國立交通大學

管理學院碩士在職專班科技法律組

碩 士 論 文

建立個人廢棄物資料庫之隱私權限制

--以輔助犯罪偵查為中心

PRIVACY LIMITATION OF BUILDING PERSONAL LITTER DATABASE:

Focusing on Criminal Investigation Assistance

研 究 生：張彥閔

指導教授：林志潔 博士

中 華 民 國 一 百 年 一 月

建立個人廢棄物資料庫之隱私權限制

--以輔助犯罪偵查為中心

PRIVACY LIMITATION OF BUILDING PERSONAL LITTER DATABASE:

Focusing on Criminal Investigation Assistance

研 究 生：張彥閔　　Student：Yen-Min Chang

指導教授：林志潔　　Advisor：Chih-Chieh Lin

國 立 交 通 大 學

管理學院碩士在職專班科技法律組

碩 士 論 文

A Thesis

Submitted to Institute of Technology Law

College of Management

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Technology Law

January 2011

Hsinchu, Taiwan, Republic of China

中華民國一百年一月

建立個人廢棄物資料庫之隱私權限制：

以輔助犯罪偵查為中心

研究生：張彥閔　　指導教授：林志潔 博士

國立交通大學管理學院碩士在職專班科技法律組

中文摘要

當犯罪案件發生後，目前的犯罪偵查模式，主要仍然依靠個案承辦人員的經驗以及其熟悉的偵查方式，對可能的嫌犯進行調查與訴追，而偵查的效率及成果，便與承辦人員個人的工作經驗習習相關。另一方面，資訊科技的進步一日千里，各種資料庫的分析工具不斷推陳出新；同時，隨著硬體製程的進步，處理大量資料的時間也不斷縮短。本研究的目的即是在探討是否能將資料探勘技術應用於輔助犯罪偵查，特別是利用建立與國民個人資料相關的關聯性資料庫，而後利用資料庫關聯分析來輔助犯罪偵查進行。

個人資料庫的建立是此一科技力量能夠輔助犯罪偵查進行的基礎，但建立個人資料庫勢必會影響到國民個人的隱私權益。本研究首先針對外國以及我國對於隱私權的發展以及隱私權特有的性質進行分析，並主張可以在適度的範圍內，蒐集個人主動棄置的個人相關資料以建立關聯性資料庫，但需排除敏感性較高的個人相關資料，例如健康資訊等。

本研究亦根據現行的科技技術，提出可用以建立及管理個人資料庫的意見，以及將此類分析結果用於犯罪訴追的助益。由於隱私權具備了知悉隱私權內容不以佔有為要件，以及隱私權內容洩漏不易察覺這兩個特殊的性質，這使得隱私權的權益範圍難以界定，同時一旦隱私權受到侵害，影響程度很可能可以持續很長的時間。因此，除了排除敏感性較高的個人相關資料，不納入個人資料庫的蒐集對象外，本研究亦主張針對此一關聯性資料庫的存取權限，需要經過適當的設計，使得在不影響資料分析的完整性前提下，僅有特定的被授權人能夠取得完整的資料分析結果。對於將資料探勘技術引進犯罪偵查，本研究主張在適當的管控

之下，針對敏感性較低的個人資料建立關聯性資料庫，便能夠在避免個人資料不慎流出的風險之外，善加利用科技的力量，達成促進犯罪訴追效率的目的。

關鍵字：資料探勘、關聯性分析、個人資料庫、隱私權、犯罪偵查、強制處分、財產權、文字辨識、物品辨識、毒品、管制藥品、犯罪資料庫

Privacy Limitation of Building Personal Litter Database: Focusing on Criminal Investigation Assistance

Student：Yen-Min Chang　　Advisors：Dr. Chih-Chieh Lin

Institute of Technology Law, National Chiao Tung University

ABSTRACT（英文摘要）

Once a crimial case happened, present criminal investigation mode, personal mainly depends on personal experience of investigators. Once there is a civilian personal database built based on relational database, it would be helpful in using the database for criminal investigation.

However, building such kind of personal database would face on the issue of civilian privacy interference. The thesis aims at the development of privacy, international and domestic, and the particular characters of privacy, and tries to provide a proper possibility to build a kind of relational database of civilian personal information but exclude highly sensitive personal information, such as healthy information.

The thesis also considers present technologies and tries to control use of the database. Since privacy has two important characters: knowing privacy contents does not require occupying the contents, and privacy contents leakage is not easy to be detected, once privacy is infringed, the damage could extend for a long time. Therefore, access authority of the relational database should be properly designed to limit only very few authorized people, such as prosecutor of the case, being able to access full analyzing results, to minimize the possibility of data leakage as well as to enhance criminal investigation.

KEY WORDS: data mining, relational analysis, personal database, privacy, criminal investigation, prosecutors' order, property, text identification, object

identification, drug, controlled drug, criminal database.

誌謝

這一本論文由契機、發想到完成，算來也跨過了八年歲月，這其間，我自服完新竹遷到台北，又回到台中定居，卻在新竹工作；從一個懵懂的門外漢，而成為以法律安身立命的工作者。我的專長在專利，最終卻完成這本「標離本業」的論文，其間過程雖未必是峰迴路轉般精彩，也與我過往十年人生歲月有緊密的關係。我的指導老師說她要以「學生最後一個學位的指導者」的心態來面對每一位學生，呼應老師如此的願力，我以這一本論文作為可能是我最後一個學位論文的交代，若我能從中獲得真實的滿足，這份榮耀當歸於摯愛我的父親、母親、家妹、家弟、以及我親愛的妻子與一雙子女。他們對我永不止息的愛與包容，支持我走過生命中重要的轉折，而最終能夠踏下這一步來。

這一本論文終能完成，首要感謝我的指導老師－林志潔老師。在老師的課堂裡，我獲得本篇論文的發想，老師也不斷地給予我相當多的指導與意見，讓我有如黏土般一團的想法開始收斂且有了發展方向；論文報告後，又花了一年時間才將其餘的骨肉長出，這中間波折不斷能夠獲得老師持續給我指導與鼓勵，是我完成全部論文的最佳動力！

我還要感謝口試委員：王敏銓老師與蔡蕙芳老師，在口試中給予我直接且中肯的意見，讓我能發現不足之處。蔡蕙芳老師也是我對刑法學科的啟蒙老師，感謝她如此

熱心嚴謹的回覆我諸多不成熟的問題，讓我對刑法這門學科始終保持高度的興趣。

謝謝劉尚志老師，一路上不斷花時間回覆我對於科法的疑問，我才終能進入科法所，遇到許多精彩萬分的老師，他們開始改變我對法律的態度，讓我瞭解過往對法律認知的狹隘，以及對事物尊重的態度。陳韋君老師是個重諾的人，印象中我從未收到她臨時要變更上課時間的通知。她是跨國律師，每月工作時數往往超過三百小時，某次為了給我們上課，工作期間由美國飛回來，隔天上完課再飛回去，我事後問她時得知時瞠目結舌，而她卻顯得從容。言教身教，她相當程度影響了我日後的工作性格。羅明通老師具有開闊的心胸，鼓勵學生踴躍發言，學期結束後，蒙老師致贈新版著作權法論，序言中赫見我在課堂上的意見，使我更懂得表達意見須謹慎為之。吳巡龍老師是檢察官，證據法在他的講述之下，字字嚴謹，句句縝密，無一處不合邏輯，卻又在關鍵處留白，讓學生非得絞盡腦汁將課前資料反覆思考後，才能連貫起一切，非常精彩！

有如此優秀的老師們之外，我還要感謝我的好同學、學長姐：儷卿、偉相、翔鴻、正義、明錫、景智、珮慈、珀如、彥婷、貞懿、怡妃、彥程、遠翔、慧珍、念勤、倍嫻。有你們並肩修課、討論、作報告，才能熬過那數十學分的挑戰，沒有這些互相砥礪，一個人能獲得的將遠少於此，而且，實在是很苦悶呀！

我也要謝謝碩班的同學們：鴻嫻、琳君、姿瑩、景澤、筑安、慧芝、可嘉、峰源、建中、嘉玲、慕嘉、泉仲、大諭，能夠與你們一起承擔所上的活動令我難忘、你們願意聆聽我這門外漢的問題，並且給予我意見我很感激！其實你們才是學長姐、我倒是佔了年紀的便宜了，感謝你們給予我的，祝福你們振翅高飛！

謝謝蔡慶龍、李麗玲、楊大勇、林宗德、陳玉玲、陳威淋、林培梅、陳靜怡、茂瑞章、陳炯榮、YL、RC、YC、CK、FL、KH、CO、LZ、Danny、Enzo、Eugene，你們是我工作上的好長官、好同事、感謝你們支持著我在工作之外、還鼓勵我追求學問精進！

特別要感謝孝華、在我面臨屈辱的時候、透過書信、交談給我清澈的、向上的力量、讓我堅定前行、清風明月、是我的貴人。

自與風城結緣、總以清筆人行走，而今下筆後卻無法停止的衝動、說是誌謝、卻更包含了對本所人、事、物的感念，我走入殿堂、今天將邁此門而出，謹以此文表意，實難忘我是科法人而已。

民國一百年一月，於新竹

秀閔

目錄

圖目錄

一、 緒論

（一）、研究動機

試想這樣的情況發生：在台北市發生了一起犯罪案件，而司法單位在案件發生前，已經依照地區的分類方式，逐漸蒐集於日常生活中隨同垃圾一併丟棄的個人資料，並依照屬性分類為各式資料庫。於是，當案件發生時，檢警人員依照現場留下的跡證，準備進行犯罪偵查工作；同時，將現場留下的跡證特徵，利用資料探勘技術，與資料庫進行比對後，便可初步歸納出符合特定生活習慣特徵之人物，而於犯罪偵查的初期，便可有效率的限縮調查範圍，迅速地找出犯罪嫌疑人，發揮協助犯罪偵查的效果。

利用日新月異的資訊技術力量，來協助犯罪偵查，甚至分析出人力所無法分析出的特徵，並非遙不可及。當犯罪發生時，檢警人員會針對犯罪現場所存留下來的跡證，開始進行偵查工作；關於證物，則會針對現有之資料庫進行比對，以試圖尋找出可能在場的人物。以往，需要使用到資料庫搜尋的技術時，多是為了要比對某一特徵是否與資料庫中所建立的檔案相符，常見者例如指紋分析，又或者是 DNA 分析。此類搜尋，所著重者為先分析待鑑定物，提取出待鑑定物的特徵之後，針對資料庫進行搜尋，找出已建立的資料中，是否存在與待鑑定物相同之資料，是一種逐一比對的技術；當搜尋到判定為與待鑑定物相同的資料，或是搜尋整個資料庫而沒有發現可用的資料時，搜尋便會結束。

相對而言，另外一種以符合資料採礦(data mining)方式建立之資料庫，係將資料以有系統的分類方式進行歸類，可理解為資料庫中具有許多分門別類的子資料庫，當需要進行搜尋時，可同時針對不同資料庫中，被定義為具有相同或類似特徵的資料進行搜尋，並產生關聯性分析結果。直觀地，若要對此類資料庫進行資料分析，則需要比前述單一資料庫比對更為強大的運算能力，方能縮短資料分析的時間。隨著資訊科技的日趨進步，現今的資訊科技已能在短時間內處理極大

的資料量，藉由資訊科技的能力，便能做到過往做不到的分析運算，而且能夠在短時間之內完成並且產生分析結果。

關聯性分析是否真能對犯罪偵查產生一定的助益，進而縮短犯罪偵查的時間，或者提高犯罪偵查結果的正確性？或許可由流行的電視劇集裡看出端倪。在美國流行的犯罪影集「Numb3rs」（台譯：數字搜查線）裡，一對兄弟，哥哥為聯邦調查局探員，而弟弟為絕頂聰明的數學天才。影集中弟弟每每運用其數學知識，協助哥哥偵破複雜的案件。在某一集裡，數宗由被害人身份看不出關聯性的謀殺案發生了，而後弟弟使用了資料採礦中的關聯性分析，從數宗案件中，藉由系統運算的結果，歸納出其中的共同點，從而找出與前述事件表面上看似無關的真正的主嫌犯。在美國，也有專書[1]討論此影集中所應用之各種數學分析工具，因此，若真能夠將此類技術引進於犯罪偵查中，便有能實現利用資料庫關聯分析來輔助犯罪偵查進行的可能性。

此類分析的基本前提為，國家必須要針對國民的個人資料，廣泛地進行蒐集，並且建立資料庫；而後，才有資訊科技介入以分析的可能性。以此觀之，國家為遂行其行政管理國家之目的，能否對國民的個人資料進行廣泛無特定目的的蒐集、分析？如果可以，又該針對哪些國民的個人資料做蒐集分析？對於哪些國民資料不能如此處理？進一步言，該如何界定蒐集國民個人資料的限制？又該如何界定分析國民個人資料的限制？若限制過多，則將導致無法產生有效的分析結果；若限制過少，則國民無異暴露於個人資料被過度揭露的風險當中。相對於前述國家之行政行為，國民對於其個人資料得否被蒐集、分析，是否有權益可以主張？若如此，前述蒐集分析行為是否將構成對國民個人權益之侵害干擾？另外，前述蒐集分析行為造成之侵害干擾是否有密度之差異？最後，若國家能遂行此一蒐集分析之行為，那麼，國家該如何管制蒐集與分析之過程，以確保在達成協助犯罪偵查目的的同時，不會因為國家對資料庫的管理不當，而導致國民的個人資

[1] KEITH DEVLIN and GARY LORDEN, THE NUMBERS BEHIND NUMB3RS: SOLVING CRIME WITH MATHEMATICS, (Plume), (2007).

料被流出。

凡此種種，應為社會發展與法治發展趨向完熟之國家所應重視之問題，即在一般人民基本權，例如生命權、財產權、自由權，受到重視討論並具有憲法保障之基礎後，所應進一步討論者，例如自由權之言論自由，人民於羈押其間所應受憲法絕對保護之權利等等。前述國家之行政管理所欲干涉之標的，即為國民的個人資料，其中公開性相對較低之資料內容，例如健康狀態、個人財務狀態等，由於其內容多半僅個人得知，並且不常公開或顯露於外，其受隱私權所涵蓋的範圍便顯得明顯，且需要保護（關於隱私權討論之演進，稍後將介紹）。此等隱私內容所受保護之程度，以及國民對該等隱私內容散佈之控制程度，近年來於國內外之個案中亦多有討論。

作為社會的一份子，大多數人民處於群居生活環境中。每個人於日常生活中，總會多多少少與社會中的組織或個人產生互動，互動過程逐漸演繹出每個人對社會的適應化行為，好比待人處事之方式，說話、飲食、書寫生活習慣等等。此一後天社會化的過程，為每個人塑造出獨特的人格特質，而人於日常生活中之種種行為，亦會受到這些社會化過程中所養成之人格特質的支配。因此，理解人的人格特質，甚至進一步判斷特定人物的人格特質，即可以相當程度的解讀該特定人物的行為模式，甚至進而預測該特定人物的可能行為模式。

（二）、現況概要

以現今臺灣的都會生活樣態而言，每人每天所收取與傳遞出的資訊內容相當豐富，包含日常慣用的電子郵件、實體信箱、交換名片、日常帳單等等。每個人在接收訊息的同時，也同時在釋放出與自身相關的各種訊息，一旦這些訊息的交流形成網絡之後，即會逐漸地形成一種自生的訊息交換。舉例而言，消費者在進行購物活動時，可能會留下個人聯絡資料（例如實體地址、聯絡電話以及電子郵件地址）、喜好產品與活動等等資料。廠商在接獲這些資料後，可能會依循消費

者留下的聯絡資料，定期發送與商品相關的特定資訊給消費者，或者廠商也可能在取得消費者同意後，將消費者資料提供給同一集團之其他廠商或合作廠商，以提供更多商品資訊給消費者。這些商品或者是會員資訊再透過各種管道傳遞給特定消費者， 最常見的形式為透過郵件、電子郵件等等管道發送資訊，當消費者丟棄這些資訊時，例如將郵件丟掉，或者將電子郵件放置到垃圾桶中，則其上所載的種種資訊也一併被丟棄。目前當消費者在申辦這些會員資格或者信用卡時，已經常可於合約條款中發現到此類的欄位，需要消費者確認是否願意將此類個人資訊提供給某些特定的合作廠商使用。若消費者不同意，則會員的資格或者申辦信用卡卡種的選擇，即會受到某些限制。

若消費者將這些文件丟棄，則消費者所丟棄的，可不僅僅只是商品資訊而已！消費者也一併丟棄了許多關於個人消費的資訊；同時，其他隨附於文件上的資訊，例如消費者的聯絡方式、性別、稱謂等等資訊，也一併被消費者丟棄了。進一步言，那些資訊經過累計分析之後，還可能傳遞出消費者的部分生活習慣。舉例而言，消費者在信箱中收到一件百貨公司的促銷活動傳單，通常這類的活動傳單係直接將消費者的姓名以及地址，以貼紙方式貼附在折頁傳單上，有些單位在寄發這些傳單時，還會在收件者欄位還會附上消費者的會員帳號代碼及/或購物累計點數。當消費者看完傳單而後將其丟棄時，其本意雖然是不再需要傳單上的商品資訊，但是丟棄傳單這個行為卻連帶地將個人資訊一併丟棄了。

當其他人拾獲這些被丟棄的傳單時，亦連帶的將取得該消費者的個人資訊。若能長期的蒐集這些資訊，並建立關聯性資料庫，則這些隨附在傳單上的個人資訊被他人讀取的結果，很可能可以藉由統計分析與關聯性分析，從而解析消費者的生活習慣，解讀出過往消費者所丟棄的這些資料中，所能夠透露出的個人行為特徵，此時，這些分析結果便逐漸跨入隱私權所涵蓋的個人領域之中。

在前述舉例中，逐一深究，便會產生許多值得進一步探討的疑問。對於已經丟棄的物品，個人是否仍有隱私權可以主張？若有，隱私權能夠主張的範圍是否

受到限制？能否涵蓋該物品後續所有可能之利用行為？相較於此，國家對於個人已經丟棄的物品，能進行何種利用？利用過程中，對於依照物品上所載資訊所建立的資料庫，各資料之間，若藉由進一步分析所能呈現之性質，是否仍有前述隱私權主張之存在？前述種種行為，若有應受保護之隱私權存在，則國家為遂行行政目的而進行前述蒐集與分析行為時，能以何種方式保護隱私權？

（三）、研究目的

為解析前述關於隱私權的進一步討論，本文先分析隱私權主張於各國之現況發展，透過理解現況下隱私權與基本權之關係為，隱私權已逐漸被各國家之行政體系與社會體系承認為係基本權內涵之一，而我國亦透過司法院大法官會議之解釋，將隱私權解釋為是一種基本權之內涵，詳述於後。因此，以隱私權人的角度出發，針對前述的行為，隱私權人所能主張之權利內涵，以及權利所能及之範圍為何？他人或國家存取此等隱私權內容時，過程的難度不同，是否導致該隱私權內容受到保護的程度有所差異？自隱私權內容所推演出來的各種分析結果，於國家存取其隱私權及/或分析結果時，又需受到如何的規範？是本文所所要討論之重點。特別是對於國家，在能夠存取國民隱私權的前提下，為了達成協助刑事案件訴追的目的，對於隱私權內容的存取以及利用，需要事前詳細的討論並且受到仔細的規範。

1. 隱私權之發展

隱私權之起源源自為一種獨處的權利，表達個人希望不受外界環境干擾的意志。雖然人生活於群居社會，但總有希望處於獨自一人環境下的時刻，此時其人應具有獨處的權利，他人於未受其同意的狀況下，不能侵犯其獨處的狀態。隨著社會發展變遷，人與人之間的交流日趨頻繁，彼此之間交流的工具也日趨複雜，隱私權亦逐步發展，演進為擴張至個人亦具有散佈個人資訊之控制權（在此所謂之散佈，雖未見明確之定義，偏向於第一次散佈）。即，個人得決定關於個人隱

私之資訊內容是否要為他人所知悉，例如大法官釋字第 603 號於探討關於國民換發新身份證時，是否需按捺指紋。個人對於某些一望即知的個人資料，例如外觀長相以及姓名等等資訊，個人對於這些資訊的流通控制力較低，意即這些資料於現今社會中，屬於容易被探知的資料，因此他人獲取這些資料的方式，不必然需要經過擁有者的同意；同時，若透過公開管道獲取這些資料，也不必然構成對該人隱私權的侵犯。

相對地，對於某些較隱密又足以代表個人特徵的資料，例如個人的指紋、生物特徵等等，雖然此等資料可能經由個人的行為，留存在公開場合，例如握持茶杯時可能留下指紋、喝水時唾液可能留下 DNA 資料等等，但他人並不容易直接取得此等資料，且並不容易對其內容進行鑑別，通常需透過適當的儀器工具輔助方能完成。因此，相對於之前容易被探知的資料而言，個人對此種隱私資料應具有更高度的隱私期待性，意即所有人應在其有意願的前提下，才允許這些隱私資料被收集或者公開。

逐漸地，隨著人們對於隱私權的認識與重視，隱私權由原本「獨處的權利」的討論，逐漸擴張至「隱私內容的流通控制」。在早期隱私權始於「獨處的權利」時，隱私權的概念係關於個人希望不被打擾時，能夠排除他人的干擾，可視為是一種相對消極的，對於自由權利主張的平衡，希望他人自由主張權利時，不要干擾到個人希望不被打擾的自由。而後隱私權的討論隨著社會發展日趨複雜，人與人的交流越來越多元化而逐漸發酵，隨著人們對於隱私權的研究加深，也開始對隱私權的性質加深研究，發覺隱私權亦可能衍生出各種不同的性質內涵。同時，隱私權內容的價值與其所有人具有高度的相關性，意即隱私權的內容散佈或利用與否，受到影響最大的，通常是該隱私權內容的所有人。故，隱私權的內容的流通控制權利，或者稱為隱私資訊控制權，便逐漸成為受到重視的議題。當隱私權人能夠適當控制隱私資訊的第一次流通時，才能較為有效地控制隱私資料不為其他人所知悉，從而減少因隱私資料流通散佈對隱私權所有人造成的影響。

相對於此，國家在為達成某些公共利益目的例如訴追犯罪的前提下，是否能以其具公權力執行之地位，在透過法規解釋及特定執行方式規範下，有限度的侵入公民之隱私權領域，而在社會利益與個人利益維護之間求取一種平衡，是本文所要討論之重點。

2. 隱私權之性質

當隱私權內容流出而進入公開領域後，通常隱私權人再難以有效控制資訊的複製及散佈，當這些公開的資訊終於回擊到隱私權人身上時，即可能對隱私權人造成一定程度的困擾，而且由於資訊公開的程度通常已難受到隱私權人的控制，故此困擾即可能更持續對隱私權人造成困擾。典型者例如金融機構或者購物網站，將客戶的個人資料外洩，導致客戶持續可能受到詐騙集團的詐騙，即便金融機構或者購物網站即時修正安全管理措施，或者對客戶的該次受詐騙交易或消費行為進行補償，亦無法確保客戶不會繼續受到詐騙集團的詐騙，因為其相關個人資料已經流出，且由於犯罪者可能會複製該些個人資料進行二次利用或者與其他集團進行交換，故該些個人資料無法保證能百分之百追回，其中部分資料，例如個人通訊地址或者永久地址，具有相對不易變更的屬性，因此這一類隱私資料流出的情況，形同個人資料已經永久流出且難以彌補。

此等狀況對於隱私權人而言並不樂見，但隱私權人需等到自己真正發現隱私資料已經流出才能察覺此狀況，否則隱私權人通常相當不容易發現其個人資料已經在自己不知道的狀況之下流出。以前述金融個人資料為例，直到發生狀況時，例如隱私權人接獲詐騙電話，隱私權人才會發覺資料外洩了，在此之前，並無法覺知其個人交易資料可能已經在未經授權的情況下被洩露出去；但等到其發覺此一個人資料洩漏狀況時，通常隱私權人已經面臨難以補救的窘境，這些未經授權便洩漏的個人資料，會持續在外面流通，使隱私權人一而再再而三的被打擾。由前述舉例可知，因此當隱私權人無法控制其自身的隱私權內容資訊的流通時，相對而言，就可能面臨無法預期的資訊流出，且造成比較嚴重的後果。

進一步言，由於現今科技的發達，有些個人資訊，原本是隱私權人認為除了自己願意揭露外，他人無法窺探者；但藉助科技力量即可能於隱私權人不知情的狀況下獲取此類資訊。例如透過紅外線感測技術或者透過遠距離聲音感測技術，即可能於遠距離外得知個人於屋內的活動狀況或者談話內容；又例如透過網路傳遞資料，例如個人資料或者信件，亦有可能於加密的狀態下，在傳遞過程中即被攔截解密，或者個人的電腦/行動裝置受到駭客程式感染，於個人未察覺狀態下，裝置中的資料透過此類程式便被發送至特定處。上述情況大致說明了個人的資料可能被直接獲取的情況，有些資料即使隱私權人認為該等資料是安全的或者中性的，若被洩漏也不會對自身造成過度困擾，於是減弱了對這些資料的控制，例如載於信件或者文書上的個人相關資料。但隨著資訊科技的發展，這些看似中性的個人資料，經過資料比對以及處理之後，可能轉化為透露出個人習慣的分析結果。而此類分析結果，雖未經與當事人比對確認結果的正確性，但極有可能具有一定程度的準確性，而並非當事人樂意見其發生之狀況。上述狀況皆有可能使得個人的隱私內容在不知不覺之間即逐漸洩露，而隱私權人對此等資料洩漏的狀況卻可能在事情發生當時並不知情。

關於分析許多零碎、中性或者無害的個人資料，而獲取個人的隱私內容，大法官釋字第 603 號中，林子儀大法官即提出如下見解：「蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。[2]」此類資料庫比對技術，隨著硬體與軟體技術的日新月異，經

[2] 參見大法官釋字第 603 號，林子儀大法官協同意見書：「蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。故為因應國家和私人握有建立並解讀個人資訊檔案的能力，避免人時時處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。本院釋字第五八五號解釋亦係有鑑於此，而將個人資訊之自主控制權納入隱私權保障範圍內，不限於個人秘密不受揭露的自由。」

過適當的設計與執行，即可能藉由瑣碎的資訊，拼湊出關於個人的行動軌跡或者其他隱私資訊。

3. 資訊科技對隱私權之影響

國家藉由行政機關行使龐大的行政力量，當其為遂行行政目的，尤其為了達成某些社會公益時，其能藉由法令所賦予的行政權的行使，對人民做出某些強制的行為，例如規置交通規則與交通號誌，使人民於道路上行動時，必須遵守這些規則與號誌，違反前述規則的，國家可以對其處以一定程度的裁罰或者限制其行動自由。或者，國家可以藉由行政機關，為其進行一些有計畫的作業，由於行政機關遍佈在國內各地區，其與人民的日常生活作息步調息息相關，同時行政機關更可藉由行政契約或者命令，使民間單位與其配合，以遂行其行政任務，因此此類的計畫性作業，由政府來施行，便具有一定程度的便利性與不可替代性，例如人民日常生活垃圾的蒐集以及處理，由於其具有公益色彩，且其需要龐大的人力、場地並且是全國性的需求，故由國家來主導處理較能發揮適當的效能。若由私人機構來處理，除可能無法滿足全國之需求外，亦可能面臨舊業主無法經營時，新業主不一定能概括承受舊業主已經建構完成的服務模式，而使人民感到不便。

在現今科技日漸發達的同時，人們也藉由科技所帶來的便利性增加了許多人與人互動的管道與機會，好比因網路發展所形成的許多溝通平台，例如即時通軟體、Web 2.0[3]概念等等，以及日漸成熟發展的資料庫比對技術，例如人們經常使用 Google 的搜尋引擎，藉由組合不同的關鍵字，來尋找所需要的資料。這些科技進展雖然可能導致個人隱私權受到未得允許的刺探的可能性增加，但另一方面，若國家能夠謹慎使用此類科技進展所帶來的優點，利用這些技術來輔助執行某些行政任務，亦可能帶來效率行政之好處。

[3] 關於 Web 2.0 概念，請參考 O'Reilly 公司的介紹，
http://tim.oreilly.com/news/2005/09/30/what-is-web-20.html，最後瀏覽日期 2009.11.17

若人民自願釋出或放棄一些個人隱私資料，使其處於公開狀態，則該些已釋出之個人隱私資料，依照目前的一般概念，由於隱私權人已經自願釋出或者放棄該些資料，國家與其他人亦能夠持有並且進一步利用。舉例而言，個人外出時，通常無法要求其他路人不能觀看並記錄其長相、外觀及衣著；又例如個人在公開的網路平台上公開個人資料時，即無法限制平台上其他用戶不能閱覽此公開資訊；再例如平日丟棄的垃圾中，若包含個人資訊之物品，亦無法要求其他人不得獲取物品並檢查其內容。此種狀態可理解為，雖然個人具有獨處的權利以及資訊自決的權利，但當個人的時間空間與他人重疊時，此種屬於個人自身的資訊內容，一旦洩漏成為公開狀態，則便無法阻止其他人自由讀取的權利。概言之，隱私權人將一些隱私權內容有意識置於公開公共空間的資訊，其他人即可具有存取該等資訊的機會。典型的例子為，在美國，個人棄置在公共空間的垃圾，政府單位可以搜索其中的物品，並在某些情況下，可以就其中所搜索到的物品為基礎，申請搜索令狀進行進一步搜索[4]。若後續警方可以證明在垃圾中所搜尋到的物品，確與犯罪事件以及該原持有人有直接相關性時，則相當程度地，警方即可以據此向管轄法院申請到對該原持有人之住宅進行合法搜索的搜索令狀。

