臺灣警察專科學校警專學報，民國 110.12
第七卷第六期：25-48 頁

取得加密通訊內容因應對策
——從通訊監察技術觀點出發

The solutions to obtain the encrypted communication content from the technological perspective of communication surveillance

林國翔 * 沈士豪 ** 李鎮宇 ***
Kuo-Hsiang Lin Shih Hao Shen Chen-Yu Li

摘要

過去透過傳統偵查，或是通訊監察，常能有效查緝各式犯罪。然而，資通訊科技快速發展，不僅為人們生活帶來便利，也改變了犯罪的樣貌，犯罪者亦運用各項新興科技躲避執法機關偵查。如今，使用通訊軟體是當前最常見的通訊方式，其提供免費通話及訊息等功能，使犯罪者不再使用傳統通話及簡訊聯繫。這些主流通訊軟體多為外國公司提供，又具有加密機制，不若國內電信事業有依通訊保障及監察法有協助執行通訊監察的義務，造成當前國安及執法機關偵辦重大犯罪案件時的瓶頸─難以取得其加密通訊內容，執法機關對於運用新興科技的犯罪模式，必須有新的因應對策。本文從通訊監察的技術標準出發，探討取得加密通訊內容的限制因素，並由先進國家的各項因應作為，提出我國未來面對此問題之對策。

關鍵字：通訊監察、科技偵查、通訊軟體、加密

Abstract

In the past, law enforcement officers who used traditional investigation techniques and communications surveillance often conduct criminal investigation effectively. However, the rapid development of communication technology has not only brought convenience to people but also changed the appearance of crime cases.

Criminals have started to use various emerging communication technologies to

* 臺灣警察專科學校科技偵查科兼任教官。
** 臺灣警察專科學校科技偵查科兼任講師。
*** 中央警察大學交通學系兼任助理教授，通訊作者（電子郵件：cibduck@gmail.com）。

avoid the sight of law enforcement agencies. Using communication applications is currently the one of the most common methods.

These applications provide free voice/video calling and text/voice/multimedia messaging functions. These applications also operate worldwide via the Internet with encrypted communication mechanisms and they do not follow the local communications surveillance regulations. Criminals no longer need to use traditional telecommunication services. This is the bottleneck of the criminal investigation today. It has been hard for Global government and law enforcement agencies to find feasible solutions to respond.

This paper presents an overview of challenges to communications surveillance technologies and standards among communication industries. The potential solutions of obtaining the encrypted communication content and their applicability in real cases are reviewed and discussed. Finally, the future countermeasures and their research direction are highlighted.

Key words: Lawful interception, communication surveillance, technology crime investigation, communication applications, encryption

壹、前言

自 19 世紀電信業興起後，電話一直是主要的通訊方式，基於語音傳輸的電信服務依賴於電路交換網路，這種網路撥打電話時會建立一個連續性的電路，一個或多個交換機透過中繼線沿著線路上的路徑串接起來。當一方掛斷通話時，釋放的線路及交換機資源可用於其他通話請求（Wetherall & Tanenbaum, 2010）。

通訊監察是一種執法機關取得嫌疑人通訊內容的方式，最早是透過在電信業者的機房及用戶之間掛線來實施（Diffie & Landau, 2009），線路將語音訊號傳送到執法人員的耳機或錄音機，達成監聽犯罪嫌疑人的通話的目的。

90 年代行動電話服務大量普及後，導致執法機關難以再用掛線的方式執行通訊監察，為此有些國家頒布了新的通訊監察法規，如同美國的「執法通信協助法案（Communications Assistance for Law Enforcement Act, CALEA）」（Landau, 2005），藉由電信業者的配合，將通訊監察功能部署於其網路之中（“Communications Assistance for Law Enforcement Act,” n.d.），隨著網際網路日益興盛，相關國際標準

組織也為網路電話及其他運用網際網路的電信服務制定了新的通訊監察標準（*ATIS Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks*, 2006; *ETSI TS 102 232-1 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery,* 2017）。

雖然通訊監察的涵蓋範圍擴大後，對執法機關已有相當助益，但在網際網路的帶動下，通訊服務開始不再受限於由電信業者提供，各類新興通訊服務如雨後春筍般的出現，使得通訊監察在技術及實質功效上產生重大變化，各種電子郵件、社交網路、點對點通信、通訊軟體等，造成執法機關取得通訊內容的方式不再像過去一樣（Caproni, 2011）。

另一方面，各式功能強大的智慧型手機及平板電腦推陳出新，可以安裝各式通訊應用程式，有些裝置甚至具備專屬的通訊功能（例如：Apple 公司的 Facetime），逐漸改變了用戶行為及其與電信業者之間的關係，過去大多數的通訊服務由電信業者提供，如今已轉變由各式網際網路服務業者（例如：LINE、WeChat、WhatsApp 及 Skype 等）提供。

這些裝置及應用程式向全球各國提供服務，要求其依據各國法令規定，協助當地執法機關通訊監察有所困難，2019 年 10 月美國聯邦調查局局長瑞伊（Christopher Wray）在美國司法部所舉辦的合法接取會議（Department of Justice Lawful Access Summit）中指出，無法取得通訊軟體的通訊內容，已成為各執法機關反恐及偵查犯罪時的嚴峻挑戰（Wray, 2019），凸顯難以要求網際網路服務業者配合取得通訊內容的問題。

針對上述通訊監察所遭遇的挑戰，許多國家紛紛提出因應對策，近年來國內已有許多法律學者提出相關研究（王士帆，2016，2019；Zöller、王士帆，2019；李榮耕，2018；林鈺雄，2021；施育傑，2020），主要著重於科技偵查法律規範之探討。本文由通訊監察技術標準切入，分析當前在通訊監察標準及技術的條件下，取得加密通訊內容所遭遇之挑戰，並蒐集先進國家取得加密通訊內容之策略，並輔以實際案例研析，探討取得加密通訊內容的各種策略的可行性及尚待克服之困難，期拋磚引玉，提供未來相關研究的參考。

