

專題研析

手機「鑑識」的取證

蔡明珊

目次

壹、前言

貳、手機鑑識之法律上定位

一、手機的取得

二、手機鑑識為取證程序

三、手機鑑識為搜索

參、手機的搜索

一、搜索的開啟

二、搜索的範圍

(一)學說見解

(二)我國實務見解：相當關連性

(三)本文見解

(四)相當關連性不足之處

(五)未來展望

肆、結論

參考文獻

壹、前言

隨著科技發展，人們蒐集、存放資料的方式，也由物理儲存方式演變成數位化存放在數位裝置中。在智慧型手機出現之後，手機不僅作為通訊工具，更包含相簿、網路瀏覽器、生活記事、電

子支付等等，又因為手機往往被人貼身攜帶，而因此可以記錄個人行蹤，若是又與穿戴式裝置連動，手機內還可能會儲存個人身體資訊，例如步行步數、血壓、月經週期、或是睡眠狀況等等。

手機與個人之間的連結如此緊密，使得幾乎可以僅通過手機就了解一個人



的各方面資訊，因此在犯罪偵查的領域，偵查機關不免想要利用手機掌握犯罪證據。此處所稱利用手機掌握犯罪證據，主要是指取得手機內部儲存的數位證據，而非指對於手機外觀的取證行為（例如觀察手機上有無沾染指紋或血跡）。

目前手機常見取證的方法，都是必須先取得手機的本體，在開機狀態下透過網路連接取證設備進行取證¹。這些取證設備可以稱為行動設備鑑識工具（mobile device forensic tools，簡稱 MDFTs），這並不是一種特定的技術或機器，而是由第三方公司研發並販售給國家、用以作為手機鑑識工具的總稱。這些工具的功能及技術可能會因為開發商的不同而有不同，但多數可以達成以下幾點核心功能：(1) 繞過安全功能以訪問鎖定的行動裝置（也就是俗稱的破解密碼）、(2) 訪問儲存在設備、雲端備份及線上帳戶中的數據、(3) 整理、分析裝置中的資訊，並輸出成單一的資料庫²。

又行動設備鑑識工具所可以擷取的

資訊，以我國偵查機關使用最廣泛的品牌 CelleBrite 公司所生產的 UFED 系列為例，可以擷取的資訊包括：所有通聯紀錄（包含還原刪除紀錄）、螢幕截圖、照片、錄影、錄音、對話紀錄、簡訊資訊（號碼、人名、時間、日期、內容）、電話資訊（號碼、手機資訊、人名、時間、日期、通話長度）、網際網路瀏覽紀錄及相關 IP 位址、解碼通訊軟體等應用程式並讀取其中內容，並可以依據上述資料，建立手機持有人通聯紀錄網路³。

手機與持有人連結緊密、蘊含資訊種類豐富、記憶體容量龐大，而手機鑑識工具的功能又可以廣泛取得手機內的資訊，則我國刑事訴訟法現行取證規定，設計之初乃是針對有體物的取證所設想，是否可以直接適用於數位證據、數位儲存裝置的搜索？是否對人民基本權，尤其是隱私權造成過大的侵害？即生疑義。以下本文將以手機內的數位證據取證為中心，首先探討手機鑑識之法律上定位，以及從基本權角度檢視目前以搜索規定處理的作法是否適當？接下

¹ 相關技術說明參陳詰昌，數位鑑識「原件不可變動原則」之適用—由行動裝置鑑識與電腦鑑識差異探討，《司法新聲》，2016年7月，119期，48頁。

² Taylor Applegate, *Mobile Device Forensic Tools: A Help or a Hindrance to Constitutional Cellphone Searches?*, 35 STAN. L. & POL'Y REV. 284, 289 (2024).

³ 周昕緯、高佳豪，手機取證系統運用於犯罪偵查之研究，《行政院海岸巡防署自行研究報告》，2017年10月，12頁。

來將說明我國目前對於處理手機取證的法律問題有何爭議存在，主要將分成開啟手機搜索及手機搜索範圍二大部分。最後將提出本文對於目前爭議問題的看法，及未來規範面上有何可以調整之處。

貳、手機鑑識之法律上定位

一、手機的取得

如果國家想要對手機進行鑑識，前提就是必須先取得手機本體，因此在討論手機鑑識的法律上定位之前，先說明取得手機的法律上方式。

依據我國刑事訴訟法（下稱本法），手機作為有體物本身，自然可以是本法第 128 條 2 項 2 款之「應扣押之物」，因此只要法官合法簽發的令狀上將手機列為應扣押之物，搜索並扣押手機本體，與搜索後扣押一本帳冊、一把刀均無二致，不是問題所在。

有問題者在於沒有搜索令狀，或是搜索票未記載手機為得扣押之物時，若搜索到手機，可否扣押？在執行本法第 130 條附帶扣押、第 131 條 1 項、2 項，或其他有票搜索但未記載得扣押手機的情況下，若搜索時剛好發現受搜索人的手機，可否扣押？此涉及「偶然發現

物」的附帶扣押問題。第 133 條規定得扣押之物為「可為證據之物」及「得沒收之物」，此在未記載於搜索票上時，必須由執行人員臨場判斷是否屬於上述兩類得扣押之物，判斷標準為必須具有「合理依據」。又「合理依據」的來源，有兩種類型：一為由發現物本身得知、二為由發現物存在的方式、狀態推知⁴。在偶然發現手機的情況下，手機本身雖非違禁品，但若結合搜索本身已知的犯罪資訊，手機可能會因此產生「附條件的合理依據」，例如因為貪瀆案件發動搜索，在被告辦公室發現手機，此時考量到貪瀆案件常見的犯罪結構，可以合理懷疑手機被用以作為雙方聯絡工具而可為本案證物，此為由手機本身得知的合理依據；至於由發現物存在的方式、狀態推知，則例如在搜索時發現多組 SIM 卡、同時可以使用的手機，則可以建立例如詐欺等犯罪的合理依據，得沒收手機。在此本文想強調的是，手機承載大量個人資訊，幾乎所有案件都可以在手機中找到證據，則手機似乎可以是很多案件的「得為證據之物」，雖然合法執行搜索容許另案扣押、附帶搜索也沒有限制只能扣押本案得為證據之物，但僅因為手機可能作為被搜索人所犯下的任何「潛在犯罪」的證據，只

⁴ 林鈺雄，註 9 書，頁 166-170。



能算是「單純的懷疑、臆測」，不足以建立扣押的合理依據而扣押受搜索人的手機。舉例而言，若容許警察以現行犯逮捕醉態駕駛者後，附帶搜索中只要發現被告的手機即可以扣押，顯然不合理⁵。

