國立臺灣大學法律學院法律學研究所

碩士論文

Graduate Institute of Law

College of Law

National Taiwan University

Master Thesis

手機科技與隱私權保障

——以手機內資訊之搜索為中心

Cell Phone Technology Meets Privacy Protection:

The Search of the Information on a Cell Phone

陳怡雯

Yi-Wen Chen

指導教授：林子儀 博士

Advisor: Tzu-Yi Lin, J.S.D.

中華民國 105 年 2 月

February 2016

國立臺灣大學碩士學位論文
口試委員會審定書

手機科技與隱私權保障
Cell Phone Technology Meets Privacy Protection

本論文係陳怡雯君（學號 R00A21021）在國立臺灣大學法律學系完成之碩士學位論文，於民國 105 年 1 月 27 日承下列考試委員審查通過及口試及格，特此證明

指導教授：林子儀

口試委員：林子儀

陳仲嶙

王泰升

鄧文聰

劉定基

謝辭

寫謝誌的這天終於到了。

最謝謝的是指導教授林子儀老師。我一直覺得自己是個資質比較駑鈍的學生，記得當初投公法論壇的論文初稿寫得偏了，除了偏向刑事訴訟法的討論、論文架構雜亂無章外，亦缺乏公法學的視角，嗣後才在老師一點一滴的指導下慢慢修整成如今面貌。非常謝謝老師在所上業務與學校課程大小事纏身之餘，仍是不厭其煩抽空細讀學生的論文、花時間與學生討論，讓學生在一個個的問題中反省自己的思考盲點。跟論文口試本比起來，充滿老師眉批的初稿更有溫度而值得紀念，也見證了研究所時光的波折與成長。

也非常謝謝四位口試委員對學生論文的指點。李榮耕老師的文章開啟了學生對電磁紀錄搜索的初步認識，也在口試時提醒學生由實務可行性的觀點，思考其之所以如此做的緣由；陳仲嶙老師非常為學生著想，除了提供法院判決的神救援以外，更點出論文中將合理隱私期待與第三人法則混淆討論之漏洞，亦為學生構築論文架構可能的修正途徑；劉定基老師的文章大為拓展學生對於雲端運算的認識，也試圖由智慧型裝置、手機資訊等不同角度切入，重新澄清學生的問題意識，提出探討問題的不同取徑；邱文聰老師則提醒學生應自更根本處著眼，由資訊隱私的理論出發，重新深究保護資訊隱私之理由何在。謝謝四位老師的問題與建議，讓學生從各種不同的觀點再次檢視已經寫出來的論文文本，重新思考自己的盲點。

謝謝小老闆瑛珠學姐一路上的照顧與提點。幫學姐蒐集文獻的過程中學到很多文書處理的厲害撇步，也從旁觀察如何將大工作切分為小工作分派完成的功夫。學姐真的是一位很貼心的小老闆，除了在期中期末與口試前給予彈性讓

我先專心完成手頭上的燃眉之急外，撰寫論文期間也給予我好多精神上支持與實質上的精闢建議。

謝謝研究所的好同學俐俐、家瑩、游董和 Emma 姐。因為自己半路出家的關係，我一直覺得沒有辦法完全打入這個圈子，謝謝你們讓我最終仍在此找到一絲絲的歸屬感，論文煎熬路上，感謝有你們相伴。尤其感謝俐俐師姐，除了總是被我巴著一起去見老師、在我緊張或挫敗時安撫情緒以外，更一手包辦論文口試大小雜事，打出超強大的紀錄！謝謝家瑩兼具雪中送炭溫情與當頭棒喝針砭的各種砥礪，「少女！」呼聲言猶在耳。謝謝康康學姐，跟論文搏鬥期間不時收到妳的打氣與鼓勵，覺得很窩心。謝謝昱中學長口試前的閒聊，讓我面對四位口委的緊張頓時消弭大半。謝謝家茹最後階段關於論文格式與離校手續的提點，順順助我走過最後一哩路。

謝謝 HRC 可愛的人們，日間寫論文所種植的大顆鴨梨，總是在晚上的揮汗如雨、笑聲如雷之中煙消雲散，讓我重新充滿能量。特別感謝板橋的餐餐 Family，每次都超期待去板橋館上課的時光，總是玩得超 high 笑得肚痛，更增添了一分歸屬感。謝謝大花，這幾年辛苦聽我哭遍各種跌宕起伏、衛生棉接眼淚，有妳真好。也謝謝俊琪，捷克黑糖牛奶家常菜、寶藏巖河濱夜景、天元宮櫻花滿開、小漁港真情流露……那些美好日常，是人生路上的珍貴光景。

最後也最重要的，謝謝我最最親愛的家人，我在你們的愛裡走到今天。謝謝爸爸，常提醒我腳步放慢、眼光放遠，每回跟您吃完飯總會寬心許多。謝謝媽媽，總是默默準備早餐、水果、晚餐、消夜……從食物中體會您滿滿的愛。謝謝老哥，總是第一時間笑嘻嘻分享最新的 3C 好康，讓我閉門造論文之餘仍能追上時代演進。謝謝子玲，每次去力霸都被餵得白白胖胖，身心靈全方位滿足。親愛的奶奶，望您在天上一切順心安好，跟親友開心玩四色牌、吃好料。

願我愛的人永遠健康平安。

中文摘要

本篇論文的研究主軸，係以手機科技為中心，試圖探討手機科技與現有隱私權概念的連結與互動，論述本文認為手機資訊應受憲法隱私權保護之理由。復引進美國法手機搜索案例作為借鏡，試圖對我國現行手機搜索扣押相關法制提出建議，盼於國家犯罪偵查需求與人民資訊隱私保障間求取平衡。

於今日資訊科技飛速進展的社會中，手機一方面使個人得以解放通訊所受地理限制，另方面亦作為個人遂行日常生活、管理親密領域之重要工具，儼然已成為現代人安身立命之媒介，地位有如精神上家宅。傳統隱私權對於「秘密空間」之解釋，係以物理空間為本位發展而來，恐與資訊科技社會的需求不盡貼合，或可適度擴張，涵蓋手機此一精神上秘密空間之保障。

此外，個人使用手機的同時，諸如通聯紀錄、簡訊文字、消費明細、瀏覽紀錄及照片影片等生活細節，也一併存放於手機之中，手機內資訊形同掌中大數據、鉅細靡遺，應受憲法隱私權之保障。復因打開手機前無法預知其內存有哪些資訊，故應將整支手機內所有資訊包裹視為一個標的給予同等保障，而不因個別資訊隱私程度高低有所差別待遇。考量到手機資訊有如完整個人檔案之特性，以及國家利用剖繪科技監控個人之風險，對於國家搜索扣押手機、取得其內資訊之規範，應採嚴格審查標準。

檢視我國現行實務作法並參酌美國法院實務判決及學說見解後，本文對我國現行手機搜索扣押法制提出以下建議：手機不得附帶搜索、手機搜索票應附加事後審查、手機密碼不受不自證己罪特權保護、手機資訊之附帶扣押及另案扣押應採重罪原則。如此既能顧及國家追訴犯罪之利益，亦讓人民適度保有一塊自由呼吸的空間，確保人格自由發展不受阻礙。

吾人解釋憲法時，應敏銳地覺察時代變化所導致之人民生活型態變遷而有所調整，力求於變遷的科技下，予人民不變的憲法保障，一再重新構築屬於當代的憲法意義，實踐保障人民權利的承諾。

關鍵字：隱私、隱私權、隱私保障、手機、手機科技、手機資訊、搜索

Abstract

This thesis is concerned with the interaction between cell phone technology and privacy protection.

People nowadays rely heavily on cell phones in their everyday lives. The mobile phones not only liberate communication from time and place, but also become an important instrument for calling, texting, reading, writing, taking photos and so on.

The information on a cell phone also offers a detailed picture about all aspects of a person's life. By searching a cell phone, the Government can reconstruct someone's life. Given the quantity and quality of information on cell phones and the risk of being profiled, people shall have self-control of such information, which should be protected under the right of information privacy of the Constitution.

When it comes to the judicial review of the search and seizure of cell phones, the court should apply strict scrutiny. Therefore, the Code of Criminal Procedure should be amended to be consistent with the principles of proportionality.

Technology might change over time, and the protection privacy should keep up with it. The court should be aware of the change and reconstruct the meaning of the Constitution again and again.

Keywords: privacy, privacy rights, privacy protection, cell phone, cell phone technology, cell phone information, search

目錄

1. 緒論

1. 1. 問題意識與問題之提出

隨著資訊時代來臨，人們使用手機聯絡溝通、處理事務之頻率日增。根據資策會 2015 年所做的調查，我國智慧型手機普及率已高達七成三，推估用戶高達 1525 萬人[1]。而 Google 針對我國所作之手機使用研究報告則顯示，高達八成之受訪者出門必定攜帶手機，形影不離，我國民眾對手機之依賴度更居於亞太地區之冠，超越第二名的日本以及第三名的香港[2]。

除了普及率高以外，以手機所引發之生活變革而論，由於現今智慧型手機功能齊全，除了接聽電話、傳送簡訊之傳統功能外，以手機閱讀電子書、收發email、撰寫個人日記、消費購物、使用手機通訊軟體、連上社群網站、拍攝照片影片上傳分享等，亦是司空見慣。人們的食衣住行育樂益發仰仗手機作為媒介，生活與手機密不可分。

惟若自另一個角度觀察，正因為手機功能包山包海、與個人生活各個面向緊密交織，人民使用手機的同時，諸如通聯紀錄、文字簡訊、社群軟體聊天訊息、電子郵件、定位資訊、生活照片、閱讀、消費、就醫與網頁瀏覽紀錄等等，也被手機詳實紀錄下來。易言之，人民使用手機時所留下之諸多數位足跡，各種開誠布公或私密敏感的個人資料，悉數存放於手機之中。由此觀之，手機科技與個人資訊隱私之間的關聯，不無探究之價值。

而在「科學辦案」掛帥之今日，鑑於手機與吾人生活緊密相關、作為行動溝通關鍵工具之特性，手機內為數甚豐之資訊，常係刑事犯罪偵查程序中之重

[1] 資策會調查：國內行動裝置用戶已超過 1600 萬，iThome 電腦報，2015 年 7 月 20 日，http://www.ithome.com.tw/news/97479（最後瀏覽日：2016 年 1 月 12 日）。

[2] *Our Mobile Planet: Taiwan*, THINK WITH GOOGLE, http://services.google.com/fh/files/misc/omp-2013-tw-local.pdf (last visited Jan. 12, 2016).

要線索，或足以定罪之關鍵證據，因而遭到檢警鎖定。警政署甚至制定「新世代行動網路 App 偵查相關系統中程計畫」，欲編列預算建置手機監察系統，意圖直接截取手機使用者的臉書、LINE、電話通聯、照片、文字以及地理位置等資訊，以利追緝犯罪[3]。

檢警因犯罪偵查需求，搜索調閱個人手機資訊，涉及人民財產權與隱私權之限制。惟當個人隱私保障與國家偵查需求互相衝突時，由於犯罪偵查的利益清晰可見（打擊犯罪、維持治安、保障人民安全等），保障隱私的好處卻隱而不顯[4]（「平日沒做虧心事，半夜不怕鬼敲門」之概念深植人心[5]），以致兩者在權衡時，天秤往往向犯罪偵查的利益傾斜，「重防患而輕隱私」，過於側重犯罪偵查之需要，卻忽略保障隱私的重要。以手機搜索而言，我國執法實務目前似僅重視手機資訊作為犯罪證據之便利性與重要性，至於手機資訊與憲法保障隱私權之關聯何在、政府取得人民手機資訊之方式有無過度干預隱私權之疑慮，相關討論付之闕如。

同樣作為個人資訊之鎖鑰，手機所受關注，似乎遠不如 DNA 或指紋資訊之多。既有文獻中不乏 DNA 資料庫建置、指紋之按捺與隱私權保障之議題討論，卻較少有人對於國家搜索手機程序之規範有所關心。本文爰以「手機科技與隱私權保障」為題，以手機為論述主軸，先介紹**手機科技對吾人現今生活引發哪些變革與風險？手機資訊涵蓋哪些層面？**奠基於對手機科技與其內資訊的理解，進一步討論**傳統隱私權概念如何回應手機科技之變革？手機資訊是否應受我國憲法隱私權保障？**最後由具體案例出發，探討**法院面對手機搜索案件**

[3] 【警察國家？】警政署花 5 億建置手機監控 APP　立委批把全民當犯人，蘋果日報，2017 年 11 月 2 日，https://tw.appledaily.com/new/realtime/20171102/1232513（最後瀏覽日：2017 年 12 月 3 日）。
[4] DANIEL J. SOLOVE, NOTHING TO HIDE : THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 2 (2011).
[5] 例如日前台北市對於「是否應於違停熱點設置監視器取締違規停車」之政策引發正反雙方激辯，正方論點不乏「不違停幹嘛怕別人抓」、「隱私是違法的人用來保護自己的藉口」云云。詳參：議員反監視器抓違停 柯：腦袋裝大便，蘋果日報，2015 年 4 月 25 日，http://www.appledaily.com.tw/appledaily/article/headline/20150425/36513866（最後瀏覽日：2016 年 1 月 12 日）。

時，如何在犯罪偵查需求與手機資訊隱私保障間求取平衡？盼能提供我國日後面對相關議題之思維，使隱私權保障與科技變遷無縫接軌。

1. 2. 研究範圍

研究議題設定上，「手機資訊」概念之指涉範圍可廣可狹，除了「手機本地端所儲存的資訊」以外，也可能意指「使用手機而儲存在他方的資訊」。例如儲存在行動電話業者的門號通聯記錄、通訊軟體聊天內容、Email 郵件、通話時的基地台位址資訊、備份於雲端伺服器的資料等等，我國實務上即曾發生警方得否向 LINE 業者調閱對話資料之爭議[6]。為避免議題過於發散，本文討論主軸與引介之美國法案例，重心置於國家搜索犯嫌或被告之手機本體及其所導致的隱私權爭議。至於檢警跳過犯嫌或被告、直接向第三人調取手機中的資訊[7]，如向電信業者調取手機基地台位址資訊，以及直接監聽手機通話所生之通訊監察問題，因係另一廣大議題，所涉爭議與搜索不盡相同，本文僅略予介紹，不另詳文討論。本文亦將討論範圍限縮於刑事偵查審判程序中的搜索，至於其他如行政搜索等，也不在本文探討範圍。

其次，本文雖旨在探討「手機」資訊之搜索，惟因現今智慧型手機功能之豐，有如微型電腦，故手機記憶體內電磁紀錄之搜索，所生爭議實與對於電腦硬碟所為之搜索近似。因此，於電磁紀錄應如何搜索扣押、一目瞭然法則是否適用之問題，本文敘述上除探討涉及手機之案例外，亦援引性質類似、搜索電腦內電磁紀錄之案例作為參考，以豐富本文之討論。

再者，以附帶搜索手機之議題而言，一般討論附帶搜索前，常會先行探討

[6] 警調閱 LINE 辦案 立委質疑侵害隱私，自由時報，2014 年 11 月 2 日，http://news.ltn.com.tw/news/politics/paper/826709；戴雅真，用 LINE 販毒 警調難監控，中央通訊社，2015 年 7 月 6 日，http://www.cna.com.tw/news/aipl/201507060165-1.aspx（最後瀏覽日：2016 年 1 月 12 日）。

[7] 此種作法涉及美國法上第三人法則（third-party doctrine）之爭議。相關案例參考 DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 172 (2004).

「於何種情況下得為附帶搜索」：諸如警察臨檢時得否為附帶搜索？盤查時有無權限為之？附帶搜索與警察職權行使法第 7 條第 1 項[8]攔停拍觸檢查規定之關係等等。惟此並非本文研究重點，本文研究範圍限縮於後階段可否對手機為附帶搜索、搜索範圍廣狹之討論，至於前階段涉及臨檢盤查與攔停拍觸是否合法合憲、如何解釋適用之爭議，不在本文討論之列。

此外，伴隨著違法搜索而生的，即是刑事訴訟法第 158 條之 4 證據排除例外之爭議。該條規定：「除法律另有規定外，實施刑事訴訟程序之公務員因違背法定程序取得之證據，其有無證據能力之認定，應審酌人權保障及公共利益之均衡維護。」惟實務上，我國法院權衡後，經常作成違法所得證據無須排除之結論，導致合法取證之前端要件形同具文，備受學界批評。本條為刑事訴訟法上的重要爭議之一，恐非隻字片語所能道盡，礙於作者心力與文章篇幅，證據排除相關爭議，亦不在本文討論的範圍。

1. 3. 研究方法

本文研究，將以文獻分析法為主，梳理分析國內外與本文主題有關之實務判決、期刊論文、專書論著等資料，作為解決我國法實際問題之基礎。國內文獻部分，由於本文所欲探討之手機科技現況、手機科技與隱私權的互動、手機資訊隱私之保障（包含得否附帶搜索手機、手機搜索票應如何核發、手機密碼是否受不自證己罪特權保障，以及手機資訊是否全盤適用附帶扣押及另案扣押等問題）仍屬新興議題，國內對此關注尚少，故本文盡可能搜羅相關的實證研究、學者意見及法院判決，奠基於前人研究結果之上，進一步深入探討。

此外，本文亦採比較法研究，希以他山之石攻我國之錯。尤以手機搜索案

[8] 警察職權行使法第 7 條第 1 項：「警察依前條規定，為查證人民身份，得採取下列之必要措施：一、攔停人、車、船及其他交通工具。二、詢問姓名、出生年月日、出生地、國籍住居所及身份證統一編號等。三、令出示身份證明文件。四、若有明顯事實足認其有攜帶足以自殺、自傷或傷害他人生命或身體之物者，得檢查其身體及所攜帶之物。」

例而論，我國實務判決似乎尚未意識到手機搜索所涉及的隱私權爭議，學界相關文獻亦不多。反觀美國，法院已作出相當多的判決先例，學界亦不乏正反聲浪。該國對於此類案件的思考與論辯，諸如各級法院的論理、學者的批評等，實值我國參考。因此，本文即以美國法院實務判決與學說見解作為研究素材，整理該國法院與學者對隱私權的見解與詮釋，以及實務上涉及手機搜索與隱私權的各級法院判決，細述法院判決理由與學者評論，作為本文討論之借鏡。

1.4. 本文架構

本文係以手機為論述主軸，重行審視手機科技與隱私權保障之互動關係。先自手機科技對吾人生活引發何種變革談起，再進一步論述傳統隱私權概念如何回應手機科技之變革、我國憲法隱私權之保障是否涵蓋手機資訊等議題。復以手機資訊搜索之具體案件為例，探討法院應如何在犯罪偵查需求與手機資訊隱私保障間求取平衡。為討論上開議題，本文採取以下之架構，依序鋪陳：

第一章為緒論，提出本文所欲研究之問題，並敘述本文的研究範圍、所採行之研究方法，並說明本文採取怎樣的架構論述所提出的問題。章末概述本文見解，以使讀者於閱讀時有所依循，並可檢視論證的有效性。

第二章則先就手機科技作一綜融介紹，先敘述手機使用現況，復說明手機科技對現代人生活帶來的正負面影響。本章引述國內外人民使用手機現況之實證調查數據，以及社會學、心理學者之觀察，點出手機既解放又制約個人、雖增添便利性卻也使得個人私領域界線漸趨模糊、手機中個人資訊涵蓋層面既廣且深等特性，試圖描繪手機科技的獨特樣貌，亦就其作為國家監視媒介之監控風險予以說明。

第三章奠基於前一章對手機的認識，進一步深究手機科技與隱私權之間的互動關係。首先論述美國與我國隱私權的發展沿革、權利內涵以及保障面向，

讓讀者對隱私權的面貌有所認識。接著切入分析手機與隱私權的互動，探討手機科技與私領域之保護、個人人格形塑、資訊自主控制之間的關聯。最後則就手機科技所引發的隱私權思考予以論述，探討手機科技如何衝擊傳統隱私權概念、手機資訊如何衍生剖繪監控風險等，進而提出本文對於手機資訊應否及如何受隱私權保障之見解。

第四章則著眼於實際案例，探討如何具體保障手機資訊之議題。本章依序以檢警逮捕時得否附帶搜索手機、逮捕後欲搜索手機時應如何聲請搜索票、取得令狀搜索手機時得否強制受搜索人解鎖手機、搜索手機資訊是否適用附帶扣押及另案扣押等具體問題作為討論主軸，先說明我國現行實務作法，再引介美國法上對於是類案件之判決與討論，觀察該國法官及學者如何思考手機科技對於個人隱私權保障所生之變革與衝突，於既有舊法架構下提出新的詮釋。章末則論述本文見解，對我國現行手機搜索規範進行合憲性檢驗並提出建議，期許我國隱私權法制能有效回應新興科技的變革，達致國家犯罪偵查與個人隱私保護之平衡。

第五章為結論，回顧本篇論文之研究主軸並總結本文。

1.5. 本文見解

於今日資訊科技飛速進展的社會中，手機使個人得以解放通訊所受地理限制，亦作為個人管理親密領域、接觸外界資訊之重要工具。本文認為，手機幾已成為現代人安身立命之媒介，地位有如精神上家宅；往昔以物理空間為本位所發展出的傳統隱私權概念，恐與資訊科技社會的需求不夠貼合，或可適度擴張，涵蓋對於精神上秘密空間之保障。

復因個人使用手機的同時，諸如通聯紀錄、簡訊文字、消費明細、瀏覽紀錄及照片影片等生活細節，也一併存放於手機之中，手機內資訊形同掌中大數

據、鉅細靡遺，亦應落於憲法隱私權保障個人資訊自主控制之範疇。此外，由於打開手機前無法預知其內存有哪些資訊，故應將整支手機內所有資訊包裹視為一個標的給予同等保障，而不因個別資訊隱私程度高低有所差別待遇。

然基本權利之保障並非絕對，國家基於追訴犯罪、證據蒐集之需求，仍得以法律明定搜索扣押等強制手段取得手機資訊。考量到手機資訊詳載個人生活細節的特性，以及國家利用剖繪科技監控個人之風險，本文認為對於國家搜索扣押手機、取得其內資訊之規範，應採嚴格審查標準。

檢視我國現行實務作法並參酌美國法院實務判決及學說見解後，本文建議我國現行手機搜索扣押適用上應有所修正：手機不得附帶搜索、手機搜索票應附加事後審查、手機密碼不受不自證己罪特權保護、手機資訊之附帶扣押及另案扣押應採重罪原則。如此始能符合憲法比例原則之要求，既能達成追訴犯罪之目的，亦兼顧憲法對隱私權之保障，讓人民享有一塊自由呼吸的空間，確保人格自由發展不受阻礙。吾人解釋憲法時，亦應隨時之變遷而有所調整，力求於變遷的科技下，予人民不變的憲法保障。

2. 手機科技之現況與影響

手機，正式名稱為行動電話（mobile phone，大陸則稱移動電話）、蜂巢式電話（cellular phone）或可攜式電話（portable phone）。社會學者觀察，在台灣，人們通常將行動電話俗稱為大哥大或手機；因為 Nokia 的成功而被譽為手機王國的芬蘭，青少年與年輕人常以 känny、kännykkä（手的延伸）暱稱手機；德文中，對手機也有 handlich（handy，手邊的、便於使用的）的稱呼。據此，學者點出，手機的學名、俗名與譯名，在中西或不同國家、文化間之所以會有差異，背後反映的可能是人民對其賦予的社會功能與社會意涵不同之故[9]。

隨著行動通訊普及，手機逐漸取代市內電話與公用電話的功能，成為現代人交往聯絡的主要工具。此點除了自「低頭族」司空見慣、坊間充斥教人如何擺脫手機制約的教學文章之現象可見一斑外，從通訊錄之編制，亦可嗅出此一時代的變遷。以往，通訊錄上記載的是個人家中的市內電話；而今，通訊錄上記載的多是個人的手機號碼。由此，足見人與人之間日益仰賴手機聯繫，手機也漸漸躋身生活必需品之列。

智慧型手機在現代社會的普及性，實已無庸贅述，惟手機究竟引發哪些個人生活中的變革，手機內所載資訊之質與量有何獨特，文獻中鮮見探討。本章爰引介手機使用之實證調查數據，以及社會學家、心理學者等對於手機之觀察與討論，試圖描繪手機科技的樣貌及其影響，為後續討論奠基。

2.1. 手機使用現況之實證研究

根據資策會 2015 年對國人所做的抽樣調查，我國智慧型手機普及率已高達 73.4%，推估用戶約 1525 萬人[10]。再細就年齡分析，行動裝置之普及，並非

[9] 王佳煌，《手機社會學？》，初版，頁 2（2005 年）。
[10] 前揭註 1。

僅限於某一年齡層，高達 56.9%之國小學童擁有可上網之智慧型手機[11]，50 歲以上之中高年齡層擁有行動裝置之比率亦達到 26.6%，顯見行動裝置已逐漸滲入各年齡層人口之生活[12]。此外，民眾使用行動上網的比例亦在提高，由 2012 年的 25.91%成長為 2014 年的 47.27%[13]。

Google 針對台灣所作之手機使用研究報告則顯示，我國民眾對手機之依賴度居亞太地區之冠，超越第二名的日本以及第三名的香港。近七成受訪者每天均使用智慧型手機，更有高達八成的受訪者出門必定攜帶手機、與手機形影不離。國人常用功能則包括上網、收發 email、照相錄影、玩遊戲等[14]。Google 全球副總裁 Chris Yerga 更於演講中表示，台灣每人每日使用行動裝置的分鐘數位居世界第一[15]。

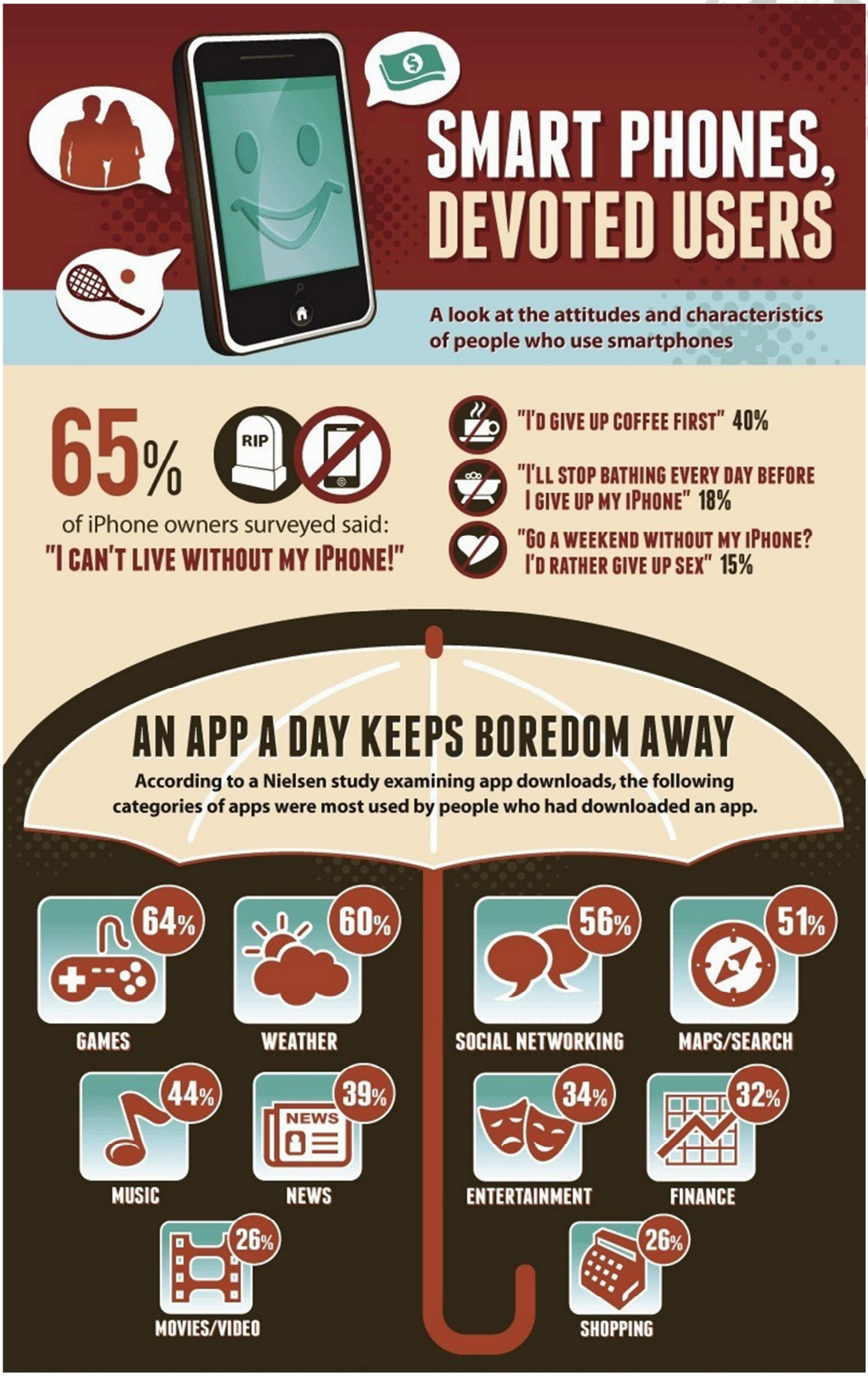
現代人過度依賴手機之現況，由 2015 年 Motorola 公司對於七個國家（印度、中國、西班牙、美國、巴西、英國、墨西哥）的手機使用者所做之全球智慧型手機調查，或可窺見端倪。高達六成的受訪者會握著手機入睡；過半數（54%）的受訪者遇上火災時第一個搶救的是手機；四成的受訪者表示自己會向手機詢問一些不會告知摯友的私密問題；甚至有兩成多（22%）的受訪者寧可為了手機放棄週末的性愛[16]。

[11] 影音隨身滑 兒少網安新挑戰 2015 國小兒童上網行為調查，台灣展翅協會，2015 年 2 月 10 日，http://www.ecpat.org.tw/dactive/knowledge.asp?qbid=695（最後瀏覽日：2016 年 1 月 12 日）。
[12] 前揭註 1。
[13] 台灣寬頻網路使用調查，台灣網路資訊中心，2014 年 8 月 19 日，http://www.twnic.net.tw/download/200307/20140820a.pdf（最後瀏覽日：2016 年 1 月 12 日）。
[14] 前揭註 2。
[15] 台灣人愛滑手機 遊戲產業大商機，聯合新聞網，2015 年 1 月 28 日，http://udn.com/news/story/7088/671952（最後瀏覽日：2016 年 1 月 12 日）。
[16] *2015 Motorola Global Smartphone Relationship Survey*, THE OFFICIAL MOTOROLA BLOG (Jul. 28, 2015), https://blog.motorola.com/2015/07/28/2015-motorola-global-smartphone-relationship-survey

圖一：Motorola 公司的智慧型手機使用調查

另一項訪問數據則指出，百分之六十五的受訪者認為沒有 iPhone 就活不下去；百分之四十的受訪者則表示寧願戒掉咖啡也不願戒掉 iPhone；百分之十八的受訪者把 iPhone 看得比每天洗澡還重要；甚至有百分之十五的受訪者願意為了 iPhone 放棄性愛[17]。上述調查或許有幾分戲謔成分在，但從中仍可窺見現代人生活受手機制約之深。

[17] Sam Laird, *Are You Addicted to Your Smartphone?*, MUSHABLE (Sep. 6, 2012), http://mashable.com/2012/09/05/addicted-smartphone



圖二：現代人與手機難分難捨的現況

2. 2. 手機科技的正負面影響

2. 2. 1. 手機科技之正面影響

2. 2. 1. 1. 手機解放通訊所受地理限制

以手機的學名而言，將這種通信裝置稱為「行動電話」、「移動電話」的主要意涵，係指此類通信裝置跨越了既定時空與場所的限制，讓使用者得以在行動中與遠方的使用者通訊溝通[18]。社會學者 Rich Ling 教授認為，行動通訊改變了社交情境的發展與實踐。此前，人們只能與身邊的人交談。紙本信件有時間遲延的缺點，電報、傳真、電話與電腦雖能讓訊息傳遞趨近同步，但仍受到裝置所在地點的限制。直到行動通訊出現，人們得以與身處地球任一端的他方談話，發話對象也由「地點（locations）」換成「個人（individuals）」，使人與人的溝通跳脫地點的束縛，這是其他通訊工具無法企及的[19]。

社會學家 Barry Wellman 持類似見解，認為手機使個人得以跳脫有線電話的地理限制，使連結的動力由地方（places）轉移至個人（individuals），促進個人對個人之間的連結（person-to-person connectivity），並將行動通訊所引發的革命稱為網路個人主義（networked individualism）的興起[20]。

Ingrid Richardson 教授亦指出，通訊科技打破了人們對地點和在場（presence）的概念，傳統物理空間上清楚分明的「這裡／那裡」、「遠／近」、「內／外」、「在場／不在場」，界線漸趨模糊，不再如以往一般截然二分[21]。

幾位教授的觀察，無非指向同一個方向：手機使人們擺脫時空限制，加強

[18] 王佳煌（註 9），頁 2-3。
[19] RICH LING, NEW TECH, NEW TIES: HOW MOBILE COMMUNICATION IS RESHAPING SOCIAL COHESION 3.
[20] Barry Wellman, *Physical Place and Cyberplace: The Rise of Personalized Networking*, 25 INT. J. URBAN REG. RES. 227, 238 (2001)。
[21] Ingrid Richardson, *Pocket Technospaces: the Bodily Incorporation of Mobile Media*, in MOBILE PHONE CULTURES 66, 73 (Gerard Goggin ed., 2008).

人與人之間的直接連結。以往有線電話、電報、傳真與電子郵件等通訊工具，固然增強了傳播通訊的能力，但始終受到地點的限制：人們必須身處通訊裝置所在之處，始能傳遞訊息。手機的出現，卻帶來了革命性的轉變，人們溝通不再受到時間與地點的限制，不再被通訊裝置綁住（必須身處電話、電腦、電報機或傳真機等通訊工具所在之處始得通訊），而是將通訊裝置帶著走，隨時隨地打給任何人。這樣的特性也模糊了人們對傳統空間概念的理解，個人可以站在「這裡」、同時卻跟「那裡」的人講話，跟近處的人相對無語、卻跟遠在半個地球外的朋友滔滔不絕。所謂的此彼遠近，不再截然分明。

2. 2. 1. 2. 手機使人民生活更為便捷

法學教授 Tim Wu 曾言，現代人的經濟與社會生活係以資訊為基礎，而這些資訊係透過網際網路傳遞。個人的生活與工作均與資訊緊密相關，對資訊之依賴日深[22]。而在智慧型手機與行動上網普及的今日，除了最基本的通訊功能外，隨著其功能不斷增加改進、應用程式推陳出新，手機更進一步成為個人接觸資訊、遂行日常生活與社交互動之重要媒介。

John Palfrey 與 Urs Gasser 兩位法學教授即指出，「數位原生代[23]（Digital Natives）」的人們，泰半時間都生活在網路上，個人越來越常利用電腦與手機等數位科技接觸資訊、創造知識與藝術。手機除了作為這世代人們與他人保持

[22] Tim Wu 著，顧佳、陳正芬、周佳欣譯，《誰控制了總開關？》，頁 16（2013 年）。

[23] 此一概念承襲自教育學者 Marc Prensky 於 2001 年探討教育改革時所提出的著名概念：「數位原生代（Digital Natives）」與「數位移民（Digital Immigrants）」。所謂的數位移民，指的是操著前數位時代的「口音」（例如必須將電腦文字印出來編輯、把人們帶進辦公室觀看有趣的網站而非直接將網址貼給別人等等），從傳統類比時代逐漸過渡到現今數位時代、試圖適應數位時代新語言的人們。相對於此，數位原生代的學生自小在數位環境中成長，在電腦、電視遊樂器、數位音樂與手機環繞的環境中生活成長。數位語言已成了現代學生的母語，電腦與手機則成了數位原生代生活中不可或缺的一部分。詳見 Marc Prensky, *Digital Natives, Digital Immigrants*, ON THE HORIZON, http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf (last visited Jan. 12, 2016).

連結的重要媒介外，更創造了一個全年無休的網路，使上線與離線的生活密不可分，將人與科技緊密聯繫起來[24]。

就日常生活而言，現今智慧型手機除了最基本的撥接電話與收發簡訊外，手機多元的功能也使得人民的生活便捷許多：個人可以利用手機收發 email 處理事務、上網瀏覽網頁、追蹤新聞、閱讀電子書籍、玩遊戲、存取 Dropbox 的檔案、預約叫車、用 Health 管理身體健康、以 Camera+拍下生活點滴、利用行動支付購買物品、用記帳軟體記錄金錢流向、連上 Facebook、Twitter、Instagram 等社群網站貼圖分享或抒發心情、使用 Evernote 撰寫心情日記及工作筆記、打開 LINE 與朋友閒話家常、甚至刻意利用手機的 GPS 紀錄自己行蹤[25]或將遺書留在手機裡[26]等等。

再以社交生活而論，根據一項 2015 年針對美國、英國、法國與德國之消費者所做的調查，「連上社群網站」即是受訪者使用手機最常做的活動，高達七成一的消費者每天都會使用手機瀏覽社群網站。若聚焦美國，亦有七成一的消費者，每週至少會使用手機上社群網站發布一次動態[27]。

由下圖 Google 調查數據即可看出我國人民使用手機的狀況。大多數的手機使用者會利用手機連結社交網路，收發電子郵件，在網站、部落格或留言板上撰寫評論，瀏覽網路內容，以及玩遊戲、聽音樂、觀看影片等。由此足見，

---

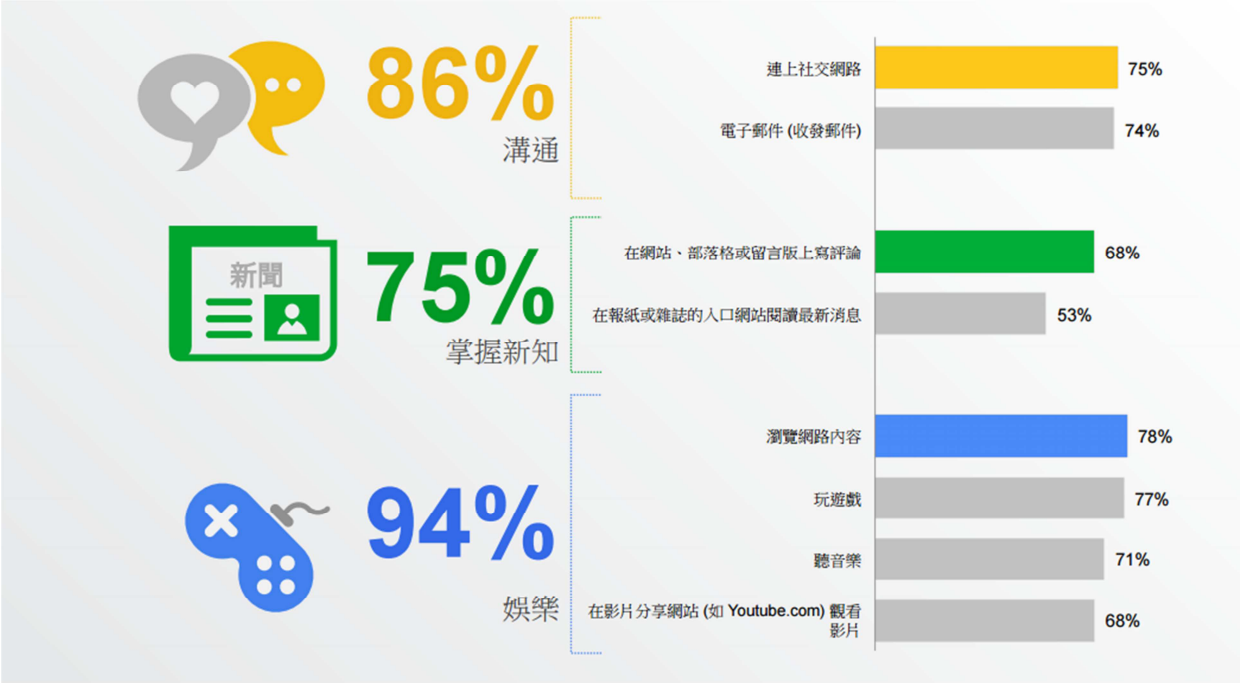
[24] JOHN PALFREY AND URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 4-7 (2010).

[25] 日前喧騰一時之媽媽嘴命案，咖啡店老闆呂炳宏因金紙店老闆娘一口咬定目擊其跟加害人一起到店裡買冥紙，而被檢警懷疑涉有重嫌，之後才還他清白。自此以後，呂炳宏養成了開啟手機定位的習慣：「我現在出門一定都帶手機開定位，省得要用的時候找不到，跳到黃河都洗不清。」詳見：呂炳宏「最恐怖的不是謝依涵」而是…，蘋果即時，http://www.appledaily.com.tw/realtimenews/article/local/20151127/741178（最後瀏覽日：2016 年 1 月 12 日）。

[26] 原諒媽 把珍寶當蠢材 林母淚 po：現在知道你對理念的堅持，蘋果日報，2015 年 08 月 02 日，http://www.appledaily.com.tw/appledaily/article/headline/20150802/36700039（最後瀏覽日：2016 年 1 月 12 日）。

[27] *2015 Adobe Mobile Consumer Survey*, ADOBE, http://landing.adobe.com/en/na/solutions/experience-manager/188465-mobile-consumer-study.html (last visited Jan. 12, 2016).

手機確實帶給人民生活上許多便利，現代人食衣住行育樂的種種需求，也愈發仰賴手機。



圖三：Google 對於台灣人民手機使用之調查[28]

2. 2. 1. 3. 手機成為管理私領域重要工具

如前所述，手機的出現，解放了通訊所受之地理限制，將人與人之間的面對面溝通予以延伸，使得人們免去交通會面的不便，即使身處異地仍能相互對談；手機的多元功能，亦使人民生活更加便捷。

除此之外，亦有論者從另一個角度理解手機的功能，認為十九世紀以降，現代都會環境充斥太多刺激，手機使得身處廣場、咖啡廳與火車車廂等公共場合的個人，可以選擇性過濾掉周遭環境的刺激，避開與陌生人非必要的接觸。此舉不代表個人從其所在之處抽離，反之，個人只是與周遭人們建立了不同形式的關係，藉由手機（或諸如書本、隨身聽等其他工具），自由管理控制自己

[28] 前揭註 2。

與所處環境、周遭人群之間的互動[29]。

心理學教授 Kenneth J. Gergen 也有著類似的觀察，直指手機賦予個人「建立空間」的能力。手機使用者得以自外於外在物理世界，與通話中的他方建立「內部空間（inside space）」，摒絕外在世界（outside space）的參與及干擾，在此一內部空間中自由往來交流[30]。

Ling 教授則認為手機增進了人們的安全感[31]，並將手機稱為「親密領域的工具[32]（the tool of the intimate sphere）」。Ling 教授認為，人們在日常生活中，雖然必須應對各種陌生或熟識的人，但有了手機，人們即得以保有與個人的親密領域，將家人、情人與最親密的朋友們涵括於內。手機不只使人們便於聯繫彼此，更促進了團體內部的互動，清楚區別誰是圈內人、誰是圈外人，創造出一個有界的凝聚力[33]（bounded solidarity）。

綜融上開論者的觀察，手機的問世，讓手機使用者得以自外於外部環境，切割出一塊獨立的內部空間，與通訊中的他方自由交流，不受外在干擾。個人亦可以手機為體、各個應用程式為用（如 LINE、Skype 等通訊軟體及 Facebook 或 Instagram 等社群軟體等），針對不同談話對象，建立起一個個獨立內部空間，在特定對象的個別空間內暢所欲言[34]，藉此往來交流、聯絡感情。個人也可以利用手機，自由管控與所處環境之間的互動，自由選擇是否避開與周遭人群非必要的接觸，在手機所創造的空間內得到喘息。

---

[29] ADRIANA DE SOUZA E SILVA & JORDAN FRITH, MOBILE INTERFACES IN PUBLIC SPACES: LOCATIONAL PRIVACY, CONTROL, AND URBAN SOCIABILITY 5-6 (2012).

[30] Kenneth J. Gergen, *The Challenge of Absent Presence*, in PERPETUAL CONTACT: MOBILE COMMUNICATION, PRIVATE TALK, PUBLIC PERFORMANCE 227, 227-41 (James E. Katz & Mark A. Aakhus eds., 2002).

[31] LING, *supra* note 19, at 3.

[32] *Id.* at 159.

[33] *Id.* at 159-174.

[34] 但手機使用者不小心跨錯空間、傳錯訊息的悲劇，亦不罕見。例如：作弊 LINE 答案罩同學 忘了老師也在群組裡，蘋果日報，2015 年 6 月 24 日，http://www.appledaily.com.tw/realtimenews/article/new/20150624/634503；北市官員上班傳股票訊息誤 LINE 柯文哲，中央社，2015 年 9 月 9 日，http://udn.com/news/story/3/1176498（最後瀏覽日：2016 年 1 月 12 日）。

一言以蔽之，手機徹底顛覆了人們對於「空間」的想像，除了使得人與人之間可以跨越時空限制直接通訊外，同時也賦予個人切割外在物理環境，建立內部空間、管領個人私密領域的能力。

2. 2. 2. 手機科技之負面影響

2. 2. 2. 1. 手機淪為制約個人之桎梏

再以手機的俗名而論，稱其為「手機」，實有兩個相互矛盾的意涵：一方面，手機可視為人類身體的延伸，由於通訊傳播能力的增強，時空對人的束縛與限制因此解除或削弱，人與人的溝通不再受到時間與地點的限制。惟就另一方面而言，手機卻也成了束縛、限制人的工具，作為社會網路與資訊通信體系的那隻手，牽引個人行動，將個人納編為網路身體與科技身體的一部分[35]。

James Katz 與 Mark Aakhus 兩位教授即指出，隨著通訊科技不斷發展，「永恆聯繫（perpetual contact）」的社會邏輯由是而生。換言之，自從手機這種行動通訊技術問世、漸次普及後，一種理想化的純粹通訊逐漸形成。藉由個人行動通訊裝置之助，人們想像自己能夠脫離身體的束縛，與其他人的心靈直接溝通，就像與天使交談一般[36]。

然而，正是因為人們對於永恆聯繫的想像，Sherry Turkle 教授認為，現今人們已經淪為「受束縛的自我（the tethered self）」。一方面，人們總是保持通訊裝置開機暢通（always-on），惟另一方面，這卻也使得個人總是處於隨時待命、可供他人聯繫的狀態[37]（always-on-you）。就此一層面以觀，正如 Paul

[35] 王佳煌（註 9），頁 2-3。
[36] James E. Katz & Mark A. Aakhus, *Conclusion: making meaning of mobiles – a theory of Apparatgeist*, in PERPETUAL CONTACT: MOBILE COMMUNICATION, PRIVATE TALK, PUBLIC PERFORMANCE 301, 307 (James E. Katz & Mark A. Aakhus eds., 2002).
[37] Sherry Turkle, *Always-on/Always-on-you: The Tethered Self*, in HANDBOOK OF MOBILE COMMUNICATION STUDIES 121, 121-22 (James E. Katz ed., 2008).