貳、通訊相關監察標準、運作方式及限制

為了符合不同國家法律、技術規範及成本考量，對於各種類型網路及服務實施通訊監察，已有許多國際標準組織建立針對不同的通訊網路及服務建立了監察標準，例如美國電信行業解決方案聯盟/電信行業協會（ATIS/TIA）、有線電視網路的纜線實驗室（CableLabs）、歐洲電信標準協會（ETSI）及第三代合作夥伴計畫（3GPP）等，表 1 列出不同標準組織所制定的重要通訊監察標準。

表 1　重要通訊監察標準

標準組織名稱	通訊監察標準名稱
美國電信行業解決方案聯盟 / 電信行業協會（ATIS/TIA）	Lawfully authorized electronic surveillance (J-STD-025A、J-STD-025B)
美國電信行業解決方案聯盟（ATIS）	Lawfully authorized electronic surveillance (LAES) for voice over packet technologies in wireline telecommunications networks (ATIS-1000678.b.v2.2010)
纜線實驗室（CableLabs）	Delivery function to collection function interface specification (PacketCable 2.0 PKT-SP-ES-DCI -C01)
歐洲電信標準協會（ETSI）	Lawful interception (LI); handover interface for the lawful interception of telecommunications traffic (TS 101 671) Lawful interception (LI); handover interface for the lawful interception of telecommunications traffic (ES 201 671) Lawful interception (LI); equirements of Law Enforcement Agencies (TS 101 331) Lawful interception (LI); ASN.1 object Identifiers in Lawful interception and retained data handling Specifications (TR 102 503) Lawful interception (LI); interception domain architecture for IP networks (TR 102 528) Lawful interception (LI); handover interface and service-specific details (SSD) for IP delivery series (TS 102 232-1~7)
第三代合作夥伴計畫（3GPP）	3G security; lawful interception requirements (TS 33.106) 3G security; lawful interception architecture and functions (TS.33.107) 3G security; handover interface for lawful interception (TS 33.108)

雖然通訊監察技術標準係由不同的組織所制定，但他們運作的方式確可以歸納成一個通用的架構（Hoffmann & Terplan, 2006）。一般而言，通訊監察有 3 個基

本功能，分別是接取（Access）、傳遞（Delivery）和收集（Collection）。接取功能通常是在業者網路內部，可能會由 1 個或多個監察功能所組成，負責監察特定通訊；傳遞功能用於將被監察的特定通訊傳送給收集功能，這個功能存在 2 個通道，內容通道及通訊相關資料通道，用於傳遞被監察的特定通訊內容及識別通訊相關資訊；收集功能，負責收集前述監察到的通訊內容及通訊身分識別資訊，提供執法機關運用，圖 1 為通用通訊監察架構。

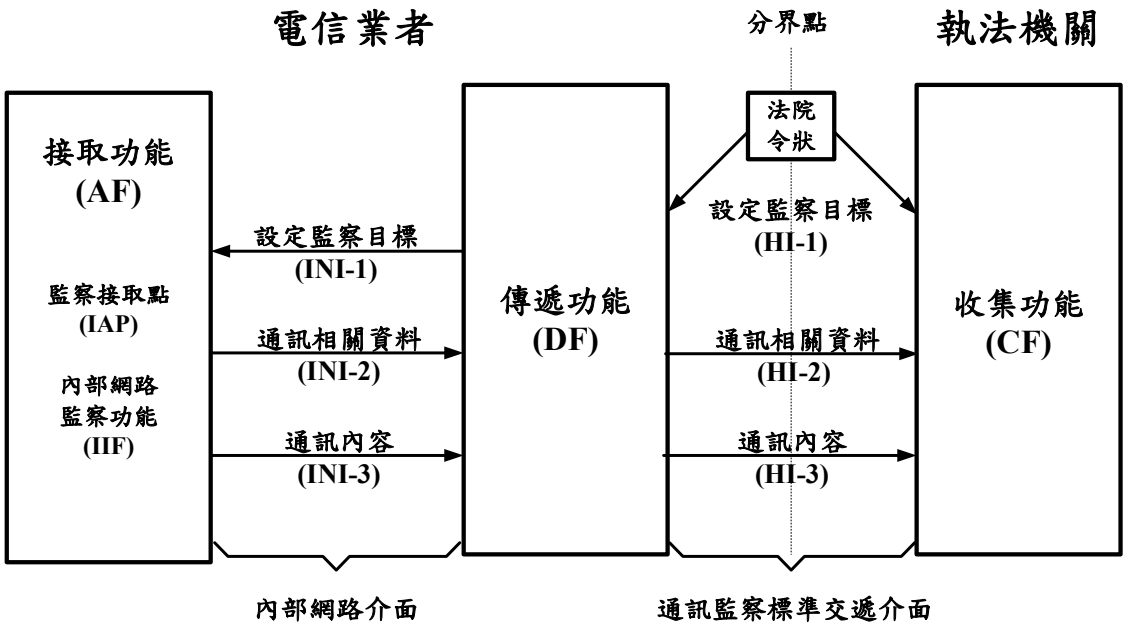

圖 1　通用通訊監察架構示意圖（Hoffmann &Terplan, 2006）

通訊監察運作流程可描述如（*Telecommunications security; Lawful Interception (LI); Requirements for network functions*, n.d.）：當授權機構（例如法院）向執法機構發出合法通訊監察的法院令狀時，執法機構將此令狀轉交給電信業者，該電信業者根據令狀所提供的資料，設定監察目標，電信業者其監察接取功能用於辨識監察目標及設定上線，完成設定後，該功能會通知執法機關已經完成上線。監察期間內，與監察目標有關的通訊內容及資訊需要透過傳遞功能分別送給執法機關，執法機關收到資料後，透過收集功能將通訊監察所得資料及監察目標進行關聯。