如果說警方能夠針對個人所棄置的物品或者資料進行搜索與分析，那麼以此為基礎，再往前延伸，便產生了一個具有討論價值的議題：為提高犯罪偵查的成功率及效率，警方可否針對個人所棄置或者釋放出來的資料，進行持續不斷地蒐集，以建立各種資料庫，並且藉由適當的資料庫比對技術，以期能夠掌握某些個人的行為軌跡，例如遷移慣性或者生活習性等等，以於犯罪發生後，輔助警方進行偵查。相對於此，雖然此類資料為個人所主動放棄的，但利用國家行政機器進行此種資料蒐集，以及後續分析的機制，是否仍可能導致對人民隱私權的直接或者間接侵害？若是，侵害的程度是否可能與侵害行為能獲致的社會公益相當？若國家得施行此種機制，國家又該以何種密度來對其進行保護？在資料蒐集階段與

[4] *See* Jim Jenkins, *The state of our trash in Florida: the use of evidence found in residential Gargabe to establish probable cause to search a citizen's home*, 82-Jan Fla. B.J. 30, 30 (2008)

資料分析階段，其檢視與保護的標準是否有所不同？這些都是值得進一步探討的問題。

本文將就現今的資料庫分析比對技術作進一步的介紹與分析，並且探討隱私權之權利主張，是否能及於個人已經公開出來的資料內容以及進一步蒐集與分析之種種可能作為。

（四）、文獻回顧

本部分的文獻回顧，主要針對國內與國外相關的文獻進行歸納整理。由於我國關於隱私權的法令規定較欠缺由上到下的系統化架構，其中與隱私權有關者，多為少數單獨的法條，散見於各部法律之中，而且我國憲法中，亦無明文關於隱私權之規範，係透過司法院大法官於案例中之解釋，將隱私權納入憲法第 22 條以及第 23 條所要保障的基本人權之中。因此，期望透過同時參考我國與國外相關文獻的整理與歸納，對本論文所要探討的隱私權議題，指引出較為明確的方向。

本論文的結構先以隱私權與資訊科技的發展現況為基礎，再接續討論隱私權的特有性質，以及利用資訊科技力量協助犯罪偵查，可能對隱私權造成干擾。因此，文獻回顧部分，亦是配合前述結構進行檢索；由於本論文所要進行的資料蒐集方式較為特殊，因此文獻回顧部分主要針對隱私權與資訊科技的發展進行歸納整理。

以保障隱私權與執行公權力兩者之間的平衡，以及資訊科技可用於犯罪偵查之應用為方向，將國內外相關文獻以地區及相關議題區分為以下大類：

一、歐美關於保障隱私權與執行公權力之案例以及論文

隱私權一詞最早出現於 1890 年美國學者 Samuel D. Warren 和 Louis Brandeis 於哈佛法學評論上發表的—隱私的權利(the Right to Privacy) [5]—一文中。本論文提出一個觀點，所謂隱私權係指一個人在一般狀況下，自行決定他的思想、觀點

[5] *See* Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

及情感，與他人交流程度之權利。有關隱私權的法律發展，在許多國家中便因應許多個案累積，透過立法、司法系統的解釋與創造，逐漸成為備受關注且重要的議題。在美國，隱私權的問題多見諸於與搜索扣押相關的刑事判決中，關於美國憲法第四修正案之討論，幾個著名的案例有：Hoffa v. United States (1966)、Katz v. United States (1967)、California v. Greenwood (1988)、United States v. Hedrick (1991)、State v. Schwartz (2004)。在 Hoffa v. United States[6]案中，法院認為憲法並不保護這種將自己的隱私內容告訴錯誤信任之人而使其內容被洩漏之狀況。將此一原則引伸適用。在 Katz[7]案中，法院確立了當事人欲主張隱私權之成立，必須具有合理的隱私期待性原則。在 California v. Greenwood[8]案中，最高法院認為，當個人將物品丟棄到垃圾桶時，由於已經拋棄了對這個物品的所有權，而且垃圾桶內的物品可以被任意搬動，因此垃圾桶內之物品的隱私內容，會被視為已經公開給公眾。在 United States v. Hedrick[9]案中第七巡迴法院以物件棄置於公開地域來判斷原持有者棄置之行為得視為其已經表現出不再想要持有該物件之意圖；此時，公眾（或其他特定不特定第三人）即具有無須棄置者同意即可檢視該物件之權利。在 State v. Schwartz[10]案中，法院認為依照 Katz 案建立的隱私權保護原則，為成立隱私權保護的可能性，個人需要對隱私內容表達合理期待性。

隨著案例的演進，許多學者也提出關於前述議題的見解。Jerry Kang 於 *Information Privacy in Cyberspace Transactions*[11]一文中指出，在提出隱私權所欲解決之問題主體乃在於個人，其著重於個人針對隱私權內容做出一決定時之意志表示。Jennifer Murphy 於 *Trash, Thermal Imagers, and The Fourth Amendment: The New Search and Seizure*[12]文中，認為類似的案件在美國逐漸引起關於搜索扣押可

[6] *See* Hoffa v. United States, 385 U.S. 293 (1966)
[7] *See* Katz v. United States, 389 U.S. 347 (1967).
[8] *See* California v. Greenwood, 486 U.S. 35 (1988)
[9] *See* United States v. Hedrick, 922 F.2d 396, (1991).
[10] *See* State v. Schwartz, 689 N.W. 2d 430 (S.D. 2004).
[11] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, (1998).
[12] *See* Jennifer Murphy, *Trash, Thermal Imagers, and The Fourth Amendment: The New Search and Seizure*, 53 SMU L. Rev. 1645, (2000).

能侵犯人民隱私權議題的討論，加上科技的進步，使得探測的能力日趨進化，更有可能以各式各樣的新技術，對個人進行探測，這使得憲法第四修正案的規範內容越來越受到挑戰。同時，以財產權為基礎所發展出來的隱私權相關解釋，可能有需要進一步修正的空間。而 Jim Jenkins 於 *The state of our trash in Florida: the use of evidence found in residential Garbage to establish probable cause to search a citizen's home*[13]一文中指出，個人將垃圾棄置在公共空間時，已放棄對於該垃圾的隱私權主張，政府單位可以搜索其中的物品，並在某些情況下，可以就其中所搜索到的物品為基礎，申請搜索令狀進行進一步搜索。中國學者岑釗梅在〈電子時代的隱私權保護--以美國判例法為背景〉[14]一文中，歸納出以隱私權之質性進行判斷，包含「獨處性」、「秘密性」、「自治性」、「匿名性」及「親密性」等性質，並且將美國關於干擾隱私權之判斷方式，歸納出以下原則：分別為知覺提升/替換原則、普遍公眾使用原則、明知且自願暴露原則、明知且被動暴露原則、第三方知情而暴露原則等等。

在歐洲，類似的隱私權爭議案件，也成為研究的對象。歐盟國家協定出了歐洲人權公約，在歐洲人權公約中，其第八條規定每個人的「私人及家庭生活、其家庭以及其通訊隱私的權利與自由必須受到尊重，若需要對此做出限制，則必須「符合法律規定」且「為民主社會所必需」[15]。另外，歐洲警察署建立有犯罪相關的個人資料庫，可供會員國彼此之間瀏覽並且交換資料，其相關規定可見於歐洲警察署公約第 8 條[16]。案例方面，在 I v. Finland[17]一案中，歐洲人權法院最終

---

[13] *See* Jim Jenkins, *The state of our trash in Florida: the use of evidence found in residential Garbage to establish probable cause to search a citizen's home*, 82-Jan Fla. B.J. 30 (2008)

[14] 岑釗梅，〈電子時代的隱私權保護--以美國判例法爲背景〉，《中外法學》，Peking University Law Journal, Vol. 20, No. 5, 頁 773-777（2008）。

[15] Article 8 – Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[16] *See* http://www.europol.europa.eu/legal/Europol_Convention_Consolidated_version.pdf

[17] *See* I v. Finland, (2008). http://epic.org/privacy/intl/echr-finland.pdf

判決「資訊系統欠缺合理安全措施，即構成隱私權侵害」，這課與了建立資訊系統者一個積極的義務。另外，在一些民事爭議案件中，雖然與刑事或者行政爭議不同，但法院於案件中對於何謂隱私權的保護，以及何謂積極作為的討論，也相當具有參考價值。在 Earl Spencer and Countess Spencer v. the United Kingdom[18]一案中，歐洲人權委員會呼籲英國政府應有義務對其國民提供有效的保護私人生活免於受干擾的措施。另外，在 Von Hannover v. Germany[19]一案中，歐洲人權法院認為德國應進一步善盡對於個人私人生活提供保護的積極義務。

二、我國關於保障隱私權與執行公權力之案例以及論文

在我國早期中，對於隱私權之保障並無專法規定，目前，關於隱私權受到侵害之處理方式，係藉由主張較為相近之民刑法之規定來保護或者去除侵害。根據司法院大法官第 293 號解釋文的相關解釋條文，大法官承認隱私權為憲法所保障的一種基本權利，第 509、503、603 號解釋文更進一步解釋如何兼顧對於個人名譽、隱私、及公共利益之保護。另外，如同前文提及，在大法官釋字第 603 號中，林子儀大法官[20]亦提出其見解。

在國內學者方面，蔡達智所著之〈隱私權初探〉[21]提出判斷是否具有隱私權之方法，包含「隱私權核心理論、同意與利益衡量」等。另在其所著之〈開放空間中的隱私權保障〉[22]中，提出開放空間中的個人隱私權的問題,主要不外乎監視、定位與追蹤三項行為，開放空間中取得的個人資訊行為到底有沒有侵害個人隱私權?在沒有一般客觀的標準提出之前，只能從各個行為的態樣與類型，予以

---

[18] *See* Spencer v. United Kingdom, Ent. L.R. 1998, 9(4), N70-71

[19] *See* Von Hannover v. Germany, 4 Int'l J. Const. L. 533 (2004).

[20] 參考大法官釋字第 603 號，林子儀大法官協同意見書：「蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。故為因應國家和私人握有建立並解讀個人資訊檔案的能力，避免人時時處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。本院釋字第五八五號解釋亦係有鑑於此，而將個人資訊之自主控制權納入隱私權保障範圍內，不限於個人秘密不受揭露的自由。」

[21] 蔡達智，〈隱私權初探〉，《法學叢刊》，50 卷 3 期，頁 93-98（2005）。

[22] 蔡達智，〈開放空間中的隱私權保障〉《月旦法學雜誌》，No.145，（2007）

歸納。唐淑美、顏上詠、顏于翔、洪德俊，於〈應用生物辨識於網站購物之隱私權探討〉[23]提出隱私權可以理解為是一種可以分辨個人與他人之間不同之一種狀態權利，而可直接或間接鑑別個體的資訊，稱為個人資訊(personal data)。廖福特於〈個人影像因私語新聞自由之權衡—Von Hannover 及 Peck 判決分析與台灣借鏡〉文中，針對歐洲的個人私人生活與新聞自由，以及國家及媒體使用個人影像之方式及界限進行研究[24]。

三、資訊科技可用於犯罪偵查之應用

利用資訊科技，可以對資料倉儲進行關聯性分析。資料倉儲係「具備主題導向、整合性、時間便異性與不可變動性之資料集合，以支援一決策過程管理」[25]，此一定義係由資料倉儲的先創者 W.H. Inmon 於 1990 年代所提出的，其明確的揭示資料倉儲具有四特性。Frawley 定義資料採礦為「一種具有不明確性、未知性、以及潛在利用性的資訊程序，以自資料庫中採集資料」[26]。而 Grupe 和 Owrang 則認為資料採礦是「由已存在的資料中，探查出新的事實，且能發現專家並未知曉的新關係」[27]。由以上的定義，可以概略瞭解資料採礦程序最終目的是希望能夠發現隱藏於龐大資料庫中的新事實，或者是隱藏在資料之間的知識價值。

林鈺雄於刑事法理論與實踐[28]以及刑事訴訟法(上)-四版[29]中，皆明確指出犯罪偵查中，例如搜索、逮捕之時機，一旦錯過，即可能成為直接影響國家追訴權

---

[23] 唐淑美、顏上詠、顏于翔、洪德俊，〈應用生物辨識於網站購物之隱私權探討〉，《產業論壇》，第九卷第二期，頁 103（2007）。

[24] 廖福特，〈個人影像因私語新聞自由之權衡—Von Hannover 及 Peck 判決分析與台灣借鏡〉，《政大法學評論》，第九十一期，頁 145-198，（2006）

[25] "A data warehouse is a subject-oriented, integrated, time-variant, and nonvolatile collection of data in support of management 's decision making process" *See* W.H. INMON, PRISM, WHAT IS A DATA WAREHOUSE? (Volume 1, Number 1, 1995)

[26] *See* Frawley, W. J., Gregory, Piatetsky-Shapiro, and Matheus, C. J., Knowledge Discovery in Databases: An Overview, AAAI/MIT Perss, California, pp. 1-30, (1991)

[27] *See* Grupe, F. H., and Owrang, M. M., Database Mining Discovering New Knowledge and Cooperative Advantage, Information Systems Management, Vol. 12, No. 4, pp. 26-31, (1995)

[28] 參見林鈺雄，刑事法理論與實踐，頁 36-37 （2002）。

[29] 參見林鈺雄，刑事訴訟法(上)-四版，頁 267 （2005）。

是否得以行使之決定因素。明確指出偵查工作進行之效率對於成敗的影響甚大。Daniel J. Steinbock 在其所著的 data matching, data mining, and due process[30]，指出有幾個因素讓文本採礦或資料採礦能夠成為犯罪偵查的利器。其中之一自然就是當面臨日漸龐大的資料庫時，必須要藉助資料工具才能順利從中找尋資料，尤其在防患未然方面，可以藉由平日的模擬與演練，事先過濾出一些「觀察名單」，以減少或消弭可能發生的犯罪。國內有黃壬聰於犯罪偵查勤務之研究[31]一文中將偵查勤務依其內容概分為受理報案、情報諮詢、查贓、盤詰檢查、現場處理、查察探訪、背景調查、跟蹤監視、搜索扣押、拘提逮捕、詢問、移送遞解、查證追贓及擴大偵破等十四項。文本採礦/資料採礦固然希望可以發揮犯罪事前預防犯罪發生的效用；在犯罪偵查時，亦能協助前述偵查勤務的執行。

目前一些國家的司法系統已經接受某些資料庫的分析結果，並且使用於協助司法案件進行，比較廣為人知的資料庫比對技術，有例如美國警方所採用的指紋資料庫比對技術[32]及英國警方採用的 DNA 資料庫比對[33]等技術。又例如，在 2007 年，歐洲警察局(Europol)的重大犯罪部門(Serious Crime division)發展出一套文本採礦分析系統，用以針對跨國組織犯罪進行資料分析。此一綜合分析系統整合了目前最先端的文本分析以及文本採礦技術，並協助歐洲警察局在執法時能夠提升到國際犯罪的層級[34]。

另外，在犯罪預防方面，「社會心理學」[35]一書中指出，一個人對於某件事

---

30 *See* Daniel J. Steinbock, Data Matching, Data Mining, and Due Process, 40 Ga. L. Rev. 1

31 參見黃壬聰，犯罪偵查勤務之研究，中央警察大學刑事系研究所碩士論文，1999 年 6 月，頁 18。

32 參見美國邁阿密達德分局關於犯罪現場鑑識部門之工作簡介網頁 http://www.miamidade.gov/mdpd/BureausDivisions/bureau_CrimeSceneInvestigations.asp，最後瀏覽日期：2009/07/27

33 參見英國國家 DNA 資料庫網頁 http://www.homeoffice.gov.uk/science-research/using-science/dna-database/，最後瀏覽日期：2009/07/27

34 關於歐洲警察局之資料庫介紹，請參見歐洲警察局官方網頁之介紹 http://www.europol.europa.eu/index.asp?page=facts，最後瀏覽日期：2009/12/2

35 David O. Sears, Jonathan L. Freedman, L.Anne Peplau, 「社會心理學」，編譯黃安邦，校訂陳皎眉，初版，民國 75 年，9 月，頁 227。

物的看待態度，可被認為是在認知、感情、行為這三項成分上，對於該人事物或觀念的一種持久取向。個人態度裡，單純的評估成分是行為的主要決定因素，意即個人對於某事物的看法整體而言傾向好或者不好，這與事實不同，因為態度除了事物本身以外，還要加入評估或情緒的成分[36]。犯罪預測的概念，典型者例如 Ernest Watson Burgess 等人於 The Workings of the Indeterminate Sentence Law and the Parole System in Illinois [37]一書中，針對假釋犯人之假釋後行為研究。他們做出了一個評量量表，總共歸納出 21 個正向特殊背景因子並指出，若能夠將行為量表化，則符合越高比例「良好行為」者，發生反社會行為的比例即會降低。

由以上介紹可知，就隱私權的性質而言，目前歐美各國對於個人主動棄置的物品，多半採取個人不再能主張隱私權之態度。同時以目前資訊科技之發展，若能在相對較短時間之內處理大量資料並完成關聯性分析，則說明資料庫之比對技術確能藉由蒐集分析許多片面資訊，進而拼湊出一個人的行為軌跡或者生活習慣，這並非僅僅是一種臆測。本研究所希望達成的目的，在於適度存取個人隱私權內容的前提下，由國家來建立與個人相關之關聯性資料庫，以輔助犯罪偵查。由於比較歐洲、美國、以及我國之案例，歸納對於處理因侵害隱私權所引發的爭議問題時，發覺此類隱私權相關討論尚未見到相關於隱私權獨特性質之討論，因此本文將針對處理因建立資料庫而侵害隱私權所引發的爭議問題時，司法系統應採取何種保護措施，以期能提出進一步的看法與建議。

（五）、研究方法

本文的研究方法如下：

1. 文獻資料分析法

---

[36] 同前揭註，P232。

37 ANDREW A. BRUCE, ALBERT J. HARNO, JOHN LANDESCO, AND ERNEST W. BURGESS, THE WORKINGS OF THE INDETERMINATE SENTENCE LAW AND THE PAROLE SYSTEM IN ILLINOIS (Springfield,Ill. Parole Board, 1928)

為理解過去至今隱私權的發展，以及既存的隱私權態樣，針對國內外已發表之論文進行分析，以歸納出隱私權的定義以及受到關注的隱私權議題與發展。

2. 比較研究法

透過對美國、歐洲、以及我國的隱私權保護之規定的不同，分析其特點及其意義，俾供我國於未來建置相關規定時能參酌。

3. 質性訪談法

針對本論文所觸及的隱私權內容，訪問專家的意見，以期能釐清本文所關注的行政行為是否可能產生益處，同時個人隱私權受到侵害時的侵害程度所可能產生的影響。預計訪談對象包含社工師、司法人員、資料庫工程師等相關人員。

（六）、研究範圍

本文之研究範圍之一為針對國家是否得針對個人棄置的隱私資訊進行處理，此部分主要係由研究美國關於垃圾棄置所引發的隱私權爭議進行探討。本文之另一研究範圍為現今資料庫比對之技術發展，試圖說明資料庫之比對技術確能藉由蒐集分析許多片面資訊，進而拼湊出一個人的行為軌跡或者生活習慣，而非空穴來風之臆測。

本研究所希望達成的目的，在於檢視於現今資料探勘技術發展下，是否能以輔助犯罪偵查之社會利益為目的，在適度存取個人隱私權內容的前提下，由國家來建立與個人相關之關聯性資料庫，以輔助犯罪偵查。由於此類隱私權相關討論亦常見於歐美各國，因此本文將比較歐洲、美國、以及我國之案例，歸納對於處理因侵害隱私權所引發的爭議問題時，司法系統態度上的不同處，以期作為我國建置相關規定時之方向參考，希望能以他山之石，促進我國相關法制之發展。

二、 資料庫比對技術

本章將簡介現今的資料庫比對技術，以從中探討將此技術應用於適合於本論文討論範圍內之可能性。

（一）、何謂資料倉儲（Data Warehouse）

資料庫比對技術乃是希望從成堆的資訊中，將預計所需的部分正確的取出來的資料處理技術。為了達成正確擷取資料的目的，我們需要一個完善的資料庫。如此，使用者在撈取資料時，才能有正確的來源，便於產生有價值的資訊。建立這種資料庫的技術，稱為資料倉儲（Data Warehouse），如同建造一個虛擬的倉庫，將各種資料依照屬性或資料本身所攜帶的線索，分門別類安置在適當的位置。當使用者需要搜尋資料時，則依循資料屬性或者線索，便能找到同種類的資料。

資料倉儲係「具備主題導向、整合性、時間便異性與不可變動性之資料集合，以支援一決策過程管理」[38]，此一定義係由資料倉儲的先創者 W.H. Inmon 於 1990 年代所提出的，其明確的揭示資料倉儲具有四特性。因此，資料倉儲可以理解為依照一種資訊系統的資料儲存理論所建構出來的資料儲存方式，此理論強調利用某些特殊資料儲存方式，讓所套件含的資料，特別有利於後續的某些分析處理，以產生有價值的資訊。利用資料倉儲方式所存放的資料，具有一但存入，便不隨時間而更動的特性，同時存入的資料會包含時間屬性，通常一個資料倉儲皆會含有大量的歷史性資料，並利用特定分析方式，以自其中發掘出特定資訊。[39]

一般而言，資料倉儲具有以下特性：a.主題導向（subject-oriented）、b.整合性（integrated）、c.不可變動性（nonvolatile）、d.時間變異性（time-variant），分

---

[38] “A data warehouse is a subject-oriented, integrated, time-variant, and nonvolatile collection of data in support of management ’s decision making process” *See* W.H. INMON, PRISM, WHAT IS A DATA WAREHOUSE? (Volume 1, Number 1, 1995)

[39] http://zh.wikipedia.org/wiki/%E8%B3%87%E6%96%99%E5%80%89%E5%84%B2 091122

別概述如下。

1. 資料倉儲特性-主題導向

主題導向指的是，一般而言，資料倉儲的儲存模型設計，是以資料所內涵的意義之種類，歸類至相同的主題之下，作為資料儲存時的判斷依歸，例如事件區隔、產品區隔等等。值得注意的是，資料倉儲並非僅僅著眼於日積月累的資料累積，而是為了決策分析所建構出的運算模型以及分析模型，因此資料倉儲通常會設計為具有一簡單且明確的特定主題，而且會排除無法支援某一特定決策分析的資料，以對眾多資料做出明確區隔。需注意的是，對於具有多重屬性之資料而言，其可能在某一決策分析中被捨棄，但在另一決策分析中被引用。

2. 資料倉儲特性-整合性

整合性意指在資料倉儲中的資料，係經過整合，且各分類具有一致性質之意。一資料倉儲通常由具有多重來源的資料所整合而成，例如關聯式資料庫(relational database)，其利用資料庫集合中，具有共同特徵之部分來搜尋資料，因此，可做出針對不同的特徵的搜尋結果，並且讓使用者容易理解與使用此種資料庫。以房屋買賣為例，資料庫中的資料可依照年度交易量作分群，或者是交易金額作分群，或者是買家/賣家資料作分群，因此使用者即可針對其所需要之分析方式，對該資料庫進行分析。符合此種架構之資料，通常亦攜帶有許多不同的特徵。

3. 資料倉儲特性-時間變異性

時間變異性指的是既然資料帶有時間屬性，則資料隨著時間經過而產生的變動，會被紀錄在資料倉儲中，而能夠追蹤；此性質能夠反映出資料隨著時間變動的軌跡，是一個重要的特質。對某些分析結果而言，欠缺了時間分析，便無法理解結果變動的趨勢，而決策分析係針對尚未發生之事件做出決定，因此欠缺了時間分析，便無法對決策分析做出具體貢獻。因此，在資料倉儲的基本概念中，攜

帶有時間標誌的資料是一個重要的特徵，

4. 資料倉儲特性-不可變動性

不可變動性指的是資料一旦經過儲存後，便不會被取代或者是被刪除，當資料有錯誤時，後續的修正，可以藉由前述資料隨著時間的變異狀況而被追蹤。此特徵能夠確保資料一旦存入後，僅能被讀取，而無法被修改、取代或者恢復原狀，因此能夠確保資料的純淨度。舉例而言，當希望對資料做出修正時，並非直接修正已經儲存的資料，而是以時間變異性的方式記錄下來，猶如在書頁空白處寫下註記，而非直接修改書中內容。如此在後續分析時，此類修正的行為以及修正的內容，亦會一同被考慮作為特徵來進行分析。

資料倉儲的架構包含上中下三層，最下層為資料庫伺服器，中層為 online analytical process (OLAP，線上分析處理)伺服器，上層則為使用者端，即發出詢問及接收報告端。為配合資料倉儲的特性，最下層的資料庫伺服器幾乎皆為關聯式資料庫形式，藉此能夠確保由其他資料庫或者外部來源蒐集來的資料能夠作為資料倉儲能用以分析的資料。中層的線上分析處理伺服器，為了與下層連結，通常採取 1.具有關聯式的操作特質；2.具有多維度(multidimensional)的操作特質。後者為一種為特殊目的設計存在的伺服器，其可以直接處理多維度資料。上層則為客戶端，亦即直接接受客戶的查詢指令，然後將指令傳遞至中層的線上分析處理伺服器進行分析處理，獲得所查詢的資料特徵之後，到下層進行關聯性資料讀取，再將資料於中層處理過後，回傳至上層客戶端，並顯示分析結果。

典型的資料倉儲可以應用在以下方面：1.資料處理 2.線上分析處理 3.資料採礦(data mining)。資料處理即是一般的根據使用者詢問而進行統計分析處理，以獲得統計分析的結果。線上分析處理比一般索引架構更著重於範圍查詢效率，尤其是對不同範圍資料的整合性查詢，其可以將資料切細以降低資料的維度（便於粹取資料），亦可以根據資料的維度，針對資料的細節進行分析，或者降低資料的

細節等等。資料採礦顧名思義，即是希望能夠在廣大的資料「礦山」中，採取到所需要的礦藏；由於資料倉儲具有收集具時間標籤資料的特徵，因此隨著時間經過，儲存的資料量會越來越多，資料採礦即是要從廣大的資料量中採取到正確所需的資料。

在本文中，我們所關注的重點亦在於利用資料採礦方式，於資料庫中比對採取出所需要的資料，並進行分析處理。

（二）、利用資料倉儲進行資料採礦（Data Mining）

Frawley 定義資料採礦為「一種具有不明確性、未知性、以及潛在利用性的資訊程序，以自資料庫中採集資料」[40]。而 Grupe 和 Owrang 則認為資料採礦是「由已存在的資料中，探查出新的事實，且能發現專家並未知曉的新關係」[41]。由以上的定義，可以概略瞭解資料採礦程序中，其所面對的資料是已知的，而且資料量是足夠多的，而其最終目的是希望能夠發現隱藏於龐大資料庫中的新事實，或者是隱藏在資料之間的知識價值。這個程序本身雖然具有不明確性，但相對於未進行資料採礦程序之前的資料庫而言，經過資料採礦程序後，所能成現出的結果，便會攜帶更具價值的資料，也更能貼近使用者的需求。這就好比現實環境中，實際進行採礦程序一般；透過採礦，能夠自土石之中採掘出具有價值的礦藏，來適應不同使用者的需求或者對應不同使用者的應用。

以下介紹幾種典型的資料採礦程序：

1. 關聯性規則採礦(Association Rule Mining)

關聯性規則採礦主要希望能夠在大量資料中，發掘出這些資料彼此之間的共通關聯性，或者是相互關係。建立資料所遵循的規則支持度以及規則的信心度是

[40] *See* Frawley, W. J., Gregory, Piatetsky-Shapiro, and Matheus, C. J., Knowledge Discovery in Databases: An Overview, AAAI/MIT Perss, California, pp. 1-30, (1991)
[41] *See* Grupe, F. H., and Owrang, M. M., Database Mining Discovering New Knowledge and Cooperative Advantage, Information Systems Management, Vol. 12, No. 4, pp. 26-31, (1995)

此種採礦程序的重點。能夠反映出所發現之資料間規則的有效性以及確定性。舉例而言，若分析結果顯示，購買 A 商品的顧客，同時也傾向購買 B 商品，且表示為支持度(support = 5%) 且信心度(confidence = 60%)。這表示在所有顧客的交易過程中，有 5%的顧客同時購買 A、B 這兩件商品；同時購買 A 商品的顧客中，有 60％會同時購買 B 商品。

在關聯性規則採礦中，有許多人提出各種演算法，其中具有代表性者，為 Agrawal 和 Srikanty 在 1994 年所提出的 Apriori 演算法。其特徵為將資料庫內所包含的資料進行分群，針對所欲搜尋的主題，產生一些可能項目集合，再由這些可能項目集合中，逐一並不斷重複地搜尋資料庫，挑出符合該主題或者出現頻率較高的項目，而後藉由各集合之間的結合運算，找出出現頻率較高的項目集合。然後不斷重複前述過程，直到找不到符合條件的項目為止。之後再將每一個集合轉換成關聯性規則，並將大於最低信心度的關聯性規則視為有意義。

2. 群組分析(Clustering Analysis)

群組方法是一種直觀的分析方法，藉由將資料物件區分成多個類別或者是群組，使得每一個類別或者是群組中的物件，具有相對較高的相似度。而不同群組間的物件，相異度就較高。因此適用這種分析方式的物件資料，通常會帶有一些屬性數值，以供分群並辨識。典型的應用例如行為模式辨識、圖像處理、市場研究等等。透過此分析方法，能將資料庫中的資料分佈模式顯現出來，使得使用者能辨識資料集中以及資料稀疏的區域，而掌握整體資料庫的分佈模式，以及各資料群組織間的相互關係。更重要的是，這種相互關係是具有資料意義的。

3. 序列分析(Sequence Analysis)

序列分析顧名思義，是針對資料庫中，資料的順序關係進行分析。例如對於時間軸上進行的時間序列分析（Time Series Analysis）。有許多資料產生的過程具有時間順序的特徵，例如交易資訊、訊息傳遞記錄、天氣資料等等。在這些資料

中，時間序列代表一個重要的特徵，因此序列分析方式能夠用來分辨這些資料，以擷取出有用的資訊。

（三）、利用資料倉儲進行文本採礦（Text Mining）

日常生活中，人們經常會丟棄的的資料裡，文本（Text）佔據了一個很重要的部分。諸如記載資料的文件、個人文件、個人與其他單位的往來聯絡信件，例如銀行帳單、某單位的會員通知等等，幾乎每天都會有新的文件傳遞到一個人的手裡。這些文件往往在閱讀過後，在未經處理的狀態下，攜帶著個人資料（例如信件就攜帶著住址、寄送日期、以及個人身份等資料）的文件，就可能會被丟棄。

