論建立涉嫌人使用 IP 資料庫之必要性暨在毒郵包案及證券交易法案之偵查應用

壹、前言

對偵辦案件的司法單位而言，資料庫被賦予能發掘案件及協助偵查之期待，故建立資料庫的概念，本局先前早已有方針並加以實施，惟實際成效仍待驗證。觀諸其他友軍單位，紛紛因應各自不同的權責及業務內容，發展出各自的獨有資料庫，例如警方查詢紀錄、海關查緝走私等相關資料庫，並確實在實務上發揮功能。本文試圖探討建立涉嫌人使用 IP 資料庫之必要性，以及建立該 IP 資料庫後，對實務上可能的助益；另外從中申論 VPN 服務實際上並不礙於 IP 資料庫建立目的和功能，甚至可能幫助司法單位在偵查犯罪一臂之力。

貳、蒐集 IP 之目的及必要性

一、目的

在網際網路的世界中，IP 位置為與真實使用者唯一的連結，使用者要使用網路服務，就必須透過電信業者（ISP）取得一組 IP[1]，並藉由該組 IP 實現網路上所有的指令，換言

[1] IPv4 因數量已不敷現代世界使用，逐漸都改為 IPv6 版本，但無礙建立涉嫌人 IP 資料庫目的。

之，IP 就是識別使用者在網際網路中一組代碼，因此在偵查實務上，會向電信業者調閱某段時間內使用該 IP 的申請者，以追查真實身分（若有埠號[2]）。故建立涉嫌人使用之 IP 資料庫，實際上就是記錄涉嫌人使用網際網路服務時的身分紀錄，可類比成記錄涉嫌人曾經使用過的車輛、住過的地址、使用過的帳戶等，在偵辦案件過程中，常常在資訊不足的狀況下，透過車輛、地點及帳戶等勾勒出犯罪組織的輪廓，故建立涉嫌人 IP 資料庫，目的在於標定曾經涉嫌犯罪的 IP，以在偵辦其他案件時，多一個資訊供承辦人連結相關性，換言之，即係對曾涉嫌犯罪行為的 IP 做上「標記」。

二、必要性

資料庫目的在於蒐集過去的資訊，從中加以歸納運用。偵辦案件過程中，每一個偵查行為一般是帶有明確目的性，查詢本身即是一種建立資訊的動作，此自警方的查詢系統可見一斑，警方將每一次的查詢留下紀錄，久而久之，該查詢紀錄成為警方辦案的獨有資料庫，並進一步將看似無關的身分證統一編號及車籍資料連結，倘若警方沒有將查詢結果儲存，就不會有如此豐富的資料庫。同理，本局偵辦案件時，

[2] 向電信業者調閱 IP 時，查得結果會是一堆相同的 IP 附加一組埠號（port），故尚需要埠號資訊，才有辦法清查真實使用者身分，此係清查申登人的必要之資訊，與建立資料庫較無關係。

只要有調閱 IP 紀錄，應可嘗試儲存起來，作為本局獨有的資料庫，例如調閱毒郵包的 IP，或是調閱股票下單的 IP 紀錄，將之儲存成資料庫，其必要性隨著近代所有犯罪與網路行為掛鉤而漸增，建立資料庫可能之運用在本文第四段再加以舉例說明。

參、VPN 對 IP 資料庫之影響

一、VPN 之作用

VPN 服務是可以隱匿真實 IP 的技術，即俗稱的跳板，藉由先連至其他伺服器再連結到真實目的地網址以隱匿原始 IP，原先目的是為能造訪阻擋特定國家的網路使用者，因此 VPN 服務的好壞指標之一是所能提供不同國家的 IP 數量，是一種需要花費金錢在其他國家架設伺服器的服務，即具有使用成本，較專業的駭客明白免費的 VPN 有更多資安風險，所以通常會願意付費購買 VPN 服務，但對於一般人來說，其實並沒有需要使用專業等級的 VPN 需求，所以若犯罪嫌疑人臨時想要隱匿自己的 IP，有很大可能都會選擇使用免費的 VPN。