從通訊監察標準及架構可以發現，運用通訊監察取得通訊內容的方式，必須在電信業者的網路內部署通訊監察功能，仰賴電信業者的配合，面對當前犯罪嫌疑人大量使用網際網路通訊服務的情況，雖然透過通訊監察可以取得嫌疑人使用

網路通訊服務的封包資料，然而這些資料經過加密，執法機關無法破解獲悉其嫌疑人實際的通訊內容，這個問題已成為執法機關面臨的嚴峻挑戰，究其原因可歸納為以下幾點：

一、網路通訊服務提供者配合通訊監察可能性極低：由通訊監察的標準可以發現，執法機關得以順利執行通訊監察必須透過電信業者的配合，電信業者透過公眾電信網路提供電信服務，在法規上須配合執行通訊監察，然而網路通訊服務藉由網際網路運作，與電信業者自行設置之電信網路營運方式差異甚大，也不需要受到政府管轄，致執法機關難以要求其配合執行通訊監察；另一方面，如提供者配合執法機關通訊監察，恐造成客戶失去信賴而大量流失，故鮮少網路通訊服務提供者會放棄自身商業利益協助執法機關執行通訊監察。

二、網路通訊服務市場變化快速：以目前最常見的行動電話作業系統 Google Android 及 Apple iOS 系統為例，其應用程式下載平臺 Google Play 現在已有 314 萬個 Android 應用程式可供下載，Apple 的 App Store 則有 209 萬個 iOS 的應用程式可以下載（“App stores - Statistics & Facts,” 2021），而中國的應用程式商店中也有總計 350 萬個應用程式可以下載（“China: number of mobile apps available on app stores 2020,” 2021），提供網路通訊功能的各式應用程式不斷推陳出新，且改版迅速，縱使執法機關傾全力得以破解，也無法追上其更新速度。

三、網路通訊服務具有加密機制：基於網路及資訊安全，許多流行的通信應用（Corpuz, 2021）中都內建了加密機制，這些加密機制的強度足以對抗目前最快的電腦運算力，除非執法機關能取得加密的密鑰後加以破解。再者，很多設備本身也具備加密機制（“800 criminals arrested in biggest ever law enforcement operation against encrypted communication ,” 2021; “Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe,” 2020a; “New major interventions to block encrypted communications of criminal networks,” 2021a），更加深執法機關之困難。

四、網路通訊服務具匿名性：網路通訊服務通常只需要申請一個帳號，即可使用。不像電信服務，需向特定電信業者申請，並於申請時核對身分資料。另外，用戶一旦申請帳號後，可以使用 5G、Wi-Fi 或光纖上網，連接網路通訊服務，當執法機關偵查時，不易調取使用者資料及通信紀錄，進行後續追查。

參、取得加密通訊內容策略

一、策略類型

由於前述限制，許多國家開始著手研究執法機關取得加密通訊內容因應對策，而就協助執法機關取得通訊內容的對象來區分，可分為由網路通訊服務提供者協助、由電信業者協助及由執法機關自行取得等 3 種型態。

由網路通訊服務提供者協助部分，可分為配合執行通訊監察、提供解密後通訊內容及提供解密金鑰等 3 種策略。

（一）配合執行通訊監察：網路通訊服務提供者比照電信業者協助執行通訊監察的義務，在其通訊服務中建置通訊監察系統，執法機關可根據法院的令狀，據以針對嫌疑人執行通訊監察（Kravets, 2015）。

（二）提供解密後通訊內容：考慮網路通訊服務提供者建置通訊監察系統造成額外的成本負擔，當網路通訊服務提供者收到執法機關從法院取得的令狀時，提供嫌疑人於令狀所定期間的通訊內容（*Intelligence Committee Leaders Release Discussion Draft of Encryption Bill*, 2016）（"The Assistance and Access Act 2018," n.d.），2018 年美國釐清境外合法利用資料法（Clarifying Lawful Overseas Use of Data Act）也是類似之策略（朱翊瑄，2019）。

（三）提供解密金鑰：該解決方案也稱為「密鑰託管（Key escrow）」（"NIST Proposes Voluntary Federal Standard for Key Escrow Encryption," 1993）或「政府存取金鑰（Government access to keys, GAK）」（Koops, 1995）。基本概念是建立一個安全通信安全的密碼系統，並兼顧執法機關的偵查工作。執法機關可根據法院的令狀，從兩個獨立的密鑰託管機構獲取特定通訊的加密金鑰，藉以還原加密通訊內容。

電信業者協助策略部分，雖藉由在電信業者端執行通訊監察，無法取得解密後的網路通訊內容，但電信業者可以建置阻擋特定網路通訊服務設備，使特定網路通訊服務無法於該電信業者的網路內運作，當嫌疑人可能改使用電信業者所提供的電信服務，執法機關得以實施通訊監察，取得嫌疑人的通訊內容（劉文斌、孔懷瑞，2010）。

執法機關自行取得部分，係由執法機關自行開發或尋求合作夥伴取得特殊軟體或設備，透過在嫌疑人的手機、電腦或伺服器中安裝來取得他們的通訊內容。使用安裝軟體或設備的方式取得嫌疑人資訊並不是一個新方法，文獻顯示至少從

1998 年開始，外國執法機關就一直在使用此類方式來協助偵查（Quinlan & Wilson, 2016），但智慧型手機大量普及後，執法機關面對多樣且安全性日趨嚴格的裝置及網路通訊服務，使得運用這種偵查方法較過去更具有挑戰性。

