交大法學評論，第 11 期，頁 31（2022）

論網路通訊監察之水平式分階段規制——以「食肉獸系統」為主要檢討素材

劉芳伶*

摘　要

本文指出，現行通訊保障及監察法（通保法）於立法之初係以中央系統通訊傳輸作為制度設計之前提，導致其在本質上難以對應分散系統通訊傳輸之規制需求。而網路傳輸即分散系統之典型例，故本文以有網路封包補食器之稱的食肉獸系統（進行通訊監察之一種科技手段）作為主要檢討素材，藉以釐清問題之所在。再以此為前提，聚焦於數位匯流之技術性特徵，改從跨巨庫觀點為進一步的綜合分析。所謂跨巨庫，係指以數位匯流技術為代表的各類情報通訊科學技術，搭配上各式各樣的感知器或探測器乃至於各種端末，而得讓各類不同的資料庫具有可跨虛擬與實境之無限連結可能性，藉此生成一個可不斷有機成長的跨領域之巨大資料庫。政府利用此一既存的跨巨庫現象來進行偵查時，可區分為四階段，即 A 設備裝置階段、B 取得資訊階段、C 儲存累積階段、D 照合分析階段，此即所謂跨巨庫觀點。本文擬由此觀點進一步深入剖析，並提出所謂水平式分階段規制論（即區分上述 A、

* 東海大學法律學院法律學系副教授；日本東京大學法學博士。本研究幸獲科技部專題研究計畫（MOST 109-2410-H-029-035）經費補助，特此銘記以申謝忱。得蒙三位匿名審查人盡心審閱並具體建言，作者由衷深謝，惟文責在己乃理之自然。
投稿日：2021 年 12 月 28 日；採用日：2022 年 5 月 27 日

B、C、D 各階段分別進行不同的規制），最後以之為據，針對現行通保法提出具體之修法建言。

關鍵詞：食肉獸系統、設備端通訊監察、特定性要求、數位匯流、第三人原則、馬賽克理論、位置情報

Cite as: 11 NCTU L. REV., September 2022, at 31

The Study on the Horizontal Phased Regulation of Internet Surveillance —Taking the "Carnivore System" as the Main Material for Review

Fang-Ling Liou*

Abstract

This article points out that the current Communication Security and Surveillance Act (CSSA) was originally based on a centralized system as its prerequisite for legislation, so it is essentially unable to cope with the problems of decentralized systems. Because the Internet is a typical example of a decentralized system, this paper takes the Carnivore System (a technological method for internet surveillance) known as a packet sniffer as the main material to clarify the problem. With this as the premise, this article focuses on the technical characteristics of digital convergence, and change it from the perspective of "the across-giant-database" to further comprehensive analysis. With the development and popularization of information technology and various sensors, everyday life in the modern world is often inseparable from a variety of giant databases that have unlimited possibility of connecting the virtual and the real world. This is the aforementioned "the across-giant-

* Associate Professor, College of Law, Tunghai University; Doctor of Laws, the University of Tokyo.

database". "The across-giant-database" as an investigative method can be divided into four stages: A stage-equipment installation, B stage-getting information, C stage-storage accumulation, and D stage-conformity analysis. This is the so-called cross-big library view. This article further analyzes this point of view and puts forward the so-called horizontal phased regulation theory to make specific suggestions for amending the current law.

Keywords: Carnivore System, Source-Telecommunications-Monitoring (Quellen-Telekommunikationsüberwachung), Particularity Requirement, Digital Convergence, Third-Party Doctrine, Mosaic Theory, Location Information

1. 前言

在我國，監聽之法依據為通訊保障及監察法（通保法），然而，同法在立法當時，原係以電話通訊為想定之規範對象來進行設計，從而要對應現今網路通訊之實際，不免捉襟見肘且有鑿枘。事實上，我國亦早有論者指摘，同法第 11 條之 1 的適用範圍，僅限於中華電信、台灣大哥大、亞太或遠傳等電信服務業者，而不及於像 LINE、Gmail、Instagram 或 Facebook 等網際網路通訊業者，並非妥適[1]。對此，作為解決方案，或有認為只要修法將通保法之適用範圍，擴及至提供網際網路通訊軟體服務等之廣義的通訊業者，而不再僅限於電信服務業者即可[2]。不過可惜的是，即便擴大適用範圍，也無法解決通保法在本質上落後時代的問題。因為，現行法的問題乃係立法構造上的問題，而非僅止於未將廣義的通訊業者納入規制此點之上。申言之，按傳統的電話通訊傳輸系統係採行所謂的中央系統（centralized system），而網路通訊傳輸系統則係採用分散系統（distributed system）[3]。現行法係以中央系統之電話通訊傳輸為前提來進行規制設計，導致其在本質上原就難以對應以分散系統之網路通訊傳輸為對象時之規制上的需求，此即通保法之立法構造上的問題核心[4]。

而所謂分散系統，係指為了實現數位通訊所建構的訊息傳送系統，與傳

1 李榮耕，「即時通訊程式的通信紀錄的調取」，月旦法學教室，第 212 期，頁 24（2020）。

2 同前註。

3 中央系統存在有一個控制整個系統的主機，相對於此，分散系統並不存在有控制整個系統的主機。*Decentralized System*, COMPUTER HOPE (June 7, 2019), https://www.computerhope.com/jargon/d/decentral.htm; *Comparison – Centralized, Decentralized and Distributed Systems*, GEEKS FOR GEEKS (Oct. 8, 2021), https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/.

4 而之所以現行法會僅以電信服務業者為規範對象，也正是因為當初立法設計就是以電話通訊中央系統作為想定的規制對象之故。

統之電話線路系統所採用的中央系統相較，乃係一正相反對的設計[5]。申言之，兩系統最大之差異在於，中央系統必須事先確保傳送物理訊息之實體線路，相對於此，分散系統則無須（且無法）事先確保傳送訊息之實體線路，而是待有需要傳輸之（虛擬）數位資料出現時，分散系統會迅速確認該時點之所有空閒的（虛擬）傳送路徑，由各個傳送機器自行判斷出[6]傳送訊息之最效率路徑，再以該路徑進行傳送[7]。此一差異，在判斷是否能夠符合令狀原則之特定性要求（Particularity Requirement）[8]上（我國實務將此要求名之為「概括搜索票禁止原則」[9]），有著至關重要的影響。要之，在以技術上必須事先確保傳送實體線路之中央系統為對象進行通訊監察時，在規制設計上便可以事先針對特定的傳送線路予以明示特定處分對象，而達到令狀原則之特

5 田村武志，図解・情報通信ネットワークの基礎，頁 6、118（2000）；井上伸雄，〔図解〕通信技術のすべて：基礎知識からクラウド、モバイル、次世代通信まで，頁 122-125（2011）。並參照，劉芳伶，「從『系統性』觀點論檢察之『特別偵查體制』建構與『事物管轄』觀念」，檢察新論，第 24 期，頁 26（2018）。

6 因係由各個傳輸機器自行判斷，而並不存在有一個統一控制的中央傳輸機器，故稱之為分散系統。

7 田村武志，前揭註 5，頁 118；井上伸雄，前揭註 5，頁 122-125；井上伸雄（ほか共著），新通信情報早わかり講座 3，頁 12（1999）；村田正幸，マルチメディア情報ネットワーク：コンピュータネットワークの構成学，頁 31（1999）。並參照劉芳伶，前揭註 5，頁 26-27。

8 美國法所稱特定性要求，係指令狀應該明確記載（Particularly Describing）應搜索扣押之範圍，以防止法執行機關濫用裁量進行一般搜索（General Searches），換言之，特定性要求限制了搜索扣押之範圍，並明確地劃定了法執行機關行搜索扣押之合法性界線。*See* Marron v. United States, 275 U.S. 192, 196 (1927). *See also* Stanford v. Texas, 379 U.S. 476, 485 (1965). 此處所稱特定性要求，在我國有論者將之稱為令狀之明示特定要件。劉芳伶，「遠距搜索扣押與令狀之明示特定」，東海大學法學研究，第 49 期，頁 47-51（2016）。

9 參見最高法院 100 年度台上字第 5065 號判決。並參照劉芳伶，「概括搜索票禁止原則與另案扣押・附帶扣押制度／最高院 100 台上 5065 判決」，台灣法學雜誌，第 291 期，頁 184（2016）。此處所稱概括搜索，相當於美國法所稱一般搜索。並參見同前註。

定性要求[10]。相對於此，在分散系統，因為在技術上無法（也無必要）事先確保虛擬的傳輸路徑，故而也就根本不可能在規制設計上要求事前針對特定虛擬路徑予以明示特定，如此一來，在網路通訊之情形，是否能夠滿足令狀原則之明示特定要求，即有可疑[11]。

基上所陳，本文認為，有必要聚焦於中央系統與分散系統在技術上之差異性，重新思考對於網路通訊監察應如何合理地設計其規制。具體上，本文擬以網路通訊監察程式而聞名於美國的「食肉獸系統」（Carnivore System）[12]

10 我國最高法院一貫認為，通訊監察在本質上係屬於搜索扣押的延伸。有同院 104 年度台上字第 1006 號判決，同院 102 年度台上字第 4353 號判決，同院 101 年度台上字第 6464 號判決，同院 100 年度台上字第 5561 號判決，暨同院 97 年度台上字第 3872 號判決等可供參照。於此意義上，通訊監察自也同受概括搜索票禁止原則亦即令狀之明示特定要求所規制。

11 舉例以言，像是通保法第 11 條雖明定通訊監察書（令狀）之應記載事項計有九款，即「案由及涉嫌觸犯之法條、監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所、監察理由、監察期間及方法、聲請機關、執行機關、建置機關」。其中「監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所」顯然係針對中央系統之電話通訊監察所為設計，因為中央系統必須在事前確保傳送物理訊息之實體線路，因此事前可以特定實體路線之電話號碼，也可以藉由事前鎖定特定之監察對象（即發話者或受話者）來特定所欲監察之實體路線；但是，在分散系統之情形，由於技術上不可能事前特定傳輸路徑，因此即便形式上記載了「監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所」，但就明示特定「傳輸過程」（通訊監察之處分對象）此點而言，根本係毫無助益。因為，分散系統乃係以虛擬傳輸路徑為對象，與以實體線路為對象之中央系統迥然不同，在前者之情形，由於傳輸過程為虛擬，其與實體的傳輸機器乃至於其他物理性要素並無物理性連結。故而即便在令狀載明「監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所」此等物理性事項，也無法藉此明示特定其所欲監察之虛擬的傳輸過程。

12 FBI 之後又開發了第三代的 DCS-1000 來取代食肉獸。*See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 651-55 (2003). 不過，有論者指摘，所謂 DCS-1000 根本就是把食肉獸換個名字而已。Jennifer DiSabatino, *Carnivore Gets a Name Change*, COMPUTERWORLD (Feb. 12, 2001), https://www.computerworld.com/article/2591165/carnivore-gets-a-name-change.html; and *see* James McClintick, *Web-surfing in Chilly Waters: How the Patriot Act's*

作為主要的檢討素材，藉以進一步具體呈現分散系統與中央系統兩者在技術上之差異為何？又因此會導致其在規制需求上產生如何之區別性？再以此為前提進一步綜合分析。

2. 食肉獸系統之技術性特徵

食肉獸系統乃係美國 FBI 於 1990 年代所開發使用於 ISP 網路的封包補食器（packet sniffer）[13]。由於此系統（由軟體與硬體所組成[14]）必須安裝在 ISP 的網路上，因此，雖說在完成安裝後，FBI 即可自主操作，但仍必須獲得 ISP 的配合與協助才能順利安裝並有效運作[15]。其程式之原始碼（the Carnivore software source code）雖尚未被正式公開過[16]，然有文獻指出，食肉獸程式可以監看網路上之一切活動[17]。以下，擬以電子郵件通訊監察為例，來說明同程式在網路分散系統上的具體運作方式，以便釐清其侵害性構造。

Amendments to the Pen Register Statute Burden Freedom of Inquiry, 13 AM. U. J. GENDER SOC. POL'Y & L. 353, n. 146 (2005).

13 Steven M. Bellovin, Matt Blaze, Susan Landau & Brian Owsley, *Seeking the Source: Criminal Defendants' Constitutional Right to Source Code*, 17 OHIO ST. TECH. L.J. 1, 12 (2021). 另有文獻指出，雖然食肉獸在 1997 年就已經被研發出來，但直到 2000 年才被公諸於世。*See* Kimberly A. Horn, *Privacy Versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Age*, 29 FORDHAM URB. L.J. 2233, 2235, 2259 (2002).

14 Gina Tufaro, *Will Carnivore Devour the Fourth? An Exploration of the Constitutionality of the FBI Created Software*, 18 N.Y.L. SCH. J. HUM. RTS. 305, 309 (2002).

15 Horn, *supra* note 13, at 2258-59. And *see also* Tufaro, *id*. at 308.

16 Frank J. Eichenlaub, *Carnivore: Taking a Bite Out of the Fourth Amendment*, 80 N.C. L. REV. 315, 327-28 (2001).

17 Graham B. Smith, *A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L. REV. 481, 492 (2001).

2.1 兩階段構造——以電子郵件通訊監察為例

食肉獸系統係以「（數位資料之）傳輸過程」作為處分對象，而在網路分散系統中，電子郵件之傳輸，係採取所謂封包交換（packet-switching）的技術來進行，因此，雖通稱為電子郵件通訊監察，然實際上之操作並非以「該郵件本身」[18]（下稱目標郵件）作為通訊監察對象，而係以「目標郵件經拆解後在分散系統中的傳輸層正在進行傳輸中之各個封包」（此即「傳輸過程」）為對象[19]。所謂傳輸過程，具體上，係指寄件者寄出信件後，至該電子郵件到達收信者之信件伺服器前之間的階段。據此，可將電子郵件通訊監察定義為：「自發信人按下信件送出鍵後至到達收信人之郵件伺服器前的這段期間內，針對分散系統中的封包傳輸過程，利用自動化徹底探索技術進行同步的監視與全面的掃描（搜索），並將掃描到可疑與犯罪事實有關（具有與犯罪事實相關的蓋然性）之封包皆予以攔截儲存（扣押）之偵查手法」[20]。具體上，其運作分為以下兩階段來進行。

第一階段為全面掃描攔截取得階段（下稱掃取階段）。在此階段，具有網路掃取機能之食肉獸程式會利用自動化徹底探索技術[21]，將網路上所傳輸流通的各個封包，全數予以掃描，過濾出符合程式所預先設定的過濾條件之封包，將之攔截取得[22]。通常係設定送件人或收件人之送件或收件地址作為過濾條件，當然，如果偵查機關手頭有更多的情資，那麼過濾的條件也可以

18 此係指偵查機關所欲取得人所可閱讀之原始電子郵件的內容。

19 Stephen P. Smith et al., *Independent Review of the Carnivore System*, at 3-23. (Dec. 8, 2000), https://www.epic.org/privacy/carnivore/carniv_final.pdf.

20 *Id*. *See also* Eichenlaub, *supra* note 16, at 322-26.

21 在食肉獸所使用之自動化徹底探索技術被名之為「packet sniffers」。*See* Jeff Tyson, *How Carnivore Worked*, HOW STUFF WORKS (Nov. 27, 2000), https://computer.howstuffworks.com/carnivore.htm.

22 *Id*. *See also* Kerr, *supra* note 12, at 651-55. And *see* Johnny Gilman, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS 111, 122-24 (2001). *See also* Tufaro, *supra* note 14, at 309, 313-14.

設定的更為精確，但不論其設定條件是較為粗糙或是更為精確，就現階段的技術而言，仍然還是無法僅針對信頭（header）[23]進行攔截保存（取得），而必須就整個封包，也就是包括信頭（非內容）與信體（內容）這兩部分都一起予以攔截保存。

而作為食肉獸的前身，其實，還有一種被稱為雜食獸（Omnivore）的掃取程式[24]。如其名稱所示，雜食獸什麼都吃，換言之，其掃取機能所能達到的過濾效果甚微，也因被強烈批判根本無法符合令狀的特定性要求[25]，故而才進一步研發出食肉獸系統，如其名所示，食肉獸並非如雜食獸一般什麼都「吃」（截取），而是只吃「肉」[26]，這意味著，食肉獸在掃取階段之過濾機能係較高於雜食獸[27]。

而在第一階段順利掃取封包後，接著會進入第二階段，也就是數位資料的抽出與還原階段（下稱抽還階段）。按若僅係取得封包，其實對於偵查目的（釐清犯罪事實）而言，並無直接助益[28]。因為，對偵查機關而言，最重要的還是要取得可資證明犯罪事實存否之數位資料內容[29]。為此，就必須進行第二階段之抽還作業，也就是必須針對封包來進一步實施電腦鑑識

23 信頭係指數位資料被切割為各個封包後，在傳輸之際追加其上的數位資料，這些數位資料乃係針對資料區（進行傳輸所需要的位址等資料）所為描述。資料傳輸時，信頭之後的資料則被稱為信體。信頭為非內容性數位資料，主要是接收端地址、控制、偵錯等等，而信體為內容性數位資料。一個封包係由信頭與信體所構成。

24 Kerr, *supra* note 12, at 651-55.

25 Peter J. Georgiton, *The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-Mail and Why There Is Nothing You Can Do About It*, 62 OHIO ST. L.J. 1831, 1847-48 (2001).