二、手機鑑識為取證程序

或許是因為手機「鑑識」之用語，過去實務多以「鑑定」程序進行手機鑑識⁶。然而，此見解應有將干預處分與證據調查混為一談的謬誤：取得證據與調查證據是不同的概念，學說上舉例：進入吸毒犯住宅搜索並扣押白色粉末，為取證過程，而將該白色粉末送請鑑定確認是否為安非他命及命鑑定人出庭，則為證據調查程序⁷。在手機鑑識的問題上，真正作為證據使用者，乃是手機中的數位資訊（如通訊軟體中的對話紀錄），而不是手機本身，因此手機鑑識目的在「取得手機裡面的數位證據」，應為前端的取得證據階段，至於手機鑑識所得之檔案，如果因為運用行動設備

鑑識工具而使得手機內的數位資訊變成以數字及符號方式呈現，而須經由具有特別知識經驗的技術人員說明以使法庭成員了解數位證據的意義內容，才是後端證據調查階段，是否應該以鑑定程序行證據調查的問題。

三、手機鑑識為搜索

(一) 隱私權

既然確認手機鑑識為取得證據的階段，則會涉及基本權干預的問題。手機內儲存大量個人資訊，而人民生活與手機密不可分，對於手機內資訊享有合理隱私期待應無疑問，則手機鑑識應屬干預人民隱私權的行為。

(二) IT 基本權？

手機取證的領域，另一個可能被討論的基本權類型，為德國法所發展的 IT 基本權，即資訊科技基本權。此為德國聯邦憲法法院所提出，保障資訊科技系統私密性與完整性的基本權。是一種補遺性基本權，只在其他特別基本權保護

⁵ 附帶一提，目前法規範解釋下，附帶搜索之扣押仍必須符合第 133 條的扣押要件，即可為證據之物或得沒收之物。惟考量附帶搜索目的之一在維護執法人員安全，是否應容許警察在附帶搜索後，至少可以「暫時保管」具有攻擊危險性、但並非違禁物或可得證據之物？例如：被告隨身攜帶的金屬叉子，可能是值得思考的問題。

⁶ 李榮耕，電磁紀錄的搜索及扣押，《臺大法學論叢》，2012 年 9 月，41 卷第 3 期，1085 頁。雖然這篇文章討論主題為「電腦鑑識」，但與本文所討論的手機鑑識，在此部分的法理應可互相援用，理由在於都是必須以鑑識技術由實體數位裝置中取得數位檔案作為證據使用。

⁷ 林鈺雄，司法警察（官）之身體檢查處分及其救濟，《月旦實務選評》，2023 年 8 月，3 卷 8 期，117 頁。

範圍所不及時，才會加以檢驗⁸。

首先說明，目前司法院解釋及各級法院裁判皆未肯認 IT 基本權為我國憲法所保障之基本權類型，但學說仍有倡議應承認之⁹，已應對科技未來發展。學說對於 IT 基本權的討論，集中在來源端通訊監察的脈絡，針對用木馬程式「駭」入手機取得資訊的偵查態樣¹⁰，認為傳統的通信監察授權條款並未包含「讓資訊設備中毒」的附隨干預權限。而在實體取得手機並進行鑑識的情況下，則未見相關討論。然而，目前手機鑑識之技術，在破解開機密碼鎖或圖形鎖、對行動 APP 進行取證、及進行檔案刪除還原等蒐證時，常必須進行「提權」操作，即取得手機的最高控制權限（Android 系統取得最高權限帳號稱為 Root，iOS 系統取得最高權限為 iOS JailBreaking¹¹），常見方式為透過刷機方式或是透過程式載入的方式進行，簡單來說就是**置換作業系統**，以取得最高權限。則此是否也是一種所謂的「駭」入手機、使手機中毒的方式？是否也會落入 IT 基本權的範圍，而可能會認為

在未有法律授權之前，不得進行手機鑑識之取證？

本文以為，首先就 IT 基本權所想要保護的對象為資訊設備的「私密性」及「完整性」觀察，似乎就是「隱私權」及「財產權」的範圍，是否真有另外創設基本權之必要，本身即存在疑義。再觀察目前 IT 基本權的討論範圍是「來源端通訊監察」，實施樣態為秘密裝設木馬程式至相對人的裝置中，且技術上無法限定在擷取某特定資訊，造成可能在手機中任意撈取各類型資訊的潛在風險，則或許可以認為，提出 IT 基本權之論者，真正在乎的重點實為「秘密施行」此類侵入手機的偵查技術，使相對人在不知情的情況下，繼續使用手機而不斷增加資訊暴露在國家監視可能的範圍，而非手機裝置本身是否被改變。則在此觀點下，手機鑑識是在國家取得手機的物理上占有後，對手機的取證行為，雖然在技術上可能也會透過提權方式改變手機的程式運作，對於手機內部任意資訊也有風險，然而此時相對人已明知手機在國家占有中，此點與來源端

⁸ 王士帆，網路之刑事追訴——科技與法律的較勁，《政大法學評論》，2016年6月，145期，350-352頁。

⁹ 林鈺雄，《刑事訴訟法實例解析》，自版，2023年8月，6版，216頁。

¹⁰ 林鈺雄，同前註9。施育傑，數位證據的載體、雲端與線上取證—搜索扣押與類型化的觀點，《月旦裁判時報》，2017年10月，64期，64頁。

¹¹ 周昕緯、高佳豪，註3文，頁9。



通訊監察此等「秘密施行」搜索技術有所不同。本文以為，此時僅以「隱私權」保護即已足，不需動用 IT 基本權的概念，此見解亦可以解釋我國目前對於 IT 基本權的討論議題範圍。

既然確認手機鑑識為對隱私權干預之取證行為，則我國法上對於干預隱私權的基本權干預授權類型為搜索，故手機鑑識應為搜索。目前實務及學說也都是在搜索、扣押的框架下討論手機鑑識及扣押搜得證據的問題，本文以下將直接以「手機搜索」的用語展開討論，而捨棄容易聯想到鑑定之「手機鑑識」用語。

參、手機的搜索

接下來要面臨的問題是，取得手機之後，是否就當然可以打開手機尋找證據？即是否可以對手機「內部」進行搜索？有認為對手機內部的搜索應屬於第 122 條「電磁紀錄」¹²，另有見解認為在 PC 時代，人們把數位化的資料儲存在 PC 中的硬碟，搜索 PC 主要目的當然就是在搜索硬碟中的數位資料，因此

PC 及其內的數位資料應該屬於第 122 條「物件」所可以包含的範圍¹³。無論採取上述何種見解，檢索手機內部是我國刑事訴訟法所容許的搜索範圍，應無疑問。

目前關於手機搜索的爭議，主要集中在搜索的執行問題。例如附帶搜索可否搜索手機內容？以及對於另案扣押在手機搜索的適用問題？此二問題一個在處理搜索的「開啟」，另一個在處理搜索的「範圍」，釐清此二問題有助於對手機搜索有全面的理解。