表 2 整理了執法機關取得加密網路通訊服務內容的因應對策及他們的限制，在實際運作上，當執法機關尋求網路通訊服務提供者協助時，部分提供者雖對外表示其對執法機關有提供協助（"Guidelines for law enforcement," n.d.; "Information for Law Enforcement Authorities," n.d.; "Law Enforcement Guidelines Us," n.d.; "LINE responding to law enforcement agencies," n.d.; "Snap Law Enforcement," n.d.; "Tumblr Law Enforcement Guidelines," n.d.; "WeChat law enforcement data request guidelines," n.d.; "WhatsApp FAQ - Information for Law Enforcement Authorities," n.d.），但由於執法機關對這些提供者未必具備管轄權，因此這些提供者常無法符合其偵查需求。此外，在擄人勒贖、詐欺及販毒等案件急迫的情況，這些提供者的回應時間能否應對案件的急迫性也是一大問題（Hymas & Kirk, 2019; Karantzoulidis, 2018）。

表 2　執法機關取得加密網路通訊內容之因應對策

提供執法機關協助之對象	策略名稱	策略說明	所取得加密網路通訊內容之特性	實施方式及困難
網路通訊服務提供者	配合執行通訊監察	網路通訊服務提供者依循國際網際網路通訊監察標準	現在及未來	需針對提供者各別開發，數量眾多，且提供者基於商業考量配合意願低
	提供解密後通訊內容	網路通訊服務提供者依據執法機關取得之令狀提供通訊內容	過去已結束	需針對提供者各別開發，數量眾多，且提供者基於商業考量配合意願低
	提供解密金鑰	網路通訊服務提供者將特定對象特定通訊之金鑰先行提供執法機關	現在及未來 過去已結束 （依據所開發的軟體而定）	需針對提供者各別開發，數量眾多，且提供者基於商業考量配合意願低
電信業者	阻擋特定通訊	電信業者建置並運用相關網路設備阻擋特定對象之特定網路通訊服務通訊	無取得通訊內容（但可針對數種通訊服務同時實施）	需於境內所有電信業者建置骨幹網路建置相關設備，並需隨網路頻寬需求擴增設備數量

提供執法機關協助之對象	策略名稱	策略說明	所取得加密網路通訊內容之特性	實施方式及困難
執法機關自行開發或尋求合作夥伴取得	安裝軟體或設備	執法機關自行研發或提出需求向第三方合作夥伴採購監察或設備	現在及未來過去已結束（依據所開發的軟體或設備而定）	需針對各別提供者、裝置及主機等進行開發，數量眾多，但無需提供者協助

二、立法現況研析

前述章節本研究歸納了執法機關取得加密網路通訊內容之因應對策及困難，後續將研析數個先進國家執法機關取得加密通訊內容的立法情形，觀察相關策略在各國的實行現況，這裡主要關注相關國家執法機關自司法機關取得令狀後，要求提供者交付資料以外之因應對策，意即不討論利用一般搜索扣押取得提供者資料的方式。

（一）英國

設備干擾（Equipment interference）（Equipment Interference Code of Practice, 2018）是英國取得加密通訊內容的特殊偵查方式，執法及情報機關用設備干擾來獲取電腦、智慧手機或行動裝置等電子設備的通信、設備資料或其他相關資訊，其規範於調查權力法案（Investigatory Powers Act 2016）中，設備干擾可以包括許多不同的方式，例如惡意軟體、間諜軟體及鍵盤記錄器等，並涵蓋實體及遠端的干擾方式，達到從相關設備中存取通訊內容的目的。

（二）德國

德國目前針對取得加密通訊內容主要有 2 個法律規定：刑事訴訟法（StPO）、和聯邦刑事警察法（BKAG）。

1. 刑事訴訟法

德國刑事訴訟法中有來源端電信監察（Quellen-Telekommunikations berwachung）和線上搜索（Online-Durchsuchung）兩種取得加密通訊內容的偵查方式（Zöller、王士帆，2019）。來源端電信監察指的是由執法機關在被監察對象所使用的電腦或手機安裝特定軟體，該軟體在通訊加密之前

進行備份並傳送到執法機關，顧名思義，此通訊內容是自被監察對象端所取得，也就是在通訊一方電腦或手機上所取得。此處須注意使用來源端電信監察時，執法機關只能監視和記錄透過公共電信網絡的當前通信或內容，並僅能出於資料收集的目的進行必要和可逆的系統更改（Beuth & Biermann, 2017）。

另一種稱為線上搜索的方式，執法機關可以使用該技術，取得儲存在電腦的其他資料，此處則不限於通訊內容（Zöller、王士帆，2019）。

2. 聯邦刑事警察法

德國聯邦刑事警察法第 20k 條規定，授予聯邦刑事警察使用技術手段秘密存取資訊系統的權力（"§20k Verdeckter Eingriff in informationstechnische Systeme ," n.d.），允許其對相關系統進行遠端搜索。聯邦刑事警察為了追蹤嫌疑人在網路上的行為，可以收集保存或儲存該嫌疑人使用的電腦資料（包含雲端的資料）（"Bundesverfassungsgericht - Decisions - Constitutional complaints against the investigative Powers of the Federal Criminal Police Office for fighting international terrorism partially successful," 2016）。

（三）法國

法國刑事訴訟法（Code de proc durep nale）有規範執法機關獲取電腦資料的法律規定，特別是 2011 年 2011-267 號及 2016 之 201-731 號法律（LOI n° 2011-267 及 2016-731）增修案，其規定合法使用「從電腦中資料的擷取資訊（De la captation des donn esinformatiques）」，另外第 706-102-1 至 706-102-9 條亦有授權執法部門使用技術和工具來獲取通訊內容，其中第 706-102-1 條指出可在未經通訊方同意的情況下，在任何地方存取電腦中資料，並記錄、保存和傳輸這些儲存在電腦系統中的資料，在下一節實際案例（L'enquête EncroChat en France, n.d.）中，法國執法機關即依據本條規定安裝裝置並取得加密通訊內容。