在資料採礦中，對於文字資料所構成的資料庫或者資料倉儲，有一個特別的分析方式，即稱為文本採礦（Text Mining）。與資料採礦的特性稍微不同，文本採礦主要運用的技術，與特定字詞在文本中出現的頻率、數量、與時間有較高的相關性。其主要運用在大量的文件累積出來的資料庫上，供作犯罪分析、案例追蹤、知識萃取、知識管理、資訊搜尋、訊息過濾、事件關聯、 趨勢預測、決策輔助等之用。

一般而言，文本採礦類似於一種文本的分析，希望能夠從大量的文字資料庫中，粹取出高品質資訊。典型的高品質資訊例如一種模式辨識，藉由將文字分類而後通過預測來產生。在處理輸入文本的時候，會將一些語言的特徵加入處理程序，並將輸入文本中的雜訊濾除掉，而後文本採礦希望達到的效果，就是由這些文本資料中，產生具有結構化的數據，如此才能接受評價。因此，高品質的文本採礦，即是指能夠找到文字資料庫中，不同分群文字彼此間的相關性、新穎性以及特殊性。

過往的文本採礦是由純粹的文字比對技術開始發展。但現今，藉由科技力量的進步，文本採礦已經能轉變為包含訊息檢索、數據挖掘、統計等等複雜的分析方式來進行。由於許多信息都至少具有文本的形式來保存，有些攜帶有文字影像

的圖像，也可以藉由文字辨識而同步儲存文本形式之料，因此文本採礦的技術即逐漸受到重視。例如，在 2007 年，歐洲警察局(Europol)的重大犯罪部門(Serious Crime division)發展出一套文本採礦分析系統，用以針對跨國組織犯罪進行資料分析。此一綜合分析系統整合了目前最先端的文本分析以及文本採礦技術，並協助歐洲警察局在執法時能夠提升到國際犯罪的層級[42]。

在文本採礦應用到犯罪偵查範疇中，最明顯的一個功能，就是用來監測多重線上以及無線通訊通道的特定關鍵字元，例如特定字詞、人名、或者個人的多重化名或者特定的嫌犯。文本採礦具有特定的特徵，可以被組織用在分析文件當中，但同樣的技術當然也可以用在組織犯罪案件的應用領域當中。因為政府組織熟悉某些犯罪活動的型態以及組織，因此可以將這些知識化為文本採礦的工具條件。目前在一些國家，例如英國，已經應用類似的資訊技術於犯罪偵防上。

更重要的一點，犯罪偵查者，例如檢察官或者警察，可以利用他們熟知的分析方式，透過資訊工具的協助，處理非常大量的資料，而且機器運行分析的時候，他們可以同時去處理其他的事務。文本採礦特別適用於沒有結構化的片段文字，可以從數以千萬計的資料中，將具有同類片段文字的資料擷取出來，也可以安排特定的文字群組，例如單字與單字之間的間隔位於多少字元之內，或者適用布林運算，將文字群組進行「及」以及「或」的交集聯集安排，以過濾出所需要的資料。又或是可以比較不同次的分析結果，以進一步限縮或者包含某些可能在單次搜尋中，因為組合邏輯不同而漏掉的資料。當然這些文字群組的設定邏輯，還是與犯罪偵防人員的經驗有著密不可分的關係，必需要藉由犯罪偵防的經驗，來定義出有效率且明確的文字群組設定，方能在眾多資料倉儲中，撈取出所需要的資料。

文本採礦與資料採礦最主要的分別，在於文本採礦的核心是語意處理分析運

[42] 關於歐洲警察局之資料庫介紹，請參見 http://en.wikipedia.org/wiki/Europol，最後瀏覽日期：2009/12/2

算，單詞的意義以及片語的意義是分析工具的核心，在這個領域中，也會引入「自然語言處理」(Natural Language Process)這種運算核心，使得使用者可以如同講話般，將心中所想的思考邏輯直接鍵入成為搜尋條件，NLP 會分析使用語言（例如中文）的語意邏輯，將使用者的語言邏輯，轉化為資料庫可以瞭解的邏輯組合。簡單地說，NLP 即是讓電腦「理解」人類的語言，然後 NLP 模組會將人類的語言轉化為電腦能夠處理的形式。舉例而言，犯罪調查人員可以直接輸入「在過去三年間，與某甲通訊次數超過 100 次的人或單位」，系統接收到此條件後，會將其拆解成為時間條件「從現在起算過去三年之間」以及搜尋條件「與某甲發生通訊行為（例如郵件、電話等等）」以及「前述行為總次數大於 100」，然後開始搜索資料庫，以便找出符合前述條件的資料。由於理解(understanding)自然語言，需要關於實際世界的廣泛知識、語言以及運用操作這些知識、語言的能力，因此理解的定義成為一個主要的問題。比如前述例子中，我們需要系統能夠「三年」是一個時間條件，且起算點為「現在」，且某甲係一人名；而不能將「三年」判斷為一個人名。

利用文本採礦之技術，便可能協助犯罪偵查進行。由於目前檢警單位之資料，大多為以文字方式儲存，或者附有文字說明，因此文本採礦之技術，相當適合用來對各式資料庫進行分析，而且個人所丟棄的物件中，包含有文字資料的更是不虞匱乏，同時文件也具有易於蒐集與分配之特性，減少了資料蒐集的困難度。

為了要讓文本採礦更有效率，在製作資料庫所需要的資料時，對資料的內容以及重點進行確實的理解是一個重點。舉例而言，如果我們隨機蒐集許多文件，辨識其內容後儲存為不具任何分類的資料集合，那麼針對這一個雜散的資料集合，應用文本採礦以期能夠獲得有效分析結果就會比較沒有效率，使用者會無法立即理解所產生的分析結果究竟與什麼行為有關，同時使用者能夠使用的限制條件也會隨之減少，導致無法準確且有效率的收斂到所需要的資料。如同在資料採礦中所題的，收集資料時，將資料進行確切的分類是重要的。

一般而言，犯罪者的手法常可能具有某些可以被歸納的方法論，因此將此類方法論套用在文本採礦中，便可以協助收斂搜尋的範圍（需要再次的強調，偵查的經驗是能夠發現此類方法論的核心）。而由於現今資訊處理硬體的進步，因此若分析結果產生後，發現分析結果偏差或者有誤的時候，可以迅速地進行修正，重新進行分析或者就分析結果進行進一步修正，以期能夠在短時間之內獲得符合預期的分析結果。

有幾個因素讓文本採礦或資料採礦能夠成為犯罪偵查的利器[43]。其中之一自然就是當面臨日漸龐大的資料庫時，必須要藉助資料工具才能順利從中找尋資料，尤其在防患未然方面，可以藉由平日的模擬與演練，事先過濾出一些「觀察名單」，以減少或消弭可能發生的犯罪。其二是現在許多商業體也針對消費者進行許多資料採礦的分析工作，例如 7-11 便會依照顧客的分類，在不同的地區鋪設不同的商品以及擺設方式，而且商業體的分析工作往往作得比行政機關來得更好，而有借鏡之處。第三就是使用硬體進行資料處理，能夠簡省人力。

文本採礦/資料採礦的分析工作，能夠發現一些資料彼此之間的差異之處，這些差異有時是誤植，有時是真正的差異，透過連續不斷地進行分析，能夠更進一步的整合這些資料，以利於往後的分析工作。

刑事偵查員即依據刑事訴訟法、調度司法警察條例、警察法等相關法律及警察法施行細則等授權命命發動犯罪偵查工作。一般而言，當刑事警察得知犯罪發生時，刑事警察即依上述原則開始進行犯罪偵查工作，包括蒐集犯罪情報，蒐集犯罪事證、追查贓證物、逮捕犯罪嫌疑人、並協助檢查官起訴犯罪嫌疑人，使其接受應有的法律審判及制裁。然在犯罪偵查中偵查勤務極為繁雜多樣，有學者將偵查勤務依其內容概分為受理報案、情報諮詢、查贓、盤詰檢查、現場處理、查察探訪、背景調查、跟蹤監視、搜索扣押、拘提逮捕、詢問、移送遞解、查證追

---

[43] *See* Daniel J. Steinbock, DATA MATCHING, DATA MINING, AND DUE PROCESS, 40 Ga. L. Rev. 1

贓及擴大偵破等十四項[44]。

文本採礦/資料採礦固然可以發揮犯罪事前預防犯罪發生的效用；在犯罪偵查時，亦能協助前述偵查勤務的執行。例如在情報諮詢階段，現今的作法為對犯罪現場周遭人物或與犯罪事件相關的人物進行諮詢，以期在諮詢的內容中，過濾出可能可以進一步採用的情報，以利後續的情報諮詢或者其他偵查活動進行。而文本採礦/資料採礦的分析結果，可以產出與該次案件較為相關之資料分類結果或者相關人物資訊，便可以用來在情報諮詢之前，初步收斂情報諮詢範圍，增進情報諮詢的效率與正確性；同時可以在情報諮詢完成後，將文本採礦/資料採礦的分析結果，與所獲得的諮詢內容進行交互比對，以進一步過濾出較高相關性之資料，或者其中之差異處，以利後續作業進行。

進一步言，某些種類的資料庫分析結果，例如指紋或者 DNA 分析結果，能在符合保管程序的狀況之下，在犯罪的偵查以及起訴審理階段，作為直接的證據；但某些種類的文本採礦/資料採礦的分析結果，並不一定能作為直接的證據，而在指控嫌犯的罪責時，被司法系統所採用，不過此類的分析結果，仍可以於案件發生時協助國家的刑事偵查系統，進行資料的過濾、整理以及勘誤等等作業，以發揮更好的作用。

（四）、由廢棄物建立個人資料庫

蒐集垃圾的目的，是希望能自垃圾中取出與使用者行為具有高度相關，又能配合犯罪偵防的資料，例如垃圾中所包含的文件，其中可能記載使用者的部分個人資料，以及部分金融帳務相關資料，而分析垃圾中所包含的物品，則可能透露出某一地區的犯罪相關訊息，例如可在垃圾中偵測出毒品反應者，則代表該地區可能具有販毒或者幫派活動，值得進一步追蹤。而這些資料若能長期保存以及更新，則藉由資料分析工具，能夠更清楚刻畫出一地區中的特定人物以及特定活動

[44] 參見黃壬聰，犯罪偵查勤務之研究，中央警察大學刑事系研究所碩士論文，1999 年 6 月，頁 18。

之軌跡，對於犯罪偵防，應具有高度的參考價值。

另，由行政程序所應該依循的比例原則[45]來看。考慮行政作為是否應該被施行時，需考慮「目的正當性」、「手段必要性」及「限制妥當性」三者之間的平衡關係。目的正當性在檢視所採取的手段必需要能夠達成所要追求的目的，方具有目的正當性。因此，行政手段必需要能夠發揮維護公益、促進社會利益之效果，且為合法的手段，並且能有助於目的的達成。而手段必要性，又稱為最小侵害原則。其意指若要能達成所要追求的目的具有多種手段，則在具有相同效力的情況下，應採取干預基本權最小之手段，以在最小範圍內侵害人民權利。另外，行政手段所欲達成之目的，以及採取該手段對於人民基本權利的干預程度，必需要能符合比例性原則。亦即，雖然某行政手段可以達成原始設計的行政目的，惟施行該行政手段時，不可施加過多的負擔到人民身上，造成人民權利過量的損失。意即，所採取的手段造成的損害，不得與所要達成的目的顯失均衡。

據此，前述的目的正當性應考慮法律的規定，不得逾越現行法的規範範疇。同時應該考慮技術可行性，以有效率、有效能的方式來設計行政手段的具體內容，以避免設計的手段無法有效地達成行政規範的目的。另外，行政手段的設立目的以及手段，亦應符合現今社會的認知，不得逾越一般社會價值的範圍，並為一般民眾所接受。在具備前述條件的前提下，再進一步選擇能夠達成目的的必要方法，以及考慮採取的方法所造成的損害，不得與所欲達成目的之利益顯失均衡。

以美國為借鏡，雖然在美國，蒐集廢棄物作為分析個人資料的標的，已見於許多案例[46]，且目前美國，在通常狀況下，仍然可以廢棄物蒐集分析後所得結果，作為進一步申請搜索令狀之根據，而不會違反美國憲法第四修正案的規範，但此類案件之發生背景，皆限定在非常特定的人物，以及該目標者棄置在其住居所附

[45]參我國目前行政程序法第七條規定，行政行爲應依下列原則爲之：一、採取之方法應有助於目的之達成。二、有多種同樣能達成目的之方法時，應選擇對人民權益損害最少者。三、採取之方法所造成之損害不得與欲達成目的之利益顯失均衡。

[46] 與隱私權相關之案例以及法理介紹，後敘於第三章。

近的廢棄物。意即，是執法單位先有了特定的追蹤目標，之後藉由廢棄物蒐集的方式來取得需要的物證，以便於採取進一步的行動。此與本文所要探討的廣泛式的針對人民丟棄的廢棄物進行資料蒐集，並不相同。

可想而知，若沒有有效的蒐集方式可供利用，則無法建立有效的資料庫。為解決此一問題，本文嘗試由兩個方向著手，第一是分析現存的廢棄物收集方式是否適合進行蒐集分析；第二是搜尋現存的軟硬體技術，是否能應用於對所蒐集物品的資料分析，希望藉由對此二目標的研究，整理並設計出一套可行的資料蒐集方法。若我國現有的廢棄物收集方式能夠與現存的軟硬體技術互相搭配，則便可能針對日常蒐集的廢棄物進行資料分析，以粹取出相對應的資料。

1. 我國現行收集廢棄物相關規定

我國於民國 94 年起施行垃圾強制分類，目前環保相關單位，於各大都會區施行的成果良好，普遍來說，施行廢棄物分類已逐漸內化成為民眾處理廢棄物時的基本準則。依照垃圾強制分類的規定，可區分為「資源」、「廚餘」以及「廢棄物」。其中資源類又可細分為紙類、鐵類、鋁類、玻璃類、塑膠類以及一些電器類等品項，而在資源類以及廚餘類以外的，則統稱為「廢棄物」。一般而言，資源類指能回收再利用的物品，而廢棄物則是指不可回收再利用的物品[47]。

目前，各縣市政府之衛生當局依照行政區域大小，以及廢棄物之種類，均設定有不同的清運路線以及廢棄物分類蒐集規則。以台北市為例，台北市環境保護局即有規定每週一、五進行平面類廢棄物之回收，包含紙類、舊衣類以及乾淨塑膠袋；而每週二、四、六則進行立體類廢棄物之回收，包含乾淨保麗龍以及一般容器與小家電等[48]。而每一行政區均依照人口以及區域大小，分派有不同的清運車輛車次，以松山區為例，便有 12 輛清運車，將松山區劃分為 12 小區，配合不

[47]請參考行政院環境保護署，資源回收管理基金管理委員會，「何謂垃圾強制分類？」http://recycle.epa.gov.tw/Recycle/index2.aspx

[48] 台北市環境保護局全球資訊網，參考 http://www.epb.taipei.gov.tw/data/search_trash.aspx，最後檢索日期：2010 年 04 月 18 日。

同時間，以特定車輛對特定小區，進行廢棄物蒐集清運之工作[49]。由此規劃，可大致得知，掌握特定清運車輛，便能掌握特定地區之廢棄物清運狀況。因此，若能針對清運車輛所蒐集得來的廢棄物，進行分析並進一步獲取其中所攜帶的個人資訊，便有可能建立與地區相關的個人行為資料庫。由於檢警單位的任務分配也是以轄區作為分野[50]，而轄區劃分亦與行政區劃分高度相關，因此若能建立與地區相關的個人行為資料庫，於犯罪發生時，能進一步利用此等資料庫進行偵查工作，則應能發揮助益，有效地協助犯罪偵防進行。

目前，前述資源類以及廢棄物類的廢棄物品項，有幾種品項是適合進行分析的，關於這一點在後文將搭配現有技術進行進一步說明。舉例而言，針對廢棄物中的文件，在回收後，可以針對其上所載的文本資料，進行擷取以及辨識，可透過例如掃瞄或者拍照等方式，將文件以影像方式擷取下來，而後再利用資訊軟體辨識其上所載的文本資料，再輔以文字語言分析軟體，便可辨識出文本中與個人相關的資料，之後，再根據不同分類將這些辨識出的文本分門別類保存起來，便可逐步建立起資料庫，供日後從中粹取出與個人相關的資料內容。在各種文本中，可能包含銀行月結帳戶資料、信用卡簽單、信用卡帳單、個人姓名與住居所、個人加入之會員資料等等各式各樣的資料，這些資料都透露出部分的個人資訊。舉例而言，住居所的地址資料，透露出個人的活動範圍；信用卡帳單以及會員資料等，則可以透露出個人平日的購物習慣，以及其花費的金額數目。將這些個人資料製作成資料庫後，便可以套入一些與行為相關的模型，以進一步推估出個人的行為模式或者心理狀況。日後當發生刑事案件時，視案件情狀不同，檢警人員分析現場狀況後，會歸納出案件偵辦的方向，當其中出現可能的人物特徵時，便可以與資料庫分析結合，在案件偵查初期，預先鎖定某些已經存在於資料庫中的

[49] 於資料檢索欄位點選「松山區」，系統便可列出松山區目前之清運車輛安排表。http://www.epb.taipei.gov.tw/data/trash_list.aspx?Address=%aaQ%a4s%b0%cf%7c%7c&KeyWord=%bd%d0%bf%e9%a4J%b9D%b8%f4%c3%f6%c1%e4%a6r，最後檢索日期：2010 年 04 月 18 日。

[50] 參考台北市政府警察局網頁，關於「轄區概況」之介紹，可發現台北市政府警察局之轄區劃分，與行政區劃分的高度相關性，http://www.tcpd.gov.tw/cht/index.php?code=list&ids=26，最後瀏覽日期，2010 年 4 月 18 日。

特定人物資料，作為第一步篩選過濾。利用資料工具進行資料庫分析的優點在於能夠針對資料庫中的所有資料進行全面性的比對，不會產生漏未審酌的人為失誤；另外，隨著軟硬體科技進步，資料工具的執行分析速度也會日漸增快，可以在檢警人員進行偵查策略佈局時，同步就輸入的條件進行分析，並快速產生分析結果，可以縮短偵查時間，有效率地提升檢警人員的偵查速度，並可能在偵查行動的早期即獲得較以往更為充分的資料，這些資料的分析結果，都可能可以成為輔助刑事案件偵查的重要線索。

2. 利用文字辨識建立資料庫

文字辨識技術目前已經相當普遍，欲從影像辨識出所包含的文字，其概念為需先攝取影像。習知技術是以掃瞄手段獲得影像資料，而後再加以辨識。此類技術發展已久，以中文辨識技術領域而言，90 年代便有許多公司開始發展光學文字辨識技術而推出產品，例如丹青辨識系統[51]、蒙恬辨識系統[52]等等。進入 21 世紀後，影像感測技術日趨演進，典型者如數位相機，在 21 世紀初期這短短數年內，已自百萬畫素開始，至今達千萬以上解析度之水準，呈現蓬勃發展的趨勢，因此以相機攝取影像後，再進行辨識的技術手段也隨之一同發展，並普及到其他行動裝置。目前幾乎所有市面上的手機，皆具有照相/攝影功能，其所擷取的單張影像像素也達數百萬，高階手機更達千萬像素之譜，經輸出到電腦後，便可應用前述文字辨識技術，來判別該影像中是否具有文字資訊；更有甚者，目前市面上許多大顯示螢幕的智慧型手機（Smart Phone）已內建文字辨識應用軟體，使用者可在以手機拍攝文件後，隨即啟動辨識軟體以辨識其中的文字資料，並轉成文本檔案儲存起來。

而在蒐集到大量的文件時，要將文件一一有序地取出、分配，現今也有其他領域之技術可供參考，例如郵局用以分揀信件之機械系統，即是利用光學辨識的

[51] 力新科技推出，參見 http://www.newsoft.com.tw/。
[52] 蒙恬科技推出，參見 http://www.penpower.com.tw/。

方法，來辨識郵件上的郵遞區號，再進行分門別類的派送。由於郵遞區號除書寫於信封上之特定區域外，亦可能書寫於信封表面之任何位置，因此此類系統能設計為可以針對可能是郵遞區號的數字序列，來進行光學辨識[53]。以目前我國郵政當局所使用之光學閱讀信函分揀機 OCR/LSM (Optical Character Reader/Letter Sorting Machine)系統而言，每一機台每小時能夠處理的信件數量已達三萬件以上之譜[54]，充分顯示出此類光學分揀之技術已達量產處理之水平。郵政當局所使用之分揀系統，是針對郵遞區號進行分揀；而在針對文件進行分析時，則是需要針對特定的字元，例如可能為姓名之二、三或四字元之組合字串、可能包含地址（具有郵遞區號）之住居所資訊、或者可能為個人財務資訊（具有對帳單、信用卡等特定字元）之文件，進行辨識及分揀。

綜上而言，以目前之技術水準，是有可能設計出專門為辨識文字使用之專用系統，例如將數位相機技術，結合文字辨識軟硬體，以及文件分類系統，便可設計出專門為辨識文件文字使用之專用機器，以作為在文件廢棄物中進行文字辨識使用。在文件廢棄物被資源回收車收集之後，回收處理之前，利用文件分揀系統以及文字辨識系統的設置，逐一將可能為目標之文件（即可能包含前述個人姓名、住居所、財務資訊之文件）取出，並且進行攝影，以取得影像檔案。而後，再將影像檔案交由電腦再次進行詳細的文字辨識，便可獲得其中的文本資料。針對其中較難以辨識之影像資訊，還可以透過專職人員以人力進行辨識，而後再依照資料庫建立規則，分門別類存放起來，以便後續分析使用。舉例而言，在前述分析中，例如文字辨識後，電腦自動認定為包含地址、人名、或特定關鍵字的（如路名、包含姓名首字並由三個字構成的單詞等者），即可判定為與個人相關，因此是資料庫所需要的資訊，可被認定為具有進一步辨識的價值，而對其所包含的文字影像繼續進行辨識。在完成整份文件的文字辨識並取得資料後，可進一步依

[53] 例如中華郵政所使用之高速郵件分揀機械系統，其信函分揀機 OCR 以及理信銷票機 CFC 即是利用光學辨識方式，來辨識郵件上的郵遞區號再進行分門別類的派送。
http://chch.tw/word/103news-4.html

[54] 林鉛平，〈郵件處理自動化管理策略之研究〉，91 年 5 月

照資料的屬性進行歸類儲存，例如依照地區、依照文件屬性等等進行分類。概言之，一旦完成文字辨識之後，便可依照資料庫建立的規則，將辨識出的個人資料分門別類的歸類，以便於有需要時進行搜尋以及分析。

3. 辨識含特定成分之物品以建立資料庫

另外，針對資源類廢棄物中的瓶罐類，以及不可回收的廢棄物，則可進行特定物質的檢測，針對瓶罐中的殘留物質，或者廢棄物中的內容物進行定性的分析，例如檢測廢棄物中是否含有毒品。由於毒品問題是各國執法單位都相當關心的問題，因此檢測包裝物中是否含有毒品的偵測技術應用發展便顯得蓬勃。一般而言，這類的偵測技術是針對洩露至空氣中的微粒進行蒐集與偵測，有藉由直接吸取空氣進行偵測者，也有透過介質，例如溶劑，進行偵測者。當微粒的數量達到某一個程度時，便可判斷出在偵測範圍內具有某些特定的毒品或者違禁藥物[55]。除此之外，也有以直接接觸偵測方式，針對不明物品進行偵測之技術。概言之，係先針對目標之毒品或者違禁藥物進行分析並獲得其特性後，依照各物品分門別類建立檔案；而後取得可疑之不明物品時，將不明物品直接放置在儀器上進行定性的分析，再將分析結果與預先儲存之檔案進行比較，便可判定該不明物品之性質是否屬於已建檔之毒品或者違禁藥物。另外，針對某些特定的違禁藥物，亦有更簡便之檢測方式，係透過將特殊的檢測劑儲存於高壓罐中，再噴灑在所欲偵測的表面，若表面含有特定的違禁藥物，則噴劑會顯示出明顯的顏色[56]。

此類檢測技術，便可以應用於檢測清運車所蒐集的廢棄物中，是否含有特定藥物。清運車中，存放已蒐集廢棄物的空間，為一半密閉空間，因此，可以藉由裝設這些器材，來對已蒐集的廢棄物進行毒品或者違禁藥物檢測。例如，先於清運車上存放廢棄物的空間內，安裝適當的檢測器材；當毒品使用者將包含著毒品的容器或者包裝，或者使用毒品之器材丟棄後，這些器具上多少會有毒品殘留，

[55] 目前已有商業公司推出相關的偵測器，除有多種物質偵測器，亦有單一裝置能同時偵測多種物質，請參考 http://www.a-security.nl/DrugDetection.html。
[56] *Id*

於是當清運車開始蒐集這些廢棄物後，操作員便可藉由使用這些檢測器材，針對已蒐集的廢棄物進行檢測。若偵測出廢棄物中具有毒品或者違禁藥物殘留，則可得知清運車於此次出勤中所蒐集之廢棄物，具有部分毒品或者違禁藥物，可間接推估於此次出勤路線範圍內，具有使用毒品或者違禁藥物者活動。

由於一般人無法透過公開正常之管道，取得毒品或者違禁藥物，因此，毒品之使用多與非法管道與黑幫活動有關；而此類非法管道與黑幫活動，多有其地域性，藉由類似的檢測技術，可以協助檢警人員早期鎖定毒品以及黑幫人員活動之範圍。而後再透過資料分析工具，便可發揮協助建立地區犯罪活動之資料庫，能夠反應出不同時期，地區犯罪活動之高低峰。當此類資料再與其他犯罪資料與檢警人員之調查技巧結合時，便可在犯罪發生時，協助檢警人員鎖定特定的調查區域及或特定的調查對象。進一步言，此類犯罪資料隨著時間漸增後，可以做成具有統計價值之犯罪資料庫，且各資料庫彼此之間亦可互相具有關連性，以便於進行資料搜尋時，能夠發掘出各資料彼此間之關連性。期望藉由使用此類資料庫，搭配檢警人員對於犯罪發生行為與模式之特徵分析及偵查方法，能夠於犯罪前發揮犯罪預防之效果，並且於犯罪發生後協助偵查工作之進行，使檢警人員能更有效率、更有效果地執行保安工作。例如，藉由透過分析前述毒品與地區關連資料庫，便可鎖定檢測出毒品反應的特定地區及其歷史資料；同時搭配既存之犯罪者資料庫及或其他藉由蒐集廢棄物之文件所建立的個人資料庫，便可能可以鎖定特定的人物，進行犯罪預防之勤務工作，例如加強巡邏或者調查特定對象。若能藉由前述系統的幫助，積極的進行犯罪預防巡邏，使潛在的犯罪者的意圖能夠或多或少的被遏止，或者取得關連分析結果後，能夠限縮特定的調查對象，搭配檢警人力配置，以便在平時積極注意相關對象的活動內容及活動範圍；而在相關犯罪發生時，能夠先針對特定對象，進行犯罪可能性過濾，希望能夠有效的先行過濾出可疑的對象，以進一步有效率地協助偵查。

前述所提的蒐集與分析廢棄物之方法，均能藉由現行可行的技術手段來達成

分析的目的，且能搭配現行已經存在於各縣市的廢棄物清運規劃來執行。易言之，為達成蒐集與分析廢棄物的目的，其中佔重要角色的廢棄物清運與回收規劃已可藉由現行行政制度來達成，無須重新另為規劃。且廢棄物清運之規劃，係以地理分隔為基礎，正好與現行檢警人員之配置方式大致相符；針對廢棄物所進行的分析結果，在歸檔到資料庫時，每一筆資料也會攜帶著地理區域的資訊，因此檢警人員在使用這些資料庫時，對於分析結果所呈現的地理特徵，亦應具備一定的熟悉度，可以有助於犯罪偵防工作的進行。

為達成此蒐集與分析廢棄物的目的，所要增加的行政手段成本，可概分為兩部分。針對文件資料，蒐集流程部分無須額外增設設備，惟需使廢棄物清運人員注意於蒐集文件資料時，文件資料的樣本盡可能不要被其他污染物污染，以減少文件蒐集之後進行分件時，與分件後進行文字辨識的困難度。另外，針對特定物品之辨識，若選擇於清運時即同步進行辨識，則需於清運車處增設辨識裝置，以及與資料庫連線之通訊設備，此類裝置的優點在於無須使清運人員進行主要的資料分析操作，僅需要於清運開始時，將辨識裝置的電源開啟，並確認與資料庫的連線正常運作即可。另外，亦可考慮於清運車回航後，在固定的清運站架設辨識裝置，並且使其與資料庫連線。這種作法的優點在於辨識裝置的硬體架設可有較大的設計空間，無須受限於清運車的硬體設計，且辨識裝置的數量可控制在較少的數目，維修較容易；同時清運站係一固定場所，因此對於辨識裝置的管理與維修以及保安程序，較容易管理控制；進一步言，若辨識裝置需要配置操作人員，此種作法亦屬於定點型態，也具有容易管理的優點。