二、VPN 並不影響資料庫建立之目的

附圖一所示，是熱心人士整理出較好用的 VPN 服務，其

中可看到需要付費的 VPN 國家數達 50 個至 100 個之間，伺服器數量（即能提供的 IP 數量）則約 3000 個至 5000 個，免費的 VPN 國家數及伺服器數量多約在 1 至 20 個，可觀察到伺服器數量付費與免費之間差 2 個數量級，即差百倍左右，雖然本文未統計所有免費 VPN 能提供的 IP 數量，但若假設大部分使用者都只使用免費 VPN 的情形，免費 VPN 提供的 IP 數量應並非龐大無法記錄及運用。具有惡意目的的犯罪嫌疑人，為規避司法單位追緝，若使用免費 VPN 服務，甚至可能有機會使用到被「標記」的 IP，換言之，犯罪嫌疑人進行犯罪行為時，為隱匿自己的真名，卻不慎使用到被司法單位「標記」的假名，如此一來，便可藉由資料庫發掘案件。

VPN	國家數	伺服器數	中資背景	最大連線數	網速	價格
NordVPN	59	5400+	非中資	6個裝置	快	US$3.71/月
ExpressVPN	94	3000+	非中資	5個裝置	更快	US$6.67/月
Surfshark VPN	65	3200+	非中資	不限數目	更快	US$2.21/月
Ivacy VPN	54	3500+	有中資	5個裝置	中等	US$1.00/月
Hotspot Shield	1	1	有中資	1個裝置	限速2M	免費
Windscribe	10	10+	有中資	不限數目	慢	免費
TunnelBear	23	23+	非中資	1個裝置	慢	免費

附圖一、110 年 VPN 推薦，網址：https://manage-money.com/vpn-recommend/，目前市面上 VPN 軟體共約一百個左右，估計免費提供的 IP 應約有上千個。

肆、偵查應用

一、毒郵包案

毒郵包在送達收件人之前，貨主或中間人可能會主動查詢郵包進度，若沒有透過 VPN 服務查詢，就會暴露查詢者的實際身分，因此實務上如附圖二，幾乎所有查詢毒郵包的 IP 紀錄（扣除司法單位的查詢紀錄），大部分 IP 都會來自其他國家，形成無法追查真實犯罪組織成員的斷點。假設涉嫌人在查詢毒郵包進度時為隱匿身分而使用 VPN，將會使得查詢毒郵包的 IP 紀錄有兩個特點：第一為幾乎全部查詢毒郵包的 IP 皆來自國外，第二為同一犯罪組織成員所查詢不同

毒郵包的 IP 或國家別有可能重複。

（一）第一個特點所能運用的偵查方式，就是當查詢某件寄至臺灣郵包的 IP 來源國家與實際寄送的寄件國家不同時，可推論該件包裹內應是有高度風險的違禁品。舉例而言，應該不太可能有一個身在美國的人要查詢一個自德國寄至臺灣的包裹進度，若發生這種情形，非常有可能是查詢者想要積極隱匿自己的身分，即該件寄至臺灣的包裹內藏有高度風險的違禁品。同理，因 VPN 使用者通常會將 IP 跳至國外，故若查詢得到的國外 IP 與寄件地相符，可合理推斷該 IP 是沒有經過 VPN，即有可能是真正的郵包賣家。

（二）第二個特點則是需要建立 IP 資料庫才能加以運用，即專門記錄查詢毒郵包的 IP。若涉嫌人等查詢毒郵包寄送進度，則一定會透過 VPN 隱匿自己的身分查詢包裹，因此，透過 VPN 連結到國外伺服器查詢包裹，則該件包裹可能就是毒郵包（若 P 則 Q，不一定若 Q 則 P，但 P 會包含在 Q 內）。因此認定某個 IP 是透過 VPN 所得到的 IP 就是關鍵工作，可藉由前開第一點的概念，只要是國外 IP 就有相當可能使用 VPN 服務（如

前述，可藉由寄送地加以限縮判斷），或是記錄查詢毒郵包的 IP，直接建立 IP 資料庫，將蒐集得到曾查詢毒郵包的 IP 交由物流業者反查，並模糊檢索條件，例如僅查詢 IP 的前兩個位元組，應可再找出其他毒品包裹。

陳ＯＯ	
147.78.122.44	歐洲-拉脫維亞
109.70.67.167	亞洲-斯里蘭卡
89.185.78.210	歐洲-斯洛伐克
45.85.82.29	歐洲-法國
178.171.54.231	亞洲-土耳其
178.171.91.116	歐洲-烏克蘭
216.74.102.25	歐洲-奧地利
92.240.206.189	北美-巴拿馬
45.73.171.209	北美-加拿大
184.174.59.206	歐洲-俄羅斯
158.46.171.193	亞洲-泰國
91.218.154.129	
88.214.3.134	
178.171.65.238	
184.174.32.137	亞洲-中國
213.182.199.200	歐洲-克羅埃西亞
158.115.242.161	
194.110.89.205	
104.227.178.22	
216.74.76.57	
181.245.4.107	
178.171.66.207	
185.15.179.132	
193.160.73.180	
67.227.110.246	
84.22.149.88	歐洲-俄羅斯
92.240.206.33	
216.74.109.113	
212.80.223.177	歐洲-艾爾蘭
193.31.72.32	亞洲-柬埔寨
178.171.117.236	
109.70.66.80	
178.171.44.248	
45.13.249.146	歐洲-西班牙
184.174.57.129	歐洲-俄羅斯
185.201.128.174	
92.240.200.218	
181.214.30.176	
10.8.6.179	