Levinson 教授所言，你我有如被手機囚禁於一個全時可及的牢房之中[38]（imprison us in a cell of omni-accessibility）。

手機對於個人的束縛與困綁，除了表現在「低頭族」氾濫的社會現實外，在工作上更是體現無遺。根據一項對國人的調查，隨著智慧型手機、通訊軟體與社群網站日益普及,除有六成多的受訪者表示自己24小時開著手機待命外，更有高達八成多的上班族曾在下班、放假時，繼續透過手機處理公務[39]。實際上更不乏有上司長期透過通訊軟體於下班後持續交辦工作，導致員工因深夜加班過勞死之情事[40]。

再以台北市政府為例，市長一方面要求各局處首長以手機通訊軟體 LINE 隨時回報最新狀況、24 小時內必須找到人，另方面亦要求每位公務員與約聘僱人員必須加入群組、「秒回」訊息[41]。市府人員則兢兢業業，無論深夜、休假、上廁所都被迫緊握手機，以免遺漏訊息或長官交辦的工作[42]。市長則自嘲自己有如小說《1984》裡的老大哥：「老大哥看著你們[43]！」自此以言，手機雖然帶來通訊上的便利，卻也使得個人必須隨時待命、供他人聯繫，如同手機牢房之中的囚犯，失去自由。

---

[38] PAUL LEVINSON, CELLPHONE: THE STORY OF THE WORLD'S MOST MOBILE MEDIUM AND HOW IT HAS TRANSFORMED EVERYTHING xiii (2004).

[39] 林絲蓉，2015 年 04 月 職場爆肝與壓力指數調查，yes123 求職網，https://www.yes123.com.tw/admin/white_paper/index_detail.asp?id=20150424160542（最後瀏覽日：2016 年 1 月 12 日）。

[40] 唐鎮宇，首例！ 通訊軟體加班族過勞死，蘋果即時，2014 年 6 月 27 日，http://www.appledaily.com.tw/realtimenews/article/new/20140627/423591（最後瀏覽日：2016 年 1 月 12 日）。

[41] 黃瀞瑩，通訊錄、LINE 全掌握柯文哲：局處長 24 小時都能找到人，ETtoday，2015 年 1 月 6 日，http://www.ettoday.net/news/20150106/447650.htm；陳瑄喻，登個沒完 北市府 LINE 到好焦慮，中時電子報，2015 年 1 月 26 日，http://www.chinatimes.com/newspapers/20150126000328-260114（最後瀏覽日：2016 年 1 月 12 日）。

[42] 林媛玲，柯 P 愛用 LINE 號令 局長如廁手機不離身，蘋果即時，2015 年 01 月 26 日，http://www.appledaily.com.tw/realtimenews/article/new/20150126/549215；謝幸恩，新北 29 區公所 LINE 群組 里長也來嗡嗡嗡，中時電子報，2015 年 7 月 15 日，http://www.chinatimes.com/newspapers/20150715000491-260102（最後瀏覽日：2016 年 1 月 12 日）。

[43] 「老大哥看著你們！」 柯文哲「盯」市政 line 不停，TVBS，2015 年 1 月 18 日 http://video.n.yam.com/20150118819564（最後瀏覽日：2016 年 1 月 12 日）。

Gergen 教授一方面認同手機之發展確實改變了人們社交互動的型態，另方面更指出「缺席的存在（absent presence）」因手機之出現而變本加厲：當我們聽著遠方的話語時，正意味著我們脫離了此時此地的現實，忽略了周遭實際的人們。身體看似在場，心神卻早已被另一個世界攫獲[44]。

生活在現代資訊社會的人們，對於手機制約人類生活的現象，或已司空見慣。在台灣，餐廳、車廂內、馬路邊低著頭滑手機的人群隨處可見，新聞媒體上亦充斥著人們以手機拍下的影像。在英國，人們以 phubber 稱呼那些在社交場合自顧自不斷滑手機的人[45]。而在美國，攝影師精準地捕捉到眾人皆醉我獨醒的一刻——明星強尼戴普出現在眼前，群眾為之瘋狂、人人忙著拿出手機拍照，只有一位老婆婆用自己的眼睛享受當下[46]。

圖四：「眾人皆醉我獨醒」

[44] Gergen, *supra* note 30, at 227-41.
[45] *2013's weird and wonderful words and phrases: Selfies joined by boiling the ocean, phubbing and buffling*, DAILY MAIL (Dec. 28, 2013), http://www.dailymail.co.uk/news/article-2530523/Forget-selfies-boiling-ocean-phubbing-buffling.html
[46] *Still living in the moment: Elderly woman pictured at a premiere becomes an online hero - because she was the only one NOT taking a picture of Johnny Depp*, DAILY MAIL (Oct. 5, 2015), http://www.dailymail.co.uk/femail/article-3260626/Elderly-woman-pictured-premiere-online-hero-one-NOT-capturing-scene-camera-phone.html

現代人忙著以手機拍照攝影的情節並不罕見：遇到飛機單邊引擎爆炸的事故，坐在灰煙瀰漫、氧氣罩掛下的機艙裡，有人選擇先掏出手機，將機艙內慌亂無章彷彿拍電影一般的場景錄下並上傳[47]，「手機錄影先於遵循指示」的情景一再上演[48]。震驚全台的高雄瓦斯氣爆案，也有不少居民並未於第一時間逃生避難，而是選擇待在氣爆現場，以手機紀錄下有如世界末日降臨，在火光中明滅的高雄市區[49]。

尤有甚者，眼見他人遇難受困時，附近人們的第一個想法，很可能不是快步趨前伸出援手，反而是隔岸觀火，先拿出智慧型手機錄影再說。英國曾發生孩童受困沙洲的事件，許多路人卻只忙著以手機錄影而不上前幫忙[50]；美國一起死亡車禍，現場一名目擊男子不僅不動手救人，甚至還闖進車內以手機拍攝垂死之傷者[51]。近日在八仙樂園發生的彩色派對粉塵爆炸事故，當時部分參與民眾看到渾身著火、尖叫奔跑的人群，第一反應不是衝上前去協助滅火，而是繼續以手機拍下有如煉獄的火場[52]。凡此種種，亦可窺見手機雖然解放了空間對於人們的限制，卻成為另一種型態的桎梏。

---

[47] Alex Williams, *A Defining Question in an iPhone Age: Live for the Moment or Record It?*, THE NEW YORK TIMES (Sep. 26, 2014), http://www.nytimes.com/2014/09/28/fashion/a-defining-question-in-an-iphone-age-live-for-the-moment-or-record-it.html

[48] 彭惠筠，國泰客機突冒煙霧迫降 旅客錄影直擊，TVBS，2015 年 8 月 2 日，http://news.tvbs.com.tw/world/news-610646；航班冒煙迫降 「衝向大海」全都錄，世界新聞網，2015 年 7 月 31 日，http://www.worldjournal.com/3361266（最後瀏覽日：2016 年 1 月 12 日）。

[49] 高雄氣爆 民眾紀錄驚恐瞬間，蘋果即時，2014 年 8 月 1 日，http://www.appledaily.com.tw/realtimenews/article/new/20140801/443908（最後瀏覽日：2016 年 1 月 12 日）。

[50] 英國兒童困沙洲 冷血路人只顧手機錄影，中央通訊社，2015 年 4 月 13 日，http://www.cna.com.tw/news/firstnews/201504130379-1.aspx（最後瀏覽日：2016 年 1 月 12 日）。

[51] 光拍片不救人！車禍目擊男子遭逮捕，TVBS 新聞，2015 年 7 月 17 日，http://news.tvbs.com.tw/world/news-608309/（最後瀏覽日：2016 年 1 月 12 日）。

[52] 八仙樂園意外 起火瞬間影片曝光，自由時報，2015 年 6 月 27 日，http://news.ltn.com.tw/news/society/breakingnews/1361442（最後瀏覽日：2016 年 1 月 12 日）。

2. 2. 2. 2. 手機作為集體監視之媒介

反烏托邦小說《1984》中，人人彼此監視的虛擬世界，在現實世界中是否有可能具體實現？知名評論家 Howard Rheingold 曾撰寫《聰明行動族》一書，書內即提及：

「如果有一天，數百萬人在日常生活中穿戴著配備感應器的可穿戴電腦，這些人本身就會變成集體的監視者：人人都是「老大哥[53]」。」

此情此景實已發生於現實社會。例如新北市交通警察大隊早於 103 年 7 月即推出「交通違規檢舉系統」，線上受理民眾檢具照片或錄影等證據檢舉交通違規；其後又為因應智慧型手機普及，更進一步推出手機應用程式：「iPolice」，提供民眾以手機直接檢舉交通違規。該市交通警察大隊即自豪地表示：「雖然交通警察無法隨時出現，但小心鏡頭就在你身邊[54]。」此語儼然將人民（與隨身手機）比擬為老大哥。

動物保護的議題也沒有自外於手機 App 的發展浪潮，動物保護專屬的 App 由是而生。台北市動物保護處於 2015 年 7 月推出「臺北市動物福利」之應用程式[55]、同年 9 月更增加「動物保護報案」功能，讓民眾能即刻將動物受虐或遭棄養的照片或影片上傳，再結合智慧型手機的定位功能，使動物保護檢查員即時獲知動物受虐或遭棄養之位置，立刻前往處理[56]。

警方也設計出一套人臉辨識比對之手機應用程式：M-Police。該應用程式

---

[53] Howard Rheingold 著，張逸安譯，《聰明行動族：下一場社會革命》，頁 295（2010 年）。
[54] 交通違規檢舉 手機嘛ㄟ通，新北市政府警察局交通警察大隊，2015 年 1 月 8 日，http://www.traffic.police.ntpc.gov.tw/cp-909-8951-27.html（最後瀏覽日：2016 年 1 月 12 日）。
[55] 何宜，檢舉動保案件　手機 APP 線上報案，台灣動物新聞網，2015 年 9 月 1 日，http://www.tanews.org.tw/info/8779；段楚禎，寵物走失不再土法煉鋼 APP 快速通報協尋，卡優新聞網，2015 年 9 月 3 日，http://www.cardu.com.tw/news/detail.php?nt_pk=28&ns_pk=26860（最後瀏覽日：2016 年 1 月 12 日）。
[56] App 推新功能　方便民眾通報受虐、遭棄養的動物，今日新聞，2015 年 9 月 3 日，http://www.nownews.com/n/2015/09/03/1802925（最後瀏覽日：2016 年 1 月 12 日）。

系統與全民身分證與護照之照片資料庫相連結，可將拍攝之照片與資料庫中照片加以比對，辨識身分。警方只要輸入帳號密碼登入系統，再拿著手機對準人臉照相，應用程式即會自動測量照片中人臉眼耳鼻口四個特徵點的距離，再連至照片資料庫中將所攝照片與資料庫中照片予以比對、自動辨識照片中人的身分並呈現身分資料。有了此一應用程式之協助，即使民眾不願配合調查，警方只要直接拍照，即可利用系統比對、辨識民眾真實身份[57]。

此外，手機亦發展出類似電子腳鐐的監視功能。例如 LINE 公司於 2015 年 8 月推出「LINE HERE」的手機追蹤應用程式，可以建立所謂的「位置分享群組」，透過手機 GPS 定位功能，與他人分享自己所在位置。往好處想，此一功能使朋友相約聚會時更方便在人潮中找到彼此、掌握每個人的位置，無須再在電話裡雞同鴨講；但往壞處想，此一功能卻也可能被不當濫用，例如老闆藉此監視員工、男女朋友間互相監視行蹤、檢警用以監視嫌疑犯等。

此外，移民署也於 2015 年推出「晶片防偽居留證查驗 APP」，開放個人下載至手機，隨身攜帶查驗[58]。這套應用程式讓手機使用者得以隨時拍攝證件條碼、輸入相關資料完成驗證，並選擇是否進一步調閱相片，查核外勞、外配及外國人持有之證件真偽。移民署甚至利用 NFC[59]技術，只要行動裝置有 NFC 功能且載有此一 APP，手機只需貼近 103 年以後發行的晶片居留證，即可自動

[57] 相關新聞參見郭建盟，人臉辨識系統已監控全民，蘋果即時，2014 年 5 月 20 日，http://www.appledaily.com.tw/realtimenews/article/new/20140520/400606；人臉「辨識神器」 警靠手機查身分辦案，東森新聞，2014 年 5 月 7 日，https://tw.news.yahoo.com/%E4%BA%BA%E8%87%89-%E8%BE%A8%E8%AD%98%E7%A5%9E%E5%99%A8-%E8%AD%A6%E9%9D%A0%E6%89%8B%E6%A9%9F%E6%9F%A5%E8%BA%AB%E5%88%86%E8%BE%A6%E6%A1%88-022819940.html；黃村杉，結合手機照像功能 警方辦案新利器「人臉辨識系統」，NOWnews，2014 年 3 月 21 日，https://tw.news.yahoo.com/%E7%B5%90%E5%90%88%E6%89%8B%E6%A9%9F%E7%85%A7%E5%83%8F%E5%8A%9F%E8%83%BD-%E8%AD%A6%E6%96%B9%E8%BE%A6%E6%A1%88%E6%96%B0%E5%88%A9%E5%99%A8-%E4%BA%BA%E8%87%89%E8%BE%A8%E8%AD%98%E7%B3%BB%E7%B5%B1-125946764.html（最後瀏覽日：2016 年 1 月 12 日）。

[58] 張企群，手機就能辨真假 移民署推「查驗居留證 APP」，中時電子報，2015 年 6 月 21 日，http://www.chinatimes.com/realtimenews/20150621002680-260402（最後瀏覽日:2016 年 1 月 12 日）。

[59] Near Field Communication，近距離無線通訊。載有此技術之電子設備，可於十公分以內之距離進行非接觸式點對點資料傳輸。

讀取晶片內容，判斷證件的有效性[60]。

移民署表示，此一 APP 之開發，旨在提升行政效率、有效管理、避免外籍人士逾期未換證。勞工團體對此強烈抗議，認為移民署明顯歧視特定族群、將外國人均視為有可能非法居留之嫌疑犯，將屬於個人、只有公權力單位能查驗的資訊，開放給所有人，使人人均可查驗嫌疑者的證件，讓每個人都變成查緝逃逸外勞之幫手，非但有警察國家復辟之嫌，移民署此舉更變相鼓勵全民成為老大哥，時時監控藍領移工，鼓吹並動員人民以懷疑的眼光看待不同國籍跟種族的人，加強監視、檢查外貌看似來自東南亞等第三世界國家的移動勞工，強化對勞工與移民的歧視[61]。

2. 3. 小結：手機引發的生活變革與監控風險

由本章之討論可知，行動通訊的進步、智慧型手機的普及，確實相當程度地為人們的生活型態帶來變革。手機讓人們跨越了時空的藩籬、擺脫以往通訊所受之空間地點的限制，將人與人之間的面對面溝通予以延伸，方便人們傳遞訊息、與親友連絡感情，自由管理私領域之親疏遠近。

手機同時也徹底改變人們對於「空間」的想像，除了打破此／彼、遠／近、在場／不在場的二分外，亦使個人得自外於外在物理環境、創設一獨特的內部空間，在其內自由休憩。現代人想休息的時候未必會回到家裡，或許窩在咖啡廳中的某個角落，在手機所創設之精神空間內略事喘息，反倒令人自在。

[60] 移民署，外僑晶片居留證效期 智慧型手機隨時查，內政記事本，2015 年 3 月 23 日，http://www.moi.gov.tw/chi/chi_moi_note/moi_note_detail.aspx?sn=849（最後瀏覽日：2016 年 1 月 12 日）。

[61] 相關新聞與評論參見 TIWA，飄零與人權》老大哥正在看著你，自由評論網，2015 年 9 月 29 日，http://talk.ltn.com.tw/article/breakingnews/1459879；王顥中，移民署推 APP 查外勞 假便民真歧視 移工團體批 鼓勵全民當警察，苦勞網，2015 年 10 月 6 日，http://www.coolloud.org.tw/node/83602（最後瀏覽日：2016 年 1 月 12 日）。

惟手機卻也有如一把雙面刃，載舟之餘亦能覆舟。其賦予人們跨越時空限制隨時連絡的便利性，卻也同時導致個人所受制約加劇，除了造就大量的低頭族外，上班族也被迫「公私不分」、「24 小時待機」。即使下了班、離開公司仍無法享受完整的私人時間，依舊深受工作的綑綁與束縛，個人私領域受侵入之境況愈顯嚴重，永無安寧。人們得隨時注意手機有沒有響起、自己有無漏讀重要訊息，淪為手機的奴隸，遭囚於 Levinson 教授所比喻的手機牢房之中。

再就手機作為監視媒介的角色而論，國家借用人民力量，鼓勵人民成為老大哥之延伸手足，以手機舉報交通違規與虐待動物、利用手機應用程式加強移工管控是類作法，實值吾人警惕。以移民署晶片查驗 App 為例，今日受此應用程式影響之主要受監控者係外籍移工，然而，將來是否會擴及你我？

進步言之，今日國家既可打著便民服務、管控外勞之名目，鼓吹人民下載手機 App 檢查周遭的可疑移工，甚至在對方不知情的情況下以手機 NFC 功能感應晶片、取得資訊；則在我國人民全面換發晶片身分證[62]的明日，國家是否更可能以「打擊犯罪」為號召，開發出另一款「晶片犯罪人口查驗 APP」，鼓勵人民使用手機時，順便查驗周遭看似可疑的犯罪分子，讓《1984》人人監控彼此的監視世界具體實現？為了安全、效率或其他目的，吾人對隱私之退讓與犧牲願意達到何種程度？實值深思。

[62] 內政部正在推動新版多合一的晶片身分證，此種身分證內建智慧晶片，期望將報稅、駕照、行照、健保卡、搭捷運、電子投票、電子錢包與自然人憑證等諸多功能悉數整合晶片身分證要不要「七合一」。詳見內政部：民眾可自行決定，ETtoday，2015 年 5 月 12 日，http://www.ettoday.net/news/20150512/505284.htm；Sanada Yukimura，台灣新版晶片身分證 2017 年上路？ 看全球 eID 趨勢，科技新報，2015 年 5 月 11 日，http://technews.tw/2015/05/11/taiwan-eid-2007（最後瀏覽日：2016 年 1 月 12 日）。

3. 手機科技引發的隱私權思考

本章奠基於前文對手機的認識，進一步深究手機科技與隱私權之間的互動關係。首先概述隱私權在美國與我國隱私權的發展過程、權利內涵以及保障面向，再自手機與隱私權的互動切入分析，探討手機如何與私領域之保護及個人人格形塑扣連，及其與資訊自主控制之間的關聯性。次就手機科技所引發的隱私權思考予以論述，探討手機科技如何衝擊傳統隱私權概念、手機資訊如何衍生剖繪監控風險等，進而提出本文對於手機資訊應否及如何受隱私權保障之見解，作為次章開展手機搜索與隱私保障具體案例之討論基礎。

3. 1. 隱私權之概念與發展

3. 1. 1. 隱私權於美國之發展

3. 1. 1. 1. 學者筆下的隱私權見解

在美國，無論憲法本文或增修條文，均無保障隱私權之明文。最早定義隱私權的專論[63]，一般以 1890 年波士頓的 Samuel Warren 與 Louis Brandeis 兩位律師[64]於哈佛法學評論合著之《The Right to Privacy》一文為宗[65]。該文採用美國法官 Thomas Cooley 的說法，將隱私權定義為「不受干擾的權利[66]（the right to be let alone）」，主張密室中的輕聲細語不應被宣揚，個人的思想、情緒與感受應予保障，以使人格不受侵犯[67]。文中亦指出，個人若自行或同意將事情公

[63] 實則，Warren 及 Brandeis 之前已有學者與判決提及隱私權，兩人見解亦受前此之討論影響，參見詹文凱，隱私權之研究，台灣大學法律學研究所碩士論文，頁 16-18（1998 年）。然而 Warren 及 Brandeis 此文為定義隱私權之首篇專論，故論及隱私權時多仍以兩人為宗。
[64] Brandeis 日後成為美國聯邦最高法院歷史上第一位猶太裔大法官。
[65] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193-220 (1890).
[66] *Id.* at 195.
[67] *Id.* at 211.

開發表，則不再受到隱私保護[68]。然而，由於美國實務的判決先例曾經否認隱私權，此等否定的見解仍影響著當時的法院，故此篇文章對實務判決的影響尚屬有限[69]。

1960 年，隱私權在侵權行為法上有了重大進展。William Prosser 教授於加州法學評論上以《Privacy》為題發表一篇專論，整理歷年來的法院案例，分析歸納實務上四種隱私權的侵害態樣──侵入（intrusion）、揭露私人事務（public disclosure of private facts）、誤導大眾（false light in the public eye）以及盜用（appropriation）[70]，嗣後將這四種侵害態樣編入美國法律協會所出版之侵權行為法整編第二版中，對該國實務影響深遠。Prosser 教授雖未正面回答「隱私權是什麼？」等涉及隱私權概念與內涵的根本問題，卻直接藉由實務案例中找尋侵害隱私權的態樣，從此奠定隱私權在侵權行為領域的基礎。

在 Prosser 教授提出隱私的四大侵害態樣之後，Edward Bloustein 教授撰寫了一篇文章回應該文[71]，強調隱私中人性尊嚴的面向，重申 Warren 與 Brandies 兩位律師所提出的「不可侵犯的人格（the inviolate personality）」。Bloustein 教授主張，侵害隱私等同於對個體性（individuality）、人性尊嚴（human dignity）的侵害。一個人如果被迫生活在監控之下，所有需求、想法、慾望、愛好與喜悅，每分每秒都必須受到公開檢視，他終將喪失自我而沒於大眾：異見不復提出、抱負不再遠大，失去屬於個人的獨特感受，趨於一同，不再是個獨特的個體[72]。

哈佛法學院的 Charles Fried 教授亦抱持類似見解，撰文指出，如果我們的每一個字和每個舉動都被公諸於世，為免被別人否定或甚至遭到報復，我們可

[68] *Id.* at 218.
[69] 詹文凱（註 10），頁 20-25。
[70] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
[71] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser,* 39 N.Y.U. L. REV. 962, 971 (1964).
[72] *Id.* at 1003.

能再也不願意發表任何意見或從事某些活動[73]。

繼上述幾位首開隱私權討論先河之後，紐約大學 Helen Nissenbaum 教授亦於 1998 年撰文探討公共領域的隱私[74]。其跳脫以公開與否、公私領域劃分隱私有無的傳統，轉而強調隱私的「情境脈絡完整性[75]（contextual integrity）」：除了資訊本身以外，更應將個人揭露資訊時的情境納入考量。例如期待員工向雇主說明過去的工作狀況與教育程度或許是合適的，但同樣的情境下，要求揭露婚姻狀況或性傾向卻相當不妥[76]。人們往往是在情境完整性被破壞時，才會認為隱私遭受侵害，因此，考量隱私時不應脫離所屬情境，僵化地認為資訊一旦公開即不受隱私保障[77]。

對於隱私權討論熱烈、學說百花齊放的現象，Daniel Solove 教授則於 2002 年撰寫《Conceptualizing Privacy》一文，臚列各家對於隱私權所提出的見解，包括最原始的獨處權理論，乃至於限制近用、秘密、控制個人資訊、人格以及親密等[78]，此類見解無非探究隱私的範圍為何，劃出應受保障與不受保護之界線，惟 Solove 教授並不採同樣的權利形成方法。詳言之，傳統上學者均試圖尋覓隱私的核心概念，使其成為一獨特的權利，以與其他權利相區隔。然而，Solove 教授認為隱私的概念本就隨著時代不斷流動演進[79]，討論隱私的抽象意義無法解決實際的隱私問題，故其轉而採取實用主義的觀點，在《A Taxonomy of Privacy》這篇文章中，由隱私侵害所造成的「問題」出發，摒棄由上而下（top down）定義隱私的執念，由下而上（bottom-up）歸納出隱私侵害的四大門路：資訊蒐集、資訊處理、資訊傳布與決策干預，其下再細分為十六種子態樣，以

[73] Charles Fried, *Privacy*, 77 YALE L. J. 475, 483-84 (1968).
[74] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998).
[75] *Id.* at 581. 此譯名參考劉靜怡，社群網路時代的隱私困境：以 facebook 為討論對象，臺大法學論叢，41 卷 1 期，頁 9（2012 年）。*See also* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).
[76] Nissenbaum, *supra* note 74, at 582.
[77] *Id.* at 584-85.
[78] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1088, 1099-1124 (2002).
[79] *Id.* at 1132.

實際遭遇的問題與權利衝突為本，探究應受隱私權保障的範疇[80]。

上舉多位學者，均對隱私的概念內涵、隱私之功能以及侵害隱私權的態樣等等，提出自己的見解。雖然每個人對於隱私的詮釋與理解不同，但都認為隱私有其重要性，應受保護。然而，在肯定隱私的聲浪之外，並非沒有論者對隱私提出質疑與批評。

目前於美國第七巡迴上訴法院任職，同時任教於芝加哥法學院的 Richard Posner 法官在 1978 年撰寫《An Economic Theory of Privacy》一文，一如文章篇名所示，立足於經濟學觀察隱私。Posner 法官以經濟學之眼對隱私進行成本效益分析，將隱私視為達成其他目的之中介工具（intermediate），而不將其本身視作終極價值[81]（final goods）。在隱私庇蔭下，人們可以隱藏關於自身不利訊息的流動，例如員工可能會向雇主隱瞞自己身體的病況，未婚夫向未婚妻隱瞞自己不孕的事實等。Posner 法官並不贊成保護這類負面的資訊，因為個人隱藏這些資訊，通常是為了誤導別人不發現自己的錯誤、操縱他人對自己的看法，或者圖謀個人的經濟利益。限制這類真實訊息的揭露，反而會產生社會成本，造成無效率的情形。因此，Posner 法官對此持保留態度[82]。

而在 2008 年的《Privacy, Surveillance, and Law》文中，Posner 法官進一步將隱私利益分為兩種：純粹利益（pure interest）與工具利益（instrumental interest）。前者單純指的是隱藏個人資料，後者的重點則是著眼於防止資訊被用在不利於己之處。關於純粹利益，Posner 法官舉例，雖然確切原因未明，但許多文化中有著「裸露的禁忌（nudity taboo）」，人們傾向於隱藏自己的裸體，裸體遭人窺見時多會感到受傷或困窘。至於工具利益，則與名譽或評價的關係較為密切，例如向雇主隱瞞犯罪紀錄等，有著欺瞞、操控的成分在[83]。Posner

[80] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 478, 488-91 (2006).
[81] Richard A. Posner, *An Economic theory of Privacy*, REGULATION(MAY/JUNE) 19 (1978).
[82] *Id.* at 21-23.
[83] Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 245-46. (2008).

法官在本文中採取與前文相同的立場，重申自己不贊同保護後者（不利於己的資訊）之隱私，直率地寫出：「隱私是恐怖份子最好的朋友[84]（Privacy is the terrorist's best friend）。」

3. 1. 1. 2. 隱私權在司法實務之發展

誠如 Posner 法官所言，隱私很可能是恐怖份子最好的朋友。恐怖份子或罪犯很可能藏匿於隱私的保護傘下，暗地籌備違法勾當，免於警方監督。因此，法院面對紛至沓來的犯罪案件，必須在犯罪追訴與隱私保障的衝突間，戰戰兢兢、斟酌求取最適切的平衡點。該國隱私權之發展，確實也與法院歷次審理搜索扣押案件時，對憲法增修條文第四條意旨之闡釋密切相關。

3. 1. 1. 2. 1. 隱私權與憲法增修條文第四條

美國憲法對於搜索扣押之規範，見於增修條文第四條：「人民有保護其身體、住所、文件與財物之權，不受無理拘捕、搜索與扣押，並不得非法侵犯。除有正當理由，經宣誓或代誓宣言，並詳載搜索之地點、拘捕之人或收押之物外，不得頒發搜索票、拘票或扣押狀[85]。」

本條明確保障人民不受不合理之搜索扣押，並揭示搜索扣押應具令狀之基本原則：令狀發給必須基於相當理由，令狀之記載必須明確特定，且搜索扣押必須合理。一方面對警方搜索扣押之行為予以限制，另方面亦保障人民隱私。自本條反面解釋，若執法機關之行為非屬搜索或扣押，即不須符合該條所定要件。因此，美國法院常面對的問題，即為判斷執法機關之行為是否屬於搜索扣

[84] *Id.* at 251.
[85] "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."

押，而須受到憲法增修條文第四條之規範。

1928 年 *Olmstead v. United States*[86]一案，美國聯邦最高法院審理政府安裝竊聽器是否屬於搜索、竊聽所得證據是否應予排除而不得作為證據之議題。本案被告涉嫌非法持有、私運與販售酒類飲料，違反當時的國家禁酒法（National Prohibition Act）。警方為蒐集犯罪證據，未聲請令狀即於被告住處外裝設電話竊聽器，錄下被告與其同黨意圖販賣酒類的大規模計劃，成為日後審判的證據。被告則抗辯，警方安裝竊聽器之行為違反憲法增修條文第四條規定，證據應予排除[87]。

最高法院於本案採取較為保守的見解，將受增修條文保護的對象限縮於實體入侵。法院採用傳統的侵入法則（trespass doctrine），認為該案警方既未進入被告居所，安裝竊聽器之處亦非房屋的一部分，因此，警方既未搜索被告身體、扣押文件或實體物件，或是侵入被告之家宅，僅於屋外安裝竊聽器之舉，不屬於憲法增修條文第四條所稱之搜索扣押[88]。

惟本案最為後世所稱述的，反而不是判決書本文，而係 Brandeis 大法官所提出的不同意見書。Brandeis 大法官指出，竊聽本質上即侵犯隱私，因為電話線被竊聽時，電話兩端發話人與受話人的隱私均已受到侵害。兩人所有的通話內容，包括正當、機密以及有權不被洩漏的對話，都被警方竊聽。此外，監聽一個人的電話線路，也會同時監聽到所有他撥打給其他人，以及他人打給他的電話。著眼於此，竊聽所造成的隱私侵害，遠較協助收繳走私物品令（writs of assistance）與空白令狀（general warrant）更為深遠[89]。

Brandeis 大法官亦於意見書中闡明其對隱私的理解，其認為憲法對人民的

[86] Olmstead v. United States, 277 U.S. 438 (1928).
[87] *Id.* at 455-57.
[88] *Id.* at 466.
[89] *Id.* at 475-76.

保障並不僅限於有形的物質，更涵蓋人民的精神本質、情感以及思想。因此，憲法保障人民享有不受政府干擾的權力：

> **「制憲者致力於保障有利於人民追求幸福的條件。他們認識到人的精神本質、情感以及思想的重要性。他們知道，在物質裡只能得到生活中一部分的痛苦、喜樂與滿足。他們力求保護美國人的信仰、思想、情緒與感受。他們賦予人民不受政府干擾的權利——對文明社會的人民而言，這是一種最廣泛且最有價值的權利。為了保護這種權利，無論政府採用什麼手段，只要不正當地侵害個人隱私，都應被視為違反憲法增修條文第四條[90]。」**

最後，Brandeis 大法官進一步提醒，當政府立意良善時，經驗教導我們更應保持警惕、捍衛自由。居心不良的統治者意圖侵犯人民自由時，生而自由的人會很自然地排斥。善意、充滿熱誠卻缺乏瞭解的人，反而可能蠶食鯨吞，成為自由最大的隱患[91]。

3. 1. 1. 2. 2. 合理隱私期待判準之發展

Brandeis 大法官的少數意見，終於在 1967 年的 *Katz v. United States*[92]一案逆轉成為多數意見。聯邦最高法院大法官於本案揚棄傳統侵入法則（物理上是否侵入被告財產）的判準，明示擴張增修條文第四條的保障範圍，表示隱私權所欲保障者係「人」而非「場所」，被告對於自己在電話亭內之通話內容仍有隱私期待，重新將無形的電話監聽行為納入適用。一個人自願暴露於大眾面前

---

[90] *Id.* at 478. 中譯為作者自譯。

[91] *Id.* at 479.

[92] Katz v. United States, 389 U.S. 347 (1967). 本案被告 Katz 於洛杉磯連續打八次電話至邁阿密與波士頓下單賭博，違反聯邦法。聯邦警探為取得本案證據，未聲請令狀即在被告打電話之公用電話亭外裝設監聽設備與錄音之電子裝置，錄下被告打電話下單賭博的通話內容。被告主張無令狀下所取得之錄音違反憲法增修條文第四條之保障。下級法院採傳統侵入法則之見解，認為警方並未實體入侵被告所據之空間，從而不屬於搜索。

之事務，縱使其身處住家或辦公室，亦不屬於增修條文第四條所保障之對象；惟若有人不希望自己的行為公開，即使身處於公眾得進出之處（如本案之公用電話亭），亦受增修條文第四條之保障[93]。

Harlan 大法官於本案協同意見書中提出著名的「合理隱私期待（reasonable expectation of privacy）」判準，以此判定警方行為是否應受憲法增修條文第四條之限制。該判準有兩個審查要件：（一）個人已表現出對於隱私實際（actual）而主觀（subjective）的期待、（二）該期待對社會而言是合理（reasonable）的[94]。合理隱私期待之判準，並不執著於畫出一條固定的界線，抑或範定隱私權固有而不受侵犯的保障範圍，而係考量行為人之主觀期待，以及該期待是否被社會認為客觀合理，留給法官彈性裁量的空間。

Hanlan 大法官此一判準受到法院廣泛採用，成為日後處理隱私權問題之判斷準則。惟本判準並非完美無缺，學界仍有質疑聲浪，例如 Solove 教授即批評，當客觀環境如喬治歐威爾所著之《1984》一書中充滿監視時，人民反而會因客觀上並無隱私期待之可能，反而不得主張隱私權保障。若完全以當時社會多數人觀點作為判斷客觀期待之依據，而非追本溯源思考隱私權的保障目的，此一判準反而可能導致箝制隱私權之惡果[95]。我國學者陳仲嶙教授亦指出，本判準僅解釋某一隱私利益是否值得保護，卻未將相關的利益加以通盤權衡；對於「合理」的定義，本判準亦有循環論證之虞[96]。

自本案判決作成後，當法院必須審查政府行為與隱私侵害之爭議時，法官

---

[93] *Id.* at 351-52. 惟美國國會於 Katz 案判決後，隨即於 1968 年制定綜合犯罪防治及街道安全法（The Omnibus Crime Control and Safe Streets Act of 1968），以此規範有線監聽之授權與限制。國會於 1986 年進一步將其修訂為電子通訊隱私法（Electronic Communication Privacy Act，簡稱 ECPA），將原先對於電話監聽之管制，進一步擴張至電子通訊資料，提高搜索相關資訊的令狀要求，分別就尚在通訊過程之訊息與已儲存之通訊訊息，設立不同搜索門檻。已有為數不少的文獻撰文介紹 ECPA，本文於此不再贅述。

[94] *Id.* at 361.

[95] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 71-74 (2008).

[96] Chung-Lin Chen, *In Search of a New Approach of Information Privacy Judicial Review: Interpretation No. 603 of Taiwan's Constitutional Court as a Guide*, 20 IND. INT'L & COMP. L. REV. 21, 34-35 (2010).

往往會援用此一標準界定政府行為是否侵犯人民隱私權。若受搜索人依上述主客觀標準具有合理隱私期待，即得主張憲法上的隱私權而受增修條文第四條之保障，警方應取得令狀並遵循相關程序規範方得搜索；反之，則政府行為非屬搜索扣押，不須事先取得令狀。然而，法院亦承認數種情況的例外[97]，允許警方得在未取得令狀的情形下，即可進行搜索扣押，後文欲探討之附帶搜索，即為其中著例。

3. 1. 1. 2. 3. 第三人法則之例外

合理隱私期待之判準受到法院廣泛採用後，法院進一步發展出「第三人法則[98]（third-party doctrine）」，用以判斷個人之合理隱私期待是否受到侵犯。根據 *Katz* 案的見解，個人自願暴露於大眾面前之事務，即非屬增修條文第四條所保障之對象；換言之，個人對於自願向他人揭露之資訊，不得再主張隱私期待。法院據此發展出所謂的第三人法則：只要是自願向第三人揭露之資訊，個人對此即喪失隱私期待。從而，政府若向該第三人索取資訊，並不會構成隱私權之侵害。第三人法則相關判決，則以 *United States v. Miller*[99]與 *Smith v. Maryland*[100]兩案最為著名。

在 *Miller* 一案，被告所承租之倉庫失火，警消意外發現被告持有可釀酒之廠房、設備與酒類，且被告並未依法繳稅。兩週後，政府向被告所開戶之兩家銀行提示由檢察官（而非法院大陪審團）所核發之傳票，要求銀行提出被告之帳戶資料文件，兩家銀行爰提出之[101]。

---

[97] 如緊急搜索、同意搜索、邊界搜索等，然與本文所欲探討之主題較無關，此處不擬深究。
[98] 國內亦有學者稱其為「自願揭露法則（the knowing expose to the public rule）」加以討論。詳見李榮耕（2015），〈科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展〉，《國立臺灣大學法學論叢》，第 44 卷第 3 期，頁 889-891。
[99] United States v. Miller, 425 U.S. 435 (1976).
[100] Smith v. Maryland, 442 U.S. 735 (1979).
[101] United States v. Miller, 425 U.S. 435, 437-38 (1976).

Miller 與其他被告嗣後即因共謀參與違法商業交易罪遭起訴。被告主張，由於個人帳戶紀錄係供銀行於特定目的使用，個人對於此等紀錄應有合理隱私期待。本案傳票既非由法院核發，取證程序具有瑕疵，相關銀行帳戶資料係政府非法搜索扣押之產物，證據應予排除[102]。

本案上訴至最高法院後，執筆多數意見之 Powell 大法官指出，系爭文件係銀行持有之「商業紀錄」，係銀行依銀行法規所須保存之紀錄，而非被告的「私人文件」，故被告不得主張相關文件之所有權。亦即，銀行存款戶對銀行所存之紀錄，不得主張受憲法增修條文第四條之保障[103]。

法院強調，個人對於明知揭露於外之資訊，不具合理隱私期待。銀行支票係屬商業交易中可轉讓之文件，財務報表、存款憑條等文件則係個人自願透露給銀行之資訊。存款戶向銀行揭露此類資訊，同時也承擔銀行會將該等資訊揭露予政府之風險。因此，被告不得主張受憲法增修條文第四條之保護[104]。

Smith v. Maryland 案則與電話有關[105]。本案多數意見係由 Blackmum 大法官主筆，爭點則在於被告對於所撥出的電話號碼有無合理隱私期待。判決書指出，本案之撥號記錄器係安裝於電信業者之中央辦公室，物理上並未侵入被告之財產。至於合理隱私期待之有無，法院則認為，本案之撥號記錄器與 *Katz* 案中之竊聽器截然有別，因撥號記錄器並未紀錄通訊內容、對話者之身分或通

[102] *Id.* at 438-39.
[103] *Id.* at 440-41.
[104] *Id.* at 443-45.
[105] Smith v. Maryland, 442 U.S. 735 (1979). 本案警方接到被害人報案遭搶，被害人則告知警方有關嫌犯及其所駕駛車輛之描述。被害人於事後又接到恐嚇及色情騷擾電話，來電者自稱係搶案之嫌犯。警方依被害人之陳述追蹤車牌號碼，得知車主係本案被告 Smith。警方未事先取得令狀或法院命令，即找來電信業者安裝撥號記錄器（pen register）記錄被告於家中撥出之電話號碼。紀錄顯示被告家中電話曾撥話至被害人之電話，警方爰以此聲請被告住處之搜索票，並於搜索後發現電話簿上關於被害人那頁被摺起。警方因而逮捕被告，嗣後再由被害人指認，確定為搶案犯嫌。被告後因搶劫罪名遭起訴，惟被告主張，警方並未取得法院令狀即擅自安裝撥號記錄器，由是衍生之證據應全數予以排除。

話是否完成等，僅紀錄撥打的電話號碼，設備功能有限[106]。

法院指出，電話用戶均應明白，個人必須向電信業者揭露所欲撥打之電話號碼，電信業者始能接通電話。此外，用戶亦應知道電信業者為確認每月的長途電話費用，會永久保存用戶所撥打的電話號碼，而保存這些資訊也符合各種正當合理的商業目的。於此情形，法院認為電話用戶對於自己所撥打的電話號碼不具有合理隱私期待。法院亦指出，無論身處何地，被告均須提供所欲撥打之電話號碼予電信業者，始得成功通話，故撥打電話之地點並非所問。本案被告即使在個人住宅內撥打電話，也只能認為被告欲將通話內容保密，保密範圍並不包含所撥打之電話號碼[107]。

法院引述 *Miller* 案，主張個人對於其自願提供給第三者的資訊，不得主張合理隱私期待；即使被告主觀上對其所撥打之電話號碼具有隱私期待，客觀上社會也不會認為此等期待係屬合理。憲法增修條文第四條並未禁止政府向第三人取得個人自願向該第三人透露之資訊，即使該等資訊係因特定目的提供予該第三人，且個人認為第三人不會背叛亦然，個人應自行承擔此等資訊遭揭露的風險。於本案，被告既然自願揭露所撥打之電話號碼予電信業者，被告即應自行承擔電信業者可能將資訊揭露予警方的風險[108]。因此，法院認定本案被告對所撥出之電話號碼不得主張隱私期待，警方安裝撥號記錄器即非「搜索」，從而不須令狀[109]。

然而，Marshall 大法官於本案不同意見書中指出，電話通訊在個人及職業關係中扮演著關鍵角色。打電話的隱私，不只對於參與犯罪活動者重要，不受限的政府監控，無疑也會困擾沒有違法情事需要隱藏的人。許多個人，諸如不受歡迎的政治團體成員、具有秘密消息來源的記者，常理而言也會避免揭露自

[106] *Id.* at 740.
[107] *Id.* at 743.
[108] *Id.* at 743-44.
[109] *Id.* at 745-46.

己的往來對象。若容許政府無須達到相當理由之門檻即可取得電話記錄，可能會阻礙某些政治結盟，以及作為真正自由社會指標的新聞工作[110]。

其引 *Katz* 案之話語：「對於一個進入公共電話亭的人，有權認為自己向話筒吐露的字句不會向世界播送」，則同理可證，個人亦應可假定其於家中所撥出之電話號碼，縱使紀錄下來，也僅限於電信業者商業目的之用。Marshall 大法官認為，執法人員向電信業者調取不在政府手中的的通話資訊之前，必須先取得法院令狀[111]。

Miller 與 *Smith* 兩案之多數意見，即為第三人法則（個人只要自願向第三人揭露資訊，即喪失隱私期待）之體現。

3. 1. 1. 2. 4. 馬賽克理論之提出與第三人法則之檢討

隨著科技創新腳步飛馳，各種蒐集個人資訊的手法日新月異，對隱私的侵害亦甚囂塵上。法院面對層出不窮的新科技，應如何在前人所訂的法律條文與既定法則下，做出因時因地制宜的解釋，即為一大挑戰。2012 年 *United States v. Jones*[112]一案，法院即必須面對全球定位系統（Global Positioning System，簡稱 GPS）此一新科技對個資蒐集與個人隱私所帶來的衝擊。

本案被告 Antoine Jones 係華盛頓區一間夜店的經營者，因涉嫌販賣毒品遭到警方鎖定。本案警方事先取得裝設 GPS 追蹤器、時限十天且範圍僅限於哥倫比亞特區之令狀，惟警方拖到第十一天才在車下安裝一枚追蹤器，且地點跨到鄰近的馬里蘭州，之後持續追蹤被告長達二十八天，無論追蹤時間或地點均逾越最初令狀聲請的範圍。被告主張 GPS 之定位資訊因違反憲法增修條文第四條應予排除，政府則認為個人在公共道路的行車資訊係自願暴露於公眾眼光

[110] *Id.* at 751.
[111] *Id.* at 752.
[112] United States v. Jones, 132 S.Ct. 945 (2012).

下，無隱私期待可言[113]。

因此，本案爭點在於，自逾越令狀授權範圍之第十一天起，政府安裝 GPS 於被告車底、紀錄被告車輛行蹤之行為，是否該當於憲法增修條文第四條所稱之搜索？

如前所述，面對此等涉及個人隱私與搜索扣押的爭議，最高法院最早之 *Olmstead* 等案採用侵入法則判斷是否為搜索。自 *Katz* 案以降，則改採合理隱私期待之判準，以主客觀標準決定當事人有無隱私期待，以此判斷政府行為是否屬於搜索。然而，面對新興之 GPS 追蹤科技，多數意見執筆者 Scalia 大法官強調，*Katz* 案的合理隱私期待理論，僅係補充而非取代傳統的侵入法則。因此，法院認為本案沒有必要處理合理隱私期待有無的議題，直接重拾 *Olmstead* 案的侵入法則，以裝設於車底的追蹤器為切入點，認定本案政府行為已實際侵入了被告之財產，構成搜索[114]。

本案多數意見採取傳統的侵入法則，技巧性避開了被告對於公共場合的行蹤有無合理隱私期待的議題，遭到少數意見的批評。Alito 大法官與其他三位大法官共同提出協同意見書，開宗明義即指責多數意見竟採用十八世紀的侵權法處理二十一世紀的監視科技，如此一來，政府之後若採其他手法監控個人行蹤（如僅傳輸電子訊號而無實體侵入），本案判決便無用武之地[115]。

對於 GPS 科技所引發之爭議，Alito 大法官主張應將長期追蹤與短期追蹤區別處理。Alito 大法官認為，短期監控一個人在公共街道上的行為，尚在社會可接受的合理範圍內。然而，本案中，執法機關以 GPS 追蹤監控被告開車時所有的行蹤長達四週，實已超出社會期待的合理範圍，從而侵害個人的合理

[113] *Id.* at 950.
[114] *Id.* at 950-52.
[115] *Id.* at 957-58.

隱私期待、構成搜索，應取得令狀始得為之[116]。

Alito 大法官的意見，應係受下級法院所提出的馬賽克理論（mosaic theory）影響。下級法院認為，整體大於個別的總和（that whole reveals more—sometimes a great deal more—than does the sum of its parts），關於個人的個別片段資訊，如同一片片馬賽克的小拼圖，個別資訊所透漏的訊息雖屬有限，惟所有資訊碎片如果被拼湊起來，便能呈現個人的生活全貌，更全面地透露一個人的一切，例如一個人經常做些什麼、不做什麼，及其整體的生活[117]。

站在多數意見關鍵票的 Sotomayor 大法官[118]，在其單獨提出的協同意見書中，先是同意 Alito 大法官應採合理隱私期待處理本案的見解，但其並不完全同意 Alito 大法官關於長期監視的意見。Sotomayor 大法官指出，監視時間長短實非緊要，即使是短期的無令狀監視，其合憲性亦有疑慮，因短期監視仍會透露一個人的許多訊息，例如至精神科、整形外科、墮胎診所或愛滋病治療中心就診，造訪脫衣酒吧、拜訪刑事辯護律師、去汽車旅館休息、參加工會會議、去清真寺、猶太教會堂或教堂，乃至於同志酒吧等，對隱私亦侵害不淺[119]。

除了短期監視可能造成的隱私疑慮外，Sotomayor 大法官進一步對第三人法則提出質疑：於現今數位時代，人民必須向第三方揭露種種資訊以遂行生活瑣事，但即使人民向業者揭露自己撥打的電話號碼與簡訊、造訪的網頁、電子郵件信箱、以及網上購買的書籍、商品與藥物等，不應逕將人民為特定目的而

---

[116] United States v. Jones, 132 S.Ct. 945, 964 (2012).