一、搜索的開啟

搜索以有令狀為原則，無令狀為例外。如果法官核發的搜索票已將手機以電磁紀錄或物件的形式記載於搜索票上，對於手機搜索的開啟已經過法官的審核，具有形式上的合法性，較無問題。至於無令狀的情況下，我國目前可作為對手機無令狀搜索的規定，有第 130 條附帶搜索、第 131 條 2 項緊急搜索及第 131 條之 1 同意搜索，其中，有學者提出對於手機搜索的同意，受搜索人可能會因為不清楚國家機關能夠取得多麼龐大的資料，而在不知道自己同

¹² 張叡文，檢視行動電話內數位資訊於我國及美國刑事偵查之合法性探討－以附帶搜索為中心，《軍法專刊》，2023 年 2 月，69 卷 1 期，174 頁。

¹³ 林鈺雄，註 9 書，頁 211-213。

意的「範圍」下同意搜索，對於人民權利保護不周¹⁴，但由於同意法理為基本權放棄，與本文所欲討論法律保留脈絡不同，且牽涉問題眾多，本文在此不處理。目前實務上對於無令狀搜索手機的爭議，集中在附帶搜索，即可否以附帶搜索搜索手機內部資訊？理由或許在於附帶搜索制度本身具有特殊目的，且為實務上常見的無令狀搜索方式，故本文以下將以附帶搜索為討論中心。

僅就條文文字觀察，第 130 條逕行搜索的範圍為身體及隨身攜帶的「物件」，而未如第 122 條有「電磁紀錄」，而如果將對於手機的搜索認為是「電磁紀錄」的話，將可能會得出附帶搜索不可搜索手機內容乃立法者有意選擇的結論。不過，我國刑事訴訟法關於搜索、扣押的規定，本就存在用語上的立法不周延：「物」、「物件」、「標的」等

混合著規定，彼此是否有差異不明，學說因此也有提出為了避免無所謂的爭議，有統一修正文字的必要¹⁵。因此，似乎並無法單以字面解讀並因此認為附帶搜索排除了手機內部資訊搜索。

目前學說及實務對於手機搜索均有採「二階段搜索」的概念，即是區分對於物理性載體的「載體標的」與數位的「資訊標的」的搜索，是兩個不同的搜索程序。合法控制了「載體標的」並不代表可以探查、保全內部的「資訊標的」¹⁶。白話一點的說，「找尋手機的物理性本體」與「搜索手機內部的數位證據」是兩個不同的搜索階段，應該分別觀察其合法性¹⁷。

目前多數見解皆認為附帶搜索僅可以搜索載體標的，而不可搜索資訊標的¹⁸。由附帶搜索的制度目的在保護執法人員安全及避免湮滅隨身證物觀察，

¹⁴ Applegate, *supra* note 2, at 293-294.

¹⁵ 施育傑，數位證據的載體、雲端與線上取證－搜索扣押與類型化的觀點，《月旦裁判時報》，2017年10月，64期，68頁。

¹⁶ 施育傑，註15文，頁60。李榮耕，註6文，頁1060。實務見解參考：臺灣高等法院臺南分院112年度上訴字第1355號刑事判決。

¹⁷ 在有票搜索的情況，會遇到的爭議是第一階段搜索（載體標的搜索）與第二階段搜索（資訊標的搜索）是否可以開在同一張搜索票？還是必須在取得載體標的之後，針對資訊標的的搜索另外向法院聲請核發搜索票？對此，實務見解認為若刑事訴訟法未就第二階段搜索票有特別規定，是故若第一階段所核發的搜索票法院核可範圍可認為包括資訊載體內的電磁紀錄，則無庸再行聲請法院針對第二階段搜索核發搜索令狀，參最高法院113年度台上字第3047號刑事判決、臺灣高等法院113年度上訴字第2531號刑事判決、臺灣新竹地方法院113年度金訴字第389號刑事判決。

¹⁸ 張叡文，註12文，頁177。法務部新聞，「搜索票已明確記載搜索內容 法務部：手機也



保護執法人員的部分，就算認為手機本身具有攻擊性，如可以做為敲擊工具，扣押手機本身即可以達到目的，至於手機內部的數位資料本身，無法對於執法人員的身體造成危害，美國法上針對附帶搜索的 Riley 案¹⁹，檢察官曾主張檢視手機內的資訊，可以間接保護警察安全，因為被逮捕人可能會以手機聯繫同夥前來支援，但法官以檢方無法證明曾經有這樣的前例發生而有未來防免的必要為理由，不予採納²⁰。至於避免湮滅隨身證據的面向，扣押手機本體可以防止被逮捕之被告當場刪除手機內資訊，因此似無立刻搜索手機內容的必要，只需要排除被告對手機本體的占有即可。不過，美國檢察官在 Riley 案所提出：為了避免手機裡的資訊被遠端清除或加密，有立刻查看、取得證據之必要。對

此，法官駁回意見認為：遠端刪除或加密僅為極端且有限的情況，又現行實務上，扣得手機的第一步驟，即是必須將手機與網路隔離，以保存手機當下的狀態，不論是美國警察常使用的、可以防止手機接收或送出任何訊息的「法拉第袋（Faraday bags）」²¹，或是直接將手機開啟飛航模式²²。由此觀察，避免湮滅隨身證據的目的，並不是一定要賦予警察可以附帶搜索手機內容才能達成，只需要取得手機本體即可。

除了上述理由之外，不允許附帶搜索手機內部資料，另一個原因就是手機所蘊含資訊量龐大²³，已超過附帶搜索制度所設想的容許範圍。在物理證據的思考下，警察逮捕被告，附帶搜索的範圍為被告「隨身可觸及之處所」，因為有物理範圍的事實上限制，附帶

可為成為搜索客體」，網址：<https://www.lawbank.com.tw/news/NewsContent.aspx?NID=121605>（最後瀏覽日：2024年11月27日）。以及雖在概念上未使用「載體標的」、「資訊標的」詞語，但同樣主張不得附帶搜索手機內所儲存的數位資訊，參曾財和，科技時代下之搜索新觀點—兼論附帶搜索行動電話內之數位證據，《法學叢刊》，2015年4月，238期，113頁，及相似意見認為應限縮手機內容附帶搜索的適用，僅限於不立即查閱手機，待證的犯罪證據恐遭變更、刪除或滅失，參黃惠婷，附帶搜索—評最高法院九十八年度臺上字第三一〇號，《刑事法雜誌》，2013年4月，57卷第2期，99-102頁。

¹⁹ Riley v. California, 573 U.S. 373 (2014).