26 這裡的「肉」係指符合預設指令的封包。而所謂的指令，則是指程式所設定之過濾條件，其通常係指定發信人與受信人之位址資訊作為系統過濾的預設條件。

27 *Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcommittee on the Constitution of the Committee on the Judiciary*, 106th Cong., 2nd Sess. 13 (2000). And *see* Kerr, *supra* note 12, at 651-55.

28 因為封包是以機器語表現，並非人類所能直接判讀。

29 也就是還原成人類可以直接讀取的目標郵件內容。

（computer forensics），具體上，係將在第一階段所掃取到的大量封包一一解析，過濾出由目標郵件所分拆而來之對象封包（封包為人類所無法直接解讀的機器語），將之從眾多封包中予以抽出後，再加以解密（若封包有被加密）並組合還原成目標郵件（也就是還原成人類可直接解讀的內容）[30]。

據上所述，我們不難發現，食肉獸系統僅係網路通訊監察過程之掃取階段所使用的程式系統而已。另一方面，雖說相較於雜食獸而言，食肉獸的掃取機能的過濾精度上，確實已經大幅提升，不過，就如食肉獸之名稱所示，該程式仍然是大範圍地擷取封包，也就是只要是該當於「肉」[31]的封包都「吃」，而且在技術上，還是必須掃描全部的封包（全面掃描），但只「吃」（攔截取得）屬於「肉」的封包而已。就這層意義上而言，食肉獸在第一階段所掃取的封包範圍，其在「掃」的部分，還是以通過傳輸節點的「全部」封包為對象；基此，有論者指摘，如此一來，食肉獸還是會該當於「無選別的一般探索」，且就「取」的部分而言，雖係限於「符合程式所預先設定的過濾條件」之封包，然而就其所實際取得的範圍，若與作為偵查對象的目標郵件本身相比較，偵查機關所可取得之封包範圍還是過大[32]。故此，有論者指摘，食肉獸系統與雜食獸也不過五十步笑百步，前者亦同樣無法符合通訊監察令狀所要求之特定性[33]。

---

30 相對於本文從美國法視點採兩階段分類法；國內有論者從德國法視點採四階段分類法，即傳送、暫存、接收、管理此四階段。王士帆，「網路之刑事追訴——科技與法律的較勁」，政大法學評論，第 145 期，頁 358-359（2016）。

31 同前揭註 26。

32 具體來說，偵查機關雖然只是要在網路上攔截 A 進行毒品交易的相關郵件，但在條件的設定上卻可能僅設定若封包的信頭係以 A 為發信人或以 A 為收信人者，皆加以攔截存取，而且無法僅就信頭做存取，必須以連信體在內的整個封包作為存取對象；而且，無論其條件如何設定，在實施技術的本質上，還是要就所有通過的封包都一一進行攔截過濾。事實上，也有 FBI 的內部備忘錄指出，食肉獸系統不僅掃取了 FBI 所設定目標對象的電子郵件，也同時掃取了非目標對象的電子郵件。*See* Eichenlaub, *supra* note 16, at 348-49.

33 Gilman, *supra* note 22, at 112, 123-24.

相對於前述之違憲指摘，FBI 則是一貫宣稱，食肉獸系統可以符合令狀的特定性要求；一則，FBI 表示，在第一階段（即前述掃取階段），可以透過網路最小化程式（internal minimization procedures），來最小化在網路上所可能截取的對象範圍，以符合令狀之特性定要求[34]；不過，此程式是否能確實最小化以達到令狀之特定性要求仍屬有疑，而且事實上，由於食肉獸需要在短時間處理極為大量的封包，因此皆設定成所謂「圍欄（大筆一劃）模式」（pen mode）[35]，所以就實際運用而言，也根本不可能達到最小化的要求[36]。另一方面，FBI 還主張，在第二階段，與第一階段不同，此時是可以僅針對封包的信頭部分進行過濾、解析與還原[37]。易言之，在第二階段，技術上是可能將信頭部分與內容部分予以分離，如此一來，在技術的操作上，就可以防止與本案無關之內容落入偵查機關的眼目之中[38]。那麼，若僅單就二階段而言，似乎就有將之解為仍有可能滿足令狀特定性要求之餘地，但問題是，即便解為利用第二階段可以在技術上將內容部分予以分離之特徵，採用法律上的規制來確保與偵查對象無關的內容不會為偵查機關所探知，藉此滿足令狀的特定性要求，問題是，如此一來是否就足以認定，藉此已經治癒了在第一階段因採用自動化徹底探索技術所為的全面掃描（探索）並不符合特定性要求之瑕疵，則仍屬有疑，故以下尚有進一步探究的必要。

---

34 *Id*. *See also* Tufaro, *supra* note 14, at 315-19.

35 所謂「pen mode」，本文翻譯為「圍欄（大筆一劃）模式」，係指在食肉獸的設定上僅設定位址訊息（addressing information）與信令訊息（signaling information） 作為掃取的篩選條件，如此一來，其所可攔截的封包還是極為大量，事實上並不符合令狀特定性要求所要達到的最小化目的。

36 Georgiton, *supra* note 25, at 1852-53.

37 Tufaro, *supra* note 14, at 309.

38 Tyson, *supra* note 21. *See also* Gilman, *supra* note 22, at 124-25.

2.2　自動化徹底檢索技術與第四修正案

首先，從美國法的觀點來看，這裡的問題核心是，食肉獸作為一種網路掃取程式，在技術的本質上，係無可避免地必須採用自動化徹底檢索技術，若此，同技術是否該當於美國憲法第四修正案所禁止之一般性、探索性的搜索，即成問題。按食肉獸在第一階段，為了要順利攔截取得該當於程式預設條件所指定之封包，就必須運用自動化徹底探索技術，對網路上的傳輸層所流通的所有封包無一遺漏地全面加以掃描（探索並暫存）。此種「全數皆無一遺漏地加以掃描」之「自動化徹底檢索技術」，就法性質之評價而言，確係具有一般性、探索性的性格，而有違令狀特定性要求之虞。

問題是，網路上傳輸層所流通之封包何止千萬，對此，斷然不可能以人力逐一進行即時的掃描，而且事實上，以封包進行傳輸時，根本係人之五感所無法認識之機器語，因此，也不可能以人之五感進行即時的監看、監聽。若此，如因自動化徹底檢索技術在本質上具有一般性、探索性的性格，便逕行將之解為當然違背第四修正案，如此一來，無異於宣告網路通訊監察，在技術的本質上，就必然違憲違法。問題是，若採此解，網路世界豈非成為難以進行偵查之法外天堂。在網路如此普及之今日，犯罪者，無論大盜小賊，多係運用既便宜又快速的網路通訊（例如電子郵件或 LINE 等通訊軟體）來進行聯繫[39]；於此背景下，若在法評價上，逕自認為國家在網路上使用自動化徹底檢索技術進行探索，即當然屬於違反第四修正案所定令狀原則之特定性要求，此解無異於係對國家之偵查行為所為之過度規制。不過，反之，若高舉打擊犯罪之大旗而一律放寬解釋，認為自動化徹底檢索技術並不違反第四修正案，如此一來，又有規制不足侵害人權之問題。有關此點，事實上，在美國亦存有違憲說與合憲說之對立，其詳如下。

39　事實上，亦有文獻指出，行動語音近年來營收大幅下滑，VoIP 服務替代為主因之一；而具體個案，像是「冠脂妥」偽藥案中，被告全用 LINE 進行聯絡。參見黃則儒、廖先志，「從德國 2017 年通訊監察法制修正論我國對通訊軟體監察之立法方向」，檢察新論，第 24 期，頁 131-132（2018）。

3. 食肉獸之合憲性問題

3.1 違憲說

在美國，違憲說論者可以 Smith 為代表[40]，其指出食肉獸系統具有一般性、探索性的技術特徵，此點已然違反第四修正案所揭示的一般令狀禁止原則，故此，對於立法者而言，只有兩種選項，亦即，若非選擇一律禁止具有此類技術性特徵之科技使用於偵查目的，就只能選擇徹底修正此種技術性特徵，以便除去其具有一般性、探索性的法問題[41]。按此說認為，現今市民越來越常利用網絡在線上從事公私活動，作為重要服務之一，通訊業者如若不能確實地提供「安全的接續」（secure connection），那麼網絡等線上服務就根本不可能被普遍使用[42]。有鑑於此種安全的接續之重要性，作為數位資料內容的本體部分自不待言，即便是非關內容之「網絡中的履歷數位資料」（internet source information），也就是數位資料的非內容部分，一般市民也對之有合理的隱私期待，而且這種期待從社會的觀點來看也是合理的，從而

40 有關食肉獸的網路通訊監察議題，前引 Graham B. Smith 論文（Smith, *supra* note 17）具有相當的代表性，例如，*Thirty-Fourth Selected Bibliography on Computers, Technology and the Law*, 28 RUTGERS COMPUTER & TECH. L.J. 485, 496 (2002). 將之列作「3.1.1 Computers and Technology in Police Operation」項下的精選論文之一。事實上，也有不少文獻引用 Graham B. Smith 論文，例如：Rich Haglund, *Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, Is Congress or the Supreme Court Best-Suited to Protect Fourth Amendment Expectations of Privacy?*, 5 VAND. J. ENT. L. & PRAC. 137, 145 (2003); Robert C. Power, *Changing Expectations of Privacy and the Fourth Amendment*, 16 WIDENER L.J. 43, 52 (2006); Olivier Sylvain, *Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance*, 49 WAKE FOREST L. REV. 485, 487 (2014).

41 Smith, *supra* note 17, at 507-08, 514. 事實上，也有論者指摘，食肉獸系統之所以可監控網路上的所有封包，根本係出於系統設計不當之所致，並指出，食肉獸系統此種設計不當實在令人憂心。Bellovin, Blaze, Landau & Owsley, *supra* note 13, at 13.

42 Smith, *supra* note 17, at 506-08.

應可認為係符合 *Katz* 案[43]所揭示之基準，故此，市民在 IT 系統中也得以主張第四修正案的保護[44]。此處 Smith 所稱 *Katz* 案之基準，係指同案 Harlan 法官之協同意見中所揭示的主、客觀兩要件，亦即：「(1)主觀的合理期待：係指個人所具有的隱私期待其人自認係屬合理；以及(2)客觀的合理期待：係指個人所具有之主觀的合理期待，就社會的觀點來看，亦可認為係屬合理」[45]。

復又 Smith 指出，像是食肉獸系統所使用的自動徹底探索技術，在技術的本質上，本來就無可避免地會對 IT 系統內的所有數位碼（0 與 1 的組合）進行全面掃描，而較諸於傳統上對電話通訊進行通訊監察之情形，這樣的探索技術所可能造成的隱私侵害顯然係更為廣泛而深刻，因為連與案情無關的多數第三人（為數眾多之其他的網路使用者）之極為龐大的情報（the vast majority of the information from innocent users）也會被一併徹底掃描[46]。若將之與傳統的電話通訊監察相類比，此舉無異於，僅僅為了取得一位特定嫌疑人之特定通訊，竟對所有的使用者之電話迴路都進行通訊監察[47]。因此，Smith 認為，食肉獸系統必須對所有的數位碼都進行掃描的此種技術性構造，具有一網打盡的（infinitely broad dragnet）特徵，此種特徵會徹底侵害所有網絡使用者受第四修正案保護的權利[48]。

3.2 合憲說

上述以 Smith 為代表的違憲說，係屬學說多數[49]。相對於此，Kerr 乃係合憲說之代表人物。作為少數說，Kerr 首先指出，在物理性空間中，先進的

43 Katz v. United States, 389 U.S. 347 (1967).

44 *Id*.

45 *Id*. at 361.

46 Smith, *supra* note 17, at 507.

47 *Id*.

48 *Id*. at 508.

49 Heal Hartzog, *The "Magic Lantern" Revealed: A Report of the FBI's New "Key Logging" Trojan and Analysis of Its Possible Treatment in a Dynamic Legal Landscape*, 20 J. MARSHALL J. COMPUTER & INFO. L. 287, 318 (2002). And *see* Kerr, *supra* note 12, at 648.

科技對隱私造成了強有力的侵害，而在網路等虛擬空間中，則必須端賴先進科技才能保護隱私[50]。具體來說，在物理性空間的情形，警察可以搜索的範圍被侷限在物理性場所之內，例如嫌疑人的房屋內，如果要搜索該嫌疑人的房屋所在的城市之全部範圍，那就必須得依靠先進的科技才有可能；要之，在物理性空間中，要搜索的範圍越廣，那麼，所要使用的探索工具就必須更強而有力[51]。不過，在虛擬空間就大不相同了，若是要對通過網路節點之所有流通的數位碼（例如，封包）進行全面的監視與記錄，在技術上極為簡單[52]，真正困難的是要設計出一款工具，其具有選別機能，而可以有效地篩選出（與案件）具有關連性的目標數位碼，並僅就該特定數位碼加以存取，於此意義上，可以說要保護在網路上的隱私，就必須依賴「先進的選別技術」（advanced filtering）[53]。從這樣的觀點來看，具有自動徹底檢索的技術性特徵之數位探索工具，也只不過是探索數位碼而已，也就是依據人所輸入的指令來探索「0 與 1 的正確排列」（the exact sequence of ones and zeros），Kerr 認為，工具本身又不會思考，也不可能依據自己的判斷來進行情報探索，究竟情報的內容如何也無法理解，於此意義上，使用具有這種技術性特徵的工具，反而是在進行網路監視（internet surveillance）時，最尊重虛擬空間中的隱私利益的一種方法了[54]。

以上兩說之爭，究竟何者立論更具說服力。其關鍵在於，第四修正案所定禁止不合理之搜索扣押，在以網路通訊為其對象時，究竟應如何理解。有關此點，就美國法之觀點而言，首應從通訊之內容（contents）與非內容（non-contents）之區分論[55]談起。

---

50 Kerr, *supra* note 12, at 651.

51 *Id*. at 650-51.

52 Kerr 指出，即便是年僅 12 歲的駭客也可以輕鬆地寫出這種全面監視記錄網路的程式。*Id*. at 651.

53 *Id*. at 651.

54 *Id*. at 650.

55 內容係指由人之意思溝通所構成之部分，而非內容則與人之意思溝通無直接關係，

3.3　內容與非內容之區分

在美國，通訊秘密自由之保障，憲法上並無特別的明文，要之，通訊秘密中所涉及的通訊情報也與其他的非通訊情報一樣，被定位為一種隱私權，同受第四修正案之保護[56]。而美國聯邦最高法院在 *Smith* 案[57]更指出，通訊之非內容的部分，非屬第四修正案之保障對象。若此，在利用食肉獸進行網路搜索扣押（我國稱之為網路通訊監察）之文脈下，就有進一步檢討，以內容與非內容之區分為前提的 *Smith* 案中所提示的「限定性」（limited capabilities）[58]法理之必要。本案的事實概要是，被害人遭遇強盜後，接到一個自稱「我就是強盜」的電話（撥打電話的即為被告，亦即本件上訴人），警方為了確認來電號碼，在電信公司的協助下（並未取得令狀），於其電話通訊交換器內裝設了（電話號碼）撥號記錄器（pen register）[59]。其爭點是，本件撥號記錄器之使用，是否該當於第四修正案所禁止的不合理之搜索，作為結論，本件法庭意見認為並不該當[60]。

首先，法庭意見指出，如 *New York Tel. Co.*案[61]所示，藉由撥號記錄器所開示之情報，僅限於與通訊內容無關的電話號碼而已，由於只會揭露非內容之部分，因此，撥號記錄器具有「限定性」[62]，從而其之使用並不該當於第

像是通訊的狀況（circumstance），例如，送信者或受信者之資訊（envelope information）或是送信端或受信端之位置情報等（source information）。

56 井上正仁，捜査手段としての通信・会話の傍受，頁 6、17（1997）。

57 Smith v. Maryland, 442 U.S. 735 (1979).

58 Smith 案所謂「限定性」（limited capabilities）係指，撥號記錄器僅具有限的功能，亦即，只能記錄所撥打的號碼，而不會記錄通話內容。

59 美國警方在監視行動中使用的一種裝置，可以記錄某一電話機所撥出的電話號碼，但不會監聽其通話之內容。

60 *See Maryland*, 442 U.S. at 735, 748.

61 *See* United States v. New York Telephone Co., 434 U.S. 159, 167 (1977).

62 同前揭註 58。

四修正案所禁止之一般性、探索性之搜索[63]。又法庭意見雖指出，第四修正之適用範圍，如 *Katz* 案所示，應以有無合理的隱私期待（reasonable expectation of privacy）來決定[64]，然而，其具體的判斷，卻仍然離不開「財產權」（下稱「財產權模式（a property-based standard）」[65]），即本件法庭意見認為，系爭撥號記錄器是裝設在電信公司（大場所）的財產（小場所）之內，被告對該財產並無任何「財產上（property）的權限」可資主張，從而該「場所」對於上訴人而言顯然不構成「憲法上所保護之領域」（constitutionally protected area）[66]。接著同判決指出，本件應適用 *Katz* 案所揭示之有無合理的隱私期待為基準，即應視上訴人之主觀期待（subjective expectation）是否合理，且該主觀期待，從客觀來看（viewed objectively）又是否合理[67]。有關本件之主觀期待，法庭意見指出，電話用戶本來就知道，在使用電話之際，電信公司會記錄其撥話與受話的電話號碼，此乃係基於電信公司要計算用戶通話之電信費用乃至於其他正當的業務目的（legitimate business purposes）所必要，此乃社會常識，而被告明知此情卻還是撥打電話，因此不能認為其主張就電話號碼之秘密性仍然應予以維持係符合一般的期待（general expectation）[68]。而就客觀期待之部分，法庭意見主要是引用 *Miller* 判決的「自願披露之風險承擔」（"assumed the risk" of disclosure）法理[69]（下稱風險承擔理論）指出，即便上訴人主張其對於電話號碼有主觀上的隱私期待，但是對於電信公司而言，上訴人是自願將電話號碼向其進行開示，屬於個人任意向第三人為開示的情報（而被第三人作成紀錄），例如，稅務紀錄或是銀行的交易紀錄等亦同，這些基於任意開示的情報所作成的紀

63 *See* Smith v. Maryland, 442 U.S. 735, 741-42 (1979).
64 *See* Katz v. United States, 389 U.S. 347, 351-52 (1967).
65 Eichenlaub, *supra* note 16, at 342-43.
66 *Maryland*, 442 U.S. at 741.
67 *Id.* at 740-41.
68 *Id.* at 742-43.
69 *Id.* at 743-44.