[117] United States v. Maynard, 615 F.3d 544, 558-562 (D.C. Cir. 2010). 相關評論參見 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012). 然 Kerr 教授對馬賽克理論持保留態度，主張法院應拒絕適用。其認為，之所以發展出馬賽克理論，係為了在科技快速變遷的現況下，讓人民得以持續享有憲法增修條文第四條所賦予的保障。但若要靠法院的個案累積，必須費時數年，個案法則勢必趕不上科技進展的速度，且法官也未必有足夠的專業科技知識作出判斷。因此，仍應回到最開始 Katz 案所建立的合理隱私期待判準，方為較適切的解決之道。

[118] 美國聯邦最高法院第一位拉丁美洲裔女性大法官，自小於單親家庭中成長，住在政府補助的房屋裡，由母親撫養長大。Sotomayor 大法官於本案判決中投下至關重要的第五票，使多數意見成為多數。

[119] United States v. Jones, 132 S.Ct. 945, 955 (2012).

向某些人（如上舉業者）揭露的訊息，完全排除於憲法增修條文第四條的保護範圍之外[120]。

由於馬賽克理論的見解、對第三人法則之檢討等，僅於協同意見出現，對下級法院而言並無拘束力，故 *Jones* 案判決作出後，下級法院面對類似案件之時，意見兩極。以人民使用手機時所產生之基地台位址資訊（cell-site location information，簡稱 CSLI）為例，美國部分法院即維持第三人法則之立場，仍認為此等資訊屬於個人自願向第三人揭露之資訊，不得主張隱私期待。第四及第五巡迴上訴法院均曾判決位址資訊係屬商業紀錄，手機用戶既自願向第三方業者揭露此等資訊以撥打電話，不得再主張合理隱私期待，從而警方無令狀調閱是類位址資訊，亦無侵犯隱私可言[121]。

然而，第十一巡迴上訴法院於 *United States v. Davis* 一案則採不同見解，未逕予適用第三人法則，而係認定個人提供基地台位址資訊予電信業者時，並不知道自己會被追蹤，個人對此等位址資訊仍應享有隱私期待，故政府取得位址資訊前若未先聲請搜索票，即侵犯被告受憲法增修條文第四條保障之權[122]。然而，本案法院最終引用善意例外（good faith）原則，認為檢警係基於有效的法院命令（a court order）取得資訊，仍否決了被告排除證據之聲請[123]。

聯邦最高法院曾以相關議案已在國會審議為由，於 2015 年 11 月拒絕 *Davis*

---

[120] *Id.* at 957.

[121] In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611-614 (5th Cir. 2013). 本案下級法院判決政府向業者索取位址資訊違反個人合理隱私期待，惟此見解遭第五巡迴上訴法院駁回，表示位址資訊係個人明知且自願向第三人揭露、業者基於商業目的而記錄之商業紀錄，故個人對此不得主張隱私期待。第四巡迴法院亦曾同此見解，詳見 United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc). 其他評論可參考 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012); Orin Kerr, *Fourth Circuit adopts mosaic theory, holds that obtaining "extended" cell-site records requires a warrant*, THE VOLOKH CONSPIRACY (Aug. 5, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/05/fourth-circuit-adopts-mosaic-theory-holds-that-obtaining-extended-cell-site-records-requires-a-warrant; Yishai Schwartz & Andy Wang, *United States v. Graham: An Overview*, LAWFARE (Aug. 7, 2015); https://www.lawfareblog.com/united-states-v-graham-overview (last visited Jan. 12, 2016).

[122] United States v. Davis, 754 F.3d 1205, 1215-17 (11th Cir. 2014).

[123] *Id.* at 1217-18.

案被告所提出的移審令聲請[124]，直至近日 *Carpenter v. United States*[125] 一案，法院始同意移審。第三人法則之適用爭議、警方無搜索票調閱手機基地台位址資訊是否侵犯人民隱私權之相關問題，有望由本案統一見解。

3. 1. 2. 隱私權於我國之發展

3. 1. 2. 1. 隱私權於我國釋憲實務之沿革

遍覽我國憲法之基本權利條款，並未明文對於隱私權有所保障。惟憲法第 10 條規範人民居住自由，即蘊含人民居家安寧不受干預之保障[126]；憲法第 12 條則明示人民享有秘密通訊自由，亦有保障人民隱私之色彩。因此，隱私權有何獨特之處？應如何與其他現存的基本權利相區隔？是否真有必要將隱私權獨立上提至憲法層次而受保護，而非將其列為法律上權利即屬已足？憲法對此既無明文，隱私權之保障，有賴於釋憲實務演進生根。

隱私權在 1992 年首登我國憲法解釋之堂。大法官於釋字第 293 號解釋處理銀行法限制公開人民存放款等財務資訊時，首次於解釋中提及「隱私權」，指出銀行法規定「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[127]」。惟本號解釋對於我國隱私權之實質內容、保障範圍，乃至於隱私權究屬於法律上權利或憲法上權利，未置隻字。

其後，釋字第 509 號解釋再度提及隱私權。大法官於本號解釋處理刑法第

[124] Todd Ruger, *Supreme Court Passes on Cell Phone Tracking Case*, Roll Call (Nov. 9, 2015), http://www.rollcall.com/news/supreme_court_passes_on_cell_phone_tracking_case-244691-1.html.
[125] 詳見 United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016). 本案爭點即為個人手機通訊的基地台位址資訊是否屬於個人自願向電信業者揭露之資訊，從而不得主張隱私期待。第六巡迴上訴法院認為，此等資訊係個人自願揭露，應適用第三人法則，個人對此不得主張合理隱私期待。本案現已由聯邦最高法院大法官審理中。
[126] 釋字第 443 號解釋理由書：「憲法第十條規定人民有居住及遷徙之自由，係指人民有選擇其居住處所，營私人生活不受干預之自由……」
[127] 釋字第 293 號解釋文參照。

310 條誹謗罪規定是否違憲之議題，其肯認言論自由受憲法明文保障，惟仍需與個人名譽、隱私及公共利益予以權衡，得出本罪並不違憲之結論。大法官雖於本號解釋中再度提及「隱私[128]」，然與前次解釋相同，對於隱私的實質內涵為何，並未多加著墨。

而在討論警察實施臨檢之規定是否違憲之釋字第 535 號解釋，大法官認為路檢、盤查等臨檢手段，屬於對人或物之查驗、干預，對於人民行動自由、財產權及隱私權等影響甚鉅，惟臨檢所依據之警察勤務條例有欠完備，有關機關應通盤檢討訂定相關法規，最終促成現行的警察職權行使法。大法官雖於本號解釋再次提及「隱私權」三字[129]，然與前兩號解釋一般，本號解釋仍未觸及隱私權的內涵，亦未明示隱私權為憲法所保障基本權之列。

到了釋字第 554 號，大法官所應對的則是廢除通姦罪的聲浪：刑法第 239 條對通姦、相姦者處以罪刑，是否違憲？本號解釋明確宣示婚姻制度受憲法制度性保障，為確保婚姻制度之存續與圓滿，性行為之自由應受制約。且通姦罪為告訴乃論，又附加經配偶縱容或宥恕者不得告訴之條件，難謂違背憲法比例原則之要求。本號解釋之理由書中指出，將通姦罪列為告訴乃論，使受害配偶得兼顧夫妻情誼及隱私，避免通姦罪之告訴反而造成婚姻、家庭之破裂[130]。惟理由書中仍未就隱私的實質內涵，夫妻間的隱私究何所指等予以深究。

---

[128] 釋字第 509 號解釋文：「言論自由為人民之基本權利，憲法第十一條有明文保障，國家應給予最大限度之維護，俾其實現自我、溝通意見、追求真理及監督各種政治或社會活動之功能得以發揮。惟為兼顧對個人名譽、隱私及公共利益之保護，法律尚非不得對言論自由依其傳播方式為合理之限制……」

[129] 釋字第 535 號解釋文：「警察勤務條例規定警察機關執行勤務之編組及分工，並對執行勤務得採取之方式加以列舉，已非單純之組織法，實兼有行為法之性質。依該條例第十一條第三款，臨檢自屬警察執行勤務方式之一種。臨檢實施之手段：檢查、路檢、取締或盤查等不問其名稱為何，均屬對人或物之查驗、干預，影響人民行動自由、財產權及隱私權等甚鉅，應恪遵法治國家警察執勤之原則……」

[130] 釋字第 554 號解釋理由書：「……矧刑法就通姦罪處一年以下有期徒刑，屬刑法第六十一條規定之輕罪；同法第二百四十五條第一項規定，通姦罪為告訴乃論，使受害配偶得兼顧夫妻情誼及隱私，避免通姦罪之告訴反而造成婚姻、家庭之破裂；同條第二項並規定，經配偶縱容或宥恕者，不得告訴，對通姦罪追訴所增加訴訟要件之限制，已將通姦行為之處罰限於必要範圍，與憲法上開規定尚無牴觸。」

直到 2004 年，面對立院調查權之行使與真調會條例之爭議，大法官作出釋字第 585 號解釋，闡明立法院行使調查權時若涉及限制隱私權等基本權利，除須有法律依據外，亦須符合憲法上比例原則、法律明確性原則與正當法律程序之要求。大法官於本號解釋理由書中首次清楚肯認，我國憲法雖未明文保障隱私權，隱私權仍係受憲法第 22 條概括條款所保障之人民基本權利[131]。

緊接著於兩天後公布的釋字第 586 號解釋，大法官於審理證管會（即今證期會）訂頒之取得股份申報要點是否違憲時，承襲前述第 585 號解釋之見解，進一步提出「資訊自主權」之用語，認其受憲法所保障，將之與財產權並列。由於系爭股份申報要點增加母法所未規範之申報義務，限制人民之資訊自主權與財產權，違反法律保留原則，因而違憲[132]。本號解釋特殊之處在於，大法官並未使用「隱私權」一詞，而係以「資訊自主權」稱之，惟解釋中未就資訊自主權與隱私權間之同異、資訊自主權之具體內涵為何予以闡明。

同年年底所公布之釋字第 587 號解釋，所處理之標的則係民法及判例禁止子女及親生父提出否認生父之訴是否違憲之議題。大法官於解釋理由書中追溯得提起否認生父之訴者僅限於夫妻一方而不包括子女之理由時，推斷原初設計或許係為避免子女涉入父母婚姻關係之隱私領域，暴露其生母受胎之事實，影響家庭生活之和諧；至於不許親生父親對受推定為他人之婚生子女提起否認之訴，也係為避免揭發他人婚姻關係之隱私[133]。本號解釋與釋字第 554 號類同，大法官均提及夫妻之間、婚姻關係中的隱私，然仍僅一語帶過，並未多言。

釋字第 603 號解釋則涉及核發身分證是否需按捺指紋之爭議。對此，大法官首先重申前述釋字第 585 號解釋之意旨，宣示隱私權係受憲法第 22 條概括條款所保障之基本權利，具有保障個人生活私密領域免於他人侵擾及個人資料

131 釋字第 585 號解釋理由書參照。
132 釋字第 586 號解釋文參照。
133 釋字第 587 號解釋理由書參照。

自主控制之功能。承此，大法官進一步闡釋後者的實質內涵，將個人自主控制資料之權利命名為「資訊隱私權[134]」。此外，本號解釋對於隱私權侵害之審查架構亦有所著墨，明示國家對資訊隱私權的侵害並非當然侵犯人性尊嚴，而應通盤衡酌考量，就具體個案採取寬嚴不同之審查[135]。本號解釋與第 585 號解釋對我國實務影響匪淺，法院審理隱私權侵害案件常援引解釋意旨[136]。

釋字第 631 號解釋則論及憲法第 12 條秘密通訊自由，事關通訊保障及監察法授權檢察官於偵查中得核發通訊監察書是否違憲之審查。大法官除重申前開第 603 號解釋保障隱私權之理由與功能外，亦首度表示「秘密通訊自由係憲法保障隱私權之具體態樣之一[137]」。本號解釋可謂隱私權與刑事程序與犯罪偵查最為密切的一號解釋。

釋字第 689 號解釋進一步討論個人於公共場合是否享有隱私權。本號解釋認為個人縱使進入公共場域，亦非完全喪失隱私期待，仍應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主。此外，大法官亦首度於解釋中明確引進美國實務「合理隱私期待」之概念及其主客觀要件，主觀上個人不受侵擾之期待需已表現於外，客觀上該期待須依社會通念認為合理，主客觀要件達致後，方受隱私權之保障[138]。

3. 1. 2. 2. 我國憲法隱私權保障內涵：私密領域、資訊自主

我國隱私權保障之實質內涵，係於司法院釋字第 585 號解釋所建立。大法

---

134 然學者對此亦有評論，認為並非所有個人資料均會涉及個人隱私，認應以「資訊自主權」取代「資訊隱私權」較為妥適，詳見李震山（2005），〈來者猶可追，正視個人資料保護問題─司法院大法官釋字第六○三號解釋評析〉，《台灣本土法學雜誌》，第 76 期，頁 222-234。

135 釋字第 603 號解釋理由書參照。

136 如高等法院 101 年度勞上易字第 8 號民事判決、高等法院 101 年度上字第 1337 號民事判決等。而在審酌是否發給法庭錄音光碟時，法官亦常引解釋意旨，認應採取嚴格解釋，如最高法院 101 年度台抗字第 878 號民事裁定、高等法院 99 年度上字第 819 號民事裁定等。

137 釋字第 631 號解釋理由書參照。

138 釋字第 689 號解釋理由書參照。

官於本號解釋理由書中清楚確立隱私權係受憲法保障之基本權利，復說明保障隱私權之理由，以及隱私權之權利內涵：

「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，並為保障個人生活秘密空間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[139]……」

由於人性尊嚴、維護個人主體性與人格發展之完整，亦為其他基本權如財產權[140]、名譽權[141]等所共通的基礎。因此，本號解釋對於隱私權的貢獻，除係大法官首次肯認隱私權係受憲法保障之基本權利外，更劃出隱私權有別於其他現存基本權之獨特內涵：隱私權係為保障「個人生活秘密空間免於他人侵擾」以及「個人資料之自主控制」而設。其為原先在基本權利系譜中定義稍嫌模糊的隱私權紮下根基，漸漸分化為與其他基本權利有所區別的一項獨特權利。

上舉「個人資料之自主控制」之實質內涵，於司法院釋字第 603 號解釋進一步奠定。本號解釋討論核發身分證需按捺指紋是否違憲時，首先重申前述釋字第 585 號解釋之意旨，宣示隱私權係受憲法第 22 條概括條款所保障之基本權利，具有保障個人生活私密領域免於他人侵擾及個人資料自主控制之功能。復闡釋後者實質內涵，揭櫫「資訊隱私權」的概念：

「就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料

---

139 釋字第 585 號解釋理由書參照。

140 如釋字第 400 號解釋文：「憲法第十五條關於人民財產權應予保障之規定，旨在確保個人依財產之存續狀態行使其自由使用、收益及處分之權能，並免於遭受公權力或第三人之侵害，俾能實現個人自由、發展人格及維護尊嚴。」

141 如釋字第 656 號解釋文：「名譽權旨在維護個人主體性及人格之完整，為實現人性尊嚴所必要，受憲法第二十二條所保障……」

記載錯誤之更正權[142]**。」**

本號解釋將個人自主控制資料之權利命名為資訊隱私權，復對隱私權侵害之審查架構有所著墨。國家對資訊隱私權的限制並非當然侵犯人性尊嚴，而應通盤衡酌考量，將國家蒐集、利用、揭露個人資訊所能獲得之公益與對資訊隱私之主體所構成之侵害予以權衡，就具體個案採取寬嚴不同之審查[143]。

大法官認為指紋具有人各不同、終身不變之特質，一旦連結個人身分，即具備高度人別辨識功能，有如完整個人檔案之鎖鑰。若指紋被國家建檔管理，足以成為得以監控個人之敏感性資訊，大法官爰於本案採嚴格審查基準，國家如以強制方法大規模蒐集國民指紋資訊，其資訊蒐集應屬與重大公益之目的之達成，具備密切關聯之侵害較小手段，並以法律明確規定之[144]。

司法院釋字第 631 號解釋，再度處理人民隱私保障與刑事偵查需求之間的互動關係。本號解釋涉及通訊監察的議題，就通訊保障及監察法授權檢察官於偵查中得核發通訊監察書之合憲性予以審查。大法官明示憲法第 12 條秘密通訊自由係憲法保障隱私權之具體態樣之一，旨在確保人民就通訊有無、對象、時間、方式及內容等事項，不受國家及他人任意侵擾，並重申此為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利。國家基於犯罪偵查之目的。國家若欲限制人民之秘密通訊自由，除應有法律依據外，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理、正當，方符憲法保障人民基本權利之意旨[145]。

---

[142] 釋字第 603 號解釋文參照。

[143] 釋字第 603 號解釋理由書：「隱私權雖係基於維護人性尊嚴與尊重人格自由發展而形成，惟其限制並非當然侵犯人性尊嚴。憲法對個人資訊隱私權之保護亦非絕對，國家基於公益之必要，自得於不違反憲法第二十三條之範圍內，以法律明確規定強制取得所必要之個人資訊。至該法律是否符合憲法第二十三條之規定，則應就國家蒐集、利用、揭露個人資訊所能獲得之公益與對資訊隱私之主體所構成之侵害，通盤衡酌考量。並就所蒐集個人資訊之性質是否涉及私密敏感事項、或雖非私密敏感但易與其他資料結合為詳細之個人檔案，於具體個案中，採取不同密度之審查。」

[144] 對於本號解釋審查標準的詳細評析，可參考 Chen, *supra* note 96, at 35-44.

[145] 釋字第 631 號解釋理由參照。

新興科技對隱私權所帶來的衝擊，則首次體現於司法院釋字第 689 號解釋對公共場合個人隱私之討論。大法官指出，資訊科技高度進步，使個人生活受到監控或揭露等侵擾的可能性倍增，若個人生活持續受到監視及揭露，即難以自由從事人際互動、言行舉止受限，致人格之自由發展受到影響[146]。

林子儀、徐璧湖大法官亦在協同意見書中進一步說明監控影響個人人格之理由：個人若知悉其被跟追或監看，往往會感受到被冒犯、憂慮甚至恐慌等情緒，言行舉止因監控而自我節制修正，個人之主體性與人格發展可能因此受到嚴重影響。而之所以將資訊自主權之保障自一般人格權中特別獨立，則肇因於資料處理之數位資訊科技日新月異、倍速發展，得以大量、迅速且無邊無際地搜集、彙整、儲存、傳遞與使用個人資料。新科技若遭濫用，對人民實有侵害之風險[147]。

本號解釋認為，個人縱使進入公共場域，亦非完全喪失隱私期待，仍應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主。此外，大法官亦首度引進美國實務「合理隱私期待」之概念及其主客觀要件：主觀上個人不受侵擾之期待需表現於外，客觀上該期待須依社會通念認為合理。主客觀要件合致後，方受隱私權之保障[148]。

本號解釋的特別之處在於，隱私權之有無，傳統上多採用所謂的「公私二分法」：亦即個人僅在私領域受有隱私保障[149]，公領域無從主張隱私權[150]。惟

---

[146] 釋字第 689 號解釋理由書：「個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響其人格之自由發展。尤以現今資訊科技高度發展及相關設備之方便取得，個人之私人活動受注視、監看、監聽或公開揭露等侵擾之可能大為增加，個人之私人活動及隱私受保護之需要，亦隨之提升。是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護。惟在公共場域中個人所得主張不受此等侵擾之自由，以得合理期待於他人者為限，亦即不僅其不受侵擾之期待已表現於外，且該期待須依社會通念認為合理者。系爭規定符合憲法課予國家對上開自由權利應予保護之要求。」

[147] 釋字第 689 號解釋，林子儀、徐璧湖大法官之部分協同及部分不同意見書參照。

[148] 釋字第 689 號解釋理由書參照。

[149] 如我國最高法院 93 年度台上字第 1979 號民事判決即明示隱私權係保障私領域之權利：「按**所謂隱私權，乃係不讓他人無端干預其個人私的領域之權利**，此種人格權乃是在維護個人尊嚴，保障

自本號解釋觀之，我國大法官在面對公領域有無隱私權時，雖引進美國法上合理隱私期待作為輔助標準，卻另闢蹊徑，明確採取與該國不同的操作方式，確立個人在公共場域仍得享有一定程度的隱私權保障，結論與美國迥異[151]。

綜觀諸號司法院大法官解釋，我國隱私權之地位，已由憲法未置隻字、妾身未明的舊況，躍昇為受憲法明確保障之基本權利。憲法維護隱私權的理由，在於維護人性尊嚴、個人主體性與人格發展完整，爰賦予人民個人生活秘密空間免於他人侵擾與自主控制個人資料的隱私權保障。

3. 1. 2. 3. 合理隱私期待與馬賽克理論之引進

美國合理隱私期待之判準，影響我國甚深。自憲法層次言，司法院釋字第689號解釋，即引進合理隱私期待之概念及其主客觀要件：若個人不受侵擾之期待已表現於外，且該期待依社會通念認為合理者，即應受隱私權之保障。但我國大法官操作該判準後，得出與美國不同的結論，認為個人在公共場域仍得享有一定程度的隱私權保障。該國第三人法則的見解，並不為我國採用。

此外，民事法院處理涉及隱私權的案件時，也不時操作合理隱私期待判準以審視隱私權侵害。我國學者林子儀教授曾統計，自民國92年至102年期間涉及隱私權的165件民事判決中，共有19件明確採用合理隱私期待作為判斷

追求幸福所必要而不可或缺者……」；台北地方法院92年度訴字第4312號民事判決亦稱：「人與人間共同生活之社會關係，可分為公領域與私領域，**人於私領域享有自我，歸屬自己。隱私權指一個人於其私人生活事務與領域享有獨自權（the right to be alone）**，不受不法干擾，免於未經同意之知悉、公開妨礙或侵犯之權利。」。

150 如於1890年《The Right to Privacy》一文，Warren與Brandeis兩位律師即認為個人若自行或同意將事情公開發表，則不再受到隱私保護，*See* Warren & Brandeis, *supra* note 65, at 218. 另，如前所述，1967年Katz v. United States一案，多數意見亦明確指出個人向公眾揭露之資訊不受保護；Harlan大法官的協同意見書亦提及，個人對於自行暴露在外之物件、活動或言談，業已喪失隱私期待，不得主張隱私權保護。詳參Katz v. United States, 389 U.S. 347 (1967).

151 然而，對本號釋字亦有批評聲浪，認其過於模糊抽象。如司改會發言人林峯正直言：「這次釋憲等於是空的，有講跟沒講一樣，未來記者採訪還是不知界線所在。」詳見張欽、孫友廉，釋憲淪空話 記者採訪仍霧煞煞，蘋果日報，2011年07月30日，http://www.appledaily.com.tw/appledaily/article/finance/20110730/33564233（最後瀏覽日：2014 年11月18日）。

隱私權是否存在之準則[152]。

至於刑事法領域，我國立法上不乏隱私秘密合理期待之文字，如通訊保障監察法[153]、警察職權行使法[154]等，均將合理期待入法。實務判決方面，學者亦曾統計，民國 92 年至 102 年期間涉及隱私權的 129 件刑事判決，其中有 25 件判決採合理隱私期待作為判準[155]。

我國刑事法院亦曾引用馬賽克理論作為論理依據。如臺灣高等法院審理司法警察未先取得令狀即私自安裝衛星定位追蹤器於人民車上是否構成隱私權侵害的案件時，即引介馬賽克理論作為裁判基礎：

> **「而此亦為美國法院近年來針對類似案件所採取之『馬賽克理論（mosaic theory）』（或譯為『鑲嵌理論』），即如馬賽克拼圖一般，乍看之下微不足道、瑣碎的圖案，但拼聚在一起後就會呈現一個寬廣、全面的圖像。個人對於零碎的資訊或許主觀上並沒有隱私權遭受侵害之感受，但大量的資訊累積仍會對個人隱私權產生嚴重危害。是以車輛使用人對於車輛行跡不被長時間且密集延續的蒐集、紀錄，應認仍具有合理之隱私期待[156]。」**
>
> **「他人之私密領域及個人資料自主，如在公共場域受到干擾，而超出可容忍之範圍，該干擾行為亦有加以限制之必要，俾有不受他人持續**

[152] 見林子儀（2015），〈公共隱私權〉，《第五屆馬漢寶講座論文彙編》，頁 43。
[153] 通訊保障監察法第 3 條第 2 項：「前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」
[154] 警察職權行使法第 11 條：「警察對於下列情形之一者，為防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動……」
[155] 林子儀（註 152），頁 43。
[156] 臺灣高等法院 104 年度上易字第 352 號刑事判決。本案上訴至最高法院後，其亦同意下級法院的見解，認為「即使個人身處公共場域中，仍享有私領域不被使用科技設備非法掌握行蹤或活動之合理隱私期待」，詳見最高法院 106 年度台上字第 3788 號刑事判決。

追蹤及侵擾之私人活動領域，而得保有『獨處之權利[157]』。」

由上開介紹可知，我國隱私權之論述，相當程度受到美國隱私權法制的影響，如合理隱私期待、獨處的權利、馬賽克理論等。然我國法院並未全盤認同該國法院的見解，而係在我國脈絡下發展出有別於該國的見解，如個人在公共場合仍享有隱私等。

經由本節之討論，我國隱私權保障發展過程與權利內涵之輪廓略為明朗，次節即以手機科技為中心切入分析，討論新興手機科技與隱私權之互動，及其對於傳統隱私權概念帶來哪些思考與挑戰。

3. 2. 手機科技與隱私

前一節已就隱私權在美國及我國之發展過程、權利內涵以及保障面向，做一概覽性的介紹。本節則自手機科技與隱私權的關聯著眼，深入探討手機科技與我國隱私權內涵——私領域之保護、個人人格形塑、資訊自主控制——之間的互動關係。

3. 2. 1. 手機科技與隱私

3. 2. 1. 1. 手機已由單純之資訊載體，躍居為個人精神寄託

我國憲法解釋明文將「個人生活秘密空間」納入隱私權保障之列，業已如前所述。在手機問世之前，家宅可說是個人最核心的私領域，係重要的個人生活秘密空間。以往，人們每天回到家中共進餐食，在家裡與家人或親友談論時事、抒發心事，得以在家中卸下在外一天的疲倦、脫下應對外人的面具，徹底放鬆，盡情地做自己，不受外人干預，言公開場合所不能言，論公共場所所不

[157] 同前註。

能論。賦閒時，則於家中招待親朋好友，談天說地，交流感情，發展個人親密關係。個人也可能如小說《1984》的情節一般，窩在家中某個角落，書寫個人的思想、疑問與抱負，復將文字藏匿於外人不得見之所。

然而，隨著時代演進，上開光景慢慢有了些變化。現代資訊社會中，人民生活型態改變：賃居人口眾多、工作早出晚歸（甚至徹夜未歸），家人間齊聚一堂共進餐食的頻率不再像以往頻繁，面對面問候聊天的機會也較以往減少。家，與其稱之為家，有時反而更像旅館，僅是個人梳洗過夜之所。

通訊科技的飛速進展，使人類跳脫時間地點的限制，讓人與人之間得以直接連結[158]。手機的出現，則讓人們得以自由創設有別於物理世界的內部空間，跳脫外界環境的紛紛擾擾。以往個人回到家中享受心靈上的平靜、遠離外界塵囂[159]，今日人們則在手機秘密空間內稍事喘息，減除外界多餘的刺激與不必要的互動[160]。以往人們利用家宅從事社會交往，發展個人親密關係[161]，在有形物理空間中齊聚一堂、溝通來往，今日個人泰半利用手機所創設的虛擬空間培植個人親密領域，與親朋好友交流互動[162]，人與人之間面對面聊天對談的頻率少了，利用手機情話綿綿、「LINE 來 LINE 去」、推文按讚聯絡感情的時間卻多了。以往個人係在家中自由從事個人活動，讀書、觀影，不受他人窺探[163]，今日個人轉而利用手機所提供的各式功能，閱讀書報、瀏覽新聞，汲取或嚴肅或輕鬆的各種資訊。

再自手機對於現代人情感上的重要性觀察，如前引 Google 研究報告所述，智慧型手機普及率已超越我國一半人口，近七成受訪者每天均會使用智慧型手機，高達八成的受訪者與手機形影不離，我國民眾對手機依賴度更已躍居亞太

[158] Wellman, *supra* note 20, at 238.
[159] Solove, *supra* note 78, at 1137-38.
[160] SILVA & FRITH, *supra* note 29, at 5-6.
[161] Solove, *supra* note 78, at 1137-38.
[162] LING, *supra* note 19, at 159.
[163] Solove, *supra* note 78, at 1137-38.

地區之冠[164]；過半數受訪者遇上火災時第一個搶救的是手機、兩成多的受訪者寧可為了手機放棄週末的性愛[165]；高達百分之六十五的受訪者表示沒有 iPhone 就活不下去[166]等等。美國甚至已經發展出無手機焦慮症（nomophobia，由 no、mobile、phobia 三個字組合而成）這個新字，用以指涉個人與手機分離的恐懼感，相關復健中心則逐漸開始開辦無手機焦慮症的團體治療[167]。

對某些人而言，手機幾乎成了第二個家，甚至比原生家庭更有家的味道。「低頭族」時時窩在手機家宅捨不得離開，將其視為生活上的寄託，在手機空間內自由從事個人活動：交往互動倚之、抒發情緒倚之、閱讀思考倚之……個人身處這個由 0 與 1 構築的數位空間，在虛擬的家裡找到安心與歸屬，這種歸屬感甚至連在傳統的家都無法獲得。與其說手機是隨身「物品」，反而更像一座隨身「家宅」，就「個人生活秘密空間」的意義而論，傳統家宅之地位，似乎正逐漸被手機所取代。手機之於現代人的重要性與日俱增，絲毫不亞於實體家宅，甚至猶有過之，成為現代人安身立命之媒介。

若就個人每天滑手機的時數與在家裡清醒活動的時數加以統計，說不定前者遠比後者多上許多。若論一般人民對「個人生活秘密空間」的保護，家宅僅止於一道門鎖、幾扇鐵窗，對手機卻是以密碼、解鎖圖片、指紋等各種推陳出新的手法，一層又一層地維護。若在路上隨機抽樣調查，如果今天家宅與手機須二擇一讓警方搜索，說不定大多數人寧可讓警方進入自己家裡，也不願手機內的個資遭人一覽無遺。由此，似可推知手機之個人精神上秘密空間，與傳統家宅之物理上秘密空間，兩者間輕重地位的變化。

---

[164] 前揭註 2。
[165] 前揭註 16。
[166] 前揭註 17。
[167] Nomophobia': Is cellphone addiction real?, PIX11 (Feb. 24, 2015), http://pix11.com/2015/02/23/nomophobia-is-cellphone-addiction-real

3. 2. 1. 2. 手機為個人探索自我、形塑人格的重要媒介

承前所述，現代資訊社會中，手機儼然成為人民精神上寄託，創造出一塊讓人得以稍事喘息的私領域，杜絕外界不必要的干擾。個人得於手機所創設的私密空間內遂行上網、瀏覽、閱讀、搜尋等活動，汲取知識與資訊，作為人格養成的基石。

舉例言之，前引調查數據顯示，四成的受訪者表示自己會向手機詢問一些不願意告知好朋友的問題[168]。如個人可能隱隱然對於自己的性別氣質、身分認同等有所懷疑，在班上卻難以啟齒、不知向誰詢問，亦不敢讓家人知情，只能壓抑自我。此時手機讓個人即使不用家中電腦或電話，亦可上網查詢相關訊息、藉由匿名軟體、匿名版面詢問，或以手機打相關社福團體的諮詢專線求助。這些個人難以啟齒的私密問題，很可能就是個人尋求自我認同，發展人格的關鍵疑問。

再自手機解放通訊之地理限制、使人際互動無遠弗屆之特性觀察，與人互動也是手機功能中相當重要的一環。個人與外界的互動狀況，亦與自我人格之發展密切相關。

社會學家黃厚銘即指出，一個人的自我認同係於社會脈絡之下，與周遭的他人互動中逐漸發展形塑而成。所謂自我認同，係一關於個人的自我敘事，包括我是誰、是怎麼樣的一個人、如何變成現在這個樣子、期待未來要做什麼、成為怎麼樣的一個人等等。而個人自我敘事，則係個人透過與周遭的人長期互動過程發展而來[169]。

學者劉靜怡教授亦由科技觀點檢視其對個人認同之影響。其認為，資訊科技改變了人我之間的界限與壁壘，因此，個人基於其對個人資訊的控制與決定

[168] 前揭註 16。
[169] 黃厚銘，〈網路上探索自我認同的遊戲〉，《教育與社會研究》，第 3 期，頁 81（2002 年）。

權，自主決定與他人建立何種社會關係，進而相當程度決定了個人在資訊社會中的定位，塑造個人身處於這個資訊社會裡的身份認同[170]。

個人的身分認同與發展受人際互動影響，而自現今社會生活之現實而論，個人人際交往幾已少不了手機之輔助。手機使個人在社交關係上，擺脫時間地點的侷限，直接與遠端通訊對象連結[171]；亦能利用手機維持個人的親密領域，與親朋好友持續交流互動[172]。如今，社交小團體使用手機溝通已蔚為風潮，個人則藉由手機於團體之中交換資訊、傳遞笑話或八卦、鞏固團體的內在聯繫，將團體成員們更緊密地連結在一起[173]。然而，水能載舟，亦能覆舟，有研究即指出個人若過度耽溺、花費太多時間使用智慧型手機，反而會對人們與同伴或配偶之間的關係造成負面影響[174]。

藉由手機之助，個人得以在手機創造的私密空間稍事喘息，並利用手機汲取資訊，探索自我。手機亦讓使用者得以自由決定社會互動的頻率與對象，與誰建立較為親密的關係，與誰則否，並自我掌控對外透露的資訊多寡；在與他人的互動交往之中，培植形塑自我人格與認同。就此而論，手機實為形塑個人自我認同之重要媒介。

3. 2. 2. 手機資訊與隱私

3. 2. 2. 1. 手機所載資訊質量俱豐，幾成個人大數據

我國憲法保障隱私權的另一面向，係保障人民對個人資訊之自主控制。手機，作為「隨身物品」的一種，論者或有質疑：將手機單獨提出論述之區別實

[170] 劉靜怡，〈網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河〉，《資訊管理研究》，第 4 卷第 3 期，頁 144（2002 年）。
[171] Wellman, *supra* note 20, at 238.
[172] LING, *supra* note 19, at 159.
[173] *Id.* at 172。
[174] 前揭註 167。

益何在？詳言之，手機與其他個人隨身攜帶之皮包、相簿、筆記本等物並無不同，均屬「載有資訊之隨身物品」。以隨身皮夾為例，皮夾裡的鈔票多寡可推測個人財力、發票紀錄個人購買哪些物品、照片透露可能的親密對象等。若個人將筆記本、小相冊等隨身攜帶，其內亦可能記載個人的所思所想、與哪些人過從甚密等等。因此，若就資訊自主的觀點而言，為何有必要將手機單獨提出討論？不無質疑餘地。

若單就手機內所儲存之資訊而論，由於現今智慧型手機功能包羅萬象，涵蓋生活各個層面的資訊，實與一般隨身物品相去甚遠。皮夾內的發票確實可能透露金錢與消費方面的收支狀況、筆記本記載著個人的行程或所思所想、便條紙則記錄著個人的行事規劃等等，均與個人資訊有關。惟無論皮包、筆記或便條，都只涵蓋個人「一部分」的資訊。假設警方搜索皮夾，確實可能由皮夾內的發票等推估個人消費習慣的蛛絲馬跡，卻難以推斷個人的所思所想或交友狀況；假設警方附帶搜索隨身筆記，或許可以推知個人近日的所思所想，卻未必能知曉交友狀況，或筆記主人去過哪些地方。

相形之下，手機則不然。殊難想像還有其他物品一如智慧型手機，記載涵蓋個人生活「全方位」之資訊。概如前文所陳，現代人的生活形貌泰半仰賴手機作為媒介，正因為手機與個人生活各個面向緊密交織的特性，反過來說，人民使用手機過程中所紀錄下的各種個人資訊，也涵蓋了使用者生活之食衣住行育樂、於公於私的各種細節，資訊的質與量愈發驚人。例如個人在使用手機的同時，諸如通聯紀錄、文字簡訊、社群軟體聊天訊息、電子郵件、定位資訊、生活照片、消費資訊與網頁瀏覽紀錄等等，各種開誠布公或私密敏感的個人資料，也一一被手機紀錄下來。鑑於手機儲存個人生活各種資訊的特性，Ling 教授將其稱為個人歷史的寶庫[175]（repository of personal history）。

[175] LING, *supra* note 19, at 97.

藉由手機內各種資訊碎片，手機使用者的生活細節全貌呼之欲出：一個人讀哪種書[176]、看什麼新聞、聽哪類音樂、與哪些人有所往來、與哪些人密切聯繫、平時的行蹤、購買什麼物品……悉數紀錄於手機裡。手機內儲存之個人資訊，其涵蓋層面既廣且深，幾可稱之為掌中大數據，個人隱私盡在其中，此點是皮包、筆記本或便條等其他隨身物品遠遠無法比擬的。

3. 2. 2. 2. 手機結合雲端，實為個人資訊之萬能鑰匙

除了前述手機本地端資訊包含萬千面向、所載資訊已遠非其他隨身物品所能企及的特性外，若再加上行動上網與雲端儲存的考量，則手機所涵蓋的資訊面向更加廣闊而深遠。手機，於此不只是單純的資訊載體，更是一把通往其他資訊寶庫的萬能鑰匙。

近年來日漸普及的「雲端運算」，係強調在本地端資源有限的情況下，使用者透過網際網路，直接取用遠端服務業所提供之資訊科技服務[177]。「雲端」之名，起源自工程師在繪製示意圖時，常以一朵雲來代表網路，故後以雲端泛指網路。雲端運算雖然方便，但同時也有隱私上的隱憂：使用者的行為、習慣、愛好等等個人隱私，也會隨著雲端服務一同被服務商紀錄下來，更直接地暴露在網路之上[178]。

作為雲端運算架構其中一環的「雲端儲存」，則是指提供線上儲存空間，

---

[176] 個人閱覽書種亦屬隱私之一環，例如日本曾發生報社自圖書館借閱卡中得知作家村上春樹高中時期的閱讀習慣，並加以報導揭露之情事，即引發侵害個人隱私之爭議。相關報導詳見林序家，揭露村上春樹高中閱讀習慣 引爆隱私權之爭，新頭殼，2015 年 12 月 2 日，http://newtalk.tw/news/view/2015-12-02/67396（最後瀏覽日：2016 年 1 月 12 日）。

[177] 若根據服務內容細分，雲端運算又可分為三個類型：軟體即服務（software as a service, SaaS）、平台即服務（platform as a service, PaaS）與基礎設施即服務（infrastructure as a service, IaaS）。詳見曹乙帆，雲端運算的儲存基礎架構 揭開雲端儲存的面貌，雲端運算智庫，2009 年 11 月，http://www.runpc.com.tw/content/cloud_content.aspx?id=105324（最後瀏覽日：2017 年 11 月 5 日）。

[178] 對於雲端運算的進一步介紹，詳見黃重憲，淺談雲端運算，臺灣大學計算機及資訊網路中心電子報，2009 年 3 月 20 日，http://www.cc.ntu.edu.tw/chinese/epaper/0008/20090320_8008.htm（最後瀏覽日：2016 年 1 月 12 日）；另參劉定基（2014），〈雲端運算與個人資料保護－以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心〉，《東海大學法學研究》，第 43 期，頁 55-57。

讓使用者將資料上傳至雲端伺服器，之後只要連上網路，即可直接存取資料，不受時間地點的限制[179]。舉凡 Google 雲端硬碟、Google 相簿、Evernote 雲端筆記本以及 Dropbox 雲端儲存空間等，均屬此類。

早在 1997 年，蘋果公司全球軟體開發者年會上，賈伯斯（Steve Jobs）回答與會者的問題時，即提及他對雲端運算的願景：

> **「這些日子以來，電腦最厲害的地方，並不只是把它們用來處理複雜的運算工作，而是將它們當作一扇窗戶，結合現今網路科技的力量，連結到各種通訊密集的服務……住在一個高速連結的世界裡，完成每日的工作[180]。」**

而在近二十年後的今天，隨著電腦運算能力增強、網路速度一日千里，以及雲端運算的迅速普及，世界已與賈伯斯的期待相去不遠。由於手機本地端空間有限，個人多已不將資訊全數儲存於手機內，而係使用雲端儲存服務，將部分資訊存在遠端業者所提供之雲端儲存空間，於需要時再透過網路下載所須使用之資訊。

雲端儲存普及前，人們可能將不同的資料存放在不同的地方：電子郵件與工作檔案存放在公司電腦的 Outlook 內、通訊錄與通聯記錄存放在手機裡、照片與影片存在相機 SD 卡中、重要文件歸檔於筆電硬碟裡……然而，雲端儲存的普及，改變了人們生活與工作的模式，以往分別存放於多處的電子郵件、檔案、相片、影片、文件等，藉由雲端儲存之助，均可透過手機這把鑰匙，直接存取使用。你我走在路上也可以利用 Google Drive 同步存取家中電腦的檔案資

[179] 前揭註 177。

[180] "Much of the great leverage of using computers these days is using them not just for computationally-intensive tasks, but using them as a window into communication-intensive tasks as you know. And never have I seen something more powerful than this computation combined with this network technology that we now have…And, I just want to focus on something that's very close to my heart, which is living in a high-speed networked world, to get your job done every day." 詳見 1997 年 WWDC 的紀錄影片：1997 WWDC Fireside Chat with Steve Jobs, YOUTUBE, https://www.youtube.com/watch?v=6iACK-LNnzM, 時間軸 13:38 以下。

訊、瀏覽 iCloud 裡頭的照片、出國旅遊時打開 Evernote 雲端筆記撰寫旅遊心得、與指導教授會面前叫出 Dropbox 裡的論文檔案再次閱讀準備等，各種雲端資訊走到哪、帶到哪，不受物理與容量的限制。

藉由雲端儲存之助，手機成了一扇連結各個企業與服務的窗戶，有如一座小叮噹的任意門，具有貫通空間的能力。使用者只需要輕鬆滑滑手指、點點螢幕……想去哪裡，便去哪裡。手機彷彿成了一把萬能鑰匙，只要鑰匙在手，即可打開個人存放在各個保險櫃（上開服務提供者）內的雲端資訊。

如果單就手機本身數十 GB 的龐大空間，即足以讓人們感受到其對個人隱私所產生的潛在隱私威脅，則雲端儲存的出現，更讓此種威脅變本加厲。承前所述，手機已成為個人歷史寶庫，但此一寶庫或許還受到藏寶箱空間大小（手機容量）的限制，總有塞滿的一天，超出容量的資訊必須忍痛刪除。然而，雲端儲存與行動上網普及後，個人所有存放在雲端之資訊，均可透過這一把手機鑰匙存取。透過手機所能近用者，已非限於手機本體，而是延伸至使用者藏於各個角落的資訊。

一般手機使用者為了方便起見，多會將手機中的應用程式保持登入狀態，除了可以存取手機本地端的通聯記錄、通訊錄、文字簡訊、瀏覽紀錄、定位資訊、閱讀紀錄等資訊外，只要連上網路、步入雲端，世界更無限延伸：申辦 Gmail 至今的每封電子郵件、iCloud 上的每張備份照片、Messenger 與 LINE 之中的每一則訊息、Dropbox 上的每個檔案或是利用 Evernote 所撰寫的每篇筆記等等，唾手可得。換言之，手機不啻成為使用者自行建置之「法眼系統[181]」，一機在手，即可觀看手機使用者生活軌跡的各種記錄。

[181] 所謂的「法眼系統」係法務部調查局於 1990 年間建構的資料庫系統，建置目的在於減少調查局向各部門函調資料之往返時間，爭取辦案時效。調查官只要使用調查局內部電腦進入此系統，即可取得政府單位的各項資料：「可以把一個人的祖宗八代，調查的清清楚楚。」相關新聞詳見林益民，調查局法眼系統 「祖宗八代清清楚楚」，蘋果即時，2015 年 9 月 8 日，http://www.appledaily.com.tw/realtimenews/article/local/20150908/687317（最後瀏覽日：2016 年 1 月 12 日）。

若自「個人歷史寶庫」的立場著眼，將手機本地端以及雲端資訊共同納入計算，手機實已進一步升級為「容量無限」的歷史資訊寶庫，無論是使用者操作手機時在本地端所留下的資訊，或者在雲端資料庫裡所留下的每一步數位足跡，個人隱私悉在掌中。

3. 3. 手機科技引發的隱私權思考

3. 3. 1. 秘密空間之擴張解釋

俗諺有云：「家是一個人的城堡[182]。」Solove 教授亦著書點出家宅對個人的重要性：家，讓個人得以豁免於政府的侵入，把公眾鎖在門外，也使個人得以遠離塵囂，在家中享受靜謐、獨處，找到心靈上的平靜、滋養個人的親密關係。人們亦得在家中自由從事讀書、觀影等私人活動，不受外界干擾[183]。

受美國國安局前雇員 Snowden 之託，揭露美國政府監聽內幕之知名專欄作家 Glenn Greenwald 亦強調，私領域使個人得以躲開他人批判眼神，自由地活動、思考、交談、寫作與探索，選擇自己要成為怎樣的人[184]。有些被別人看到會感覺難為情的事，諸如跳舞、懺悔、探索性行為、分享實驗性的想法，人們只有在獨處時才會做。人們只有在相信無人觀看時，才能自在而安心地實驗、測試極限、探索新的思考與生活方式、探索做自己的真正意義[185]。若私領域的保障不再，人們會大幅度改變自己的作為，亦步亦趨地遵守社會規範，畫地自限避免任何脫序或不正常的行為，努力符合期待，以避免受到羞辱和譴責[186]。

---

[182] "A man's home is his castle."

[183] 惟 Solove 教授亦指出，現代意義上的家宅其實是工業化以後的產物。工業化以前，家宅同時也是工作與處理公事的空間。除了家宅主人外，還有學徒、佣人、其他房客等一同居住，居住空間龐大而嘈雜，個人在當時並無法享有如今日家宅一般的隱私。*See* Solove, *supra* note 78, at 1137-39.