（四）澳洲

1. 監視設備法（The Surveillance Devices Act 2004）

澳洲監視設備法規定了執法機關可以安裝及使用監視設備的授權、緊急授權及跟踪設備授權的法律程序（Surveillance Devices Act 2004 Annual Report 2019-20, 2020）。該法案有監視設備令狀（The surveillance device

warrant）及電腦存取令狀（The computer access warrant）。在監視設備令狀中，針對監視設備其中一個定義是任何能夠用於記錄或監控電腦訊息輸入或訊息輸出的設備或程式，這裡所稱之電腦則被定義為作為用於儲存或處理資訊的任何電子設備（包含智慧型手機或行動裝置）。監視設備令狀之中的資料監視設備，其包括用於記錄或監視電腦的輸入或輸出。

電腦存取令狀是為取得電腦所保存的資料的偵查方式，其中還包含必要時可增加、複製、刪除或更改目標或其他電腦的資料，或是監察電腦的通訊以取得相關犯罪證據。

2. 協助及存取法（The Assistance and Access Act 2018）

為因應有偵查價值的通訊內容都被加密，澳洲於 2018 年另外制定了協助及存取法，希望確保澳洲執法機關具備維護人民生命財產安全所需的偵查工具。該法案幫助執法機關獲取所需的證據及情報，除加強通訊及設備提供者與執法及安全機關合作機制外，並提高執法機關存取嫌疑人的電腦權限（“The Assistance and Access Act 2018,” n.d.），技術協助包含執法機關請求提供者自願協助、執法機關要求提供者提供技術協助（在提供者已有能力提供所需的幫助的前提下）及要求提供者開發新功能（提供商還無法提供此類協助的情況下），該法案還建立了新的電腦存取令狀（The computer access warrant），允許為調查嚴重犯罪秘密存取設備，同時隱藏該設備已被存取的情況（“Assistance and Access: Overview,” n.d.）。但澳洲政府一再重申所謂的協助並沒有允許在加密設備和通信系統中創建「系統弱點」或後門的協助，像是請求或要求相關提供者避免修復漏洞、建立解密能力，或降低其系統的安全性（“Assistance and Access: Overview,” n.d.）。

三、實際案例

前 2 節闡述了不同國家執法機關取得加密通訊內容的因應對策及相關法制，發現已有許多執法機關透過在嫌疑人的手機或電腦中安裝軟體或裝置來取得通訊內容，究其原因主要係執法機關與通訊服務提供者的合作上存在許多問題（“Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019,” 2019），使其成為許多國家採行的方案，近期已有實際案例出現，透過案例可以觀察，執法機關以安裝軟體或裝置之方式，來取得通訊內容的真實情況。

（一）法國執法機關破解 EncroChat 加密手機網路

2017 年起，法國憲兵隊及相關執法機關發現 EncroChat 的手機常被出現在組織犯罪集團案件的現場，由於該手機具有極佳的匿名特性，無法用 SIM 卡或設備關連到特定的對象，同時具有雙作業系統及無法被偵測的加密介面，該手機本身除了鏡頭、麥克風、GPS 和 USB 介面被移除外，也有遠端手機資料銷毀功能（“Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe,” 2020），在 2020 年初，EncroChat 已成為最大的加密通訊提供者之一，法國執法機關發現 EncroChat 用戶出現的熱門區域是許多毒品交易的來源國、目的國及洗錢中心，研判有極高比例的用戶可能將其用於從事犯罪。幸運的是，執法機關發現該公司位於法國的伺服器上，可安裝一種技術設備，用來取得用戶未加密的通訊內容（L’enquête EncroChat en France, n.d.）。

2020 年 7 月 2 日歐洲司法組織（EUROJUST）發布的新聞指出，運用上述方式所取得的通訊內容，法國及荷蘭警方才得以破獲跨國重大販毒及非法槍枝走私集團，查獲超過 10,000 公斤古柯鹼、70 公斤海洛因及 12,000 公斤大麻、1,500 公斤安非他命、19 個製毒工廠及各式非法槍械，在歐盟的其他國家像是挪威、英國及瑞典也有許多販毒及暴力犯罪嫌疑人被捕（“Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe,” 2020）。

（二）比利時及荷蘭執法機關破解 Sky ECC 加密電話網路

在法國及荷蘭警察等執法機關破解 EncroChat 加密電話網路後，犯罪組織轉投向新的加密電話供應商 Sky ECC，它是一個在加拿大及美國營運的公司，標榜自己是人們所能購買最安全的訊息傳送平台，該公司甚至對外提供 500 萬美金的獎金給任何能夠在 90 天之內破解的人。Sky ECC 提供用戶訊息自我銷毀、安全語音及加密保險庫外，還具備偽裝模式，也可以由常見手機改裝使用，當地執法機關研判全球有 17 萬人使用該工具，每天交換約 300 萬條訊息，而其中超過 20%的用戶位於比利時及荷蘭，執法機關發現這種電話在荷蘭安特衛普港附近使用最為廣泛，該港口是當地販毒的重要目的地（Goodwin, 2021; “New major interventions to block encrypted communications of criminal networks,” 2021）。