錄，都沒有適用第四修正案的餘地，此點，亦早有本院歷來諸多判決先例予以確立，因此，本件上訴人既然係自願向電信公司開示電話號碼，那麼對於該號碼所持有之主觀期待即不能認為具有社會上、客觀上的合理性[70]。

不過，要注意的是，儘管美國聯邦最高法院拒絕為電話號碼提供第四修正案之保障，但其後，立法者在 ECPA（The Electronic Communications Privacy Act of 1986） 中明訂，若要使用撥號記錄器，仍須事先取得法院令狀[71]。換言之，美國實務的主流見解認為，電話號碼等非內容之通訊並非憲法保障之對象，而僅係立法保障之對象。相對於此，*Smith* 案的反對意見 Stewart 法官則認為，即便如電話號碼等亦係屬於憲法保障之對象。具體上，其指出，*Katz* 案已經承認公共電話在私人通訊中扮演重要角色，相較之下，私人電話所扮演的角色更為重要，法庭意見認為上訴人明知電話公司會記錄號碼卻自願提供，所以不受第四修正案保護，但是 *Katz* 案已經表明，即便是公共電話用戶也有權假設，他對著話筒所說的話不會向全世界擴散，這裡的重點是，在私人電話的情形，是否亦有權做同樣的假設，Stewart 法官認為，從私人電話撥打的號碼，就如同其所說的談話內容一樣，是在 *Katz* 案所承認的第四修正案之保障範圍內，因為撥打的號碼即便比談話本身簡要，但不意味著號碼就是「非內容」，Stewart 法官並進一步指稱，其對於是否有人會願意向全世界公開他們所撥打的號碼深感懷疑，因為，如此一來，將很容易暴露出使用者的身分以及他撥打電話時之所在地，從而藉此揭露出一個人生活中最私密的細節[72]。

4. 綜合分析

承上所析，以下應續行討論之點有三，其一，食肉獸之法性質是否與撥

70 *Id.* at 743-44.

71 *See* 18 U.S. C. § 3121 - General prohibition on pen register and trap and trace device use; exception. *See also* Horn, *supra* note 13, at 2250-51.

72 *See* Smith v. Maryland, 442 U.S. 735, 746-48 (1979) (Stewart, J., dissenting).

號記錄器一樣，具有「限定性」？其二，使用食肉獸的情形，是否也可以一體適用傳統的財產權模式與風險承擔理論？其三，就通訊隱私之保障而言，是否應區分內容與非內容而異其保護程度？此三點依序分項析之如下。

4.1 限定性法理與特定性要求

首先，前述合憲說指出，第一階段掃描的對象僅是 0 與 1 的組合，並非人所可辨識的內容（即非內容），因此肯定自動化徹底檢索技術合憲性[73]。若按此說，食肉獸與電話記錄器具有相同的性質，因此可以適用 *Smith* 案之限定性法理。相對於此，違憲說則認為食肉獸所掃描擷取的對象是網路上傳輸中的封包，而封包係由內容與非內容（信頭）所構成，故而顯然與僅取得非內容部分的電話記錄器並不相同，因此無法適用限定性法理。若採後說，食肉獸並不具有限定性而無 *Smith* 案之適用，接著，就必須進一步判斷其是否符合令狀原則之特定性要求。以下將之與電話通訊監察相對比，再為進一步的分析。

在電話通訊傳輸之情形，係使用中央系統，故而必須事先確保傳送物理訊息之實體線路。因此，在法規制上的意義是，此時得以事前預測其所要使用的電話傳輸之實體線路，而以該線路作為通訊監察之對象。換言之，電話通訊監察之範圍得以單一的傳輸過程為實施對象。於此意義上，自可符合令狀原則之特定性要求。當然，雖我國最高法院也指出，通訊監察之本質為搜索扣押[74]。不過，其與傳統之搜索扣押仍有不同，按前者係繼續性處分，後者為一次性處分。所謂繼續性處分，係指通訊監察會持續一段期間而非一次

---

73 按前述違憲說之核心係在於，食肉獸所使用的自動化徹底檢索技術具有全數無一遺漏地加以掃描之特徵，因此不可能符合第四修正案所要求的「特定性」（或稱令狀的明示特定要求）；相對於此，合憲說則提出反論認為，食肉獸只是電腦程式，根本「讀不懂」「內容」，而所謂「內容」係指「人所能理解之文字符號的排列」，第四修正案之一般令狀禁止原則所要求的「特定性」，係針對「（人看得懂的）內容」而言，因為只有「（人看得懂的）內容」才會涉及隱私權，食肉獸使用自動化徹底檢索技術進行全數無一遺漏之掃描的對象是「0 與 1 的正確排列」，並非人所能理解之文字符號的排列，跟第四修正案所要保障的隱私權顯然無關。

74 同前揭註 10。

即可結束。從而，雖說電話通訊監察之範圍得以單一的傳輸過程爲實施對象，但就實際的運作而言，也可能同時以複數的通訊者（撥話人與受話人）所爲複數的傳輸過程爲監察對象[75]。惟此時其與網路通訊監察之情形所謂同時以複數的通訊者所爲複數的傳輸過程爲監察對象者，仍有本質上的不同。兩者之差異可以圖示如下。

4.1.1　中央系統與分散系統之差異

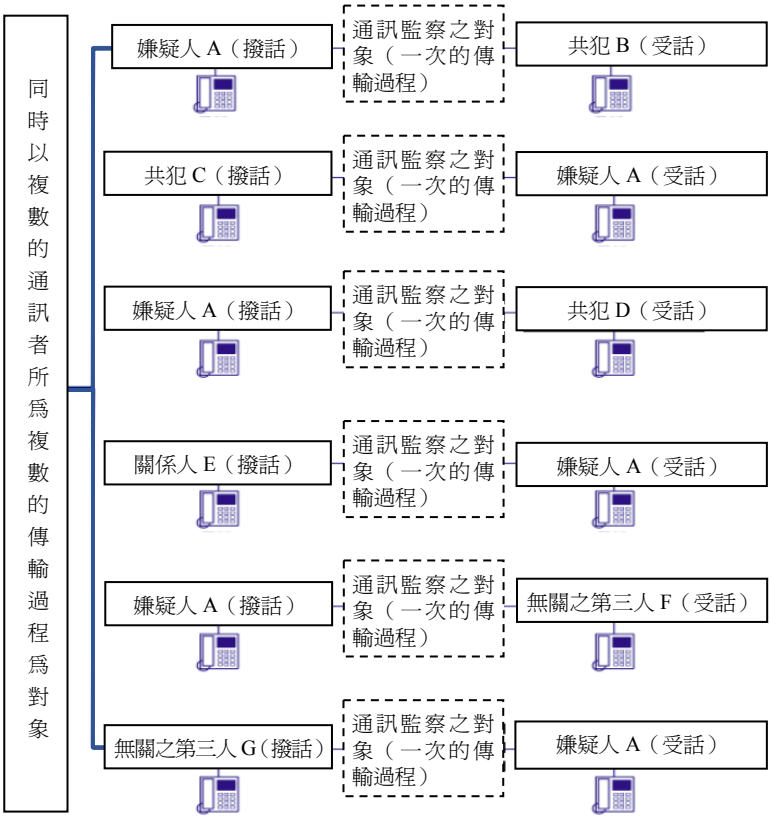

圖 1　（作者自行繪製）

75　川崎英明，「盜聽立法の憲法的問題点」，法律時報，第 69 卷第 4 号，頁 50（1997）。

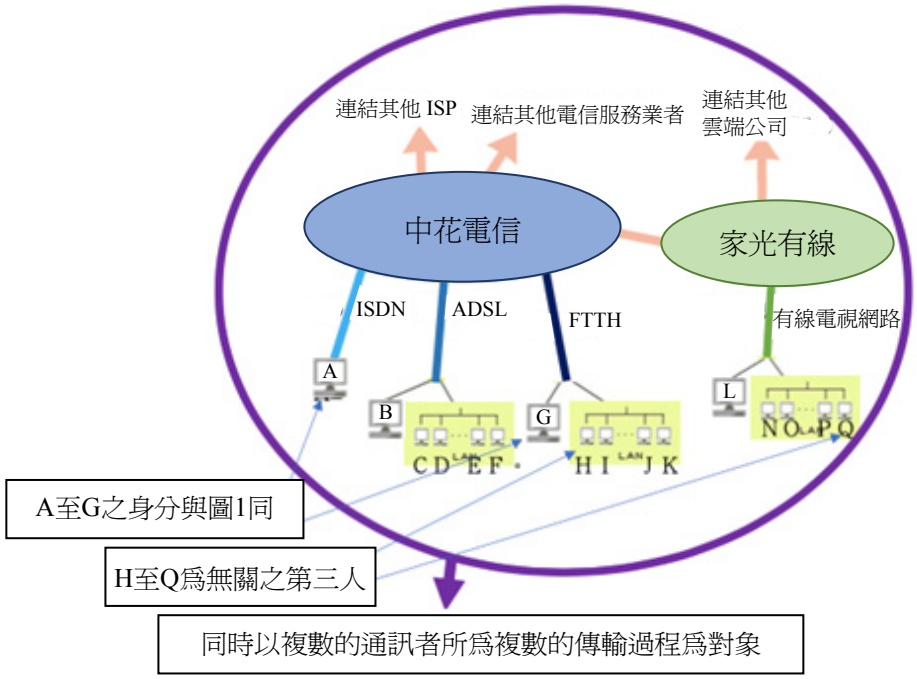

圖 2 （作者自行繪製）

如圖 1 所示，電話通訊監察，可以同時掛六條線，即「A-B」、「C-A」、「A-D」、「E-A」、「A-F」、「G-A」，來進行監聽，藉以達到同時以複數的通訊者（撥話人與受話人）所爲複數的傳輸過程爲監察對象之效果。然而，這六條線在監聽當下，係分別獨立，互不連結，且皆可事前特定其實體線路；於此意義上，係可符合令狀之特定性要求。相對於此，如圖 2 所示，網路通訊監察，在技術上本來就會使用自動化徹底檢索技術，對特定網域進行封包攔截，也就是必須將通過傳輸節點的全部封包進行無一遺漏的掃描（暫存），此階段根本沒有所謂實體線路，更重要的是，虛擬的網路傳輸回線根本不可能事前固定，而係由電腦於要進行傳輸的當下進行自動化運算，從當下所有空閒的回線中，選出最效率的路徑來進行封包傳送，如此一來，自然不可能符合令狀之特定性要求。申言之，在網路的分散系統中，並

不可能如傳統中央系統的電話回線一般事先特定「A-B」、「C-A」、「A-D」、「E-A」、「A-F」、「G-A」此六條個別獨立的傳輸線路，也就是說，在核發令狀的當下，技術上的狀況就是，「A＊B＊C＊D＊E＊F＊G＊H＊I＊J＊K＊L＊N＊O＊P＊Q……」之間皆具有相互無限連結之可能性[76]，而且，封包究竟係經由哪條虛擬回線進行傳輸，不到傳輸當下，根本無法預先知悉，故此，為了攔取到目標郵件的構成封包，也只能將所有的封包毫無遺漏地全面掃描。

4.1.2　質的限定與量的限定

據上可知，其實，*Smith* 案所稱之限定性，乃係「質」的限定問題，也就是以所欲搜索扣押（網路通訊監察）之對象係通訊之「內容」部分抑或是「非內容」部分來做區分[77]。相對於此，令狀的特定性要求，則是「量」的限定問題。若此，封包既然係由內容與非內容兩部分所構成，因此與質的限定並無關係，其所涉及者，乃係量的限定問題。由於網路分散系統與封包交換的技術性特徵，確實無法做到事前特定之要求，於此意義上，似乎是前述違憲說較具說服力。惟話雖如此，食肉獸的運作區分為兩階段，第一階段是掃取，第二階段是抽還，雖說在第一階段無法區分內容與非內容，然而，在第二階段卻可以明確區分內容與非內容，因此，若在法律上以及技術上可以擔保第一階段的掃描，係即掃即刪，且不可能落入警察之眼目也無遭流用之危險，以此為前提，在第二階段若專以非內容為對象進行抽出還原之作業，換言之，警方僅係要確認對象電子郵件發信源，於此意義上，似乎還是有解釋為可得適用限定性法理之餘地。若採此解，則前述合憲說也似乎非無道理。

不過，要特別注意者係，與美國[78]不同的是，我國通說認為，不論是通

76　＊（米字號）代表相乘之意。

77　若係後者，在 Smith 案的情形是本來就會向電信業者公開之固定的電話號碼，因此被認為並非第四修正案所保障之對象。

78　如前所述，美國聯邦最高法院拒絕對電話號碼等非內容之部分提供第四修正案之保

訊之內容抑或非內容之部分，皆在中華民國憲法第 12 條所定通訊秘密自由保障的射程範圍內（只是保障的程度有所不同）[79]。因此，美國聯邦最高法院所提案的限定性法理（非內容部分不受憲法第四修正案保護），在我國，本無適用餘地[80]。要之，就臺灣的問題狀況而言，應聚焦在「量」的限定性（也就是令狀之特定性要件）的問題上來做討論，而無法從「質」的限定性觀點來肯認像是食肉獸之類的通訊監察手段的合憲性[81]。雖說就食肉獸的第一階段而言，因為在技術上本就必須進行徹底的無選別掃描，所以確實難以符合所謂應事前予以明示特定之令狀特定性要求。不過，若能將第一階段與

護。

79 林鈺雄，「干預保留與門檻理論——司法警察（官）一般調查權限之理論檢討」，政大法學評論，第 96 期，頁 219（2007）；江舜明，「論通訊保障及監察法第三條之立法妥當性」，法學叢刊，第 50 卷第 3 期，頁 116-117（2005）；林三欽、陳愛娥、郭介恆、陳春生，「通訊監察與秘密通訊之自由學術研討會」，憲政時代，第 23 卷第 2 期，頁 5（1997）；林富郎，通訊監察法制化之研究（司法研究年報第 21 輯第 12 篇），頁 11（2001）。

80 要注意的是，限定性法理雖以區分論為前提，但並非採區分論者皆適用限定性法理。按我國通說雖肯認不論內容或非內容之部分皆為憲法之通訊秘密所保障，但實務與學說之多數皆認為，對於通信紀錄等非內容之部分與通話等內容之部分，在立法的層次上可以異其保障範圍，非內容之部分不需要給予如內容之部分一樣高的保障密度，於此意義上，我國主流之立場亦可理解為係採取區分論（只是與美國的區分論並非完全相同）。參見最高法院 100 年度台上字第 1972 號判決，並參見林鈺雄，「論通訊之監察——評析歐洲人權法院相關裁判之發展與影響」，東吳法律學報，第 19 卷第 4 期，頁 145（2008）；林俊益，刑事訴訟法概論（上），頁 415-417（2021）。要之，與美國不同的是，我國的區分論（區分內容與非內容）不是用來劃分基本權保障的界線，而係用來決定立法規制的保障密度；換言之，就臺灣實務通說之理解而言，不論內容抑或非內容，都係屬於憲法第 12 條的保障對象，加以區分，只是為了在立法上給予不同的保障程度；相對於此，美國的區分論則是用來劃分基本權保障的界線，亦即，非內容之部分不受憲法第四修正案保護。

81 亦即，如何對於欲以之為通訊監察對象的通訊之內容乃至於非內容部分的「量」在符合令狀所要求之事前明示特定。換言之，就我國憲法而言，雖說區分性質而異其保障程度（同前揭註 80），但不論其性質係屬內容或非內容，都係通訊秘密的保障對象。因此無法將其性質屬於非內容之情形，解為具有「質」的限定性。

第二階段合併觀察但分別規制，則還是有符合此要求的可能。亦即，至少，在第一階段，必須先在技術上以及法律上共同擔保兩件事，第一，自動化徹底檢索技術在進行全面掃描與攔取時，會進行自動化的即掃即刪；第二，此階段所攔取之數位資料（通訊封包）絕不會落入執法機關之眼目也無遭流用之危險。接著，在第二階段進行選別、抽出、還原之作業時，執法機關還必須得另行取得令狀方得行之。此時，作為令狀之應記載事項，應明示特定其所欲抽出（搜索）之對象，並應載明其預定採行的抽出技術與步驟，藉以擔保其所採行的抽出技術與步驟，確實只會以令狀上所明示特定之對象來進行。