4. 不進行辨識與蒐集之個人相關資料

針對具有高度隱私性的個人生理資訊，考量其特殊的性質，以及對於達成犯罪預防及偵查協助之目的的效益，並不適宜進行辨識與蒐集，分述如下。

具有高度隱私性的個人生理資訊，例如醫療記錄、血型、基因資料等，此類

資料具有高度的個人鑑別性以及與個人健康息息相關；另外，此類資料中，直接屬於個人生物特徵部分者，例如血型、基因資料、指紋等，更具有恆久不會變動之特質，自個人出生後，便已固定，不會隨著時間經過而有所改變。而醫療記錄與個人過往就醫之資料息息相關，並且可透露出許多一般人無法從觀察外表便可獲知的個人健康訊息。此類資訊，除非個人願意透露，否則他人便難以從一般管道獲悉資訊的內容。而此類資訊內容，若在非個人意願下公開出來，便有可能使個人在社會上活動時，面臨一些不必要的責難。以醫療記錄為例，例如個人可能患過某些疾病，雖不影響其日常生活作息，但若被知悉，便可能影響其工作機會，使雇主相對地較不願意雇用他。又例如個人丟棄的廢棄物中，亦可能攜帶有具高度隱私性的個人生物特徵資料，例如使用過的保險套其上可能包含有個人的體液等等。又例如女性可能曾經進行墮胎，若被知悉，則可能使其面臨親友及同事的過度關心及/或無謂責難，甚至影響其婚姻狀況，而導致傷害。另以基因資料為例，若被知悉，則可能因為基因的特徵，被社會上的其他人分類，例如被分類為容易罹患癌症者、容易肥胖者等等，而面臨無謂的壓力。而上述這些可能的狀況，在此類生理資訊不被公開的狀態下，均可以避免其發生。

因此，相較於個人住址或者消費習慣等可因個人住居或行為改變而隨之改變之個人資料而言，隱私權人對於此類個人生理資訊之隱私期待性亦應較高，且為隱私權人相對不願意透露之個人隱私權內容。因此若針對個人生理資訊進行蒐集與分析，並建立資料庫，則可能引起人民較高度的關切並引發必要性之爭議。進一步言，此類具有個人生理資訊之資料，多係用於核對個人身份時發揮作用，其與個人行為模式互為獨立。亦即，考量本文所討論之個人資料庫之建立，係為協助犯罪偵查以及發揮犯罪預防之目的，若進一步蒐集並建立個人生理資訊之資料庫，其實亦較難以藉由偵測並判斷個人生物特徵之資料，達成對個人行為模式進行預測判斷之目的，因此無法直接與犯罪事實發生連結。能夠與犯罪事實發生連結者，系於犯罪現場採集到可能疑犯之殘留痕跡，例如毛髮、血液、唾液、體液

等等攜帶個人生物特徵之資料，而後於逮捕疑犯時，再由疑犯身上採取毛髮、血液、唾液、體液等等檢體，以與先前於犯罪現場採集之物證進行比對。惟此類分析模式，係為確定疑犯是否於犯罪發生時處於犯罪現場，因此是以犯罪現場所採集到之證物為基礎，而後再與疑犯之檢體進行比對以求證；此與本文討論之事先採集分析跡證以建立資料庫之模式不同。

另，由前述行政程序所應該依循的比例原則來看。考慮行政作為是否應該被施行時，需考慮「目的」、「手段」及「限制」三者之間的平衡關係[57]。個人生理資訊，例如基因、病例等等，一旦被不當揭露，則能夠被用來相當程度地影響個人的身體以及心理健康，甚至造成不可彌補的損害。無論此類侵權事件發生的可能性有多微小，這對於基本權利受到侵害國民來說，是幾近不可接受的後果。因此若對人民的個人生理特徵也採取蒐集與分析的手段，來建立資料庫，則在資料庫管理無論如何無法盡善盡美滴水不漏的前提下，對於人民身心健康的基本權利的侵害屬於無法判定影響範圍大小的類型。故，若採取此手段，對於人民的來說，亦可能產生極大的心理負擔，而導致對於此資料庫的全面性恐慌，對於此資料庫的其他分類資料，採取排斥的態度。

因此，考慮達成犯罪預防及偵查協助之目的，若在個人資料庫建立時，亦同時採取蒐集並建立此類個人生理資訊資料庫之手段，尚難謂能發揮積極的協助效果。另一方面，建立此類個人生理資訊資料庫後，即便以高度嚴格要求之保存程序來建立此類個人生物特徵資料庫，並同時以高度嚴格要求之管制程序來限制存取此類資料庫之權，若資料庫之內容外洩，幾乎一定會對個人隱私權內容造成難以挽回之傷害。由於隱私權內容一旦被公開後，其散佈情形幾乎無法被控制，且對於已經知悉內容之人，亦無法以各種手段使其忘記記憶中之知悉內容，恢復為不知悉之狀態；因此面對此種可能發生之後果，資料庫建立者幾乎無法補救此類個人生理資訊外洩所造成之影響。故目前階段，除醫療機關因執行業務需要而建

[57] 城仲模，〈論公法上之比例原則〉，「行政法之一般法律原則」，初版，民國 83 年，頁 119-137。

立的患者資料以外，不對此類個人生物特徵資料進行前述的辨識與蒐集，應是較為合適之作法。

三、 隱私權的發展

雖然現今對於隱私權的認知，已經普遍認為其係一種基本權利，但相對於生命、言論、財產等具有悠久歷史的基本權利而言，隱私權仍屬於後期逐漸發展開來的一種概念，且隨著社會的溝通管道日趨多元、熱絡，以及科技能力的不斷進步，逐漸發展出日趨複雜的隱私相關權利理論。本章將就隱私權於歐美以及我國的發展，作一介紹，以為本論文之後關於資訊科技對於隱私權造成的衝擊討論之基礎。

（一）、隱私權的發展

何謂隱私權？其一詞最早出現於 1890 年美國學者 Samuel D. Warren 和 Louis Brandeis 於哈佛法學評論上發表的—隱私的權利(the Right to Privacy)—一文中出現的。本論文提出一個觀點，所謂隱私權係指一個人在一般狀況下，自行決定他的思想、觀點及情感，與他人交流程度之權利[58]。這便是隱私權的濫觴，在人口還並不十分稠密的美國社會中，已有學者注意到隨著工業革命的成熟發展，社會逐漸轉型的過程中，人與人的相處將會越來越熱絡。而隱私權，便是在這種情況下需要被重視的一種權利。其核心精神在於，個人可以自行決定與他人交流的程度。

然而，一百多年過去了，隨著社會發展趨向多元化以及便利性，加上人口成長，大都市的人口稠密度逐漸上升，因此個人能夠獨享的空間便逐漸縮小了。以我們目前面臨的日常生活為例，人與人之間的交流日趨頻繁，從面對面的實際接觸到虛擬的透過網路的交流，從寄發信件到接收電子郵件，而個人活動的範圍，也因為交通工具以及大眾運輸的發達，逐漸擴張。因此，個人於日常生活中，更難以與其他人保持明確的界線。再加上生活環境的多元化發展，一個人在社會中常常需要同時扮演許多角色，舉例而言某人可能既是某公司職員，又是學校學

[58] *See* Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 harv. L. Rev. 193 (1890).

生；又或者既是家庭的一份子，又是網路社群的參與者；平日是上班族，到了假日便成為假日農夫或者餐廳老闆或者參與社團活動等等，凡此種種，在現今社會中已不是新鮮事了。因此，人與人相處之間，重疊的時間與空間也會日益增大，導致個人所要提供以及收取的資訊日趨多量及複雜，人與人之間的相處，要能夠完全由個人自行決定與他人交流的程度，難度便增加許多。此時再回頭來檢視隱私權最初的發源--獨處的權利以及與他人交流程度的權利。便不難理解，今後的社會中，除了獨處已經越來越難以實現外，為了適應社會的生活步調，與他人交流程度的權利，除了需要考慮個人的意願外，也必須要一併考量與個人發生交流的其他人的立場。

1. 隱私權在美國的發展

有關隱私權的法律發展，在許多國家中便因應許多個案累積，透過立法、司法系統的解釋與創造，逐漸成為備受關注且重要的議題。漸漸的，隱私也成為一種基本的人權，透過明文法規或者法律解釋，成為受到重視以及法律保護的權利。在美國，隱私權的問題多見諸於與搜索扣押相關的刑事判決中，關於美國憲法第四修正案之討論[59]。美國憲法第四修正案係規定「任何公民的人身、住宅、文件和財產不受無理搜查和查封，沒有合理事實依據，不能簽發搜查令和逮捕令，搜查令必須具體描述清楚要搜查的地點、需要搜查和查封的具體文件和物品，逮捕令必須具體描述清楚要逮捕的人」[60]。其內容主要是針對政府的公權力執行進行限制，限制政府機構，諸如行政機關、警察機關等等以非法或無理的手段進行證據蒐集。需注意的是，第四修正案的規範主體是政府機構，而非私人，因此若係由私人取得證據，則無論其取得證據之方法是否合法，一般而言，政府在刑事訴訟中，均可以出示該證據，此時即不適用第四修正案。

[59] *See* Katz v. United States, 389 U.S. 347. *See* California v. Greenwood, 486 U.S. 35 (1988).
[60]" The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

在討論到搜索與扣押對隱私權所造成的影響中，經常被提出案件便是 Katz 案件，其係關於檢警蒐證程序是否抵觸憲法第四修正案所保護的主體。Katz 案之簡介如下：1967 年，在洛杉磯，一名叫 Katz 的人在公用電話亭中撥打電話至邁阿密以及波士頓下注，而在電話中傳播賭博信息違反了當時賭博法律的相關規定。在 Katz 不知情的狀況下，FBI 人員利用監聽設備，側錄了 Katz 該次下注的談話內容，並且作為呈堂的證據，在對 Katz 的審判中，控方出示了對 Katz 的電話錄音作為證據，錄音是通過對 Katz 使用的公用電話亭安裝竊聽設置得到的。。根據該錄音內容之證據，Katz 因此被判為有罪。

本案的重點狀況為，檢方該次的側錄程序事先並沒有取得任何令狀，包含搜索令以及任何法律文件。於是 在案件審理中，Katz 主張該次的側錄行為，違反了憲法第四修正案對於正當程序的規定，而檢方則主張電話亭既是公共場所，則此場所不在第四修正案所要規範的範圍之內。這是由於第四修正案的文字明白規範了受保護範圍為「任何公民的人身、住宅、文件和財產」等，檢方認為此文字規範應解釋為僅包含私人住居範圍，因此檢控方堅持認為電話亭是公共場所，不受第四修正案保護，無須搜查令就能進行竊聽與側錄等行為。

上訴法院認可了檢方的主張，同時認為檢方的監聽行為亦無實際上物理侵入電話亭內部，因此側錄行為應具有正當性，而沒有違反憲法第四修正案的規定。Katz 繼續上訴到最高法院，這次最高法院駁回了上訴法院的決定，認為憲法第四修正案所欲保護的不被政府無理入侵的隱私權，其主體應是人民，而不受限於人民所處的地方。因此，當人民對於其自身行為，表現出合理的隱私期待性時，其隱私權應該受到保護，「無論該人處於辦公室、朋友的住居所、或者在計程車中」[61]，亦即不必然受到人民所處的環境的限制。在本案中，最高法院認為，當 Katz 使用電話亭時，即已表現出仰賴電話亭之物理區隔，以進行私密談話之意圖，應該受到憲法第四修正案的保護；檢方利用監聽器材才能側錄到的談話內

[61] *See* Katz v. United States, 389 U.S. 347, 352 (1967)。

容，已經逾越了公眾於電話亭外所能得知的訊息範圍，這樣的監聽側錄被視為實質侵入了 Katz 的私密範圍，是違反憲法第四修正案的。進一步來說，在 Katz 案中最高法院解釋憲法第四修正案不受地點之拘束，同時 Katz 案亦將憲法第四修正案的保護範圍擴張到例如私人談話內容等無體物，而非僅保護如同條文內容所列舉之有體物。即使人民所處之地為公共場所，若他/她不希望自己的某些行為或者隨身物品讓公眾知悉，且表現出適當的隱私保護意圖，則這種隱私主張的權利，就屬於憲法第四修正案的保護範圍。本案中 Katz 於電話亭內的談話內容，受到電話亭的區隔，外界的公眾難以獲知其談話內容，應視為 Katz 並不欲讓公眾得知此次談話內容，係一種隱私權主張的行為，故檢方利用儀器側錄的過程，違反憲法第四修正案，該次側錄所獲得的內容，屬於非法的證據，不能作為呈堂證物。

自 Katz 案起，隱私權的具體表現即有了一個標準，亦即合理的隱私期待性，這成為討論隱私權是否得以主張並且受到法律保護的主要核心。由此出發，合理的隱私期待性逐漸發展出兩種判別模式，分別是以過程為標準的判斷模式以及以結果為標準的判斷模式。前者主要發展出二原則，分別為知覺提升/替換原則，以及普遍公眾使用原則；相對於此，後者發展出明知且自願暴露原則、明知且被動暴露原則、第三方知情而暴露原則等等[62]。

1.1 以過程為標準的判斷模式

此判斷模式主要針對個人與公眾發生關係時，個人的行為是否得為公眾所知悉，無論個人有無意圖保持隱私。舉例而言，若個人與人交談或打電話時，音量過大，則其身邊周圍之人即可能在正常狀況下，聽聞其談話內容，在此狀況下，該人欲主張其談話內容具有隱私期待性而可以成立之可能性即低。類似的情況在現今社會中，搭乘大眾運輸工具時或有所體驗，即乘客透

[62] 岑釗梅，〈電子時代的隱私權保護--以美國判例法爲背景〉，《中外法學》，Peking University Law Journal, Vol. 20, No. 5, 頁 773-777（2008）。

過行動電話交談時，經常會有過大的音量，導致身邊的人即使不願意，也會得知該次談話內容（至少是發話者的談話內容）。而知覺提升/替換原則，即是指在工具輔助之下，若透過該工具輔助，係用以提升人類之五感，例如透過望遠鏡提高可視距離；或者用以替換人類之五感，例如透過紅外線攝影機偵測熱能，取代一般之視力。則此類技術所提升/替換的能力程度差異，自然代表侵入他人領域程度的不同。因此，若僅僅只是提升人體五感來察覺他人的行為或者事物，則在美國一般咸認不會侵犯他人之隱私權內容。但是當技術能力提升到替換人類五感能力時，例如前述以紅外線攝影機取代一般視力，由於此類技術所呈現出來的效果已經超越正常人類所可能表現出來的能力，因此透過此類知覺替換技術來察覺他人的行為或者事物，即相當可能被判定為已經侵犯他人之隱私權內容。

隨後發展出的普遍公眾使用原則，即是針對能達成知覺提升效果的工具，其能使用但不會造成侵犯隱私權內容的工具效能範圍，進行進一步討論。意即雖然某工具是用以達成知覺提升之效果，若該提升效果過於強大，而超出當代公眾的普遍認知時，使用該工具進行偵查即可能會被認定為侵犯他人之隱私權內容。例如在 Dow Chemical Co. v. United States[63]一案中，環保署所使用的高空精密攝影器材，使得環保署人員能夠搭乘飛機於高空中，針對 Dow Chemical Co.之工廠內部進行拍照，其所得之照片精細度，甚至可以清楚揭示 1/2 英吋內的事物細節，即使在 2009 年的現在，這種儀器都並不是一般公眾能夠且會使用的工具，因此若在該案中，Dow Chemical Co.能夠主張並且適用此普遍公眾使用原則，則環保署的作法很可能會被判定為已經逾越一般的水準，而侵害了 Dow Chemical Co.的隱私權內容。值得注意的是，此普遍公眾使用原則會隨著時代的演進而需要逐步修正，即公眾所使用的器材亦會逐漸進步，使得從前被認定為效能過高而有侵權之虞的工具，在

[63] *See* DOW CHEMICAL CO. V. UNITED STATES, 476 U. S. 227 (1986)

未來即可被認定為不會夠成侵權。例如現代的數位攝影器材，普遍具有高感光度(ISO)設定，在這種設定下，僅需少量的光線，即可拍攝出足夠清晰的照片，使得攝影者在微光中仍然能夠拍攝出曝光程度很足夠的照片。目前來說，許多數位攝影器材的高感光度設定幾乎均可達到 ISO 3200 以上仍然清晰的等級，而這是過往使用底片作為感光元件所無法企及的效果。

前述二原則所面臨的最大問題，即是到底怎樣的工具屬於感官提升，且又屬於公眾普遍得以使用之工具，加上現今世界各國之間交流頻繁，所謂「公眾」之認定是否因不同國家而有所不同，都是法院於審理時難以認定的事實。

1.2 以結果為標準的判斷模式

此類判斷模式主要針對造成隱私暴露之結果進行判斷。以 Katz 案舉例，被告於電話亭中打電話，代表其對該次談話具有主觀上的隱私權主張意圖；若被告係於一人來人往的廳堂中使用公共電話，由於四周可能隨時有他人經過，或許被告之談話內容即可能被認定為主觀上不具有隱私權主張之意圖。在 Katz 案中，即有法官指出類似的意見，認為若某人明知此訊息會披露給公眾得知，即使該人位於私人辦公室或者住宅，這種訊息也不是憲法第四修正案所要保護的標的[64]。因此，明知且自願暴露之行為，便可能會破壞訊息內容受到隱私權保護的範圍。

但有些狀況，人們明知會面臨資訊暴露的狀況，可是為了另一個不得不達成的目的，僅能選擇被動暴露。例如搭乘飛機時，每一個乘客都需經過 X 光檢查以及安全人員的進一步確認無影響飛安之虞後，才能夠登機。乘客雖然知道將要通過這些檢查，但是為了搭乘飛機，卻無法選擇不接受這些檢查。在這種狀況下，由於此類檢查係為了公眾利益的目的，即確保飛航之安全，因此此類公共利益的維持被認為大於對於個人隱私權的保護，這種獲取

[64] *See* Katz v. United States, 389 U.S. 347, 351 (1967).

被動釋出的隱私權內容行為，也常被認為是合乎法律規範的行為。進一步言，當要達成一個行政目的所能夠帶來的公眾利益程度相對降低時，行政行為本身便會受到較為嚴格的限制。以類似的強制檢查為例子，例如警察於道路上進行例行臨檢或盤查，由於其並非已經發現犯罪事實而針對嫌犯可能脫逃的路線進行過濾，而較屬於一強化治安穩定並發揮事前警惕效果之勤務行為，因此警察人員僅能於要求駕駛停車後，針對其所能目視之範圍進行檢查；除非發現明顯可疑且具有犯罪可能性之事跡，否則不能進行進一步的檢查行為，例如不能要求駕駛員或乘客開啟行李箱、進行搜身等等。

亦有學者認為，當情況為第三方知情而被動暴露時，個人也不能主張隱私權合理期待[65]。此種狀況為，如果個人對於自己的訊息並沒有主動揭露給公眾，而只是在基於信任而假定第三人不會洩漏訊息的情況下，主動揭露給第三人，可是該第三人卻將此訊息透露給其他人，則該個人應當自己承受此類訊息可能被洩露之風險；因為要求第三方為其保守秘密的期待性，在沒有契約的狀況下，是不合理的。在 Hoffa v. United States[66]案中，法院認為憲法並不保護這種將自己的隱私內容告訴錯誤信任之人而使其內容被洩漏之狀況。將此一原則引伸適用，在 California v. Greenwood[67]案中，最高法院認為，當個人將物品丟棄到垃圾桶時，由於已經拋棄了對這個物品的所有權，而且垃圾桶內的物品可以被任意搬動，因此垃圾桶內之物品的隱私內容，會被視為已經公開給公眾。

由以上的法規以及案例，可以大致理解，在美國，關於隱私權或者憲法第四修正案的關注重點，主要在於證據取得過程的正當程序（due process）原則之討論，正當程序的本質是一種對政府行為和權力的檢驗和審查，美國的正當程序制度是法院運用司法權力對政府行為和權力進行廣泛干預的重要手段，其目的是保

[65] 同前註 8，頁 777。
[66] *See* Hoffa v. United States, 385 U.S. 293 (1966)
[67] *See* California v. Greenwood, 486 U.S. 35 (1988)

障個人權利，是一項重要的司法審查制度[68]。正當程序是一個重要的法律原則，主要源自於英美法系國家，內容為，政府必須要尊重任何依據內國法賦予給人民的法律上之權利，而非僅尊重其中一部分或大部分的權利[69]。透過維持正當程序，能彰顯法治觀念與憲法原則的重要精神，即自然正義和自由精神[70]。而透過正當程序所取得之資料，即可利用於案件的審理程序，在此所著重的是將事後審查重點放在重視程序正義是否得以維持。

2. 隱私權在歐洲的發展

另一方面，在歐洲，類似的隱私權爭議案件，也成為研究的對象。與美國不同之處，在於歐盟國家協定出了歐洲人權公約，針對人權相關議題進行跨國家的規範，以期能在國家範圍之外，進一步確保人權在歐洲能夠獲得充分的保護。針對人權相關案件，若當事人在其管轄國家利用完所有可能的訴訟程序後，仍然無法獲得雙方都覺得滿意的審判結果，則可以上訴到歐洲人權法院，讓歐洲人權法院進行最後的裁決。在歐洲人權公約中，其第八條規定每個人的「私人及家庭生活、其家庭以及其通訊隱私的權利與自由必須受到尊重，若需要對此做出限制，則必須「符合法律規定」且「為民主社會所必需」[71]。本條文明確的規定，使每個人皆有免於受到非法搜索的權利。更有進者，在某些時候，本條文亦課予了國家「積極義務（positive obligations）」，以明確宣示在某些時候，為了達成對人權的保護，使人民能實質的享受並主張此等權利，必須要課予國家更積極的義務，亦即國家必須要有所「實質作為」，在人民的隱私被侵犯之前，便能讓人民的隱私能夠受到保護。

---

[68] 丁瑋，〈美國憲法上的正當法律程序〉，中國政法大學，2005

[69] *See* 28 Am. Bus. L.J. 567, 567-569 (1967).

[70] *Id*

[71] Article 8 – Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

歐洲人權法院指出，所謂個人內在範疇（inner circle），不應被限縮解釋。亦即若個人內在範疇被限制在個人可以過其所選擇之生活型態，則太過狹隘了；個人內在範疇不應排除圍繞在其個人周邊的外在環境，應該要納入一起考量，才能完整的解釋個人內在範疇。因此在探討私人生活的同時，也必需要相當程度地探討個人與其他人之間的關係的建立與發展[72]。因此，所謂私人生活的概念，便包含個人身份確認資料、心理以及生理的可視以及不可視的部分，以使個人能夠發展及實踐其人格之範圍。因此，在歐洲人權法院的認知下，隱私權是包含於私人生活範疇之內的一個範圍，屬於人權的一部份。

另外，歐洲警察署建立有犯罪相關的個人資料庫，可供會員國彼此之間瀏覽並且交換資料。根據歐洲警察署公約第 8 條[73]之規定，歐洲警察署之個人資料庫僅限於與犯罪相關之資料。可包含 1.在會員國內涉嫌犯罪或已經審判為有罪之個人資料 2.非常可能被判有罪者之個人資料。其中個人資料可包含：姓名、出生日地、國籍、性別、必要時可以加註不可改變之身體特徵。另外，個人資料庫可以記載犯罪案件資料、犯罪工具、會員國當局之處理案件資料、犯罪組織之可疑人物、有罪判決。而且會員國彼此之間可以交換資料。歐洲警察署公約所規範者，在於資料庫的內容以及利用資格，至於會員國將要如何處理此類資料，則並不在前述規定範圍之內。

在歐洲人權公約中，要求會員國家必需要負擔積極義務來保護個人的資料不致遭到濫用。何謂積極義務？以下案例或可作為實施積極義務之參考。在 I v. Finland[74]一案中，原告 I 原為醫護人員，在一次醫院的檢查中，被診斷為 HIV 陽性，之後 I 繼續在該醫院工作，但是由於當時醫院並未限制工作人員查閱病患

[72] "However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings." *See* Niemitez v. Germany, judgment of 16 december, (1992)

[73] *See* http://www.europol.europa.eu/legal/Europol_Convention_Consolidated_version.pdf

[74] *See* I v. Finland, (2008). http://epic.org/privacy/intl/echr-finland.pdf

資料的權限，因此原告開始懷疑醫院的同仁得知他的檢查結果，於是醫院更改了權限設定，使得僅有相關的醫護人員才能閱覽負責病患的資料。I 嗣後離職，並於離職後請求主管機關查閱是否其個人資料有被不當閱覽。但醫院沒有相關閱覽紀錄。於是原告對當地的主管機關提起民事訴訟，一直上訴到最高法院被拒絕後，轉而向歐洲人權法院提起訴訟，主張芬蘭違反前述歐洲人權公約第 8 條之規定。

雖然醫院主張其沒有保留相關閱覽記錄並非直接能證明有人閱覽了原告的醫療記錄，但歐洲人權法院最終判決「資訊系統欠缺合理安全措施，即構成隱私權侵害」 。這課與了建立資訊系統者一個積極的義務，便是需要在建構資料庫的同時，也建構合理的安全措施，否則無論有無隱私權侵害的事實發生，如此欠缺合理安全措施的系統本身，便已足以構成隱私權侵害。

另外，在一些民事爭議案件中，當事人在本國的訴訟中提出了關於隱私權的主張未果後，也轉而向歐洲人權法院提出上訴。國內有學者針對歐洲的個人私人生活與新聞自由，以及國家及媒體使用個人影像之方式及界限進行研究[75]。這些民事爭議案件雖然與刑事或者行政爭議不同，但法院於案件中對於何謂隱私權的保護，以及何謂積極作為的討論，也相當具有參考價值。歐洲人權法院在一些案件[76]中不斷強調，歐洲人權公約第八條之規定，要求國家必須負擔一定程度的積極義務，包含採取適當措施以保障個人之私人生活不受干擾，此私人生活之範圍包含個人彼此間之互動。

由前述美國以及歐洲的案例看來，歐美對於處理隱私權相關爭議問題的方式有所不同。美國對於處理隱私權相關爭議問題，主要採取的觀點係從正當法律程

---

[75] 廖福特，〈個人影像因私語新聞自由之權衡—Von Hannover 及 Peck 判決分析與台灣借鏡〉，《政大法學評論》，第九十一期，頁 145-198，（2006）

[76] *See* I v. Finland, (2008). http://epic.org/privacy/intl/echr-finland.pdf. *See* Spencer v. United Kingdom, Ent. L.R. 1998, 9(4), N70-71. *See* Von Hannover v. Germany, 4 Int'l J. Const. L. 533, (2004).