[184] GLENN GREENWALD, NO PLACE TO HIDE 172 (2014).

[185] *Id.* at 174.

[186] *Id.* at 173.

「一個意識到自己持續受到監視的公民，很快就會變得順從而膽怯[187]。」

以手機內的通聯紀錄而論，即使撥出之號碼並未透露雙方通話之內容，卻會透露個人通話對象、時間長短等資訊。政府若有心，即可透過這些資訊分析使用者於何時與何人通話，檢視推敲個人的生活細節。只要能掌握個人通話對象與頻率，則個人交友狀況、生活作息也呼之欲出。政府僅需搜索某一異議人士之手機，即可由通聯紀錄得知與該異議人士有所往來之人，甚至採取進一步行動。個人為了不被政府盯上，很可能乾脆拒絕與該異議人士往來，以避免不必要的困擾，進而導致言論壓制之寒蟬效應。

以我國憲法隱私權保障「個人生活秘密空間免於他人侵擾」的面向而論，若單就字面上解讀，所謂的「個人生活秘密空間」，保障範圍似乎僅限於個人家宅等秘密「空間」，手機屬於物品、非屬空間，似非文義所涵括。然而，若單就文義解釋，將手機與其他物品一視同仁，直接否認將手機區別處理、特別保護之必要，只怕完全忽略了數位時代科技變革所附隨的改變與衝擊，亦無視於手機已躍居現代人生活所賴所倚之精神上秘密空間的地位。

隨著時代變遷，個人所倚重的秘密空間亦有所推移。如前所述，現代人生活型態改變，個人待在實體家宅的時間大為減少，身處數位家宅的時間反而增多，若將個人待在家裡活動與低頭滑手機之時數予以比較，後者可能遠勝於前者。個人藉由手機此一媒介，向內探索自我、向外發展親密關係，所謂「神聖不可侵犯」的私領域，似乎也漸由家宅轉移至手機。

隱私權旨在保障人民得以享有一塊純屬私人、不受干擾的領域，得以在這塊領域裡自由探索、交流、做自己。此一領域的形式（實體空間或數位空間）實非緊要，實質（個人自在休憩之所）才是重點。吾人在解釋憲法保障的「個

[187] *Id.* at 3.

人生活秘密空間」時，實應考量到科技進展所帶來的改變。一如司法院釋字第392號解釋理由書所言：

> **「憲法並非靜止之概念，其乃孕育於一持續更新之國家成長過程中，依據抽象憲法條文對於現所存在之狀況而為法的抉擇，當不能排除時代演進而隨之有所變遷之適用上問題[188]。」**

舊時人民以面對面為主流交往的生活方式下，憲法保障個人享有物理上的秘密空間（如家宅等），保障人民免受政府或他人恣意干擾。時日推移至今，生活型態改變，現代人的交流往來未必以面對面交談為大宗，而係藉由手機創設出一個個虛擬私密的小密室，在密室中與個別好友暢談、於密室內自由思考閱讀。

因此，本文認為，在解釋所謂的「個人生活秘密空間」之時，不應拘泥於傳統上的物理空間，而應「對於現所存在之狀況而為法的抉擇」，視現代社會科技發展的狀況、個人生活方式的變遷而有所調整，擴張解釋。

實則，手機的問世，業已改變人們對於「空間」的想像，使個人得以切割外在物理環境、創設獨特的內部空間，使個人免於他人干擾、自由從事個人活動、保有個人親密領域。由此觀之，手機已由單純的資訊載體轉化為現代人的數位私密空間，躍居為個人精神上的家宅，甚至是安身立命之媒介。

鑑於手機科技之特性，解釋上似可考慮將隱私權保障之生活秘密空間予以擴張，延伸涵蓋手機之類精神上秘密空間，給予手機等同實體秘密空間之高度保護，以此保障個人的思想、情緒與感受，不受恣意干擾侵犯。

[188] 釋字第392號解釋理由書參照。

3. 3. 2. 剖繪科技之監控風險

政府搜索手機取得個人資訊，有何不可？憲法所保障個人享有之資訊自主權保障若未能落實，國家基於偵查犯罪之需求、私人企業追求經營上的效率，得以恣意檢視蒐集個人資訊，又會有什麼後果？

誠如前述，手機內儲存的大量資訊，使其有如個人的「大數據」，詳細記載手機使用者的興趣、喜好、行動、交友等。此一特性，潛藏著另一個危機：剖繪科技（profile technology）之風險。

Solove 教授即指出，最常被隱私論者引述作為警惕的《1984》老大哥，在現今社會未必完全適用[189]。小說《1984》的世界裡，係由中央集權的老大哥遂行監控工作，但現今社會的資料蒐集，卻不完全是由政府掌握，還包括不受中央控制、目的在於促進購買與服務而非壓迫人民的企業；大多數的政府也不像《1984》的老大哥那般有著監控全局的野心。老大哥的目標在於控制人民生活中最私密的細節，但個人數位檔案（digital dossiers，係指關於個人的大量資訊累積）裡的資訊，卻未必那麼私密或罕見[190]。

惟一個人閱讀、購物、病史與網路活動的詳細記錄，卻使政府可以繪出一個人的金融、健康、心理、信仰、政治、興趣與生活型態的輪廓。即使一個人在網路上使用暱稱或假名，但數位檔案裡的資料卻可揭穿他的身分，暴露全部與他有所聯繫以及有生意往來的人[191]。政府與企業往往在人民不知情的情況下蒐集、利用這些關於個人的資訊，甚至進一步據此決策。例如企業運用這些數位檔案決定如何與我們交易、金融機構以此評價個人的信用等級、政府據此展

[189] 其他評論家亦注意到，更深的隱私侵害可能來自於商人，而非往昔之祕密警察。詳參 Howard Rheingold 著，張逸安譯，《聰明行動族：下一場社會革命》，頁 295（2010 年）。
[190] SOLOVE, *supra* note 7, at 7.
[191] *Id.* at 5.

開對人民的調查等等[192]。

以私部門而言，作家 Christopher Steiner 亦指出，將個人資料結合演算法處理運用之例，並非罕見。以個人「交談話語」為切入點，將系列文字或語言模式作為基礎，由個人說話方式與句構判定個人性格並加以分類之演算法，早已在發展中。藉由此類演算法，機器人可以預先判定來電者的性格，並將電話轉接給性格與來電者類似的客服專員，提高解決問題的效率[193]。

再就公部門而論，為了達成執法目的，執法機關常常向私部門（如公司、金融機構）索求個人資訊，以調查詐騙、白領犯罪、毒品交易、電腦犯罪、兒童色情以及其他犯罪活動[194]。美國政府甚至已經在發展以數位檔案預測行為模式的方式，例如美國國防部所開發的 Total Information Awareness（簡稱 TIA，後改名為 Terrorism Information Awareness）方案，政府先向私部門取得並累積個人資訊，建立龐大的個人檔案資料庫後，再以剖繪科技預測哪些人比較可能參與犯罪活動[195]。惟此一方案因反彈聲浪強烈，最後胎死腹中[196]。

除了 TIA 方案外，美國聯邦政府亦實施所謂的 Computer Assisted Passenger Prescreening System II（簡稱 CAPPS II）方案，作為登機前的篩選機制。政府利用電腦資料庫的資訊，於乘客登機之前，先行剖繪並判定個人的「威脅等級（threat level）」係屬綠燈、黃燈還是紅燈。被判定為綠燈（安全）的乘客僅需通過一般的安全檢查，黃燈乘客則需接受進一步的搜索，至於被分類為紅燈之乘客，將被禁止登機。政府並未透露如何蒐集相關資訊、如何剖繪人民、種族與國籍是否為因素之一，以及人民得否挑戰自己的分類等等。這樣的分類法卻造成許多乘客的困擾與延誤，例如實務上即發生人民僅因有著穆斯林姓，而被

[192] *Id.* at 3-4.
[193] CHRISTOPHER STEINER, AUTOMATE THIS: HOW ALGORITHMS TOOK OVER OUR MARKETS, OUR JOBS, AND THE WORLD 177-183 (2013).
[194] SOLOVE, *supra* note 7, at 5.
[195] *Id.* at 5-6.
[196] *Id.* at 168-69.

歸類在禁止搭機之列，在登機前被擋下。即使事後申訴通過，飛機也早已起飛[197]。就此以觀，於私部門與公共紀錄（public records）持續累積的數位檔案，似乎正逐漸轉變為政府監控調查人民的工具[198]。

國內學者劉靜怡教授亦指出，政府機關與企業組織透過資訊科技，根據個人資料或由各種個資所歸納出的進一步資料，對使用者的「網路形象」進行型塑（profiling）。這些形象很可能涉及諸如宗教認同、政治偏好、性傾向（諸如異性戀、同性戀或雙性戀者）等屬於個人極端私密領域的特徵，一旦公諸於世，甚至未經同意被行政機關根據行政需求肆意濫用，其所造成的不悅或傷害難以彌補。面對此類型塑工程，一般使用者目前亦處於被動地位，並無主動參與的可能性[199]。

日本學者小倉利丸的見解亦值吾人參考。小倉教授指出，個人活動所累積的各式資訊，原係由個別電腦管理，累積在個別的資料庫中。然而，國家若以「指紋」此等受廣泛使用的個人識別資訊作為媒介，將四散於網絡系統中的各資料庫連結共用，即可以此識別資訊為基礎，重構「私人」之人格，甚至能統一掌握每個個人的行動，予以追蹤。政府便能組合相關數據，擅自描繪個人，透過各種數據的累積，斷言個人是否為恐怖份子、是否合於資格等。如此，個人已然喪失自我說明的權利，僅國家或警察握有詮釋個人的話語權[200]。小倉教授的見解雖係討論指紋資訊時所提出，惟若將「指紋」換成「手機」，國家蒐集資訊所產生的威脅，並無不同。

我國學者邱文聰亦提醒，蒐集利用個人資訊並進行分析，藉以產出與人有關之各種圖像的知識／權力的生產活動，可能會造就過於僵化的自我認識與自

[197] *Id.* at 182.
[198] *Id.* at 5-6.
[199] 劉靜怡（註 170），頁 146。
[200] 小倉利丸，〈日本型監視社会に対抗するために〉，《世界のプライバシー権運動と監視社会》，頁 13-49（2003）。

我批判的基準。故為維護個人人格內在形成的彈性空間、使其自由開展，資訊隱私權必須對此類生產活動進行必要的制衡與約束，以抵抗其對個人人格的形塑作用[201]。

上舉諸學者之見解，無非指向同一個方向：國家與企業對於涉及個人之資訊仰賴日深，甚至以此類資訊與數據重塑、描繪個人人格，恣意斷定一個人的價值、是非或犯罪傾向，採取相應行動。就此而論，政府、企業所觀察並據以判斷作出決策的，已非「個人」本身，而僅僅是片段「數據」的積累堆疊。個人的數位檔案不見得完全正確，也未必能確切反應一個人的真實樣貌，惟個人在此架構下業已喪失對自己的詮釋權。

我國司法院釋字第 603 號解釋之意旨，於此亦可供參照。司法院大法官除明確闡釋憲法保障個人資訊自主控制權，賦予人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權外，解釋理由書中更指出指紋應受特別保護之理由：

> 「指紋係個人身體之生物特徵，因其具有人各不同、終身不變之特質，故一旦與個人身分連結，即屬具備高度人別辨識功能之一種個人資訊。由於指紋觸碰留痕之特質，故**經由建檔指紋之比對，將使指紋居於開啟完整個人檔案鎖鑰之地位**。因指紋具上述諸種特性，故**國家藉由身分確認而蒐集個人指紋並建檔管理者，足使指紋形成得以監控個人之敏感性資訊。**」

舉輕以明重，本文認為，手機雖不具有指紋人各不同、終身不變、具備高度人別辨識的特性，惟就連結個人資訊、居於開啟完整個人檔案鎖鑰之地位，

[201] 邱文聰，〈從資訊自決與資訊隱私的概念區分—評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，第 168 期，頁 176-177，（2009 年）。

以及國家得藉此掌握對個人人格詮釋權之性質，手機與指紋並無太大差異，前者甚至遠勝於後者。

國家若取得人民指紋，尚須以指紋為憑，耗時費日向各個資料庫分散查詢個人資訊。惟今日國家若獲授權取得人民手機一支，則檢警連奔波各資料庫調取資料的工夫都可省下，只需要輕輕鬆鬆、滑滑手機，便可取得手機使用者所有公開與非公開、中性或敏感、近期與長期的各式資訊。個人完整數位檔案，悉在指掌之間。國家大可基於手機中大大小小的資訊，透過數據累積，重構使用者樣貌，擅自斷言個人的想法、恣意描繪個人人格，個人於此時則完全喪失發言權，任由國家監控解讀。

前引 Google 研究報告顯示，百分之六十的受訪者每天都會使用智慧型手機，透過搜尋引擎搜尋資訊[202]。換個角度觀察，這六成手機使用者所關心的事務、性傾向、敏感病史等，即可藉由手機搜尋紀錄一覽無遺。例如搜尋紀錄若含有戒毒村、戒酒門診等關鍵字，或可推論使用者或許飽受毒癮或酒癮所苦。於此情形，個人不復為個人，而是淪為片段資訊的集合體。

再者，有關個人的資訊是否真的這麼確實、這麼絕對？憑藉著所謂的「大數據」，是否真能精確重構一個人的人格、精準預測一個人的行為，再如美國政府胎死腹中之 TIA、現行的 CAPPS II 等方案一般，依據預測結果採取相應行動？Solove 教授即指出，以資料探勘（data mining）來預測個人將來的行為是相當不精確的。個人行為並不像重力一樣恆定規律，反而比天氣更加難以捉摸預測[203]。

於此，本文想引諾貝爾文學獎得主、波蘭裔女詩人辛波絲卡的《履歷表》一詩作結。在這個資訊至上，政府、企業搶著蒐集解讀大數據的時代，資訊所

[202] 前揭註 2。
[203] SOLOVE, *supra* note 4, at 186.

能告訴我們的事情，或許不總是那麼完整，也不見得那麼真切。在這個一切講求數據、追求效率的時代，試圖以瑣碎片段的資訊與數據定義一個人的樣貌、將人分門別類、劃分等第，究竟是理所當為，還是荒謬可笑？

「需要做些什麼？

填好申請書

再附上一份履歷表。

儘管人生漫長

但履歷表最好簡短。

簡潔、精要是必需的。

風景由地址取代，

搖擺的記憶屈服於無可動搖的日期。

所有的愛情只有婚姻可提，

所有的子女只有出生的可填。

認識你的人比你認識的人重要。

旅行要出了國才算。

會員資格，原因免填。

光榮記錄，不問手段。

填填寫寫，彷彿從未和自己交談過，

永遠和自己只有一臂之隔。

悄悄略去你的狗，貓，鳥，

灰塵滿佈的紀念品，朋友，和夢。

價格，無關乎價值，

頭銜，非內涵。

他的鞋子尺碼，非他所往之地，

用以欺世盜名的身份。

此外，再附張露出單耳的照片。

重要的是外在形貌，不是聽力。

反正，還有什麼好聽的？

碎紙機嘈雜的聲音[204]。」

3. 3. 3. 手機資訊與隱私權保障

3. 3. 3. 1. 手機資訊應受憲法隱私權保障

概如前文所陳，現代社會中，手機使個人得以創設一個獨特的私密空間，免除他人眼光的評價與干擾，自由獨處、閱讀、思考，汲取資訊、探索自我。手機亦屬現代人交流往來不可或缺之重要工具，個人利用手機撥打電話、發送簡訊、拍照攝影、連結社群網站等功能，維持社交關係與親密領域，於與他人的交流互動之中，追尋自我認同、形塑自我人格。

然而，人民使用手機的同時，大量公開或私密、中性與敏感的個人歷史資訊，也鉅細靡遺記錄於手機之內。手機內片段累積的資訊，有如一片片馬賽克拼圖，將其拼湊起來，即可湊出一個人的生活梗概：個人獨處時的活動喜好、與他人社交的互動軌跡，盡在其中。

[204] Wislawa Szymborska 著，陳黎、張芬齡譯，《辛波絲卡》，頁 146-148（2015 年）。

若論手機資訊之深度及廣度，只怕絲毫不亞於 DNA 或指紋資訊，甚至猶有過之。查閱現代人的手機，幾可重構使用者的生活樣貌細節。自此以觀，手機資訊雖不具有指紋人各不同、終身不變、具備高度人別辨識的特性，惟就其連結個人資訊、居於開啟完整個人檔案鎖鑰之地位，兩者則屬同一，手機資訊甚至猶有過之。若許國家檢視人民手機，其內資訊實屬得以監控個人、重構生活細節之敏感性資訊。因此，本文認為手機資訊應受憲法隱私權保障。

或有論者會質疑，手機內資訊各有不同，通聯紀錄、簡訊、照片、日記、思考筆記、消費資訊、電子郵件、電子書、定位資訊、社群軟體、網頁瀏覽紀錄、雲端儲存檔案等等，隨著資訊性質不同，隱私程度亦高低有別，應對手機內不同性質之資訊給予程度多寡不一之保障。

本文並不同意此種想法。由於檢視手機之前無法預知其內存有哪些資訊，必須要點開手機、一一查閱後，才會確知資訊的內容，就此而論，手機有如一個未知的包裹，手機內資訊則為包裹內的各式物品，應受相同程度的保護。以國家搜索包裹為例，吾人不會以包裹內放的物品重要程度有別為由給予不同評價，而是將整個包裹視為一個搜索標的。同理可證，吾人亦不應以手機內資訊的隱私程度不同而給予差別待遇，而應將手機資訊包裹為一個標的看待，統一保護。

綜上所述，有鑑於手機實已成為個人精神上秘密空間，此一私密領域應享有不受侵擾之自由；手機資訊質量俱豐，幾已成為掌中大數據，別具重要性與特殊性，人民就自身手機資訊之自主控制，亦應受憲法資訊隱私權保障。人民得自主決定是否揭露手機資訊，並享有在何種範圍內、於何時、以何種方式、向何人揭露之決定權。

3. 3. 3. 2. 犯罪偵查與隱私保障之價值折衝

手機資訊雖應受憲法隱私權保障，然基本權利之保障並非絕對，於符合憲法第二十三條意旨之範圍內，國家仍得以法律明確規定，對其予以適當限制。如國家為達證據保全之目的、確保刑事訴訟程序順利進行，有實施搜索扣押等強制處分之必要，在合於憲法第二十三條之要求下，仍得以強制手段取得個人手機內資訊。

著眼於手機資訊質量俱豐、甚至作為個人檔案萬能鑰匙之特性，其於今日犯罪偵查所扮演的角色也愈顯吃重。刑事偵查程序中，檢警常鎖定手機取證，試圖從手機內的資訊查找可能的偵查線索或定罪證據，諸如毒販之間的通聯記錄、通訊軟體的交易文字、性侵害加害人手機中的被害人裸照[205]、案發現場或贓物之照片錄影等[206]，手機資訊於犯罪偵查漸佔有一席之地，輔助認定犯罪事實。然而，現代人生活起居極度仰賴手機，其內資訊幾成為個人生活縮影、隱私盡在其中，搜索手機對個人所造成的隱私侵害，亦值吾人關注。

當人民眼睜睜看著存有許多敏感個人資料的手機於眼前被員警打開，私密日記、親密照片、網頁瀏覽紀錄與不願見諸於人的聊天內容等諸多隱私，悉皆攤在員警面前，任由員警恣意翻找、質問，甚至取笑，此景有如在世界面前赤身裸體[207]、無所遮蔽，對個人人格更是極大的傷害，而這般羞辱與傷害，亦是

[205] 加害人手機內的被害人裸照，常成為性侵案件定罪之證據。例如王揚傑，壯漢 Line 變小白兔 誘騙少女傳裸照，中時電子報，2015 年 3 月 24 日，http://www.chinatimes.com/newspapers/20150324000511-260107；張文川，找友誘妻開房間 測忠誠度，自由時報，2015 年 5 月 9 日，http://news.ltn.com.tw/news/society/paper/878759（最後瀏覽日：2016 年 1 月 12 日）。

[206] 如八仙樂園彩色派對粉塵爆炸案，參與民眾在事故發生當下以手機拍攝的現場影片，也成為檢警偵查、鑑定的證據。八仙塵爆 火災鑑定分格蒐證影像，Yahoo 奇摩新聞，2015 年 6 月 28 日，https://tw.news.yahoo.com/%E5%85%AB%E4%BB%99%E5%A1%B5%E7%88%86-%E7%81%AB%E7%81%BD%E9%91%91%E5%AE%9A%E5%88%86%E6%A0%BC%E8%92%90%E8%AD%89%E5%BD%B1%E5%83%8F-074847455.html（最後瀏覽日：2016 年 1 月 12 日）。

[207] 比喻借自 Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser,* 39 N.Y.U. L. REV. 962, 1006 (1964).

事後完全無法彌補的[208]。此際，現實中實現的隱私狀態（achieved privacy）低於人民欲求的隱私狀態（desired privacy），會傷及個人的隱私感情，而會產生困窘、羞恥、不快、痛苦等負面感受[209]。

如喧騰一時的阿帕契貴婦參觀團案，檢察官問及案情時，被告概稱忘記，手機內照片也已遭刪除。檢警試圖還原手機中被刪除的照片，並找到被告漏未刪除的 LINE 對話紀錄與照片，成為本案鐵證[210]。然而，被告手機資料全數還原後，涉案照片僅占不到三分之一，另外三分之二的其他生活照與個人私密照片，卻一併攤在檢方眼前[211]。本案最終以不起訴作結，桃檢雖宣稱無關本案之照片已全數銷毀，惟涉案諸人私密照片遭人閱覽之羞辱感，卻已無從彌補。

當個人隱私保障與國家偵查需求有所衝突時，由於犯罪偵查之利益清晰可見，保障隱私的好處卻隱而不顯[212]，以致權衡兩者時，天秤有時會朝犯罪偵查的利益傾斜，過於側重犯罪偵查之需，隱私保障之重要卻遭忽略。以警方無合理懷疑、違法盤查人民身分的案件為例，許多評論的民眾態度均傾向「沒犯法為什麼不敢給警察看」、「查證身分也是為了治安」云云[213]。日前員警追車致少女撞車身亡案，警界人士發言稱：「犯罪嫌疑人臉上沒有寫字啊！」，所謂「見警就逃、非奸即盜」的觀念亦不乏大批民眾支持[214]。自此觀之，我國民意風向

---

[208] 誠如 Bloustein 教授所言: "Unlike many other torts, the harm caused is not one which may be repaired and the loss suffered is not one which may be made good by an award of damages. The injury is to our individuality, to our dignity as individuals, and the legal remedy represents a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered." *Id.* at 1002-03.

[209] 參考陳仲嶙，〈隱私權概念的理解與充填〉，《台灣憲法之縱剖橫切》，頁 643-646（2002 年）。

[210] 應訊裝傻！貴婦團急刪照 Line 留對話成鐵證，蕃新聞，2015 年 4 月 7 日，http://video.n.yam.com/20150407960516（最後瀏覽日：2016 年 1 月 12 日）。

[211] 朱明，阿帕契案》李蒨蓉等手機還原 私密照讓檢方瞠目結舌，風傳媒，2015 年 8 月 21 日，http://www.storm.mg/article/63291（最後瀏覽日：2016 年 1 月 12 日）。

[212] SOLOVE, *supra* note 4, at 2.

[213] 詳見此則新聞下的民眾意見：直擊！依法盤查遭民眾咆嘯 警嘆尊嚴掃地，蘋果日報，2015 年 8 月 29 日，http://www.appledaily.com.tw/realtimenews/article/local/20150829/680309（最後瀏覽日：2016 年 1 月 12 日）。

[214] 攔檢追車 少女逃竄撞死 警 po 文惹議「死是妳選的」，蘋果日報，2015 年 9 月 10 日，http://www.appledaily.com.tw/appledaily/article/headline/20150910/36770461（最後瀏覽日：2016 年 1 月 12 日）。

似乎認為，為了維持社會治安、打擊犯罪，個人權利略受限制，並無不可。

惟吾人須小心的是，此一邏輯再延伸下去，下一步或許就是「拒絕搜索，非奸即盜」、「查看手機也是為了治安」、「沒犯法為什麼不敢給警察看[215]」。吾人是否要容許國家偵查犯罪、維護治安之利益一再凌駕於個人權利保障之上，即不無研求之餘地。

偵破罪案、維護治安，確實係讓人民願意犧牲隱私的極佳誘因。然而，此際或許可以回頭深入思考，若執法者未能妥適保護人民的手機資訊隱私權，個人手機資訊置於隨時可能遭受國家權力檢視之情狀下（不妨想像學生在校，隨時可能遭受老師突襲搜書包檢查的景況），個人使用手機之活動隨時有受窺看之風險，吾人將立於何等處境？

此時，或可參酌 Glenn Greenwald 在 TED 之演講所引述著名反烏托邦小說《1984》中，國家大規模監控之景況，以及主角所面對的監控系統，作為前車之鑑：

> **「當然，你無法知道自己何時被監視，但他們隨時可以將監視你的線路插上，你必須、也確實在一個漸漸變成本能的習慣裡生活：假定自己發出的任何聲音都會被監聽，除了在黑暗中以外的所有動作都會被監看[216]。」**

Greenwald 認為，這種大規模監視的可怕之處，並非在於國家隨時隨地監視人民，而是人民知道他們可能隨時被監視[217]。即使人們沒受到監視，也會有如受到監視時一般，盡可能順從、服從並合乎期望，避免任何脫序或不正常的

---

[215] 然而，論者 Greenwald 即曾指出，諸如打電話向自殺防治專線求助、前往墮胎診所、常常瀏覽色情網站、預約復健診所、正在做某種疾病的治療或告密人打給記者等，這些人有許多保密的理由，卻不涉及違法或犯罪。*See* GREENWALD, *supra* note 184, at 181.

[216] Gleen Greenwald, Why Privacy Matters, TED, http://www.ted.com/gleen_greenwald_why_privacy_matters, 時間軸 10:40 以下。

[217] *Id.*

行為，不敢有絲毫逾矩，以免遭到羞辱和譴責[218]。

此等擔憂並非空穴來風。精神科醫師王浩威即指出，社會對「差異」的容忍度其實並不高：

> **「我們的社會是不容許任何差異的，從言談舉止到道德理性，幾乎都恨不得大家像機器人般一模一樣。這樣的社會理念已強大到無孔不入的程度，連當事人的意識也都充滿了這種社會典範的警告聲響，以致於自責地認為自己是十足的怪物了[219]。」**

> **「人類的社會從來都沒有想像中理性或科學，反而是自以為是的要求一致的標準，任何逸出常態的人事物，就會被斥為異常而遭驅逐。而在童年和青少年階段，就面臨社會集體的拒絕，更是讓人只能發展出一套全然不尋常的生存方式。於是，在主流社會的眼光中，他們更不正常了[220]。」**

牛津大學 Viktor Mayer-Schonberger 教授亦點出，在數位科技與全球網路的推波助瀾下，常態由「記得」取而代之，「遺忘」反倒成了例外[221]。由於你我一言一行都記錄在可輕易存取的數位記憶中，必須面對當代甚至未來的批判，如此縝密的數位記憶，有如一座更邪惡的數位圓形監獄（digital panopticon），造成寒蟬效應，使得個人成為驚弓之鳥，不願意再發表言論[222]，且會開始自我審查[223]。

若未賦予人民手機資訊充足之保護，等同於人民的精神上秘密空間隨時有暴露於國家機器眼前之風險。當個人的所有需求、想法、慾望、愛好與喜悅，

---

[218] GREENWALD, *supra* note 184, at 173-75.
[219] 王浩威，《我的青春，施工中——台灣少年記事》，初版，頁 198（2003 年）。
[220] 同前註，頁 209。
[221] VIKTOR MAYER-SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 2 (2009).
[222] *Id.* at 11.
[223] *Id.* at 5.

陷於隨時可能曝光（遭到國家權力介入檢視）的風險之中，為了不要變成別人眼中的怪胎、遭人異樣眼光看待，個人很可能會迎合世俗眼光而扭曲人格、隱藏自我。例如一位男同志若知道自己手機所存資訊可能會隨時遭受檢視，他可能會將手機內的同志交友軟體刪除、不再使用手機瀏覽同志相關網站，偽裝成「正常的異性戀」，隱沒於大眾[224]。

再設想一對交往中的男女朋友，倘若女方之手機任何時候都可能被男方突襲檢查，女方很有可能會自我監控，例如減少與其他男生聊天、不再明目張膽上網看帥哥照片、不敢出入男方所不喜之場所等，行為模式多少會與不受監看時有所差異，人格自由發展因而受到限制[225]。

男女朋友間的手機監視，尚且對個人人格有如此影響。如果今天有權檢視者係國家權力，人民手機內之資訊有可能冷不防被攤在檢警眼前時，國家除以打擊犯罪為名目，檢查人民手機有無違法跡證外，亦可能打著安全的旗號，羅織罪名檢查人民手機，意圖箝制不利政府的資訊流通。

實際上，中國當局曾以安全檢查為名，對西藏拉薩人民（尤其是喇嘛）之手機進行大規模搜索，藉以掃除對外傳播西藏訊息的份子。日前發生之四川藏民自焚抗議中共西藏政策之事件，由於相關消息與照片泰半係透過手機傳布，

[224] 事實上，同志畏懼他人眼光，隱藏真實性傾向、偽裝成「正常」異性戀假結婚的案例，屢見不鮮，詳見：同志悲歌！與妻結婚 30 年如陌生人 只為「正常」，中時電子報，2015 年 6 月 30 日，http://www.chinatimes.com/photo-app/20150630002078-260804；楊政郡、蘇金鳳，嫁 22 年做不到 10 次 才知老公是同志，自由時報，2015 年 5 月 29 日，http://news.ltn.com.tw/news/society/paper/884540（最後瀏覽日：2016 年 1 月 12 日）。

[225] 以所謂的「恐怖情人」為例，此類人對另一半往往控制慾極強，例如無時無刻要求伴侶交代行蹤、每次見面都檢查手機內容，以及掌握通訊軟體以完全監控另一半的訊息狀況等。一旦另一半與其他異性有多餘的互動，就會在另一半頭上扣以不忠、背信、謊言之類的大帽子。受到嚴密監控的他方伴侶，則因時時生活在被監控的恐懼之下，除行為模式言行舉止多所限制外，更容易產生自卑、恐慌、憂鬱、緊張等負面情緒，個人人格所受戕害不可謂不大。詳見 Leo，避免交往到「恐怖情人」，精神科醫師：小心這三種類型，The News Lens 關鍵評論，2014 年 10 月 20 日，http://www.thenewslens.com/post/83676；魯皓平，該如何聰明分手？辨別恐怖情人的 5 大徵兆，遠見，2014 年 9 月 23 日，http://www.gvm.com.tw/webonly_content_3357_1.html（最後瀏覽日：2016 年 1 月 12 日）。

亦引來中共當局以安全檢查為名，對藏人手機的大規模搜索與監控[226]。南韓檢方亦曾以防止網路散播侮辱總統的言論為由，調閱用戶對話紀錄、監控 LINE、Kakao Talk、WhatsApp 等時下流行之通訊軟體，意圖箝制反對總理朴槿惠之言論[227]。

由此觀之，若吾人未能正視手機之特殊性，未給予手機資訊足夠的保護，而讓手機資訊有可能冷不防被攤在國家面前，或隨時可能遭到當局檢查，個人很可能會自我監控修正（如減少使用手機、遠離異議人士或批評政府之資訊、避免發表當局所不喜之意見或參與當局所不喜之活動等），人格發展亦因而受到箝制。

當「老大哥正在看著你（Big Brother is watching you）」的外在監視陰影如影隨形，個人不斷自我監控修正之下，人格失去自由發展的空間，終將生長成扭曲變形的樣貌[228]。國家偵查犯罪固有其必要，惟法院仍應適時踩下煞車，為人民隱私守住最後一道防線。

早在 1928 年 *Olmstead v. United States* 一案，美國聯邦最高法院 Brandeis 大法官在其不同意見書中便已警告，人民應對政府的舉措有所戒心：

「當政府立意良善時，經驗教導我們更應保持警惕、捍衛自由。居心不良的統治者意圖侵犯人民自由時，生而自由的人，會很自然地排斥。

---

[226] 相關新聞詳見 China launches crackdown on personal cellphones in Lhasa, Tibetan Centre for Human Rights and Democracy (Mar. 11, 2013), http://www.tchrd.org/2013/03/china-launches-crackdown-on-personal-cellphones-in-lhasa；【中國禁聞】5 月 21 日完整版，新唐人新聞網，2015 年 5 月 23 日，http://www.ntdtv.com/xtr/b5/2015/05/23/a1198729.html（最後瀏覽日：2016 年 1 月 12 日）。

[227] Sid Weng，南韓監控 LINE 等通訊軟體 箝制反朴槿惠言論，THE NEWS LENS 關鍵評論，http://www.thenewslens.com/post/82740（最後瀏覽日：2016 年 1 月 12 日）。

[228] 監控對個人可能產生的傷害，可參考林子儀（2015），〈隱私權法制的新議題：監控與隱私自我管理〉，《第五屆馬漢寶講座論文彙編》，頁 78-81。

善意、充滿熱誠卻缺乏理解的人，反而可能蠶食鯨吞，成為自由最大的隱患[229]。」

此言實可作為我國的借鏡。國家安全、追訴犯罪固然重要，人民權利卻也可能在偵查辦案的過程中一點一滴被侵蝕殆盡。如果我們一再容許國家擴張監視與搜索的容許範圍，推到極致，小說《1984》所描繪的天羅地網指日可待，自由不復存在，小說終將不只是小說。

誠如 Greenwald 所言，警方某些舉措固然可以遏阻犯罪，例如警察如果可以無令狀搜索家宅、國家有權在你我家中裝設監視器、聯邦調查局可以監聽扣押我們的談話與通訊，或許確實能夠較容易地掌握犯罪情資，防杜違法情事。惟憲法增修條文第四條的重要目的，即在於避免政府國家恣意入侵。限制政府行為，確實有提高犯罪率、置己身於更高風險之可能，但絕對的實質安全並非我們唯一重要的社會價值。私領域與生活品質的許多要素——創意、探索、親密——息息相關，將國家摒除於私領域之外，係凌駕於實質福祉之上的核心價值[230]。

犯罪追訴與隱私保障之間，說到底，終究是價值選擇的問題。誠如林子儀大法官在司法院釋字第 603 號解釋之協同意見書所言：

「此刻，我們必須停下來思考，究竟我們想要什麼樣的社會？想要以什麼為終極目的的國家？如果一個社會裡的成員，人人皆盡透明，沒有什麼動態可以逃脫於國家的監視之下，所有成員的資訊都鉅細靡遺地掌握在國家機器之中，並且可以輕易地透過某一則個人資訊追溯其全部行蹤與活動，這或許將是一個零犯罪的社會，而且很可能是一個非常有效率的政府，但人們也可能將過著充滿被監視恐懼的生活。治

[229] Olmstead v. United States, 277 U.S. 438, 479 (1928). 中譯為作者自譯。
[230] GREENWALD, supra note 184, at 207-08.

安與效率都是國家應該追求之重大公益，惟其終究必須停留在某個界限之後，不能無止境地一昧向前，犧牲其他一切[231]。」

我們想要生活在哪一種社會？是賦予檢警莫大的偵查權限，無所不用其極地挖掘出可能的犯人，即使犧牲個人隱私也無所謂的淨化社會？抑或願意承受一部分罪犯逃脫法網的代價，換取個人更多的呼吸空間，減少讓所有人民的隱私悉數暴露於檢警眼光的風險？隨著所踩立場不同，對於國家搜索人民手機資訊的限制寬嚴，亦會有所變動。我國搜索扣押制度是否應予修正，是否應慮及手機的獨特性質而有所調整，以兼顧個人隱私保障與國家保全證據之需求，即為後文所欲探討的問題。

3. 3. 3. 3. 違憲審查應採嚴格審查標準

承前所述，手機資訊雖應受憲法隱私權保障，然國家因有追訴犯罪、保全證據之需要，於符合憲法第二十三條意旨之範圍內，仍得由法律明確授權檢警以強制手段取得個人手機內資訊。對於此等限制人民隱私權之法規範，應採何種審查基準進行違憲審查，或可借鏡司法院釋字第 603 號解釋審查指紋資訊案的思考脈絡。

大法官於本案指出，在違憲審查密度的選擇上，須視所蒐集個人資訊之性質是否私密敏感、或易與他資料結合詳細之個人檔案，對具體個案採取不同密度之審查：

「……（國家強制取得個人資訊之）法律是否符合憲法第二十三條之規定，則應**就國家蒐集、利用、揭露個人資訊所能獲得之公益與對資訊隱私之主體所構成之侵害，通盤衡酌考量**。並**就所蒐集個人資訊之**

[231] 釋字第 603 號解釋，林子儀大法官之協同意見書參照。

性質是否涉及私密敏感事項、或雖非私密敏感但易與其他資料結合為詳細之個人檔案，於具體個案中，採取不同密度之審查[232]**……**」

本案中，考量到指紋係個人身體之生物特徵，具有人各不同、終身不變之特質，一旦與個人身分連結，即屬具備高度人別辨識功能，經由建檔指紋之比對，將使指紋居於開啟完整個人檔案鎖鑰之地位等特性，大法官最終對於本案採取嚴格審查標準：

「國家基於**特定重大公益之目的**，而有大規模蒐集、錄存人民指紋，並有建立資料庫儲存之必要者，應以法律明定其蒐集之目的，**其蒐集之範圍與方式且應與重大公益目的之達成，具有密切之必要性與關聯性**，並應明文禁止法定目的外之使用[233]。」

若參考大法官論述指紋資訊的思考脈絡，再將目光聚焦於手機資訊，其恐不僅僅是指紋般的「開啟完整個人檔案之鎖鑰」，而係「完整個人檔案」本身。如前所述，手機已成為現代人歷史資訊之寶庫，手機使用者的各種生活細節，悉皆記錄在其中。對人民手機之搜索，形同讓人民的精神上秘密空間、生活中最私密的細節（如不欲人知的私密日記、親密照片等個人隱私），盡皆暴露於國家機器之目光下。若許國家恣意發動手機搜索，檢警可迅速自手機內的通話、訊息、照片、社群軟體等資訊，監控個人生活樣貌。輕則導致人民成為驚弓之鳥，行為多所節制，只求隱沒於大眾；重則可能促使人民不斷自我監控、自我修正，人格發展扭曲變形[234]。

正因手機資訊既可能涉及私密敏感事項，亦有如詳細之個人檔案，手機搜

---

[232] 司法院釋字第 603 號解釋理由書參照。

[233] 同前註。

[234] 監控對個人的不利影響，詳見前文之討論。另參司法院釋字第 689 號解釋理由書：「蓋個人之私人生活及社會活動，隨時受他人持續注視、監看、監聽或公開揭露，其言行舉止及人際互動即難自由從事，致影響其人格之自由發展。」

索對人民隱私實造成嚴重干預，本文認為，對於國家以強制力取得手機資訊之規範，應採取嚴格審查標準，即立法目的須為追求重大公共利益，手段與目的之達成間具直接及絕對必要關聯，且賦予人民獲立即司法救濟之機會，始符合憲法比例原則及保障人民基本權利之本旨。

此外，本文認為，法院審查相關規範時，亦應謹記司法院釋字第 392 號解釋理由書之提醒，隨社會整體之變遷而適時檢討改進，「依據抽象憲法條文對於現所存在之狀況而為法的抉擇[235]」。如此方能防杜政府可能的濫權搜索，避免人民生活在可能恣意受到搜索的恐懼之中，也為人民留下一塊不受干預、自由發展的淨土，落實憲法對人民隱私權之保障。

[235] 司法院釋字第 392 號解釋理由書參照。

4. 手機資訊隱私之保障——以美國法手機搜索案件為借鏡

德國學者 Roxin 嘗云：「刑事訴訟法是憲法的測震儀[236]」，執法實務如何解釋實踐刑事訴訟程序，事涉憲法保障之人民權利得否具體落實。承續前文之討論，基於維護人性尊嚴與尊重人格自由發展等理由，隱私權已藉由歷次大法官解釋，躍居受憲法保障之基本權利。然而，憲法對基本權利之保障並非絕對，基於公益之必要，國家得於不違反憲法第二十三條之範圍內，以法律明確規定強制取得所必要之個人資訊。

由於手機內所載資訊既廣且深，刑事偵查程序中，檢警常鎖定手機取證，試圖從手機內的資訊查找可能的偵查線索或定罪證據，諸如作案犯嫌的通聯記錄及簡訊、手機內的定位紀錄[237]、性侵害加害人手機中的被害人裸照、案發現場之照片或錄影等，均為偵辦案件時的重要證據，故其之於犯罪偵查程序益發重要。除了手機內的資訊外，手機本體也可能藏有涉案證據，我國實務上即有警方於犯嫌手機背蓋內搜出毒品之前例[238]。

國家為確保刑事訴訟程序順利進行，追訴犯罪時為達證據保全之目的，有實施搜索扣押等強制處分之必要。基於正當法律程序之保障，檢警偵查時若認有搜索扣押之必要，必須踐行令狀原則等法定程序要件，方得實行[239]。換言之，個人隱私非受絕對保障，檢警搜索亦非絕對禁止，但必須具備相當理由、向法

[236] 引自林鈺雄，《刑事訴訟法（上）》，6 版，頁 20（2010 年）；林鈺雄，《干預處分與刑事證據》，初版，頁 5（2008 年）。

[237] 手機的定位紀錄，有時會被檢警作為在場或不在場證明的依據。

[238] 萬華毒販：手機背蓋裡面沒有毒品 立馬被警方揭穿，ETtoday，2014 年 10 月 24 日，http://www.ettoday.net/news/20141024/417512.htm（最後瀏覽日：2016 年 1 月 12 日）。

[239] 最高法院 93 年台上字第 664 號刑事判例：「刑事訴訟，係以確定國家具體之刑罰權為目的，為保全證據並確保刑罰之執行，於訴訟程序之進行，固有許實施強制處分之必要，惟強制處分之搜索、扣押，足以侵害個人之隱私權及財產權，若為達訴追之目的而漫無限制，許其不擇手段為之，於人權之保障，自有未周。故基於維持正當法律程序、司法純潔性及抑止違法偵查之原則，實施刑事訴訟程序之公務員不得任意違背法定程序實施搜索、扣押……」

官聲請搜索票，始與正當法律程序之保障無違。

自手機資訊之性質觀之，實屬電磁紀錄[240]之一種。電磁紀錄有別於實體證據（例如文書、兇刀、兇槍等），具有易於無痕複製修改、回復可能性高、不易證實來源及完整性、不易確定製作人身分、內容無法直接被人類感知理解而需要藉由電腦等設備顯示內容，以及蒐證困難等特性[241]，其搜索扣押程序亦與傳統實體證據有所不同。

以違法持有槍枝的案件為例，其屬傳統一階段的搜索扣押，亦即警方多會將現場搜索完畢後隨即扣押槍枝，而不會將處所內鍋碗瓢盆等物，全數扣回偵查機關後，再一一篩選過濾[242]。但若警方所欲取得者係電磁紀錄（如毒品交易紀錄、綁匪與共犯的通訊內容等），由於電磁紀錄載體內所存之資料甚鉅，常須借助專家之力鑑識，且需耗費大量時間，故警方大多會先將現場硬體全數扣回，回到偵查機關後再行鑑識，對載體中的檔案逐一檢視搜索，以取得犯罪證據。這樣的程序等同進行兩次搜索，且兩次搜索之時間、地點與執行者多不相同。若硬將傳統實體證據搜索扣押程序套至電磁紀錄上，即會產生一些看似矛

[240] 許多論者以「數位證據」為名對此加以討論，例如法思齊（2011），〈美國法上數位證據之取得與保存〉，《東吳法律學報》，第 22 卷第 3 期，頁 95-147；徐仕瑋（2013），〈數位證據與現行搜索、扣押法制間之適用問題——以硬碟等儲存媒介之搜索、扣押為中心〉，《檢察新論》，第 13 期，頁 29-46。然數位證據一詞尚未為我國刑法與刑事訴訟法採用，目前仍以電磁紀錄稱之，如刑法第 10 條第 6 項：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」及同法第 220 條第 2 項：「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。」以及刑事訴訟法第 122 條：「對於被告或犯罪嫌疑人之身體、物件、電磁紀錄及住宅或其他處所，必要時得搜索之。對於第三人之身體、物件、電磁紀錄及住宅或其他處所，以有相當理由可信為被告或犯罪嫌疑人或應扣押之物或電磁紀錄存在時為限，得搜索之。」及同法第 165-1 條：「錄音、錄影、電磁紀錄或其他相類之證物可為證據者，審判長應以適當之設備，顯示聲音、影像、符號或資料，使當事人、代理人、辯護人或輔佐人辨認或告以要旨。」為行文之便，本文均使用「電磁紀錄」一詞。

[241] 綜合整理自王旭正、柯永瀚（2007），電腦鑑識與數位證據：資安技術、科技犯罪的預防、鑑定與現場重建，頁 37；林一德（2000），電子數位資料於證據法上之研究，台灣大學法律學研究所碩士論文，頁 124-129；劉秋伶（2010），數位證據之刑事證據調查程序，政治大學法律學研究所碩士論文，頁 23-26。

[242] 本例引自李榮耕（2012），〈電磁紀錄的搜索及扣押〉，《國立臺灣大學法學論叢》，第 41 卷第 3 期，頁 1059。

盾、扞格不入的論理[243]。

此等搜索扣押強制處分，即使踐行正當程序，其對人民之隱私權及財產權之限制是否適切，仍不無討論餘地。為求犯罪證據而搜索扣押整隻手機，有如為尋找一本書而搜索扣押整座圖書館的書籍，似有不符比例之嫌，亦可能對個人隱私造成過度限制。

鑒於國家犯罪偵查需求與個人資訊隱私保障之衝突，本章爰以手機內資訊之搜索為中心，引進美國法案例作為借鏡，探究我國現行手機搜索規範是否符合比例原則。論述案例之安排邏輯，則以檢警逮捕時得否附帶搜索、逮捕後欲搜索手機時應如何聲請搜索票、取得令狀搜索手機時得否強制受搜索人解鎖手機、搜索手機資訊是否適用附帶及另案扣押，依序討論。

第一節先就我國手機搜索之執行現況予以說明，針對手機附帶搜索、搜索票之記載核發、手機密碼之提出以及手機內電磁紀錄如何搜索等具體案件，試圖描繪我國現行實務作法之輪廓。第二節則以美國法院實務判決與學說見解作為研究素材，引介涉及手機搜索之案例，並整理該國學者的見解與詮釋，觀察該國法院身處手機科技飛速進展之脈絡下，當犯罪偵查需求與手機隱私保障有所衝突時，如何求取兩者之間的平衡，期能作為我國日後面對手機相關議題時之借鏡。第三節為本文見解，論述美國法院判決所帶來的省思，復對我國現行手機搜索規範進行合憲性檢驗，並提出修法建議。