本文認為，若能落實上述分階段規制之發想，便有可能克服像是食肉獸系統中所使用的自動化徹底檢索技術，其在本質上所具有的一般性探索性特徵難以符合令狀特定性要求之問題。要之，前述之違憲說與合憲說雖立場正相反對，然兩者皆欠缺分階段規制之發想。亦即，前者，僅關注掃取階段之全面探索性[82]，顯有過度規制之疑慮。而後者，則堅持掃取階段之非內容性[83]，則有規制不足之問題。不同於此兩說之對立觀點，本文的主張是，像是食肉獸此類在技術上本來就會使用自動化徹底檢索技術之偵查手法，其合憲性得以獲得肯認之關鍵乃至於其立法之正當化基礎，應求諸於制度設計上是否採行「搭配高度科學技術門檻」[84]之「分階段規制」此點要求之上。亦

82 違憲說僅聚焦在第一階段（掃描）必須使用自動化徹底檢索技術，即否定應其合憲性，未免速斷。

83 合憲說則認為，第一階段雖然要全面徹底掃描，但這些被掃描的對象僅是 0 與 1 的組合，並非人所可辨識的內容（亦即「非內容」），因此便肯定自動化徹底檢索技術的合憲性。問題是，在我國，不論內容或非內容都是通訊秘密（基本權）保障之範圍（只是在保障程度可以不同，但還是要給予相對應的基本權保障。），因而難以採取種解釋手法。

84 所謂「搭配高度科學技術門檻」，係指此種分階段令狀，與傳統的搜索扣押令狀並不相同，因為作為分階段令狀之應記載事項，除了跟傳統的令狀一樣，必須明示特定其所欲搜索（抽出）之對象外，還必須載明其所預定要採行的搜索技術與步驟，因為，唯有如此，法院才能判斷，偵查機關所欲採行的搜索技術與步驟，是否確實

即，若能在法律上與技術上之兩面共同擔保，此點要求能被具體落實，即可肯認此種手法的合憲性。

4.2 從財產權模式到隱私利益權衡模式

所謂財產權模式，其實，並非前引 *Miller* 案首創；又其與 *Katz* 案所揭示的對隱私之合理的期待之主觀與客觀基準之關係，看似相互對立，實則緊密關連。首先，有關財產權模式，可從 1886 年 *Body* 案[85]談起。在同案，美國聯邦最高法院指出，搜索扣押係以被處分人之財產權（property）為對象，並以此為前提，承認了違法取證之證據排除法則之適用。到了 1914 年 *Week* 案[86]，法庭意見也指出，第四修正案所保障的是市民的人身自由與財產權。而 1928 年 *Olmstead* 案[87]更認為第四修正案之適用係以「物理性侵入」（a physical intrusion）為必要，秘密錄音既然無法構成物理性侵入，因此並不在第四修正案之保護射程範圍內。其後，1942 年 *Goldman* 案[88]則援用 *Olmstead* 案所揭示的「物理性侵入」基準（the "trespass" doctrine），並以此為前提指出，在判斷是否構成「對場所之侵入」時，對該場所是否有「管理權」乃係重要的判斷要素。由此可知，於此時期，第四修正案之適用，即係採行以「物理性侵入」基準為中心之財產權模式[89]。而「物理性侵入」基準，被持續援用，直至著名的 1967 年 *Katz* 案[90]，才被推翻。

只會以其所明示特定之對象來進行搜索。

85 Body v. United States, 116 U.S. 616 (1886).

86 Week v. United States, 232 U.S. 383 (1914).

87 Olmstead v. United States, 277 U.S. 438 (1928).

88 Goldman v. United States, 316 U.S.129 (1942).

89 此一模式一直持續到 1967 年以前皆未曾有改變，惟話雖如此，其間也曾出現少數幾例，放寬「物理性侵入」基準之判決，例如，Silverman v. United States, 365 U.S. 505 (1961).

90 Katz v. United States, 389 U.S. 347, 353 (1967).

4.2.1 Katz 案與「合理的隱私期待」基準

Katz 案法庭意見明確指出，第四修正案所保護的是「人」而不是「場所」，並正式將同院一直以來所確立的「物理性侵入」基準予以廢止，改以「合理的隱私期待」之有無為同修正案之適用基準[91]。*Katz* 案的重點有二，其一，第四修正案的保護對象不限於有體物（tangible items），包括無體物像是口頭的會話紀錄等（the recording of oral statements）[92]；其二，即使是私人場所，如果向公眾開示，就不屬於第四修正案之保護對象，反之，雖然是公共場所，如果可得認為有合理的隱私期待者，仍可主張第四修正案之保護[93]。

就這樣，*Katz* 案明確地揚棄了「物理性侵入」基準，從此點而言，同案將隱私權正式納入第四修正案之保護射程範圍內，抑或者更精確地說，*Katz* 案確實已將第四修正案之法益保護的核心，從財產權移往隱私權。但要注意的是，這並非意味著，在 *Katz* 案以後（下稱後 *Katz* 時代），已經完全揚棄了所謂財產權模式。事實上，即便在後 *Katz* 時代，第四修正案之法益保護核心雖然已經移往隱私權，但不能否定的是，同修正案也仍然持續地保護著財產權[94]。於此意義上，也就不難理解，為何在後 *Katz* 時代，還是無法與傳統的財產權模式完全地分道揚鑣。只不過，在後 *Katz* 時代，要討論的問題已經不再是有無「物理性侵入」，因為「物理性侵入」之有無已經完全不重要了，轉而聚焦在「究竟要如何判斷隱私期待是否合理」之上。對此，美國聯邦最高法院係採利益權衡作為判斷基準，此即本文所謂隱私利益權衡模式[95]。

---

91 *Id*. at 351-53.

92 *Id*. at 352.

93 *Id*. at 351-52.

94 佐伯仁志，「プライヴァシーと名誉の保護――主に刑法的観点から―3―」，法学協会雑誌，第 101 巻第 7 号，頁 1420 以下（1984）。

95 美國有論者稱之為「a doctrine that balances interests」。*See* Eichenlaub, *supra* note 16, at 342-43.

而有關此模式之具體運用，1978 年 *Rakas* 案[96]與 1960 年的 *Jones* 案[97]，作為指標性判決，具有相當的啟發性，故以下有必要針對此兩案作進一步的對比分析。

4.2.2 Rakas 案與 Jones 案

首先，*Rakas* 案的事實概要是，被告乃係被搜索車輛的乘客，其主張對於系爭車輛有合法的留滯（待在車內）權利（legitimately on premises），且該權利因為系爭搜索而遭到侵害，對此，法庭意見認為，被告對於系爭車輛並不具有財產權抑或財產性的利益（property or possessory interest），因此認為被告對該車輛並不具有合理的隱私期待，從而不得主張其第四修正案之權利因而遭受侵害[98]。要之，法庭意見認為，即便「對場所有合法的留滯權利」，也未必皆能主張第四修正案之保護，因為第四修正案的適用基準並非「對場所（premises）有合法的留滯權利」，而是「對隱私之合理的期待」之有無[99]。

相對於此，*Katz* 案以前（下稱前 *Katz* 時代）的 1960 年的 *Jones* 案，則是將「對場所有合法的留滯權利」作為第四修正案的適用基準[100]。兩相對照，似乎，進入後 *Katz* 時代，雖說改採所謂「合理的隱私期待」基準，不過卻仍然以「財產權」作為判斷要素，而且其適用的結果所劃定之保護射程，乍看之下，似乎竟還較諸前 *Katz* 時代更為狹窄。然而，事實上，若將兩案再

96 Rakas v. Illinois, 439 U.S. 128 (1978). 當然，應注意的是，事實上，美國學界及實務界，對於應如何判斷合的理隱私期待，其具體的細部基準為何，見解分歧，有採（隱私細節）遭探知可能性（probabilities）說、有採權利基準（right-based approach）說、亦有採規範基準（norm-based approach）說等等，惟就本文此處之討論而言，實無一一介紹瑣碎分析之必要；因為各說內容雖屬有異，但取其最大公約數而言，皆可併同納入隱私利益權衡模式之下。而本文此處所要傳達的也不過是，財產權模式與隱私利益權衡模式此兩大模式之發展趨向與相互關係而已。

97 Jones v. United States, 362 U.S. 257 (1960).

98 *Illinois*, 439 U.S. at 147-48.

99 *Id*. at 143.

100 *United States*, 362 U.S. at 262-63, 265-67.

進一步比較，即可知之，事實並非如此。首先，在 *Jones* 案中，與「財產權模式」有關的重要爭點事實之要素有三，即被告其人，「(1)持有被搜索處所之房門鑰匙，且(2)常常在該房間過夜，又(3)搜索當時人就在現場」[101]。相對於此，在 *Rakas* 案中，因為被告只是乘客，換言之，只該當(3)之要素，因而 *Rakas* 案認為同案被告對於系爭車輛（場所）並沒有「管理權」（屬於財產權），因此否定其對該場所得主張具有對隱私之合理的期待。於此，我們不難發現，後 *Katz* 時代的 *Rakas* 案，在判斷是否具有對隱私之合理的期待之時，仍然援用「管理權」作為判斷要素。而最有趣的是，「管理權」本來是前 *Katz* 時代之 *Olmstead* 案所揭示的「物理性侵入」基準之下的一個判斷要素。申言之，後 *Katz* 時代判斷基準丕變，亦即，不再是 *Olmstead* 案所揭示的「物理性侵入」，而改為 *Katz* 案所提出之「合理的隱私期待」基準，但卻仍然援用 *Olmstead* 案所揭示的「管理權」作為 *Katz* 案基準之判斷要素。換言之，在後 *Katz* 時代，因為採「合理的隱私期待」為基準，因此所謂「管理權」已經與「物理性侵入」無關，但既然是對於財產之管理權，因此仍然與「財產權」息息相關，尤其，與構成「場所」之財產權有極為密切不可分之關係。

4.2.3 隱私、場所與財產權

要之，即便 *Katz* 案確立了第四修正案之法益保護核心，乃係在於保護「人」之「隱私」而非「場所」，然而，問題是，在判斷是否該當於第四修正案所保護之「隱私」時，「場所」作為一種財產權之概念，卻仍然扮演著非常重要地位[102]。換言之，在後 *Katz* 時代，雖然將重心從「財產權模式」移往「隱私權模式」[103]，不過，在「隱私權模式」下，若欲判斷是否該當於

101 *Id.* at 259.

102 Katz v. United States, 389 U.S. 347, 361 (1967) (Justice Harlan).

103 不過要注意的是，即便在後 Katz 時代，也不乏有以財產權為保護核心的見解，例如 2012 年的 Jones 案（同後揭註 116）即為適例。由此亦可見得，雖說 Katz 案揭示第四修正案之保障核心為合理的隱私期待，然事實上，也無法否定財產權仍在同修正

「合理的隱私期待」之基準時，仍然必須借助與「財產權」有關之諸要素，尤其是「場所」此一概念至關重要。然而，問題是，在網路進行搜索扣押（也就是我國所稱之網路通訊監察）之情形，因為在網路的虛擬空間中根本沒有「場所」之觀念，更大的問題是，事實上，在網路這類的 IT 系統中所傳輸、儲存之各類數位資料的性質，並非固定，而會依存於不同的文脈[104]產生變動，換言之，在網路中根本無法預先區分所謂隱私性的數位資料與非隱私性的數位資料了[105]。事實上，若以自動化情報處理為前提，根本已經不存在所謂不重要的數位資料了[106]。而前述違憲說與合憲說雖然兩相對立，但就採取「合理的隱私期待」為基準此點之上卻屬共通，也因此兩說有著共同的問題，也就是在 IT 系統中無法借助與「財產權」有關之諸要素來判斷隱私期待是否合理，更糟的是，IT 系統本來也無法事前劃分隱私與非隱私之區塊，從而導致前述規制過剩乃至於規制不足之問題。而同樣係以隱私權作為保護核心之我國通保法（同法第 3 條參照），自亦存在有糾結於失之過嚴與失之過寬之間而致進退維谷的問題[107]。

案之保護射程範圍內，從而也就不難理解，為何後 Katz 時代在何謂合理的隱私期待之判斷上，依然無法與財產權脫鉤。

104 這裡所謂「文脈」的原文是「Kontext」也就是英文的「context」。具體上係指與 IT 系統利用者的使用位置、動作以及狀態等各種情事之關連性。

105 BVerfG, 1 BvR 370/07 vom 27.2.2008 (Rn. 1-333) Rn. 197, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (letztes Zugriffsdatum: 09.11.2018).

106 BVerfGE 65, 1 (45); 松本和彦，「基本権の保障と論証作法（二）――ドイツ連邦憲法裁判所の国勢調査判決を素材にして」，阪大法学，第 45 巻第 2 号，頁 354-355（1995）。

107 我國通保法第 3 條第二項所定「前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」云云，就網際網路之保護而言，就顯得相當蒼白無力。因為，此種區分隱私與非隱私之而異其保護之立法模式，實際上也頂多就僅能對應於傳統的中央系統的電話通訊之情形罷了，而根本無法對應分散系統的網路通訊之實際狀況，因為在分散系統中，數位資料本身之性質會隨著文脈而變動，從而根本就無法預先以數位資料本身之性質來區分其為隱私性抑或非隱私性的情報。

4.3 風險承擔理論與第三人原則

接著要討論的是，有關 *Miller* 案[108]所揭示之風險承擔理論，若適用在網路通訊監察之規制上，又會帶來怎樣的問題。有關此點，事實上，此一理論，在美國實體法上，也早有具體化的規定，即彼邦之「存儲通信法」（Stored Communication Act, SCA）除了規範像是網路通訊服務業者（ISPs）等第三方（third-party internet service providers）出於自願性或義務性的提供其所儲存的通訊資料外[109]，同時也有規定若基於具體之特定事實（specific and articulable）而有合理根據（reasonable grounds）可得認為調取之紀錄與偵查中之本案犯罪事實具有實質關連性（relevant and material）時，得申請法院核發調取票（court order）[110]。此等規定，其立法之正當化理論基礎即所謂「第三人原則」（Third-Party Doctrine）[111]。而同理論之論據乃係由前述之 *Miller* 案（本案涉及的是商業紀錄）與 *Smith* 案（本案涉及的是電話號碼）所共同確立。要之，第三人原則係指，若個人將自己的情報出於「自願性」而「任意」地提供給第三人，就必須自行承擔該第三人可能將該情報提供給政府之風險[112]。問題是，此種以風險承擔理論為核心之第三人原則，若直接套用在網路通訊監察之文脈下，將會產生如下所述極為荒謬的情形。

4.3.1 網路世界中適用第三人原則之不合理性

首先，在網路通訊之情形，所謂自願提供之部分，並不僅止於非內容之電話號碼而已，再者，以現今社會之網路使用實態而言，能否謂之為「自

108 United States v. Miller, 425 U.S. 435 (1976).

109 Title II of the ECPA, the Stored Communications Act (SCA). *See also* 18 U.S.C. § 3121.

110 18 U.S. C. § 2703 (d).

111 *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 562-66 (2009). 第三人原則使得自願提供情報給第三人之個人將不再受到第四修正案之保護，由於現代情報社會下生活的實態，事實上，很多時候人們根本是不得不「自願」提供，因而此理論受到許多研究第四修正案的學者之批判。相對於此，此處所引 Kerr 論文，則是堅決支持第三人原則，對這些批判一一提出駁斥。

112 *See Miller*, 425 U.S. at 443; and *see* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

願」提供，也非無疑。按網路通訊係在分散系統中採取封包傳輸，要傳輸的情報（通訊）會被拆解成數個封包，封包係由內容（信體）與非內容（信頭）之部分共同構成，這些複數的封包會經由分散系統所判斷之當下空閒的最效率之複數虛擬線路予以傳輸。換言之，在電話通訊之情形，就進行傳輸之目的而言，並不需要記錄通話內容，而且其之所以必須要記錄通話號碼，也係為了通訊費計算等正當業務目的；相對於此，在網路通訊之情形，要進行傳輸，在技術的本質上就必須同時複製（記錄）通訊的內容與非內容之部分，要之，網路傳輸其實就是對原始情報（通訊的數位資料）進行一連串的複製（記錄）過程。而且如果使用者不同意提供，就意味著無法使用網路服務，問題是，在現今社會中，不論是日常生活乃至於一般工作，都對網路有著高度的依存性，於此實情下，使用者根本是不得不同意。從而，若將第三人原則也一體適用在分散系統的文脈下，那麼理論上偵查機關是可以透過向各通訊業者請求提供所欲取得之對象通訊內容的方式，來架空令狀（通訊監察書）的制約[113]。

4.3.2 Carpenter 案的啟發

事實上，美國聯邦最高法院也已經開始注意到，傳統的第三人原則，在某些情況下，確實會出現適用上的不合理性。像是同院在 *Carpenter* 案[114]就指出，執法機關雖係依據存儲通信法第 2703 條(d)，合法申請法院核發調取票，藉以強制 Sprint 電信公司以及 MetroPCS 電信公司，分別提供 7 天與 152 天的過去已儲存之行動電話基地台位置情報（Cell-Site Location Information, CSLI）[115]，然由於調取票並非以相當理由作為令狀核發的審查門檻，因而侵

113 取得過去已結束之通訊內容，只不過在即時性上較通訊監察慢了一點罷了。不過，事實上，通訊監察雖說係即時同步監察，然實際上，不論是傳統的電話通訊或網路通訊，囿於人力之所限，皆係先行預錄（或預先儲存），之後再以人力或科技方式進行排查。若此，以向各通訊業者請求提供所欲取得之對象（已結束之）通訊內容的方式，就理論上而言，也未必在速度上就會遜於通訊監察。

114 Carpenter v. United States, 138 S. Ct. 2206 (2018).

115 *Id*. at 2212, 2226. Sprint 電信公司實際上提供 2 天（*Id*. at 2227），MetroPCS 電信公司

害被告受第四修正案保護之合理的隱私期待。其主要之論據係，本案透過取得大量的行動電話基地台位置情報，來推知個人過往活動之全部，此情顯然不同於 *Miller* 案與 *Smith* 案之情形，而係類同於 2012 年的 *Jones* 案[116]，蓋若認爲用戶打電話即屬於自願性揭露位置情報給電信公司而得以適用傳統的第三人原則，此解無異於賦予國家執法機關得以全面監視個人生活隱私，卻完全不受事前之司法審查，從而，本案法庭意見認爲，即便行動電話基地台位置情報係由第三人所控制，然而個人對該情報仍享有合理的隱私期待，偵查機關調取此等情報即構成第四修正案之搜索[117]。

相對於此，本案之不同意見與檢方則主張應適用第三人原則。對此，法庭意見則予以反駁指出，其一，本件系爭位置情報乃係使用行動電話所必然自動產生之紀錄（automatic nature of its collection）[118]，使用者除了開機以外並沒有其他任何積極的作爲（without any affirmative act on the user's part beyond powering up），所以並不該當第三人原則所稱「自願揭露」（voluntary exposure），從而自無法以此推定使用者自願承擔揭露風險[119]。其二，第三人原則之適用，係以「所欲取得之特定資料之本質」（the nature of the particular documents sought）作爲判斷是否具有合理的隱私期待之基準，而非以「自願揭露」爲基準[120]。本件所涉及的是長期持續大量積累的位置情報（the exhaustive chronicle of location information），相對於此，*Miller* 案的商業紀錄乃至於 *Smith* 案之撥號紀錄都是屬於類型限定的個人資料（the

則是提供 127 天（*Id*. at 2218）。

116 United States v. Jones, 565 U.S. 400 (2012). 警方在遭竊車輛內秘密裝置 GPS 定位追蹤裝置，藉此長期追蹤被處分人之每個活動（every movement），構成對第四修正案所保障之合理的隱私期待之侵害。

117 *United States*, 138 S. Ct. at 2209-10.