序進行探討，而前述幾個歐洲人權法院的判決顯示，歐洲法院在處理隱私權相關爭議問題時，主要的重點在於國家的實際作為，以及偏向隱私權利用目的的正當性討論。歐洲法院關注對於隱私權的干擾或者侵入，國家是否能夠以積極的作為來防止事件發生，或者對於隱私權內容的刺探，是否能引發正當的公眾討論，藉此試圖在公眾利益與個人權益之間做出一較為平衡之判斷。

3. 隱私權在我國的發展

隱私權於我國之發展，相對前述歐美各國，尚未發展出較具完熟規模之討論或造成實體法之修法，時間亦較為短暫。隱私權於我國之發展，主要仍是因個案狀況，上訴到最高法院後，由司法院大法官解釋之理由書中可見，隱私權一詞開始逐漸被使用，並且開始引入相關解釋以適用於個案中之狀況。雖然目前為止，我國關於隱私權並無任何明確的法條規定，亦未明文修入於憲法之基本權利內，但隨著社會發展以及案件累積，在過去許多大法官解釋文中，逐漸累積獲得我國對於隱私權的認知與規範。

在我國早期中，對於隱私權之保障並不是很重視，亦無專法規定（近年來有例如電腦處理個人資料保護法之提出，亦可視為隱私權相關法條開始逐漸受到重視，本法於 2010 年修改為個人資料保護法，不再限制於電腦處理部分，惟本法並非特別針對隱私權所立之法）。目前，關於隱私權受到侵害之處理方式，僅能藉由主張較為相近之民刑法之規定來保護或者去除侵害。典型者有例如刑法第 28 章之妨害秘密罪，係關於侵害非公開個人秘密之罪責。另外又有如民法第 18 條第 1 項規定「人格權受侵害時，得請求法院除去其侵害；有受侵害之虞時，得請求防止之。」；這是藉由將隱私權，透過司法解釋，解釋為人格權涵攝之範疇，而轉而援引民刑法中相關條文之規範，來保護或者去除侵害。民法經修法後，亦將隱私納入保護之範圍內，而於民法第 195 條明文規定不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，

被害人雖非財產上之損害，亦得請求賠償。大法官釋字第 656 號[77]即是針對本條文適用範圍所做出之解釋文，其判決重點為民法第 195 條第 1 項後段由法院為回覆名譽適當處分是否合憲之議題。

由過往的司法院大法官解釋文中，可以略窺隱私權於我國之發展過程。早期，在司法院大法官第 293 號解釋文中，處理了議會是否得要求銀行提供放款資料的爭議。而理由書之首段即明文指出「 中華民國七十八年七月十七日修正公布之銀行法第四十八條第二項規定：「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密。」旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。」其指出人民與銀行彼此間之財產往來資料，係一種隱私權之內容，應受到保障，不得輕易揭露。在此解釋文中，雖然並未進一步解釋何謂隱私權，然隱私權一詞已開始為法院所使用，且由事件中，可概略得知，法院開始認為有一些個人資料，是屬於隱私權的保護範疇，非有個人的授權，其他知悉資料之人不能任意公開。後續的許多大法官解釋文亦多有引用隱私權一詞，例如司法院大法官第 509、535、603 號解釋文，進一步解釋如何兼顧對於個人名譽、隱私、及公共利益之保護。我國憲法第 22 條規定「凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法保障。」以及憲法第 23 條規定「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持 社會秩序，或增進公共利益所必要者外，不得以法律限制之。 」可視為一個補遺規定，透過個案逐漸累積，隱私權逐漸被承認為一種人民之權利，而後即得以符合憲法第 22 條以及第 23 條之概括規定形式，成為受到憲法保障的人民基本權利之一。

前述之第 603 號[78]解釋文，便是為處理受到矚目的「戶籍法第 8 條第 2、3 項捺指紋始核發身分證規定違憲?」爭議。緣民國 94 年間，我國開始全面換發新

[77] 司法院釋字第 656 號解釋，
http://www.judicial.gov.tw/CONSTITUTIONALCOURT/p03_01.asp?expno=656
[78]司法院釋字第 603 號解釋，
http://www.judicial.gov.tw/CONSTITUTIONALCOURT/p03_01.asp?expno=603

型身份證，以取代舊有之身分證，而原戶籍法第八條第二項強制十四歲以上國民於請領身分證時按捺指紋，釋憲申請人認為此條文因侵犯人性尊嚴、人身自由、隱私權、人格權及資訊自主權等基本權利，並違反比例原則、法律 保留、法律明確性及正當法律程序原則而違憲。在解釋文中，大法官開宗明義即揭示「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第二十二條所保障。」從本案開始，最高法院即明確地承認隱私權是維持人格權完整性之一重要基礎，因此成為受到憲法層級保障的基本權利，其法理基礎即為憲法第 22 條之概括規定。

在 95 年度訴字第 540 號刑事判決[79]中，法院針對於私人處所進行活動是否表達出隱私期待性做出表示。在本案中，藝人小 S 等人於隱密的別墅之中進行派對，在上開活動中並有比較親暱之肢體動作。由於別墅之建築以及與鄰房間之樹木，已足以達到防止他人窺視之效果，因此，壹週刊之記者刺探派對之行為，已經構成妨礙秘密罪名。法院認為若當事人選擇於隱密之處所進行私人活動，便已彰顯出隱私期待性，此時，若針對當事人之私人行為進行刺探，即屬於侵害當事人隱私之行為。另外，在最高法院 95 年度台上字第 4879 號判決[80]中，法院則針對私人場所與公共場所之區隔，進行進一步的定義。在本案中，員警喬裝客人，進入 KTV 內攝影，進行是否發生違法行為之蒐證。法

[79] 參考臺灣台北地方法院，95 年度訴字第 540 號判決，「…可知該別墅之大門、圍牆及與鄰房間之樹木，均足以達到防止路人窺視之效果，他人於該別墅外之正常行止間，並無從目睹、監視該別墅大門及圍牆範圍內之活動。況告訴人等在上開活動中，曾與友人有較親暱之肢體動作，如擁抱、親吻等，此有系爭壹週刊報導所刊登之照片可證（同偵卷第十三、十四、十六頁），核之該等行為態樣相當私密，可知告訴人等人主觀上對於該等活動有隱私之需求及期待。綜上各情，堪認告訴人丙○○等人於九十年八月四日在上址別墅內進行之上揭私人聚會，告訴人丙○○等人主觀上不欲公開，且所選擇之地點亦具有客觀上之場所私密性，自屬非公開活動無疑，應享有隱私權不受侵害之合理期待。…」

[80]參考最高法院，95 年度台上字第 4879 號判決，：「… 歌唱城係公共場所，坐檯小姐在未上鎖之公開包廂內，其言行在主客觀上均無隱私權之合理期待，… 」，因此進一步的認為：「由員警…喬裝男客至該歌唱城蒐證，員警蒐證之錄影器材僅為其耳目之輔助，其攝錄內容在於補強員警供證之真實性，與搜索之定義不符，更非通訊保障及監察法所保障之通訊範疇，… ，則原審認該錄影帶具有證據能力，採為上訴人不利之認定，復無違誤。」。

院認為 KTV 雖然每一包廂均有門，但並無法上鎖，任何人均可能由外進入，故，包廂內之空間，應仍屬於公共空間，坐檯小姐在包廂中之行為，在主客觀上無法主張具有隱私期待性。在一些其他案件[81]中，法院亦認為公眾得自由進出之場所，便應該被認定為公開場所，而在公開場所進行一般行為之人，便無法對其行為主張隱私期待性。

另外，針對個人資料，最高法院於 91 年度台上字第 3388 號判決[82]中，指出個人資料屬於隱私權保護之範圍。在本案中，被告係分任台北市政府警察局中山分局、內湖分局警備隊之警員，被控收受賄賂提供有關人民入出境記錄及前科、通緝、更名與勞工保險等職務上應保守秘密之資料。法院認為，「個人之車籍、戶籍、口卡、前科、通緝、勞保等資料及入出境紀錄或涉個人隱私或攸關國家之政務或事務，均屬應秘密之資料，公務員自有保守秘密之義務。」，這些資料，均屬於個人隱私所保護的範圍。

而關於進一步理解隱私權於社會發展中所扮演之角色與判斷隱私權是否得以主張之方法，以及隱私權逐漸演繹出的各式各樣受到重視的實體性質，各國學者亦提出許多不同切入點之研究；例如開放空間中的個人隱私權的問題，主要不外乎監視、定位與追蹤三項行為，且開放空間中取得的個人資訊行為到底有沒有侵害個人隱私權?在沒有一般客觀的標準提出之前，只能從各個行為的態樣與類型，予以歸納[83]。又如以判斷是否具有隱私權之方法，包含「隱私權核心理論、

[81] 請參閱高等法院 93 年度上易字第 1077 號刑事判決、94 年度上易字第 1143 號刑事判決、91 年度上易字第 114 號刑事判決等。

[82]參考最高法院，91 年度台上字第 3388 號判決，「復說明：為維護車主權益及社會治安，查閱車籍資料以各級政府機關以公函查詢者為限；個人戶籍、口卡、前科、通緝等資料，係由台北市政府警察局戶口科負責，應依據「內政部警政署（下稱警政署）受理犯罪資料查詢作業規定」處理，屬於秘密資料，警員電話查詢須依警政署函領之「代號及代碼」始得查復。警局戶口通報台所建立之口卡資料、素行紀錄卡，非公務及非公務身分不得查詢。另入出境紀錄、勞工保險資料亦屬於應秘密之資料。迭經內政部警政署戶口查察作業規定並經交通部、台北市政府警察局、台北市監理處、勞工保險局明令在案。丙○○、甲○○皆為依據法令從事公務之警察人員，根據公務員服務法第四條規定，負有絕對保守政府機關機密之義務，不論是否為其主管之事務均不得洩漏，乃任意對外提供上述應秘密之消息以牟取不法報酬，其違背公務員服務法之規定，情至顯然，不因甲○○非主管勞工保險職務而有所不同。至於丙○○利用警察人員從事調查職務之機會，向警局通報台或相關業務主管機關查詢管制資料，其違背職務尤不待言等情綦詳。所為論斷，俱有卷內證據資料足憑，從形式上觀察，原判決並無違背法令之情形存在。」

[83] 蔡達智，〈開放空間中的隱私權保障〉《月旦法學雜誌》，No.145，（2007）

同意與利益衡量」[84]、例如以隱私權之質性進行判斷，包含「獨處性」、「秘密性」、「自治性」、「匿名性」及「親密性」等性質[85]。

（二）、隱私權發展的轉變

在前述 1967 年於美國發生的 Katz 案中，法院確立了當事人欲主張隱私權之成立，必須具有合理的隱私期待性原則[86]。依此原則，美國繼續發展出從主觀及客觀角度來針對合理的隱私期待性進行判斷之原則。例如所有人將垃圾放置在垃圾桶或者交由垃圾處理人員處理後，由於其已遺棄該垃圾及內容物，因此，將被判定為所有人已不可再行主張對於垃圾內容物之隱私權。這是基於財產權的觀念所演繹出來的判斷標準，將隱私權解釋為附於物品之上之某種無體價值，一旦所有人主觀地決定將該物品丟棄之後，該物品之財產權即被視為不再專屬於原所有人，而後續持有該物品之人，便可取得該物品之所有權，以及附在該物品上之資訊內容，自然也包含了隱私內容。

另外，在 State v. Schwartz 案中[87]，南達科塔最高法院針對其州內搜索與扣押的規定是否符合憲法第四修正案之規定進行判決。本案中，被告 Schwartz 被控告非法使用藥物，政府探員將置放在被告住居所附近的垃圾桶取走，並檢視丟棄在垃圾桶裡的物品，結果發現許多具有燒焦痕跡的錫箔紙、殘留一些粉末的吸管，以及一些綠色的葉子殘留。隔週，探員再次搜索同一個垃圾桶，並且又發現許多具有燒焦痕跡的錫箔紙。探員認為這些自垃圾桶中蒐集到的物品是吸毒跡證，便將這些物品拿去化驗，結果也呈現毒品的反應，於是探員即以這些證物申請並取得對被告住居及人身的搜索票，隔天探員帶著申請到的搜索票搜索被告的住居處並且發現非法藥物，並據此起訴被告。在審理過程中，被告提出抗辯，認

[84] 蔡達智，〈隱私權初探〉，《法學叢刊》，50 卷 3 期，頁 93-98（2005）。

[85] 岑釗梅，〈電子時代的隱私權保護--以美國判例法爲背景〉，《中外法學》，Peking University Law Journal, Vol. 20, No. 5, 頁 768-771（2008）。

[86] *See* Katz v. United States, 389 U.S. 347 (1967).

[87] 689 N.W. 2d 430 (S.D. 2004).

為探員在垃圾桶內搜索到證物的過程是非法的，因為探員並沒有取得搜索這些垃圾桶的搜索令狀，並認為根據垃圾桶內的證物取得搜索票的過程，以及之後自被告住居處搜索到的證物，也都因為毒樹果實原則[88]，由於其先置的搜索過程違法，所以後續取得的相關證物也都不能在法庭上使用來對抗被告。

在 Schwartz 案中，法院認為依照 Katz 案建立的隱私權保護原則，為成立隱私權保護的可能性，個人需要對隱私內容表達合理期待性。進一步的，在本案中，法院認為是否有隱私權保護的可能性，除了參酌被告是否對其棄置的垃圾表達出合理的隱私期待性之外，亦認為要考慮社會對涉案事件的隱私期待性的看法。總結來看，本案被告將垃圾丟棄於公共垃圾桶的時候，已經放棄了對於垃圾的持有權利以及合理的隱私期待，因為棄置在公共垃圾桶的垃圾已經不再為個人所有了，且同時社會大眾對於將垃圾棄置在垃圾桶之行為，亦認為應不再適用以提出隱私期待性之主張，因此本案並不適用憲法第四修正案中對於政府干擾個人隱私權內容之規範，判決被告的主張不成立，探員最初所蒐集到的證據以及之後的搜索過程，都是合法有效的。

類似的案件在美國逐漸引起關於搜索扣押可能侵犯人民隱私權議題的討論，加上科技的進步，使得探測的能力日趨進化，更有可能以各式各樣的新技術，對個人進行探測。美國聯邦第十巡迴上訴法院曾經表示「探測科技的演進，可能使得憲法第四修正案的規範內容越來越受到挑戰」[89]。另外針對前述棄置垃圾後，是否仍得主張隱私權而言，美國最高法院過往採取的一個判斷標準是「棄置分析(abandonment analysis)」，允許法院採行以財產權為基礎的解釋方式，認為當某一個物品被拋棄時，原持有者即已視同放棄對其之財產權主張，後續持有者可完全擁有該物品[90]，而原持有者不得再針對該物品與其上所攜有之資訊，主張隱私權。棄置分析指出，原持有人丟棄一物品時，亦喪失對該物品之所有權、控制

[88] 關於毒樹果實理論，可參見王兆鵬，刑事訴訟講義，頁 42-48（2002）。
[89] *See* Jennifer Murphy, *Trash, Thermal Imagers, and The Fourth Amendment: The New Search and Seizure*, 53 SMU L. Rev. 1645, 1649-1650 (2000).
[90] *Id. at* 1659-1660.

權，他人拾獲該物品時，即可依自己之意思處理該物品，無須再獲得該原持有人同意，這是一種以財產權為基礎的解釋，並廣為美國法院所接受。

類似地，各國關於隱私權之發展議題，都逐漸朝向提出隱私權所欲解決之問題主體乃在於個人[91]，其著重於個人針對隱私權內容做出一決定時之意志表示[92]。在美國的 Greenwood 案[93]中，法院即提出三種方法可以檢測個人是否得以在本案中主張隱私權：

(1) 法院根據 Katz 案，認為對垃圾有隱私期待性是不合理的；

(2) 法院根據 Katz 案，認為人們明白知悉其棄置垃圾袋時，其隱私期待性必定被破壞；

(3) 法院依據使用者拋棄垃圾的動作，來訂出一個界線；當個人棄置垃圾時，對於該垃圾袋及其內容物來說，由於已經喪失了控制的權利，因此是沒有隱私期待性可主張的。

在 Greenwood[94]案中，警察懷疑 Billy Greenwood 販賣毒品，然而警方並未有足夠的證據，得以申請搜索令狀，以進入 Greenwood 住處進行搜索。然而警方發現 Greenwood 將垃圾放置於一個黑色不透明的塑膠袋中，並且丟棄在住家附近的垃圾桶，警方因此去搜查這個被 Greenwood 丟棄的垃圾袋，並且在垃圾袋中發現疑似使用毒品的遺跡。警方便依照搜索垃圾袋所獲得的證據，申請獲得搜索令狀，進而對 Greenwood 住處進行搜索，且在其中發現了毒品，並且逮捕 Greenwood。

在法庭上，Greenwood 認為他對垃圾袋的內容物得主張隱私權，而警方搜索垃圾袋進而申請獲得搜索令狀的過程侵害了他的隱私權。但法院認為，需要對某物品表達一種主觀上的隱私期待，才具備主張隱私權的基本要件。在本案中，

---

[91] *Id*

[92] See Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1202-1203 (1998).

[93] *See* California v. Greenwood, 486 U.S. 35 (1988).

[94] *Id*

Greenwood 並無法提出任何證據證明他對於垃圾袋內的東西具有主觀上的隱私期待性，因為當垃圾被棄置在垃圾桶中後，除了垃圾清運人員以外，其他路過者、流浪漢，均有可能去翻閱那個垃圾袋。亦即，當 Greenwood 丟棄了那個垃圾袋時，其便已經破壞了對那個垃圾袋的隱私期待性，因此無法就該垃圾袋以及其內容物主張隱私權被警方侵害，因為警察的所作所為，只不過是其他路過者都可能會作的事情而已。

在後 Greenwood 案時代，美國各級法院對於如何處置垃圾與隱私權爭議的問題開始發酵。例如第七巡迴法院在 United States v. Hedrick 案中，自行發展出「明知暴露測試 (knowing-exposure test)」判斷方法，其類似於前面的財產權基礎法則。第七巡迴法院以物件棄置於公開地域來判斷原持有者棄置之行為得視為其已經表現出不再想要持有該物件之意圖；此時，公眾（或其他特定不特定第三人）即具有無須棄置者同意即可檢視該物件之權利[95]。雖然在 Greenwood 案中，最高法院的多數意見認為上訴人主張對垃圾具有隱私期待性是不合理的，因上訴人在拋棄垃圾時，應被認定為已經放棄對於垃圾的隱私期待性了，上訴人之主張應被認定是於案件發生後，為迴護自己的利益而生的抗辯說詞；但在本案的不同意見中，布南大法官(Justice Brennan)指出，即使是一個垃圾袋，亦可能攜帶製造垃圾者之個人生活習慣，而搜索垃圾袋所能探知的隱私內容，其效果與進入私人臥房內進行搜索已無異相同[96]。前述的棄置測試，乃是根據財產權基礎發展出來的測試方式，由於有體財產的所有會隨著持有人的轉移而跟著轉移，因此前述測試認為，當個人棄置垃圾時，由於已經放棄了持有狀態，因此後續第三方取得該垃圾時，即一併取得該垃圾上所攜帶的資訊，故先前持有該垃圾之個人，即沒有

[95] *See* United States v. Hedrick, 922 F.2d 396, 1991, and Jennifer Murphy, *Trash, Thermal Imagers, and The Fourth Amendment: The New Search and Seizure*, 53 SMU L. REV. 1645, 1663 (2000).

[96] *See* Jennifer Murphy, *Trash, Thermal Imagers, and The Fourth Amendment: The New Search and Seizure*, 53 SMU L. REV. 1645, 1663 (2000), 1662, " a single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it. A search of the bedroom, can relate intimate details about sexual practices, health, and personal hygiene.' 'it cannot be doubted that a sealed trash bag harbors telling evidence of the intimate activity associated with the sanctity of a man's home and the privacy of life".

隱私期待性可以主張。布南大法官不同意法院透過以財產權基礎發展出的棄置測試來判斷當事人是否放棄了隱私期待性[97]，但他並沒有進一步提出應該以怎樣的測試方式或者基礎來判斷當事人有無隱私期待性意圖。縱使如此，布南大法官的不同意見，仍然告訴我們，以財產權為基礎所發展出來的隱私權判斷方法，無法解決財產權與隱私權在性質上的不同，亦即財產權的實體佔有通常僅能被單獨佔有；而隱私權則否，其重點在於隱私權的資訊內容，而不是資訊所附著的物品。

1. 隱私權與財產權之差異-知悉隱私權內容不以佔有為要件

前述幾個案例中，法院的判斷準則仍然不脫以財產權為基礎，概括地來說，前述案例可歸納為當個人明知地丟棄物品時，即不得對後續持有該物品之人主張隱私權。進一步來說，類似的判斷準則認為，當個人有意識的將物品或垃圾放置在公開的領域，特別是垃圾集散地點或者垃圾桶時，由於個人已經不再持有該物品，且依照社會的習慣來看，當個人將物品棄置在公開領域中時，意味著他自願將這些物品放置在可以受到其他不特定人物可觸及的範圍內，其他人均可能可以拾得並持有該物品，這與垃圾棄置在自家後院的情況並不相同，個人可以限制他人出入其家園，但無法限制他人在公開地域活動的行為。或者，個人將物品棄置在垃圾集散地點時，社會的習慣會認定將會有垃圾車或者清潔人員來蒐集並處理這些垃圾，而放置在家裡的垃圾則不會受到如此的對待，清潔人員不會主動跑到家裡來將垃圾取走。因此當個人在這些特定的地點棄置物品時，可被推定為有明確的放棄所有權意圖，不得對後續持有該物品的人主張附隨於該物品上之資訊隱私權。在 Schwartz 案以及 Greenwood 案中，警察人員先搜索垃圾中的物品取得初步證據後，再對被告進行進一步搜索的行為，正是透過類似的準則檢驗，均被法院認為並未違反憲法第四修正案的規範內容。

惟以前述案例而言，有幾點狀況值得進一步思考。首先，以垃圾袋為例，既然是棄置在垃圾集散地點或者公開地點，那麼如何證明垃圾袋中之物品是與何人

[97] *Id. at* 1645.

有關？以 Schwartz 案為例，那些疑似非法藥物使用的痕跡，如何能夠初步證明是被告所遺留？根據該些使用痕跡而進一步申請搜索票的過程，其核發搜索票的決定是否容有疑義？另外，在前述案例中，原持有人將附載有個人資訊之物品丟棄時，依照社會的習慣，應該是認定這些物品會被清潔人員帶走並做為垃圾處理掉，而不是認為這些物品會被拿去進行進一步的資料統計及分析，進而被其他人獲知該原持有人之個人生活習慣或其他隱私權所涵蓋的個人特徵。

前述以財產權為基礎，來理解隱私權的方式，將會忽略隱私權與財產權所不同的一個重要特質。不同於物品必需要接觸以及持有來使財產權之主張能夠成立，知悉隱私權內容之行為，可為一無須接觸便可重複知悉之行為。以美國最高法院針對處理垃圾與隱私權議題中所採取的解釋而言，當個人公然棄置垃圾時，即已代表其放棄對這個垃圾的財產權主張，後續持有者可完全持有該垃圾。因此陸續發展出若個人符合某些棄置測試時，則他人在個人棄置垃圾之後，持有該垃圾之行為，並不會被認定為侵犯該個人之隱私權。此一論述的重點在於財產的持有，通常以某一特定人為限，亦即某甲持有一物品時，某乙即無法持有該物品。但隱私權的重點並不在持有，隱私權所著重者，乃其可代表隱私權人之個人生理心理特徵或者行為結果之資訊內容。一旦隱私權的內容被其他人知悉之後，便很容易被以各種形式散佈出去，例如個人的健康狀況，可以文字形式記載於醫院之病歷，而要知悉個人的健康狀況，並不需要持有該病歷，僅需要閱讀病歷之後，便能獲得相關資訊；且要散佈前述隱私內容，也不需要持有該病歷，可以在知悉之後，另行記錄或者透過口耳相傳，便能將此隱私內容散佈出去。當隱私權之內容被散佈出去後，每一個接觸到該隱私權內容之人，皆可知悉並且散佈該隱私權內容，從而造成對隱私權人的隱私內容之侵入與干擾；其更可藉由有形或無形之複製進一步散佈，尤有甚者，即便是口耳相傳，亦可能對隱私權人造成干擾或傷害。此一特質，是隱私權不適宜以財產權來作為解釋基礎的重要差別，這類的狀況，也非財產權所會面臨的問題。

由布南大法官於 Greenwood 案中所提出的不同意見，已可理解布南大法官已預見隱私權與財產權性質之差異存在。他提出的不同意見可被進一步理解為，搜索垃圾袋對於隱私權的破壞，並不在於後續發現者是否能持有個人丟棄的物品，而在於後續發現者能探知物品上所攜有的資訊，這些資訊才是構成隱私權內容的主體；後續發現者若僅是單純持有該丟棄的物品，並不會破壞個人所想要保護、隱匿的隱私權內容主體，但後續發現者若於持有該丟棄的物品後，進一步針對物品上所搭載之資訊進行分析，則其分析結果，縱非百分之百，亦將相當程度地侵入個人之隱私權內容主體。因此，即使是一個垃圾袋所包含的物品，在經過適當的分析之後，亦可能獲得製造垃圾者之個人生活習慣，而搜索垃圾所能探知的隱私內容，實與進入私人臥房搜尋無異。若經過長期的資料蒐集與分析，將有可能可以拼湊出個人的行為模式與生理心理特徵。

更直觀的來說，國內有學者亦提出隱私權可以理解為是一種可以分辨個人與他人之間不同之一種狀態權利[98]，而可直接或間接鑑別個體的資訊，稱為個人資訊(personal data)[99]。根據司法院大法官第 293 號解釋文的相關解釋條文，大法官承認隱私權為憲法所保障的一種基本權利，第 509、503、603 號解釋文更進一步解釋如何兼顧對於個人名譽、隱私、及公共利益之保護。如同前述，大法官釋字第 603 號中，林子儀大法官即提出如下見解：「蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。[100]」此類資料庫比對技術，隨著硬體與軟體技術的日新月異，經過適當的設

[98] 唐淑美、顏上詠、顏于翔、洪德俊，〈應用生物辨識於網站購物之隱私權探討〉，《產業論壇》，第九卷第二期，頁 103（2007）。

[99] 同前揭註，頁 104。

[100] 參考大法官釋字第 603 號，林子儀大法官協同意見書：「蓋隨電腦處理資訊技術的發達，過去所無法處理之零碎、片段、無意義的個人資料，在現今即能快速地彼此串連、比對歸檔與系統化。當大量關乎個人但看似中性無害的資訊累積在一起時，個人長期的行動軌跡便呼之欲出。誰掌握了這些技術與資訊，便掌握了監看他人的權力。故為因應國家和私人握有建立並解讀個人資訊檔

計與執行，即可能藉由瑣碎的資訊，拼湊出關於個人的行動軌跡或者其他隱私資訊。個人在日常生活中，不可避免的會因為與他人或者社群互動而產生許多垃圾或者資訊交換的行為，這些交換的資訊或者產生的垃圾，必然與其行為以及行為發生的時間具有不可切割的連續關係。舉例而言，這些垃圾或者資訊，猶如個人行為之「足跡」，只要個人持續地進行活動，這個足跡就會繼續存在並且隨著時間向前延伸。因此，如同分析足印可以獲得個人之特徵，例如身高、體重、步行習慣等等一般，分析這些個人製造出來的資訊，亦將能拼湊出個人之某些生活習性與行為特徵，尤其加上時間參數後，累積了一定數量的資料可以藉由資料採礦或者文本採礦的科技工具的輔助，獲得更多訊息。

2. 隱私權與財產權之差異-隱私權內容洩漏不易察覺

除此之外，隱私權與財產權仍有其他性質上的不同，例如權利被侵害時的察覺程度，二者便不相同。以財產權而言，對物品持有權的轉移通常較容易被發現，例如某人外出時遺失一物品，則某人之後檢視自己所持有之物品時，很快就會發現該物品遺失了；又例如某甲將自己的汽車借給某乙，則兩人都立刻知道現在該汽車之持有權，已從某甲暫時轉移到某乙。凡此種種有體財產權之轉移，皆是容易迅速被察覺的，即便不是當下立刻察覺，也能夠很快發現。但隱私權內容的洩漏或者散佈，並非如此明顯地會被原持有人察覺。再以前述垃圾為例，當某人丟棄垃圾時，在其一般的認知下，應是認為他將垃圾丟棄後，預想該些物品將被垃圾車收集，並以垃圾處理的方式破壞或者消滅；此時若有其他人收集某人所丟棄之垃圾，並分析垃圾中物品上所載之資訊，而後意圖從這些分析結果中，推估與某人相關之行為特徵資料時，一般而言，某人並無法察覺此狀況。同時，這些特徵資料雖然僅係單方面由其他人建立，並未事先經過某人檢視其分析結果，或者獲得某人之證實其內容正確與否，惟該等經由分析所得之資料，仍將某程度地反

案的能力，避免人時時處於透明與被監視的隱憂之中，隱私權保障的範圍也應該隨之擴張到非私密或非敏感性質的個人資料保護。本院釋字第五八五號解釋亦係有鑑於此，而將個人資訊之自主控制權納入隱私權保障範圍內，不限於個人秘密不受揭露的自由。」

映出某人之行為特徵及/或生活習慣，甚至是個人自己沒有察覺的特徵或者生活習慣。對個人而言，其他人藉由這種經由個人並未體認或知悉之方式，來獲取關於個人隱私權內容之資訊，在個人體認或知悉其隱私內容已經被分析與散佈之前，由於尚處於一無所知的狀態，因此個人並不會產生困擾的感覺。直到其他人開始利用這些隱私內容干預個人的生活，並且被個人知悉時，他/她才會真正發現這些隱私內容已經洩漏出去，而這種隱私內容洩漏的情況將開始影響正常的日常生活，並且影響到某人後續面對類似狀況時的處理態度。以前述垃圾丟棄狀況為例，如某人可能開始改變他或她處理垃圾的方式，又例如我國社會上經常可以聽聞的詐騙電話，即是個人的金融交易資料與個資外洩造成的結果，但是國民在收到詐騙電話之前，是沒有辦法得知其隱私內容已經被洩漏給詐騙集團的。

（三）、隱私權在我國的進一步發展

前述隱私權的特殊性質，使得我們必需要重新檢視過往至今對於隱私權的理解，例如雖然個人棄置的物品，無法再行主張財產權，但依照「棄置分析」或其他類似的見解，對於個人棄置的物品，是否得以完全自由地分析其上所可能攜帶的隱私權資料內容，便值得進一步思考。又，許多看似無害的個人隱私資料內容，在拼湊起來之後，便可能透露出許多進一步的個人訊息，針對這一類的資料分析，是否必要對其進行限制。而針對許多可能觸及隱私權資料內容的應用技術，國家應該要負擔何種責任，使得這些利用的最終結果，能夠對社會公益產生正面的效果，同時又能適度合理的保護個人的隱私資料內容避免被不當利用，都是值得思考的問題。

而資訊科技發展到現在，是否能夠在現今的體制之下，對於個人的部分隱私權內容進行分析，並且獲得進一步的分析結果，以協助犯罪偵查進行，將在下一章節中進行介紹。


E S A
1896

四、 建立廢棄物資料庫應用於刑事偵查與隱私權之關係

（一）、我國刑事訴訟法之強制處分

在前面的章節中，我們看到了各國關於隱私權議題的發展與現況，也看到了現今資訊科技技術能夠對資料分析產生的效果，這驅使我們開始進一步思考何謂隱私權的性質？何謂侵犯隱私權？何謂保護人民的隱私權免於被侵犯？國家能否為了社會公益的目的，而適度的干涉人民的隱私內容？即便人民的隱私內容被國家所知悉，但當國家並未對個人採取行動之前，個人其實並未意識到自己的隱私內容已為國家所知悉，他或她並不會有任何不快的感受；此時，隱私權更像是一個不會實質影響生活的代表名詞。前述隱私權被認為具有「獨處性」、「秘密性」、「自治性」、「匿名性」及「親密性」等性質，可視為探討個人隱私權本身自我控制被利用程度之性質。若關於個人隱私內容的資訊可以被國家蒐集並且處理，那麼國家又必須肩負怎樣的積極作為來保護這些國民的隱私資料？而自隱私權內容的保存與應用，對隱私權人可能產生的影響切入，來探究刑事訴訟法中，強制處分對這些隱私權應該被注意的性質之影響，是本章節所要探討的重點。

強制處分原為在犯罪偵查階段，法院受到偵查機關之請求而發動特定的處分，其重點在於期待發現並保全被告及與犯罪相關之各種證據，保全證據部分，例如搜索、扣押、身體檢查、通訊偵查等等，因此強制處分實質上往往成為影響國家追訴權能否行使之重要因素。特而言之，例如搜索、逮捕之時機，一旦錯過，即可能成為直接影響國家追訴權是否得以行使之決定因素[101、102]。

就強制處分之性質論，可理解為「刑事訴訟上之基本權干預」[103]，刑事訴訟法中關於強制處分之規定諸如傳喚、拘提、通緝、身體檢查及監聽等等，其中身體檢查及監聽很明顯地會干預人之隱私權，而後者亦具有秘密進行之特質，受處

[101] 參見林鈺雄，刑事法理論與實踐，頁 36-37 （2002）。
[102] 參見林鈺雄，刑事訴訟法(上)-四版，頁 267 （2005）。
[103] 同前揭註，頁 268。

分人無法察覺其影響，與傳統型態例如拘提、逮捕、羈押等干預處分顯然不同[104]。

強制處分目的之一既在保全證據，則發動時機與追訴效率即成為執行強制處分之考量重點；相對於此，關於強制處分之審查，可概分為法官保留原則及偵查機官決定原則，發展至今，亦有依偵查中及審判中區隔之混合類型。上述各種審查類型，皆可理解為在效率與分權制衡中求取平衡共榮之努力，希望既能顧及追訴效率，又能不過度干預受處分人之基本權。因此，為達成國家機關追訴犯罪之目的，以強制處分之模式，適度地干預受處分人之基本權，應是社會可以接受之作法。而本文接下來所欲討論的主要課題，即在於我們是否可以思考透過廣泛地蒐集人民的隱私相關資料，以企圖於犯罪前後，達成犯罪預防及協助犯罪偵查之目的。