[243] Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 86-90. (2005). *See also* Bryan K. Weir, *It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21 GEO. MASON U. C.R. L.J. 83, 85 (2010)；李榮耕（註 242），頁 1059-60。

4. 1. 我國手機搜索實際情況之介紹分析

4. 1. 1. 手機之附帶搜索

我國刑事訴訟法第 130 條規定：「檢察官、檢察事務官、司法警察官或司法警察逮捕被告、犯罪嫌疑人或執行拘提、羈押時，雖無搜索票，得逕行搜索其身體、隨身攜帶之物件、所使用之交通工具及其立即可觸及之處所。」本條即為附帶搜索制度，授權執法人員得於逮捕拘提當下為無令狀搜索。之所以如此規範，主要係著眼於逮捕或拘提被告現場瞬息萬變之特殊性：由於被告可能以身上藏匿的凶器傷人拒捕，抑或湮滅隨身攜帶之證據，故授予檢警附帶搜索之權，直接確認被告身上是否攜帶凶器或證據，以維執法人員安全，亦收證據保全之功[244]。

觀附帶搜索制度之立法目的，本係設想被逮捕人身上可能攜帶刀槍、毒品等凶器或證據，故賦予檢警附帶搜索之權，以茲因應。然隨著科技進步，電子產品日新月異時，附帶搜索之執行漸生爭議。舉例言之，警方逮捕被告並行附帶搜索時，若被告身上攜帶手槍、小刀、毒品等物，因此類物品有傷人或遭湮滅之虞（如以隨身小刀或手槍傷警拒捕，或將毒品沖入馬桶湮滅證據），警方行附帶搜索後予以扣押，較無爭議。但警方如於被告身上搜出一支手機，此時警方得否附帶搜索被告手機中簡訊、照片、定位資訊、通聯紀錄等所有資訊？抑或僅得暫行扣押，必須另外聲請搜索票，方得就其內資訊為搜索？自我國實務以觀，由於目前搜索扣押手機之相關執行規範未臻明確，導致涉及手機之爭議案例並不在少數。

例如我國警方曾於逮捕犯人時，強行「代為保管」受逮捕人之手機，執法

[244] 參林鈺雄，《刑事訴訟法（上）》，6 版，頁 412（2010）；王兆鵬，《刑事訴訟講義》，5 版，頁 149（2010）；林鈺雄（2001），〈拘提證人與附帶搜索〉，《月旦法學雜誌》，第 75 期，頁 14-15；王兆鵬（1999），〈論附帶搜索〉，《月旦法學雜誌》，第 55 期，頁 118。

理由則係「怕他又打電話找來一群人」致使逮捕與偵訊受到阻礙[245]，此一代為保管之行為究應如何定性？而在陳情抗議之現場，警方以公共危險等罪嫌將抗議人士以現行犯逮捕時[246]，也有被逮捕之抗議人士表示，警方當下係直接沒收其手機，甚至直接刪除手機內檔案[247]；嗣後檢察官開偵查庭時，亦在未向法院聲請搜索票的情況下，要求被逮捕人交出手機、當庭檢視手機內的通訊軟體之對話內容，引發被逮捕人抗議[248]。是類行為是否可認為附帶搜索之一種？似未見討論。

對於得否附帶搜索手機之議題，我國實務尚未對此作出明確之結論。惟我國法院曾著有一則判決，該案被告涉嫌毒品案件遭警方逮捕，手機則被附帶扣押。回警局後，兩周前向被告購買毒品之人正好於此時打電話來，欲向被告再次購買毒品。警方未經同意即偽裝成被告接聽電話，與其相約會面交易，交易時將其當場逮捕。後依其供述，查悉兩周前之販毒情事[249]。

被告於審判中爭執警方未經同意取走被告之手機，亦未聲請監聽票而接聽被告之電話，相關證據應無證據能力。然法院認為，被告因涉嫌毒品案件被警

[245] 楊忠翰，沒收洪崇晏手機　警：怕他撂來一群人，蘋果即時，2014 年 5 月 5 日，http://www.appledaily.com.tw/realtimenews/article/new/20140505/392215（最後瀏覽日：2016 年 1 月 12 日）。

[246] 人肉鎖鍊擋座車 魏揚遭逮，蘋果日報，2014 年 6 月 27 日，http://www.appledaily.com.tw/appledaily/article/headline/20140627/35921557（最後瀏覽日：2016 年 1 月 12 日）。

[247] 林朝億，學者：讓警察上法庭當被告 法治才會進步，新頭殼 newtalk，2014 年 7 月 5 日，http://newtalk.tw/news/2014/07/05/48921.html（最後瀏覽日：2016 年 1 月 12 日）。

[248] 詳參黑色島國青年陣線總召魏揚之臉書：「昨天烏來行動之後，午夜召開的偵查庭中，某位檢察官在庭訊一開始就要求我們的某位成員繳出手機，甚至當庭親自滑手機，檢視我們成員手機內的通訊軟體之對話內容，之後隨即表示要扣押，經過折衝之後才改為要求我們成員日後提供螢幕截圖。另外一位夥伴的手機更是直接被扣押作為證物，只因為他在現場負責攝影、蒐證等自我保護的動作。以上程序完全沒有妥善的『搜索票』等程序……」參魏揚，Facebook，2014 年 6 月 27 日，https://www.facebook.com/dennis.wei.90/posts/818410921504606（最後瀏覽日：2016 年 1 月 12 日）。

[249] 本案被告涉嫌販賣毒品予 A 男，且以手機作為聯絡工具。被告販毒當時並未被警方查獲，然兩周之後，被告開車行經台南某一交叉路口時，因服用安眠藥之故，被告竟在駕駛座上昏睡，車子停在路中央快車道上。警方巡邏時見此情狀察覺有異而上前盤查，盤查時看到乘客座上有個拉鍊未關上的小錢包，內有疑似海洛英的粉末。經被告同意搜索、打開錢包檢視後，發現其內確實是海洛英，員警遂將被告帶回警局偵訊。詳見高等法院台南分院 96 年上訴字第 1358 號刑事判決。之後最高法院 97 年台上字第 1972 號刑事判決維持原判。

方依法逮捕，手機亦被附帶搜索扣押，而在警方之保管持有中。因販毒者通常皆以電話為聯繫毒品交易之犯罪工具，故他人撥打被告行動電話，有相當理由可信其與所涉犯毒品案件有關，因而警方之接聽應屬「蒐集被告犯罪證據目的範圍內之必要處分行為」，所得證據應有證據能力[250]。

法院雖未對警方有無權力附帶搜索受逮捕人之手機內容明確表示意見，惟就本案情節而論，法院認警方為蒐集犯罪證據之目的，即有權檢視並接聽被告之手機。法院日後是否會依此邏輯，擴及認定檢警附帶搜索手機、檢視其內資訊之行為，亦屬蒐集被告犯罪證據目的範圍內之必要處分，值得吾人繼續觀察。

4.1.2. 手機搜索票之核發

檢警若欲實行搜索扣押等強制處分，除了法定例外情狀外，原則上必須先行聲請令狀。令狀制度之初衷，係鑑於搜索扣押等強制處分對人民財產、隱私等基本權利有所侵害，為於國家追訴犯罪與人民權利保障間求取平衡，爰要求執法機關執行搜索扣押必須具備「相當理由」之實質原因、特定所欲搜索之標的物，進一步向法院聲請搜索票後，始得為之。此制旨在避免檢警過度重視犯罪偵查而忽視人民權利，爰建立事先審查制，一方面藉由聲請程序促使警方判斷搜索相當理由之有無、提升辦案細心度；另方面亦由中立超然之法院事先予以審查，以此避免無實質原因或非必要的強制處分[251]。

於傳統涉及實體證據之案件，法院所核發之搜索票，應具體而特定地記載欲搜索之物為何，以防免概括搜索之流弊[252]。詳言之，人民除受到令狀原則保護外，令狀上之記載亦須明確特定，違法搜索所得之證據原則上應予排除。如

[250] 同前註。
[251] 王兆鵬，《刑事訴訟講義》，5 版，頁 85-91（2010 年）。
[252] 同前註，頁 138。

檢警欲搜索一間房子，應扣押之物若為槍，檢警即不得打開比槍更小的信封檢視信件內容；若為拘捕搜索，檢警亦不得打開無法藏人之抽屜搜索其他證物。此等規範運作下，人民隱私得以受到適度保障。

惟令狀明確性之要件，遇上搜索電腦、手機等電磁紀錄載體時，由於搜索人員事前並不知道涉案檔案會以什麼形式、什麼路徑存放在載體上，搜索票之記載便有困難。我國學者法思齊教授即指出，現行實務上，我國法院為予執法人員方便，對於電磁紀錄之搜索，多承認較簡易且有彈性的描述方式，允許搜索票應扣押之物僅記載「應扣押之與本案有關之電腦及其相關設備、磁片、光碟及其他電磁紀錄」。惟其亦點出此種作法可能過於概括，不符搜索扣押客體應具體特定以維護人民隱私之要求[253]。

就此而論，於電磁紀錄搜索票核發上，我國實務對於令狀明確性之要求似乎有所放寬，並未要求警方應視個案情狀與所得情資特定所欲取證之資訊，而是容許較為概括的記載。

4.1.3. 手機密碼之提出

隨著科技進展、隱私意識抬頭，檢警取得手機內容作為犯罪證據之路愈發艱難。由於智慧型手機資料容易外洩，定位功能也可能反被警方用以追蹤，傳統舊式手機近日越來越受毒販青睞[254]。而在智慧型手機部分，蘋果公司宣布，自 iPhone 6 起的最新加密系統有別以往，不再留下安全門。如此一來，即使法院命令該公司破解手機，該公司亦無計可施[255]。蘋果公司執行長 Tim Cook 為

[253] 法思齊（2011），〈美國法上數位證據之取得與保存〉，《東吳法律學報》，第 22 卷第 3 期，頁 143。
[254] 販毒者最愛「機王」 諾基亞 8210，蘋果日報，2015 年 4 月 30 日，http://www.appledaily.com.tw/realtimenews/article/new/20150430/602239（最後瀏覽日：2016 年 1 月 12 日）。
[255] Government Information Requests, APPLE, http://www.apple.com/privacy/government-information-requests (last visited Jan. 12, 2016).

此變革下了註解：「人們有權擁有隱私[256]。」政府若欲取得手機內的資料，只剩下兩條路：其一是想辦法自行破解，惟破解加密系統常需費時數年[257]，甚至永遠解鎖不開；其二則係逼迫被告說出破解密碼。

若審判中確有檢視被告手機資料的必要性，是否可以強行要求被告輸入密碼將手機解鎖？主要爭點在於，強迫被告提供密碼解鎖手機，是否違反不自證己罪特權？亦即，密碼是否屬於不自證己罪所欲保護的客體？被告對此有無權利保持緘默？

被告有無義務吐露手機密碼，涉及緘默權保障，緘默權又源於不自證己罪特權。相較於美國憲法增修條文第五條明文保障人民享有不自證己罪特權[258]，我國憲法並未對此明文。不自證己罪，意指不得強迫被告在刑事程序中成為對自己不利的證人，不得強迫被告自白犯罪[259]。之所以賦予被告此等權利，其最主要的目的，係防止國家機關強迫被告揭露其所知、所信、所思，再藉此入被告於罪[260]。被告若無緘默權，將陷於三難處境：陳述不實須受偽證處罰、拒絕陳述則為藐視法庭、據實陳述等於自我入罪[261]。

因此，針對受不自證己罪所保護的客體，國家不得以強制力取得，亦不得因被告拒不合作，而施以間接或直接的法律上制裁或事實上處罰[262]。此項權利體現在刑事訴訟法上，即為被告之緘默權[263]，以及證人之拒絕證言權[264]。緘默權係不自證己罪特權核心內涵之一，被告對於被控訴之罪嫌，可由對己最有利

---

256 *Id*.
257 iPhone 6 加密後 若無用戶密碼　解鎖要花 5 年半，ETtoday，2014 年 9 月 29 日，http://www.ettoday.net/news/20140929/407141.htm（最後瀏覽日：2016 年 1 月 12 日）。
258 美國憲法增修條文第 5 條：「……不得強迫刑事罪犯自證其罪……」
259 王兆鵬（2008），〈不自證己罪保護之客體〉，《一事不再理》，頁 225、227。
260 同前註，頁 227。
261 王兆鵬（註 251），頁 340。
262 王兆鵬（註 259），頁 227。
263 如我國刑事訴訟法第 95 條第 1 項第 2 款。
264 如我國刑事訴訟法第 180 條以下之規定。然因本段主軸係討論被告有無義務吐露手機密碼，故不另探究證人之拒絕證言權。

之防禦角度，選擇是否陳述以及保持緘默與否[265]。惟此一特權之射程範圍，究竟僅限於不得強制取得被告具供述或溝通性質之供述證據[266]，抑或更廣泛地包括禁止國家要求被告配合偵查而主動提供非供述證據[267]，目前尚無定論。

在美國，由於有藐視法庭罪（contempt of court）之設，故在判決密碼非屬供述證據、不受不自證己罪保護的幾個州，法院實務上會命令被告輸入密碼，或提出一個「解除加密的硬碟（或手機）」。若被告拒不提出，法院即以藐視法庭罪處罰被告，將被告關到他願意輸入密碼為止。

遍覽我國刑事訴訟法之規定，唯一可能強制被告解鎖的管道，應係刑事訴訟法第 133 條第 2 項之提出命令:「對於應扣押物之所有人、持有人或保管人，得命其提出或交付。」惟本條目前對於拒絕提出之情況未設有罰則，僅於同法第 138 條規定：「應扣押物之所有人、持有人或保管人無正當理由拒絕提出或交付或抗拒扣押者，得用強制力扣押之。」對於實體證據，或可強制搜索扣押[268]，惟就手機密碼而論，由於密碼僅存在被告或嫌疑人腦中，並無以強制力扣押之可能，因此，我國法院目前實務做法，多半是將上鎖的裝置委由刑事警察局、法務部調查局資通安全處等相關單位破解[269]。

手機密碼與不自證己罪特權之關係，在我國尚未受到重視。實務僅有判決

---

[265] 林鈺雄，《刑事訴訟法（上）》，6 版，頁 158-59（2010）。
[266] 王兆鵬（註 251），頁 375。
[267] 林鈺雄（註 265），頁 159。
[268] 如臺灣高等法院 102 年度上易字第 1256 號刑事判決，法院即請工人直接以電鋸打開上鎖之保險箱：「101 年 3 月 7 日法院人員強制執行當日，伊、被告、張仁龍律師、法院人員、警察、公證人均在場，執行標的是要打開姜孟璋在仁富公司的專用保險箱，該保險箱是工人用電鋸打開，因要開姜孟璋的專用保險箱，不知內容有哪些，故伊找公證人在場確認裡面東西，以便認證處理，打開保險箱，看到什麼就是什麼……」。
[269] 如臺灣高等法院刑 103 年度上重訴字第 35 號刑事判決，法院將殺人案被害人已加密之電腦硬碟送請刑事警察局解密，惟解密失敗；又如臺灣高等法院 103 年度金上訴字第 5 號刑事判決，法院將被告之筆記型電腦送刑警局鑑識，破解硬碟內之加密文件（內容為犯案計畫）等。除刑事警察局外，有時亦送法務部調查局資通安全處處理。如高等法院 101 年上易字 2837 號刑事判決，將被告使用之電腦送該實驗室鑑定比對監造日報表修改前內容；又如高等法院 101 年侵上訴字 122 號刑事判決，亦將被害人之電腦送該實驗室鑑定 MSN 訊息對話紀錄並未遭竄改等，均由資安處處理。

提及警方涉嫌毆打拒不提供密碼之嫌犯[270]、嫌犯被捕時迅速將手機關機稱忘記密碼[271]等，惟並未就得否強迫被告吐露手機密碼之爭議有所處理。法院是否認為手機密碼是否等於筆跡、DNA 或抽血檢驗，得強制被告提出？檢警或法院有無權力強制被告輸入手機密碼以解鎖？目前尚乏論述。

4.1.4. 手機資訊之附帶扣押與另案扣押

現今社會中，手機資訊儲存量龐大，業如前述。檢警搜索人民手機的過程中，若意外發現本案其他證據或涉及他案之證據，是否一律適用附帶扣押及另案扣押[272]得為證據，即值討論。

附帶扣押之規定，見於刑事訴訟法第 137 條第 1 項：「檢察官、檢察事務官、司法警察官或司法警察執行搜索或扣押時，發現本案應扣押之物為搜索票所未記載者，亦得扣押之。」附帶扣押係授權執法人員在執行搜索扣押時，發現涉及「本案」而應扣押卻未記載於搜索票上之物時，亦得扣押之。刑事訴訟法第 152 條則係另案扣押之規定：「實施搜索或扣押時，發見另案應扣押之物亦得扣押之，分別送交該管法院或檢察官。」所謂另案扣押，顧名思義係指執法人員執行搜索扣押時，若意外發現非涉本案之「另案」應扣押之物，亦得予以扣押[273]。

自我國法院判決以觀，檢警為偵辦某一特定猥褻案件而搜索被告所有之電磁紀錄載體，過程中若同時發現其他猥褻案件之犯罪證據，法院直接承認自該電磁紀錄載體內搜出之所有本案及他案證據（裸照及猥褻影片）之證據能力，

---

[270] 詳見臺灣高等法院 101 年度上訴字第 2336 號刑事判決被告之抗辯：「惟被告乙○○原審審理中則稱：當天警察要問我的手機密碼，我回答不知道，魏彥鼎因此憤而動手打我，在動手前，魏彥鼎還刻意叫一個警察去把甲○○帶進來……」。

[271] 見臺灣高等法院 99 年度上訴字第 506 號刑事判決：「逮捕被告時，被告有掙扎、反抗，將其行動電話迅速關機，嗣稱忘記手機密碼藉以阻礙警方辦案，被告當時態度很不配合……」。

[272] 我國附帶扣押與另案扣押之制度，源於美國一目瞭然法則。參王兆鵬（註 251），頁 208。

[273] 林鈺雄（註 265），頁 426。

以之作為論罪科刑依據[274]。

由此觀之，針對電磁紀錄搜索扣押，我國法院似未與實體證據區別處理，而係全面適用附帶扣押與另案扣押制度，搜索過程中所得之所有本案及他案證據，均得作為證據。換言之，搜索 A 案電磁紀錄載體時，若意外發現 B、C、D 案之證據，涉及 A 案之本案證據得適用附帶扣押，涉及 B、C、D 案之他案證據則適用另案扣押，全數均有證據能力而得分別論罪。搜索硬碟時如此，搜索手機時應亦如是。

對我國法院所採見解有所了解後，次節即引介美國法院審理手機搜索之案例，作為我國日後處理相關案件及法制修改之借鏡。

4. 2. 美國法院對於手機搜索之見解

承前所述，美國憲法增修條文第四條明確保障人民不受不合理搜索扣押，並揭示搜索扣押應具令狀之基本原則：搜索扣押必須具備法院之令狀，令狀發給必須基於相當理由，令狀之記載必須明確特定。一方面對執法機關搜索扣押之行為予以限制，另方面亦適度保障人民的隱私。

[274] 如我國高等法院 102 年侵上更(一)字第 17 號刑事判決：本案被告於海軍陸戰隊上校退役後，與妻共同經營國小幼齡學童之課輔安親班，並擔任補習班班主任。其先以情緒化而嚴厲之方式管教學童，使學童噤若寒蟬不敢違逆，復見時機成熟，遂佯裝關懷並擁抱女童，見女童對此肢體接觸不為反抗，再漸次為猥褻及性交行為並拍攝裸照。大部分女童因年幼難以訴說被害情節及經過，被告亦在行為後警告女童不得向外透露，否則將「有事」發生。嗣後因其他被害女童之家長發現有異而報警。檢察官獲報後，持搜索票對被告之住處、租屋處及補習班等處所加以搜索，在補習班內一樓辦公室之電腦及外接式硬碟內，以電腦刪除資料回復軟體還原被告已刪除之十名被害女童之裸照、猥褻及性交照片檔案數張，同時另扣得數位相機及外接式硬碟，始查悉上情並起訴被告。
高等法院 101 年侵上訴字第 451 號刑事判決案情亦類似：本案中，被害人 A 女因注意力不足及過動而至復健專科診所治療。被告係該復健診所之職能治療師，在對 A 女進行一對一個別治療時，利用其年幼心智發展未臻成熟，要求 A 女將全身衣服褪去，並以手與下體對其強制猥褻，事後告訴 A 女這是兩人間的秘密、要求她不得告訴外人云云，猥褻時間長達五年。A 女年幼識淺，從未對家人提及上開情事。嗣後係因另一位女童告發被告，警方查扣被告之數位攝影機，將該攝影機送內政部警政署刑事警察局還原已刪除之視訊檔案後，赫然發現其中存有 A 女之影片，向 A 女詢問後方得悉上情，爰蒐集證據並將被告起訴。
上舉二例中，被害人均未主動報案，而係檢警於搜索他案證據時意外發現被害人之影片，方才得悉案情而一併偵辦。

而在認定政府行為是否屬於搜索時,法院多半會引用 Harlan 大法官於 *Katz v. United States* 一案協同意見書中所提出的「合理隱私期待」判準：個人已表現出對於隱私實際而主觀的期待，且該期待對社會而言是合理的。警方行為若會侵害個人的合理隱私期待，即屬搜索，原則上須事先向法院聲請令狀，始得為之[275]。

然美國聯邦最高法院亦創設了若干例外以因應實務需求，授予警方於特定情狀下，雖無令狀仍得逕行搜索之權，附帶搜索即為一例[276]。附帶搜索制度起源於十七世紀[277]，歷經 *Weeks v. United States*[278]、*United States v. Rabinowitz*[279]、*Chimel v. California*[280]、*United States v. Robinson*[281]、*New York v. Belton*[282]、

[275] Katz v. United States, 389 U.S. 347, 361 (1967).

[276] 其他尚包括如緊急搜索、同意搜索、邊界搜索等。

[277] 王兆鵬（2003），〈論附帶搜索〉,《搜索扣押與刑事被告的憲法權利》，頁 168。

[278] Weeks v. United States, 232 U.S. 383 (1914). 本案被告 Week 係快遞公司之職員，警方認其涉及運送彩券而逮捕被告，又於未取得令狀下搜索被告居處兩次，扣押文件及信件、信封等作為證據。被告主張警方係無令狀違法搜索，請求返還扣押物。聯邦最高法院認為，警方逮捕時確有附帶搜索之權，藉以取得犯罪證據，然搜索範圍並不及於受逮捕人的居處。故本案警方無令狀搜索被告居處，已侵犯被告受憲法增修條文第四條保障的權利，證據應予排除。本案除係最高法院首次論及附帶搜索制度之判決外，亦為證據排除法則之始。

[279] United States v. Rabinowitz, 339 U.S. 56 (1950). 本案警方於被告的辦公室中逮捕被告，並在未另行取得搜索票的情況下搜索被告的辦公室達一個半小時之久。最高法院認為，因辦公室很小，警察對於受逮捕人立即且完全可控制的範圍內為搜索，係屬合理搜索，並未違反憲法增修條文第四條之規定。

[280] Chimel v. California, 395 U.S. 752 (1969). 本案警察至一名竊盜罪嫌之家中逮捕該名嫌犯，並以合法逮捕得行附帶搜索為由，徹底搜索嫌犯所居住的三房之屋，閣樓與停車間亦在搜索之列，部分房間內的抽屜也被打開。法院推翻之前 Rabinowitz 案的見解，限縮附帶搜索之適用範圍。法院認為，附帶搜索之範圍僅限於被逮捕人之人身，及其立即可觸及之範圍。至於被逮捕人無法立即觸及之處所，並不在附帶搜索容許之列，警方應另外聲請搜索票始得搜索之。法院於本案明確宣示附帶搜索之兩個理由：其一，由於被逮捕人很可能以武器拒捕或逃逸，故應容許搜索嫌犯、取走其身上的武器，以確保執法人員安全與逮捕之執行；其二，亦應容許執法人員搜索並扣押被逮捕人身上的證據，避免嗣後遭到隱匿或湮滅。

[281] United States v. Robinson, 414 U.S. 218 (1973). 本案警方因被告 Robinson 駕駛牌照已遭吊銷之汽車而將其逮捕。警方於其身上搜出一包皺巴巴的香菸盒，然並不確定盒內所裝之物為何。打開包裝後，警方發現 14 顆裝有海洛因粉末的膠囊。本案爭點在於，警方為附帶搜索時，是否有權檢視被告身上的容器？最高法院認為，合法逮捕屬憲法增修條文第四條之例外，也是該條意義下的「合理搜索」。因此，警方有權打開被告隨身攜帶的所有物品與容器，至於容器打開與否並非所問。法院於本案判決之中特別宣示,附帶搜索並不需要逐案裁量是否有安全維護與證據保全之搜索必要性。換言之，只要是合法逮捕，警方有絕對的權限可以徹底搜索被逮捕人的人身與隨身物品，而非由法院事後判斷該情狀下是否有可能發現武器或證據。附帶搜索之絕對原則（categorical rule）或明確原則（bright-line rule）即在本案告確立。

Arizona v. Gant[283]等案之論述與修正。惟此一法則究否適用於手機，美國各級法院見解歧異，直到 2014 年，才由聯邦最高法院之判決定於一尊。

4. 2. 1. 手機豁免於附帶搜索之適用：*Riley v. California*[284]

美國各級法院對於附帶搜索究否適用於手機，各有不同見解。有認為手機有如隨身容器，應准許為附帶搜索；亦有認為手機性質與一般容器迥異，不得附帶搜索者。法院的分歧意見，導致警方執法無所適從，也引發相當多的學者討論。為了弭平爭議，聯邦最高法院受理了兩個事實類似但結果完全不同的案件：*Riley v. California* 與 *United States v. Wurie*。兩案爭點均為警方逮捕被告、行附帶搜索並扣押手機後，可否在無令狀的情況下，搜索檢視被逮捕人手機內的資訊？

下級法院見解分歧：*Riley* 案法院對此採肯定見解，警方對被告 Riley 之智慧型手機進行附帶搜索並不違法；*Wurie* 一案結果恰恰相反，法院認為附帶搜索被告 Wurie 的傳統手機與維護安全、保全證據的目的不符，員警不得為之。面對下級法院的分歧意見，最高法院決定受理兩案，並將其合併審理。以下分就兩案之事實予以敘述，再詳加介紹最高法院的見解。

---

[282] New York v. Belton, 453 U.S. 454 (1981). 本案中，警方攔阻一超速行駛之汽車，盤查時聞到車內傳來大麻味，爰逮捕被告並命令其與車上四名乘客均下車。員警行逮捕後附帶搜索整輛汽車，於車後座的被告夾克發現毒品。被告抗辯本案附帶搜索違法，所得毒品不得作為證據，應予排除。但最高法院將 Chimel 案「立即可觸及之範圍」延伸至整輛車內部與車內所有容器。所謂容器，係指所有可容納其他物品之物，且無論開閉均得搜索。之所以容許員警打開容器檢視，並非因為乘客對於容器內的物品沒有隱私期待，而係認為合法逮捕本身係限制乘客隱私利益之正當理由。因此，本案之附帶搜索並無不法。然而，法院於判決書中一併指出，汽車後行李箱並不屬於犯嫌立即可觸及之範圍，故不得對後行李箱為附帶搜索。

[283] Arizona v. Gant, 556 U.S. 332 (2009). 法院於本案重新闡釋 Robinson 案所建立之明確原則，復將 Belton 案對附帶搜索的發動要件予以修正。最高法院表示，執法人員逮捕嫌犯後，原則上仍必須先聲請搜索票，始得搜索該車輛。惟最高法院仍在原則之外開了兩扇小門：若員警有相當理由相信可以在車內發現本案相關證物，或者逮捕時嫌犯尚未完全受制，可能從車上立即可觸及之範圍內取出武器，威脅警方人身安全時，即可搜索。本案共有五名執法人員，且警方已將 Gant 一行人銬於警車內，被逮捕人根本無從接觸其車輛，更遑論取得車輛內的物品拒捕或傷及員警安全，或湮滅、藏匿犯罪證據，因此，警方無令狀附帶搜索車輛之舉，並不合法。

[284] Riley v. California, 134 S. Ct. 2473 (2014).

4. 2. 1. 1. 案例事實

Riley 一案，警方因被告 Riley 駕駛牌照過期之汽車而將其攔下，攔查後發現其駕照已被吊銷，爰扣押該車並依警局政策搜索車內物品。警方於引擎蓋下搜出兩把手槍，隨即轉以持有槍械之罪名逮捕被告。對被告進行附帶搜索時，警方搜出一支智慧型手機，未聲請令狀即打開手機並檢視資訊。員警發現許多文字前都註記 CK，推測其為 Crip Killers 之縮寫，係日前曾犯下槍擊案之 Bloods 幫派成員所使用的暗語。回警局後，一位專辦幫派案件之警探再度檢視手機內容，找出影片以及被告與涉案汽車之合照等證據。最後 Riley 被依謀殺未遂、槍擊等罪名遭到起訴。被告主張警方在無令狀亦無緊急情況下搜索手機內容，違反憲法增修條文第四條，請求排除證據[285]。

而在 *Wurie* 一案，被告 Wurie 因涉嫌販賣毒品而遭警方逮捕並帶回警局。警方扣押被告身上的兩支手機，其中一隻折疊式手機卻不斷接到來電，來電顯示為「我家（my house）」。警方未取得令狀即打開手機檢視「我家」的電話號碼，循此找到 Wurie 的公寓，並聲請令狀搜索之，於公寓內發現 215 克的高純度古柯鹼、大麻、毒品吸食器、槍枝、子彈與現金。嗣後 Wurie 被依散布毒品、意圖散布而持有毒品以及持有武器之重罪等罪名遭到起訴。被告抗辯，搜索公寓所得證據係非法搜索手機所生之毒樹果實，應予排除[286]。

4. 2. 1. 2. 本案爭點

上述兩案事實雖異，惟爭點則屬同一：警方逮捕被告並扣押手機後，可否不聲請搜索票，直接附帶搜索被逮捕人手機內的數位資訊？

[285] *Id.* at 2480-81.
[286] *Id.* at 2481-82.

4. 2. 1. 3. 判決理由

4. 2. 1. 3. 1. 搜索手機資料與附帶搜索之原意相悖

本案判決由首席大法官 John Roberts 所主筆。判決理由首先爬梳附帶搜索例外自 *Weeks* 案、*Chimel* 案、*Robinson* 案及 *Gant* 案等案件的發展歷程，重申附帶搜索之授權理由有二：防止被逮捕人以隨身物品傷害執法人員、防止隨身證據遭到湮滅。法院認為，搜索手機資訊與這兩個理由不符[287]。

詳言之，以確保執法人員安全而言，數位資料本身明顯無法對警方的人身安全造成任何威脅，故不應容許對手機內資料為搜索。若員警欲檢視者係手機外觀，例如檢視機身與機殼之間是否藏有刀片等物件，由於此類物品確實可能危害警方安全，則無不許之理[288]。

再以防止證據湮滅而論，政府主張，如不許附帶搜索手機，即使已將手機扣押，手機內資料仍可能遭遠端刪除[289]，或因加密技術而永遠無法破解讀取[290]。針對上述疑慮，法院提出了解套方式：其一係將手機關機，抑或拔除電池，以防手機連上網路；其二，若有資料加密的疑慮（例如手機自動鎖定或重開機需輸入密碼），警方亦可讓手機保持開機，並將其放到可隔絕外界訊號之處，例

[287] Riley v. California, 134 S. Ct. 2473, 2482-85 (2014).
[288] *Id.* at 2485.
[289] 意指手機連上無線網路時，收到刪除資料的訊號。此可藉由第三人發送遠端訊號，或者預先設定程式在進出特定區域時自動將資料刪除（即所謂地理圍籬（geofencing））而達成。
[290] 政府主張，由於逮捕當下被逮捕人可能正在使用手機，手機呈解鎖狀態，若不許員警於此時搜索手機，等到之後手機自行鎖定，嗣後鑑識人員就算花費無數的精力與時間，費時數年也未必能破解。詳情可參考 United States v. Wurie 案口頭辯論，美國司法部副檢察長（deputy solicitor general）Michael R. Dreeben 所提出的主張："Because if the phone turns off and becomes encrypted, officers can go to the magistrate and ask for a warrant, but it may be months or years or never if they can break through the encryption and actually obtain the evidence. So to the extent that the traditional destruction-of-evidence rationale justified the search of a cell phone or justified the search of traditional items, it applies even more strongly with respect to cell phones than it does with most of the items that might be seized from a person." 取自 *Riley v. California*, OYEZ, http://www.oyez.org/cases/2010-2019/2013/2013_13_132 (last visited Jan. 12, 2016).

如將其置入法拉第袋[291]中，隔絕外來的無線電波[292]。

然而，若於特定個案警方仍認為證據有滅失的潛在風險，真的面臨「現在或永不（now or never）」的兩難困境，例如被告手機的資料可能立刻被遠端清除，此時警方可援用「緊急情況」之例外，立即搜索手機。或者，警方正好扣押未上鎖之手機，此時警方有權解除手機自動鎖定的功能，防止該手機自動鎖定及加密資料[293]。

4. 2. 1. 3. 2. 利益權衡下本案人民隱私重於政府利益

除討論附帶搜索的原始目的外，最高法院進一步權衡政府利益與個人隱私之輕重。考量到逮捕情境瞬息萬變，附帶搜索確實有保護員警人身安全與保全證據之重大政府利益。至於人民的隱私期待，雖因其受逮捕而減低，仍非完全不受憲法增修條文第四條所保障[294]。

政府曾主張，搜索手機內資訊，一如傳統搜索實體物件，兩者之間並無實質差別。然法院駁斥此等見解，認為這有如在說騎馬上月球與搭機飛向月球兩者並無不同，都是由 A 點到 B 點的方式云云，並不可採[295]。就本案所涉及的手機而言，其上所儲存之資訊，無論質與量都與實體物件相去甚遠，現今手機已成為具備通話功能的小型電腦，而這台電腦同時具備相機、影片播放器、通訊錄、日曆、錄音機、圖書館、日記、相簿、電視、地圖或報紙等各種功能[296]。且觀現今人手一機的普遍性，也可能讓火星來的訪客誤以為手機是人類解剖上

[291] 法拉第袋（Faraday bag）係一以鋁箔製成、大小類似三明治袋的小袋子。其以著名科學家法拉第命名，可以阻絕外界的電磁訊號。
[292] Riley v. California, 134 S. Ct. 2473, 2487 (2014).
[293] *Id*.
[294] *Id*. at 2488.
[295] *Id*.
[296] *Id*. at 2489.

之重要特徵[297]。

法院舉例指出數位與實體搜索之間的區別。手機問世前，搜索個人受到物理限制，隱私侵害有限，人們不可能將所有的信件、照片或書籍隨身攜帶。即使有人當真如此，也必須拖著行李箱出門，警方則須聲請令狀以搜索行李箱，而非如 *Robinson* 案的香菸盒般直接行附帶搜索[298]。如判決書中所述：

> **「大多數人不太可能拖著過去幾個月收到的所有信件、曾經拍攝的每張照片或是自己看過的所有文章和每一本書出門——人們沒有能力也沒有動機這麼做[299]。」**

但搜索手機時，隱私侵害即無此等物理限制。現代手機儲存空間龐大，使其儲存各種資訊的能力倍增，除了將位置、便條、處方、銀行對帳單、影片等不同種類的資訊匯整在一處，較資訊散布各處時透露出更多訊息外，亦使得單一種類的資訊可以透露較以往為多的訊息。例如，個人手機中數以千計附有日期、地點與描述的照片，即可拼湊一個人私生活的全貌；智慧型手機的定位資訊，可以精準定位到個人身處哪個城鎮的哪棟建築物裡，如此即可重建某人每時每刻的足跡，產生精確而完整的個人外出行蹤紀錄，揭露大量關於家庭、政治、職業、宗教甚至是性關係的細節。手機應用程式則提供許多管理個人生活各種資訊的工具，像是民主黨新聞或共和黨新聞、酒癮藥癮或賭癮、懷孕症狀追蹤、禱告邀請分享、預算管理、任何想得到的嗜好或消遣、改善情感生活等。智慧型手機使用者平均會安裝三十三個應用程式，將其綜合起來，即可拼湊出使用者的生活全景，搜索手機所暴露的資訊甚至遠比搜索家宅還多[300]。

此外，法院亦意識到雲端運算可能引起的爭議：

---

[297] *Id.* at 2484.
[298] *Id*. at 2489.
[299] *Id.*
[300] *Id*. at 2490-91.

「使用者在許多現代手機上瀏覽的資訊，可能並沒有實際儲存在裝置內……手機使用者往往不知道特定資訊究竟是儲存在裝置上還是放在雲端，而這其實也沒有太大的差別。同一種類型的資訊，某一使用者可能存放在本地裝置，另一個使用者則可能存在雲端[301]。」

「若允許執法機關附帶搜索手機的雲端資料，就有如於嫌犯口袋裡找到一把鑰匙後，即可開鎖並搜索嫌犯的屋子。當執法人員在搜索手機資料的時候，一般也不太清楚其正在瀏覽的資訊，究竟是在逮捕當下已儲存在本地端，或者是從雲端抓下來的……這類搜索可能擴大到被逮捕人隨身文件、財產以外之物[302]……。」

綜上所述，法院認為，相較於傳統實體物件，應將手機視為一個新的類別。手機搜索所涉及的隱私利益遠遠超過舊時的香菸盒、手提包或皮夾等物，數位資料應與實體物件區別處理[303]。惟在緊急情狀下（如證據確有立刻遭到遠端刪除之風險、誘拐兒童者在手機中存有被害人的位置資訊等），警方仍可適用緊急例外為無令狀搜索，事後再由法院進行個案審查[304]。

法院並不諱言本案判決會衝擊執法機關打擊犯罪的能力，對此，Roberts大法官寫道：「隱私是有代價的[305]（Privacy comes at a cost）。」在犯罪偵查上，手機已成為犯嫌溝通聯絡的重要工具，其內常存有重要的犯罪證據。然就隱私而論，就手機內所儲存的龐大資訊以觀，人民生活隱私盡在其中。科技發展至今，使人民得以將這些資訊攜至掌中，但制憲者對這些資訊的保護並不因此減少。鑑於這一事實，法院對於搜索手機的回應非常簡單：「聲請搜索票[306]（get a warrant）。」

---

[301] *Id*. at 2491.
[302] *Id*.
[303] *Id*. at 2493.
[304] *Id*. at 2494.
[305] *Id*. at 2493.
[306] *Id*. at 2494-95.

4. 2. 1. 3. 3. Samuel Alito 大法官之協同意見

Alito 大法官雖同意本案的判決結論，惟論理上則與多數意見有所不同，爰另提一份協同意見書，提出兩點意見。

第一，Alito 大法官指出多數意見對於附帶搜索認知上的謬誤。其並不同意多數意見認為附帶搜索旨在維護執法人員安全、防止證據湮滅的論理，復援引文獻與判決先例指出，附帶搜索制度至少在憲法增修條文第四條制定一世紀前即已形成，而 *Weeks* 案以前的案件則認為附帶搜索係基於取得證據之需求。此外，維護安全與防止湮滅兩個理由，亦無法解釋判決先例所建立的附帶搜索範圍。例如先例准許警方得檢視受逮捕人隨身文件、審判中並得作為證據。惟文件一旦離開受逮捕人，證據湮滅與員警安危兩個風險均不存在。因此，Alito 大法官認為 *Chimel* 案對於附帶搜索的論理實有違誤，不應以此錯誤論理影響本案之論證[307]。

Alito 大法官亦指出，數位時代以前發展出的原則，不應機械性適用於手機搜索。鑑於手機的特殊性，應於執法與隱私利益間取得新的平衡。多數意見尋得的平衡點讓數位資訊比紙本受到更多保護，惟此一取徑實有矛盾。若兩名嫌犯同時遭到逮捕，一號嫌犯的口袋有市話帳單、皮夾裡有照片，兩者均可證明犯罪；二號嫌犯的口袋則有一支手機，手機中的通聯紀錄與照片亦可證明犯罪。警方依判決先例可以無令狀搜索扣押前者的帳單及照片，依本案見解卻不得無令狀搜索儲存在手機內的資訊。

惟本案作法雖有矛盾，Alito 大法官仍認為目前別無更好的替代方案。執法機關需要手機附帶搜索的明確原則，法院則需藉由更多的時間與案件建立更精

[307] *Id.* at 2495-96.