118 跟電話號碼不同的是，電話之使用者有進行撥號的動作，但位置情報就完全是經自動化情報處理所產生之資訊。

119 *United States*, 138 S. Ct. at 2210-11.

120 *Id*.

limited types of personal information），後者有限定性，前者並沒有，所以兩者在本質上完全不同，從而，在前者之情形，顯然已經不適宜僵化地套用傳統的第三人原則[121]。其三，素來本院的判例，從未允許執法機關得向第三人調取具有合理的隱私期待之紀錄資料（subpoena third parties for records in which the suspect has a reasonable expectation of privacy），本案所涉之位置情報（personal location information）與 *Miller* 案之商業紀錄迥然不同，前者所關涉者乃係第四修正案之保護核心，若允許其亦得逕行適用第三人原則，那麼無異於宣告（對第三人之）調取票即爲第四修正案保護之例外，換言之，若個人對於第三人所持有的紀錄資料係具有合理的隱私期待時，仍應適用第四修正案之令狀原則予以保護[122]。

4.3.2.1 「全面性」與「自動化情報處理」

如上所析，因爲分散系統的特徵，傳輸即複製，因此，人們在使用網路的同時，也必然會將其通訊相關之一切內容與非內容之資料提供給 ISP，此外，還有系統自動生成的各種數位資料，也會同時提供給 ISP。若在此文脈下，依然一體適用第三人原則，其結果無異於否定了第四修正案之權利保障。此點，就如 Leon 法官所指摘，第三人原則正引領美國聯邦法院進入奧威爾式的臨界點（an Orwellian tipping point），並使得 *Katz* 案所確立的「合理的隱私期待」基準變得不合理[123]。對此，本文認爲，可以援用 *Carpenter* 案的法庭意見所揭示的法理，讓變得不合理的隱私期待基準回復其合理性。不過，具體上，並非係全然否定第三人原則，而是合理地限縮該原則之適用範圍。申言之，若是銀行商業紀錄、電話號碼乃至於監視錄影取得之紀錄抑或此類紀錄中有揭露位置情報等情，並不在 *Carpenter* 案之判旨射程適用範圍內，換言之，此種情形仍然可以繼續適用傳統的第三人原則。要之，本文認爲，只有在符合 *Carpenter* 案的法庭意見所言及之「揭露既廣且深而有全

121 *Id*. at 2210, 2219-20.

122 *Id*. at 2210, 2221-22.

123 *See* Margaret Hu, *Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1850-51 (2017).

面性」（本文將之抽象化為「全面性」要件）以及「揭露係屬不可避免且為自動化處理」（本文將之抽象化為「自動化情報處理」要件）此兩項特徵時，方有同案判旨之適用[124]。而「全面性」要件，可評價為乃係脫胎自 2012 年的 *Jones* 案所揭示的馬賽克理論（Mosaic Theory）[125]，其侵害性核心即在於「持續大量累積」，亦即，若持續大量累積看似與隱私無涉之資訊片斷，即有可能藉此拼湊出涉及核心隱私之資訊全貌。而「自動化情報處理」要件，其侵害性核心則在於「揭露之不可避免性」，申言之，在現代情報化社會下，人們根本「毫無選擇的餘地必須自願揭露」，因為，若不將其個資等情報提供給電信公司、通訊業者、商場、信用卡公司、銀行等提供各樣服務之第三方，便根本無法使用各該服務，而且為了使用各該服務，事實上，也必須聽任各該服務系統之自動化情報處理不斷生成與其相關之各類數位資料，按若不如此，人們根本不能在現今社會下正常工作、生活。因此，本文認為，此種「不得不的揭露」乃至於「自動化生成的揭露」，根本不能認為係該當於「自願揭露」。

---

124 Carpenter v. United States, 138 S. Ct. at 2223. "We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment." 其中所稱「depth, breadth, and comprehensive reach」之部分，本文將之稱為「全面性」要件，而「the inescapable and automatic nature」之部分，則謂之為「自動化情報處理」要件。雖本案法庭意見特別強調"Our decision today is a narrow one. We do not express a view on matters not before us." Carpenter v. United States, 138 S. Ct. at 2220, 但此點，並無礙於本文援用其所言及之「揭露既廣且深而有全面性」以及「揭露係屬不可避免且為自動化處理」之法理，予以進一步轉換成抽象化之要件。

125 *See* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010); United States v. Jones, 565 U.S. 400 (2012). And *see* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320-26 (2012).

4.3.2.2 對於「風險承擔理論」與「區分論」之反思

對本文而言，*Carpenter* 案之價值，除了提供合理地限縮第三人原則於現今情報化社會之文脈下之適用範圍上所需要的法理依據外，還同時顛覆了 *Smith* 案之限定性法理之（內容與非內容之）區分論此一固有的思維框架。申言之，自 *Smith* 案以降之傳統見解認為，像是電話號碼此類非內容之通訊，並非第四修正案之保障對象，至多僅係立法者得裁量決定是否以實定法加以保護的對象罷了。但本文認為，若該當全面性暨自動化情報處理兩要件之前提下，即便形式上係屬於非內容之資訊（例如 *Carpenter* 案所涉及之位置情報），亦應解為係在第四修正案之保障範圍內。而更有趣的是，提供顛覆區分論之立論基礎的 *Carpenter* 案之多數說立場，正好是當年 *Smith* 案之少數說之立場的翻版。蓋 *Smith* 案之反對意見，早有指摘，「在實際上個人根本無從選擇的情況下來談論『承擔』風險是毫無意義的」[126]，並進一步指出「所謂隱私期待是否具有適法性，若按 *Katz* 案所揭示的基準，其判斷並非取決於人們將個資向第三方揭露時所可以接受的風險，而是取決於他在自由開放的社會中應該被迫承擔的風險」[127]。此論，與本文所稱自動化情報處理要件之核心意旨，可謂係完全若合符節。

而事實上，在我國實務上，也不乏可見所謂風險承擔理論之精神，像是最高法院 103 年度台上字第 1352 號刑事判決（下稱 103 年判決）指出：「對話之一方為保護自身權益及蒐集對話他方犯罪之證據，並非出於不法之目的而無故錄音；且因所竊錄者係對話之一方，對他方而言其秘密通訊自由並無受侵害可言，所取得之證據，即無『證據排除原則』之適用。」由此可以推知，所謂風險承擔理論，就我國實務的理解而言，乃係源自於所謂基本權拋棄的思想[128]。針對此種思想，學說上有指摘，此論有招致基本權保障

126 *See* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

127 *Id*. at 750-51.

128 並參照最高行政法院 105 年度判字第 531 號判決：「依最高法院 103 年度台上字第 1352 號、98 年度台上字第 2513 號判決等意旨，對話之一方為保護自身權益及蒐集對話他方犯罪之證據，並非出於不法之目的而無故錄音，且因所竊錄者係對話之一

空洞化之危險，故而認為其拋棄必須係出於實質上的自發性意思，且不得為概括性無期限的拋棄，拋棄的範圍乃至於結果必須明白具體且為本人所認識[129]。確實，不論是前述的 *Miller* 案或 *Smith* 案乃至於我國 103 年判決，若要求所謂風險承擔必須係基於實質上的自發性意思，那麼，實際上各該案件之情況皆不該當，換言之，此論之指摘等於完全否定擬制的風險承擔。於此意義上，應可將此論評價為較諸前述 *Carpenter* 案提供了更進一步的保障，要之，*Carpenter* 案並未修正風險承擔理論之內涵而僅係某程度地限縮其適用範圍，相對於此，此論則將同理論之內涵予以大幅縮減，即改以出於實質上的自發性意思而自願為風險承擔之情形為限。

另一方面，以非內容之通訊為對象之通保法第 11 條之 1 所定調取票，在審查門檻上也低於以內容之通訊為對象之監察令狀。此種設計，顯然也係基於區分論之思維。惟有不同者係，雖我國通說肯認，不論內容或非內容皆為憲法之通訊秘密之保障對象，此點，與美國的 *Smith* 案實屬有異；不過，在立法層次上，就非內容之部分所給予的保障低於內容之部分，則與彼邦基於區分論之法制設計思維係屬異曲同工。於此意義上，對我國而言，由 *Carpenter* 案所啟發而進一步予以抽象化的全面性要件、自動化情報處理要件乃至於不區分論，亦應具有相當的參考價值。而事實上，我國亦有論者參酌

方，對他方而言其秘密通訊自由並無受侵害可言，所取得之證據，即無『證據排除原則』之適用」。此外，在同意搜索之文脈下，也有引用所謂風險承擔理論作為正當化論據。例如我國最高法院 109 年度台上字第 5631 號刑事判決：「第三人對於被搜索之處所有得以獨立同意之權限，則被告或犯罪嫌疑人在主客觀上，既與該第三人共享空間，自其隱私之合理期待而言，應已承擔該共同權限之第三人可能會同意搜索之風險，此即學理上之『風險承擔理論』。惟根據前述基本權拋棄之說明，此所謂之『共同權限』仍應指具有共通進入、接近與相互使用兩種完整管領支配權限者，始得稱為適格之同意權人。則於同居共財之夫妻、父母對子女或家長對家屬間，因其彼此存有相互依存或主從之生活關係，對於處所享有完整管領支配權，原則上仍得肯認其同意權存在。警方本於此有共同權限之第三人同意所為之無令狀搜索，自屬有效搜索，所扣押之被告或犯罪嫌疑人之物，應有證據能力。」

129 小山剛，「憲法上の権利」の作法，頁 40（2016）。

Carpenter 案之判旨，進而建議通保法第 11 條之 1，在立法上，應該採取更高的審查門檻，亦即，其主張，同條應併同適用以相當理由進行審查之令狀原則為妥[130]。相對於此，本文則認為，通保法第 11 條之 1，是否應依據嚴格的令狀原則予以規制，非得一概而論，關鍵還是在於其是否符合 *Carpenter* 案所啟發的不區分論的適用前提。要之，就本文立場而言，雖同樣主張在自動化情報處理之文脈下 *Carpenter* 案所啟發的不區分論應值採取；不過，所謂不區分論，係以「透過自動化情報處理來持續大量累積而致有全面揭露的危險之情形」為前提；若不該當此前提，則本文認為，便應解為並不在 *Carpenter* 案之判旨的適用射程範圍內，換言之，此時，自無必要依據嚴格的令狀原則予以規制。

接下來的問題是，*Carpenter* 案所啟發的「全面性要件」與「自動化情報處理要件」相當抽象，像是前者，究竟要到什麼程度才該當於所謂「全面性」；而更有問題的是，在後者之情形，該案以「自動化情報處理」作為「否定提供之自願性」之理由，認為這是一種「不得不提供」；然而奇妙的是，在 *Miller* 案之商業紀錄，乃至於 *Smith* 案之電話號碼，在那個年代，雖然確實不該當本案所謂「自動化情報處理」之情形，但是，對於用戶而言，都是為了使用銀行乃至於電信服務所以「不得不提供（揭露）」，為何在該兩案就可以擬制為自願揭露，而到了 *Carpenter* 案，卻又轉而認為，若係在「自動化情報處理」之文脈下所為之「不得不提供」（揭露之不可避免性），就不會該當於自願揭露。要之，這裡的問題是，其實 *Carpenter* 案並未清楚說明，究竟為何在「自動化情報處理」之文脈下所為之「不得不提供」就不該當於自願揭露。為此，以下有必要從跨巨庫觀點[131]再為進一步分析。

---

130 溫祖德，「調取歷史性行動電話基地台位置資訊之令狀原則——自美國 Carpenter 案之觀察」，月旦法學雜誌，第 297 期，頁 146-147（2020）。

131 何謂跨巨庫觀點，詳請參見劉芳伶，「從跨巨庫觀點論全面探析偵查手法之合憲性問題——以『線上搜索』為檢討起點」，東海大學法學研究，第 62 期，頁 57-60（2021）。

4.4　本文提案

4.4.1　跨巨庫現象與跨巨庫型偵查手法

所謂跨巨庫，係指在我們生活的社會中，隨著情報科學技術之高度發展，已經自然而然地形成一個可以橫跨實存世界與虛擬世界進行無限連結可能性之有機融合體的巨大資料庫，此種社會現象之產生，乃係由於在現今高度情報化社會下，人們的生活已經無法脫離各種高度情報處理技術之影響乃至於支配，申言之，像是伴隨著各種智慧型端末之普及，透過「這些智慧型端末不斷地記錄著每個人的日常，而這些大量且多樣的紀錄，不但會儲存在端末中，也必然存留於通訊業者處，甚至會自動地被上傳雲端，存有許多備份，且各個資料庫系統（通訊業者、公司、醫院、政府機關等）又可以彼此相連結，成為橫跨數個不同系統的巨大資料庫，於此之上，經過大數據之運用，又不斷地產出更多的數位資料；再加諸 AI 科技之勃興及各種感測器之普及，讓整個社會轉變成為一個有機的巨大資料庫，這個巨庫可以橫跨『虛擬世界』（IT 系統）與『實存世界』（非 IT 系統）之間，不斷地探索、吸收各類大量的情報，並進而分析以增生各種新情報，而被稱為跨巨庫」[132]。

上述跨巨庫現象之文脈下引發了偵查法上新的規制難題，也就是所謂跨巨庫型全面探析偵查手法應如何規制之問題，此種手法通常可區分為四階段，即 A 設備裝置階段、B 取得資訊階段、C 儲存累積階段、D 照合分析階段[133]。其中，又以 C、D 階段為核心[134]。而此種偵查手法之侵害性核心，即

---

132 同前註，頁 58。「IT 系統」與「非 IT 系統」之定義，參見同論文同頁之註 3 與註 4 之說明。並參見劉芳伶，「從跨巨庫觀點論刑事訴訟法新設『科技設備監控處分』之定性與規制——以『GPS 科技之利用』為檢討中心」，月旦法學雜誌，第 306 期，頁 115（2020）。

133 「照合分析」乃係日文漢字，其意係指透過高度情報處理技術（例如 AI 或是大數據運算等）在複數資料庫之間，實施數據之精確或模糊的對比、碰撞或匹配，並據此進行數據之解析、推演乃至於預測。因無適合的中文對應譯語，故採直接援用日文漢字（此於我國法界並非少見，像是不當利得、起訴狀一本主義、辯護人倚賴權等等皆係直接援用日文漢字）並加註解釋之方式處理。並參見劉芳伶，前揭註 132，頁 127。

在於其具有可達成「聚沙成塔，一葉知秋」效果之「全面探析」機能。「所謂『聚沙成塔』，可借馬賽克理論為其提供具體的說明；而大數據的預測機能，則為『一葉知秋』效果之一種體現」[135]。

4.4.2 匯流技術與跨巨庫

另一方面，要特別注意者係，此種跨巨庫現象，不僅在偵查法之規制上引起新的問題，在通訊傳播分野中，也引發其規範立法模式產生巨變，即從傳統的垂直式轉向水平式。所謂垂直式立法，係以單一產業或特定技術為管制單位，針對每一個業別有個別對應的管制法規，具體上，區分固定電話、行動電話、廣播電視以及有線電視等，但自 1990 年代起，因科技創新而躍起之數位匯流（Digital Convergence）技術，產生電子通訊網路中立性之現象，而使得一個傳輸網路可以支援多個不同的產業所提供之服務，如此一來，各個產業便得以跨越業種藩籬而與其他產業相連結[136]。此種匯流技術所帶來的中立性現象，正是孕育跨巨庫不斷滋長茁壯的沃土。