在歐洲刑警組織及司法組織的支持下，比利時、法國及荷蘭的司法及執法機關合作對 Sky ECC 通信服務工具的犯罪使用情況進行監控，透過對其網絡進行兩階段滲透：首先，執法機關監察儲存了來自 Sky ECC 網路的加密通信，並由專家研究如何將它們解密，隨後執法機關研究出能取得 Sky ECC 網路發送的即時通訊方式，至 2021 年 2 月時，相關執法機關已能夠監控 Sky ECC 約 70,000 個用戶的訊息，執法機關隨即於 3 月展開行動，首先比利時警方突襲了大約 200 個處所，逮捕 48 人，沒收 185 台採用 Sky ECC 加密的設備（Goodwin, 2021），並從運往安特衛普的貨物中，查獲 2,764 公斤古柯鹼（Thomson, 2021）；另外，荷蘭執法機關同步搜索 75 個處所並逮捕 30 人，找到 28 把非法槍械。

（三）綠光 / 特洛伊之盾（Greenlight / Trojan Shield）行動

有鑑於加密通訊屢受組織犯罪集團青睞，美國聯邦調查局與澳大利亞聯邦警察自 2019 年起開始密切合作，特別為組織犯罪集團開發並秘密經營了一家名為 ANOM 的加密設備公司，其標榜不論是全球各地組織犯罪、販毒和洗錢組織，ANOM 都能為其提供具犯罪所需功能的加密設備，由於 ANOM 功能上類似於前述的 EncroChat 及 Sky ECC，藉以說服犯罪組織轉而使用該設備。2020 年起由於 EncroChat 及 Sky ECC 相繼遭到執法機關瓦解，導致他們的客戶紛紛轉移到 ANOM，眼見時機成熟，16 個國家在 2021 年 6 月在開始進行了大規模執法行動，搜索 700 多個處所，逮捕 800 多人並查獲了 8,000 公斤古柯鹼、22,000 公斤大麻、2,000 公斤安非他命、250 支槍及超過 4,800 萬美元全球各種貨幣與加密貨幣，此外還瓦解了 50 個製毒工廠（“800 criminals arrested in biggest ever law enforcement operation against encrypted communication,” 2021）。

肆、未來研究方向

藉由分析取得加密通訊內容策略、法制及運用的實際案例，許多國家立法策略及執法機關的選項中，均有利用安裝軟體或裝置來取得加密通訊內容的方案，它類似於法務部科技偵查法草案所提出之設備端通訊監察，或許是我國未來應對此問題時的候選方案之一。然而，從外國運用的實際案例中進一步研究可以發現，利用安裝軟體來取得通訊內容，可能會衍生許多許多實務運行時需考慮之處，例

如，此種偵查手段對於隱私權可能造成之侵害，如何有效對其監督管理，提升人民及社會各界之信賴；另外，開發相關軟體或裝置需針對各別提供者、裝置及主機等進行開發，其數量極為眾多，執法機關應該如何整合產官學相關資源投入研發工作也應加以考量。

考量法律層面先前已有許多學者進行深入探討，故以下謹針對軟體設計及其系統運作機制、監督稽核機制及研發資源整提出後續可能的研究方向。

一、軟體設計及其系統運作機制

在通訊監察標準中，通訊雙方無法察覺是否被監察，且電信業者的通訊網路及其服務不會因為通訊監察而有所改變（Lawful Interception (LI); Requirements of Law Enforcement Agencies, 2017），但藉由安裝軟體取得通訊內容時，安裝的軟體會造成電腦、手機及相關系統改變，甚至可能造成相關系統異常、安全性被破壞等情況，有些警覺性較高的嫌疑人甚至可能透過防病毒軟體或鑑識工具及程式（“Chaos Computer Club analyzes government malware,” 2011; Marquis-Boire, Marczak, Guarnieri, & Scott-Railton, 2013）找到線索。另外，破解 EncroChat 電話網路後所取得的資料，在法院審理時遭到許多挑戰，像是取得的資料未遵循英國警察協會提出數位證據最佳實踐指南（Good Practice Guide for Digital Evidence）及取證時未符合 ISO 17205 測試實驗室標準等（Goodwin, 2021）。

以德國為例，其針對來源端通訊監察定有標準化服務描述（Standardisierende Leistungsbeschreibung, SLB），各項來源端通訊監察軟體須經過廣泛的測試程序並確定符合法律要求以及 SLB 後，才能提供使用，同時依據德國執法機關實際作業需求進行開發（“Quellen-TKÜ und Online-Durchsuchung,” n.d.），SLB 相關內容類似我國資訊委外採購案的建議書徵求說明書。

因此，執法機關對於所安裝的軟體的設計，應考量其對目標電腦、手機及相關系統的改變情況並確認是否影響系統正常運作、安裝後是否存衍生安全性問題、如何避免未經授權的人利用該軟體或衍生的安全性問題造成非法存取資料的情況、能否限制取得法院令狀所定範圍資料而不會超取、取得的資料如何能符合 ISO 27037 數位證據規範、具備資料回傳加密、隱藏、反鑑識及透過匿名網路傳輸資料等機制、是否能通過最新的防毒軟體及防火牆偵測等需求，據以制定相關規範。

二、監督稽核機制

監督機制可以分為 2 個部分，其一是軟體及其系統的認證測試及稽核機制，再者是執法機關實際運用時的稽核機制。

針對軟體及其系統的認證稽核機制部分，以德國來源端通訊監察軟體來說，須經過 5 道測試程序（Meister, 2018）：TÜV-IT 公司（TÜV Informationstechnik GmbH）的軟體測試（確認符合 SLB）、德國聯邦資訊安全局（BSI）的滲透測試、德國聯邦刑事調查局（BKA）的功能測試、德國聯邦刑事調查局（BKA）進行的系統測試及德國聯邦刑事調查局（BKA）採購驗收測試；而先前破解 EncroChat 的案例中，法國宣布其所使用的技術為「軍事國家機密」（Goodwin, 2021），不願對外揭露技術細節，如我國考慮對安裝監察軟體的偵查方式進行立法，如何在兼顧人權、透明及國家安全的前提下，提出讓人民及社會可信賴的監察軟體驗證機制，是一項極為重要的課題（“Judgment in investigatory powers legal challenge,” 2019）。