緻的原則。與此同時，人民攜帶的電子裝置之本質亦仍不斷變動[308]。

也由於電子裝置不斷變動的本質，Alito 大法官進一步提出第二點意見：立法機關比法院更適合解決此類爭議。其引述判決先例指出，在 *Katz* 案判決電子監控雖未侵害財產利益仍屬搜索之後，國會隨即制定 1968 年綜合犯罪防治及街道安全法（The Omnibus Crime Control and Safe Streets Act of 1968），改以法律（而非法院判決）規範電子監控之授權與限制[309]。

手機除了被用於各類重大犯罪、產生許多嶄新的執法上難題以外，鑑於其在現代生活扮演的角色，搜索手機內容會涉及非常敏感的隱私利益。科技一再變遷發展下，法院並不那麼適合理解與判斷此等爭議。21 世紀的隱私保護，也不適合由聯邦法院以增修條文第四條此一「鈍工具（blunt instrument）」來解決。比起法院，由人民選舉出的立法部門，更適合去衡量與回應現今以及將來的變遷[310]。

4. 2. 1. 4. 相關評論

由於 *Riley* 案是最高法院對附帶搜索於數位時代之適用首次表示意見，早在法院同意頒布移審令時，即已引發不少關注。判決書一出，本案被報章譽為數位時代隱私權大獲全勝[311]、憲法增修條文第四條進入數位時代[312]，學者討論亦如雨後春筍。

---

[308] *Id.* at 2496-97.
[309] *Id.* at 2497.
[310] *Id.* at 2497-98.
[311] Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N. Y. TIMES (Jun. 25, 2014), http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html
[312] Jeffrey Rosen, *How the Supreme Court Changed America This Year*, POLITICO MAGAZINE (Jul. 1, 2014), http://www.politico.com/magazine/story/2014/07/how-the-supreme-court-changed-america-this-year-108497.html

判決作出隔日，Adam Gershowitz 教授立刻撰文分析本案。其點出本判決的三個特點：法官意見的一致性、法院拒絕妥協（未將不同手機區別處理）、法院採用絕對的明確原則禁止所有無令狀的手機搜索。就第一點而言，本案法官意見相當一致，僅 Alito 大法官提出一份簡短的協同意見。Gershowitz 教授認為，這可能係本案開庭時間已近議事期的尾聲，法官沒有充足時間整合不同意見之故。至於第二點，本案判決涉及智慧型與折疊式兩種手機，然法院除了給予新舊手機同等保護外，更明確摒棄 *Gant* 案標準（警方合理懷疑可搜出本案證據時，即可無令狀搜索）之適用。對此，Gershowitz 教授推測，係因法官意識到手機搜索與他們自身休戚相關、較能同理自身手機資訊揭露於他人眼前的困窘羞愧感，從而拒絕妥協，藉以保護如他們一般，同屬中產或菁英階級的人民。最後，本案判決立下十分明確而嚴格的標準，並未留下過多模糊地帶。即使仍留有緊急情狀的空間，惟警方必須證明相當理由之存在，就過往經驗言，門檻非常高。因此，Gershowitz 教授認為本案判決實為一縷清新的空氣[313]。

Daniel Solove 教授亦指出，本案削弱了第三人法則之基礎。法院注意到兩個重要關鍵：其一係資料有聚集效應（aggregation effect），少量資料或許無傷大雅，但資料量一大，一加一大於二，即可通盤描繪出一個人的生活。其次，法院也承認，在科技不斷變遷下，舊時的物理考量（地點、範圍）重要性漸減，真正重要的是資料本身，及其對個人生活的揭露。因此，就第三人法則而言，手機內的資訊雖多存於第三方（如服務提供者），依該法則應不受保護，惟法院於本案仍將手機內資訊納入保護，並未採取該法則之見解[314]。

---

[313] Adam Gershowitz, *Symposium: Surprising unanimity, even more surprising clarity*, SCOTUSblog (Jun. 26, 2014), http://www.scotusblog.com/2014/06/symposium-surprising-unanimity-even-more-surprising-clarity

[314] Daniel Solove, *Does the U.S. Supreme Court's Decision on the 4th Amendment and Cell Phones Signal Future Changes to the Third Party Doctrine?*, LINKEDIN (Jun. 25, 2014), https://www.linkedin.com/pulse/20140625172659-2259773-does-the-u-s-supreme-court-s-decision-on-the-4th-amendment-and-cell-phones-signal-future-changes-to-the-third-party-doctrine

論者 Ryan Watzel 也是從第三人法則的視角出發，再將議題進一步延伸至雲端儲存的問題。政府於本案曾主張，手機中的通聯紀錄，依第三人法則應不受保護；然另方面也讓步承認，未儲存於手機之雲端資訊因非屬「受逮捕人立即可觸及之範圍」而不得搜索。由於最高法院於本案並未對第三人法則適用與否明確表示意見，Watzel 爰舉例提問：警方雖無法附帶搜索 iPhone，惟若一位 iPhone 使用者將其個人資料悉皆備份至 Apple's iCloud 上，警方可否主張使用者自願向 Apple 揭露資訊，依第三人法則已無合理隱私期待，無須聲請令狀即得直接向 Apple 取得所有資料[315]？

Watzel 認為，依照 *Riley* 案的論理，應採否定見解，亦即使用者對雲端資訊仍有隱私期待。首先，依判決理由所述，法院肯認手機與雲端資訊就如同鑰匙與房子，不能因為警方搜出鑰匙（容量有限的手機）即允許其無令狀搜索整間房子（容量幾無上限之雲端）。再者，法院指出手機內的資訊包含瀏覽紀錄，其可能反映個人興趣或關心。這些資訊雖屬個人自願揭露予網際網路服務提供者的資訊，法院仍然認為其屬隱私。其三，判決書中明確指出：「手機使用者往往不知道特定資訊究竟是存在裝置還是雲端，**一般而言這沒什麼差別**」。所謂的沒有差別可能有兩種解讀：其一係指雲端資訊應受與本地端資訊相同的保護，其二則係，無論資料存於何處，無令狀搜索均侵犯了增修條文第四條的保障。無論何者，Watzel 均認為，自此句以觀，雲端資訊絕非不受保護[316]。

Orin Kerr 教授則主張法院應擴大本案判決的射程範圍，將本案論理延伸適用於其他電子儲存裝置。詳言之，*Riley* 一案之判決主要標的雖為手機，惟主筆之大法官 Roberts 既已於判決書中清楚指出手機等同於微型電腦，則本案判決理應進一步延伸適用至電腦、iPad 等其他裝置。本案為冰山一角，數位時代

[315] Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73 (2014).
[316] *Id.*

既已來臨，資料之質與量亦不可同日而語，此次既然開創了附帶搜索的新規則，其他法則亦應有所調整為是[317]。

Kerr 教授亦觀察本案與馬賽克理論之間的關係。其指出，Roberts 大法官於第一個註解即已否定本案與馬賽克理論有所關聯，判決理由中則同時有贊同該理論（手機中的各式資訊可重構一個人的生活）以及不贊同該理論（資訊累積至何時方達搜索之門檻並不明確）的兩種論述。因此，Kerr 認為本案並未採用馬賽克理論之見解[318]。

然並非所有學者均對最高法院判決表示肯定。任職於美國聯邦第七巡迴上訴法院、同時於芝加哥大學法學院任教之 Richard Posner 法官，即對本案論理以及令狀的實效性有所質疑。最高法院闡述憲法增修條文第四條要求搜索除緊急情狀外需具備令狀，以保護人民隱私，於 Posner 法官看來並非史實。增修條文第四條確實保護人民不受不合理搜索扣押，但其並未要求令狀，而係要求相當理由、宣誓（書），並特定搜索扣押之地點與物品。Posner 法官認為，本案最高法院雖要求搜索手機應具令狀，惟令狀核發之程序係執法機關單方為之、核發容易，事後質疑搜索合法性之成功機率微乎其微。其雖不反對搜索票之要求，卻也質疑憲法已失去原意，淪為法官造法之藉口而已[319]。

此外，哈佛法學論叢的評論中也提及，本案原可在討論附帶搜索手機不符附帶搜索原始目的後即可告終，惟法院卻不尋常地進一步採用合理性權衡（reasonableness balancing）的取徑，將政府利益與人民隱私予以權衡。此法於

---

317 Orin Kerr, *The significance of Riley*, THE VOLOKH CONSPIRACY (Jun. 25, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley。下級法院受本案判決影響，已開始將手機自汽車搜索例外之中排除，詳見 Orin Kerr, *Cell phones exempt from the automobile search exception, Ninth Circuit rules*, THE VOLOKH CONSPIRACY *(Dec. 11. 2014),* http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/12/11/cell-phones-exempt-from-the-automobile-search-exception-ninth-circuit-rules

318 *Id.*

319 Richard A. Posner, *The last thing a woman about to have an abortion needs is to be screamed at by the godly*, SUPREME COURT BREAKFAST TABLE (Jun. 26, 2014), http://www.slate.com/articles/news_and_politics/the_breakfast_table/features/2014/scotus_roundup/scotus_end_of_term_remembering_town_of_greece_and_more_on_cellphones_buffer.html

本案得出人民隱私應予保護之結論，一方面可能係因手機普及且與法官切身相關，二方面也可能是缺乏替代方案之故。然而，回顧先前 *Maryland v. King*[320]、*Florence v. Board of Chosen Freeholders*[321]等案，最高法院權衡下均犧牲人民隱私之判決，法院日後審理其他搜索案件（尤其對象是不受歡迎的族群時），未必能如本案般易地而處、保護隱私，實有隱憂[322]。

亦有論者對本案效力抱持著較為悲觀的態度。曾任美國司法部電腦犯罪部門副組長、現為律師之 Mark Eckenwiler 即表示，本案要求搜索手機須取得令狀，則警方此後必會改採同意搜索作為例行公事，而「異常多數的受逮捕人也會同意搜索，一如人們幾乎同意各式各樣對於車輛或容器的搜索，即使對其個人非常不利亦然」，故其並不認為此一判決會遏阻調查[323]。

4. 2. 2. 手機搜索票應明確特定：*United States v. Winn*[324]

如前所述，美國憲法增修條文第四條對搜索扣押設有規範，保障人民不受不合理之搜索扣押，並揭示搜索扣押應具令狀之基本原則：搜索扣押必須具備法院之令狀，令狀發給必須基於相當理由，且令狀之記載必須明確特定。

惟令狀明確性之要件，遇上搜索電腦、手機等電磁紀錄載體時，由於搜索人員事前並不知道涉案檔案會以什麼形式、什麼路徑存放在載體上，搜索票上之記載便有困難。對此，美國法院實務上已有針對智慧型手機之判決，認為手

---

320 Maryland v. King, 133 S.Ct. 1958 (2013). 法院於本案判決執法機關可以直接採取受逮捕人之DNA，無須事先取得令狀或有合理懷疑。其將「執法人員以安全且精確之方式確認受拘留人身分之需求」與「極小的侵害與減低的隱私期待」予以權衡，得出前者重於後者的結論。

321 Florence v. Board of Chosen Freeholders, 132 S.Ct. 1510 (2012). 法院於本案判決，拘留所有權對所有剛入所的受拘留人行脫衣搜身（strip search）。無論所涉犯罪輕重，亦無須存有合理懷疑，均屬合理搜索。多數意見權衡政府利益與對個人隱私之侵害程度後，認為脫衣搜身符合機構管理需求與受拘留人隱私間的平衡。

322 The Supreme Court, *2013 Term—Leading Cases*,128 HARV. L. REV. 251, 256-260 (2014).

323 John Schwartz, *Cellphone Ruling Could Alter Police Methods, Experts Say*, THE NEW YORK TIMES (Jun. 25, 2014), http://www.nytimes.com/2014/06/26/us/cellphone-ruling-could-alter-police-methods-experts-say.html

324 United States v. Winn, 79 F.Supp.3d 904 (2015).

機之搜索票仍須明確特定欲搜索之內容，始與美國憲法增修條文第四條保障人民隱私之旨無違，以下即就該案予以介紹。

4. 2. 2. 1. 案例事實

本案中，被告 Winn 一邊以手機偷拍游泳池中的一群年約 13、14 歲之未成年少女、一邊伸出手來自慰。警方擔心，被告若知自己被鎖定調查，可能會湮滅手機裡的證據，故探員前往被告家中與其談話後，要求被告交出手機。被告起先拒絕，但後來仍同意扣押[325]。幾天後，該名探員套用範本向法院聲請搜索票，搜索票上記載，聲請搜索被告手機中的所有檔案、SIM 卡與 SD 卡，搜索內容包括但不限於行事曆、通訊錄、聯絡人、簡訊、電子郵件、圖片、影片、相片、鈴聲、音檔、通聯記錄、安裝的應用程式、GPS 紀錄、WIFI 資訊、網路瀏覽歷程與用量以及系統檔案，已刪除之檔案亦屬之[326]。

探員獲得搜索票後，便將手機交給鑑識人員處理。鑑識人員以手機鑑識工具 Cellebrite UFED Touch machine，先以自動方式取出被告手機的資料，此時並未找到涉及本案之證據，卻搜出其他與本案無關之兒童色情圖片，以及三段偷拍未成年少女的影片。嗣後鑑識人員再改以手動方式搜索整支手機，於圖片庫中找到涉及系爭泳池偷拍案的照片[327]。

被告提出四項抗辯，主張手機內的證據資料應予排除：警方扣押手機後拖延九天才取得搜索票、探員無相當理由足認證據會存在手機裡、搜索票過於廣

[325] *Id.* at 909-10.
[326] 範本原文為：any or all files contained on said cell phone and its SIM Card or SD Card to include but not limited to the calendar, phonebook, contacts, SMS messages, MMS messages, emails, pictures, videos, images, ringtones, audio files, all call logs, installed application data, GPS information, WIFI information, internet history and usage, any system files on phone, SIM Card, or SD Card, or any data contained in the cell phone, SIM Card or SD Card to include deleted space. *Id.* at 911.
[327] *Id.* at 911-12.

泛而不符明確特定之要求、搜索範圍踰越令狀授權[328]。

4. 2. 2. 2. 本案爭點

本案爭點在於，警方搜索手機之令狀，其上之記載是否過於廣泛、不符明確特定之要求？搜索範圍是否踰越令狀授權[329]？

4. 2. 2. 3. 裁定理由

本案中，法院核發之搜索票，授權警方得搜索整支手機上「所有檔案」。對此，法院認為，系爭搜索票授權之搜索範圍明顯過於廣泛，既逾越相當理由所支持的搜索範圍，亦不符明確性之要求[330]。

詳言之，警方並非對於手機上「所有檔案」均具有得以搜索之相當理由，惟令狀卻授權警方搜尋所有檔案。特別是在輕罪（misdemeanor crime）案件，殊難想像警方為何需要搜索扣押如此大量的檔案。再就本案情節（公然猥褻）而言，法院認為只有兩類檔案符合足以搜索的相當理由：照片與影片。至於其他諸如行事曆、通訊錄、聯絡人等其他列在得搜索清單之檔案，並沒有得搜索之相當理由[331]。

系爭搜索票唯一設下的搜索限制僅有「與被告 Winn 所犯之罪相關」，法院認為這與憲法增修條文第四條明確特定之要求明顯不符，警方應更加精確地描述所欲搜索之檔案，或增加更多的搜索條件[332]。

法院指出，警方應依據事先調查所得、對於案情之了解，將搜索檔案之類

---

[328] *Id.* at 912.
[329] 本案法院判決係針對被告四項抗辯逐一回應，惟本文為簡潔並聚焦故，僅將本案介紹範圍鎖定於後兩個涉及手機搜索票之爭點。
[330] United States v. Winn, 79 F.Supp.3d 904, 919 (2015).
[331] *Id.* at 919-20.
[332] *Id.* at 921.

型與搜索之方式予以特定。於本案，由於警方並未依據相當理由，將搜索檔案之類型限縮於照片與影片，故整張搜索票實過於廣泛[333]（overbroad）。

此外，法院更進一步認為，即使警方具備相當理由得以搜索照片與影片，搜索票上僅指定檔案類型、而未敘述特定標的之作法，亦不夠明確特定（particularity）。以本案為例，令狀上若僅指定照片與影片兩個類型，將使警方得以搜索扣押手機上「所有」的照片與影片，但警方實應依據所得資訊，將搜索範圍依案發地點與照片主題予以限縮，例如特定拍攝地點（案發游泳池）、內容（在泳池邊穿著泳衣的女孩）與時間（案發當日），排除其他不相干的檔案，如此始合乎令狀明確性之要求[334]。

綜上，系爭搜索票之記載因過於廣泛、欠缺明確性，有概括搜索之嫌，而與憲法增修條文第四條之要求有違，由被告手機中所取得的所有證據，應予全數排除。

4. 2. 2. 4. 相關評論

對於本案判決結果，Kerr 教授點出其局限之處：判決先例指出，只要有相當理由認為電腦內存有一張兒童圖片，即可正當化搜索整顆硬碟（及其內別張兒童色情圖片）的行為。因此，如果案件情狀有所不同，例如政府有相當理由認為本案被告 Winn 手機內存有兒童色情圖片，將會變得相當棘手[335]。

除了本案搜索手機內部照片所生爭議外，亦有論者指出，搜索時若涉及雲端資訊，執法人員更無從事先猜測犯嫌會使用哪些雲端服務，更遑論特定搜索

[333] *Id.* at 922.
[334] *Id.* at 920-21.
[335] Orin Kerr, Court invalidates cell phone warrant as overbroad, THE VOLOKH CONSPIRACY (Feb. 23, 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/02/23/court-invalidates-cell-phone-warrant-as-overbroad

客體所在之處，畢竟證據資料可能存在各個不同的服務提供者端[336]。

既然事前以令狀限制似有困難，則電磁紀錄搜索之限制，究應採事前限制抑或事後審查，容有爭議。美國部分法院仍建議採行事前限制的作法，要求法官於事前檢視並同意搜索的步驟。Kerr 教授整理法院判決歸納出四種限制：在實體搜索階段限制硬體的扣押、限制電子搜索進行的時間、限制電子搜索進行的方式、限制何時須返回扣押硬體，以此限縮執法人員搜索的範圍[337]。

然而，考量到鑑識過程瞬息萬變而無法預測的本質，Kerr 教授認為此種作法有嚴重的缺失。其認為檢察官與治安法官於搜索開始前，並沒有足夠認知足以詳述整個搜索過程，須於打開載體、檢視檔案後，方知以何種工具何種程序搜索才能最快地找到所需證據。因此，法院實無法有效於事前（ex ante）評估電子搜索的合理性，故應於事後（ex post）再審查搜索的合理性即可[338]。

目前已有法院對於手機搜索票核發採取與 Kerr 教授相近之見解。如在 *United States v. Bazar* 一案，法院即認為，搜索數位證據時，由於檔名是可以變更的，犯嫌大有可能將藏有犯罪活動的證據改換一個無關的檔名以規避搜查。無論是文字檔、涉及多人之圖片等，均可能是系爭案件之證據，事前限制實有困難，故即使搜索票略有過於廣泛之情事，仍可容許[339]。

我國檢察官對此一議題亦曾撰文，採取與 Kerr 教授類似的見解。其指出數位鑑識過程之繁簡因個案而異，每案的證據與鑑識手段常隨著每個鑑識步驟有所不同，事前控制過於不切實際，而應容許對於儲存媒介（即電磁紀錄載體）窮盡檢索。是故，法官不宜越俎代庖，而應立於被動態勢，尊重數位搜索的專

[336] Aaron J. Gold, *Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software*, 56 WM. & MARY L. REV. 2321, 2348 (2015).
[337] Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure: A Reassessment*, 96 VA. L. REV. 1241, 1249-60 (2010).
[338] *Id.* at 1292-93. *See also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 574-76 (2005); Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 115 (2005).
[339] United States v. Bazar, Not Reported in F.Supp.3d, 2015 WL 6396011, at 2 (2015).

業性、技術性以及執法人員的判斷餘地，僅於事後審視個案程序的適法性，以證據排除法則防止政府濫權為已足[340]。

惟 Paul Ohm 教授對此則不表贊同。其認為以現今態勢而論，除了硬碟空間大幅增長外，人們亦習於將大量的敏感性資訊存在電腦硬碟中，例如出遊照片、通訊往來紀錄（電子郵件）等，硬碟內的資訊甚至會與他人連通分享，從而搜索已不僅影響受搜索人一人的隱私，甚至會導致數以百萬計的他人隱私亦遭侵害，其敏感性質與檔案櫃（filing cabinet）或 Kerr 教授比喻之資訊倉庫[341]（warehouse of information）大不相同。有鑑於電腦搜索性質上與概括搜索票（general warrants）極為相似，對人民隱私侵害甚鉅，故即使事前限制會造成執法人員沉重的負擔，然 Ohm 教授仍相信如此限制，始能促使執法人員想出在尊重人民權利的前提下有效執行搜索的方式，故仍以事前限制為妥[342]。

4. 2. 3. 手機密碼受不自證己罪保障：*Virginia v. Baust*[343]

隨著加密技術不斷進展，破解之路愈發艱難。誠如 *Riley* 一案政府於言詞辯論時所提出之主張，若不許員警於現場附帶搜索手機、放任犯嫌之手機自行鎖定加密，嗣後鑑識人員即使花費無數的精力與時間，仍未必能夠破解[344]。若鑑識人員確實無法破解手機，則可能的解套方式之一，即是強制被告自行輸入密碼。惟此舉是否侵犯被告受美國憲法增修條文第五條所保障之不自證己罪特

[340] 徐仕瑋（2013），〈數位證據與現行搜索、扣押法制間之適用問題──以硬碟等儲存媒介之搜索、扣押為中心〉，《檢察新論》，第 13 期，頁 44-45。類似見解：李榮耕（註 242），頁 1099-1100。
[341] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005).
[342] Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. In Brief 1, 6 (2011); 類似看法：Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 110 (1994).
[343] Virginia v. Baust, 89 Va. Cir. 267 (2014).
[344] 見前註 290。

權[345]？容有爭議。

關於得否強制吐露密碼的爭議，最有名的論述，當屬 1988 年 *Doe v. United States*[346]一案，Stevens 大法官於不同意見書中所提出的呼籲：

> **「被告可以被迫提出有罪的實質證據。指紋、血液、聲紋、筆跡或其他從被告身上採樣的物證，可以違反被告意願強制採取。但可以強迫被告運用其心智協助訴訟、入己於罪嗎？我認為不行。在某些案件中，或許可以強迫被告交出涉案文件所在保險櫃的鑰匙，但我不認為可以強迫其吐露牆上保險櫃的密碼──無論以口頭或行動[347]。」**

Stevens 大法官認為，強制被告簽署同意書予強制取得物證之間的差別，一如人類與動物之間的差異。若被告被迫運用自己的心智，以協助政府偵辦本案，則其將被迫成為「對自己不利之證人（a witness against himself）」，使政府取得之前並未存在的證據，再進一步使用這些證據追訴被告。Stevens 大法官進一步引先例指出，憲法增修條文第五條所反映的，係對於個人人格不可侵犯

---

[345] U.S. Const. amend. V: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; **nor shall be compelled in any criminal case to be a witness against himself**, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

[346] Doe v. United States, 487 U.S. 201 (1988). 本案大陪審團要求聲請人提出外國銀行的帳號協助調查，但聲請人被問到關於銀行帳號的存在及地點時，主張受到憲法增修條文第五條不自證己罪之保護而拒絕陳述。外國銀行依其本國法，則須得到客戶本人同意，始得將帳號紀錄交給政府。政府無法確定該等帳號是否確實存在，仍直接要求聯邦地方法院命令嫌犯於同意書上簽字。地方法院駁回聲請，認為強迫其簽署同意書違反不自證己罪的保護，惟遭上訴法院撤銷發回。地院更審後，命令聲請人應簽署同意書，聲請人不從，地院即判處其藐視法庭，上訴法院亦維持原判。本案嗣後上訴至聯邦最高法院。

最高法院費了極大篇幅回顧往例，討論同意書之簽署究否具有供述性質。法院認為，簽署同意書並未揭露嫌犯所知，亦不等於承認自己在外國金融機構擁有或控制銀行帳戶，不會表明是否有涉案文件存放在該外國銀行而可得出此類帳戶確實存在的結論 。即使該同意書讓政府得以接近潛在證據，惟同意書本身並不會指出其他潛在證據之所在，政府仍須自行尋找 。所謂的供述證據，必須是與事實主張或資訊揭露明確或隱然相關之口頭、書面陳述或行為，同意書之簽署並不具此等供述性質，故強迫嫌犯簽署同意書，並未侵犯其不自證己罪特權。本案多數意見在註腳 9 中對於 Stevens 大法官的不同意見亦有所回應，表示簽署同意書的情形比較像是強迫被告交出鑰匙，而非密碼的強迫揭露。承此，同意書之簽署有如強迫被告交出保險櫃鑰匙，不具供述性質，並不受保護。惟牆上保險櫃密碼之吐露則屬供述證據，應受不自證己罪保護而不得強迫被告為之。

[347] *Id.* at 219.

的尊重[348]（our respect for the inviolability of the human personality）。Steven 大法官這段文字，常被日後處理密碼案件的法院所引用。

早在智慧型手機普及以前，美國法院即已處理過許多得否強制輸入密碼解鎖電腦硬碟的爭議，下級法院意見分歧。例如 *In re Boucher*[349]、*United States v. Fricosu*[350]、*Commonwealth v. Gelfgatt*[351]等案，法院均認為，由於檢警事前已於

[348] *Id.* at 219-21.

[349] In re Grand Jury Subpoena to Sebastien Boucher, Not Reported in F.Supp.2d, 2009 WL 424718 (2009). 本案被告 Boucher 與其父開車自加拿大經佛蒙特州入境美國。邊境檢查站官員檢查 Boucher 之筆電時，發現電腦中一些檔案的檔名很可能與兒童色情有關，如「兩歲兒換尿布時遭到強暴」，於是請來另一名美國移民及海關執法局專辦兒童色情案件之特別探員協助。該名探員檢視筆電後在 Z 槽中發現為數眾多的成人色情檔案，以及許多兒童色情圖片與影片，Boucher 因此遭到逮捕，筆電則在關機後扣押。惟在日後的審判程序中，由於 Boucher 使用 Pretty Good Privacy 此一軟體將 Z 槽加密，Z 槽內之資料需要密碼始得讀取。政府鑑識人員證稱，由於此軟體並未留下後門，唯一可行的方式，係以程式持續猜測可能的密碼，而此一程序可能費時數年。因此，大陪審團發出傳票要求 Boucher 提供密碼或相關資料，Boucher 則抗辯此一要求侵犯其不自證己罪特權，請求法院撤銷傳票。

對於 Boucher 所提出的不自證己罪抗辯，原治安法官 Niedermeier 認為，密碼之輸入具有供述性質。至於證據發現是否已成定局，法官則認為政府對於 Z 槽中的檔案僅有先前已知之小部分之掌握，對其他可能的犯罪證據毫無所悉，不符合定局原則之要件。此外，由於定局理論應僅適用於有體物，而密碼無形、僅存在 Boucher 腦中，自無此原則之適用。因此，法院應被告所請，將原傳票撤銷。惟上訴審之 William K. Sessions III 法官推翻原見解，其認為提出行為會傳遞入罪事實須具備兩個要件：其一係政府對證據之存在與位置並無所知，其二係提出行為會透露物品係由被告持有掌握。就前者而言，法院首先討論所謂的定局，認為其並非意味著政府需要知道檔案的內容，與此相反，政府僅須對證據之存在與位置有合理明確之掌握即可。由於政府當初在 Boucher 配合搜索時已知悉筆電內藏有兒童色情檔案，被告提供解密之硬碟對於政府關於涉案證據存在與地點之所知幾無增益，從而並不符合第一個要件。就後者而論，Boucher 早已承認電腦為其所有，不需要藉由 Boucher 提出解密硬碟以證明此點，第二個要件亦不成立。因此，法院駁回 Boucher 撤銷原傳票之請求，命被告提出解鎖之 Z 槽。被告之後配合法院要求，遭判有罪確定。

[350] United States v. Fricosu, 841 F.Supp.2d 1232 (2012). 本案被告涉及不動產交易詐欺而遭偵辦。偵查程序中，警方聲請令狀搜索被告住處、扣押相關證據，其中包括三台桌電與三台筆電。於被告房中扣押的其中一台筆電受 PGP Desktop 程式上鎖加密，無法檢視內容，僅看得見硬碟名稱含有被告的名字。搜索結束後，被告打給服刑中的前夫，兩人談話中提及「東西在我的筆電裡」云云。該通電話被警方錄音，據此懷疑該上鎖筆電內存有涉案資料。為搜索其內證據，警方聲請該筆電的搜索票，並請求法院命被告交出解密後的硬碟資料。

地院法官 Blackburn 認為，即使政府無法確切指出特定檔案的存在及其內容，惟藉由先前通話錄音以及含有被告姓名的硬碟名稱，政府已得知涉案檔案存在於筆電之中、扣案筆電係由被告持有使用，故被告的提出行為並不會提供其他新的資訊。因此，解密電腦與提出檔案之行為即非供述，強迫被告提出硬碟資料並未侵犯其不自證己罪特權。綜上，法院裁定被告應提出解密後的硬碟，該提出行為本身則得享有證據使用豁免。

由於被告始終不願透露密碼。一個月後，警方自被告前夫處取得一系列可能的密碼清單，成功破解該筆電，解決此一困境。被告於判決做出隔年進入認罪協商程序，本案由是終結而未繼續上訴。

搜索時或其他間接證據得知涉案證據之存在，證據之發現已成定局[352]（foregone conclusion），密碼之提供實不具供述性質，故得強制被告解鎖。若法院要求被告解鎖硬碟（如命令被告輸入密碼，或提出一個「解除加密的硬碟」），被告卻拒絕提供，即可以藐視法庭罪處罰被告，將其關到願意輸入密碼解鎖為止

反之，在 *United States v. Kirschner*[353]、*In re Grand Jury Subpoena Duces*

---

[351] Commonwealth v. Gelfgatt, 468 Mass. 512, 11 N.E.3d 605 (2014). 本案被告為律師，涉嫌以偽造文書方式進行房貸詐欺，不法獲利超過一千三百萬美元，遭到警方鎖定偵查。警方除逮捕被告外，一併聲請搜索票搜索被告的住處與車輛，於被告住處扣押兩台桌電、一台筆電與其他電子裝置，以及被告車裡一台小筆電。然而，由於被告使用 DriveCrypt 軟體將四台電腦加密，該軟體並未留下後門，鑑識人員亦無法破解密碼，從而無法檢視電腦內之資料。政府主張本案重要證據很可能存在這些數位裝置中，且被告輸入密碼的行為不會傳遞其他未知的訊息，非屬供述，故不受憲法增修條文第五條之保護，爰請求法院強制被告輸入密碼，將電子裝置解鎖。
本案法院首先承認被告輸入密碼解鎖的行為確實可能揭露訊息，例如被告持有、控制這些電腦與其中內容。就此點而言，密碼之輸入與血液樣本、筆跡樣本之提供並不相同。惟法院進一步援引定局原則的例外：若證據之提出會傳遞的訊息早已為政府所知（提出行為僅些微增進政府所知或毫無助益），此時強制被告提出證據即未侵害不自證己罪特權。換言之，政府必須證明三件事：證據之存在、證據係在被告持有或控制之中、證據之真實性。政府基於先前的調查，已得知被告擁有這些電腦、被告以電腦進行交易、涉案資料存於電腦且受加密保護、被告確有能力解鎖等情事。承此，法院認為被告輸入密碼所傳遞的訊息已為政府所知而屬定局，並不具供述性質，不受憲法增修條文第五條之保護，最終判決被告應解鎖所有電腦。
惟本案也有兩位法官共同提出不同意見。不同意見書指出，就政府日前訊問被告所取得的資訊以觀，政府僅知被告以電腦進行不動產交易、懷疑證據可能存在電腦之中、電腦中的資料遭到加密等等，但對本案證據之有無、證據是否存在與位置之掌握毫無所悉。就此觀之，本案並未達到合理明確之標準，證據之發現自然非屬定局。
此外，由於被告係律師，電腦中尚存有其他案件當事人的資訊，被告亦自陳將電腦加密的理由之一即係考量隱私，若強迫被告輸入密碼，將使政府可以接觸到其他案件當事人的資訊。因此，在律師與當事人秘匿特權的考量下，亦不應強制被告解鎖。綜上，兩位法官提出不同意見書，認為不得強制被告輸入密碼。

[352] 詳見 Fisher v. United States, 425 U.S. 391 (1976). 此案為日後法院處理密碼相關案件樹立了重要的判斷基準。本案被告涉嫌稅務詐欺，法院認為，由於政府對於涉案文件已有合理確定（reasonable particularity）之掌握，證據之發現已成定局（foregone conclusion），故 Fisher 之提出行為（act of production）已無供述性質可言，不受憲法增修條文第五條之保護。換言之，若警方已知證據存在，且能證明證據所在位置時，即使強迫嫌疑人提供該證據，亦與不自證其罪特權無涉，理由係此種情形強迫被告提供證據僅等同於強制搜索。反之，若警方事前對證據是否存在、證據位於何處並無所知，此時若強迫被告提出證據，等於強迫被告自證其罪，違反不自證其罪特權。

[353] United States v. Kirschner, 823 F. Supp. 2d 665 (2010). 本案被告 Kirschner 涉嫌以電腦接收兒童色情檔案遭到起訴。為了取得被告電腦中的證據，政府方的律師向大陪審團聲請傳票，要求被告提供電腦及其內任何檔案所使用或相關的密碼，被告則以此侵犯不自證己罪特權為由，請求撤銷該傳票。
法院首先說明供述的定義，即強迫被告吐露對於該罪事實之所知，迫使其與政府分享自己的思想與信仰。回到本案，法院認為，強迫被告提出密碼會向政府傳遞事實上的主張，亦等同於強迫被告揭露自己之所知，具有供述性質。其援引 Stevens 法官在 Doe 案不同意見與 Hubbell 案多數意見鑰匙鎖保險櫃與密碼鎖保險櫃之著名比喻，指出本案政府欲經由被告心理活動獲取密碼，卻未提供相應足夠的證據使用豁免（政府只願就提出行為本身提供豁免），侵犯了被告之不自證己罪特權。因此，撤銷原傳票。

Tecum[354]兩案，由於檢警並未確知涉案證據是否存在所欲搜查的客體，定局原則在此並不適用，密碼仍受不自證己罪特權之保護。此時，則視政府是否願意提供證據提出行為與衍生使用之證據豁免，決定密碼之強制提供是否侵害被告不自證己罪特權。惟兩案中政府僅願提供提出行為之證據豁免，對於衍生使用則不願退讓，法院因而作出對被告有利、不得強制解鎖的判決。

上舉諸案所欲強制解鎖之客體，雖係電腦而非手機，惟電腦密碼與手機密碼之論理應屬同一。美國最高法院對於得否強制解鎖手機之議題，尚未如 *Riley* 案一般做出統一而明確的見解，惟下級法院已於 *Virginia v. Baust*[355]一案，獨樹一幟將指紋與密碼區別處理。法官認為按捺指紋有如提供鑰匙、筆跡或聲紋，毋須揭露內心所思所想，不涉及自證己罪的問題。反之，密碼之吐露，等同於強制說出個人心中所知所想、揭露內心知識，實具有供述性質，故法院不得強

---

[354] In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335 (11th Cir., 2012). 執法機關調查 Youtube 上一名使用者涉嫌分享未成年女孩之兒童色情圖片，循線查到本案被告係在加州的一間旅館租房上傳。警方取得法院搜索票後進入該房間，扣押兩台筆電與五顆外接硬碟。警方懷疑兒童色情圖片存在硬碟裡，惟被告將硬碟中部份資料加密，連 FBI 鑑識人員也打不開。鑑識人員證稱，被告使用 TrueCrypt 之軟體加密硬碟資料，導致無法取得資料，惟其相信應有資料存在其中；被告則就此點予以質疑，認為加密部分未必存有資料。大陪審團命令被告將硬碟內資料解密交出，被告則主張自己受增修條文第五條不自證己罪特權保護。被告始終拒絕將硬碟解密，遭地方法院判決藐視法庭而被監禁。法院首先引述 Fisher 與 Hubbell 兩案，重申兩案之差別，以及政府對證據掌握的多寡、證據之發現是否已成定局等要件。此等要件進一步影響證據之提出行為是否具供述性質。法院認定兩種提出行為非屬陳述：其一係毋須動腦之純粹行為，諸如提供保險箱之鑰匙；其二係，若政府對證據之所在已有合理明確之掌握、證據之發現已成定局，則發現證據乃屬必然，此時要求被告提出證據，即與不自證己罪無涉。
基於上述兩個前提，法院認為，將硬碟解密與提出內容，需要被告提供腦中的知識（密碼），且等同於作證證明自己知道涉案檔案之存在以及儲存之處，並非單純的肢體動作而已，應屬供述。法院援引最高法院的著名類比：檢警可以要求被告交出保險箱的鑰匙，卻不能要求被告吐露密碼式保險箱的密碼。就此，若將手機與保險箱類比，手機密碼自然比較類似於密碼組合，而非鑰匙。由於輸入解鎖密碼需要相當的心智運作，法院認為密碼應屬供述證據，應受不自證己罪特權之保護，故而不得強制被告將手機解密。此外，政府與鑑識人員對於檔案之存在與否以及檔案內容一無所知，又無法合理明確地知悉被告有解密之法，故證據之發現非屬定局。法院亦將本案與前述 In re Boucher 一案區別。本案政府主張法院應與該案做出相同判決，得強制被告將硬碟解鎖。惟法院認為，該案中政府已將被告之筆電打開檢視過，確知筆電硬碟中存有涉案檔案，兩案情形無從相提並論。
再就證據使用豁免而論，政府僅願意提供被告享有提出行為本身的豁免，至於硬碟中其他檔案之衍生使用（derivative use）並不在豁免之列。法院卻認為，若要強制被告解鎖硬碟，證據豁免應同時涵蓋提出行為本身以及衍生證據，如此方不致侵犯被告之不自證己罪特權。綜上所述，法院撤銷原地方法院之裁定。本案判決除了不自證己罪的討論外，尚論及證據排除法則之適用範圍大小的議題。惟本文為了聚焦，暫將該等爭點略去不提，僅就不自證己罪的部分予以探討。

[355] Virginia v. Baust, 89 Va. Cir. 267 (2014).

制為之。在定局原則的討論上，由於真實密碼僅被告自己心知肚明，外人不得而知，亦不適用此一例外。以下即以該案為例，觀察法院如何在新興手機科技的脈絡下，解釋適用不自證己罪的保障。

4. 2. 3. 1. 案例事實

本案被告Baust涉嫌於臥房內對女友勒絞施暴，遭政府以勒絞致傷罪起訴。被害人表示，案發當時，臥房中有一台機器持續錄影，且該機器會自動將影片傳至被告的智慧型手機（iPhone 5S）中。警方聲請令狀後，自被告處起出手機、錄影設備、各種光碟、隨身碟以及電腦設備等，而被害人向警方表示，與被告手機連線之錄影設備可能錄到事發當時的影片，手機內也可能存有錄影檔，被告 Baust 亦承認之。然而，Baust 的手機受到加密保護，須以密碼或指紋解鎖，故警方向法院聲請命令，強制被告說出密碼或以指紋解鎖手機，以確認手機內是否存有涉案之影片證據[356]。

4. 2. 3. 2. 本案爭點

本案爭點在於：手機密碼或按捺指紋，是否屬於供述，受到憲法增修條文第五條不自證己罪特權之保護[357]？

4. 2. 3. 3. 裁定理由

對於本案爭議，維吉尼亞州主張，密碼與指紋之存在係屬定局，密碼亦非供述而不受保護。被告則認為其具供述性質，應受不自證己特權保障[358]。

[356] *Id.* at 267-268.
[357] *Id.* at 268.
[358] *Id.*

本案承審法官 Frucci 則將指紋與密碼區別處理。法院細數先前 *Hubbell*[359]、*Fisher*[360]、*Kirschner*[361]等案的判決先例，說明供述證據（事實與信念之表達）與實體證據（血液樣本、字跡、聲紋等）的分野，重申不自證己罪之對被告保護僅涵蓋前者，而不及於後者[362]。

本案法官復指出，手機真實密碼為何，僅有被告自己心知肚明，維吉尼亞州並無所知，故不適用定局原則之例外規定[363]。其進一步將指紋與密碼區別討論：按捺指紋有如交出鑰匙，並未要求被告揭露任何心理歷程（divulging anything through his mental processes），亦即，指紋之按捺不具供述性質，被告無須表達任何內心所知，故與不自證己罪之保護無涉。相對於此，強制被告說出密碼，等同於強制被告揭露內心的思想，與指紋等實體證據之提出迥異。因此，法院認為，因指紋非屬供述，故得強制被告按捺指紋、解鎖手機；反之，密碼之揭露受到增修條文第五條之保護，不得強制被告為之[364]。

---

[359] United States v. Hubbell, 530 U.S. 27 (2000). 本案多數意見係由 Stevens 大法官主筆，並援引 1988 年 Doe v. United States 案的保險箱類比處理本案。本案被告 Hubbell 涉及數宗稅務與詐欺案件，獨立檢察官發出攜證出庭傳票，要求被告攜帶 11 類相關文件到庭繳交給大陪審團。然被告到庭時主張受到不自證己罪之保護，既未攜帶亦拒絕陳述自己是否持有此類文件。對此，檢察官再度發出命令要求被告履行該傳票之要求，並保證其在法律保障之範圍內有證據使用豁免權。被告之後提出了一萬多頁的文件，並承認這些文件為自己所有。檢察官爰依文件內容以及衍生取得之證據，以數宗稅務與詐欺罪名起訴被告。地方法院認為，該等藉傳票所取得的文件，均係直接或間接經由被告的供述而來，應屬證據使用豁免之列，故駁回檢察官之起訴。然而，上訴法院撤銷地院之裁定，認為應重新審酌傳票核發當時，政府對被告相關事證的掌握程度。若政府當時無法合理確定（with reasonable particularity）文件係在被告掌握之下，則起訴有瑕疵（tainted）。
本案爭點在於，當政府無法合理確定被告是否持有犯罪證據時，憲法增修條文第五條之不自證己罪特權，是否保障被告無庸揭露陷己入罪之證據？最高法院抱持肯定的態度。法院特別將本案與 Fisher 一案區分，認為政府對於本案證據之掌握未成定局。因此，提出本案證據時，證人必須作證陳述自己是否持有該等證據，證據所在之確切地點等等，此類陳述具有供述性質。法院認此類似說出密碼式保險箱的密碼，而非僅僅是提供保險箱的鑰匙而已，故應屬供述證據而受不自證己罪之保護。因此，若政府無法合理確定被告是否持有犯罪證據，不得強制證人揭露本案證據（在本案即涉案文件）的所在之處。此外，法院同時藉本案指出，若證人被迫提出此類證據，證據使用豁免的範圍應擴其所有衍生證據，只有完全靠政府獨力取得的證據才得以在審判中使用。

[360] Fisher v. United States, 425 U.S. 391 (1976).

[361] United States v. Kirschner, 823 F. Supp. 2d 665 (2010).

[362] Virginia v. Baust, 89 Va. Cir. 267, 268-70 (2014).

[363] *Id.* at 271.

[364] *Id*.

法院亦於判決最後一段特別提及，不得強制被告提供解密之影片。自證人證詞以觀，尚無法認定影片之存在已成定局，政府所知亦僅限於影片「可能存在」。惟自反面言之，該影片亦「可能不存在」。因此，解密影片之提出，實具有供述性質，因為被告必須承認影片存在、影片係在被告擁有支配之中且影片是真實的。因此，要求被告提出未加密之影片，等同強制其自證己罪，應不得強制被告為之[365]。

4. 2. 3. 4. 相關評論

由上開介紹可知，法官於 *Baust* 一案選擇將指紋與密碼區別處理。法官認為，按捺指紋有如提供鑰匙、筆跡或聲紋，毋須揭露內心所思所想，不涉及自證己罪的問題。反之，密碼之吐露，等同於強制說出個人心中所知所想、揭露內心知識，實具有供述性質，故法院不得強制為之。在定局原則的討論上，由於真實密碼僅被告自己心知肚明，外人不得而知，亦不適用此一例外。綜上，法院判定指紋按捺與不自證己罪特權無涉，故得強制被告按捺指紋解鎖；相反地，密碼之揭露屬於供述，受增修條文第五條之保護，不得強制被告為之。

究竟應否授權政府強制被告揭露密碼或按捺指紋，藉以解鎖手機、取得涉案證據？對於此一問題之肯否，John Villasenor 教授提出精闢的質問：

> **「我們當真想為恐怖份子或人口販子的涉案文書提供一張牢不可破的法律盾牌？如果一個性侵或謀殺犯，僅因其利用加密技術藏匿證據（例如被害人住處的數位地圖）而得以脫罪，這樣真的更有利嗎？如**

[365] *Id.*

此的法律架構，是否會讓違法的未成年照片得以藉由加密技術交換、儲存，逸脫於法網之外[366]？」

Villasenor 教授進一步點出，法院目前是以 1791 年批准生效的憲法增修條文第五條為本，佐以 1970 年代的判決先例，處理 21 世紀的數位加密問題。數位時代來臨前，個人腦中的內在思緒與形諸於紙本的外在資訊，兩者分野遠較今日清晰得多，憲法對前者的保護亦遠優於後者。然而，現代加密技術卻模糊了兩者的分界，個人得以將近乎無限多的資訊紀錄存放於數位設備中，再用僅有自己心知肚明的密碼將其上鎖[367]。

為解套此一困局，Villasenor 教授認為可重新闡釋定局原則。此原則原本要求政府對涉案文件之「位置」有所掌握，但這對存放檔案數以億計之電子裝置、雲端運算漸次普及的世界而言，顯不適用。因此，將本原則內涵調整成政府僅須證明被告「持有」此等文書，即可強制被告解鎖，或為可行之道[368]。

Kerr 教授則自尋求衡平（equilibrium-adjustment）的角度出發，論述加密技術引發的爭議。其認為，隨著新科技的發展，刑事偵查程序也不斷變化。檢警藉助新科技偵查犯罪，犯嫌利用新科技試圖匿跡，美國最高法院則透過對於憲法增修條文第四條的重新詮釋，對於科技變遷與社會實踐予以回應，力圖於科技發展與隱私保障、檢警擴權與縮權之間求取平衡[369]。然而，手機加密技術卻破壞了此等平衡，若檢警即使取得令狀也無法獲得手機內資料，原有的平衡將會傾斜，反而會導致檢警使用更多其他手段去取得所需資訊。一來一往間的利弊得失，實有再予斟酌之必要。加密技術可以讓我們把不應進來的人拒於門

366 John Villasenor, *Can the Government Force Suspects To Decrypt Incriminating Files?*, SLATE (Mar. 5, 2012), http://www.slate.com/articles/technology/future_tense/2012/03/encrypted_files_child_pornography_and_the_fifth_amendment_.html

367 *Id*.

368 *Id*.

369 Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

外，卻也有其代價，因為某些應該入內的人可能也會不得其門而入[370]。

Kerr 教授認為 *Baust* 案法院受到政府原初聲明之限，法院僅就得否強制按捺指紋與揭露密碼作出判決，得出前者可後者否之結論。然而，法院卻未處理到可能的另一種情形：政府得否不強制被告說出密碼，僅要求被告自行輸入密碼（毋須揭露予他人知悉）將手機解鎖即可？法院於本案並未對此做出裁判[371]。

進步言之，由於密碼本身即可能係入罪之證據（例如數名犯嫌共用同一密碼，則使用此一密碼之被告極有可能參與犯罪），若採此法，則被告輸入密碼之行為，所揭露者僅有「知悉密碼」此一事實而已，而這項事實常因手機係由被告使用中，而為政府所知之定局。因此，Kerr 教授認為，若不要求被告說出密碼，僅要求其解鎖，可將其與增修條文第五條之間的關聯縮到最小[372]。

然而，也有論者從根本上質疑，完全沒有必要區分揭露密碼（供述）與輸入密碼解鎖檔案（非供述）兩個行為，認為重點其實在於政府對於證物之所在究竟是否知情。其舉實體物件為例：若 FBI 探員聲請搜索票，搜索某家宅中的密碼式保險箱，惟該保險箱卻堅固到無法打開，此時法院仍不得強制個人提出解鎖密碼，因打開保險箱需用到個人心中所知內容。但此時可否強制個人提出保險箱之內容物？依 *Doe* 案之論理，只要政府無法說明保險箱裡藏有何物，便不得強制個人提出。但若政府監聽時聽到被告將贓款藏在該保險箱內，依

---

[370] Orin Kerr, *Apple's dangerous game, part 3: Where do you draw the line, and what's the privacy tradeoff?*, THE VOLOKH CONSPIRACY (Sep. 22, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/22/apples-dangerous-game-part-3-where-do-you-draw-the-line-and-whats-the-privacy-tradeoff

[371] Orin Kerr, *Virginia state trial court ruling on the Fifth Amendment and smart phones*, THE VOLOKH CONSPIRACY (Nov. 3, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/03/virginia-state-trial-court-ruling-on-the-fifth-amendment-and-smart-phones

[372] *Id*.

Fricosu 與 *Boucher* 兩案之論理，即可強制被告提出贓款。就此點觀之，數位與實體並無區別處理之必要[373]。

Baust 案將指紋與密碼區別處理之見解其實並非創舉。早在本判決作成一年前，在蘋果公司發表新一代的 iPhone 將引入指紋辨識技術時，Marcia Hofmann 教授即已撰文警示，憲法增修條文第五條之不自證己罪特權僅保護供述，亦即個人心中的所思所想；與個人內心知曉記憶之密碼相較，由於指紋等生物辨識技術毋須揭露個人的所思所想，將來可能不受憲法之保護[374]。一年後，指紋、臉部、虹膜等辨識技術漸漸出現在你我生活周遭的今日，本案判決進一步證實 Hofmann 教授的擔心並非空穴來風。然而，Hofmann 教授亦提出簡單的解法：同時使用指紋與密碼將手機上鎖[375]。

除此之外，Glen Kopp 與 Kedar Bhatia 兩位律師亦注意到科技因應法律判決時的互動與角力。*Baust* 案雖裁定法院可強制個人按捺指紋解鎖，惟新一代的蘋果 iPhone 手機則設定手機剛開機及 48 小時未使用後不得以指紋解鎖，法院可能很快又得再度面對與 *Baust* 案類似的難題[376]。

Dan Terzian 律師則主張應直接摒棄保險箱鑰匙或密碼的二分法。奠基於 *Riley* 案之論理，該案啟示在於，在新科技浪潮下，應限縮適用數位時代來臨前所作成之判決先例，力圖求取政府與人民間的平衡。自此一角度著眼，*Riley* 案摒棄將手機與一般實體物件同視之類比，對於手機附帶搜索採取否定見解；

---

373 Jody Goodman, *Forced Data Decryption: Does It Violate the Fifth Amendment?*, CRIMINAL JUSTICE, http://www.crowell.com/files/Forced-Data-Decryption-Does-It-Violate-the-Fifth-Amendment.pdf

374 Marcia Hofmann, *Apple's Fingerprint ID May Mean You Can't 'Take the Fifth'*, WIRED, http://www.wired.com/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth/

375 *Id.*

376 Glen Kopp and Kedar Bhatia, *Fingerprint Lock Won't Protect Phone From Law Enforcement*, LAW 360, http://www.law360.com/articles/603831/fingerprint-lock-won-t-protect-phone-from-law-enforcement

則在是否得強制解鎖的議題，亦應摒棄將手機視為保險箱的類比，另闢蹊徑。若此，為了維持政府權力與人民隱私之間的平衡，強制解鎖應屬合憲[377]。

詳言之，加密技術出現前，若須實體證據，政府只要先行聲請令狀，之後便能取得所需資料。即使保險箱上了鎖，政府仍能將其撬開破壞。至於手機，政府只要握有令狀，亦能取得資料[378]。加密技術出現後，一切就此改觀，政府與人民間的平衡遭到破壞。加密技術難以破解，使得權力完全失衡倒向人民這一端，由人民取得證據的生殺大權（以加密技術控制政府能否取得）。為重新獲得平衡，唯一解法只有認定強制解鎖合憲，其下又分為兩種作法：在任何情況下都合憲，或只有在無從以他法取得證據時，強制解鎖始合憲。Terzian 律師之立場偏向後者，卻也指出前者的好處在於有著 *Riley* 案一般明確而絕對的標準，可以避免情狀判別的爭議，適用上更為簡易[379]。

4. 2. 4. 手機搜索不適用一目瞭然法則：*People v. Herrera*[380]

前文曾述及，美國聯邦憲法增修條文第四條雖對搜索扣押有所規範，惟實務亦發展出許多令狀法則之例外。除前述之附帶搜索外，一目瞭然法則亦為其中之一，其操作標準則於 1990 年的 *Horton v. California*[381] 一案正式確立。該案中，警方取得搜索票至被告 Horton 家中搜索涉及一宗搶案的證據，主要是三枚戒指。惟警方於搜索過程中並未發現戒指，卻發現令狀上未記載（但警方所提出的報告中曾提及）之武器，警方爰將武器扣押。本案之爭點即在警方是否有權無令狀扣押未記載於搜索票上之其他犯罪證據。

---

377 Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How Riley Matters*, 109 Nw. UL Rev. Online 56, 62 (2014).
378 *Id.*
379 *Id.* at 63. 另參 Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISC. 298, 311-312 (2014); Dan Terzian, *Forced Decryption as a Foregone Conclusion*, 6 CALIF. L. REV. CIRCUIT 27, 28-30 (2015).
380 People v. Herrera, 357 P.3d 1227 (2015).
381 Horton v. California, 496 U.S. 128 (1990).