所謂匯流，分三種類型，其一，科技匯流，主要係指資訊、電信、電子媒體三大部門之匯流[137]。相對於此，現行通保法卻只關注電信部門（以電信服務與電信服務業者為規範對象），顯然與今時科技發展之現況有所齟齬。其二，網路匯流，係指運用數位化以及數據壓縮技術，使所有資訊皆能轉換為數位格式，從而實現跨不同業種之相異網域之服務，例如電信網路透過網路匯流技術亦可提供傳播廣電服務[138]。相對於此，通保法顯然並未正視現今已進入通訊傳播匯流之時代，仍固守於傳統的垂直式立法，僅以電信服務業所提供之通訊網路為規範對象，而舊時立法者如此設計於今則顯有規制不足

134 同前註。

135 劉芳伶，前揭註 131，頁 59。

136 江耀國，「論水平架構之通訊傳播法制革新——層級模式、馬來西亞及英國法制與臺灣之革新草案」，月旦法學雜誌，第 224 期，頁 214（2014）。

137 同前註，頁 218。

138 同前註。

之問題。其三，服務匯流，此乃受惠於前兩項匯流技術所衍生之類型，其係指混合多種科技之網路服務或創新服務，像是隨選視訊（VOD）[139]抑或是居家電子銀行（home banking）等[140]。此種服務匯流顯然也屬於通訊，尤其VOD之使用紀錄通常涉及著作權侵害犯罪之證據收集，而取得犯罪者利用居家電子銀行之紀錄，對於追蹤金流而言更是必要不可欠；問題是，現行通保法，僅以電信服務為規範對象，自然無法包括服務匯流之情形。

對於前述三種匯流，傳統的垂直式立法顯然無法對應，因而有不少論者參酌網路分散系統之概念提出所謂水平式立法模式，又被統稱為「層級模式理論」[141]。此論，與本文採分散系統與中央系統相互對照之研究視角可謂係完全契合。所謂層級模式理論，其細部主張，雖因論者而異，惟取其最大公約數而言，可分四點說明：其一，實體層，係指提供傳輸與接收之網路實體基礎設備，其二，邏輯層；係指控制數據資訊能正確傳輸之管理系統，像是通訊協定等；其三，應用服務層，係指提供給終端使用者（消費者或其他使用者之端末）之各類通訊服務；其四，內容層，係指使用者接收或傳遞之資訊內容[142]。由此以觀，現行通保法在規制上顯然僅及於一與四，至於二與三則不在考量範圍內。事實上，前述 LINE、Gmail、Instagram 或 Facebook 非屬於電信服務業者，而係屬於應用服務層業者，然其提供之多樣通訊服務早已取代了傳統電信服務[143]，就重要性而言，絕對不遜於電信服務業者，但應用服務層之通訊業者卻非現行通保法之規範對象，在規範設計上顯然無法跟上時代發展之腳步。

4.4.3　水平式分階段規制論

基上所陳，本文認為，在跨巨庫時代下，各種通訊業透過匯流技術已經無所謂分業藩籬可言，要之，在技術面上，資訊、電信、電子媒體已經從分

139 係指使用者可以透過網路自行選擇所欲觀賞之視訊內容之系統。
140 江耀國，前揭註 136，頁 218。
141 同前註，頁 219。
142 同前註。
143 在臺灣，大概已經很少人打行動電話，而多用 LINE 等免費通訊軟體了吧。

業獨立之區分論走向打破分業藩籬的不區分論。而作為規制的法，自然也該採取同等對應才能切合現今技術發展的實際；故而本文認為不僅在通訊傳播的行政規制上應採水平式之分層模式理論，在通訊監察之偵查規制上也應採水平式立法；具體以言，上述所揭示四個分層之（廣義的）通訊業者皆應納入通保法規範，而不應僅侷限於電信服務業者。以此為前提，本文建議，在現今匯流技術下，應採如下表[144]所示之水平式分階段規制論作為通訊監察之法規範設計之基盤：

	四階段	水平式對應關係
水平式分階段規制論	A設備裝置	1 實體層：主要係以電信業者為處分對象，但可外擴至其他提供支援通訊傳播匯流所必要硬體設施之業者。 3 應用服務層：以各類通訊服務（不限於電信業者）提供者乃至於使用者（消費者）為處分對象。
	B取得資料	1 實體層：同 A 階段所述。 2 邏輯層：以通訊協定管理者[145]為處分對象。 3 應用服務層：同 A 階段所述。
	C儲存累積	1 實體層：同 A 階段所述。 3 應用服務層：同 A 階段所述。
	D照合分析	1 實體層：同 A 階段所述。 2 邏輯層：同 B 階段所述。 3 應用服務層：同 A 階段所述。 4 內容層：透過照合分析將 B、C 階段之機械語[146]轉為人類所能理解之內容。

144 本表係參酌劉芳伶，「論運用『車牌辨識技術』所為『N 系統偵查』之適法性判斷構造與要件」，軍法專刊，第 67 卷第 4 期，頁 119-120（2021）之表格予以增刪而成（惟本文所繪製之表格內容與同文該表之內容已迥然不同）。

145 例如網際網路工程任務組（IETF）、電氣電子工程師學會（IEEE）負責有線無線傳輸，國際標準化組織（ISO）等。

146 B、C 階段係由情報科技設備進行自動化處理，因此係以人類所無法直接理解之機械語型態取得與儲存。

如上表所示，在水平模式下應區分四階段進行規制：即 A 設備裝置階段、B 取得資訊階段、C 儲存累積階段、D 照合分析階段[147]。而就法規範之意義而言，A、B、C 三階段，在現今自動化情報處理之文脈下，係有可能排除以內容層為處分對象，換言之，於此三階段，在技術上係足以擔保偵查機關所取得者僅限於人類所無法直接理解、感知之非物理性的機械語（0 與 1 的組合）或物理性的訊號，而到了 D 階段透過照合、分析才將之還原成人類所能直接理解、感知的內容。因此，如前所析像是食肉獸系統等採用自動化徹底檢索技術之通訊監察工具，僅能在 A、B、C 三階段被允許使用，而且必須在技術上與法律上擔保其所取得、儲存累積之資料不會落入偵查機關的眼目，如此才能正當化其使用的合憲性與合法性。而在 D 階段，則係完全禁止使用此類自動化徹底檢索技術作為偵查手段。又有關 A、B、C、D 各階段之規範重點，其詳如下。

4.4.3.1　A 與 B 階段之規範重點

首先，在 A 與 B 階段之規範重點是，以中央系統與分散系統作為基準來進行類型化區分之規制。具體以言，像是通保法第 13 條第一項規定「通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之。但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」即係屬於 A 階段之處分。在電話通訊的中央系統思維下，要進行通訊監察係透過所謂電信服務業者，在電信服務業者的機房中進行掛線監聽，換言之，A 設備裝置階段其實係以電信服務業者為實際的被處分人。事實上，通保法第 14 條第二項也規定「電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。」不過，這些規定在分散系統的觀點下重新檢視，就會顯現出過度規制或規制不足之問題。申言之，在 A 階段，除了獲得電信業者之協助來完成安裝外，也可以由偵查機關自行安裝，而 B 階段，除可由偵查機關自行操作外，技術上，也可由業者協力代為操作。而現行法所謂的協力義務，是否可以包括代

147　劉芳伶，前揭註 132，頁 127。

為操作，則容有解釋論上的灰色地帶，畢竟 ISP 等業者並非公權力機關，就法規制上的意義而言，是否宜由其代為操作，並非無疑，故而本文以為此部分也應修法明定為妥。且若以中央系統與分散系統為類型化區分之基準，則重點將會放在 B 階段，因為，中央系統與分散系統乃係傳輸技術之分類，自係對應於 B 之取得階段。基此，可類型化區分如下圖 3 所示：

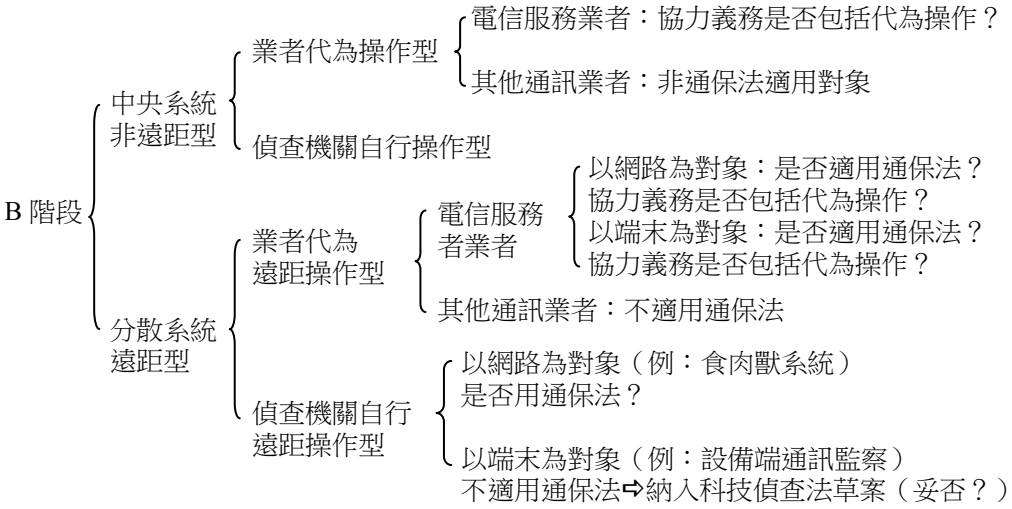

圖 3 （作者自行繪製）

如上圖 3 所示，上揭類型化區分最大的特徵在於，中央系統因為有實體的線路進行傳輸，屬於非遠距型，分散系統沒有實體的線路進行傳輸，屬於遠距型。由此類型化區分可知，通保法第 13 條第一項後段雖明定「不得於私人住宅裝置竊聽器、錄影設備或其他監察器材」云云，但問題是，在遠距型之情形，是可以藉由像是以對象者的手機、桌電、筆電甚至智慧型家電等端末為對象，植入間諜程式之方式來進行通訊監察，此時，即便形式上沒有在私人住宅裝置竊聽器、錄影設備或其他監察器材，但實質上卻可以達到與在私人住宅裝置竊聽器、錄影設備或其他監察器材一樣的效果。由此亦可窺見現行法確有規制不足之問題。當然，通保法之問題不僅止於此，同法之問題

核心是，由於欠缺分散系統之觀念，因而根本沒有意識到遠距型與非遠距型之區分在法規範上有著迥然不同的意義。首先，在遠距型之情形，不論是以網路傳輸層抑或係以端末為對象，都必須要進行「植入（可供遠距操作的間諜）程式」此一「線上侵入」步驟，而此步驟是否該當於通保法第 13 條第一項前段所定「截收」此一用語之最大文義射程範圍內，抑或是否該當於同段所稱「其他類似之必要方法為之」，已屬有疑[148]。接著，如上圖 3 所示，最值得注目之例有二，一為食肉獸系統，二為設備端通訊監察[149]。此兩例更能充分展現現行通保法欠缺分散系統觀念而導致在規範上有過與不及之問題。

首先，在食肉獸系統之情形，若就我國現行通保法之規制而言，該系統係用在掃取階段，由於其在技術上必須使用自動化徹底檢索技術，因而若僅就掃取階段來看，恐怕還是根本無法達到現行法所定通訊監察令狀之特定性要求。若此，是否可以現行通保法為據來運用食肉獸系統進行網路通訊監察，自非無疑。有關此點，本文認為，本於令狀原則之要求，若無分階段規制，單就掃取階段技術上必須使用自動化徹底檢索技術此點而言，應解為食肉獸系統並非我國通保法所允許的通訊監察手段為妥。

而在設備端通訊監察之情形，其乃係以線上搜索的方式來進行通訊監察，自屬於通訊監察之一種類型，但奇妙的是，在法規制之設計上，法務部

148 具體上，像是以線上搜索的方式，就可以遠端控制對象者家中的桌電、筆電、手機的攝錄機能，達到與於私人住宅裝置竊聽器、錄影設備或其他監察器材一模一樣的效果，但是，現行通保法對此卻無力規制。

149 科技偵查法草案稱之為設備端通訊監察，亦有翻譯為源頭通訊監察，其原文為「Quellen-Telekommunikationsüberwachung」，此種通訊監察手段運用線上搜索技術，以端末為對象，在送件者剛輸入後才送出前的這個「當下」之時點，抑或於送出後經傳輸而剛到達收件者伺服器之「當下」的這個時點，會進行「同步」記錄（監視、取得），而這兩個時點又可以被解釋為係屬於傳輸過程的一環，也因此，在法性質上，設備端通訊監察就被理解為通訊監察的一種。Vgl. Cerrit Hornung, Ein neues Grundrecht－Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“, CR (2008), S. 229. 德國刑事訴訟法在 2017 年修法增訂（同年 8 月 24 日生效）授權國家實施源頭通訊監察之相關規定，有關修正過程與內容之介紹，可以參見黃則儒、廖先志，前揭註 39，頁 131-144。

並非將之納入通保法加以規範，而係擬另立所謂科技偵查法予以規制。法務部此舉，從形式上而言，恐難免招致有割裂法體系之譏[150]；惟話雖如此，就實質面而言，由於現行通保法仍係侷限在傳統中央系統的規範思維框架內，若要將利用分散系統傳輸之設備端通訊監察納入通保法之中，亦確實有格格不入之感。又加諸拜前述匯流技術所賜，事實上，即便在 A 階段係採取中央系統之物理性裝置，但透過匯流技術，在 B 階段也可能轉為透過分散系統之傳輸路徑進行資料的取得[151]。因此，本文建議，通訊監察在規範上，應明定遠距操作型與非遠距操作型之類型化區分而異其規範方式。具體上，有可能在 A 階段遠距植入在 B 階段遠距取得，也可能在 A 階段物理性（非遠距）設置但在 B 階段遠距取得[152]。但凡係屬遠距操作之情形，不論是 A 階段之裝置抑或 B 階段之取得，其所涉及者，就不僅止於隱私或資訊自決權之侵害問題，還會涉及被處分人的行動端末之財產權侵害以及同端末系統乃至於網際網路之傳輸層 IT 系統之安全性侵害等問題；換言之，在此種情形，其間諜軟體的植入乃至系統內的探索、分析，皆係透過遠距操作之方式來實現，因此較諸非遠距操作之情形，會具有更高度的侵害性[153]。要之，遠距操作的情形，具體上，其實包括了「侵入（系統）」、「植入（軟體）」、「探索（系統）」、「複製（所有可疑為構成目標情報之拆解封包等數位資料）」、「回傳（所有可疑為構成目標情報之拆解封包等數位資料）」、「分析、抽出、還原（將經分析後抽出並解密的拆解封包等數位資料還原成目標情報）」等一連串步驟。由此可知，遠距操作之情形有必要用到線上搜索技術，而為了有效規範此種具有更為高度侵害性之一連串步驟，其立法原則（即合憲性要件）有四，即「(1)須存在有對極為重大的法益之侵害，(2)須有法官所發付的事前令狀，(3)應提供足資保護私生活形成之核心領域之預防

150 按設備端通訊監察既為通訊監察的一種類型，卻不放入通保法而另立科技偵查法，在法體系分類上顯有鑿枘之感。

151 運用數位化以及數據壓縮技術，使所有資訊皆能轉換為數位格式。

152 此即以線上搜索之方式進行通訊監察，也就是設備端通訊監察（同前揭註 149）。

153 更進一步的詳細說明，可以參照劉芳伶，前揭註 132，頁 121-123。

措施，(4)應採行高度的科學技術門檻之制約」[154]。

上揭(1)係素來所稱的重罪要件，此點並無特出之處，無待贅言。而(2)雖看似與我國令狀主義（通訊監察令狀）之要求相同，然實際上仍屬有異，亦即，事實上，上揭(2)之事前令狀，並非以我國實務通說所理解之「概括搜索票禁止原則」[155]為主軸，而係聚焦在所謂「比例原則」之上，換言之，此處的重點不在於「特定性」，而在於「最小侵害性」；按若對令狀主義之理解，係採用傳統所認知的「概括搜索票禁止原則」之「特定性」為核心要件，就會導致像是食肉獸系統這類的偵查手法在本質上就必然違背憲法所要求的令狀主義之結論，原因無他，按此類偵查手法在構造上係採取所謂自動化徹底檢索技術而使其在本質上就具有概括搜索之特性[156]。反之，若改採「比例原則之最小侵害性要求」為規制主軸，便有可能為自動化徹底檢索技術之合憲性提供分階段規制之正當化基盤。申言之，雖說不論是比例原則抑或特定性要求，其最終目的都在於追求侵害能達到最小化之目的，但特定性要求在執行上顯然較少彈性，而就自動化徹底檢索技術之使用而言，若僅單就前述 B 階段來看，是斷然無法滿足特定性之所謂應於令狀上事前明示特定應搜索扣押（通訊監察）對象之要求，相對於此，比例原則就保有較大的彈性，因其並不要求於令狀上事前明示特定應搜索扣押（通訊監察）對象，而可以靈活地以其他替代方式作為最小化的手段。故本文認為，在跨巨庫時代下，應以「比例原則之最小侵害性要求」作為令狀原則之核心，才能兼顧人權與偵查之兩難[157]。而本文所提案之分階段規制，就是這裡所謂（作為最小化的手段之）其他替代方式，具體上，就 B 階段之規制重點是，應在技術上與法律上確實擔保其所取得之內容不至於落入偵查機關的眼目[158]，於此前提