²⁰ 張叡文，註12文，175頁。李榮耕，數位資料及附帶搜索—以行動電話內的資訊為例，《臺北大學法學論叢》，2016年2月，100期，頁273、274。

²¹ 李榮耕，註20文，275頁。張叡文，註12文，176頁。

²² 周昕緯、高佳豪，註3文，頁12。

²³ 李榮耕，註20文，頁276。

搜索所可能干預的隱私權也有限，因此以保護執法人員安全及避免湮滅隨身證據為理由，無令狀的侵害被告隱私權，還可以用「被逮捕後隱私期待的降低」（reduced expectations of privacy）的法理²⁴來說明並取得正當化基礎。然而在手機搜索的情況下，手機物理體積很小，其內卻可能蘊含極大量的數位化資訊，資訊內容更是可能包山包海，此並非附帶搜索制度設計時所設想得到的情況。又觀本法第 130 條附帶搜索的規定，事前由執行逮捕的執法人員（通常是警察）逕行發動，事後亦無需呈報檢察官或法官核可²⁵，是本法中門檻最低的搜索類型，不應容許搜索範圍擴及於手機內容的搜索，以避免過度侵害人民隱私權，此見解可資贊同。

最後一個問題是，國家是否可以主張要搜索手機內部，以判斷手機是否屬於可為證據之物而決定可否扣押手機本體？例如 Susteen 公司推出的 DataPilot 10 手持式數位採證儀，商品說明「使用者能在第一現場過濾取證手機的聯絡

人、通聯紀錄及簡訊等資料，並且保存必要採證資料，進行評估是否需要進一步送往採證實驗室。²⁶」必須先說明，此與學說上常在手機的附帶搜索脈絡下討論的「封閉容器理論」不同，封閉容器理論爭點在於：附帶搜索容許警察打開容器檢視，則對於手機內部資訊搜索是否也可以認為是對於封閉容器的搜索而在附帶搜索的容許範圍內？對此學說見解認為：第一，封閉容器的物理空間有限，但是手機所蘊含的資訊量，卻不受手機物理體積的限制；其次，真正的重點並不是手機是否可以類比為「封閉容器」，而是檢視手機內部資訊無法達到附帶搜索「保護執法人員安全」以及「避免湮滅隨身證據」的目的²⁷，因此又會回歸到上述的討論，並得到相同的否定結果。

而 DataPilot 10 手持式數位採證儀的問題，是可否主張必須要進行初步手機內部搜索，以此判斷手機本體有無得為證據之物的扣押事由？本文採取否定見解，理由同樣是基於保護手機內部

²⁴ United States v. Robinson, 414 U.S. 218 (1973) at 232.

²⁵ 未有如第 131 條 3 項事後呈報的規定，就算認為附帶搜索的扣押應可依照第 137 條 2 項準用事後呈報規定，也只能處理「有扣押物」的情況，但是如果有實行附帶搜索，卻沒有得到扣押物，即完全沒有事後呈報的規定。

²⁶ 碩文拓智慧科技股份有限公司 SWT Solutions Inc. 網頁產品資訊介紹。網址：<https://www.swtsolution.com.tw/products-article.aspx?id=133>（最後瀏覽日：2024 年 11 月 27 日）

²⁷ 張叡文，註 12 文，176、177 頁。



龐大隱私的目的，容許警察先瀏覽手機內部資訊，已造成人民基本權的極大干預，並且事實上也無法要求警察「忘記」已瀏覽過的資訊，對於人民的隱私侵害無法回復，也會完全違背將「載體標的」與「資訊標的」分為二階段搜索的目的。因此本文立場認為，只要是對於手機內部的檢視，都不在附帶搜索的授權範圍之內。此見解或許可能會因此使國家機關無法有效率的取得手機內的證據，惟此為保護隱私權下所必須忍受的成本²⁸。不過若是在執行手機本體扣押的階段，無可避免、非蓄意的接觸到手機儲存的資訊，例如在將手機調整成飛航模式的過程中，看到解鎖畫面上的未讀訊息內容，本文認為「調整為飛航模式」的行為本身，只是保全手機現在狀態的方式，不涉及資訊的撈取，並非刑事訴訟法上的搜索，而非蓄意見到未讀訊息，並非國家刻意打開手機頁面、打開 APP 尋找資料所取得，而為執行過程中的附帶干預，可以認為是在第一階段手機本體的搜索、扣押所取得的資訊。

結論上，附帶搜索僅得扣押手機本體，不能檢視手機內部資訊，如果要檢

視手機內部資訊，應另外檢討搜索發動的合法性。而此第二階段的搜索，仍是以有令狀搜索為原則，不過，美國法 Riley 案的法官，也並沒有排除如緊急搜索等無令狀搜索的適用可能性²⁹。在我國法的框架下，考量到第 131 條 2 項緊急搜索乃由檢察官發動，且有層報檢察長、三日內陳報法官的規定，發動要件較附帶搜索更完善，應可以肯定例外得以緊急搜索取代搜索票，惟如何避免實務運作上原則變例外的情況，仍是有待解決的問題。

二、搜索的範圍

討論完手機內部搜索的「開啟」後，接下來討論手機內部搜索的執行問題。此問題不管是在有票搜索或無票搜索的情況下都會出現，就算是有搜索票的情況下，搜索也必須在聲請案由的合理範圍內施行，才會具有正當性，對此，關於搜索票的記載，學說也曾存在爭議。有認為基於搜索具有高度不可預測性，故搜索票核發的容許範圍不必要求諸如鑑識軟體、方式或程式等，以免造成不必要的限制，不利搜索的彈性調整，而將重點放在法院的「事後審查」³⁰。惟另有學說批評認為，我國操作第 158 條

²⁸ 李榮耕，註 20 文，313 頁。

²⁹ Riley, 134 S.Ct. at 2486-87, 2494.