由於隱私內容能某程度地透露出個人之資訊，對於犯罪偵查而言，具有輔助性質，因此，若能透過事前的資料蒐集分析，建立相關資料庫，在犯罪發生後，即可能透過現場跡證保全，再與資料庫內容進行比對，例如前述的資料採礦以及文本採礦，以限縮偵查的範圍，將可能可以進一步鎖定特定區域以及特定特徵的犯罪嫌疑人，協助國家進行犯罪偵查。

（二）、資料庫比對技術應用於刑事偵查

如前所述，資料庫或者資料倉儲的特徵是具有非常大量的資料，若再加上與時間相關的資料累積與更新，那麼資料量將更趨龐大。資料採礦與文本採礦的概念或許已存在於更早之前的研究當中，但直到 1990 年代才開始有學者提出實際的研究方法，並且加以驗證與發展的主要原因之一，即在於硬體的處理能力必需要足夠強大，方有可能實現良好的資料倉儲，以及資料採礦。由於資訊工業之進步，單一電腦能夠處理的資料量及處理速度均快速地成長，加上網絡聯繫處理之技術發展，以往需要許多電腦方能處理之資料量，例如影像處理及特定資料比

[104] 同前揭註，頁 265-284。

對，現在僅需要數量較少之電腦，即可在更縮短之時間內，獲得與之前需要多數電腦及較長處理時間所能獲得之相同的結果。因此，從前概念上可行但技術上不可行的想法，藉由資訊硬體以及處理技術的進步，便逐漸變得可行。關於硬體上的進步，舉例而言，現今個人電腦的中央處理器，相較於五六年前個人電腦的中央處理器，其單位時間內的運算量，大約增進了將近三十倍[105]。這代表現代的個人電腦若連續運作一整天都不休息，則其一天的運算總量，已是五六年前的舊電腦需要運作一整個月才能運算完畢的資料量，易言之，電腦處理速度在五六年間，有長足的進步，其處理速度之差異是非常明顯的。假定資料庫的大小相同，利用相同的資料採礦方式以試圖分析出所需的資料，則利用現代的硬體技術，便能夠在相對極短的時間之內收斂到產生可用的結果，若在五六年前，則可能因為資料採礦的時間過長，而喪失了時效性。在刑事偵查中，偵查時效性是一個極為重要且需要掌握的部分，能夠即時產生分析結果的資料處理技術，才能發揮其輔助的功能。

若再輔以其他資訊處理技術，例如分散式運算系統，將資料處理之工作量，透過網路，分散給眾多電腦進行處理，再將各電腦處理所得之結果回傳給主電腦進行整合，則可以更為縮短資料處理時間。這也歸功於網路技術不斷進步，使得網路的傳輸速度亦不斷提高，同時構建網路的通道也變得多元化；以往需要透過硬體骨幹才能相互連接的網路架構，近年來已經有 3G 等無線網路骨幹可以選擇，這也大大地減少了資料處理技術的限制。舉例來說，若有需要，則犯罪事件發生時，警察可以攜帶筆記型電腦抵達現場，一旦發現有跡證可以配合資料倉儲進行進一步分析比對時，可以直接透過例如 3G 無線網路連線技術，在現場便可連線回單位內之資料庫主機，進行資料比對。隨著網路連線的頻寬增大，分散式運算的效能可以更被彰顯出來，以前述電腦處理速度的比較為例，搭配分散式運算模式，若欲將取得之資料與已建立之資料倉儲進行比對，則以往需要耗時數個

[105] 以 Intel(R) Xeon(R) CPU E5405 @ 2.00GHz(四核 run Win2003) 之運算總量對比於 AMD Athlon(tm) XP 2200+ (單核 run LINUX)之運算總量。

個月才能獲得的比對結果，現在可在一天之內便完成比對分析。

前述資訊處理技術的進步，使得運用資料庫來協助犯罪偵查在技術上逐漸變得可行。這些數位化的資訊處理技術所取得的比對結果，若能確保資料來源與保存鍊的正確度及潔淨度，則分析比對的結果也能夠具有證據能力以及適當程度的證據力，而得以搭配偵查時取得的其他實體證據，作為審理案件時的適格證物。目前一些國家的司法系統已經接受某些資料庫的分析結果，並且使用於協助司法案件進行，比較廣為人知的資料庫比對技術，有例如美國警方所採用的指紋資料庫比對技術[106]及英國警方採用的 DNA 資料庫比對[107]等技術，指紋比對通常係用以證明或者反證某人是否曾經觸碰過某物，來用以推知某人是否曾經在某現場出現，或者用來檢證其證詞是否與跡證調查結果吻合。不同的資料庫比對，尚須不同的演算法支援，方能發揮最大的效能，完成比對。前述之指紋比對舉例，當所採取之指紋或者用來作為資料庫內建資料的指紋並不完全或有破損時，則需要面臨辨識影像、殘缺指紋等等狀況[108]，此時資訊處理硬體以及處理技術的進步，便能發揮其優點，將過往不能處理或者必須廢棄的有缺陷證據，轉化為有用的證據。

前述利用資訊處理技術以協助犯罪偵查之例，係針對犯罪發生後之刑事偵查，至於於犯罪發生之前，是否得以利用科技力量，對人民之資料進行蒐集以建立資料庫，則需要考慮隱私權與公共利益之衡量。有前例者，美國最高法院之判決文曾指出只有存在更優越的公共利益考量時，才允許限制資訊自決權。且此限制必須有合乎憲法的法律基礎，而這個法律基礎必須符合所謂規範明確性之法治國家的要求[109]。類似地，歐盟為了保護自然人的基本權利及自由，特別是指個人

[106] 參見美國邁阿密達德分局關於犯罪現場鑑識部門之工作簡介網頁 http://www.miamidade.gov/mdpd/BureausDivisions/bureau_CrimeSceneInvestigations.asp，最後瀏覽日期：2009/07/27

[107] 參見英國國家 DNA 資料庫網頁 http://www.homeoffice.gov.uk/science-research/using-science/dna-database/，最後瀏覽日期：2009/07/27

[108] 參見「NEC 現場指紋比對技術於 NIST 評比測試獨占鰲頭」 http://ct.acnnewswire.com/article.asp?art_id=1374&lang=CT，最後瀏覽日期：2009/07/27

[109] （判決譯文詳見司法院秘書處。1990）

資訊經編輯所涉及的隱私權保護，以及不使歐盟國家對於此類資訊於歐盟內的流通做出限制，歐盟亦訂定了歐盟個人資料處理及自由流通保護指令（E.U. Directive 95/46 EC）。

犯罪預測的概念[110]，典型者例如 Ernest Watson Burgess 等人針對假釋犯人之假釋後行為研究[111]。此研究完成於 1928 年，針對伊利諾州約三千名假釋犯進行研究，其研究方式為，在已知的違反假釋行為平均率條件下，針對不同特殊背景的假釋犯表現出的違反假釋行為比率進行比對。例如「之前未具有工作經驗之假釋犯」違反假釋行為比率、「具有打工工作經驗之假釋犯」違反假釋行為比率、「具有正常工作經驗之假釋犯」違反假釋行為比率等等。當某個特殊背景之假釋犯違反假釋行為比率低於平均率時，這個特殊背景就會被歸類為「正向的」或者是「好的」特殊背景因子。這個研究方法希望透過對實際資料的統計分析，製作出一個評量量表，藉此來預測假釋犯假釋後的可能再犯情況，作為日後進行假釋評量的參考。在這個評量量表中，總共歸納出 21 個正向特殊背景因子，而日後依此評量量表來觀察假釋犯，發現在符合超過 16 個正向特殊背景因子的假釋犯人數中，約有 98.5%的高比率並未違反假釋條例，即表現良好；而在符合 2-4 個正向特殊背景因子的假釋犯人數中，僅有 24%的比率表現良好[112]。換言之，這類的研究指出，若能夠將行為量表化，則符合越高比例「良好行為」者，發生反社會行為的比例即會降低。

關於犯罪預測的研究指出，按照預測的對象，可以區分為犯罪宏觀預測以及犯罪微觀預測，前者針對一特定時空範圍內的整體犯罪現象進行預測，例如預測城市的犯罪率消長，以便能制訂出因應的對策；後者針對特定的個體，在未來期

[110] 關於犯罪行爲預測之資料內容，係訪談現職社工人員，加上文獻整理而得。

111 Andrew A. Bruce, Albert J. Harno, John Landesco, and Ernest W. Burgess, The Workings of the Indeterminate Sentence Law and the Parole System in Illinois (Springfield,Ill. Parole Board, 1928)

[112] *See* Peter. P. Lejins, Parole Prediction: An Introductory Statement, Crime Delinquenccy, 8, 209 (1962)

間之內產生反社會行為的可能性進行預測，以使相關單位能夠採取必要的措施。另外也有針對預測時間的長短，區分為短期、中期、長期的犯罪預測。這些犯罪預測都是希望能夠在犯罪發生之前，能夠盡量減低犯罪發生的可能性，畢竟，犯罪發生之後，被害人所受到的傷害是無法彌補的，無論生理或者心理方面，而犯罪發生後的訴追，也僅能以逮捕犯人並透過司法程序將其定罪為目的而已。

惟隨著時代演進，多元化的社會造就了人的許多面向，同時人與人之間的互動也日趨頻繁。依照行為特徵進行資料蒐集，能夠獲得的資料量相當龐大，因此，要如何分析這些資料便成為一個難題。所幸資訊工程亦是日漸進步，藉由資訊工程的介入，分析資料便開始成為可能的目標，政府單位也才有建立龐大資料庫的可能性。最典型的資料庫即如同指紋、DNA 等資料，結合曾經被定罪的犯罪者或者嫌犯之個人資料後，便可成為一個簡單的保安資料庫。如此，當發現某些曾經被定罪或者涉嫌犯罪者出現於某些區域，或者某些案件中時，相關單位即能夠特別注意這些人的動態或者行為。例如印度當局，其國家犯罪存錄局（National Crime Record Bureau）即儲存有國家級的犯罪資料庫，並且透過犯罪資料採礦技術來分析犯罪資料庫，藉此協助相關單位人員進行執法行為或者犯罪偵防。由於犯罪資料數量實在相當龐大，因此存錄與分析這些犯罪資料無法藉由人工執行來完成，必需要藉由資訊工程技術做為媒介方能完成。印度當局發展出一套國家級的犯罪罪犯資訊系統，此系統的設計目的就是用來存錄、分析、以及呈現犯罪罪犯的個人記錄，同時此系統還支援多語以及線上使用之功能，以便印度境內的各執法單位均能夠即時地存取此系統之資料。其針對印度境內較常發生之犯罪，設計為實現下列目的：1.連結犯罪案件與罪犯及財物、2.連結一罪犯到與其相關之案件、3.連接一財物到與其相關之案件、4.連結無法確認之死亡者、被綁架者、失蹤人口之資料、5.將遭竊財物返還給原物主等等。

此犯罪資訊系統之介面如下圖所示

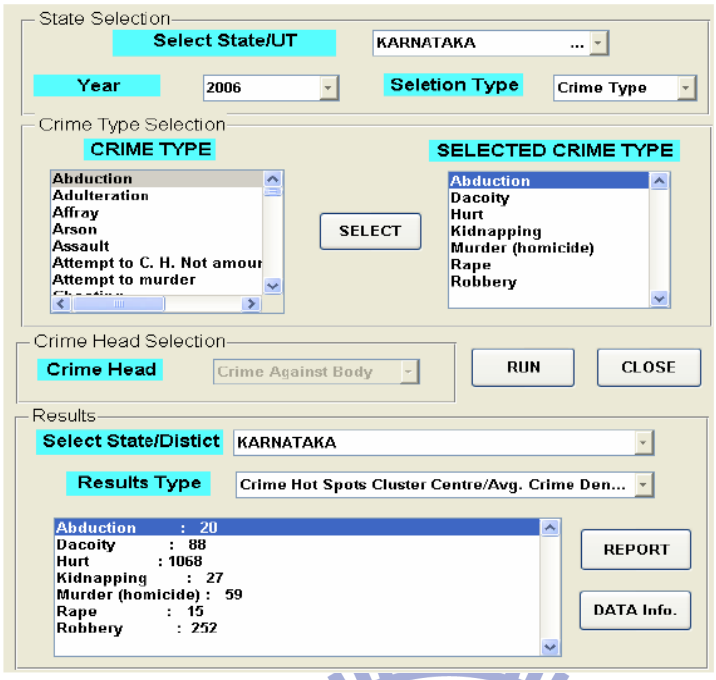

圖 1：印度國家犯罪存錄局之犯罪資訊系統介面

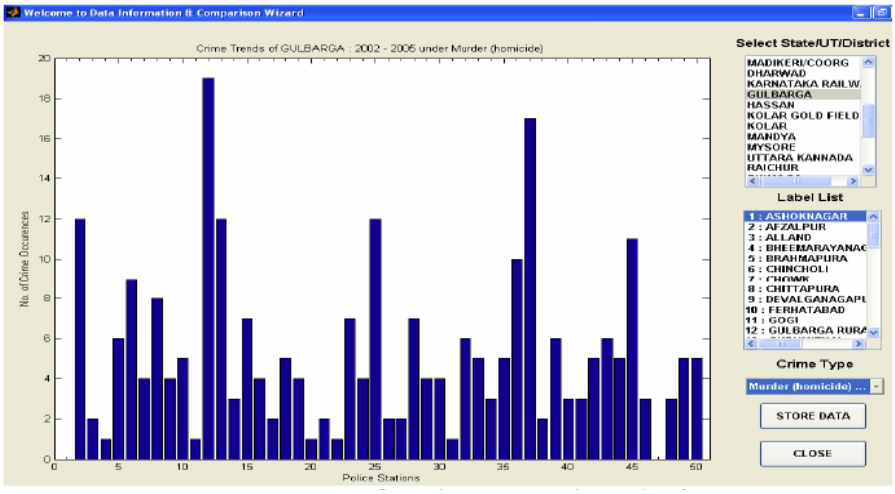

圖 2：印度國家犯罪存錄局之犯罪資訊系統查詢結果示意圖

印度當局評量使用該系統之後，認為警方更能掌握即時以及相關性高之資料，以進一步協助警方執行日常勤務[113]。印度警方在使用此一系統後，認為此一系統之主要功能具有以下四點：1.偵測犯罪發生地點以及分析產生犯罪熱點資訊、2.分析後提供預防犯罪以及降低犯罪之策略、3.藉由分析犯罪模式，降低同

[113] *See* Manish Gupta, B. Chandra and M. P. Gupta, Crime Data Mining for Indian Police Information System.

類型犯罪的發生率、以及 4.藉由分析結果，有效率地聚焦預防策略以及偵查策略。而這都是過往依靠人力分析或者個人辦案經驗累積所較難以達成的效果。

此類分析系統之中央主機一般具有適應性，亦即可以透過不斷地由各處單位所回報的資料來自我分析並且成長，如此，當之後需要針對資料進行分析時，便可更迅速地產生分析結果。犯罪分析工具可概分為具有三種模組：資料粹取模組、犯罪分析模組、以及資料比較模組。

資料粹取模組主要是用來於資料蒐集階段，當區域使用者欲從中央系統搜尋資料時，可以由中央系統將資料下載到區域主機內，將所需的資料依照資料倉儲的分類方式分門別類標示標籤並予以收藏，若中央系統的資料更新，則區域主機亦可透過定時更新方式，擷取更新的資料；而後當區域使用者欲進行搜尋時，便可直接在區域主機上進行。印度警方目前所採取的這種作法可以減低中央系統的運算負荷，若引進分散式運算系統，在網路品質穩定的狀況下，可將網路內所連結到的所有主機都作為運算硬體，資料庫則儲放於中央系統，當需要分析時，提出需求之區域主機輸入搜尋需求，而後位於連線網路上之各主機分別貢獻部分運算負載量，至中央系統讀取資料，並完成整個運算，最後將運算結果透過網路回報給提出需求之主機，呈現分析結果。

犯罪分析模組係設計用來標示出犯罪熱點、犯罪型態、以及可能發生犯罪事件的特定區域。印度當局目前將國內之犯罪型態區分為 105 種型態[114]，使用者若欲參考過往的歷史資料，可以選定任一年份（或任一時間區間）、任一區域，而後再選擇犯罪的態樣，便可選定之後進行分析的資料庫態樣，亦可針對特定的文本內容，進行資料分析。這種介面設計，係與資料採礦/文本採礦之特性相符，要求使用者在進行資料分析之前，便先針對所需要的搜尋目標，進行分類。優點在於能夠更快速的產生分析結果，但缺點在於橫跨不同分類資料庫的分析可能會具有實現上的困難。畢竟，若使用者於分析之前便先將所需的搜尋目標限縮至某

[114] *Id*. at 394

一範圍後，則自然限制了在其他資料庫的搜尋可能性，而較容易忽略了不同犯罪分類之間所可能具有的關聯性。

資料比較模組則是用以呈現選定的區域、時間範圍、犯罪型態三者之間的分佈關係，給定其中一個因素之後，便可以得知另外兩個因素的相對應變化。例如選定一特定的地區，便可以產生依照年份不同，犯罪型態的消長狀況。這對於預測犯罪情況或者警力調配，具有一定程度的參考價值。

我國對於個人隱私及公共利益維護之權衡，雖憲法未有明文規定，但歷年司法院大法官之解釋亦常觸及此類議題。根據過往司法院大法官所做成之解釋文，我國已承認隱私權為憲法所保障的一種基本權利，並需兼顧對於個人名譽、隱私、及公共利益之保護。 因此，當衡量行政作為是否能夠對個人隱私權進行適度干預的時候，亦必須謹慎考量該行政作為所可能產生的種種後果，以預先進行防範。

另外，在一些我國的實體法中，亦已經針對類似狀況提出概括式的條文。例如在我國電腦處理個人資料保護法(民國 99 年 6 月已修法並更名為個人資料保護法，以將保護範圍自限於電腦處理之個人資料中釋放出來)中，即有定義個人資料為指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料[115]。同時在同法第 11 條第 3 款規定關於犯罪預防、刑事偵查、執行、矯正或保護處分或更生保護事務者，得不適用前條規定。我們從該法之法規規定中，已可見到我國開始導入以電腦處理之個人資料庫來作為輔助「犯罪預防」以及「刑事偵查」之手段，相對於目前刑事訴訟法中對於追訴犯罪時方能發動之強制處分而言，似乎更具有著重於預防之效果，同時亦能協助追訴犯罪時之偵查工作進行。

惟，此等條文之涵攝範圍自不可能無限上綱地擴展至所有以達成前述「犯罪

[115] 電腦處理個人資料保護法第 3 條。

預防、刑事偵查、執行、矯正或保護處分或更生保護事務者」之目的所為之電腦處理個人資料手段，皆能先取得免責之地位。

（三）、國家取得個人隱私資料對於犯罪訴追之助益

依照一般人的社會活動習慣，通常個人會丟棄於垃圾中的物件，可以視為是個人認為與自身所關心之隱私相關度較低，或者對於其生活而言價值較低或無價值之物品。除了誤將應該保存的資料丟棄於垃圾中的狀況以外，若某物件或者文件上所攜帶的資料或物品價值對於個人而言屬於重要的，那麼依照一般的生活習慣，個人應當會採取適當的保護或保存措施來安置這些物件或者文件，而經過其檢視判斷為應當丟棄者，即屬於相對中性（即個人判斷為與隱私內容無關）或者相對低價值的資料，例如銀行的優惠通知或對帳單、個人參加社團的會員記錄、壞掉的物品等等。這些看似中性的資料，經過長時間的累積之後，仍可能判斷出個人的生活習慣。舉例而言，例如某人總是會收到金融機構的對帳單，則至少可判斷某人係經常從事金融交易；例如某人總是會收到中華電信的電話費帳單，則至少可判斷該帳單所登記之住所經常有人居住，才會有人使用電話。凡此種種，即便是個人僅丟棄資料的信封或者部分內容，皆有可能在足夠的資料累積之後，透過資料採礦的分析處理，獲得某些私人資訊。

若國家希望於平時便能有限度地蒐集人民的個人資料，則這些國民個人判斷為中性或者價值低的資料，在類同於美國的隱私權測試方式檢證下，應可推論為國民相對不具有或具有較低之隱私期待性。如果是國民自願拋棄的資料，那麼當國家認為針對例如犯罪偵查等重大的社會公益有利時，希望進行資料庫的建立，那麼國家應可以在配套的蒐集程序與保存系統完善後，廣泛的蒐集此類中性的資料。惟其保存需要完善，並且以積極方式避免此類資料庫被洩漏出去，遭到其他人之濫用。

另一方面，在國家蒐集資料的過程中，其實對國民的影響並不巨大，因為在

資料倉儲中的資料，僅是依照不同的屬性以及時間差異，被分門別類存放著。當這些資料因應特定的目的或者案件，被國家處理分析時，才真正會對國民的隱私造成干擾與侵害。因此對於在何種目的之下，該進行多高密度以及多廣深度的資料採礦之程序判斷，是需要非常精細的設計，且需要與時俱進的檢討改善。而處理分析後所產生的結果，由於與國民之私人資訊具有相當強的連結關係，因此也必需要嚴格規範存取分析結果之過程與授權，同時亦需要如同資料倉儲的資料存入般，對於分析結果的存取亦僅能允許讀取而不允許更改，且存取的時間與次數等料也需要被逐一紀錄下來。如此，透過對使用資料庫的目的正當性與申請審查進行嚴格的限制，方能保護國民的資料不被濫用。

我國刑事訴訟法對於科學證據的適用與否並沒有特別的規定，甚至我國對於證物的保存程序亦沒有明確的規定。雖然如此，關於科學證據於司法系統中適用的證據能力，仍有一些相關規定可供參考。例如鑑定制度，我國目前現行規定鑑定人由司法機關選任，當事人並得申請迴避，以維持鑑定人之中立客觀屬性（刑事訴訟法第 200 條）。刑事訴訟法第 203 至第 205 條以下分別條列國家賦予鑑定人之權能，其中關於物之鑑定部分，有例如 1.受命法官或檢察官於必要時，得使鑑定人於法院外為鑑定，並將關於鑑定之物，交付鑑定人（第 203 條第 1、2 項），2.鑑定人因鑑定之必要，得經審判長、受命法官或檢察官之許可，檢閱卷宗及證物，並得請求蒐集或調取之（第 205 條第 1 項），以及 3.鑑定人因鑑定之必要，得經審判長、受命法官或檢察官之許可，採取分泌物、排泄物、血液、毛髮、或其他出自或附著身體之物，並得採取指紋、腳印、聲調、筆跡、照相或其他相類之行為（第 205 條之 1 第 1 項）。雖然上述所列之程序，均在刑事訴訟程序發生之後，即案件調查或者已經起訴且進入審理階段，方能為之，即，鑑定人或者鑑定單位需在前述階段之後，方能發揮其科學證據鑑定之能力；於案件進入調查或者審理階段之前，目前我國並無相關程序規定，使得鑑定單位或者鑑定人得針對特定或者不特定對象，進一步主動採取相關證物。

然，前述規定至少指出，我國法院在調查或審理案件時，得以使得透過科學證據方法鑑定之物證，進入法院，成為輔佐審理案件之證物，在我國，鑑定人之角色並非證人，而是檢察官或者法院的輔佐者，一般而言，鑑定人之專業意見遠超過法院及兩造雙方之知識範圍，故，若案件之爭議重點繫屬於應受鑑定之物，則鑑定人之鑑定意見，往往成為案件的判決關鍵。

在美國，並非如同我國一般區分為證人以及鑑定人，而是將證人區分為一般證人以及專家證人。專家證人所提出之意見，仍然被視為是證人之意見，由法官或者陪審團決定專家證人證詞之接受度。在美國，科學證據採納之判斷標準，先有佛萊法則(Frye Rule)[116]之適用，後有道伯測試法則(Daubert Test)[117]之修正。前者法院判斷認為科學證據必須是被該領域之專門知識者所普遍接受(general acceptance)者，才得以具有容許性(admissibility)，而能被法院接受。但在 Daubert 案中，法院認為佛萊法則過於死板，若以此作為科學證據採納之唯一標準，則過於嚴苛，因此修正為科學證據若符合相關性(relevant)以及可信賴性(reliable)，即可具有容許性，被法院接受。值得注意者，聯邦最高法院在 Daubert 案中，亦同時指出，科學知識(scientific knowledge)、技術知識(technical knowledge)、與其他特別知識(other specialized knowledge)有所不同，只有以科學方法與程序為基礎之知識才適用於該法則[118]。在此案中，由於牽涉到藥物對於孕婦之影響，故前述三種知識之區分尚非難解，但在其他案件中，有時候科學知識以及技術知識之區隔，並非如此容易。總之，聯邦最高法院意見的重點在於，科學知識具有真實性，並且不會隨著時間經過以及不同操作者進行操作而有所改變，因此透過科學方法與程序為基礎所獲得之知識，應使其具有被法院採納之地位。

我國偵查案件時使用資料庫現況可概分為警察機關以及檢察機關。其中警察機關若需請非公務機關提供與個人相關之各項資料者，例如網路服務提供者、銀

[116] Frye v. United States, 293 F. 1013 (D.C. Cir, 1923).
[117] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
[118] *Id* at 588-590

行、醫療院所等之客戶資料，多半是利用公文函、電子郵件或電詢請業者提供資料。雖然這類的作法並沒有明確的法規可以依循，不過一般而言，非公務機關在接獲警察機關的詢請文函時，均會配合警察機關的請求，提供個人資料。而在檢察機關方面，針對非公務機關之作法，也類似於警察機關，多以公文函請業者提供資訊。

而針對檢察機關，法務部有建立各類之資料庫，供檢察官辦案時查詢所用。若辦案時有所需要，則檢察官可以直接使用配給之電腦，以個人之身分及密碼開啟查詢介面後，輸入偵辦之案號，便可以查詢一些與犯罪相關的個人資料，例如戶籍、前科等等，至於各式資料的閱覽權限，則依照法務部對內頒佈之命令進行分級，獲得不同授權者，可以進行不同程度的閱覽。而法務部亦有統一與非公務機關之資料庫，簽訂合作契約，使檢察官能夠直接由地檢署連接該等資料庫，進行查詢。而針對某些法務部認定較為私密之個人檔案，則僅授權地檢署特定人能查詢，例如電信業者之通聯記錄、國稅局之財稅資料等，此類資料並非所有的檢察官，甚至是案件承辦檢察官，能夠直接查詢閱覽其內容。法務部的現行作法，具有資料庫分級使用之概念，但實際作法上較接近以內部命令直接規範不同使用者的使用權限[119]。

（四）、我國關於處理個人隱私資料之規定

然而，在案件進入調查程序或者審理程序之前呢？是否科學證據或者鑑定意見，能夠成為輔助案件立案前調查，或者進一步發生協助防範犯罪之效果？以本文所要討論之標的，藉由對人民之日常拋棄資料，進行蒐集，並進一步製作成可用於資料採礦及文本採礦之資料倉儲而言，有個人資料保護法，以及通訊保障及監察法之規定可參。

1. 個人資料保護法

[119] 本段資料內容係訪談現職檢察官整理而得。

我國為保障電腦處理個人資料，於民國 84 年制訂公布有「電腦處理個人資料保護法」[120]，並於民國 99 年 6 月修正為「個人資料保護法」(下稱個資法)，原意用於保護經過電腦處理之個人資料，惟有鑑於資訊科技發展日新月異，近年來行政院多有提出修法之提案，以將所及範圍擴大為「個人資料處理」，而非僅限於「電腦處理」。2008 年提出之修正草案[121]及修正後法規，亦將規範的主體由公務機關與「列舉之非公務機關」[122]，擴大為公務機關與「經明文排除之非公務機關」[123]。相較於美國憲法第四修正案所規範對象為公務機關不得任意侵犯人民之隱私權內容，非公務機關則不在規範範圍；個資法為周全對於個人資料之保護，所規範對象除公務機關外，更包含非公務機關，無論是現行法的「列舉之非公務機關」，或者是修正草案的「經明文排除之非公務機關」。顯見，在隱私權內容中，關於個人資料部分，我國法的規範主體較為寬廣。事實上，現今各種資料幾乎都需經由電腦處理後，方能達到資料傳遞、資料解讀、資料分析、粹取內容等等目的，因此，無論是現行的個資法，或者正在進行中的個資法修正草案，其影響範圍已可謂廣泛。

雖個資法開宗明義於第 1 條指出，個資法設立目的之一係避免人格權受到侵害，惟進一步理解個資法之規定內容後，可發現其相當程度地著重於人格權中之個人隱私權以及個人隱私內容之蒐集與利用之保護。參照相關司法院大法官釋字之內容，例如釋字第 585 號以及釋字第 603 號，均認為隱私權

120 「電腦處理個人資料保護法」，民國 84 年 08 月 11 日公布，http://law.moj.gov.tw/Scripts/Query4B.asp?FullDoc=%A9%D2%A6%B3%B1%F8%A4%E5&Lcode=I0050021。

121 「電腦處理個人資料保護法修正草案條文對照表」，www.moj.gov.tw/public/Attachment/622285243 21.pdf，最後瀏覽日期 98 年 12 月 10 日。

122 個資法第 2 條第 7 款：「非公務機關：指前款以外之左列事業、團體或個人：(一) 徵信業及以蒐集或電腦處理個人資料爲主要業務之團體或個人。(二) 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。(三) **其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。**」

123 個資法修正草案第 2 條第 8 款：「非公務機關：指前款以外之自然人、法人或其他團體。」；第 7 款「公務機關：指依法行使公權力之中央或地方機關或行政法人。」。

屬於人格權之個人資訊之自主控制權，同時隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障。因此，個資法之立法意旨，可理解為係針對隱私權中之個人資訊之蒐集及利用之規範，至於因隱私權之蒐集與利用所生之其他關於人格權之爭端，並不在個資法主要探討的範圍。