另一方面，在執法機關實際運用的稽核機制部分，除考慮納入既有通訊監察稽核機制（例如現地稽核及電子監督設備稽核等）外，亦可考慮建立單純提供軟硬體設備而未接觸通訊內容機關，其運作機制可參照現有通訊監察標準及運作機制進行修改，例如一般電信監察與設備端通訊監察概念上的差異，可以想像成將電信業者網路的內部監察功能（IIF）延伸至被監察對象的裝置上（如圖 2），而通訊監察執行的流程，亦可參考既有電信監察執行流程設計（如圖 3 及表 3），降低外界對此偵查方法之疑慮。

三、研發資源整合

如同 EncroChat、Sky ECC 及 ANOM 一樣，市面有各式各樣的設備及通訊工具可供消費者選擇。執法機關需要為不同的設備及工具則要開發相對應的軟體或系統，這意味著開發的成本相當高昂，除此之外，設備的操作系統及通訊軟體的頻繁更新，也增加了開發困難及額外成本，在 EncroChat 的實際案例中（L’enquête EncroChat en France, n.d.），除法國國家憲兵刑事研究所（The Institute for Criminal Research of the National Gendarmerie, IRCGN）是研究是開發相關技術設備的關鍵外，其與法國國家憲兵鑑識實驗室（Forensic Laboratory of the Gendarmerie）、荷蘭鑑識研究所（the Netherlands Forensic Institute）及都柏林大學（University College of Dublin）組成的破密及研究解除系統保護因應兒童剝削（CERBERUS）計畫，旨

在透過開發及實現歐洲解密平臺，藉以阻止包括恐怖分子、政治極端分子、毒販在內的犯罪集團和性剝削犯罪組織，該計畫從 2019 年至 2021 年共投入 230 萬歐元（“Judgment in investigatory powers legal challenge,” 2019）；另外以德國為例，德國執法機關已投入 600 萬歐元設計 2 個監察軟體（Meister, 2018），我國未來考慮立法授權運用安裝軟體取得通訊內容時，亦可借鏡先進國家如何整合相關資源。