³⁰ 李榮耕，註 6 文，1097-1100 頁。

之 4 的結果，事實上極少證據被排除，事後審查模式「如同根本沒有審查」，對人民保障不足³¹。故仍應以「犯罪類型」、「犯罪時點」與證據可能存在之「檔案類型」做綜合觀察，正面得出應搜索之範圍，或是反面排除某些範圍不得搜索。以盡可能滿足搜索票特定明確原則之要求，但又不要求具體指明應搜索檔案為何、儲存何地，以保留搜索的動態彈性³²。

除了搜索票必須盡量記載明確之外，在合法的搜索中，如果看到未記載於搜索票上的本案得扣押之物或是另案得扣押物，以及無票搜索所發現的本案或另案得扣押物，可以依照本法第 137 條、第 152 條發動附帶扣押。在此說明，有學說提出第 137 條、第 152 條本質上都是附帶扣押³³，都是發現預期以外之物，只是依照偶然發現物為本案或他案證據區分。本文以下將以附帶扣押統稱。

為了避免「釣魚式」的搜索，附帶扣押必須限於「偶然發現物」³⁴，通常

以所謂「一目瞭然法則」限制偶然發現的範圍。而在手機內部資訊的搜索，應如何界定附帶扣押的範圍，有所爭議。

(一)學說見解

我國文獻上對於手機搜索附帶扣押的討論，主要是跟隨美國法的發展而來，主要分為三說³⁵：

1. 例主觀說

美國聯邦第十巡迴上訴法院 U.S. v. Carey 案³⁶，警方以毒品販賣案件取得對於電腦的搜索令狀，但最後警察在搜索時發現關於兒童色情的照片，並以此為證據起訴兒童色情相關罪名。關於這些兒童色情圖片的證據能力，檢察官主張是基於一目瞭然法則所合法取得的證據，有證據能力，但本案法官認為，警方在發現色情圖片後，便停止搜尋原本搜索票所要找的毒品案件證據，轉而開始尋找更多的色情圖片，這樣的行為已經超過搜索票容許範圍，為惡意令狀違反，應排除證據能力。

2. 重罪原則

此見解認為，手機鑑識屬於對隱私

³¹ 張叡文，註 12 文，179 頁。

³² 張叡文，註 12 文，179 頁。

³³ 林鈺雄，註 9 文，166 頁。

³⁴ 林鈺雄，《刑事訴訟法》上冊，自版，2024 年 9 月，13 版，454 頁。

³⁵ 以下整理參見李榮耕，註 6 文，1103-1107 頁。

³⁶ U.S. v. Carey, 172 F.3d 1268, 1273-1276 (10th Cir.1999).



的重大侵害，因此手機搜索中發現的另案證據，如果該他案屬於法定重罪，則有證據能力，反之則無。此說的優點在於判斷標準明確，法官只須審查該另案證據是否屬於法定重罪即可，不必爭論偵查人員主觀惡意與否，可以避免在手機搜索的情況下，難以用過去判斷執法官員是否惡意違反搜索票之「不得開啟比應扣押物小的空間或處所」標準來判斷手機搜索的合法性（因為資料本身為無形的數據，無所謂大小）。但缺點在會出現重罪的範圍被立法者不斷擴張，導致例外變原則、原則變例外的情況。我國有學者主張應採此說³⁷。

3. 一律排除說

此說主張應一律排除附帶扣押在手機搜索的適用，即不管以任何方式發現非屬本案之證據，一律無證據能力。此說雖然面臨認為此種作法過於極端的批評³⁸，但我國學者亦有基於一目瞭然法則在物理搜索時，目視範圍會受到物理上有形之限制，所以可以限制附帶扣押對於人民隱私權的侵害範圍，但此在手機搜索時卻無法達成；以及手機搜索的動作可在極短時間完成，在外觀上難以分辨先後順序，使得一目瞭然法則適用

困難為理由，主張應該採取一律排除說。³⁹

(二)我國實務見解：相當關連性

臺灣臺南地方法院 112 年度訴字第 111 號刑事判決案例事實：A 涉及與 B 的一件洩密案件（洩密案 1），檢察官合法取得搜索票後扣押 A 的手機，搜索手機時發現 A 與本件被告甲的 LINE 聊天紀錄中有涉及刑法第 132 條洩密罪的證據，因此以該證據起訴甲（洩密案 2）。甲之辯護人爭執證據能力，主張：檢方所取得的搜索票是針對洩密案 1 所核發，因此無權查看 A、甲之間的 LINE 通訊對話內容。本件搜索的「本案」（洩密案 1）與「他案」（洩密案 2）都是洩密案，都可以合理懷疑在 LINE 聊天室中可以找到證據，因此，本案爭點為：**搜索 LINE 時是否可以點開與本案無關的其他聊天室？**

本案一審判決認為無證據能力，理由為「查扣證人 A 之手機後，除非進一步點選手機內的 APP，進一步查閱相關通訊內容，否則無法看到本案被告甲與 A 的 LINE 對話內容；而關於數位採證所得之 A 的 LINE 通訊內容，所得到的只是 A 所有 LINE 通訊軟體的對話紀

³⁷ 李榮耕，註 6 文，1108 頁。

³⁸ Applegate, *supra* note 2, at 313.

³⁹ 張叡文，註 12 文，180-182 頁。

錄，除非進一步翻找查閱，否則無法找到被告甲與 A 之對話內容。是以，不管是直接在手機上或是數位採證後的紀錄，都無法簡單的一望即得被告甲與 A 之對話內容，在在都需要進一步點選查找，或是翻閱查找，即與上揭最高法院裁判意旨揭露之『另案扣押』之要件之一：『一目瞭然』法則不合。⁴⁰

然而上訴二審法院臺南高分院，二審法院對於證據能力之意見與一審法院相反，理由在於二審法院傳喚執行手機鑑識之偵查人員到庭詢問，得知手機搜索的實際操作過程中，將手機連上電腦後，手機內部資訊會在電腦上轉成一個個檔案，檔名的呈現無法直接看出內容，例如 112.07.456，需要點進去看才會知道內容為何，以 LINE 為例，也沒辦法呈現同一個檔案全部都是與某人相關。因此，二審判決認為，「在開啟電腦設備後，資訊以檔案方式儲存，偵查人員無法以視線所及方式，發現某檔案內所儲存之資訊是否即為嫌疑人涉案之相關證據，因此一目瞭然原則明顯無法適用於數位證據之搜索、扣押採證上」。雖然二審法院否定了一目瞭然原則在手機內部搜索的適用，但也認為必

須有一定的規範限制搜索的範圍，以避免在搜索目的之外，擴大或深化對受搜索人隱私的干預。故二審法院進一步傳喚訊問偵查人員後得知：目前手機內部搜索的方式，是採取輸入與犯罪事實相關的關鍵字、日期區間等方式查找，且可能必須在此過程中多次設定關鍵字、日期區間搜尋，漸漸縮小或擴大搜尋範圍，這是效率最高、成效最好的方式。二審法院因此提出一個可以在手機內部搜索領域取代一目瞭然原則的新原則：「相當關聯性」，只要搜尋方法與聲請時所敘明及法院據此審查而核發搜索票記載範圍具有相當關聯性，即屬合法搜索，而可扣押作為本案或另案之證據。因此在本案適用上，偵查人員輸入關鍵字為「資料、文件、銀行、書、多少錢、給我、LINE 給我、給你」等，並未偏離原審法院核發之搜索票所准許搜索、扣押範圍，只是因為本次搜索的本案（洩密案 1）與他案（洩密案 2）犯行具有高度相似性，而使得另案證據自然落入搜索關鍵字內，可認為是合法的另案扣押⁴¹。