彭ＯＯ	
191.101.96.208	
216.74.76.31	
216.74.77.45	
178.171.67.222	
178.171.108.189	亞洲-喬治亞
178.171.64.235	
92.240.207.24	
158.46.168.246	亞洲-泰國
193.31.72.234	亞洲-柬埔寨
84.22.148.198	歐洲-俄羅斯
158.46.187.198	歐洲-立陶宛
207.230.121.219	
66.78.20.128	歐洲-瑞士
92.240.204.210	
92.240.206.251	
45.73.171.22	北美-加拿大
176.105.250.198	
193.31.72.125	
213.182.194.199	
157.119.40.100	
212.80.203.219	
92.240.206.200	
158.46.186.247	歐洲-立陶宛
191.101.213.16	
158.46.171.44	亞洲-泰國
66.78.36.8	亞洲-中國
176.105.251.220	
91.218.154.37	
178.171.46.251	
178.171.64.233	
178.171.45.231	
178.171.23.15	
178.171.52.129	
92.240.207.68	
212.80.220.238	歐洲-艾爾蘭
92.240.206.18	
156.0.103.68	
173.211.107.176	
212.80.200.97	

附圖二、二個毒郵包案自郵局回復查詢包裹 IP 資料，可觀察到兩個案例皆有 178.171.xxx.xxx、92.240.xxx.xxx、216.74.xxx.xxx、45.73.171.xxx、213.182.xxx.xxx、92.240.xxx.xxx、212.80.xxx.xxx、193.31.72.xxx 等國外 IP，推論此二個毒郵包曾使用同一個 VPN 服務查詢，甚至背後屬同一犯罪集團。

（三）綜上，以國外 IP 查詢包裹，可能係透過 VPN 查詢，故該包裹內夾藏違禁品可能性高，又因為同一運毒集團所使用之 VPN 軟體相同，故可能會經相同外國區域 IP 查詢，而全球 VPN 所能提供的 IP 數量如前述，免費版數量估計約為上千個，付費版可能也僅達數十萬個，故建立 VPN 所能提供的 IP 資料庫，做為發掘案件的參考應有其可行性。

二、證券交易法案

相較於毒郵包案，股票下單的 IP 紀錄就無法直接連結到不法行為，除 IP 來源可能為固網及行網外，非常規的交易亦可能夾藏在正常交易中，僅鎖定涉嫌人使用的 IP 恐無法推斷此 IP 所進行的交易都是違法行為。然而，固網的 IP 則會直接連結到涉嫌人住居所或習慣下單的場域，其中若是使用例如連鎖店、公司企業的 Wifi，則 IP 就應為固定不變，因此針對此種 IP 建檔有其積極意義：考慮涉嫌人被本局執行前，或執行後交保釋回，可能會在其習慣下單的場域進行其他的股票交易，此類 IP 可列為高風險交易者，換言之

，證交所或櫃買中心向券商調閱嫌疑人的交易 IP 紀錄，內容可能是夾雜固網及行網的 IP，相當雜亂且無法分析，但本局可加以清查後挑出固定的 IP 回饋給證交所及櫃買中心，列為警示 IP，協請證交所及櫃買中心加強觀察此類 IP 交易行為，或可再次發現不法情事。

伍、結語

建立涉嫌人使用的 IP 紀錄，可類比成記錄涉嫌人曾使用的犯案工具，可能是以自己名義申登，或以他人名義申登，然而都無礙於建立資料庫的目的，即這些曾做為犯案工具本身與犯罪行為雖無因果關係，但卻有高度相關，雖然涉嫌人犯罪曾使用的工具，未必一定會進行犯罪行為，但卻可做為查緝單位的參考依據，本文提出毒郵包及證交法兩種案例，闡釋建立涉嫌人 IP 資料庫的功能及可行性，在隨著各類犯罪行為都逐漸難與網路行為脫鉤的時代，建立涉嫌人使用 IP 之資料庫係可以審慎考慮的偵查作為。