154 同前註，頁 124-125。

155 同前揭註 9。

156 劉芳伶，前揭註 131，頁 109。

157 同前註，頁 109-110。

158 具體上，此時應在令狀載明，其所欲使用之自動化徹底檢索技術為何，並具體說明在技術上如何擔保，其在運用上僅係全數掃描（暫時存取）但有限制的儲存且不會

下，再透過後續的 C 階段與 D 階段，進行分階段的進一步規制，如此便可達到比例原則之最小侵害性要求，若此，自可肯認使用自動化徹底檢索技術之合憲性。

4.4.3.2 C 與 D 階段之規範重點

接著要討論的(3)與(4)的要件，此乃為 C 與 D 階段之規範重點。首先，(3)之所謂必須有足資保護私生活形成之核心領域之預防措施，係指必須在技術上與法律上擔保不會產生跨巨庫型偵查手法之所謂「聚沙成塔，一葉知秋」之侵害性問題。聚沙成塔係單憑 C 階段的累積就可能達成，但是一葉知秋則必須動用到 D 階段的照合分析。具體以言，美國所謂馬賽克理論，其所體現者，正是跨巨庫型偵查手法「聚沙成塔」的部分[159]。亦即，馬賽克理論所指摘「取得『大量片斷』所合成的『整體』可能將完整揭示『個人私生活的全貌』」此一機能性特徵，即如將一個個的拼圖碎片拼湊成一幅完整的全圖一般，此在跨巨庫型偵查手法下，稱之為「拼圖機能」[160]。而所謂「一葉知秋」之情形，事實上並非係政府「取得」偵查所需要的情報，而是透過自動化情報處理技術（例如資料庫比對分析、AI 技術、大數據碰撞等）的「預測機能」進行情報之「產出」[161]。要之，從跨巨庫觀點來看，(3)之侵害性核心，其實並不在於持續大量累積，而係在於藉由高度自動化情報處理技術之

落入檢警之眼目。

159 詳請參見劉芳伶，前揭註 132，頁 115。

160 同前註，頁 115-116。不過，跨巨庫觀點的拼圖機能與馬賽克理論仍有不同，要之，在跨巨庫的理解下，個別「單一」的「取得」資訊路徑本身的「累積」時間長短乃至於取得「量」本身皆非重點，即便，單一的「取得」資訊路徑本身時間很短且取得資訊量不大，但其所取得的「斷片資訊」與「其他資料庫」加以「照合分析」若得以解析出受監控人生活型態或社交活動類型，那麼該「斷片資訊」可以說是拼湊出那「全幅拼圖」（受監控人生活型態或社交活動類型）所不可欠卻之最重要的一塊拼圖碎片（關鍵性片段資訊）了，此仍該當於強制處分。要之，馬賽克強調取得情報之大量累積，但跨巨庫則重視取得之後的自動化情報處理效果。參見同文頁 128。

161 劉芳伶，前揭註 131，頁 60。

「拼圖機能」以及「預測機能」，即有透過「大量或少量之片斷資訊」甚或是僅從「一個關鍵的片斷資訊」，就可以「拼湊出」乃至於「生產出」個人的「私生活形成之核心領域」之「情報的全貌」之「危險性」乃至於「實害性」。因此有必要在技術上與法律上擔保該「情報的全貌」並無被「拼湊」乃至於「生產」出來之「危險性」乃至於「實害性」。

而此處所謂「聚沙成塔，一葉知秋」之侵害性效果，正可以進一步具體化前述 *Carpenter* 案所啟發的「全面性要件」之內涵。要之，「不論是聚沙成塔型或是一葉知秋型，其實都屬於拼湊行為，只不過，前者係以過去事實的推理為目的之非預測型拼湊，而後者則是以將來可能發生的事實之推理為目的之預測型拼湊」[162]。前者的侵害性「在於收集大量的片斷數位資料後，透過情報處理以及資料庫的照合與分析，就有可能從一部分的片斷數位資料來逆推知原始數位資料的全貌，如此持續累積，最後可能將目標對象之全人格像加以完全解析」[163]。此種情形，當然該當於「全面性」，但所謂的「全面性」並不以此為限，按後者之侵害性，並不以大量、持續累積為必要，「即便，單一的『取得』資訊路徑本身時間很短且取得資訊量不大，但其所取得的『片斷資訊』與『其他資料庫』加以『照合分析』，若得以解析出受監控人之生活型態或社交活動類型之全貌，那麼該『片斷資訊』可以說是拼湊出那『全幅拼圖』（受監控人之生活型態或社交活動類型的全貌）所不可欠缺之最重要的一塊拼圖碎片（關鍵性片斷資訊）」[164]；此時，仍會該當於「全面性」要件所稱之全面侵害性內涵。

最後，有關(4)之高度的科學技術門檻，具體以言，像是如果要立法允許國家利用線上侵入技術，就必須採行適當且有效的科技措施藉以防止第三人搭便車[165]。「因為 IT 系統一旦處於被侵入的狀態，即國家利用線上侵入技術打開系統的後門，作出可以迂迴系統保全設定的被侵入狀態，此時不僅僅

162 同前註，頁 103。
163 同前註，頁 102。
164 同前註，頁 97。
165 BVerfG (Fn. 105), Rn. 204.

是國家，在線上虛擬空間中閒晃的第三人，若意外發現該系統處於此種被侵入的狀態，很有可能會因此搭便車而順道擅入該系統，故此，國家如果要立法正當化……此種偵查行為，就必須在法律上提供防止此種搭便車行為的技術性擔保」[166]。要之，不論遠距植入或取得，都以能順利侵入（進入）系統為前提，若係屬於技術上有權限的進入，自無造成 IT 系統之安全性疑慮之問題，但若是在技術上並無權限，而係依據令狀進行侵入，那麼，此種國家所為侵入系統之駭客行為，就很可能對 IT 系統之安全性上造成嚴重問題。而(4)所要求的高度的科學技術門檻，就是要國家確保其遠距侵入、探索乃至於取得之諸處分行為，不會對系統安全造成損害。

此外，在分段規制之觀點下，通保法就立法論之設計而言，還必須明定「有照合分析之預定」與「無照合分析之預定」此兩種類型而異其規範基準。所謂照合係指利用資料庫進行比對，所謂分析係指利用 AI 等各類自動化情報處理技術進行聚沙成塔型或一葉知秋型之拼湊行為。若該當於「有照合分析之預定」之類型者，「其合憲性要件有六，即(1)須存在有對極為重大的法益之實害，(2)須由法官進行符合『比例原則之最小侵害性要求』之事後審查機制，(3)應提供足資保護私生活形成之核心領域之預防措施，(4)應提供確保資料庫正確性之機制，(5)應提供擔保自動化照合分析具有透明性與異議可能性之機制，(6)應提供防止標籤化與連坐性之保護機制」[167]。(1)至(3)之要件，其內涵如前所述，於此不贅。而此處之(4)之要件則係指政府有義務於法律上與技術上確保資料庫內所載之各種情報資料乃至於其照合分析之結果的正確性[168]。(5)係指「自動化情報處理」必須受「人的監督」，而且「人的監督」必須是「由擁有變更自動化決定結果權限之人來加以實行」[169]。(6)係

166 劉芳伶，前揭註 132，頁 125；並參照劉芳伶，前揭註 8，頁 89。

167 進一步詳細說明，請參見劉芳伶，前揭註 131，頁 106、110。

168 同前註，頁 104-105。

169 第一，補強法則：亦即偵查機關不得僅以自動化照合分析結果作為處分之唯一依據，而必須有其他人為監督之下所取得或形成的依據以資補強，且此種補強依據的取得或形成的過程與內容必須是人所能理解。第二，說明義務：偵查機關對於自動

指偵查機關應就如何防止標籤化與連坐性提出具體方策，並確保該方策確實能在實施時獲得具體之落實，如此方足以肯認實施跨巨庫全面探析偵查手法之適法性[170]。

不過，上述(1)至(3)，雖適於採行令狀制度予以規制，惟(4)至(6)，若僅單採令狀規制則顯有不足[171]。對此，本文建議可併採「構造性規制」。所謂「構造性規制」，係由日本學者稻谷所提出，同論者主張，應以「代理兩難」（エージェンシー・スラック＝agency slack）理論作為基礎，以「偵查活動最適化」[172]作為判斷基準，於此前提下，其指出，作為強制處分規制的

化照合分析的過程與結果負有說明義務。進一步詳細說明，請參見劉芳伶，前揭註131，頁105-106。

170 即便資料庫係屬正確，也確保了其透明性與異議可能性，問題是，在跨巨庫之情形，有各種各樣的資料庫，例如像是透過 DNA 資料庫進行所謂「基因監察」（Genetic Surveillance），具體的作法，像是透過「家族 DNA 探索」（Familial DNA Search），意即以已經建檔之犯罪者的 DNA 資料為起點，進一步擴及其尚未建檔之親屬也作為可能的犯嫌，此舉，除有標籤化的問題外，也有古代連坐法復辟之嫌，具有連坐性侵害之性質。劉芳伶，前揭註131，頁106。

171 而至於在 C 儲存累積與 D 照合分析的二階段（對應(4)至(6)之部分），要如何踐行事前的令狀規制，會是一個難題。因為，就現行法而言，只有單一階段之令狀制度的設計，顯然係完全不足以對應 C 與 D 階段所具有的「聚沙成塔，一葉知秋」的侵害性。對此，本文認為可以採行「多階段令狀」論予以對應，此論牽涉複雜，限於篇幅，無法於此併述，僅能期待他日另行撰文申論之。此處若僅扼要以言，應說明之點有二，其一，應在刑事訴訟法中新設「對情報之搜索、扣押與拼湊」處分（情報種類千般萬別，現行法卻僅以電磁紀錄為對象，根本不足以對應跨巨庫時代下的偵查實際需求），此乃建構「分階段令狀」論所不可欠缺之實定法的制度性基盤。其二，「分階段令狀」論，在令狀制度設計上之特色有二：(1)在令狀最小化要求上，會導入「偵查活動最適化」基準，故而會要求偵查機關按各階段需求分別於事前提出 C 階段的儲存、累積（用以建構資料庫）計畫書乃至於 D 階段的照合分析計畫書，法院按照其所提出之計畫書決定是否為令狀之發放；(2)作為配套，應新設令狀應記載事項之事後追加、變更之制度，以兼顧高度情報處理技術之複雜與多變。

172 所謂「偵查活動最適化」的內涵係指，可以讓「偵查活動所產生之社會利益」獲得「最大化」之效果來「將有限的資源予以分配」的狀態，換言之，也就是經濟學上

手段，本來就並非必須採令狀主義，也可以採用構造性（アーキテクチャ＝architecture）規制主義[173]。所謂代理兩難理論，係指委託人與代理人之間，因兩人目標不同而產生的利益衝突現象[174]。同理論在政治學與經濟學中深受重視，稻谷將之運用在偵查規制上，亦即，政府為人民之代理人，人民為本人，「因代理人的不正行為（不為本人牟利而為自己謀利，也就是出現代理兩難問題）而造成的社會成本」，與「防止代理人的不正行為所需要的社會成本」，兩相平衡，規制的重點在於「合理的削減代理兩難問題所生的社會成本」[175]。所謂構造性規制，又可分為內部構造控管與外部構造控管，所謂內部構造控管即係指法執行機構（包括法執行機構的手足的延伸[176]）本身對於 C 階段乃至於 D 階段應有事先明訂的抽象管理規則與機制[177]，而外部構

所謂「實現了最效率的資源分配」的狀態。稻谷龍彥，「刑事司法の最適化と情報技術・ビッグデータの活用——GPS 最高裁判決を超えて」，情報法制研究，第 3 卷，頁 9（2018）。

173 同前註，頁 8-10。

174 同前註，頁 9-10。

175 同前註。

176 如前所述，由於食肉獸系統必須安裝在 ISP 的網路上，且必須獲得 ISP 的配合與協助才能順利安裝並有效運作，因此 ISP 作為偵查協力者，即為法執行機構的手足的延伸，屬於廣義的法執行機構。

177 「偵查活動最適化」與「內部控管」之關係係指，若只有「外部控管」之時，並無法讓「偵查活動所產生之社會利益」獲得「最大化」之效果，換言之，會造成資源分配的不效率，也就是「規制成本」之支出與「規制效果」之獲益（權利保護）兩者間不成比例，此時就必須併同搭配「內部控管」。由於跨巨庫型偵查手法涉及高度的技術性，如果僅進行「外部控管」，將會造成「規制成本」不成比例的大增（像是法院、立法機構等往往欠缺外部控管上所需要的技術人才與軟硬體設備，若只有外部控管，此時必須要花費相當大的成本才能獲取這些技術人才與軟硬體設備），若此時，在「外部控管」之同時也搭配「內部控管」，便可以有效的降低「規制成本」（因為法執行機關本身必然有相對應技術人才與設備，按惟有如此才能操作跨巨庫型偵查手法，利用這些既存的人才與設備，便可以有效控制成本），與此同時還可以提高「規制效果」（因為內部控管，一方面可以讓權利保護的階段獲得前置，另一方面也可以為外部控管提供審查的指引）。

造控管又可區分為立法機構控管、司法機構控管與獨立行政機構控管此三種類型。雖我國檢警機關乃至於調查局對於通訊監察作業具體實施皆設有要點或注意事項等內規[178]，又就外部構造控管之前兩種類型，現行法亦有類似規定[179]，只可惜，各該內規與現行法之類似規定，皆非立基於分階段規制論之前提下所為設計，而僅止於作業實施之標準化的層次[180]，抑或多出於急迫處分之思維[181]，乃至於事後報告以資備查之性質[182]所設罷了。故而就法規範上的意義仍有不足。要之，各該規定就聚沙成塔乃至於一葉知秋的侵害性問題根本無所意識，更遑論對各該問題之抑制與克服了。故此，本文認為，有必要從水平式分階段規制論之角度，重新設計內部構造控管之內規（命令）與外部構造控管之法律，尤其在後者，除立法機構控管、司法機構控管之外，更應設立獨立行政機構控管機制，因為 C、D 階段所涉及的情報量極為龐大，且專業性與技術性極高，需要通曉情報通訊技術乃至於自動化情報處理技術之人才方能全其功，若僅單靠現有的立法機關與司法機關來進行外部構造管控，恐因既存業務繁雜之重壓下兼囿於專業能力之不足，而無法克盡其功。

如上所陳，在匯流技術的推波助瀾下，跨巨庫的連結性，不僅可以跨業種，還可以跨虛擬與實體之間[183]，其間所涉及的情報處理之質與量之複雜性

178 例如，執行通訊監察作業應行注意事項（中華民國 85 年 11 月 25 日）、警察機關執行通訊監察管制作業要點（中華民國 96 年 12 月 4 日內政部警政署警署刑通字第 0960016085 號函修正）、檢察機關實施通訊監察應行注意要點（民國 107 年 10 月 23 日）。

179 立法機構管控之代表例，像是通保法第 32 條之 1 第一項規定「法務部每年應向立法院報告通訊監察執行情形。立法院於必要時，得請求法務部報告並調閱相關資料」。而司法機構管控之代表例，像是事後補發令狀制（通保法第 11 條之 1 第四項）。

180 同前揭註 178。

181 例如，通保法第 11 條之 1 第一項。

182 例如，通保法第 32 條之 1 第一項。

183 劉芳伶，前揭註 131，頁 57-59。

與巨大性，絕非人腦所能負荷，而必須依賴 AI 技術進行自動化情報處理，但問題是，AI 技術最大的特色，即在於其具有不透明性，因為 AI 是讓電腦程式自我學習，以便快速且效率地自動化處理大量有關人的數位資料，但問題是，此種電腦自我學習乃至於自律地進行自動化情報處理之過程，其實並不具有可視性（可檢驗性），換言之，事實是，實際上根本連電腦程式的設計者或操作者，也無法知悉，電腦究竟會如何學習、計算，又最後會運算出怎樣的結果[184]。由此亦可以合理地說明為何 *Carpenter* 案會認為在「自動化情報處理」之文脈下所為之「不得不提供」，應將之解為並不該當於自願揭露。因為，在自動化情報處理之文脈下，其實，使用者並不真正清楚自己究竟提供了什麼，甚或本以為自己只「自願」提供了「無關緊要」的 X 情報（自認為是無關緊要的），但萬萬沒有想到，透過自動化情報處理的資料庫照合分析竟會「產生」出 Y 情報、Z 情報乃至於 W 情報等（沒想到 X 竟然是產出 Y、Z、W 的關鍵片斷資訊）。要之，如前所析，所謂自願揭露之風險承擔理論乃至於第三人原則，本係源自於所謂基本權拋棄的思想。且如前引論者所指摘，其拋棄之範圍乃至於結果必須明白具體且為本人所認識，才能正當化此種基本權拋棄。而在「自動化情報處理」之文脈下，由於 AI 技術等之不透明性，導致其拋棄之範圍乃至於結果根本不可能達到明白具體之要求且也不可能為本人所預先加以認識，如此一來，自不可將之解為已為基本權之拋棄，而應將之解為非自願揭露，若此自無自願揭露之風險承擔理論乃至於第三人原則之適用。