(三) 本文見解

附帶扣押⁴²容許執法人員在執行合

⁴⁰ 臺灣臺南地方法院 112 年度訴字第 111 號刑事判決參照，為求便利，本文以代號取代真實姓名。

⁴¹ 臺灣高等法院臺南分院 112 年度上訴字第 1355 號刑事判決參照。

⁴² 包括本案附帶扣押、另案附帶扣押，相關說明參林鈺雄，註 34 書，453、454 頁。



法搜索時，如果看到得扣押之物，得予以扣押。這是因為此時搜索行為並未擴大或加深對受搜索人隱私權之干預，考量到此時對於搜索人權利之影響極輕微⁴³，又不應讓執法人員對於面前出現的證據或得沒收之物坐視不管，因而容許之無令狀扣押類型。一目瞭然原則，目的也是在圈出「執行合法搜索，未擴大或加深對受搜索人隱私干預」的附帶扣押合法前提要件。

手機內部搜索與傳統物理搜索同樣會出現無意間找到得扣押之物的情狀，一律排除說讓手機搜索完全無法主張附帶扣押，是完全否定上述基本法理，且造成物理搜索與手機內部搜索有不同的法律適用，應有正當性說理。重罪原則則被批評應該是屬於違法取證後第 158 條之 4 的證據能力衡量問題⁴⁴。此外，一目瞭然原則可以由基本權干預、附帶扣押容許性的法理推導得知，但主觀說、重罪原則及一律排除說均無法以任何法律解釋的方式由第 137 條、152 條中得知，故這三說實為立法論問題，無法直接適用在我國現行法。

除此之外，本文以為上述三說的真正問題，在於其對附帶扣押的處理邏輯並非以「限制搜索範圍」的角度出發，

如上述，一目瞭然原則之提出，在於圈出「執行合法搜索，未擴大或加深對受搜索人隱私干預」的附帶扣押合法前提要件，則當場景由物理搜索轉向手機內部搜索，因為資料儲存的方式沒有物理空間的概念，無法由資料夾看出內在空間範圍、打開資料前無法預測即將搜索的可能範圍，一目瞭然原則無法再發揮限制搜索範圍的功能，但附帶扣押的法理原則並未消失，此時處理邏輯應該是要找出其他可以取代一目瞭然法則、限制手機搜索範圍的新原則。

嘗試提出限制手機搜索範圍的新原則者，除了上述二審之臺南高分院外，細究 *U.S. v. Carey* 案，也可以找到類似的論述。雖然 *Carey* 案最後是以警察未先停止搜索並聲請新的搜索票，反而放棄原搜索目的，轉而搜索新發現案件的證據，惡意違反搜索票為由駁回證據能力，但是判決中法官也提到：警察所持的搜索票僅容許對於「文件」的搜索，因此不可以點開圖檔（JPEG.），這也是法官嘗試限制合法搜索範圍所提出的標準。然而，嘗試將此標準適用到上述我國實務案例中，就會發現 *Carey* 案的標準不夠精緻，因為洩密案 1 和洩密案 2 都存在 LINE 證據，都屬於「文件」，

⁴³ 張叡文，註 12 文，181 頁。

⁴⁴ 張叡文，註 12 文，182 頁。

Carey 案標準將使手機中所有的文件證據都在搜索範圍，並不合理。尤其是在當所涉案件情節輕微，卻出現證據可能以多種形式呈現的情況下，容許這樣的搜索行為，對人民隱私權侵害過大。

因此本文認為，上述臺南高分院揚棄一目瞭然原則，改以相當關連性原則以限縮搜索範圍的見解，是在理解現行手機搜索實務的情況下所做出的結論，且此標準所劃分的範圍，不僅可以處理同一類型檔案的搜索範圍，如本件要搜索 LINE 聊天室，可否打開與其他無關第三人的 LINE 聊天室（兩者都是文字類型的檔案），也可以處理某些案件證據可能以多種類型存在，導致搜索票記載內容看似容許搜索「所有」類型檔案的情況，應為目前最值得贊同的見解。

（四）相當關連性不足之處

然而，臺南高分院提出取代一目瞭然原則的相當關連性見解，雖然是一個較為合理的見解，但仍有其不足之處，主要體現在以下兩點：其一是「相當關聯性」之判斷標準可能在各法院之間產生歧義，本案例更一審判決對於本件因另案扣押而得之證據，採取無證據能力

之結論，理由在於：偵查人員採用「逐步擴大關鍵字」之偵查方法，無法將搜索範圍限制在原搜索票的特定對象，射程過於寬廣，極易尋得與本次搜索不相關之人之證據，而認為已經構成原搜索令狀所不容許的另一次搜索，而應另外取得搜索票始得為之⁴⁵。彰顯在同一案之中，對於「相當關聯性」的範圍，不同法官之間存在歧義，仍有待實務見解持續累積案例，發展穩定見解。不過，基於鑑識科學具有高度專業性及技術性，及數位證據容易存在以更改檔名、副檔名（如將 .jpg 更改為 .txt），或以變更輸入方式（以數字 0 代替英文字母 o）、將重要詞彙以暗語替代等方式規避關鍵字搜尋⁴⁶，本文認為法院不宜過度介入偵查人員依據個案所為的偵查判斷，若有爭議應傳喚偵查人員說明關鍵字與搜索案由之間的關聯性，並採取原則上尊重執法人員於個案判斷餘地之基本立場。

第二個不足之處在於，由於此見解僅在處理取證合法性的證據能力問題，因此若是在未扣押證據並呈現在法庭上的情況，相當關連性說則無法發揮限制

⁴⁵ 臺灣高等法院臺南分院 113 年度上更一字第 40 號刑事判決參照，此為本案最終事實審，上訴最高法院爭點與本文討論主題無關，本案已確定。

⁴⁶ 徐仕璋，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》，2013 年 1 月，13 期，35 頁、43 頁。



搜索的功能，例如，偵查人員輸入不具有相當關連性的關鍵字進行手機搜索，但剛好未找到他案證據。當然，此並非相當關連性所特有的問題，所有從證據能力出發的規範，包括物理世界搜索的一目瞭然原則，都會遇到同樣的問題，然而，在傳統物理世界的搜索，因為有搜索「在場」的規定⁴⁷，所以如果搜索人員在搜索過程中有違反一目瞭然原則的行為，例如找到標的物後又回頭釣魚式搜索，或是打開不該打開的櫃子，都可以及時被發現並依照刑事訴訟法第 416 條準抗告⁴⁸的規定提起救濟。但是在手機搜索的情況下，通常必須將手機本體帶回鑑識中心進行搜索，此不僅是因為鑑識設備無法輕易移動的問題，也因為鑑識過程以電腦分析資訊，有時可能會花費過長的時間⁴⁹，故無法滿足在場的規定，同時，也為了保障追訴成效、必須使國家擁有偵查階段的資訊優勢等理由，不宜將國家所掌握的設備、偵查技術公開，因此現實上也不宜讓當