個資法第 3 條係一用詞定義規定，其中第 1 款即定義個資法之客體-「個人資料」-為「個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。」；修正後第 2 條第 1 款，更增列「護照號碼、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式，及其他得以直接或間接方式識別該個人之資料」。可見此一法條之規定核心在於「足以識別該個人之資料」，無論是文本或者非文本，直接記載或者間接可得，均是立法者在設立本款規定時，所欲納入之範圍。這個範圍可謂包山包海，除法條中例示之資料類別外，不在例示範圍內之資料類別，只要足以識別個人，亦在規範範圍之內。另外修正後法規除於第 2 條第 1 款增列「護照號碼、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式」等個人資料類別外，更於第 6 條規定「有關醫療、基因、性生活、健康檢查及犯罪前科等個人資料，除符合該條所定之要件者外，原則上不得蒐集、處理或利用。」說明了修正草案對於個人資料開始進行個人私密性高低之區別，增列於修正後法規第 6 條之個人資料類別，即是被認定為與個人私密性高度相關之個人資料，而應該加強管理。惟所謂「有關」高度個人私密性之資料，究竟係直接可呈現該種個人資料之資料，或者亦包含間接與該種個人資料相關之資料。例如個人之性生活相關資料，若係由與當事人曾經發生過親密關係之人，或者聽聞此類傳言之第三人所口述呈現，是否亦得成為受規範之對象？此類之口述

內容，以刑事訴訟法之相關規定[124]，若符合傳聞證據之排除法則，且未符合例外原則，即不可成為具有證據力之證據。對於在個人資料蒐集與利用方面，是否可適用類似刑事訴訟法關於傳聞證據之規定，容有進一步討論之空間。

個資法第 3 款定義「電腦處理」為「電腦處理：指使用電腦或自動化機器為資料之**輸入、儲存**、編輯、**更正**、**檢索**、刪除、輸出、傳遞或其他處理。」其中輸入、儲存、更正、檢索即可謂已經包含資料採礦/文本採礦之核心技術特徵，而資料採礦/文本採礦之時間性特徵雖然並未包含在法條中，亦可透過對輸入、儲存資料之進一步解釋，納入法條涵攝範圍，畢竟當資料輸入時，便可隨之輸入資料產生時間及/或輸入時間。修正後法規第 2 條第 1 款，更增列「複製以及連結或內部傳送」之處理行為，作為一補充規定，大致上將電腦或機器能夠對資料發生的處理方式都包含在內了。

另外，在修正說明中，亦有指出「由於蒐集個人資料之行為態樣繁多，有直接向當事人蒐集者；有間接從第三人取得者，為落實保護個人資料隱私權益，爰參考德國聯邦個人資料保護法第三條規定，修正第四款「蒐集」之定義。」，代表立法者設立個資法所欲規範之行為，係包含各種蒐集個人資料之行為態樣，並非僅特定限於條列或者明示之蒐集行為。

個資法之修正草案亦加強了行政監督的責任，課與主管機關更強的主動監督責任。在修正後法規第 22 條[125]增列「中央目的事業主管機關」或「地

[124] 我國刑事訴訟法(民國 98 年 07 月 08 日 修正)地 159 條第 1 項規定：「被告以外之人，於審判外之言詞或書面陳述，除法律有規定者外，不得做爲證據。」爲傳聞證據之排除法則。

[125] 個資法修正後第 22 條規定：中央目的事業主管機關或直轄市、縣（市）政府爲執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員爲必要之說明、配合措施或提供相關證明資料。
中央目的事業主管機關或直轄市、縣(市)政府爲前項檢查時，對於得沒入或可爲證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制爲之。
中央目的事業主管機關或直轄市、縣(市)政府爲第一項檢查時，得率同資訊、電信或法律等專業

方政府」發現非公務機關違反本法規定或認有必要時，得進入檢查，認為有問題之資料，並得扣留或者複製，必要時得施以強制措施，且規定參與檢查之人員負有保密義務等。顯示了個資法之修正草案，亦認同主管機關應該賦予積極行政之義務，以強化對於個人資料之保護；此立法意旨，與歐洲人權法院之相關判決意旨，認為主管機關應當發揮積極行政之作為的見解，可謂不謀而合。

個資法對於個人已經公開之資料應當如何處理，並沒有明確的規定，僅在第 18 條第 3 款規定「非公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得為之：...三、已公開之資料且無害於當事人之重大利益者。...」。但在修正草案中，這樣的情形有了明顯的改變，在修正草案中，針對已公開之個人資料被蒐集之相關情況，有了較為詳細的規定，例如修正草案第 6 條「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：...四、當事人自行公開或其他已合法公開之個人資料。...」，修正理由稱：「當事人已自行公開或其他合法公開之個人資料，隱私已無被侵害之餘...」因此立法者似認為對於此種**自行公開之個人資料之蒐集與利用，即無進一步限制之必要**。惟，與當事人自行公開之資料直接相關之隱私內容，固然因為當事人自行公開而無法再主張合理的隱私期待性，但此種自行公開之資料，在結合其他資料後，可能拼湊出當事人之其他隱私內容，此一部份即可能為當事人所不欲公開之內容，例如同一類型之資料，經過經年累月之累積蒐集後，若加以分析，可能可以推斷出當事人之某些行為「習性」，而此類的行為習性，當然亦屬於當事人之個人隱私部分，且極有可能是其不願意公開之內容。此種狀況猶如進行心理測驗時，當事人對於每個問題的回覆看似都不會

人員共同爲之。
對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。
參與檢查之人員，因檢查而知悉他人資料者，負保密義務。

透露出太多個人資料，但是將當事人對整份心理測驗之所有提問之內容綜合分析之後，即可能判斷出當事人之某些特定心理狀態與習性。可見資料與資料之間，若能透過某些模型的運算處理，是可能推導出進一步的個人隱私資料，尤其是關於個人較為私密的心理狀態部分。因此，對於個人資料之自行公開，或許需要進一步界定自行公開之意義，或者是否僅得於當事人自行公開之範圍內，對公開之資料進行較少限制之利用；而相同的公開資料，在當事人自行公開的範圍之外，若要進行利用，則需要進一步的限制，以免過度侵害當事人之隱私權利。換言之，本文認為，參酌歐洲人權法院對於使用個人資料時，應注意其使用目的之合理性之判決意旨，建議我國公務或非公務機關，於使用合法蒐集所得之個人資料時，除確認個人資料之蒐集過程係符合相關規定以外，於使用這些個人資料時，無論是否為當事人自行公開的，均應注意使用結果對於當事人之影響，較不宜直接認定當事人自行公開之個人資料之蒐集與利用，無進一步限制之必要。例如當事人自行公開之私人照片，日後被用以評價其公開領域行為之正當性，雖看似符合修正草案之要旨，但參酌歐洲人權法院之意見，同時考量對於當事人可能產生之影響，或許未來修正草案仍有再審議之必要，而不應遽以認定如此之利用係完全地正當。

另外，個資法修正內容亦加重了違法責任，包含行政、民事、刑事責任。其中修正草案第 28 條第 4 項[126]將損害賠償總額由個資法之新台幣二千萬元提高至新台幣五千萬元，而在修正後更將草案的五千萬元額度拉高到二億元，在例外狀況還可能超過此限額；修正後第 41 條[127]以行為人是否具有「意

[126] 個資法修正草案第 28 條第 4 項：「基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣五千萬元爲限。但因該原因事實所涉利益超過新臺幣五千萬元者，以該所涉利益爲限。」

[127] 個資法修正草案第 40 條：「違反第六條、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。

意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」

圖營利」之主觀要件，來區分刑事責任，若為意圖營利之行為，則刑事責任將加重至「處以五年以下有期徒刑，得併科新台幣一百萬元以下罰金」；修正後第 50 條新增對於非公務機關之代表人、管理人或其他有代表權人之自然人之處罰，規定「非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條[128]規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受**同一額度罰鍰之處罰**。」凡此種種日趨嚴苛之違法責任訂定，均能夠顯示立法當局對於維護個人資訊隱私權之重視。

若說個資法還遺漏了部分應該規定而未規定的，或許可說是蒐集資料時，蒐集之資料並未具有個人資料之特徵，或者蒐集者並非是為了蒐集個人資料為目的，但在後續處理時，這些資料卻轉化為能夠相當程度地揭露或者分析出個人特徵資料的，或者產生得以識別個人之效果的；關於此類資料的蒐集或者運用是否亦為得適用個資法之規範對象，便具有進一步討論的價值。同時，個資法均無規定專責主管機關，以統一管轄蒐集與利用個人資料之公務機關與非公務機關，若政府單位欲更有效能地採取積極行政之作為，來保護個人資料的蒐集與利用，則設置專責之獨立行政機關[129]，負責監督公務機關與非公務機關，並且能夠適時地提出行政指導或者行政處分，若欲有機關不服處分時，同時作為訴願之審查機關，將是一可以考慮之作法。藉由設立專責機關，可以集中處理此類爭議狀況，並藉由處理經驗之累積，對立法技術提出進一步的實際建議，以更周全我國對於個人資料之保護。

---

[128] 個資法修正後第 47 條前項：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之…」
個資法修正後第 48 條前項：「非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣(市)政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰…」
個資法修正後第 49 條：「非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣二萬元以上二十萬元以下罰鍰。」

[129] 參見湯德宗，〈電腦處理個人資料保護法 2008 修正草案評釋〉，台灣法學會 2008 年年度法學會議，臺灣法學會，s2008 年 12 月。

2. 通訊保障及監察法

在現今社會中，人與人間之通訊日趨頻繁，且管道從過往的書信、電話、電報，擴展到電子郵件、個人部落格、影音電話、無線通訊等等多元管道。憲法第 12 條明訂人民有秘密通訊之自由，即，一般狀況下，人民之秘密通訊自由應受到保障，不可被破壞；惟，為維護社會秩序以及確保國家安全，有時特定的公務機關得對人民之秘密通訊進行監察。為使個人與公益間之權利競爭能夠調和，我國制訂有通訊保障及監察法（以下稱通訊監察法），並經過歷次修正[130]，以配合社會演進，並符合人民對於法規適當性的期待。

雖然通訊監察法係規範需經過事前審查之通訊監察行為，然其對於監察所得之資料，特別是郵件及書信資料，之保存保密以及相關罰則，是值得借用至本文所要討論之資料倉儲制度建立時參考。

通訊監察法中關於取得資料之保存方法，規定於第 16 條，按照規定，執行者必須至少按月向檢察官、核發通訊監察書之法官、或國家情報首長報告執行情形，另一方面，前述人員亦得隨時命執行者提出報告。進一步言，並有規定同法第 5-6 條[131]之通訊監察之監督，偵查中由檢查機關、審判中由

---

[130] 通訊保障及監察法之沿革，http://zh.wikisource.org/wiki/%E9%80%9A%E8%A8%8A%E4%BF%9D%E9%9A%9C%E5%8F%8A%E7%9B%A3%E5%AF%9F%E6%B3%95，最後瀏覽日期：98 年 12 月 20 日。

[131] 通訊保障及監察法(民國 96 年 07 月 11 日 修正)第 5 條：「有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書。……前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權以書面記載第十一條之事項，並敘明理由、檢附相關文件，聲請該管法院核發；檢察官受理申請案件，應於二小時內核復。如案情複雜，得經檢察長同意延長二小時。法院於接獲檢察官核轉受理申請案件，應於二十四小時內核復。審判中由法官依職權核發。法官並得於通訊監察書上對執行人員為適當之指示。
前項之聲請經法院駁回者，不得聲明不服。
執行機關應於執行監聽期間，至少作成一次以上之報告書，說明監聽行為之進行情形，以及有無繼續執行監聽之需要。法官依據經驗法則、論理法則自由心證判斷後，發現有不應繼續執行監聽之情狀時，應撤銷原核發之通訊監察書。
違反本條規定進行監聽行為情節重大者，所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均**不得採為證據**。」
第 6 條：「有事實足認被告或犯罪嫌疑人有犯刑法妨害投票罪章、公職人員選舉罷免法、總統副總統選舉罷免法、槍砲彈藥刀械管制條例第七條、第八條、毒品危害防制條例第四條、擄人勒贖罪或以投置炸彈、爆裂物或投放毒物方法犯恐嚇取財罪、組織犯罪條例第三條、洗錢防制法第十

法院進行監督；第 7 條係關於蒐集外國情報必要者之通訊監察之監督，由國家情報機關進行監督。所有偵查中之案件，法院均得隨時派員監督機關執行情形。值得注意的事，若違反了前述法規中規範之監督情況，或違反了前述法規中定義之監聽行為，而情節重大者，所取得或衍生之證據，在所有的法定程序中，均不得採為證據，沒有例外的規定。這代表通訊監察法在此對於維持正當法律程序之要求相對為高，若有重大的違反情況，即會導致所有的相關監察行為成果均付諸無效，也凸顯了司法系統對於個人隱私權的重視，在透過公務機關力量干預個人隱私權時，採取了極為小心的立場。

至於通訊監察所得之資料，即具有嚴格保存之必要性，通訊監察法中，關於此類資料之保存與不同單位間利用之規定，亦可作為我國未來發展與犯罪相關之資料倉儲制度時之參考。通訊監察法第 17 條規定監察通訊所得之資料，應該嚴加封緘以及保存，不得增、刪、變更，此點與建置資料倉儲時的資料輸入要求相同，顯見保存資料之初始不變性，是對資料保存的一個基本要求，在建立資料倉儲時固然如此，在建立證據時亦然。而同條進一步規定資料保存五年後，予以銷毀。訂定一個保存期限，是為了避免受監察之當事人之資料，在案件的時效性經過之後，有流出之風險；由於適用通訊監察法之對象，係已有可能涉入案件者，因此保存期限之訂定有其必要性，且保存期限也不能過長，以免喪失訂定期限之風險管控意義。另一方面，在資料倉儲中，亦可考慮訂定一資料保存期限，惟考量到資料倉儲建立之意義並非針對特定案件或者特定對象，其期限可以延長，以確保後續分析時具有足夠

一條第一項、第二項、第三項、刑法第二百二十二條、第二百二十六條、第二百七十一條、第三百二十五條、第三百二十六條、第三百二十八條、第三百三十條、第三百三十二條及第三百三十九條，爲防止他人生命、身體、財產之急迫危險，司法警察機關得報請該管檢察官以口頭通知執行機關先予執行通訊監察。但檢察官應告知執行機關第十一條所定之事項，並於二十四小時內陳報該管法院補發通訊監察書；檢察機關爲受理緊急監察案件，應指定專責主任檢察官或檢察官作爲緊急聯繫窗口，以利掌握偵辦時效。

法院應設置專責窗口受理前項聲請，並應於四十八小時內補發通訊監察書；未於四十八小時內補發者，應即停止監察。

違反本條規定進行監聽行爲情節重大者，所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，**均不得採爲證據**。」

之資料量。

同法第 18 條規定除非法定之單位，否則通訊監察所得之資料不得提供給其他之機構。此處所適用之法律原則，乃絕對法律保留原則；由於通訊監察所得之資料，乃受到憲法明文保障之個人權利內容，因此對於通訊監察所得之資料之後續利用，自應受到較高密度之規範，故適用絕對法律保留原則[132]，將判斷得以利用通訊監察所得資料之機構之責任，交由立法機關訂定之。相對於相對法律保留，可交由有法律明確依據之行政命令加以規範之等級，其對象包含關係生命、身體以外之其他自由權利的限制等等，以及非屬法律保留範圍，屬於執行法律之細節性規定等等。顯見通訊監察法認為關於個人隱私權內容之保留層次，應適用絕對法律保留，必須由法律自行規定，代表隱私權內容已與剝奪人民生命或限制人民身體自由之事項具有等同之重要地位，非透過立法之規定，不得輕易地授權其他單位具有存取通訊監察所得之個人資料之權限。透過絕對法律保留所規範之事項，雖然立法機制較為繁瑣，且無法具有相對的時效性，但如此舉措，能夠藉由較縝密之立法機制，詳細並費時地推敲討論後，規範出能夠利用該等個人資料之單位，其具有不易變動之可信賴性（需藉由一定之修法/立法程序，方能變更法規內容），亦免除社會對於個人資料可能遭到過度使用之疑慮產生，對於彰顯隱私權受到重視之立場而言，具有正面價值。

通訊監察法亦如同個資法，對於違反法規規定而洩漏監察他人通訊所得之資料者，規定負有損害賠償責任，同時若名譽被侵害，亦得請求回復名譽之適當處分，此可參考刑法中關於妨害名譽罪之相關規定以及回復名譽之施行方式。除了能依照通訊監察之日數以及每日新台幣一千元以上五千元以下之基礎計算賠償額度以外，若被監察之人能夠證明所受損害高於前述公式計

[132] 層級化法律保留體系，由高至低分爲憲法保留、絕對法律保留、相對法律保留以及非屬法律保留四層級，參考司法院大法官釋字第 443 號解釋文，http://www.judicial.gov.tw/CONSTITUTIONALCOURT/p03_01.asp?expno=443。

算之金額者，不在此限。同時被監察之人能併同適用民法以及國家賠償法中關於損害賠償之相關規定[133]。

相較之下，個資法之法定賠償金額範圍似乎較通訊監察法為大，另一方面，通訊監察法亦有著重於回復名譽之處分，二者均有值得借重之處。資訊採礦/文本採礦之對象，介於通訊監察之非常特定對象，以及電腦處理個人資料之眾多分類之間，其對象既非如通訊監察之對象般如此特定，且其欲設計之適用範圍是關於電腦處理個人資料中之個人公開部分之資料分類，在思考公務機關利用資料倉儲，進行資訊採礦/文本採礦所可能產生的損害賠償問題時，或許應同時兼採二者之長處。

通訊監察法亦有針對各種違法之狀況，課以相對人刑事責任。例如對於違法監察他人通訊者、對於明知為違法監察之資料而無故洩漏或者交付者/意圖營利而犯前項罪者、以及對於公務員或曾任公務員之人，或非公務員，因職務或業務知悉或持有秘密之資料，而無故洩漏或交付者，若發生前述違法之行為，均課以一定程度之刑責[134]。由於具有能夠進行通訊監察之公務機關或者非公務機關相對於其他機關而言為明確且集中，因此若前述規定之相關人員發生違法之行為，相對於其他犯罪行為，較容易被發現而訴追。

（五）、個人廢棄物資料庫應用於刑事訴訟之保全流程設計

依照前文所提及之內容，在我國社會，國民日常生活中，於公開領域活動時，

---

133 參考通訊保障及監察法第 19、20、23 條相關規定。

134 通訊保障及監察法第 24 條：「違法監察他人通訊者，處五年以下有期徒刑。執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處六月以上五年以下有期徒刑。意圖營利而犯前二項之罪者，處一年以上七年以下有期徒刑。」
第 25 條：「明知爲違法監察通訊所得之資料，而無故洩漏或交付之者，處三年以下有期徒刑。意圖營利而犯前項之罪者，處六月以上五年以下有期徒刑。」
第 26 條：「前二條違法監察通訊所得之資料，不問屬於犯人與否，均沒收之。犯人不明時，得單獨宣告沒收。」
第 27 條：「公務員或曾任公務員之人因職務知悉或持有依本法或其他法律之規定監察通訊所得應秘密之資料，而無故洩漏或交付之者，處三年以下有期徒刑。」
第 28 條：「非公務員因職務或業務知悉或持有依本法或其他法律之規定監察通訊所得應秘密之資料，而無故洩漏或交付之者，處二年以下有期徒刑、拘役或新台幣二萬元以下罰金。」

可能會產生大量已知的公開資訊，包含例如個人自願棄置的廢棄物、個人於私人機構，例如全省合計超過九千家之便利商店[135]，被保全攝影機所拍攝之影像、以及個人自願公開之相片、文件、個人資料等等。這些資料分別來看，均可能不會透露過度的個人資料，因此當事人通常亦不會認為這些資料的透露會對個人之隱私權內容產生進一步的影響。一個人對於某件事物的看待態度，可被認為是在認知、感情、行為這三項成分上，對於該人事物或觀念的一種持久取向[136]。個人態度裡，單純的評估成分是行為的主要決定因素，意即個人對於某事物的看法整體而言傾向好或者不好，這與事實不同，因為態度除了事物本身以外，還要加入評估或情緒的成分[137]。由於態度牽涉到一種持久的評估或者情緒，對於瑣碎的事物而言，便很難獲得一種確定的態度。當國民為了生活之所需，需要進行前述之日常活動時，例如進入便利商店購買午餐，即便見到保全攝影機時可能會稍有遲疑，但由於對生活便利性的渴求大於對保全攝影機的反感，且大部分的國民應該會認為進入便利商店是為了採購而非為了為非作歹，因此日常生活的便利性便使得當事人無視於便利商店之保全攝影機運作，而進入便利商店購物。概言之，或許大部分人進入便利商店之前，從未關心過該便利商店是否架設保全攝影機，以及保全攝影機之位置。

類似地，當個人丟棄廢棄物時，若日常垃圾中包含了許多關於個人資料的文本，例如信用卡帳單、百貨公司的會員通知、因職務所加入之工會團體寄發之定期刊物等等，這些文本至少都記載了個人地址以及收件人姓名，同時，這些定期寄發之文本常具有時效性，前述之帳單、會員通知、以及定期刊物均為此類文本，通常經過一段特定時間之後，就喪失資料價值。有些人或許會保留每月之信用卡帳單用以核對帳目，但經過一長時間，例如年度報稅完畢之後，這些累積的實體

[135] 7-11 超過 4800 家，全家、萊爾富、OK 合計亦超過四千家，參考「台灣 7-11 創新行銷學」，http://www.rod.idv.tw/blog/blog20071107.html，最後瀏覽日期 98 年 12 月 20 日、「不用搶！超商平價口罩今全面供應」，自由時報，2009-5-6，最後瀏覽日期 98 年 12 月 20 日。

[136] David O. Sears, Jonathan L. Freedman, L.Anne Peplau, 「社會心理學」，編譯黃安邦，校訂陳皎眉，初版，民國 75 年，9 月，頁 227。

[137] 同前揭註，P232。

資料對於個人而言，便是一種負擔，因此經過一段時間之後，多半會將這些文本予以丟棄。在乎個人資料是否隨著文本丟棄而暴露之人數，推估並非多數，因此這些個人資料便會隨著文本丟棄而一同被流出。若國家藉由各縣市處理垃圾之系統，將這些資料分類出來，便可能可以建立關於個人之相關資訊。例如透過長期觀察個人之信用卡帳單應繳金額與循環利息使用狀況，便可得知個人之消費負債狀況是否嚴重；類似地，透過對一個地區的個人觀察，便可得知某一地區總體而言的消費負債狀況是否嚴重。當消費負債狀況日趨嚴重時，可粗略得知人民所需要背負的利息壓力便會升高，此時系統可以針對個人或者區域之壓力指數進行門欄值設定，當壓力指數超過設定之門欄值時，若是個人，則代表個人可能會發生反社會的行為，若是地區，則代表該地區可能會面臨人民生活壓力增加之狀況，而引發一些區域混亂的行為，例如較可能因為壓力而產生攻擊性行為[138]。

個人丟棄的廢棄物中，亦可能包含其他與犯罪相關之跡證，例如廢棄物中，可能包含法規所禁止之管制藥物，如毒品，之遺跡，透過科技的輔助[139]，可以偵測出包含這些管制藥物的垃圾，而後再回溯追蹤運送此車次垃圾之垃圾車路徑，便可知悉這些管制藥物出現之地區。透過長期的觀察，可與檢警單位之犯罪資料庫進行比對，再藉由資料採礦之工具輔助，便可獲得關於管制藥物流入地區情況之相關預估情報，對於預防毒品交易、偵查毒品交易、預防黑幫犯罪等等保安工作，便可發揮輔助的功效。亦可將檢警單位之犯罪資料庫中，已知的相關黑幫人物及其相關人之姓名、綽號作為搜尋之關鍵字，針對累積之資料倉儲進行文本搜尋與分析，便可能有機會可以得到相關之資料，進一步在犯罪發生之前便能夠調度相關之警力配置，以預防犯罪發生；或者在犯罪發生之後，協助偵查工作迅速地獲得重要的突破，儘早發現關鍵人物之可能出沒地點。

---

[138] 同前揭註，引起憤怒之原因可能爲遭受他人之攻擊或凡擾，或者挫折，即個人欲達成之目標受到干擾或阻礙。P460-464

[139] “Building an E-Nose”， http://www.sciencefriday.com/videos/watch/10128，最後瀏覽日期：98 年 12 月 10 日，以及「可偵測毒品以爆炸物的新型 ETD」，http://next.itri.org.tw/insight/node/1080，最後瀏覽日期：98 年 12 月 10 日。

為了使用並且分析關聯性資料庫[140]內容，以達成犯罪預防及偵查協助之目的，需要兩方面的操作，包含建立具備關聯性分析條件的個人資料庫，以及後續針對個案的狀況不同，存取資料庫內容。由於本文所要建立的資料庫，係與個人之隱私權相關，並且要能夠符合能進行關聯性分析之要件[141]，因此需要針對資料庫建立以及存取之流程，設計較完善的保全程序，以避免個人的隱私權資料，或者分析後所得之資料，在前述過程中被有心人輕易取得，而破壞了建立此類資料庫的意義。

一般的資料庫存取控制，多利用「使用者分級」以及「密碼設定」兩類方式來進行控制管理。使用者分級為將使用者依照授權等級的不同，區分為有限授權使用者以及管理授權使用者，前者為依照授權內容，對不同檔案具有「讀、寫、刪」之不同權限，可再細分為許多不同等級，舉例而言，某些等級的有限授權使用者可能無法檢視某些機密等級較高之檔案(甚至無法在瀏覽檔案清單時看到有此檔案之存在)，又或者某些等級的有限授權使用者，僅可以讀取檔案內容，而無法編寫或者刪除檔案[142]。而密碼設定，除了可以阻擋非授權者的存取以外，當然也可以結合使用者分級，在使用者登入時即獲知使用者的授權等級，而在登入完成後，賦予不同的檔案存取權限[143]。通常，為了追蹤使用者的登入及使用狀況，資料庫系統還可以附隨產生使用者使用記錄檔案，以便得知使用者對於資料庫內的資料使用的狀況。

不過這一類的資料庫存取控制模式，尚無法直接適用在本文所討論的資料庫存取架構。此乃因此類與個人資料相關之資料庫，除了需要安全的存取機制外，對於資料外洩的管制亦需要十分嚴格。此處所謂之資料外洩，除了針對資料外洩

[140] 關於各式資料庫的簡介，請參閱王威澤，〈原生型 XML 資料庫關聯規則之探勘與利用關聯規則探勘壓縮資料庫〉，92 年 6 月。
[141] 關於關聯式資料庫的簡介，請參閱同前揭註。
[142]關於各式存取權限的簡介，請參閱 Microsoft 公司所提供之介紹，http://technet.microsoft.com/zh-tw/library/ms174786.aspx，最後瀏覽日期 2010 年 08 月 15 日。
[143] 關於密碼學的簡介，請參閱楊宗偉，〈密碼學的發展與應用〉，97 年 6 月。

行為在事後會處以極嚴厲之罰則外，更重要的，是需要在前端即防止資料外洩發生的可能性。資料外洩時，可能產生的危害為個人的資料與個人的姓名同時被知悉，因此獲得資料者，可以直接得知其獲得的資料為某特定人的個人資料，因此這些資料便成為有意義的資料，不只是某個未知人物的某筆資料而已。有心人可以藉由姓名的資料，繼續查詢到該特定人的其他資料，或者將其散佈開來，使該特定人的隱私權內容被其他人知悉，而承受隨後可能產生的更大風險[144]。舉例而言，若我們看到一筆資料，僅顯示某個人的財務狀況，或消費帳單，除此之外，並不顯示此人為誰，或者其住居地址，則此筆資料引起閱覽者注意的機會相對偏低，因為其並不具有指示性，無法指出資訊的所有人是誰。但若此筆資料除了顯示上述內容外，還顯示了所有人的姓名，及/或其住居地址，則閱覽者在閱覽到此筆資料時，可能第一時間會先將此姓名與其記憶中認識的人的姓名作一比較，若碰巧是其所認識之人，則此筆資料便可能引起閱覽者的注意。另外一方面，若閱覽者獲知資料所有者的姓名，則亦有可能透過進一步的搜尋，獲得此人之其他資料，甚至聯絡資料，而使資料所有者面臨不必要的風險。

因此，在個人資料庫中，個人的姓名及/或住居地址可被視為是一種識別個人的關鍵資料，而由於姓名具有無法輕易變更的特性，因此相較于住居地址而言，更能夠成為將資料庫中，每個人的資料，由統計上的分析地位，連結為同時代表識別個人的關鍵資料。因此，若能夠將個人姓名於資料建立與存取時另外獨立加密，並輔以資料庫使用者權限的分級設定，將更能有效地避免資料庫內容外洩。

換言之，在建立資料庫時，以及建立資料庫後，存取資料庫時，可利用程序設計，輔以資訊加密的技術設計[145]，使得僅有少數的被授權者（例如檢察官）能

[144] 關於資料外洩所可能引起的風險，例如 2009 年於臺灣發生的知名購物入口網站 pchome 的個人資料外洩事件(參考 http://www.zdnet.com.tw/news/web/0,2000085679,20142200,00.htm)；更多的個人資料外洩案例，可參考全民個人資料保護聯盟網頁，網址：http://tahrpapd.wordpress.com/，最後瀏覽日期，2010 年 04 月 20 日。

[145] 密碼學傳統意義上來說，是研究如何把訊息轉換成一種隱蔽的方式以防止其他人在非經授權

夠獲知分析結果的全貌，包含相關人士的姓名以及其行為分析結果。而在蒐集資料、分析資料、建立及維護資料庫過程中，需要技術人員操作的部分，則將每一筆資料中的人名加密或者遮蓋[146]，使技術人員依其工作內容之分類，僅可能接觸到每一筆資料的內容，而無法得知資料究竟屬於何人所有。如此一來，對於技術人員而言，由於其所會接觸的資料，限於人名以外的其他資料，因此，每一筆資料的內容便無異於一般的資料庫資料內容。而由於限制技術人員閱覽的資料僅有人名，因此技術人員可以根據其他所有的資料，進行日常的資料庫維護以及分析工作，對於其要進行完整的分析工作並無影響。最終，技術人員再將分析結果傳回被授權者，接著，被授權者便可將人名部分的資料解密，將其獲得的完整分析結果與特定人物連結。以下以流程圖說明上述方法。

