題。本文於分析M+Messenger判決後也嘗試檢討可能、合法的作爲，像是業者可考量先取得使用者同意，若有不同意者，則以屏蔽或不顯示電信業者別之方式作爲解套。又在如2015年9月悠遊卡公司開放民眾以電話訂購波多野結衣悠遊卡，因瘋狂搶購塞爆訂購專線電話，事後app軟體Whoscall分享訂購電話統計數據，意外引發網友質疑Whoscall在用戶不知情下擅自紀錄手機撥出的電話號碼因而侵犯用戶隱私的「波卡事件」（蘇文彬，2015）。但細想如此一來，這種個資法下「告知同意原則」，極可能摧毀軟體設計本身所欲達到之效果，究竟資料合理利用（創新）與個資隱私保護（管制）該如何兼備，值得有識者持續研究。

參考資料

〈Netflix是如何用大數據捧紅紙牌屋〉，《INSIDE》，2013/02/26，http://www.inside.com.tw/2013/02/26/netflix-big-data-houseof-card。

林其樺 （2015.12）。〈一般常見把姓名、身分證字號隱碼的做法，其實並不等於將個人資料「去識別化」〉，《關鍵評論》，2015/12/23，http://www.thenewslens.com/article/33049。

林錦鴻 （2007）。《警察運用監視器之法律問題分析—以警察職權行使法爲中心》，國立台灣大學法律學研究所碩士論文。

邱忠義 （2014.12）。〈談個人資料保護法之間接識別〉，《月旦裁判時報》，第30期，頁95-103。

范姜眞媺 （2013.12）。〈個人資料保護法關於「個人資料」保護範圍之檢討〉，《東海大學法學研究》，第41期，頁91-123。

徐仕瑋 （2014.12）。〈個資法所保護個人資料之範圍界定〉，《月旦裁判時報》，第30期，頁123-138。

黃彥棻 （2015.10）。〈擴大開放資料廣度的關鍵下一步，個資匿名和去識別化也有國家標準〉，《iThome》，2015/10/3，http://www.ithome.com.tw/news/98997。

經濟部標準檢驗局 （2016.2）。〈「個人資料去識別化」驗證標準規範研訂及推廣〉，2016/2/23，http://www.slideshare.net/vtaiwan/ss-58562437。

劉定基 （2012）。〈個人資料的定義、保護原則與個人資料保護法適用的例外—以監控錄影爲例（上）〉，《月旦法學教室》，第115期，頁42-54。

蘇文彬 （2015.9）。〈Whoscall分享波多野結衣悠遊卡搶購統計數據，因紀錄用戶撥出電話涉隱私爭議〉，《iThome》，2015/9/4，http://www.ithome.com.tw/news/98533。

Brill, Julie (Mar. 2, 2012). Remarks at Fordham University School of Law: Big Data, Big Issues, https://www.ftc.gov/sites/default/files/documents/public_statements/big-data-big-issues/120228fordhamlawschool.pdf.

Cate, Fred H. (2006). The Failure of Fair Information Practice Principles. *In* Consumer

Protection in the Age of the Information Economy 341-378 (Jane K. Winn ed.).

Cavoukian, Ann & Castro, Daniel (2014). *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*, http://www2.itif.org/2014-big-data-deidentification.pdf.

Cavoukian, Ann & Jonas, Jeff (2012). *Privacy by Design in the Age of Big Data*, https://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf.

Chung, Yuen Yi (2014). Goodbye PII: Contextual Regulations for Online Behavioral Targeting. *Journal of High Technology Law* 14: 413-450.

Cohen, Julie E. (2013). What Privacy For. *Harvard Law Review* 126: 1904-1933.

Council of Europe (Sep. 13, 1990). Recommendation No. R (90)19 of the Committee of Ministers to Member States concerning the protection of personal data used for payment and other related operations.

Cukier, Kenneth (Feb. 25, 2010). Data, Data Everywhere. *The Economist*, http://www.economist.com/node/15557443.

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

ENISA (Dec. 2014). Privacy and Data Protection by Design – from policy to engineering, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/at_download/fullReport.

European Commission (Oct. 13, 2014). Frequently asked questions: Public-Private Partnership (PPP) for Big Data, Memo IP/14/1129, http://europa.eu/rapid/press-release_MEMO-14-583_en.htm.

FTC (2009). Self-Regulatory Principle for Online Behavioral Advertisement, FTC Staff Report, http://www.perma.cc/BQ5U-NTZA.

FTC (2012). *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Business and Policymaker.*

FTC (2015). *Internet of Things: Privacy & Security in a Connected World* (FTC Staff Report), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-

report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Gellman, Robert (Feb.11 2015). Fair Information Practice: A Basic History. ver. 2.13, http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

Goodman, Marc (2015). *Future Crimes: Everything Is Conncected, Everyone Is Vulnerable and What We Can Do About It.*

Konkel, Frank (Apr. 26 2013). Boston Probe’s Big Data Use Hints at the Future. *FCW*, http://fcw.com/articles/2013/04/26/big-data-boston-bomb-probe.aspx.

McCallister et al. (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

Nissenbaum, Helen (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.*

OECD (Sept. 23, 1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343, en_2649_34255_1815186_1_1_1_1,00.html.

Ofcom (Jan. 27, 2015). Promoting Investment and Innovation in the Internet of Things: Summary of responses and next steps, http://stakeholders.ofcom.org.uk/binaries/consultations/iot/statement/

IoTStatement.pdf.

Ohm, Paul (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* 57: 1701-1777.

Richards, Neil M. & King, Jonathan H. (2014). Big Data Ethics, *Wake Forest Law Review* 49: 393-432.

Salmon et at. (2009). *Distributed Situation Awareness: Theory, Measurement and Application to Teamwork.*

Schwartz, Paul M. & Solove, Daniel J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review* 86: 1814-1894.

Schwartz, Paul M. & Solove, Daniel J. (2014). Reconciling Personal Information in the

United States and European. *California Law Review* 102: 877-916.

Sloan, Robert H. & Warner, Richard (2014). Beyond Notice and Choice: Privacy, Norms, and Consent. *Journal of High Technology Law* 14: 370-414.

Tene, Omer & Polonetsky, Jules (2012). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review* 64: 63-69.

Tene, Omer & Polonetsky, Jules (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property* 11: 239-273.

Tene, Omer (2011). The Complexities of Defining Personal Data: Anonymization. *Data Protection Law & Policy* 8(8): 6-7.

The White House (2014). *Big Data and Privacy: A Technological Perspective*, http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

The White House (Feb. 2012). *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

The White House (May 2014). *Big Data and Privacy: A Technological Perspective*, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

Tsesis, Alexander (2014). The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data. *Wake Forest Law Review* 49: 433-484.

Wang et al. (2012). Understanding Road Usage Patterns in Urban Areas. *Nature Scientific Reports* 2: 1-6. http://www.nature.com/srep/2012/121220/srep01001/pdf/srep01001.pdf.

Warren, Samuel & Brandeis, Louis (1890). The Right to Privacy. Harvard Law Review 4(5), 193-220.

Willis, Lauren E. (2014). Why Not Privacy by Default? *Berkeley Technology Law Journal* 29(1): 61-133.

WP 216 (Apr. 10, 2014). Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN.

Ybarra, Laura. (2011). The E.U. Model as an Adoptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany and the United States. *Loyola of Los Angeles International & Comparative Law Review* 34: 267-294.

Zittrain, Johnathan (Mar. 21 2012). Meme patrol: "When Something Online is Free, You're Not the Customer, You're the Product," *The Future of the Internet*, http://blogs.law.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/