事人可以在場監督鑑識過程。這樣的結果會使得受搜索人幾乎無法在檢方沒有提出搜索所得證據的情況下，自主的發現偵查執行過程中的瑕疵。再結合手機內部可能存放比物理空間更多、更隱私的資訊觀察，偵查執行過程不受監督，所可能導致的後果將是更嚴重，例如可以想像應該防止如下的違法搜索發生：偵查人員將手機鉅細靡遺的翻遍，目的不在取得當下可以扣押的證據，而是要發現其他潛在案件，並以此開啟其他案件的偵查，或是包裝違法所得的資料來源，以此聲請搜索票⁵⁰。此問題無法在現行法下進行有效防堵。

(五)未來展望

針對上述縱使採取相當關聯性原則，仍會出現無法有效監督搜索範圍合法性的問題，本文就此提出幾點可能的應對之道：

首先在搜索票的核發上，必須採取上述學說以「犯罪類型」、「犯罪時點」與證據可能存在之「檔案類型」綜合觀

⁴⁷ 參見刑事訴訟法第 148 條、第 149 條、第 150 條及第 42 條的規定。相關概念說明參林鈺雄，註 34 書，444-446 頁。

⁴⁸ 在此有第 416 條處分主體未包括警察，導致警察所為之處分無法救濟之爭議，應採取類推適用之見解以符合憲法有權利即有救濟之原則。相關說明參林鈺雄，註 9 書，137、138 頁。

⁴⁹ 例如需要以不停試錯的方式解開手機密碼。

⁵⁰ 搜索票的聲請僅為程序性事項，不適用嚴格證明原則，因此如果偵查人員將非法手機搜索所得證據以「線民來報」作為證據來源，也可能因此得到合法的搜索票。嚴格證明、自由證明概念參林鈺雄，註 34 書，513、514 頁。

察，盡量劃定搜索範圍的見解。惟以搜索票限制搜索範圍，固然是重要並且正確的思路，但此會與相當關連性說面臨同樣的問題，即是此等事前的限制，如果沒有有效的事後審查機制存在，可能也就只能淪於對於執法人員的良性勸說，無法發現並處理違法搜索範圍的問題。

另一種可能的方式則是要求偵查人員製作搜索紀錄⁵¹。在採取相當關聯性的基礎上，要求偵查人員紀錄搜索過程中所輸入的關鍵字，若未來對於搜索合法性有爭執，可提出報告以供事後審查之用。這當然會遇到若技術上只能以人力記錄，則只要偵查人員故意不記錄違法搜索情事，也很難會被發現，因此導致事實上的限制功能不彰的問題，但本文認為，要求記錄本身，即可使偵查人員有更高的自覺，提高違法搜索的成本，而可以在一定程度內發揮效用。

此外，除了上述規範面的選擇，也有學者提出可以借助科技發展的力量，一方面助力、一方面限制手機搜索的適用⁵²。行動設備鑑識工具（MDFTs）技術上可以整理、分析在手機中所撈到的

資訊，並整理成資料庫，或甚至製作圖表已如上述⁵³，因此，在科技的發展下，也可以利用 MDFTs 先識別手機中的圖片檔案並分類（例如可以分類出兒童色情或毒品、武器的圖片），或是篩選出有可疑對話的聊天紀錄，並以此劃定出偵查人員不得進入之「禁區」，如果再引入人工智慧作為輔助，分類可以更細緻、更精準。此外，也可以鼓勵或以法律要求 MDFTs 廠商設計出記錄偵查人員使用軌跡的功能，以此解決上述本文提出由偵查人員自己記錄，在偵查人員未如實記錄時，就無法發揮事後審查功能的弊病。或是更甚者，可以直接要求 MDFTs 只提供「非禁區」的資料庫供偵查人員搜索，以此斷絕違法超過搜索範圍的可能，然而，此時要面對的困難將會是，如果 MDFTs 在此部分的功能出錯，在圈出過大範圍的情況下，將會犧牲人民隱私權；在圈出過小範圍的情況下，將犧牲國家追訴利益。

另外也有學說主張，基於手機搜索對於隱私的高度侵害危險性，應將行動設備鑑識工具的使用限於特定犯罪類型才可以使用，例如暴力犯罪或列舉重

⁵¹ Applegate, *supra* note 2, at 309.

⁵² 以下整理參 Applegate, *supra* note 2, at 307-310.

⁵³ 本文貳。



罪⁵⁴。本文認為，在技術上及規範上無法有效監督偵查人員搜索範圍是否超過合法範圍的階段，以重罪原則限制手機搜索的發動的確可以一定程度保護人民隱私權，然而，此也同樣會遇到上述附帶扣押問題中對重罪原則的批評：可能因為列舉重罪的不斷擴張，喪失重罪原則對於國家的限制功能。另外在框列重罪的範圍時，也要考量到部分犯罪雖然犯罪情節並不嚴重，但證據往往必須透過手機才可以取得⁵⁵，而必須納入容許範圍。

最後則是有關資料刪除的規定，美國法學者主張應有保留期間的限制，最長不超過 6 個月。刑事訴訟法上的扣押，只是用以保全可為證據或得沒收之物的「暫時」占有⁵⁶，在證據扣押的情況下，當該扣押物完成證據目的後，則不可繼續扣押⁵⁷，並應將扣押物發還⁵⁸。在手機內部搜索的情況，因為手

機搜索技術必須留存手機本體，故扣押標的也為手機的物理性存在本身⁵⁹，而發還時的發還對象也為手機本體，故在此會產生國家可否複製、留存手機內檔案的問題。本文以為，若容許國家以任何形式留存透過手機搜索所得之資料，將有進一步侵害人民隱私權的風險，也已超過扣押目的，顯非扣押規定的授權範圍。故在立法論上應參考個人資料保護法及通保法上關於資料刪除、銷燬的規定⁶⁰，規範國家在目的達成後必須刪除由受搜索人手機內所得資料。

肆、結論

數位時代下，手機漸漸取代物理空間成為各種資料的儲存地，國家機關也開始面臨由手機中取證的技術面及法律面問題。目前，手機取證在技術層面上，已經可以撈取手機中儲存資料及

⁵⁴ Applegate, *supra* note 2, at 312.