1. 資料庫建立之保全流程

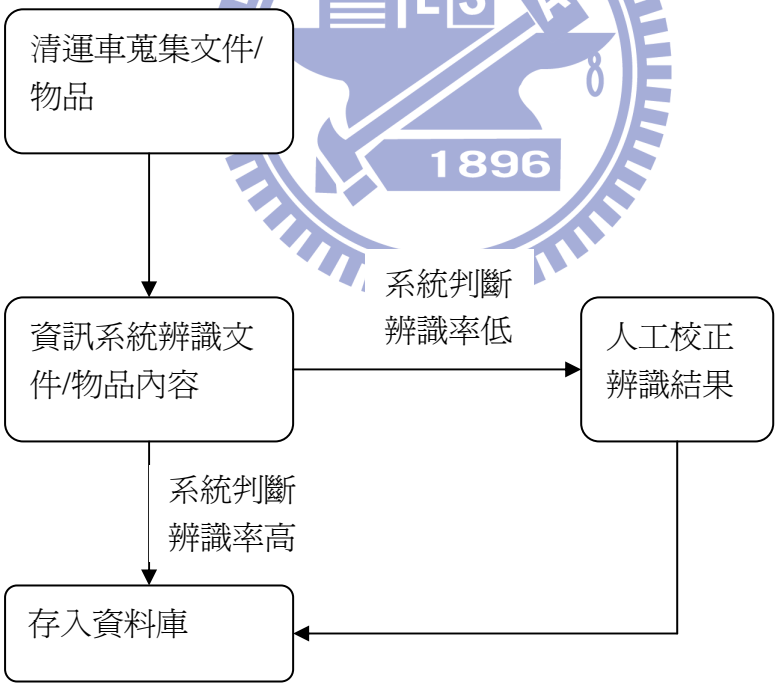

圖 3 資料庫建立流程圖

的狀態下獲得訊息內容。密碼學發展至今，藉由資訊科技的進步，已衍生出非常精密以及繁複的系統。請請參閱楊宗偉，〈密碼學的發展與應用〉，97 年 6 月。

[146] 參考現行司法院「法學資料檢索系統」之裁判書查詢資料庫，其中裁判書將當事人之個人資料隱去，使一般人於查詢裁判書內容時，僅能獲知案件事實，而對於當事人之姓名則無法得知。司法院法學資料檢索系統請參考 http://jirs.judicial.gov.tw/Index.htm。

關於前述流程圖中，將資料建立到資料庫中的程序，首先利用現行的清運車清運系統，其會將廢棄物中的文件以及物品分開蒐集，因此可便於後續的辨識作業執行。接著，在清運車蒐集完文件/物品後，可將文件與物品分別處理。對於文件，可利用前述的分件系統，將文件一一分出，並且進行文件上的文字辨識。利用影像擷取技術，將文件先製作成影像檔案，而後再利用辨識軟體辨識影像中所包含的文字。文字辨識完畢之後，對於文字辨識的結果，系統先進行判斷，將文字辨識結果被判斷為辨識率低於某一預定參考數值的文字，以文字與圖像同時呈現的方式，提供給技術人員進行人工校正辨識結果[147]。為使技術人員不要得知文件所記載的內容，可採用一次一字的方式，或者隨機排列文字的方式，將需要校正的文字逐一提供給技術人員；如此，可使技術人員僅針對文字本身的正確度於否進行校正，而不會得知文件本身記載的內容。辨識後的文字，再由系統放回文件中正確的段落，而後，將文件的文本與影像，對應地存入資料庫中。日後於分析過程中，使用到此資料庫內容時，若對其內容有所疑義，還可以同步調閱掃瞄獲得的影像檔案，以對疑問處進行釐清。

另一方面，針對物品辨識，由於物品辨識的目的是為了鑑定清運車所蒐集的物品中，是否含有特定的成分，最主要為管制藥品與毒品，因此，技術人員的主要工作，為確認鑑識系統是否正常運作；至於鑑識系統鑑定出來的結果，並非技術人員所應該知悉的內容，以防止鑑定結果被外洩。因此，針對此類特定物品的鑑識系統，技術人員主要工作有二，分別為確保鑑識系統能夠正常運作，以及確保鑑識系統與資料庫系統能夠正確連線，以便將鑑識系統的鑑定結果回傳到資料庫系統中，完成資料庫中的資料建立。因此，針對物品辨識，並不會有如同文件

[147] 光學字元辨識可同時提供待辨識圖像以及已完成辨識之字元，供使用者確認。相關資訊請參考 http://zh.wikipedia.org/zh-tw/%E5%85%89%E5%AD%B8%E5%8A%83%E8%A8%98%E7%AC%A6%E8%99%9F%E8%BE%A8%E8%AD%98。最後瀏覽日期，2010 年 2 月 10 日。

辨識般，發生系統辨識率低而需要人工進行辨識的狀況。

前述流程可相當程度減低資料庫於建立資料時，不慎發生資料庫之資料不當外洩的狀況，而對於資料庫建立後，存取資料庫以進行分析時，如何減低於分析過程時，以及分析結果產生時，資料及/或分析結果不當外洩的狀況，則需要搭配有限資格的授權[148]，以及加解密系統，如下所述。

2. 資料庫存取分析之保全流程

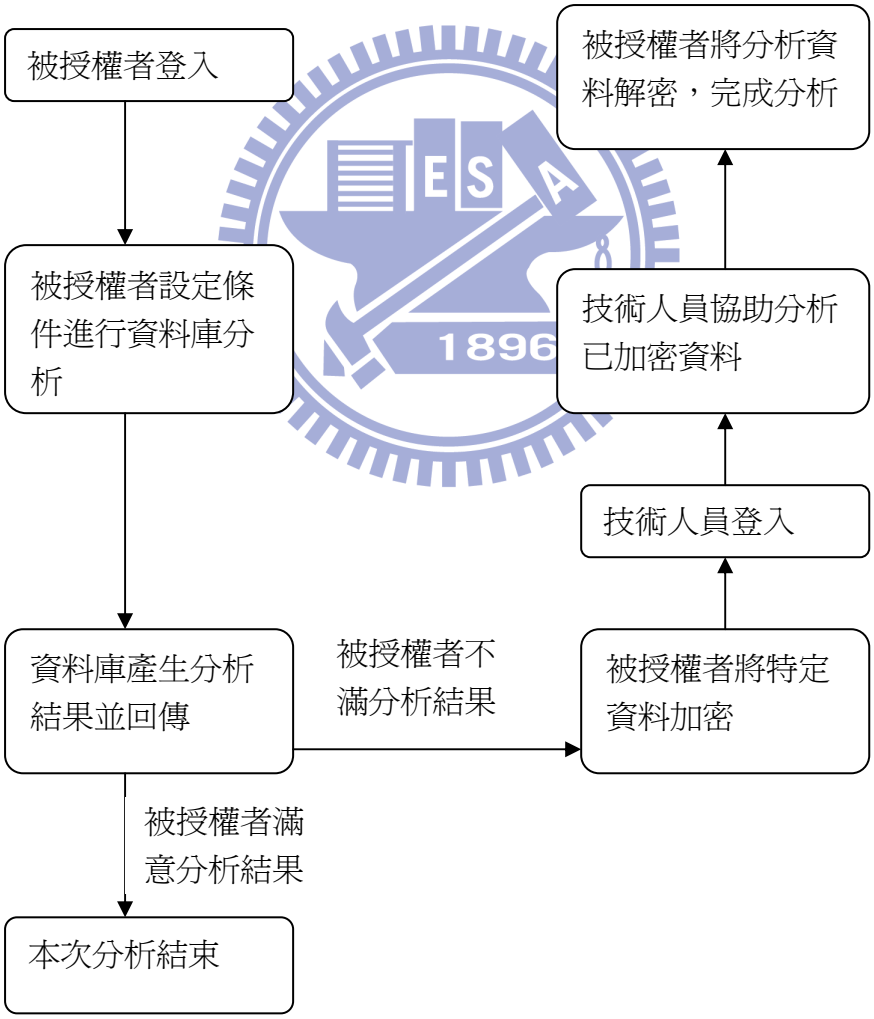

圖 4 資料庫分析流程圖

[148]關於各式存取權限的簡介，請參閱 Microsoft 公司所提供之介紹，http://technet.microsoft.com/zh-tw/library/ms174786.aspx，最後瀏覽日期 2010 年 08 月 15 日。

能夠被賦予啟動資料庫分析權限者，即為被授權人。因犯罪偵查所需，可限定被授權人為檢察官，或者特定的警察人員。在此分析方法中，以特定資料為人名為例說明，僅有被授權者能夠得知每一筆資料的所有人之姓名，此乃為確保個人的資料不至於被不當的讀取。按一般人對於資料閱讀的習慣，雖然可由資料本身判斷出可能為某人的個人資料，但當無法得知姓名時，此筆資料對於閱讀者而言，便僅是一筆紀錄著某人行為的資料，且對於此筆資料之理解，也會較偏向以類似理解統計資料般的方式來看待資料本身。另一方面，當閱讀者能夠於閱讀資料的同時，亦獲知資料所有者的姓名時，通常閱讀者的直接反應，是將自己所認識的人物之姓名，與資料所有者進行比對，試圖在自己的記憶中，搜尋與此人物有關之各種連結關係。幾個廣為人知的範例，例如社會報導中，對於新聞事件中，對於未成年人姓名僅做局部性顯示，例如僅顯示姓氏。又如現在法院判決文中，對於某些當事人，亦僅顯示其姓氏，或者以假名代替之。因此，將資料的所有者姓名予以加密或者遮蔽，而僅限被授權人能夠解密或閱覽，便可以使當事人之個人隱私受到一定程度之保護。而至於其他文字資料，則可以開放給其他授權等級較低的人員，於分析資料時閱覽並使用。

當被授權人登入系統後，可直接操作資料庫，被授權人對於資料庫所進行的分析需求以及獲得的分析結果，系統皆會記錄下來，以便對被授權人之查閱分析行為進行紀錄與事後審查。當被授權人直接操作資料庫，便可獲知其所需要之分析結果時，便無須技術人員之協助，可直接結束分析流程。但當被授權人對於分析的結果並不滿意，而需要技術人員協助，進行更細緻的資料分析時，則可將其所關注的特定資料加密或遮掩。為避免個人資料被不當外洩，加密人名是最能達成此目的的作法，可將系統中的人名轉換為一加密後的假名或代號，當技術人員進行資料分析協助時，仍然能夠針對此人名所對應的種種資料進行存取與關聯性

分析，但無從得知被分析對象的姓名[149]。如此，既可避免因過多的限制，導致技術人員要進行分析時過於困難，亦可避免除被授權人外，其他未經授權者獲知個人資料並且將其外洩的可能性。由於具有權限啟動資料分析流程者，僅有被授權人，同時被授權人對資料庫系統所進行之各種操作，皆受到紀錄，因此能夠將有權限閱讀完整資料者之人數，限制在相對容易受到管控的範圍。而能夠獲得授權者，通常是檢警系統中，已受考核通過或者具有一定資歷者，因此其能夠獲得被授權之基礎，已較其他人為高，因此資料庫內容被不當洩漏的機會應已可被顯著降低。

3. 資料庫比對技術應用於刑事偵查

當資料庫建立之後，便能用來輔助刑事偵查。例如當透過儀器，檢查出清運的垃圾中殘留有法規所禁止之管制藥物時，則掌握此項訊息之檢警人員，便可以透過資料庫，回溯出該次清運垃圾之垃圾車路徑，而後便可以得知垃圾原存在於哪個地區之中，便可合理推斷出在該地區內可能有毒品交易等不法行為發生。接下來，便可以透過與其他犯罪資料庫的比對，查詢資料庫中是否紀錄有該地區的相關犯罪事件與犯罪集團/犯罪者之記錄，早期掌握狀況。然後警察人員可以開始對該地區加強巡邏，以及針對該些可能進行犯罪者進行追查。便可能在犯罪發生之前，減少犯罪發生的可能性；或者在犯罪發生的初期，便先得知犯罪可能發生的狀況，進而提高對該地區犯罪發生的關注力。

又例如在透過分析文件，建立與個人相關的各種資料庫後，例如記載個人財務資料的信用卡帳單、通訊資料、會員資料等等相關資料庫；當犯罪發生時，檢警人員透過對犯罪現場的證據蒐集，可能會分析出一些可疑人物名單，此時透過與個人相關的資料庫進行關聯性比對之後，可以分析出許多可用的結果。例如透過通訊地址與人名的比對，可以過濾出可疑人物名單中，經常在該地區活動的人

[149] 透過限制能夠使用系統進行查詢的人數以及資格，可避免資料外洩之風險發生。例如通聯記錄，我國早期的檢察機制，每一位檢察官均能利用法務部所建置的資料系統進行查閱，但現今僅能透過申請，藉由專人查詢後，將查詢結果回報給檢察官。

物，以及其日常生活中可能會活動的範圍（透過分析信用卡帳單的消費地點、分析參與會員活動的內容等等），便可以更迅速且有效率地掌握可疑人物的可能活動範圍。又例如透過分析可疑人物的信用卡帳單以及銀行對帳單等等資訊，可以分析特定人物的消費習慣以及財務狀況，當這些財務活動透露出不正常的消費行為時，也可能有助於發現可疑人物的犯罪動機。

進一步言，由於各資料庫之間的資料可以進行關聯性分析，且此類比對係由電腦進行，因此能夠同時比對多個事件彼此之間的關聯性。當同一或不同的行政區發生多個事件時，現有的檢警系統，多僅能使檢警人員單獨對其所負責的案件進行追查，但對於各案件之間彼此可能相關的部分，則較難進行分析，尤其是跨越不同管區的案件，更難以進行案件彼此間的交互分析。此時，透過關聯性分析，便有可能找出各事件與資料庫內容的關係，再透過交互分析，便可能找出各事件之間可能存在的關聯性，然後同時提供給負責的檢警人員，進一步縮短案件訴追時間並且提高案件偵查之成功率。

在逐步建立資料庫後，經過時間的累積，資料庫的內容將會越來越豐富，且能夠顯示出某些具有時間性的特徵，例如消費習慣、活動範圍習慣、社交習慣等等。透過定期對資料庫內容設定一些風險管控的參考數值，可以透過操作資料庫，篩選出一些高風險係數的活動或者特定人物，便可在早期階段，投注較多的關注力在這些特定的事件或者人物身上，以避免可能犯罪的發生。當然這些被標示為可能具有高風險係數的活動或者特定人物，在真正的犯罪事件發生後，檢警人員進行資料比對的同時，也會在符合比對條件時，被系統標示為高風險係數，輔助檢警人員進行後續調查。

因此，對於國家蒐集國民公開之資料，並依照資料倉儲之特性建立包含各種分類之資料庫，應得採取較開放之態度。首先，這些資料必須為國民所自行公開者，雖然國民公開之資料有可能與生活之便利相關，但國民對於這些資料的公開釋出亦或多或少經過其內心的評量；再者，這些資料蒐集的行為，對於國民日常

生活的影響程度並不高，同時國民個人隱私內容中，與這些資料直接相關的並非高度敏感部分，因此對於蒐集此類公開資料採取開放的態度，對於國民的隱私權侵害程度應相對偏低。

而後續利用這些公開資料時，便需要嚴格限制其利用目的，與具有存取資料庫分析工具之資格者，對於違反規定者，亦需要課與相對較高的行政、民事以及刑事責任。此乃因透過資料分析所產生的分析結果，可能會透露出國民所不願公開的個人習性與行為特徵，若對於利用資料庫之限制較為寬鬆，則除了獲得存取資格者之人數與機關可能增加並且不易管控外，對於分析結果之散佈範圍管制亦可能相對困難，這種狀況可能會導致對於國民隱私內容之過度侵害。尤其是這些分析結果可能是在任何危害公共利益之事件，例如犯罪事件、暴力事件等等，發生前便著手分析的，非施以嚴格之目的與利用管制，無法彰顯國家對於隱私權之保障確已達到憲法所保護之基本權之保障。

再者，現今檢警人員，其實已有較簡單的資料系統可以查詢，例如警察於道路執行臨檢時，憑藉國民的姓名及/或身份證資料，便能查詢到基礎的資料，包含有無前科，以及身份證是否曾被冒用等等資料。又例如檢察官於日常辦理案件場合，便能透過法務部所建置的案件資料系統，查詢特定人過往曾經牽涉的案件資料。能夠使用這些資料庫者，均需要使用特定的器材，或者先行經過認證，成為被授權之使用者，以特定名稱及密碼登入系統。私人的資料庫，例如銀行或購物網站的客戶個人資料，或有時聽聞有不當外洩之狀況，而導致客戶可能遭受不必要的電話或簡訊騷擾，但來自檢警系統的規模性個人資料外洩，則仍未有聽聞媒體報導。因此，以更加嚴格的方式來對本文所討論的資料庫存取、分析進行規範，應能在完成協助犯罪偵防的目的時，同時有效地防止資料外洩。前述資料庫建立與分析讀取的流程，並不需要繁瑣的資料系統結構，因此並不會增加顯著的硬體成本，其核心精神，在於限制能夠讀取完整資料之人數，並且將關鍵資料予以加密，又能夠不影響資料分析工作的進行。另外，這些行政司法單位現今已經

建置並且持續更新的資料庫，未來將可以與本文所提及的，具備關聯性分析的資料庫進行連線，使得檢警人員能夠獲得更加有助益的資料分析結果，協助犯罪偵查行為與預防犯罪發生。

五、 結論與後續研究

我國現有的犯罪偵查方式，依靠檢警人員過往的辦案經驗，針對在犯罪現場中所搜尋到的跡證來擬定犯罪偵辦方向，並且在偵查中，隨著偵查進行，發掘出更多證據，便可逐漸修正偵辦方向，最終偵結案件。然而利用日新月異的資訊技術力量，來協助犯罪偵查，甚至分析出人力所無法分析出的特徵，已是可能實現的。以往，需要使用到資料庫搜尋的技術時，多是為了要比對某一特徵是否與資料庫中所建立的檔案相符，常見者例如指紋分析，又或者是 DNA 分析。這種分析是一種逐一比對的技術；當搜尋到判定為與待鑑定物相同的資料，或是搜尋整個資料庫而沒有發現可用的資料時，搜尋便會結束。而現今資訊科技的進步，已使得另一種可以進行關聯性分析的資料分析工具能夠在各種符合資料採礦(Data Mining)方式建立之資料庫之間，進行關聯性搜尋，而產生綜合的分析結果。隨著資訊科技的日趨進步，現今的資訊科技已能在短時間內處理極大的資料量，藉由資訊科技的能力，便能做到過往做不到的分析運算，而且能夠在短時間之內完成並且產生分析結果。若我們能夠建立此類資料庫，佐以關聯性資料分析介面，則檢警人員便能夠將其自身的案件承辦經驗，納入分析系統；藉由在各種資料庫之間進行關聯性分析，能夠更準確地找出與案件具有可能相關性的人物，而在偵查初期即能有效掌握可能涉案的特定人物，即使這其中有某些人物在案件偵查的初期，由表面的跡證看起來可能完全不相關，亦有可能成為案件偵查的重點。而這類在案件初期可能不被注意到的人物，便能藉由關聯性資料分析方式，在初期便被列出成為可能的調查對象，既能加強案件偵辦效果，又能減少漏網之魚的可能性，同時能夠在偵查初期便可以早一步鎖定對象，更能掌握案件偵查的效率。

能夠用於關聯性分析的資料庫，需要依照特定規則建立，並且隨時間不斷地增加資料庫內容，方能發揮關聯性分析的優點。由於所要蒐集的資料，與個人相關，則不可避免地，必定會觸碰到隱私權的議題。在我國，隱私權已透過司法院

大法官解釋文，承認為包含於基本權之範圍內，因此，針對個人所不願意提供出來的隱私權資料，除非具有極強的社會公益，或者透過執行已經立法之法規規定，才能要求個人提供這些隱私權資料；顯然地，這些個人可能不願意提供出來的隱私權資料，無法用來建立資料庫，否則資料庫的內容很可能面臨欠缺完整性之困擾。

另一方面，針對個人自願揭露的個人資料，則無論是政府機關或者其他任意第三人，均可能可以對其進行蒐集，以目前歐美各國的案例來看，對於這一類自願揭露的資料，個人無法再行主張有隱私權的適用。個人於日常生活中，最容易丟棄的資料，便是隨著垃圾、廢棄物丟棄之各式物品，這樣的丟棄行為，可以被視為是一種自願揭露的行為。在個人丟棄之各式物品中普遍記載個人相關資料的，就是各種信件與文件；另外，透過對於廢棄物的物質定性分析，亦可能檢測出廢棄物是否攜有特定的物質。長期累積這些資料並分門別類建立資料庫之後，便能夠透過關聯性分析介面，逐步勾勒出關於個人的行為習慣，以及各行政區域中，是否有違禁藥品的使用狀況。當案件發生的時候，或者在案件發生之前，便能夠透過對這些資料庫的分析，取得協助調查或者防範犯罪的分析結果，提升檢警打擊犯罪的效率。

個人自願揭露會破壞隱私權主張的概念，來自於美國的「棄置分析(abandonment and privacy standard)」，但隱私權與財產權有以下幾個不同特性，1.知悉隱私權內容不以佔有為要件；2. 隱私權內容洩漏不易察覺。這使得單純利用棄置分析來解釋隱私權得否主張時，會產生疑慮，雖然個人棄置的物品，無法再行主張財產權，但依照「棄置分析」或其他類似的見解，對於個人棄置的物品，是否得以完全自由地分析其上所可能攜帶的隱私權資料內容，便值得進一步思考。許多看似無害的個人隱私資料內容，在拼湊起來之後，便可能透露出許多進一步的個人訊息，針對這一類的資料分析，是否必要對其進行限制。而針對許多可能觸及隱私權資料內容的應用技術，國家應該要負擔何種責任，使得這些利用

的最終結果，能夠對社會公益產生正面的效果，同時又能適度合理的保護個人的隱私資料內容避免被不當利用，都是需要思考的問題。

過往的文本採礦是由純粹的文字比對技術開始發展。但現今，藉由科技力量的進步，文本採礦已經能轉變為包含訊息檢索、數據挖掘、統計等等複雜的分析方式來進行。由於許多信息都至少具有文本的形式來保存，有些攜帶有文字影像的圖像，也可以藉由文字辨識而同步儲存文本形式之料，因此文本採礦的技術即逐漸受到重視。例如，在 2007 年，歐洲警察局(Europol)的重大犯罪部門(Serious Crime division)發展出一套文本採礦分析系統，用以針對跨國組織犯罪進行資料分析。此一綜合分析系統整合了目前最先端的文本分析以及文本採礦技術，並協助歐洲警察局在執法時能夠提升到國際犯罪的層級。文本採礦與資料採礦最主要的分別，在於文本採礦的核心是語意處理分析運算，同時也會引入「自然語言處理」(Natural Language Process)這種運算核心，使得使用者可以如同講話般，將心中所想的思考邏輯直接鍵入成為搜尋條件，NLP 會分析使用語言（例如中文）的語意邏輯，將使用者的語言邏輯，轉化為資料庫可以瞭解的邏輯組合。因此，在資料運算能力充足的狀態下，便能夠以檢警人員容易理解的搜尋方式對資料庫進行搜尋。

我國於民國 94 年起施行垃圾強制分類，這使得蒐集廢棄物的難度降低，尤其是文件與其他的廢棄物是分開處理的，更增加了文件辨識的便利性。目前，各縣市政府之衛生當局依照行政區域大小，以及廢棄物之種類，均設定有不同的清運路線以及廢棄物分類蒐集規則。由於檢警單位的任務分配也是以轄區作為分野，而轄區劃分亦與行政區劃分高度相關，因此若能建立與地區相關的個人行為資料庫，於犯罪發生時，能進一步利用此等資料庫進行偵查工作，則應能發揮助益，有效地協助犯罪偵防進行。前述所提的蒐集與分析廢棄物之方法，均能藉由現行可行的技術手段來達成分析的目的，且能搭配現行已經存在於各縣市的廢棄物清運規劃來執行。易言之，為達成蒐集與分析廢棄物的目的，其中佔重要角色

的廢棄物清運與回收規劃已可藉由現行行政制度來達成，無須重新另為規劃。且廢棄物清運之規劃，係以地理分隔為基礎，正好與現行檢警人員之配置方式大致相符；針對廢棄物所進行的分析結果，在歸檔到資料庫時，每一筆資料也會攜帶著地理區域的資訊，因此檢警人員在使用這些資料庫時，對於分析結果所呈現的地理特徵，亦應具備一定的熟悉度，可以有助於犯罪偵防工作的進行。為了避免爭議，針對具有高度隱私性的個人生理資訊，例如醫療記錄、血型、基因資料等，考量其特殊的性質，以及對於達成犯罪預防及偵查協助之目的的效益，並不適宜進行辨識與蒐集。

為了使用並且分析關聯性資料庫內容，以達成犯罪預防及偵查協助之目的，需要兩方面的操作，包含建立具備關聯性分析條件的個人資料庫，以及後續針對個案的狀況不同，存取資料庫內容。由於本文所要建立的資料庫，係與個人之隱私權相關，並且要能夠符合能進行關聯性分析之要件，因此需要針對資料庫建立以及存取之流程，設計較完善的保全程序，以避免個人的隱私權資料，或者分析後所得之資料，在前述過程中被有心人輕易取得。本文所採用的方式為在建立資料庫時，以及建立資料庫後，存取資料庫時，可利用程序設計，輔以資訊加密的技術設計，使得僅有少數的被授權者（例如檢察官）能夠獲知分析結果的全貌，包含相關人士的姓名以及其行為分析結果。而在蒐集資料、分析資料、建立及維護資料庫過程中，需要技術人員操作的部分，則將每一筆資料中的人名加密或者遮蓋，使技術人員依其工作內容之分類，僅可能接觸到每一筆資料的內容，而無法得知資料究竟屬於何人所有。如此一來，對於技術人員而言，由於其所會接觸的資料，限於人名以外的其他資料，因此，每一筆資料的內容便無異於一般的資料庫資料內容。而由於限制技術人員閱覽的資料僅有人名，因此技術人員可以根據其他所有的資料，進行日常的資料庫維護以及分析工作，對於其要進行完整的分析工作並無影響。雖然於制度上與現行法規研究上，這樣的個人廢棄物資料庫具有可行的可能性，但是在考慮付諸實行的時候，仍然必需要考慮國民對於此類

行政措施所可能產生的觀感與相對反應，這些反應，都可能會影響到這類行為的最終成效，以及國民與政府之間的關係。

後續研究

雖然科技的進步，使得我們可利用各式資料庫的關聯性分析，協助犯罪偵查以及預防犯罪發生，並可以相當嚴密地防止資料庫的分析內容遭到不當的外洩，但在希望促進檢警人員的工作成效，又能不過當地干擾國民的隱私權的前提下所設計出的這套個人廢棄物資料庫建立與保全程序，卻可能影響到國民對於個人隱私權的關注程度。舉例而言，或許以現今的種種判決內容看來，國家的確可以針對個人所丟棄的廢棄物進行蒐集；然而，一旦國家真的開始進行這類的行為，則人民的生活方式必將會有所改變，例如人民開始需要花費成本來將攜帶有個人資料的文件銷毀，或者人民開始對於政府保存資料庫的努力存疑，而對政府產生不信任感等，凡此種種影響，均是在國家考慮國民個人隱私權與行政效率時，需要詳加關注的要點。

隨著科技的進步，未來還可能有許多技術能夠建立出更多種類的資料庫，使得這個資料庫網絡更加完備，更能夠協助檢警人員進行犯罪偵查。例如，在影像處理技術更臻成熟之後，或許現在都市中隨處可見的防盜攝影機，其影像品質便能夠達到可以進行人像辨識的程度，於是防盜攝影機所儲存的資料，也能夠變成一個可以使用的資料庫，而能針對人物與影像進行關聯性分析。當然，資訊科技的進步，必定也會使針對資料庫進行分析的時間能夠不斷地縮短，更進一步提升分析的效率，這些都是科技進步所帶來的優點。

另一方面，由於社會的發展越來越多元，人們彼此之間的活動與聯繫也隨之多元化並且越來越緊密；這些人與人之間的行為軌跡，在科技進步之下，都逐漸變得可以被追蹤。個人資料庫的建立有賴於這些技術的進步來達成，相對的，建立個人資料庫也會逐步地模糊了個人隱私權的界線；畢竟，多數人無法離群索居

過生活，群體生活具有其便利性，個人想要進行的各式活動，幾乎都能在群體生活中獲得滿足，也因此，個人的隱私權界線便很難劃分。舉例而言，在都市生活的個人，每隔一段時間便會收到許多信件文件等等，這些信件都載有個人資料，若要防止這些個人資料被蒐集，最佳的方式是在閱讀後，或者經過一段時間之後，將每一封信都銷毀，然而這樣的作法很難真正的普及到每個人的生活中，因此我們還是可以在紙張垃圾中發現許多信件。國家在開始蒐集個人資料以建立資料庫一段時間之後，隨著檢察機關的辦案效果提升，人民便會開始意識到這些資料庫的存在，而存在並且利用這樣的資料庫，是否會反而影響到人民的生活，使人民開始產生不舒服的感覺，甚至影響社會的正常活動，是實施此類行政措施時，在考量法律上適當性以及執行效果以外，需要仔細評估的後續影響，這可能關係著國民對於政府的信賴感，不可不慎重對待。期待後續的研究能夠在科技進步與個人隱私權保障之間做出衡平的機制，便能兼取兩者之優點，使社會治安能夠更進一步的受到保障。