聯邦最高法院於本案分析個人隱私與合法搜索之間的關係。法院指出，政府執行搜索票時，搜索損及個人的隱私利益，扣押則剝奪人民的財產權。就隱私利益以觀，由於執法人員根據令狀，具有合法權限進入搜索現場，若一件物品處於舉目可見之地，掃視該物或加以扣押，對個人的隱私利益並不會有更多侵害，故未與憲法增修條文第四條有所牴觸[382]。

法院於本案明確宣示一目瞭然法則之操作標準，警方於符合該案所定三個要件時，可進行無令狀的搜索扣押：（一）該物體立即且顯而易見地涉及犯罪、（二）警方係合法處於該物體目視範圍之處所、（三）警方具有取得該物體之合法權限。一目瞭然法則爰於本案告確立[383]。

一目瞭然法則亦有調和犯罪追訴與隱私保障的效果，如美國 *Arizona v. Hicks*[384]一案，警方雖有相當理由合法進入被告家中，卻於無令狀下挪動被告音響抄錄序號，比對後雖確定該音響為贓物，然法院認為一目瞭然法則僅容許員警以目光檢視，挪動音響行為雖小，仍屬非法搜索，證據應予排除。由此可見，此制一方面雖擴張檢警得以另案扣押之範圍，另方面卻也畫出一條界線，適度尊重人民隱私權。

然而，一目瞭然法則，本係因應物理空間、實體證據之搜索扣押而設，此一原則是否能原封不動地套用於電磁紀錄之搜索扣押？便產生不少爭議。各巡迴上訴法院之見解即分裂為兩派，例如第五巡迴上訴法院於 *United States v.*

[382] *Id.* at 133.
[383] *Id.* at 136-37.
[384] Arizona v. Hicks, 480 U.S. 321 (1987).

Runyan[385]一案，將整張磁片視為一封閉容器，就先前已受私人搜索打開檢視之磁片言，因被告對該容器的隱私期待已被破壞，警方即使無令狀進一步檢視磁片內容，仍非搜索；然就私人搜索未檢視之碟片，法院則認其因逾越私人搜索範疇而無證據能力。而於 *United States v. Finley*[386]一案，被告主張手機為封閉容器，即使警方合法附帶扣押手機，但應無檢視手機內容之權限。然法院認本案為附帶搜索，其對象不限於隨身武器，身上的其他犯罪證據、容器無論開閉亦得一併搜索，故本案即認被告之隨身手機係封閉容器，檢視手機內資訊並未違法[387]。

相對於此，第十巡迴上訴法院則將電磁紀錄載體中的個別檔案視為一個個獨立的封閉容器。於 *United States v. Carey*[388]一案，警方原欲搜索毒品犯罪證據，

---

385 275 F.3d 449 (5th Cir. 2001). 本案被告Runyan之前妻Judith趁被告不在家時返家取回個人用品，尋找個人物品的過程中，Judith 打開了一個黑色露營用品包，卻於其內發現色情書刊、光碟片以及電腦硬碟等物。Judith 之後找來朋友將被告家中的個人電腦、電腦旁所有的 3.5 吋軟碟片、光碟片與壓縮磁片取走，回家檢視部分磁片與光碟後，發現其內存有兒童色情圖片，故報警處理並將磁片交予警方。警方檢視磁片確認內容後，聲請兩張搜索票，第一張搜索已得之個人電腦及磁片中所有違禁圖片，第二張則是搜索被告住處中所有電腦軟硬體及相關設備。最後，被告因持有兒童色情圖片等罪名遭到起訴。被告於審判中抗辯，警方檢視 Judith 所遞交磁片的內容實為搜索，卻未取得搜索票，侵害其受憲法增修條文第四條所保障之權利，非法取得證據應予排除。
第五上訴巡迴法院於本案將搜索所得之磁片類比為容器。就 Judith 與友人曾打開過之磁片而論，警方對已打開之容器逐一檢視內容是否為新的搜索？法院認為容器（磁片）既已被私人打開，容器主人即已喪失對該容器的合理隱私期待，故警方即使更詳細地檢視內容物（逐一檢視檔案），亦非搜索。惟 Judith 及友人尚未打開之磁片而言，由於警方無從確定其他磁片內所儲存者全係兒童色情圖片，因此，就 Judith 與其友人並未檢視的碟片，法院認定因逾越私人搜索範疇而無證據能力。

386 477 F.3d 250 (5th Cir. 2007). 本案警方因毒品犯罪逮捕被告 Finley，同時扣押 Finley 隨身攜帶之手機，其後並搜索之，嗣後被告因持有並意圖散播甲基安非他命遭到起訴。惟被告於審判中爭執警方無令狀搜索其手機內容之行為，抗辯手機與封閉容器（closed container）類似，即使警方係合法扣押手機，但應無檢視手機內容之權限，故手機內之通話紀錄與簡訊之證據應予排除。
對此，法院首先論述附帶搜索的合法性，引其他判決先例說明附帶搜索之對象不限於隨身武器，身上的其他犯罪證據亦得一併搜索之，從犯嫌身上搜出之容器亦然，且無論容器已被打開或封閉均可搜索。因此，於本案情形，警方係在合法逮捕的情況下附帶進行搜索，即使承認 Finley 之隨身手機係封閉容器，檢視手機內資訊亦無違法可言。

387 從本案論理可知法院將整支手機視為一封閉容器，惟於附帶搜索部分之論理，已被前述之 Riley 案所推翻。

388 172 F.3d 1268 (10th Cir. 1999). 本案被告 Carey 起初因涉嫌持有及買賣古柯鹼受到調查，嗣後遭到警方逮捕。被告口頭同意警方搜索他的住處，警方則於公寓中起出古柯鹼、大麻及迷幻蘑菇，並扣押兩台電腦，欲從中找出毒品交易之證據。將電腦帶回警局後，警方聲請令狀以搜索電腦，令狀上記載的搜索標的為「涉及買賣散布管制藥品之人名、電話號碼、帳目收據、地址及其他紀錄證據」。搜索過程中，警方檢視並印出電腦硬碟中的檔案目錄（directories），發現許多檔名有情色之嫌的 JPG 檔，復回到電腦上將圖片打開、確認係兒童色情圖片，隨即將 244 張影像檔拷貝至磁片中，檢視完拷貝的檔案後始重行搜尋與毒品交易之證據。

過程中意外搜出他案之兒童色情圖片後仍持續搜索，法院認為警方此舉明顯逾越令狀授權，爰判決所得圖片無證據能力。法院表示，電腦中每個檔案都是封閉的，需點開方知內容，不應驟然套用一目瞭然法則。其後 *United States v. Walser*[389]一案，案情與 *Carey* 案相似，警方亦於搜索電腦內毒品交易紀錄時意外發現兒童色情圖片，然此時警方並未繼續搜索，而係立刻暫停並向法院聲請一張新令狀，得到新令狀後始繼續搜索，故法院認為警方之搜索仍屬合理，所

Carey 抗辯警方搜索所得之色情圖片應無證據能力，因若容許警方搜索與毒品案無關之兒童色情資訊，等同核發概括搜索票（general warrant），不符合明確特定（particularity）的要件，警方搜索明顯逾越了本案範圍。警方則主張，毒販常以不相干的檔名隱藏真正的毒品交易紀錄，所有格式的檔案均可能與該等犯罪有關，圖片檔亦然。警方有如於檔案櫃中大海撈針翻找文件，故其應有權檢視電腦中的所有檔案。本案警方並非蓄意針對兒童色情案件搜索，發現該圖片純屬搜索交易紀錄時之意外，應得依一目瞭然法則扣押。搜出第一張兒童色情圖片後，即有相當理由懷疑其他圖片均係類似檔案，故得繼續搜索。

本案法院首先重新審視搜索票的內容，確認警方依令狀得搜索之範圍僅限於毒品交易相關證據。其次，法院細緻討論警方搜索時的主觀意圖：警方係基於尋找毒品交易證據的想法打開第一個 JPG 檔，然而，打開之後，基於這張圖片的內容以及其他檔案的情色檔名，警方應可預料其他 JPG 檔含有類似的情色內容。因此，警方係基於「會找到兒童色情圖片（而非毒品交易證據）」之主觀意圖打開其他 JPG 檔，甚至持續搜索情色圖片五小時後方回頭尋找毒品交易證據，明顯逾越令狀授權，所得圖片應無證據能力。警方雖主張電腦有如龐雜檔案櫃，須將抽屜一個個打開確認，但法院認為本案警方打開抽屜前已有相當理由可知內容物為何，並無逐一檢視的必要。此外，法院認為電腦中每一個檔案都是封閉的，需要打開方知其內容，亦無一目瞭然法則之適用，故判決警方檢視電腦內兒童色情照片已逾越令狀範圍，所得證據應予排除。

[389] 275 F.3d 981 (10th Cir. 2001). 本案中，警方有相當理由推測被告 Walser 之電腦內可能存有毒品交易之帳冊或施用毒品的照片，爰搜索被告電腦硬碟內之資料，然檢索過程卻意外發現成人色情圖片。此時，警方立刻將電腦關機並扣押，欲於事後再進行更徹底的檢索。五天後，警方對被告之電腦續行檢索，於打開一 AVI 檔的過程中，意外找到兒童色情圖片。警方隨即暫停檢索，並向法院聲請另一張搜索標的為兒童色情圖片之搜索票後，始續行搜尋。事後，Walser 被依持有兒童色情圖片之罪名遭到起訴。Walser 於審判中抗辯警方欲尋找者係毒品交易的紀錄，搜索過程中不應打開 AVI 檔，警方搜索實已逾越搜索票的範圍。

對此，法院首先引述 Carey 一案指出，隨著電子時代來臨，電腦內可以存放與圖書館相匹敵的資訊，遠超過憲法原則預想的範圍。若將電腦類比於其他如衣櫥或檔案櫃的有體物，常常無法說明法官在適用搜索扣押法則所遇到的狀況。憲法增補條款第四條適用於電腦時，確實有關鍵性的差異。儲存在電腦中的資料可能涵蓋一個人生活的各個面向，當警方搜索電腦中的證據時，文件混雜的程度與隱私侵害的可能性亦因而增加，故執法人員必須清楚知道欲搜索的檔案為何，避免搜索令狀上未記載的檔案。承此，法院復檢視整個搜索流程，認為警方係有系統地先打開我的文件、資源回收桶，再打開 Program Files 資料夾下的 Microsoft Works 子資料夾。因交易資料很可能以試算表紀錄，故法院認為警方檢視該資料夾亦無不妥。有爭議者係，警方是否有權打開該資料夾下的 AVI 檔案？Walser 爭執 AVI 檔屬於聲音或影像檔，不可能存有警方所欲搜尋的交易紀錄，故警方打開該檔案已逾越搜索票範圍。然而警方持反對意見，認為副檔名可以被修改以掩蓋真正的內容，故警方應有權檢視所有類型的檔案以確認內容，故打開 AVI 檔並無疑問。對此爭議，法院表示打開該 AVI 檔仍在令狀的容許範圍之內，由檢索人員發現第一張色情圖片後隨即暫停搜索並聲請新令狀之舉，可知其相當節制，並無恣意侵犯 Walser 隱私權之意，而與 Carey 案之情形有間，故法院認為其仍屬合理搜索，Walser 之抗辯為無理由。

得圖片有證據能力[390]。

簡言之，自第五巡迴上訴法院於 *Runyan* 與 *Finley* 兩案所採見解以觀，該院將電磁紀錄載體（如磁片、手機）視為封閉容器，此等封閉容器一旦打開，主人即喪失隱私期待，警方可對於容器內的資訊無限制地搜索，開啟的檔案均得適用一目瞭然法則作為證據。反之，第十巡迴上訴法院於處理 *Carey* 與 *Walser* 兩案時則採較嚴苛之解釋，將載體中每個檔案視為一封閉容器，一目瞭然法則僅於意外發現的第一項他案證據有所適用。警方若發現他案證據，應立即暫停搜索，另行聲請搜索票後始得繼續。

各巡迴上訴法院對於電磁紀錄載體性質認知不同，至今尚未得到統一之見解。然就本文論述主軸之智慧型手機而論，科羅拉多州最高法院於 2015 年 10 月所判決之 *People v. Herrera*[391]一案，對於智慧型手機內資訊是否一律適用一目瞭然法則之爭議，作出明確裁斷：手機內各訊息匣均屬封閉容器，非逕適用此一法則。下文即就本案之事實、法院之判決理由予以詳述。

4. 2. 4. 1. 案例事實

本案係某未成年少女 Faith W.的母親看到女兒與被告 Herrera 在網上的談話後，將對話內容印出、連同 Herrera 之手機號碼，一併向佛里蒙特警長辦公室舉報其與女兒發生性行為。嗣後探員 Dodd 假冒為一名 14 歲少女 Stazi 與被告互傳訊息，幾周後將被告 Herrera 逮捕，並扣押其手機[392]。

[390] 可惜本案法院仍然迴避了最關鍵的一個問題：於毒品案件，警方有無權利打開 AVI 檔？（"We leave the government's argument regarding “disguised” files for another day."）本案法院僅就警察事後的行為十分節制，認定其並未過度侵害人民的隱私，卻未討論警方是否能打開看似無關的檔案。在此假設一個極端的情形：警方是否得恣意檢視任何格式的檔案，只要在意外發現他案證據時再暫停搜索並補聲請一張令狀即可？

[391] People v. Herrera, 357 P.3d 1227 (2015).

[392] *Id. at* 1228.

扣押手機後，探員 Dodd 向法院聲請手機搜索票獲准，搜索票上則記載得搜索之內容有三：其一係被告與 Stazi 互傳的文字訊息，其二係被告與 Stazi 互傳文字訊息內附加的照片，其三則係足以證明此一手機係由 Herrera 所持有之證據[393]。

警局探員 Slattery 先依照一般搜索手機的作業流程，使用名為 Cellebrite Device 的工具進行鑑識工作。惟被告 Herrera 之手機與 Cellebrite Device 並不相容，探員爰改以手動方式進行搜索。其先瀏覽手機收件夾中的文字訊息，再瀏覽通訊軟體 Kik 中的訊息。由於通訊軟體 Kik 的訊息是依照姓名排列，探員找尋 Stazi 的過程中，見到另外一位名為 Faith Fallout 者與被告互傳訊息，探員懷疑其係先前與被告發生關係之 Faith W.，爰點擊訊息並進入觀看，確認其確實是 Faith W.與被告 Herrera 之談話，被告因此被起訴性侵未成年少女、對兒童進行網路性剝削、上網誘拐兒童等罪。被告則主張 Slattery 探員係違法搜索，請求排除 Kik 軟體中 Faith W.與被告談話之證據[394]。

4. 2. 4. 2. 本案爭點

本案爭點在於，探員檢視被告手機中與 Faith Fallout 聊天紀錄之行為，是否逾越搜索票授權搜索之範圍？若逾越令狀範圍，手機內資訊是否仍適用一目瞭然法則，所得證據無須排除[395]？

[393] *Id.* at 1229.
[394] *Id.* at 1229-30.
[395] *Id.* at 1230.

4. 2. 4. 3. 判決理由

4. 2. 4. 3. 1. 本案搜索逾越令狀授權之範圍

對於被告 Herrera 所提出的證據排除抗辯，政府主張，由於搜索票授權執行者得以搜索「足以證明此一手機係由 Herrera 所持有之證據」，則因被告手機中與 Faith Fallout 之聊天紀錄，亦有可能證明此一手機係 Herrera 所有，故探員之搜索並未逾越令狀授權之範圍[396]。

對此抗辯，法院認為，若採信政府的說法，則手機中任何資訊均可能證明此一手機係 Herrera 所有，無疑使此一令狀授權政府進行概括搜索（general search），從而不符合憲法增修條文第四條要求搜索票之記載必須明確特定之要件。政府之主張，將使令狀執行者得以恣意而不受限地瀏覽翻閱個人手機中的所有私密資訊，此與令狀明確性之要求明顯不符。因此，法院判決探員搜索被告與 Faith Fallout 聊天紀錄之行為，係屬逾越令狀授權之違法搜索[397]。

4. 2. 4. 3. 2. 一目瞭然法則不適用於手機資訊

法院判定政府之搜索係屬逾越授權範圍之違法搜索後，進一步判斷手機資訊是否有一目瞭然法則之適用。政府主張，根據一目瞭然法則對令狀原則所創造的例外，令狀執行者合法搜索時，得一併扣押舉目可見的犯罪證據。因此，搜索被告與 Stazi 通訊文字的過程中所觀察到的 Faith Fallout 訊息匣，應可打開搜索[398]。

對於政府的主張，法院首先重申 *Horton* 一案所建立之一目瞭然法則三要件：（一）警方係合法處於該物體目視範圍之處所、（二）該物體立即且顯而易

[396] *Id.*
[397] *Id.* at 1230-31.
[398] *Id.* at 1231.

見地涉及犯罪、（三）警方具有取用該物體之合法權限。法院認為本案符合前兩個要件，因為警方持有搜索票、Faith Fallout 的名字亦立即且顯而易見地涉及犯罪[399]。

惟就第三個要件而論，法院將手機內 Faith Fallout 訊息匣認定為獨立的封閉容器（closed container）。令狀僅授權搜索被告與 Stazi 間的聊天紀錄，而被告與 Faith Fallout 和 Stazi 的聊天紀錄係各自獨立的，警方既沒有理由認為會在 Faith Fallout 的訊息匣內找到被告與 Stazi 的聊天紀錄，也沒有證據指出被告有變造訊息匣標籤之行為，警方實應另外聲請令狀，方得檢視 Faith Fallout 訊息匣，故不符合第三個要件而不適用一目瞭然法則[400]。法院判決書特別指出，將一目瞭然法則適用於數位資料之搜索時，必須格外謹慎[401]。

4. 2. 4. 4. 相關評論

誠如前文所引之 *Runyan*、*Finley*、*Carey* 與 *Walser* 等案，美國各巡迴上訴法院間對於電磁紀錄載體性質如何認定之議題，見解仍有出入。在智慧型手機部分，科羅拉多州最高法院則於 *People v. Herrera* 一案明確認定手機內各訊息匣均屬封閉容器，並未逕行適用一目瞭然法則。因聯邦最高法院尚未對此作出判決，各級法院仍有各自發揮的空間，電磁紀錄之搜索，容有爭議。

實則，是否應將一目瞭然法則自傳統實體證據延伸適用於電磁紀錄搜索之爭議，源自對於概括搜索的擔心。早在 1994 年，Raphael Winick 教授即已認識到電腦搜索所引發之概括搜索的風險，其指出，電腦內所儲存之數以百萬計的文字，一如實體房間檔案櫃裡汗牛充棟的文件，爰呼籲搜索電腦應遵循 *United States v. Tamura* 一案處理混雜文件時所立下的程序：執法機關的拖網式搜查

399 *Id.*
400 *Id.* at 1232-33.
401 *Id.* at 1233.

（investigatory dragnet）係憲法增修條文第四條所欲禁止的，故即使涉案證據混雜於其他文件之中，執法人員得扣押之範圍仍非漫無邊際，依然限於搜索票上所載之文件類型[402]。Winick 教授立基於此，進一步主張應將檔案視同混雜文件處理，執法人員搜索電腦時，亦需特定檔案類型，而非漫無邊際地恣意搜索所有檔案[403]。

然而，隨著時日過去，資訊科技日新月異、電腦技術一日千里，Winick 教授的主張便會遇到許多問題。Thomas Clancy 教授即引諸多判決指出，有心藏匿犯罪證據的嫌疑犯很有可能將涉及犯罪的檔案取一些看似無關的檔名或副檔名，藉以規避檢警的搜索。因此，以檔名或檔案類型作為得否搜索的標準，實際執行上便有窒礙難行之虞，畢竟很少有人會把非法交易之文件取名為「犯罪紀錄」，等著警方來檢索。故較好的方法應是授權警方檢視所有檔案，確定檔案內容是否涉及犯罪，即使看似無關亦然[404]。

針對一目瞭然法則本身，Kerr 教授則主張，應完全摒棄該法則之適用。其認為，鑑識分析是一門藝術，而非科學。鑑識過程瞬息萬變、無從預料，且需要專門技術，難以簡化成數條規則。因此，應給予執法人員搜索證據之完全權限，讓其得以盡其所能地用盡所有工具、試遍所有方法，以搜索載體中可能的犯罪證據。然而，搜索過程中若取得其他令狀上未記載的他案證據，除非符合獨立來源（independent source）或必然發現之證據（inevitable discovery）這兩個證據排除法則的例外，否則全數無證據能力，也不會被揭露。Kerr 教授謂此作

[402] United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir.1982). 該案判決作成於資訊時代來臨前的 1982 年，涉及之資料均為紙本。在該案中，執法機關欲扣押被告 Tamura 收款之相關事證，證物則存放在雇主 Marubeni 處。惟因文件數量龐大，且雇主其他員工又拒絕幫忙，要於現場特定出與該款項有關之文件實屬不易，故該案執法人員直接將所有可能涉案之文件資料扣回，再慢慢篩選過濾涉案證據。對此，法院認為，執法人員合理的扣押範圍應僅限於搜索票上所載之文件類型，而非不分青紅皂白一律扣押。

[403] Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 107-09 (1994).

[404] Thomas K. Clancy, *The Search and Seizure of Computers and Electronic Evidence: The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 210-13 (2005).

法雖不完美，但能在給予執法人員辦案取證所需權限的同時，藉由他案證據之排除以保障人民隱私，亦降低執法人員搜索無關本案資訊之動機，在隱私與執法上取得最適切的平衡[405]。

惟國內學者李榮耕教授並不同意 Kerr 教授完全摒除他案證據的作法。若採此法，則搜索時如果意外發現其他重大犯罪的證據，此時若將該電磁紀錄絕對排除，將使犯罪者逍遙法外，嚴重影響犯罪的訴追及處罰。有鑑於目前電腦鑑識多涉及高度技術性的專門知識，需要執法人員依據過往的經驗智識，就實際搜索狀況臨機應變、檢索判讀，尋找涉案證據。就此，過程中接觸他案證據，幾屬無可避免[406]。

為兼顧人民隱私及犯罪偵查，李教授認為應採「重罪原則」。換言之，循比例原則思考，鑑識對人民隱私之侵害雖屬重大，然而，仍不應斷然排除所有他案證據，讓犯罪者就此逍遙法外。此時應折衷地讓鑑識中所取得之他案證據僅得用以證明法定重罪，如屬輕罪，則應予以排除。若採此法，應可降低執法人員搜索無關本案之資訊的動機。惟此一作法也有缺點，即立法者有可能會不斷擴充重罪的範圍，讓另案證據得以使用[407]。

美國憲法學者 Akhil Reed Amar 教授檢討該國憲法增修條文第四條的解釋時，曾經主張該條文之核心實非相當理由有無或令狀具備與否，而係執法人員之搜索是否「合理（reasonable）」。至於合理性之有無，其實跟人民與警察的直覺有關，嚴重的犯罪與迫切的需求，足以正當化更重大的搜索扣押[408]。Amar 教授的主張，其實也可說是重罪原則的體現。

至於地毯式搜索的主張，如前所述，美國法院於 *United States v. Winn* 一案

---

405 Kerr, *supra* note 341, at 582-84.
406 李榮耕（註 242），頁 1108-09。
407 同前註。另參 William J. Stuntz, *Local Policing after the Terror*, 111 YALE L.J. 2137, 2183-85 (2002).
408 Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 802 (1994).

之判決即明確指出地毯式搜索不可行，要求執法者應特定搜尋檔案類型。Susan Brenner 教授與軟體鑑識分析師 Barbara Frederiksen 亦提出兩個反對地毯式搜索的理由：首先，授權國家進行如此廣泛的搜索，對於未犯罪的無辜人民不受違憲搜索之保障，顯有不足；其次，如此搜索也架空了令狀對人民的保障。因此，更好的解決方法，應自搜索程序著眼，參考美國法律協會（American Law Institute）的訊前程序模範法典（Model Code of Pre-Arraignment Procedure），建立一套有系統的搜索程序，就整個搜索程序、地點（現場或帶回）、範圍、方法、時間與追加令狀等，予以明確規範，並由治安法官控管令狀允許之搜索範圍[409]。

此外，其亦指出一目瞭然法則為何不應逕予適用於電磁紀錄搜索之理由。在現實世界，當警察執行搜索票、進入房間時，其視野一翻兩瞪眼：東西放在看得到（in sight）或在看不見的地方（out of sight），沒有模糊空間。若要求令狀上需記載執法人員搜索時哪些能看、哪些不能看，既荒謬又不具可行性。要求執法人員假裝自己沒有看到某些視線內的物品，也是件不合理且不切實際的事。於此脈絡下，一目瞭然法則實屬合理，且易於適用[410]。

惟電腦世界卻完全是另一回事。當執法人員搜索文本內容時，圖片等非文字檔案，並不會出現在執法人員的視線內。若以現實世界的情況類比，這些圖片就好像放在一個關著或是上鎖的箱子裡，需由執法人員另外解鎖、開箱後才能看到內容，從而落在一目瞭然法則的適用範圍之外。就此點而言，現實世界與電腦世界實有不同，該法則之適用應予限縮[411]。

---

[409] Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 100-106 (2002).
[410] *Id.* at 94.
[411] *Id.*

4. 3. 反思與建議

4. 3. 1. 美國判決帶來的省思

4. 3. 1. 1. 自願揭露與第三人法則

誠如前述，美國法院在判斷警方行為是否屬於搜索、應受憲法增修條文第四條之限制時，多以 Harlan 大法官所提出的合理隱私期待作為判斷依據。美國法院在操作合理隱私期待判準，認定人民對某一資訊有無主客觀隱私期待時，若人民已同意向第三方揭露該資訊，而政府僅向第三方（而非本人）取得資訊時，法院往往會直接適用第三人法則，認為人民既已自願揭露，不得再就該等資訊主張隱私期待，故政府行為並非搜索。如 *Smith* 案多數意見認為，個人對自願提供予電信業者之通話號碼，不得主張合理隱私期待[412]；*United States v. Carpenter* 案之巡迴法院判決亦指出，個人既自願向電信業者揭露位址資訊以遂行通話，已無隱私期待可言，故警方得無令狀調閱手機基地台位址資訊[413]。

Solove 教授對於法院將「秘密」作為隱私保護中心、僅個人私密領域與試圖隱藏之資訊方受保護之觀點有所批判。Solove 教授認為，現今人們的生活已與資訊密不可分，無數機構均紀錄著個人資訊，凡走過必留下痕跡，此種觀點已無法有效回應現今資訊社會的隱私議題[414]。此外，若客觀環境如喬治歐威爾所著之《1984》一書中充滿監視時，因人民無從主張客觀隱私期待，進而無法受到隱私權保障。如未能追本溯源思考隱私權的保障目的，僅完全以當時社會多數人之觀點作為判斷客觀期待之依據，合理隱私期待之判準反而可能導致隱私權受箝制之惡果[415]。

---

412 Smith v. Maryland, 442 U.S. 735 (1979).
413 United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016).
414 SOLOVE, *supra* note 7, at 8.
415 SOLOVE, *supra* note 95, at 71-74.

然而，在 *Riley* 案判決作成後，Solove 教授與論者 Ryan Watzel 均指出，如果法院堅守第三人法則，個人若自願將手機內之資訊提供予第三方（如將通聯號碼提供予電信業者、手機中有備份於雲端的資料等），本案應得出手機資訊不受保護、政府搜索並未侵犯人民隱私的結論。但法院似未援用該法則而為判決，仍給予手機資訊保障，由此觀之，第三人法則似有鬆動的跡象[416]。

身處現代資訊社會，為遂行生活所需的社交互動與日常活動，個人被迫向服務提供者揭露各式資訊。以手機為例，通電話時需先告知業者所欲撥打之號碼、傳簡訊時需將文字傳送給業者再由其轉發收訊人等，均屬此例。消費者為了使用服務，面對服務提供者的隱私權政策，及業者提出的「不平等條約」，即使對相關條款有所疑慮，惟因面對「全有或全無」的處境，只有「同意」業者蒐集資訊，才能使用服務，無從拒絕。

惟如 Solove 教授所提醒，一般人面對條文龐雜難以理解的隱私權政策，不見得會細細閱讀，對隱私的重視也不如表面上所表現出的那麼高，一般人為了能夠使用服務，往往在不甚明白也不想多了解的情況下便按下同意[417]。若此，則執法者是否該進一步討論此等同意的範圍與有效性，而非將消費者的「被迫同意」擬制為個人完全放棄隱私期待？

我國學者林子儀教授即指出，於現今資訊網路時代，吾人日常生活上為與他人往來，往往會自願透露部分資訊予他人，若固守第三人法則之傳統見解，重視隱私者恐須離群索居，且網路上的資訊及紀錄亦均落於隱私保護之外，實與憲法保障隱私權之目的背道而馳[418]。隱私合理期待之判斷準則應隨時空環境變遷而有所調整，才不會淪為不當減少個人隱私保障之憑藉[419]。

---

[416] Solove, *supra* note 314; Watzel, *supra* note 315.
[417] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883-88 (2013).
[418] 林子儀（註 228），頁 88-89。
[419] 林子儀（註 152），頁 58-59、62。

對於此一難題，或可借鏡前文介紹過之 Nissenbaum 教授所提出之「情境脈絡完整性」的概念[420]。同樣一則資訊，在某些情境下可能屬於敏感性資訊，在另外的情境下則否。比方說，在醫病關係的脈絡下，病人會主動向醫生揭露自己的病況，但這不代表醫生可以脫離脈絡、與其他無關之人討論該病患的病況；又如一位男同志即使在身處的同志社群中出櫃，不代表他願意將自己的同志身分昭告天下，人盡皆知。

承此以言，個人因通話需求向電信業者揭露自己所欲撥打的號碼及自身位置、因資料備份需求而將手機內之資訊同步至雲端、因聯絡需求而將手機簡訊傳給友人等，並不表示個人對於此等資訊毫無隱私期待，而欲公諸於世。

實則，資訊社會中的個人，為了使用手機，不得不向外（服務提供者）揭露各式資訊，例如向電信業者揭露所撥打的電話號碼、簡訊內容、通訊位址、向通訊軟體業者傳送 LINE 的文字圖片訊息、向社群網站上傳照片與心情文字、向通路業者下單欲購買的書籍、商品與藥物等。若吾人未意識到手機在現代資訊社會中所扮演的特殊角色，進而予以多一分的關注與保障，則憲法保障人民隱私的美意，恐遭架空。

我國大法官論斷人民於公共場所是否享有隱私權時，並未採取美國第三人法則「自願揭露即不受保護」的論理，仍使個人享有「依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主」，明採與美國不同的見解[421]。然大法官此一論理（自願揭露仍受保護）將來是否會一體適用於新興科技，仍有待觀察。

本文認為，個人為了通訊需求，雖向業者揭露所撥打之電話號碼、Email

[420] Nissenbaum, *supra* note 74.
[421] 司法院釋字第 689 號解釋理由書參照。

或通訊內容[422]，或是為了上網查詢資訊而向網站揭露 Cookies 等紀錄，並不代表個人願意向其他無關的第三人揭露同樣的資訊，例如個人使用手機通話時，往往也不會隨意將通話對象之電話號碼與身分昭告天下。若採美國部分法院拘泥於判決先例第三人法則的見解，認為個人自願揭露資訊即代表對於這些資訊毫無隱私期待，不得主張受隱私權保護，此舉等同架空個人隱私權之保障，似屬率斷。

因此，吾人在操作「合理隱私期待」判準時實應格外小心。於現今資訊社會中，人民生活形態與以往迥異，「自願揭露」與否，已不該作為判斷隱私期待有無之唯一標準，更應將個人公開資訊時的目的與情境納入考量為是。

4. 3. 1. 2. 新興科技與權力分立

由於科技不斷發展變動，導致新的爭議與挑戰也一再產生。權力分立的問題亦於此時浮現：此等爭議究應由立法者以法律明定，或由司法者判斷權衡？換言之，何者較適合解決科技帶來的爭議？與司法部門相較，具有民意基礎的立法部門是否更適合衡量與處理？

前引 *Riley* 一案，Alito 大法官即於協同意見書指出，立法機關比法院更適合解決此類爭議，舉例說明在 *Katz* 案判決電子監控雖未侵害財產利益仍屬搜索之後，國會隨即制定 1968 年綜合犯罪防治及街道安全法，改以法律明確規範電子監控之授權與限制。Alito 大法官亦稱美國憲法增修條文第四條為「鈍工具」，認為 21 世紀的隱私保護，不適合由聯邦法院以此一鈍工具解決。鑑於

[422] 在我國，由於 LINE 等通訊軟體常被用作犯案的輔助通訊工具，實務上亦曾發生警方得否向 LINE 業者調閱對話資料之爭議，詳見黃揚明，毒品氾濫　警調：LINE 無法監控是難題，蘋果即時，2015 年 7 月 6 日，http://www.appledaily.com.tw/realtimenews/article/new/20150706/642175；警調閱 LINE 辦案 立委質疑侵害隱私，自由時報，2014 年 11 月 2 日，http://news.ltn.com.tw/news/politics/paper/826709；戴雅真，用 LINE 販毒 警調難監控，中央通訊社，2015 年 7 月 6 日，http://www.cna.com.tw/news/aipl/201507060165-1.aspx；警方將全面監控 LINE？ 王卓鈞：連查 IP 都沒達成協議，ETtoday，2014 年 11 月 4 日，http://www.ettoday.net/news/20141104/421484.htm（最後瀏覽日：2016 年 1 月 12 日）。

手機在現代人生活中扮演的角色，其一方面可能被用於各類重大犯罪、產生許多嶄新的執法難題以外，另方面，搜索手機內容也會涉及非常敏感的隱私利益。科技一再變遷發展下，法院並不那麼適合理解與判斷此等爭議。比起法院，由人民選舉出的立法部門，更適合去衡量與回應現今以及將來的變遷[423]。

Kerr 教授於此一議題上亦採類似見解，對於「增修條文第四條能有效回應新科技」之主流觀點有所批評，認其過於浪漫而有失真確，轉而強調立法者所應扮演的角色。Kerr 教授認為，在科技快速變遷的現狀下，需要的是制度上的完整規範。自此以觀，立法者對隱私所提供的保護，往往比增修條文第四條更為充足。如果刑事偵查上對於新科技的需求漸增，則執法人員清楚認識美國法典（United States Code）的重要性，即不亞於美國裁判彙編（United States Reports）。立法者制定綜合完整的法律保護，將促使整個司法體系發展出更細緻、清晰的規則，求取隱私與公共安全間適切的平衡[424]。

惟 Solove 教授完全不同意 Kerr 教授的見解，其認為立法者未必能做得比司法者更好，兩者甚至說不定一樣笨拙。其指出，由於科技快速變遷，每條法規可能都在制定一年後即顯得過時而落伍，則法律永遠只能氣喘吁吁地跑在後頭，而且永遠都追趕不上[425]。

針對 Kerr 教授的主張，Solove 教授明確提出三點批判：其一，法律所提供的保護並沒有比憲法增修條文第四條更加全面，例如 GPS、衛星監控等新興科技，根本是法律規範真空；即使是有所規範的領域，依舊漏洞百出。其二，法律並沒有比增修條文第四條更加清楚，很多法律條文甚至更為模糊、複雜而令人困惑。其三，面對新科技所帶來的議題，立法者未必比法院更能妥適處理，例如在網路、電子郵件、監聽、電腦或其他新科技的規範上，議會僅制定少數

[423] Riley v. California, 134 S. Ct. 2473, 2497-98 (2014).
[424] Orin. Kerr, *The Fourth Amendment and New Technologies: Constitution Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805-06 (2004).
[425] SOLOVE, *supra* note 4, at 165.

規則，回應科技的速度亦相當緩慢。因此，在回應新科技的表現上，Solove 教授認為立法者遠比司法者更糟。反之，當新科技新議題於案件中浮現時，司法者被迫在第一時間處理，回應新科技的頻率與速度遠遠優於立法者[426]。

我國學者林子儀教授亦指出，由於法律經常落後於科技發展，若案件當事人針對隱私及隱私權的具體爭議尋求司法救濟，法官實應就系爭權利是否為隱私權、系爭行為是否構成隱私侵害等議題，審慎解釋適用所涉法規範後作出具體判斷，除了能維護個人隱私權外，亦可作為立法、行政部門修法時的經驗基礎，有助整體隱私權法制之發展[427]。

本文認為，新興科技所引發的問題應該由誰來解決，司法、立法，並非一山不容二虎的關係。立法者若能於前端即制定完整而全面的法律規範，使相關單位執法時有所依循、避免侵害人民權利，固然甚好。但在立法怠惰或違憲立法之時，仍需司法者在後端予以控管。否則若採 Alito 大法官或 Kerr 教授的見解，豈非賦予立法者於新興科技領域內有違憲審查之豁免權，成為司法真空的境地？

詳言之，立法部門雖具有民意基礎，「理想上」應能反映民意之所向，在第一時間反映民意、回應科技變遷。然而，「實際上」，一如 Solove 教授所言，由於法律制定修改不易，立法者的速度相當緩慢，只能在新科技的後頭望洋興嘆。自我國搜索監聽相關刑事程序修法過程以觀，亦與 Solove 教授的觀察相去不遠，立法者均是發生相關案件、意識到搜索監聽有可能威脅到自己時，始大刀闊斧地迅速修法，修法品質堪慮。悲觀而論，我國立法者實有怠惰之嫌，如同懶惰的馬兒，鞭子抽一下才動一下。若此，是否要到哪一天，我國某位立委的手機被檢警附帶搜索致生爭議時，才會引起立委諸公對此之重視，火速「回應新科技變遷」而通過相關立法？（且通過的法律是否適宜，又是另一回事）

[426] *Id.* at 165-67.
[427] 詳參林子儀（註 228），頁 114-115。

因此，本文認為，與其對立法者抱持過高的期待，司法者似乎比立法者更能有效回應科技進步與社會變遷。正是因為法院必須審理個案的特性，以及憲法與法律條文本身留有的餘地，賦予司法者因時制宜的解釋空間，使法院法官更能於具體個案逐一審視判斷人民隱私期待是否合理、政府侵害之有無（但此亦有前提：法官受過良好的憲法與隱私權教育）。

此外，即使立法者當真反映人民期待，回應科技變遷而制定相關法律，具有釋憲權限的司法者，仍應就涉及爭議的法律規範提出違憲審查。當立法者制定之法律過於偏頗，如過於側重追訴犯罪之公益，而將人民隱私棄若敝屣時，李震山、湯德宗兩位大法官於司法院大法官釋字第 699 號解釋所提出之不同意見書，或可做為警鐘：

> **「……現代風險社會中，國家採取限制人民基本權利方法所造成之損害，之所以常會與所欲達成目的之利益顯失均衡，其重要原因之一是，國家在欠缺科學數據支持之風險預斷下，往往以風險預防為名過早立法限制人民基本權利，由於不能對症下藥且無助於立法目的之達成，在病灶難除而無計可施下，只好藥愈下愈重，馴至失衡而不自知[428]。」**

每當立法者有立法不當之虞時，司法者之職責與可貴之處即顯露無遺。無論法律如何制定、無論其是否涉及新科技的領域，若涉及合憲性的爭議，司法者仍應考量憲法之制定精神與保障人權之理念，公正審查涉及爭議的法律規範是否違憲，固守捍衛人民基本權利的最後一道防線。

4. 3. 1. 3. 搜索票之審理核發

或有認為，維護治安亦係國家重要任務，為了追訴犯罪，監控通訊、搜索手機係必要之惡，只要以令狀制度與法官事前審查把關，即可有效杜絕政府濫

[428] 釋字第 699 號解釋，李震山大法官提出、湯德宗大法官加入之不同意見書參照。

權搜索之弊。一如 *Riley* 案的判決結論所稱，政府若欲搜索人民手機，法院的回應非常簡單：「聲請搜索票[429]。」然而，以相當理由與聲請令狀作為門檻，由法院掌理搜索票之審理與核發，是否即能落實憲法對於人民隱私權之保障？亦屬未必。

之所以設定「相當理由」作為程序發動的門檻，係著眼於偵查階段與審判階段的不同：審判階段，若欲判決被告有罪，法官須達到「毋庸置疑」的心證，寧可錯放一百，不可錯殺一人；惟在偵查階段，檢警常需面對倉促、突發、混沌的狀況，不可能永遠都作出正確的判斷，爰授予檢警一些犯錯空間，僅要求執法有「相當理由」之確信，即可發動偵查，同時也以相當理由作為強制處分權的最低標準，證據未達此一門檻，不得任意對人民搜索扣押[430]。根據一項對美國聯邦法官所作的實證研究顯示，所謂的相當理由，確信程度的平均值為百分之四十五點七八[431]。

然而，令狀制度的法院審查、相當理由的心證門檻，程序上看似嚴謹而符合正當法律程序的要求，但實質上是否真能有效為人民權利把關？答案卻非如此肯定。例如美國學者 Lawrence Lessig 點出「法官態度左右令狀核發」之事實：若法官審查寬鬆，警察即可輕易取得令狀[432]。我國學者王兆鵬教授亦曾指出，由於令狀之審理程序，僅有檢警一方說詞，被搜索人並無反駁之機會；此外，由於法官僅對令狀為書面審理，幾乎不太對警察作相當理由有無之實質詢問，最終法院常淪為警方的橡皮圖章[433]。

通訊監察，涉及秘密通訊自由，對人民隱私權侵害之鉅，實與搜索扣押不相上下，故監聽票之統計數據亦有值得參考之處。我國曾因特偵組監聽立委案

[429] Riley v. California, 134 S. Ct. 2473, 2495 (2014).
[430] 王兆鵬（註 251），頁 68-69。
[431] 同前註，頁 72-73。
[432] LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 159 (2006).
[433] 王兆鵬（註 251），頁 87。

[434]鬧得滿城風雨，濫權監聽之議題因而浮上檯面。林鈺雄教授即指出，我國通聯紀錄及用戶個資調取案，八成係由警察調閱，每年高達八十幾萬件，若以人口比例換算，我國約是德國的兩百多倍[435]。民間團體也質疑，台灣二千三百多萬人口，但每年法院核發的監聽件數，竟與擁有三億多人口數的美國不相上下[436]。

由上開數據可見，我國雖號稱有中立超然之法院審查，惟相關令狀之核發仍有浮濫之嫌。自此以觀，我國相關強制處分令狀改由法官核發後，看似符合正當法律程序的要求，但實質上似乎未必能有效為人民隱私權把關。搜索票之審查與核發，究應由何人職司，方能達到憲法保障人民隱私權的要求？此雖屬立法者之立法形成自由，惟仍不妨由憲法權力分立與功能最適原則的角度，重新思考。司法院釋字第 613 號解釋曾提及權力分立的目的：

> **「蓋作為憲法基本原則之一之權力分立原則，其意義不僅在於權力之區分，將所有國家事務分配由組織、制度與功能等各方面均較適當之國家機關擔當履行，以使國家決定更能有效達到正確之境地，要亦在於權力之制衡，即權力之相互牽制與抑制，以避免權力因無限制之濫用，而致侵害人民自由權利[437]。」**

就此以觀，權力分立之目的有二：積極功能係為增進政府效率，亦即功能最適原則，將國家事務分配由組織、制度與功能等各方面均較適當之國家機關擔當履行，使國家決定更能趨於正確；消極功能則為避免政府濫權，亦即權力

---

[434] 曾韋禎，監聽不可原諒！王金平曾被馬政府長期政治偵防，自由時報，2014 年 11 月 5 日，http://news.ltn.com.tw/news/politics/breakingnews/1149440（最後瀏覽日：2016 年 1 月 12 日）。

[435] 德國人口約為我國四倍，全德國調取通聯紀錄一年案件數總計 8316 件、法院核發調取令總計 13904 張。詳見林鈺雄，濫調通聯紀錄何時了？，自由時報，2014 年 1 月 13 日，http://talk.ltn.com.tw/article/paper/746352（最後瀏覽日：2016 年 1 月 12 日）。

[436] 錢利忠，法界保守估計：每年 600 萬人被監聽，自由時報，2013 年 9 月 25 日，http://news.ltn.com.tw/news/politics/paper/716685（最後瀏覽日：2016 年 1 月 12 日）。

[437] 釋字第 613 號解釋理由書參照。

制衡原則，避免權力因無限制之濫用，侵害人民自由權利[438]。

形式上來看，搜索票、監聽票等有一道由中立法官審查核發的手續，看似符合正當法律程序之要求，對人民權利有所保障。但由上開學者批評與實際數據可知，法官有淪為橡皮圖章之嫌，相關令狀之核發率並不低，故實質上似乎未必能有效為人民隱私權把關。若此，我國目前令狀制度的設計，是否符合憲法權力分立、功能最適原則的要求，是否能避免權力濫用而對人民隱私有所侵害，不無檢討餘地。

如果連中立之法官都無法確切保障人民隱私，則究竟應由誰來負責搜索票之審理與核發，始能達到權力分立功能最適之理念？本文認為，由於搜索扣押制度在我國非屬憲法保留事項，屬立法裁量範圍，較之美國（憲法增修條文第四條對搜索扣押制度已有明言）有較大的立法形成空間[439]。由於令狀制度並非憲法保留事項，是否可能考慮引進類似人民觀審之制度，由人民參與搜索票之審查？

人民參與審理為何更能有效維護個人隱私？Ben Wizner 律師一語道破：「引起當權者注意的方式，就是**向他們證明這些議題與他們自己切身相關**[440]。」此話值得吾人借鑒。美國錄影帶相關隱私法制的修正，即屬此例。1987 年，Robert Bork 被提名為聯邦最高法院法官。提名審查期間，華盛頓城市報將該法官之錄影帶店租片紀錄登上報紙。雖然其中沒有惹人非議的影片，此舉卻引起國會議員恐慌，火速修法通過保護錄影帶租借隱私之法案，侵害隱私須負民

[438] 權力分立消極積極之功能分類與進一步討論，詳參林子儀、葉俊榮、黃昭元、張文貞，《憲法權力分立》，2 版，頁 134-136（2009 年）。

[439] 如檢察官本握有羈押權，然自司法院釋字第 392 號解釋作出後，羈押權改由法院掌理；搜索票之核發權限，在檢察官大肆搜索辦公室、引起立委諸公憤慨後，亦轉移至法官；監聽票在司法院釋字第 631 號解釋作出後，改由法院核發；去年九月著名的馬王政爭後，通訊保障監察法再度修法、更趨嚴格，導致檢警辦案不易、實務界人士多所批評，以至於再次修法放寬要件的聲浪又慢慢浮現等等。詳細相關修法爭議與過程，因非本文討論重點，於此不再贅述。

[440] "The way to get the attention of people in power about these issues is to demonstrate that they have skin in the game, sometimes literally skin in the game." Ben Wizner, *In Defense of Doing Wrong*, THE POINT, http://thepointmag.com/2015/politics/in-defense-of-doing-wrong (last visited Jan. 12, 2016).