⁵⁵ 例如詐騙集團的重要證據是對話紀錄，屬於已結束的通訊故無法以通訊監察方式取得，而現今大多通訊軟體公司不會留存使用者的通訊內容，故僅得由對話者之一方（被害人）自主提供，否則就必須透過手機搜索取得證據。

⁵⁶ 林鈺雄，註 34 書，452 頁。

⁵⁷ 林鈺雄，註 9 書，184 頁。

⁵⁸ 刑事訴訟法第 142 條。

⁵⁹ 此處可能因此扣押到非屬得為證據之物或得沒收之物而非得合法扣押之物，但學說上認為應容許之。李榮耕，註 6 文，1081、1082 頁。

⁶⁰ 個人資料保護法第 11 條、通訊保障及監察法第 18 條之 1。

進行整理、分析，並以資料庫的方式呈現。而在法律面上，我國目前並未針對手機另設特別規範，而是在過去搜索、扣押的框架下進行討論。本文首先由手機搜索的最前緣即手機本體的取得，以附帶搜索時發現手機可否扣押為例，說明必須實質判斷所發現的手機是否有得為證據之物或得沒收之物的合理懷疑，不可僅因為手機本身可以儲存多種潛在犯罪類型的證據，即以此單純的懷疑，在任何案件中，只要發現手機則一律扣押，侵害人民隱私權。

接著，本文確認手機鑑識屬於刑事訴訟法中的取證規定，並分析可能干預的基本權，結論上認為手機鑑識干預隱私權，為實質意義的搜索。

其次是關於手機內部的搜索，本文分為手機內部搜索的開啟、手機內部搜索的範圍兩層次進行討論。就手機內部搜索的開啟，爭點在附帶搜索的範圍是否包含對於手機內部的搜索，整理學說見解後，本文基於附帶搜索創設時所想像者乃是在保護執法人員人身安全、避免湮滅隨身證據的目的下，對於受拘捕人進行範圍有限的搜索，對於隱私權干預程度較輕微；然而在手機內部搜索的情況下，手機儲存空間遠大於手機的物理上體積，若容許搜索手機內部，對人民隱私權干預過大，且亦無助於上述附帶搜索目的之達成，故同意目前學說見

解認為，應區分為二階段搜索，對於手機本體的合法搜索、扣押，並不等於可以對手機內部資訊進行搜索、扣押，應另外判斷其合法性，並以有令狀為原則。

而在手機內部搜索的範圍，以搜索時的附帶扣押、是否適用一目瞭然原則為爭議中心。問題意識在於手機搜索中，沒有空間大小的概念，過去用來限制物理世界搜索合法性的一目瞭然原則，似無法直接套用在手機搜索。本文認為應以「限制搜索範圍」的角度出發，因此不贊同學說上所提出的主觀說、重罪原則及一律排除說，並認為我國實務上所提出的相當關連性原則，認為應以搜索時所輸入查找的關鍵字，是否與本案搜索票所載案由有相當關連性？來限制搜索的範圍，在此範圍內所得本案、另案證據，都可以作為扣押標的，應為目前符合實務操作、合理，而可以在手機搜索領域取代一目瞭然原則的標準。

最後，本文指出上述相當關連性說不足之處，在於只能處理違法搜索並且因此取得證據、並於法庭上主張使用的情況，若是違法搜索但未提出證據於法庭，則因為手機搜索通常無法踐行搜索在場的規定，因此不容易被發現，而造成違法搜索侵害人民隱私權。本文嘗試討論各種可能解決方式，結論上認為未



來可以要求偵查人員記錄搜索過程、或是以重罪原則限制此等侵害隱私權可能性重大的偵查手段的運用，以及吸納學者建議，期待未來科技發展下，手機鑑識工具可以協助偵查人員限制或分析手機內資訊，劃出偵查人員不得進入之禁區，或是自動記錄偵查人員搜索過程以供事後審查。

結論上本文認為，目前手機搜索以搜索、扣押規定處理，雖有部分不足之處，但大致上仍有透過解釋論解決的空間，至於是否要針對手機、電腦的數位取證另外設計規定，或創設新的基本權保護，是未來值得思考的問題。

參考文獻

一、中文文獻

(一)專書

1. 林鈺雄（2024），刑事訴訟法（上冊），13版。
2. 林鈺雄（2024），刑事訴訟法實例解析，6版。

(二)期刊論文

1. 王士帆（2016），〈網路之刑事追訴——科技與法律的較勁〉，《政大法學評論》第145期。
2. 李欣芳、楊中皇（2011），〈智慧型手機鑑識系統設計與實作——以Android平台為例〉，《全國資訊安

全會議》第21屆。

3. 李榮耕（2012），〈電磁紀錄的搜索及扣押〉，《臺大法學論叢》第41卷第3期。
4. 李榮耕（2016），〈數位資料及附帶搜索——以行動電話內的資訊為例〉，《臺北大學法學論叢》第100期。
5. 周昕緯、高佳豪（2016），〈手機取證系統運用於犯罪偵查之研究〉，《行政院海岸巡防署自行研究報告》。
6. 林宜隆（2012），〈建構數位證據鑑識標準作業程序（DEFSOP）與案例實證之研究〉，《司法新聲》第101期。
7. 林鈺雄（2023），〈司法警察（官）之身體檢查處分及其救濟〉，《月旦實務選評》第3卷8期。
8. 施育傑（2017），〈數位證據的載體、雲端與線上取證——搜索扣押與類型化的觀點〉，《月旦裁判時報》第64期。
9. 徐仕璋（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。
10. 張叡文（2023），〈檢視行動電話內數位資訊於我國及美國刑事偵查之合法性探討——以附帶搜索為中心〉，《軍法專刊第69卷》第1期。
11. 陳詰昌（2016），〈數位鑑識「原件不可變動原則」之適用——由行動裝置

鑑識與電腦鑑識差異探討》，《司法新聲》第 119 期。

12. 曾財和 (2015)，〈科技時代下之搜索新觀點－兼論附帶搜索行動電話內之數位證據〉，《法學叢刊》第 238 期。
13. 黃惠婷 (2013)，〈附帶搜索－評最高法院九十八年度臺上字第三一〇號〉，《刑事法雜誌》第 57 卷第 2 期。
14. 溫祖德 (2015)，〈行動電話內數位資訊與附帶搜索——以美國聯邦最高法院見解之變遷為主〉，《月旦法學雜誌》第 239 期。

(三) 網路資源

1. 法務部新聞 (2014)，「搜索票已明確記載搜索內容 法務部：手機也可為成為搜索客體」，<https://www.lawbank.com.tw/news/NewsContent.aspx?NID=121605>。
2. 碩文拓智慧科技股份有限公司 SWT Solutions Inc. 網頁產品資訊介紹，<https://www.swtsolution.com.tw/products-article.aspx?id=133>。

二、外文文獻

1. Taylor Applegate, Mobile Device Forensic Tools: A Help or a Hindrance to Constitutional Cellphone Searches?, 35 Stan. L. & Pol'y Rev. 284 (2024).