5. 結論

綜上，本文認為，在跨巨庫時代下，自動化情報處理技術日新月異不斷推陳出新，*Carpenter* 案所提示之不區分論之思維，確實值得傾聽[185]，而來

184 同前註，頁 105。

185 要特別說明者係，本文雖受 Carpenter 案所提示的不區分論之思維所啟發，然本文所謂的不區分論，其視野更超越 Carpenter 案之觀點，不僅僅侷限於「內容性與非內容

自同案啟發由本文更進一步抽象化之「全面性」要件乃至於「自動化情報處理」要件之內涵，業已具體化如上所析。要之，本文主張，現行通保法應打破「通訊本身」之「隱私性與非隱私性」乃至於「內容性與非內容性」之僵化的「屬性」區分，且要跨越「電信與非電信」之區分藩籬，在此不區分論之前提下，方能關注到數位匯流跨巨庫之技術面運作實際，並聚焦於「全面性」暨「自動化情報處理」此兩要件，進行分階段之法規制[186]。而透過分階段之法規制，便可以克服如食肉獸此類使用自動化徹底探索技術之偵查手法之違憲性隱憂，而得以在偵查必要與人權保障之間取得平衡。據此，針對我國通保法將來修法之方向，本文有以下兩點建議：

第一點，有關通訊監察之法規制，應以不區分論為前提，採行水平式的分階段規制。為此，首應刪除通保法第 3 條第二項所定：「前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」按如前析，在 IT 系統中，數位資料之屬性會隨文脈而變動，故而無法預先區分其屬性係屬隱私抑或非隱私；更重要的是，在自動化情報處理之現代，基本上，已經不存在所謂不重要的數位資料，因此，本條規定並非妥

性」之區分，更擴及「隱私性與非隱私性」乃至於「電信與非電信」之區分，於此意義上，本文觀點與以 Katz 案所揭示「合理的隱私期待」之保障為前提的 Carpenter 案仍屬有異。

186 當然，這裡順帶一提，或許會有論者質疑，網路監察就算可以大量地蒐集傳輸中的資料，但在傳遞的過程中的封包往往會被加密；在加密技術日新月異的現代，是否還會有本文以上所討論的各樣問題？事實上，此種疑問顯然係放錯重點，本文既然以食肉獸為檢討素材，當然係以可以還原封包予以解密之情形為前提，實際上，加密技術雖然日新月異，解密技術也是推陳出新，若是有無法解密之情形，偵查機關也不會運用食肉獸進行封包掃取，而會改運用前述線上搜索（同前揭註 131）或設備端通訊監察（同前揭註 149）來進行偵查（此兩種偵查手法，在技術上可以迴避無法解密的困境，至於為何可以迴避，請參見同前揭註 131 所引論文之說明）。總之，本文要處理的主題就是食肉獸系統（當然以可以解密為前提），至於無法解密乃至於封包加密、解密技術對網路使用者基本權干涉之問題，根本已經完全是另一個議題了，顯然並不在本文討論射程範圍內。

適[187]。接著，內容與非內容之區分也應予以打破，因此，通保法第 11 條之 1 也應予以刪除，換言之，即便是非內容，若符合「全面性」暨「自動化情報處理」兩要件，也應適用嚴格的令狀原則，不過，這也僅限於傳送中的非內容方有適用。若係如第 11 條之 1 所定過去已經結束的通信紀錄等非內容履歷之數位資料，其實就與刑事訴訟法中所謂的電磁紀錄一樣，應該作為搜索扣押之對象。換言之，本文主張，所謂通訊監察應該專以傳送中的通訊為對象，過去既已結束之網路通訊，不論是內容亦或非內容之數位資料，都該當於刑事訴訟法之搜索扣押之對象，而不應納入通保法中加以規範。

第二點，作為水平式的分階段規制之配套措施有四：其一，應合併採行類型化之規制，主要應設計成兩大類，第一類係區分「遠距操作型」與「非遠距操作型」，第二類是區分「有照合分析之預定」與「無照合分析之預定」此兩種類型。其二，應採行令狀規制與構造性規制之雙軌制。令狀規制主要係針對 A 設備裝置階段與 B 取得資訊階段，而 C 儲存累積階段與 D 照合分析階段，若僅單有令狀規制仍屬不足，還應併同採行構造性規制，方得完整。其三，應採行高度的科學技術規範門檻。因為自動化情報處理，涉及 AI 等各類情報科學技術，此類技術若使用於偵查，如僅有法規範上的制約擔保，顯然不足，還必須加諸技術上的安全性擔保，舉例以言，如前所析，若國家要使用線上侵入技術進行設備端通訊監察，那就必須確保已經在技術上採取足以防止第三人搭便車趁機混入遭國家執法機關所侵入之系統。因為在現代社會中，IT 系統運作之效能性與安全性能否被維持，此點，其所涉及的是國家存立之根本。要之，跨巨庫時代下，人們的生活日常與工作乃至於國

187 我國有論者提出應該依據通訊資訊之私密程度建立層級化之管控機制。劉耀明，「通訊監察之層級化事前管控機制」，刑事法雜誌，第 60 卷第 6 期，頁 56-58（2016）。相對於此，本文則認為，此論於現今跨巨庫時代已經不合時宜，因為在自動化情報處理之文脈下，所謂資訊之私密程度根本無法單就該資訊本身來做判斷，而必須依存於判讀該資訊之文脈為何而定，即便本身看似與隱私無關之私密程度極低的通訊資訊，透過 C 階段的大量累積抑或 D 階段的照合分析也可能拼湊抑或預測出與核心隱私相關的極密資訊。

家秩序、經濟發展等都無法脫離 IT 系統，於此意義上，高度的科學技術規範門檻之必要性乃至於重要性也就不言可喻。其四，在自動化情報處理之文脈下，若有產生「聚沙成塔，一葉知秋」此種全面性侵害之可能性者，就無適用風險承擔理論或第三人原則之餘地。

最後要附帶說明者係，法務部於 2020 年 9 月所公告之科技偵查法草案，在當時，引起各界強烈的質疑與反對，故其立法進程被迫暫停，延宕迄今。而該草案第三章第 14 條以下所定設備端通訊監察之各該條項，即如本文所前指摘，就體系而言，本屬於通訊監察之一環，奇妙的是，法務部卻不納入既存的通保法予以規範，而係另立所謂科技偵查法，此舉實有割裂體系之嫌，自難謂為妥適。惟話雖如此，然就實質而言，整部通保法，係以中央系統作為制度設計之前提，根本難以規範設備端通訊監察此類跨巨庫型偵查手法，從而另立他法以為規範，或許也是另一種囿於現實之不得已的解方亦未可知。然而，問題是，如前所析，由於跨巨庫型偵查手法，在技術之本質上就必須使用自動化徹底檢索技術，而具有高度的基本權干預性，若不打破區分論並同時改採水平式分階段規制，根本無法克服其所帶來的高度侵害性，也就難以肯定其立法之正當性。

而綜觀科技偵查法草案的立法架構，根本上，其實與通保法並無二致，亦即，其在本質上還是延續區分論的舊思維，妄圖藉由區分隱私與非隱私來保護分散系統中的隱私[188]，藉此對抗設備端通訊監察之侵害性，而其結果就是，必然難以保護且無法對抗[189]。更大的問題是，該草案根本完全沒有中央系統與分散系統之差異性觀念，如此一來也就根本不可能意識到跨巨庫型偵查手法有 A、B、C、D 四階段，應採行分階段規制之問題，更遑論要注意到匯流科技對於通訊監察在規範上之意義。因此，就法理論以及法政策而言，本文認為，只要確保立法規範之設計，係能克服跨巨庫型偵查手法所使用之

188 參見通保法第 3 條第二項；以及同草案第 2 條第一項第二款、第三款，第 3 條第一項。

189 因為分散系統中的數位資訊本身的屬性（是否為隱私）會隨文脈而變動。

自動化徹底檢索技術之全面探析機能所具有的「聚沙成塔，一葉知秋」之侵害性，即可獲得立法論上的正當性，而得以肯認跨巨庫型偵查手法之合憲性與合法性；反之，則否。由此觀點以言，科技偵查法草案之規範設計，也不過是在現行通保法已採行的隱私與非隱私之區分論的延長線上所為固有設計思維框架下的產物，由於其並未採取高度的科學技術規範門檻之分階段規制，顯然係完全無法克服跨巨庫型偵查手法所具有的「聚沙成塔，一葉知秋」之侵害性，從而並不具備肯認其合憲性與合法性的正當化之論據。要之，從本文立場而言，割裂體系另立所謂科技偵查法並非立法論的上善之策，比較妥適的作法是，應採行分散系統之跨巨庫觀點以徹底改變現行通保法之體質，並導入水平式分階段規制論，再將設備端通訊監察此類跨巨庫型偵查手法一併納入一體規範方為正途。

參考文獻

中文書籍

林俊益，《刑事訴訟法概論（上）》，新學林，臺北（2021）。

林富郎，《通訊監察法制化之研究（司法研究年報第 21 輯第 12 篇）》，司法院，臺北（2001）。

中文期刊

王士帆，〈網路之刑事追訴——科技與法律的較勁〉，《政大法學評論》，第 145 期，頁 339-390，2016 年 6 月。

江舜明，〈論通訊保障及監察法第三條之立法妥當性〉，《法學叢刊》，第 50 卷第 3 期，頁 101-126，2005 年 7 月。

江耀國，〈論水平架構之通訊傳播法制革新——層級模式、馬來西亞及英國法制與臺灣之革新草案〉，《月旦法學雜誌》，第 224 期，頁 213-252，2014 年 1 月。

李榮耕，〈即時通訊程式的通信紀錄的調取〉，《月旦法學教室》，第 212 期，頁 23-25，2020 年 6 月。

林三欽、陳愛娥、郭介恆、陳春生，〈通訊監察與秘密通訊之自由學術研討會〉，《憲政時代》，第 23 卷第 2 期，頁 4-50，1997 年 10 月。

林鈺雄，〈干預保留與門檻理論——司法警察（官）一般調查權限之理論檢討〉，《政大法學評論》，第 96 期，頁 189-232，2007 年 4 月。

林鈺雄，〈論通訊之監察——評析歐洲人權法院相關裁判之發展與影響〉，《東吳法律學報》，第 19 卷第 4 期，頁 109-152，2008 年 4 月。

黃則儒、廖先志，〈從德國 2017 年通訊監察法制修正論我國對通訊軟體監察之立法方向〉，《檢察新論》，第 24 期，頁 131-144，2018 年 8 月。

溫祖德，〈調取歷史性行動電話基地台位置資訊之令狀原則——自美國 Carpenter 案之觀察〉，《月旦法學雜誌》，第 297 期，頁 130-147，2020 年 2 月。

劉芳伶，〈概括搜索票禁止原則與另案扣押・附帶扣押制度／最高院 100 台上 5065 判決〉，《台灣法學雜誌》，第 291 期，頁 183-186，2016 年 3 月。

劉芳伶，〈遠距搜索扣押與令狀之明示特定〉，《東海大學法學研究》，第 49 期，頁 45-96，2016 年 8 月。

劉芳伶，〈從「系統性」觀點論檢察之「特別偵查體制」建構與「事物管轄」觀念〉，《檢察新論》，第 24 期，頁 9-31，2018 年 8 月。

劉芳伶，〈從跨巨庫觀點論刑事訴訟法新設「科技設備監控處分」之定性與規制——以「GPS 科技之利用」為檢討中心〉，《月旦法學雜誌》，第 306 期，頁 111-138，2020 年 11 月。

劉芳伶，〈論運用「車牌辨識技術」所為「N 系統偵查」之適法性判斷構造與要件〉，《軍法專刊》，第 67 卷第 4 期，頁 91-122，2021 年 8 月。

劉芳伶，〈從跨巨庫觀點論全面探析偵查手法之合憲性問題——以「線上搜索」為檢討起點〉，《東海大學法學研究》，第 62 期，頁 55-119，2021 年 10 月。

劉耀明，〈通訊監察之層級化事前管控機制〉，《刑事法雜誌》，第 60 卷第 6 期，頁 25-60，2016 年 12 月。

日文書籍

小山剛，《「憲法上の権利」の作法》，3 版，尚学社，東京（2016）。

井上正仁，《捜査手段としての通信・会話の傍受》，有斐閣，東京（1997）。

井上伸雄（ほか共著），《新通信情報早わかり講座 3》，日経 BP 社，東京（1999）。

井上伸雄，《〔図解〕通信技術のすべて：基礎知識からクラウド、モバイル、次世代通信まで》，日本実業出版社，大阪（2011）。

田村武志，《図解・情報通信ネットワークの基礎》，2 版，共立出版株式会社，東京（2000）。

村田正幸，《マルチメディア情報ネットワーク：コンピュータネットワークの構成学》，共立出版株式会社，東京（1999）。

日文期刊

川崎英明，〈盗聴立法の憲法的問題点〉，《法律時報》，第 69 巻第 4 号，頁 47-52，1997 年 4 月。

佐伯仁志，〈プライヴァシーと名誉の保護——主に刑法的観点から—3—〉，《法学協会雑誌》，第 101 巻第 7 号，頁 1406-1473，1984 年 7 月。

松本和彦，〈基本権の保障と論証作法(二)——ドイツ連邦憲法裁判所の国勢調査判決を素材にして〉，《阪大法学》，第 45 巻第 2 号，頁 339-360，1995 年 8 月。

稲谷龍彦，〈刑事司法の最適化と情報技術・ビッグデータの活用——GPS 最高裁判決を超えて〉，《情報法制研究》，第 3 巻，頁 3-14，2018 年 5 月。

英文期刊

Bellovin, Steven M., Matt Blaze, Susan Landau & Brian Owsley, *Seeking the Source: Criminal Defendants' Constitutional Right to Source Code*, 17 OHIO ST. TECH. L.J. 1 (2021).

Eichenlaub, Frank J., *Carnivore: Taking a Bite Out of the Fourth Amendment*, 80 N.C. L. REV. 315 (2001).

Georgiton, Peter J., *The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-Mail and Why There Is Nothing You Can Do About It*, 62 OHIO ST. L.J. 1831 (2001).

Gilman, Johnny, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS 111 (2001).

Haglund, Rich, *Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, Is Congress or the Supreme Court Best-Suited to Protect Fourth Amendment Expectations of Privacy?*, 5 VAND. J. ENT. L. & PRAC. 137 (2003).

Hartzog, Heal, *The "Magic Lantern" Revealed: A Report of the FBI's New "Key Logging" Trojan and Analysis of Its Possible Treatment in a Dynamic Legal Landscape*, 20 J. MARSHALL J. COMPUTER & INFO. L. 287 (2002).

Horn, Kimberly A., *Privacy Versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Age*, 29 FORDHAM URB. L.J. 2233 (2002).

Hu, Margaret, *Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819 (2017).

Kerr, Orin S., *Internet Surveillance Law After the USA Patriot Act: The Big Brother that*

Isn't, 97 NW. U. L. REV. 607 (2003).

Kerr, Orin S., *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

Kerr, Orin S., *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

McClintick, James, *Web-surfing in Chilly Waters: How the Patriot Act's Amendments to the Pen Register Statute Burden Freedom of Inquiry*, 13 AM. U. J. GENDER SOC. POL'Y & L. 353 (2005).

Power, Robert C., *Changing Expectations of Privacy and the Fourth Amendment*, 16 WIDENER L.J. 43 (2006).

Smith, Graham B., *A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L. REV. 481 (2001).

Sylvain, Olivier, *Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance*, 49 WAKE FOREST L. REV. 485 (2014).

Thirty-Fourth Selected Bibliography on Computers, Technology and the Law, 28 RUTGERS COMPUTER & TECH. L.J. 485 (2002).

Tufaro, Gina, *Will Carnivore Devour the Fourth? An Exploration of the Constitutionality of the FBI Created Software*, 18 N.Y.L. SCH. J. HUM. RTS. 305 (2002).

其他英文參考文獻

Comparison – Centralized, Decentralized and Distributed Systems, GEEKS FOR GEEKS (Oct. 8, 2021), https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/.

Decentralized System, COMPUTER HOPE (June 7, 2019), https://www.computerhope.com/jargon/d/decentral.htm.

DiSabatino, Jennifer, *Carnivore Gets a Name Change*, COMPUTERWORLD (Feb. 12, 2001), https://www.computerworld.com/article/2591165/carnivore-gets-a-name-change.html.

Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcommittee on the Constitution of the Committee on the Judiciary, 106th Cong., 2nd Sess. (2000).

Smith, Stephen P., J. Allen Cridern, Henry H. Perritt, Jr., Mengfen Shyong, Harold Krent, Larry L. Reynolds & Stephen Mencik, *Independent Review of the Carnivore System* (Dec. 8, 2000), https://www.epic.org/privacy/carnivore/carniv_final.pdf.

Tyson, Jeff, *How Carnivore Worked*, HOW STUFF WORKS (Nov. 27, 2000), https://computer.howstuffworks.com/carnivore.htm.

其他德文參考文獻

BVerfG, 1 BvR 370/07 vom 27.2.2008 (Rn. 1-333) Rn. 197, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (letztes Zugriffsdatum: 09.11.2018).

Hornung, Cerrit, Ein neues Grundrecht－Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme“, CR (2008), S. 229-306.