刑事責任[441]。回顧我國搜索權與通訊監察權的修法過程，亦與此雷同，均是發生相關案件、立委意識到搜索或監聽有可能威脅到自己時，始大刀闊斧地修法，提高保護。

Wizner 律師之語，亦與前述 Gershowitz 教授對 *Riley* 案之評論不謀而合。Gershowitz 教授認為，最高法院之所以於 *Riley* 一案作出這麼明確之判決而拒絕妥協，很可能係因法官意識到手機搜索與他們自身休戚相關、較能同理自身手機資訊揭露於他人眼前的困窘羞愧感，以此保護如他們一般，同屬中產或菁英階級的人民[442]。

哈佛法學論叢的判決評釋中亦曾提及，在與法官較不那麼切身相關、涉及罪犯（不受歡迎的族群）的案件，諸如 *Maryland v. King*、*Florence v. Board of Chosen Freeholders* 等案，最高法院作利益權衡後，決定犧牲人民隱私，這也可能是因為法官未能易地而處之故[443]。

Akhil Amar 教授即主張，搜索合理性有無之判斷，不妨交由陪審團斷定。合理性大致上取決於常識，而陪審團則代表了一般人民的常識。對美國人民「安全」的威脅，同時來自於政府與暴徒。陪審團最適合決定在特定情形下，他們比較害怕警察還是搶匪，而此一判斷本來就會因時因地有所變數。在整個思考評議的過程中，陪審員們將會互相教育，了解憲法的意義、政府政策、合理性的概念競合以及自治共和體制下的公民職責[444]。

綜上所述，法官未必真的那麼「客觀中立」，其價值判斷很多時候仍受個人喜惡所左右[445]，判決論理也會因為結果是否影響自己而有所搖擺[446]。因此，

---

[441] 詳見Ellen Alderman、Caroline Kennedy 著，吳懿婷譯，《隱私的權利》，頁446（2001 年）。
[442] Gershowitz, *supra* note 313.
[443] The Supreme Court, *supra* note 322, at 256-60.
[444] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 818-19 (1994).
[445] 對於法官行為理論之討論，美國著名法官 Richard Posner 即指出，法官的判決受到個人特質、背景特徵（如種族、性別）與生命經驗等所左右。詳參 Richard A. Posner 著，李忠謙譯，《法官如何思考》，頁 456（2010 年）。

若自功能最適的角度思考，由法官負責搜索票之審理與核發，未必能夠真正發揮最適功能，不見得能做出有利人民的正確決定。反之，若能參考美國陪審制或現在力圖推動的人民觀審制，於事前或事後適度引進人民意見，可能是另一種解套方式。

由我國日前死刑存廢之辯論可知，民眾受「包青天」之傳統影響仍深，多半希望可能的犯罪者被繩之以法，甚至除之而後快，例如日前設監視器抓違停之爭議，不乏「隱私是違法的人用來保護自己的藉口」或「不違停幹嘛怕別人抓」之聲浪[447]，因此對於搜索票審查應會趨於寬鬆。然而，另一方面，陪審員也會意識到，自己說不定就是下一個被聲請搜索的對象，從而較同情被搜索者[448]；今天的抉擇，同時隱含著「將來自己是否也會被這樣大肆搜索」、「將來自己是否也會遭受手機內資訊被一覽無遺的窘困感」的價值決定，故審查又會趨於嚴謹。

這種作法其實有點類似請人民在 John Rawls 所設計的無知之幕（veil of ignorance）後下決定，迫使人民從社會最弱勢者（下一個受搜索人）的角度來考慮問題與社會制度（搜索票核發與否），使個人更有可能做出客觀中立的判斷。從而，天平的兩端就會在「追訴犯罪」與「保護自己」之間，取得適切的平衡點，人民隱私因而得到保障。

因此，本文認為，或許應從功能最適的角度重新思考令狀制度。形式上，搜索票由法官把關，符合正當法律程序的要求，惟實質上法官未必真如憲法所

---

446 Gershowitz, *supra* note 313.

447 議員反監視器抓違停 柯：腦袋裝大便，蘋果日報，2015 年 4 月 25 日，http://www.appledaily.com.tw/appledaily/article/headline/20150425/36513866（最後瀏覽日：2016 年 1 月 12 日）。

448 詳見王兆鵬（註 251），頁 315。論者或謂：法官也有可能是下一個受搜索人，就此點而言應與人民無甚差異？惟本文認為人民跟法官自始就站在不同的立足點上:陪審團的組成涵蓋社會各個層面，包含販夫走卒；法官則如前述 Gershowitz 教授所言，較多屬於中產或菁英階級。就此以觀，兩者受到搜索的可能性仍有高低之分，故一般人民較之法官有更大的誘因，謹慎考慮允許搜索可能引發之惡果。

期待的那般客觀與中立，能夠設身處地確實保護人民隱私。反之，若能於審查令狀時適度引進人民意見，或許更能在追訴犯罪與利己誘因兩者間取得平衡，不失為另一種思考方向。

4.3.2. 我國手機搜索制度之檢討與建議

如第三章所討論，本文認為手機資訊涵蓋詳細之個人檔案，更可能涉及私密敏感事項，應受憲法隱私權保障。然憲法對於個人資訊隱私權之保護並非絕對，國家基於公益之必要，得於不違反憲法第二十三條之範圍內，以法律明確規定強制取得所必要之個人資訊。

惟搜索人民手機資訊，形同讓人民的精神上秘密空間、生活中最私密的細節，盡暴露於國家機器之前。國家可藉手機資訊輕易重構個人生活樣貌，進而形成得以監控個人的敏感性資訊，實對人民隱私造成嚴重干預。故對於國家以強制力搜索人民手機、取得資訊之法規範，本文認為應採取嚴格審查標準。亦即，立法目的須為追求重大之公共利益目的，手段與目的之達成間須具直接及絕對必要關聯，始符憲法比例原則及保障人民基本權利之本旨。

本章所舉的四個美國手機搜索案例，扣回我國搜索法制，即是附帶搜索、搜索票之審查、不自證己罪適用範圍以及附帶扣押與另案扣押的問題。以下即分別對其進行合憲性之檢討與建議。

4.3.2.1. 附帶搜索手機資訊

審酌刑事訴訟法第 130 條附帶搜索之立法目的，係著眼於逮捕現場瞬息萬變的特殊性，旨在維護執法人員安全、防止證據遭到湮滅，以使國家刑事訴訟程序能順利進行，立法目的係為追求重要之利益。惟就手段與目的之達成之關聯性而論，在搜索客體係武器、毒品等實體物件時，附帶搜索之手段確實有助

達成上開目的；惟搜索客體換成手機資訊時，實有斟酌空間。

蓋就維護執法人員安全之目的而言，手機實非傷人凶器、不至危及執法人員安全；即使退一步承認手機內可能藏有凶器（如 *Riley* 案例示之手機夾層間藏有刀片等），此時僅需授權警方檢視手機外觀實體部位檢視是否藏有凶器或毒品，並扣押涉案手機即可，附帶搜索手機資訊並無助於安全目的之達成。

次就防止證據遭到湮滅之目的言，賦予警方附帶搜索手機資訊之權，或許有助前開目的之達成（可即時備份涉案證據等），然此一手段是否具絕對必要性，容有疑慮。實則，為免手機內證據遭到湮滅，警方僅需扣押手機，即可排除受逮捕人手動刪除證據之風險；若擔心證據遭遠端刪除，亦可採 *Riley* 案所建議的方法，如將手機關機、拔除電池，或解除手機自動鎖定、讓手機保持開機並隔絕外界訊號[449]等，即屬侵害較小而同等有效之手段。就此以言，授權警方於逮捕當下檢視手機內容，手段與目的之間並不具必要關聯，應認其不符比例原則而違憲。警方若覺有搜索、備份手機資訊之必要，應先扣押手機，再另行聲請令狀檢視其內資訊即可。

至於 Alito 大法官於 Riley 一案所提出的疑問：多數意見尋得的平衡點（手機不得附帶搜索），賦予手機裡的數位資訊比紙本受到更多保護，論理實有矛盾。同樣是涉案資訊，為何隨身皮包可以搜索，隨身手機則否[450]？本文認為，若自我國憲法隱私權的脈絡出發，兩者之間最大的區別，即在於前文所強調之概念：就手機的特質言，其之於個人的地位已由單純的「隨身物品」躍昇為「精神上秘密空間」，其有如精神上家宅，成為現代人安身立命之媒介。此一特性使手機應與其他隨身物品有所區別處理，應受憲法隱私權更高度的保護，而不論其內所存資訊之多寡。

[449] Riley v. California, 134 S. Ct. 2473, 2487 (2014).
[450] *Id*. at 2496-97.

再以手機功能眾多、與個人生活緊密交織的特性而論，個人在使用手機的同時，通聯紀錄、文字簡訊、生活照片、消費、就醫與瀏覽紀錄等各種公開或私密的個人資料，也全數存放在這座手機家宅之中。手機搜索暴露於政府眼前的資訊，只怕遠比徹底搜索房屋還多，因為手機除了將各種紀錄以數位形式保存外，更存放了大量不會以任何形式放在家宅內的敏感資訊[451]，私密照片即為一例。因此，自手機中所儲存的資訊質與量以觀，實與皮包或筆記本等其他隨身物品大相逕庭，反而與家宅並駕齊驅，有過之而無不及。

現制為避免過當而不合理的隱私侵害，既不許員警於逮捕時附帶搜索嫌犯身處之房屋，而須事先聲請搜索票，則手機亦應比照辦理。若將手機與其他隨身物品一視同仁，認為沒有將手機區別保護之必要，無不許附帶搜索之理，只怕完全忽略了科技變革所帶來的改變與衝擊，亦無視於手機資訊無論質或量，均非傳統實體物件可比之現實。

對此，或可採取與司法院釋字第 656 號解釋類似的作法[452]，審酌附帶搜索原始目的與手段對隱私權侵害之程度，將附帶搜索之適用，採取合憲性限縮解釋。亦即，限縮附帶搜索的適用空間，將搜索範圍限縮於傳統實體證據或武器之搜索。至於手機（或性質類似之筆電、iPad 與 iPod 之類存有大量個資的電磁紀錄載體），則因性質迥異，不得附帶搜索，應先經由法院介入審查控管，認確有必要核發搜索票後，檢警始得搜索取證。如此方能兼顧國家追訴犯罪之利益與憲法保障人民隱私權之意旨。

---

[451] *Id*. at 2490-91.

[452] 釋字第 656 號解釋：「民法第一百九十五條第一項規定……其名譽被侵害者，並得請求回復名譽之適當處分……惟如要求加害人公開道歉，涉及加害人自我羞辱等損及人性尊嚴之情事者，即屬逾越回復名譽之必要程度，而過度限制人民之不表意自由。」本號解釋即限縮民法第 195 條第 1 項後段所稱之回復名譽之適當處分之範圍。

4. 3. 2. 2. 手機搜索票之審查

搜索票制度之設，係著眼於搜索扣押等強制處分對人民基本權之侵害，爰建立事先審查制，要求執法者須具備相當理由、明確特定搜索標的物、聲請令狀後始得搜索，以此求取國家追訴犯罪與人民權利保障的平衡，避免無實質原因或非必要的強制處分[453]。

惟令狀明確性之要件，於搜索電磁紀錄載體時，法院對於明確性之要求似乎有所退讓，容許搜索票上為較寬鬆而模糊的記載[454]。如此是否符合憲法對於手段必要性之要求，不無疑慮。

就此，如前文所指出，本文認為手機有如一個未知的包裹，執法者檢視手機之前無從預知手機內存有哪些資訊，須待打開手機查閱後，始能得知內容，此為技術上限制所不得不然。本文亦承認，數位鑑識之手段、過程與步驟，常因個案而有所不同，若事前過度要求搜索票之明確性，無異緣木求魚，犯嫌亦可能會變更涉案證據之格式或存放路徑，以逸脫執法者之搜索。

然而，令狀明確性之退守，固然授予檢警極大空間，可窮盡搜索手機內所有可能涉案之證據；然此舉同時也讓個人或大或小、或公開或私密之資訊，赤裸裸於檢警眼前一覽無遺，更遑論手機資訊恐非僅影響受搜索人一人，他人隱私亦可能同受搜索（通聯紀錄、簡訊、照片均有此性質），就此以觀，實對人民隱私造成重大干預。地毯式搜索之授權，手段與目的之達成間是否具備必要關聯，實有討論空間。

對此，本文承認現行搜索技術上的限制，於今尚未發展出有系統而毋需人力的機械性鑑識方式，仍須以人力逐一點開查詢，始知涉案檔案之所在。以性侵害加害人手機中所存有之被害人裸照為例，涉案證據固然可能存在手機的圖

[453] 同前註 251。
[454] 法思齊（註 253），頁 143。

片庫中，但也可能以附件檔案形式附加在 Evernote 的筆記內，或是以雲端儲存的方式備份於 Dropbox 的資料夾裡[455]。法官並非鑑識專業，若於事前對於手機搜索的程序、範圍、方法予以過多限制，恐過於天真而有食古不化之嫌，亦加諸搜索人員過多枷鎖，導致搜索難竟其功，例如犯嫌可能把握此一漏洞，將涉案檔案變更形式或改換其他看似無關的儲存路徑，藉以規避檢警之搜索。因此，本文認為事前應給予檢警較多的空間，法院僅於事後審查搜索行為是否過當即可。此應屬國家追訴犯罪、取得證據之必要手段，尚與比例原則之要求無違。

然而，考量到手機資訊與個人生活緊密連結的特殊性，本文仍期許執法者仍應精益求精，力求建立一套有系統而不至過度干預人民隱私的搜索程序（例如設計如緝毒犬般，得以特定犯罪證據的新形態搜索方式，可由機器自動搜索出涉及犯罪的特定檔案），或對手機搜索訂出一套標準作業流程，讓一線員警有跡可循，否則無異於架空令狀明確性的要件。唯有如此，方能於有效執行搜索的同時，又能適度尊重人民隱私權。

4. 3. 2. 3. 手機密碼與不自證己罪

在美國，因有藐視法庭罪之設，有權處罰不依法院命令輸入手機密碼之被告，監禁至其願意輸入為止，故密碼是否受到不自證己罪特權保護而不得強制被告輸入，即成為攻防重心。該國最高法院雖未對此作出判決，惟歸納下級法院的判決，目前實務處理此類案件已有基本模式可循。法院同意手機密碼之性質與保險箱密碼類似，故具有供述性質而為受保護之客體，本於此一前提，再進一步認定個案事實是否符合定局原則而排除保護。*Baust* 案法院則將指紋與密碼區別處理，將指紋按捺視同鑰匙、筆跡或聲紋之提供，非屬供述，至於密碼則受不自證己罪特權之保護，除非符合定局原則之例外，不得強制被告揭露

[455] 至於儲存在雲端之資訊得否搜索之爭議，係另一更大的議題，本文不擬深論。

[456]。

相對於此，就我國目前法制現狀而論，法院目前似無強制手段命被告解鎖手機，僅得將上鎖的手機委由刑事警察局等相關單位破解，暫時無須面對強制解鎖是否侵犯不自證己罪特權之爭議。惟我國將來若修法增訂類似規定，得強制被告提交手機密碼時，相關爭議即會產生，故美國法院就此一問題之論辯，仍有值得我國借鏡之處。

對此，就手機密碼之提出而論，本文認為細究密碼之本質，實與鑰匙無異，僅其形式由實體鑰匙轉為數位金鑰而已：昔時以實體鑰匙打開上鎖的保險箱，今日則以數位鑰匙將鎖定之手機解鎖。密碼本身是中性的資訊，密碼之提供僅作為打開涉案手機的工具，有如命令被告提交實體鑰匙，並未進一步要求被告陳述是否涉案或所涉案件的內容及過程等，亦與犯案與否的評價無涉。因此，應認手機密碼不具供述性質，而與聲調、筆跡等證據類似，非不自證己罪保障範圍。

此外，考量到加密技術複雜度不斷提升、破解加密裝置愈顯艱難之現況，若不許國家強制個人揭露密碼、解鎖手機，形同讓受搜索人享有一塊不受搜索的「絕對領域」，即使聲請令狀仍無法搜索取證。如此將讓人民完全握有是否開放搜索的權柄，有如持有一個永遠打不開的保險箱，犯嫌盡可將犯罪證據悉數藏匿其中，令國家偵蒐犯罪之目的窒礙難行。就此而論，得強制解鎖上鎖手機之舉，應屬達成國家追求犯罪偵查目的之必要手段。

退萬步言，即使承認手機資訊之揭露具有供述性質，應受不自證己罪特權保護，則本文亦建議可引進美國法所發展出的定局原則：若政府可提出其他證據，證明所欲搜索之證據確實存在於手機之內，即可強制個人解鎖；然若政府仍無法確定證據是否存在，便不得強制個人提出。此法可求取政府與人民之間

[456] 詳參前文對於 Baust 一案之討論。

權力的平衡，亦能間接減少政府濫行搜索對人民隱私之侵犯，應值可採。

4.3.2.4. 附帶扣押及另案扣押於手機資訊之適用

美國法院對於一目瞭然法則是否適用於手機資訊搜索扣押之討論，回到我國即是附帶扣押及另案扣押是否適用之問題。Kerr 教授主張應摒棄一目瞭然法則，容許執法者盡一切手段搜索本案證據，至於他案證據則一律排除且不得揭露，如此可降低執法者搜索無關本案資訊之動機，既可維護國家偵查利益，亦可適度保障人民隱私[457]。

然本文認為 Kerr 教授著實過於樂觀。若採 Kerr 教授之見解，執法人員只怕會案案均採地毯式搜索，務求窮盡搜索載體內所有的資訊以免遺漏，結果對隱私的侵害不減反增。此外，設想一極端案例：若於搜索電腦時意外發現屍體的照片，卻須依上述處理原則而將證據排除，絕非妥當，犯嫌更有可能利用此漏洞，先以輕罪引誘警方上門搜索，再將重罪證據置於易被發現之處（如手機桌面），令警方「因小失大」。

本文結論上支持前述學者所提之重罪原則[458]，然論理略有不同。採取重罪原則是否能大幅降低執法人員搜索無關本案資訊之動機，進而保障人民隱私？本文仍持保留態度。未徹底檢視所有檔案前，如何知悉本案最重要的一張照片或其他重案關鍵性的影片不會藏在最後一個打開的檔案裡？可以想見偵查機關仍會傾向地毯式搜索，避免掛一漏萬、遺漏重要證據，故重罪原則對人民隱私權的保障似乎未必有所幫助。

承續前文之討論，本文承認目前技術上的限制：因對電磁紀錄搜索尚未發展出有系統而毋需人力的機械性鑑識方式，搜索時勢必須由人力逐一將檔案點

[457] Kerr, *supra* note 341, at 582-84.
[458] 李榮耕（註 242），頁 1108-09。

開、檢視是否與案件有關，故而無論案件輕重，偵查機關必須對電磁紀錄載體進行地毯式的搜索，方知載體內犯罪證據之有無。此舉雖對人民隱私有所干預，然非此不能探知涉案證據之有無，仍屬必要之惡。

然而，此時實應附以比例原則的考量：所欲保護之法益必須是生命、人身自由等極為重要的法益，始符國家追求重大公共利益之要求，正當化搜索手機對人民隱私權之干預。如僅為輕罪，則所欲保護法益輕微，但人民所受隱私侵害甚鉅，顯有不符比例之虞，而與憲法保障隱私權之旨有違。因此，本文支持重罪原則之見解，認附帶扣押及另案扣押僅於重罪方適用之。

實際執行上，或可借鏡監聽風波修法後，現行通訊保障及監察法的作法。根據該法第 5 條第 1 項，得進行通訊監察者僅限於最輕本刑為三年以上有期徒刑之罪與該項列舉之其他罪名，此一要件可以說是重罪原則的具體實踐，直接將法定刑較輕之輕罪排除在外。手機資訊之搜索扣押，若未能仿效通保法的作法，以重罪原則嚴加控管，則檢警很有可能藉故以合法的「本案搜索」，掩護違法的「他案搜索」，假小案查大案[459]。

綜上，本文認為，應對附帶扣押與另案扣押採合憲性限縮解釋，搜索人民手機資訊時，僅於重罪範圍內適用，輕罪則排除之。如此一來，方能落實比例原則之要求，於國家追訴犯罪之餘，仍兼顧人民隱私權之保障。重罪原則雖非完美，至少以現階段而言，仍屬較為可行之方法。

[459] 桃園地院錢建榮法官即曾於研討會上指出實務上鑽漏洞的作法：「有時候，檢察官很愛進行所謂的「釣魚監聽」，像是乙打給甲買毒品，但明明甲犯的才是販毒重罪，檢察官卻為了釣魚，連乙也申請監聽，甚至就把乙列為犯罪集團之一，忽略乙犯的只是使用毒品罪，根本不是能夠監聽的輕罪……詳參【監聽爭議】通保修法：保障人權？阻礙辦案？，公視新聞議題中心，2014 年 3 月 10 日，http://pnn.pts.org.tw/main/2014/03/10/【監聽爭議】通保修法：保障人權？阻礙辦案？（最後瀏覽日：2015 年 7 月 11 日）。

4. 3. 2. 5. 小結

就現有涉及手機搜索之判決以觀，處理手機內電磁紀錄之搜索時，我國司法實務似未能配合社會演進之實狀，意識到手機科技的特殊性，作出符合規範目的之調整。人民對手機內資訊是否享有合理隱私期待、政府能否或如何搜索手機始不致過度侵害人民隱私權等討論，似不見討論。

如前所述，警方逮捕現行犯時曾逕行沒收手機，甚至直接檢視、刪除手機內檔案；檢察官開偵查庭時，未先聲請搜索票即要求被逮捕人交出手機、當庭檢視手機內容等，引發被逮捕人抗議；法院亦曾判決警察無令狀接聽被告手機屬「蒐集被告犯罪證據目的範圍內之必要處分行為」等，而未就手機資訊搜索與憲法隱私權保障之權衡加以論述。

法院未針對手機資訊之搜索發展出新的見解，而係沿用過往處理實體證據的規範處理，之所以如此，一方面或許是被告及律師並未想到就搜索扣押所生隱私侵害予以爭執，另方面，卻也可能是因為法院缺乏隱私權意識之故。

核發電磁紀錄搜索票的搜索前階段，我國法院在令狀明確性原則上似乎有所退讓，容許搜索票上為較寬鬆而模糊的記載，允許檢警得對電磁紀錄載體為地毯式之搜索以取得證據。至於搜索執行完畢的後階段，我國法院則全面承認附帶扣押與另案扣押，搜索所得均可作為證據。即使檢警機關有違法取得證據之嫌，法院也常援引刑事訴訟法第 158 條之 4[460]，權衡之後仍認定違法取得之證據有證據能力。

令狀明確性的退守、地毯式搜索的權限，授予檢警極大的空間。此舉固然可將手機等電磁紀錄載體內所有可能存在的證據一網打盡，但與犯罪事實無關的諸多個人隱私（如照片、影片、瀏覽紀錄、簡訊文字等），卻也全數暴露在

[460] 刑事訴訟法第 158 條之 4：「除法律另有規定外，實施刑事訴訟程序之公務員因違背法定程序取得之證據，其有無證據能力之認定，應審酌人權保障及公共利益之均衡維護。」

檢警面前。

於美國法院涉及手機搜索之案件判決理由可看出，該國法院已逐漸意識到既有隱私權法制適用於手機時的扞格與侷限，重新審視手機之特殊性及其與隱私的密切關係，不再僵固適用舊時所發展出的法則，而係針對手機創設有別以往之見解，試圖讓隱私權保障跟上科技變革的腳步。

與美國相較，我國面對手機搜索案件時，執法者尚未能針對人民是否對手機內資訊享有合理隱私期待、檢視手機內資訊是否應事先取得搜索票、政府搜索手機資訊之方式是否過度限制人民隱私等加以考慮。由此足見執法者對手機搜索所生隱私侵害關注不足，並未適度調整以求取搜索扣押與隱私保障之間的平衡，實有為德不卒之憾。

綜合前文之討論，本文認為，我國既有之搜索扣押法制，於搜索手機資訊時，適用上應有所修正：手機不得附帶搜索、手機搜索票應附加事後審查、手機密碼不受不自證己罪特權保護、手機資訊之附帶扣押及另案扣押應採重罪原則，如此方能平衡人民隱私權與國家追訴犯罪之利益。

4.3.3. 動態的隱私權保障

誠如學者林鈺雄所言：「刑事訴訟法不容許以不擇手段、不問是非及不計代價的方法來發現真實[461]。」當犯罪追訴與人權保障之間互相衝突時，兩者不應有所偏廢，而係盡力謀求平衡[462]。

要如何在國家追訴犯罪之需求與憲法保障人民隱私權之間取得平衡，確實係一難題。以令狀原則與一目瞭然法則為例，均是當時的立法者或執法者因應當時的法律與案例，於犯罪追訴與人權維護間所取得的平衡點，力求於追訴犯

[461] 參林鈺雄（註 265），頁 12。
[462] 同前註。

罪時，兼及人民權利之維護。

以令狀原則為例，英國原有之空白搜索票（general warrant）使偵查機關得以不受限地恣意進行地毯式搜索，此制固然有助於發現真實，讓檢警有權翻天覆地盡可能搜索出所有的犯罪事證，人民隱私卻蕩然無存。令狀原則應運而生，該原則雖限縮了發現真實的範圍，卻有助於維護人民的權利。又如附帶搜索的適用範圍限制、對於搜索票明確性的要求、不自證己罪的保護範圍與一目瞭然法則適用與否等，均同此理。

惟於當初時空背景下畫出的線，適用於科技變遷快速的今日，卻常有窒礙難行之處。本章所選的四個美國法院判決，即是傳統法制遇上手機此一新興科技所生之爭議。由判決中可以觀察到，美國法上搜索扣押法制常與人民隱私權之保障緊緊相扣，法院適用早先發展出的法則時，多自隱私權之保障出發，審慎考量現時手機科技對人民生活與隱私觀念所帶來的變革，進一步探討原有的搜索扣押制度應如何調整修正，或直接不予適用，以兼顧追訴犯罪與維護隱私之需求。

在美國，政府搜索扣押受到憲法增修條文第四條之限制，法院爰藉由審理一件件政府行為是否侵害隱私而構成搜索之案件，權衡求取政府執法與人民隱私的平衡。涉及新興科技的爭議時，合理隱私期待有無、隱私權侵害之肯否，亦常係原被告攻防之重點，以及判決書詳加著墨之處。

美國法院因應科技變遷、舊法新詮之作為，實值我國借鏡參考。望我國法院亦能如司法院釋字第 392 號解釋理由書所示，不只是僵固地適用舊法，而係因時制宜：

> 「**憲法並非靜止之概念，其乃孕育於一持續更新之國家成長過程中，依據抽象憲法條文對於現所存在之狀況而為法的抉擇，當不能排除時**

代演進而隨之有所變遷之適用上問題。從歷史上探知憲法規範性的意義固有其必要；但憲法規定本身之作用及其所負之使命，則不能不從整體法秩序中為價值之判斷，並藉此為一符合此項價值秩序之決定[463]。」

以手機資訊的搜索扣押為例，本文認為，執法者不應抱殘守缺、拘泥前人見解，無視手機之類電磁紀錄載體與一般實體證據明顯不同的性質，僵化地套用附帶搜索、另案扣押等舊制而毫無調整。反之，法院應重新自隱私權的角度思考，正視手機、筆電等電磁紀錄載體其內儲存的龐大資料、對其搜索所導致的隱私侵害不可與傳統有體物同視之客觀現實，將兩者區別處理，甚或發展出新的處理法則。

但也不無另一種可能，例如將來隨著大數據（big data）發展，檢警設計出如緝毒犬般得以特定（sui generis）犯罪證據的新形態搜索方式[464]，一如 Facebook 漸趨精確的臉部辨識或 Gmail 的關鍵字掃描等，可由機器自動搜索出涉及犯罪的特定檔案，與犯罪無關的檔案則毋庸暴露於檢警之前。此等搜索手段可以有效減少對人民隱私之侵害，僅就犯罪證據為搜索。到了那時候，違憲審查基準之操作，或許又是另一番光景。

再以加密技術的進展而論，技術上已發展出所謂的可否認式加密（deniable encryption），使檢警辦案更加棘手。詳言之，如 TrueCrypt 軟體提供設定隱藏加密區之功能，可設定不同密碼對應不同加密區，例如輸入 A 密碼時，顯示出來的是 ABCD 等與本案無關之檔案，輸入 B 密碼時，才會顯示 EFGH 等真正涉案的證據。道高一尺，魔高一丈，藉由可否認式加密的技術協助，被告很有可能防患未然，預先將犯罪證據存在隱藏加密區中，待被法院強迫要求解鎖時，

[463] 釋字第 392 號解釋理由書參照。

[464] 美國最高法院認為，緝毒犬之嗅聞僅會揭露違禁品之存在，既不須打開旅客行李，相對於一般搜索亦屬輕微，故非屬憲法增修條文第 4 條所稱之搜索。詳見 United States v. Place, 462 U.S. 696 (1983).

輸入的卻是另一個表層加密區的密碼，達到堂皇否認（plausible deniability）的目的，進而逍遙法外。若此，則加密技術究否應予管制[465]？檢警究應如何突破加密技術的重重封鎖？金鑰信託（key escrow）或金鑰復原（key recovery）是否為可能的解套方案？想必是今後不得不面對的課題。

面對新科技與舊法則之間適用上的齟齬時，執法者實應重新思考隱私權之本旨，並將科技變革及其影響納入考慮，重新權衡犯罪追訴所欲保障之利益，以及過程中對人民權利造成的侵害，以落實憲法保障隱私權之美意。無論科技怎麼變遷、侵害無可避免，執法者仍應以造成較小損害之必要手段為之，致力在兩者之間找出新的平衡點。

社會與科技的發展並不會停留在此處，今日個人的私密空間漸由實體家宅轉移至手機數位空間，明日，或許又有尚未預見的嶄新科技，使這塊神聖私領域又轉移至什麼新領域，亦未可知。無論科技如何改變，不變的是隱私權賦予個人領域的保障，其賦予個人一塊自由不受干擾、免於國家干預的空間、自主控制是否揭露個人資訊，使個人能自在探索、交往溝通、自由形塑自主人格，這才是隱私權之核心價值所在。

亦即，無論形式（家宅、手機、未來的某種新科技……）如何改變，不變的是隱私權對於實質（個人不受干預之私密領域與資訊自主掌握）的保障。因此，對於憲法隱私權的解釋，應時時回溯思考憲法所欲保障的權利本質為何，這樣的本質是否會因為時代變動而有不同表現形式。法院應敏銳地覺察時代變化所導致之人民生活型態變遷，一再構築屬於當代的憲法意義，以實踐保障人民權利的承諾。

[465] 事實上，加密技術應否管制、業者是否應留有後門等，早在本章所列案件判決前便已經歷一番立法論辯與官學爭執。政府方主張，為免犯罪人藉加密技術藏匿證據，應限制加密技術之使用。惟民權團體則持相反態度，認為此係個人保有隱私、防範政府監控的最後機會。惟相關爭論並非本文重心，點到為止。

5. 結論

本篇論文的研究主軸，係以手機科技為中心，試圖探討手機科技與現有隱私權概念的連結與互動，論述本文認為手機資訊應受憲法隱私權保護之理由。復引進美國法手機搜索案例作為借鏡，試圖對我國現行手機搜索扣押相關法制提出建議，望於國家犯罪偵查需求與人民資訊隱私保障間求取平衡。

藉由本文的討論可知，手機為現代人安身立命之媒介，重要性有如精神上家宅，應屬憲法隱私權保障之個人生活私密領域；個人生活各方面細節盡在手機之中，手機資訊形同掌中大數據，亦應落於憲法隱私權保障個人資訊自主控制之範疇，且應將整支手機內的所有資訊包裹視為一個標的受到同等保障，不因個別資訊隱私程度高低而有差別待遇。國家若欲以強制方法取得手機資訊，對既有搜索扣押法制應採嚴格審查標準，解釋適用上應作如下修正：手機不得附帶搜索、手機搜索票應附加事後審查、手機密碼不受不自證己罪特權保護、手機資訊之附帶扣押及另案扣押應採重罪原則。如此，方能兼顧國家追訴犯罪之利益，以及憲法對隱私權之保障，讓人民享有一塊自由呼吸的空間，亦適度避免剖繪科技所生之監控風險，確保人格自由發展不受阻礙。

本文謹以手機科技所生隱私權相關討論為引，期許我國實務能夠漸漸增加對新興科技與隱私權相關議題之關注，以符合大法官的期待：「依據抽象憲法條文對於現所存在之狀況而為法的抉擇」。對於憲法與隱私權的解釋，不應拘泥於原本條文之詮釋或考證，而須回溯思考憲法所欲保障的權利本質為何，以及權利本質之體現形式，是否會因為時代變動而有所變化，使憲法賦予之保障有所連動。執法者應敏銳地嗅聞時代的變遷與人民的需要，在有限的條文下實踐保障人民權利的承諾，重新形構出屬於當代的憲法意義。期許國家致力追訴審判犯罪之餘，亦能追隨時代腳步，跟上科技進步，舊法新詮，捍衛人民受憲法保障之隱私權。

附錄：參考文獻

1. 中日文部分

1. 1. 書籍

Ellen Alderman、Caroline Kennedy 著，吳懿婷譯（2001），隱私的權利，台北：商周。

Richard A. Posner 著，李忠謙譯（2010），法官如何思考，台北：商周。

Tim Wu 著，顧佳、陳正芬、周佳欣譯（2013），誰控制了總開關？，台北：行人。

王兆鵬（2010）。《刑事訴訟講義》，5 版。台北：元照。

王旭正、柯永瀚（2007）。《電腦鑑識與數位證據：資安技術、科技犯罪的預防、鑑定與現場重建》，初版。台北：博碩文化。

王佳煌（2005）。《手機社會學？》，初版。台北：學富文化。

王浩威（2003）。《我的青春，施工中——台灣少年記事》，初版。台北：心靈工坊。

林子儀、葉俊榮、黃昭元、張文貞（2009）。《憲法權力分立》，2 版。台北：新學林。

林鈺雄（2008）。《干預處分與刑事證據》，初版。台北：元照。

林鈺雄（2010）。《刑事訴訟法（上）》，6 版。台北：自刊。

1. 2. 專書論文

小倉利丸（2003）。〈日本型監視社会に対抗するために〉，收於：白石孝、小倉利丸、板垣竜太等編，《世界のプライバシー権運動と監視社会》，頁 13-49。東京：明石書店。

王兆鵬（2008）。〈不自證己罪保護之客體〉，收於：《一事不再理》，頁 223-237。台北：元照。

王兆鵬（2003）。〈論附帶搜索〉，收於：《搜索扣押與刑事被告的憲法權利》，頁 167-197。台北：元照。

林子儀（2015）。〈公共隱私權〉，收於：《第五屆馬漢寶講座論文彙編》，頁 7-62。台北：馬氏思上文教基金會。

林子儀（2015）。〈隱私權法制的新議題：監控與隱私自我管理〉，收於：《第五屆馬漢寶講座論文彙編》，頁 65-115。台北：馬氏思上文教基金會。

陳仲嶙（2002）。〈隱私權概念的理解與充填〉，收於：《台灣憲法之縱剖橫切》，頁 637-661。台北：元照。

1. 3. 期刊論文

王兆鵬（1999）。〈論附帶搜索〉，《月旦法學雜誌》，第 55 期，頁 118-131。

李榮耕（2015）。〈科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展〉，《國立臺灣大學法學論叢》，第 44 卷第 3 期，頁 871-969。

李榮耕（2012）。〈電磁紀錄的搜索及扣押〉，《國立臺灣大學法學論叢》，第 41 卷第 3 期，頁 1055-1116。

李震山（2005）。〈來者猶可追，正視個人資料保護問題─司法院大法官釋字第六○三號解釋評析〉，《台灣本土法學雜誌》，76 期，頁 222-234。

邱文聰（2009）。〈從資訊自決與資訊隱私的概念區分──評「電腦處理個人資料保護法修正草案」的結構性問題〉，《月旦法學雜誌》，第 168 期，頁 172-189。

林鈺雄（2001）。〈拘提證人與附帶搜索〉，《月旦法學雜誌》，第 75 期，頁 14-15。

法思齊（2011）。〈美國法上數位證據之取得與保存〉，《東吳法律學報》，第 22 卷第 3 期，頁 95-147。

徐仕瑋（2013）。〈數位證據與現行搜索、扣押法制間之適用問題──以硬碟等

儲存媒介之搜索、扣押為中心〉,《檢察新論》，第 13 期，頁 29-46。
黃厚銘（2002）。〈網路上探索自我認同的遊戲〉,《教育與社會研究》，第 3 期，頁 65-106。
劉定基（2014）,〈雲端運算與個人資料保護－以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心〉,《東海大學法學研究》，第 43 期，頁 53-106。
劉靜怡（2002）,〈網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河〉,《資訊管理研究》，第 4 卷第 3 期，頁 137-161。

1. 4. 網路文獻

曹乙帆，〈雲端運算的儲存基礎架構 揭開雲端儲存的面貌〉，雲端運算智庫，http://www.runpc.com.tw/content/cloud_content.aspx?id=105324（最後瀏覽日：2017 年 11 月 5 日）。
黃重憲，〈淺談雲端運算〉，臺灣大學計算機及資訊網路中心電子報，2009 年 3 月 20 日，http://www.cc.ntu.edu.tw/chinese/epaper/0008/20090320_8008.htm（最後瀏覽日：2016 年 1 月 12 日）。

1. 5. 學位論文

李明勳，合理隱私期待之研究——以定位科技為例，政治大學法律學研究所碩士論文，2013 年。
林一德，電子數位資料於證據法上之研究，台灣大學法律學研究所碩士論文，2000 年。
詹文凱，隱私權之研究，台灣大學法律學研究所博士論文，1998 年。
劉秋伶，數位證據之刑事證據調查程序，政治大學法律學研究所碩士論文，2010

年。

簡陳由，論附帶搜索與隱私權保障之衝突，中國文化大學法律學研究所碩士論文，2015 年。

2. 英文部分

2. 1. 專書

Greenwald, Glenn. 2014. *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York: Metropolitan Books.

Lessig, Lawrence. 2006. *Code: And Other Laws of Cyberspace, Version 2.0.* New York: Basic Books.

Levinson, Paul. 2004. *Cellphone: The Story of the World's Most Mobile Medium and How it Has Transformed Everything!*. New York: Palgrave Macmillan.

Ling, Rich S. 2008. *New Tech, New Ties: How Mobile Communication is Reshaping Social Cohesion.* Cambridge, Mass: MIT Press.

Mayer-Schonberger, Viktor. 2009. *Delete: The Virtue of Forgetting in the Digital Age.* Princeton, NJ: Princeton University Press.

Palfrey, John and Urs Gasser. 2010. *Born Digital: Understanding the First Generation of Digital Natives*. New York: Basic Books.

Silva, Adriana de Souza e and Jordan Frith. 2012. *Mobile Interfaces in Public Spaces: Locational Privacy, Control, and Urban Sociability.* New York and London: Routledge.

Solove, Daniel J. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press.

Solove, Daniel J. 2008. *Understanding Privacy.* Cambridge: Harvard University

Press.

Solove, Daniel J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York: NYU Press.

Steiner, Christopher. 2013. *Automate This: How Algorithms Took Over Our Markets, Our Jobs, and the World*. New York: Portfolio.

2. 2. 期刊論文

Amar, Akhil Reed. (1994). Fourth Amendment First Principles, *Harvard Law Review* 107:757-819.

Bloustein, Edward J. (1964). Privacy as An Aspect of Human Dignity: An Answer to Dean Prosser, *New York University Law Review* 39: 962-1007.

Brenner, Susan W. & Frederiksen, Barbara A. (2002). Computer Searches and Seizures: Some Unresolved Issues, *Michigan Telecommunications And Technology Law Review* 8:39-114.

Chen, Chung-Lin. (2010). In Search of a New Approach of Information Privacy Judicial Review: Interpretation No. 603 of Taiwan's Constitutional Court as a Guide, *Indiana International & Comparative Law Review* 20:21-45.

Clancy, Thomas K. (2005). The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, *Mississippi Law Journal* 75:193-286.

Fried, Charles. (1968). Privacy, *Yale Law Journal* 77:475-493.

Gold, Aaron J. (2015). Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software, *William and Mary Law Review* 56:2321-2350.

Kerr, Orin S. (2005). Search Warrants in an Era of Digital Evidence, *Mississippi*

Law Journal 75:85-138.

Kerr, Orin S. (2005). Searches and Seizures in a Digital World, *Harvard Law Review* 119:531-585.

Kerr, Orin S. (2010). Ex Ante Regulation of Computer Search and Seizure: A Reassessment, *Virginia Law Review* 96:1241-1293.

Kerr, Orin S. (2011). An Equilibrium-Adjustment Theory of the Fourth Amendment, Harvard Law Review 125:476-543.

Kerr, Orin S. (2012). The Mosaic Theory of the Fourth Amendment, *Michigan Law Review* 111:311-354.

Nissenbaum, Helen. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law & Philosophy* 17:559-596.

Nissenbaum, Helen. (2004). Privacy as Contextual Integrity. *Washington Law Review* 79: 119-157.

Ohm, Paul. (2011). Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, *Virginia Law Review In Brief* 97:1-12.

Posner, Richard A. (2008). Privacy, Surveillance, and Law, *The University of Chicago Law Review* 75:245-260.

Prosser, William L. (1960). Privacy. *California Law Review* 48:383-423.

Solove, Daniel J. (2002). Conceptualizing Privacy. *California Law Review* 90:1087-1155.

Solove, Daniel J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154:477-560.

Solove, Daniel J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126:1880-1903.

Stuntz, William J. (2002). Local Policing after the Terror, *Yale Law Journal*

111:2137.

Terzian, Dan. (2014). Forced Decryption as Equilibrium—Why It's Constitutional and How Riley Matters, *Northwestern University Law Review Online* 109:56-63.

Terzian, Dan. (2014). The Fifth Amendment, Encryption, and the Forgotten State Interest, *UCLA Law Review Discourse* 61:298-312.

Terzian, Dan. (2015). Forced Decryption as a Foregone Conclusion, *California Law Review Circuit* 6:27-36.

The Supreme Court. (2014). 2013 Term—Leading Cases, *Harvard Law Review* 128: 251-260.

Watzel, Ryan. (2014). Riley's Implications for Fourth Amendment Protection in the Cloud, *Yale Law Journal Forum* 124:73-79.

Warren, Samuel D. and Brandeis, Louis D. (1890). The Right to Privacy. *Harvard Law Review* 4:193-220.

Weir, Bryan K. (2010). It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches, *George Mason University Civil Rights Law Journal* 21:83-121.

Wellman, Barry. (2001). Physical Place and Cyberplace: The Rise of Personalized Networking, *The International Journal of Urban and Regional Research* 25:227-252.

Winick, Raphael. (1994). Searches and Seizures of Computers and Computer Data, *Harvard Journal of Law & Technology* 8: 75-128.

2. 3. 專書論文

Gergen, Kenneth J. (2002). The Challenge of Absent Presence. Pp. 227-241 in

Perpetual Contact: Mobile Communication, Private Talk, Public Performance, edited by James E. Katz and Mark Aakhus. Cambridge/New York: Cambridge University Press.

Katz, James E. and Mark Aakhus. (2002). Conclusion: making meaning of mobiles – a theory of Apparatgeist. Pp. 301-318 in *Perpetual Contact: Mobile Communication, Private Talk, Public Performance*, edited by James E. Katz and Mark Aakhus. Cambridge/New York: Cambridge University Press.

Richardson, Ingrid. (2008). Pocket Technospaces: the Bodily Incorporation of Mobile Media. Pp. 66-76 in *Mobile Phone Cultures*, edited by Gerard Goggin. New York; Routledge.

Turkle, Sherry. (2008). Always-on/Always-on-you: The Tethered Self. Pp 121-137 in *Handbook of Mobile Communication Studies*, edited by James E. Katz. Cambridge, MA: MIT Press.

2. 4. 網路文獻

Gershowitz, Adam. 2014. Symposium: Surprising unanimity, even more surprising clarity, SCOTUSblog (Jun. 26, 2014), http://www.scotusblog.com/2014/06/symposium-surprising-unanimity-even-more-surprising-clarity

Goodman, Jody. Forced Data Decryption: Does It Violate the Fifth Amendment?, Criminal Justice, http://www.crowell.com/files/Forced-Data-Decryption-Does-It-Violate-the-Fifth-Amendment.pdf (last visited Jan. 12, 2016).

Hofmann, Marcia. Apple's Fingerprint ID May Mean You Can't 'Take the Fifth', Wired (Sep. 12, 2013),

http://www.wired.com/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth

Kerr, Orin. The significance of Riley, The Volokh Conspiracy (Jun. 25, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley

Kerr, Orin. Apple's dangerous game, part 3: Where do you draw the line, and what's the privacy tradeoff?, The Volokh Conspiracy (Sep. 22, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/22/apples-dangerous-game-part-3-where-do-you-draw-the-line-and-whats-the-privacy-tradeoff

Kerr, Orin. Virginia state trial court ruling on the Fifth Amendment and smart phones, The Volokh Conspiracy (Nov. 3, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/03/virginia-state-trial-court-ruling-on-the-fifth-amendment-and-smart-phones

Kerr, Orin. Court invalidates cell phone warrant as overbroad, The Volokh Conspiracy (Feb. 23, 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/02/23/court-invalidates-cell-phone-warrant-as-overbroad

Kopp, Glen and Kedar Bhatia. Fingerprint Lock Won't Protect Phone From Law Enforcement, Law 360 (Dec. 12, 2014), http://www.law360.com/articles/603831/fingerprint-lock-won-t-protect-phone-from-law-enforcement

Posner, Richard A. The last thing a woman about to have an abortion needs is to be screamed at by the godly, Supreme Court Breakfast Table (Jun. 26, 2014), http://www.slate.com/articles/news_and_politics/the_breakfast_table/features/

2014/scotus_roundup/scotus_end_of_term_remembering_town_of_greece_and_more_on_cellphones_buffer.html

Prensky, Marc. Digital Natives, Digital Immigrants, On the Horizon, http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf (last visited Jan. 12, 2016).

Solove, Daniel. Does the U.S. Supreme Court's Decision on the 4th Amendment and Cell Phones Signal Future Changes to the Third Party Doctrine?, LinkedIn (Jun. 25, 2014), https://www.linkedin.com/pulse/20140625172659-2259773-does-the-u-s-supreme-court-s-decision-on-the-4th-amendment-and-cell-phones-signal-future-changes-to-the-third-party-doctrine

Villasenor, John. Can the Government Force Suspects To Decrypt Incriminating Files?, Slate (Mar. 5, 2012), http://www.slate.com/articles/technology/future_tense/2012/03/encrypted_files_child_pornography_and_the_fifth_amendment_.html