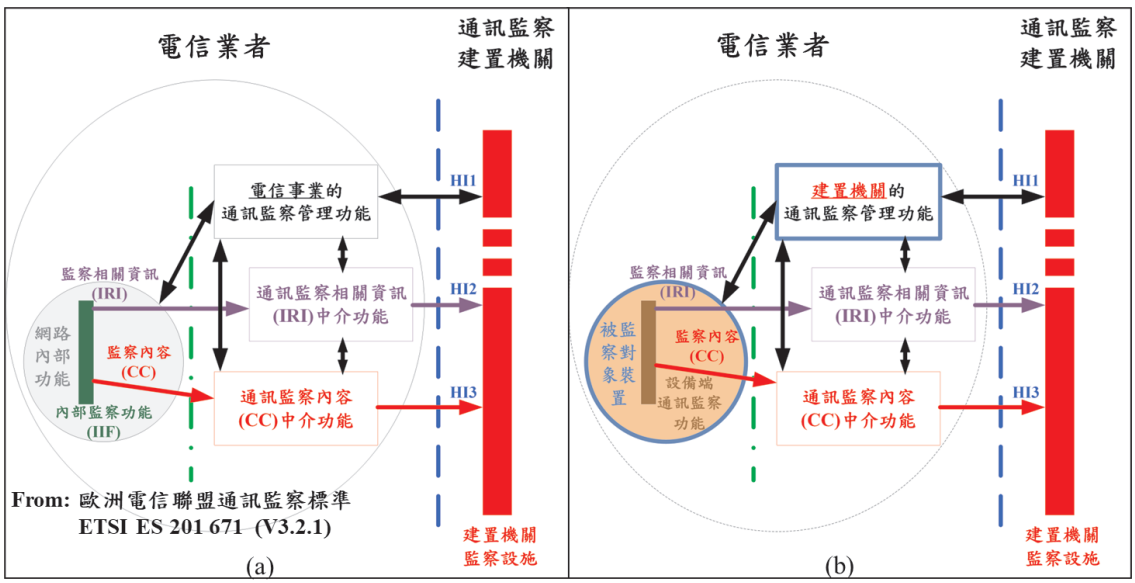

圖 2　(a) 國內通訊監察所採用之歐洲電信聯盟通訊監察標準架構；(b) 設備端通訊監察可能採行的概念性架構

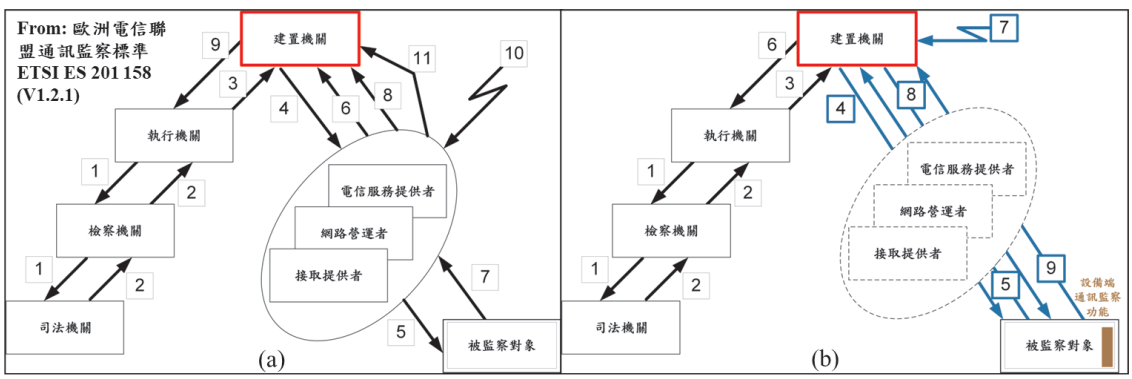

圖 3　(a) 國內通訊監察所採用之歐洲電信聯盟執行通訊監察流程示意圖；(b) 設備端通訊監察可能採行的執行通訊監察流程示意圖

表 3　電信監察與設備端通訊監察執行流程比較

流程	現有通訊監察執行步驟	流程	設備端通訊監察可能執行步驟
1	執行機關向檢察及司法機關聲請核發通訊監察書	1	執行機關向檢察及司法機關聲請核發通訊監察書
2	司法機關核發通訊監察書	2	司法機關核發通訊監察書
3	執行機關將通訊監察書傳遞給建置機關	3	執行機關將通訊監察書傳遞給建置機關
4	建置機關於電信事業監察設施設定目標身分（常見為電話號碼）	4	建置機關於目標裝置設定裝置端通訊監察功能
5	電信事業監察設施根據令狀中的資訊確定相關的目標身分	5	目標裝置的裝置端通訊監察功能回覆建置機關已收到指令並完成設定，並將監察所得資料從目標裝置傳遞到建置機關，並燒錄通訊監察所得資料光碟
6	電信事業回覆建置機關已收到通訊監察書並完成設定		（相關步驟於流程 5 已完成）
7	監察所得資料從目標端傳遞到電信事業		
8	監察所得資料從電信業者傳遞到建置機關監察設施，並燒錄通訊監察所得資料光碟		
9	建置機關向提供執行機關通訊監察所得資料	6	建置機關向提供執行機關通訊監察所得資料
10	根據司法、檢察或執行機關的要求或當通訊監察書授權期限屆滿時，電信事業停止監察	7	根據司法、檢察或執行機關的要求或當通訊監察書授權期限屆滿時，建置機關停止監察
11	電信事業停止監察	8	建置機關停止監察

伍、結論

在維護隱私並兼顧國家安全的前提下取得加密通訊內容，不論在外國及國內都是一個存在激烈辯論公共政策議題。政府機關表示他們被迫使用先進的監察軟體、設備或系統的來保護國家及人民安全，然而人權團體及非政府組織強烈反對執法機關這些偵查作為，他們認為執法機關使用的偵查方法和技術具侵略性，會損害隱私權及通訊安全。

本文從通訊監察技術觀點出發，探討取得加密通訊內容因應對策，首先簡要介紹了通訊監察的現狀及限制對執法機關所造成的困境後，再從策略類型、法制現況及實際運用案例，分析先進國家取得加密通訊內容的策略，考量網際網路服務提供者的配合情況，先進國家已開始採取安裝監察軟體的策略用於取得加密通訊內容，其似為我國未來考慮的立法及偵查發展方向。然而，如何讓人民及社會信任此種監察方式至關重要，本文針對應用該方法時軟體及其系統運作、監督稽核機制及資源整合等機制等研究方向進行探討，期為未來規劃相關制度規範時提供參考，俾利保障人民隱私權及秘密通訊自由不受非法侵害，並達到維護社會治安之目標。

參考資料

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（145）：339-390

Mark A. Zöller、王士帆（2019）。來源端電信監察與線上搜索——德國刑事追訴機關之新手段。司法新聲（130）：106-123

王士帆（2019）。當科技偵查駭入語音助理——刑事訴訟準備好了嗎？。臺北大學法學論叢（112）：191-242

朱翊瑄（2019）。美國《雲端法》（CLOUD Act）。資策會科技法律研究所。取自：https://stli.iii.org.tw/article-detail.aspx?no=67&tp=5&d=8291

李榮耕（2018）。初探遠端電腦搜索。東吳法律學報（29）：49-83

林鈺雄（2021）。科技偵查概論（上）——干預屬性及授權基礎。月旦法學教室（220）：46-57

林鈺雄（2021）。科技偵查概論（下）——干預屬性及授權基礎。月旦法學教室（221）：42-52

施育傑（2020）。科技時代的偵查干預處分——兼論我國法方向。月旦法學雜誌（306）：154-174

劉文斌、孔懷瑞（2010）。中共網際網路控制作為研析。展望與探索（8）：24-49

§ 20k Verdeckter Eingriff in informationstechnische Systeme. (n.d.). Retrieved February 16, 2018, from https://www.gesetze-im-internet.de/bkag_1997/20k.html

800 criminals arrested in biggest ever law enforcement operation against encrypted

communication. (2021, June 8). Retrieved July4, 2021, from EUROPOL website: https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

800 criminals arrested in biggest ever law enforcement operation against encrypted communication . (2021, June 8). Retrieved July3, 2021, from EUROPOL website: https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

App stores - Statistics & Facts. (2021). Retrieved July3, 2021, from https://www.statista.com/topics/1729/app-stores/#topicHeader__wrapper

Assistance and Access: Overview. (n.d.). Retrieved July3, 2021, from The Department of Home Affairs website: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-overview

ATIS Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks (No. ATIS Standard PP-1000678.2006). (2006). ATIS Standard ATIS-PP-1000678.2006.

Bundesverfassungsgericht - Decisions - Constitutional complaints against the investigative Powers of the Federal Criminal Police Office for fighting international terrorism partially successful. (2016, April 20). Retrieved February16, 2018, from Bundesverfassungsgericht website: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1bvr096609en.html

Caproni, V. (2011). *FBI — Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*. Retrieved from https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

Chaos Computer Club analyzes government malware. (2011, October 8). Retrieved February24, 2018, from Chaos Computer Club website: https://ccc.de/en/updates/2011/staatstrojaner

China: number of mobile apps available on app stores 2020. (2021). Retrieved July3, 2021, from https://www.statista.com/statistics/1058715/china-mobile-applications-available-app-stores/

Communications Assistance for Law Enforcement Act. (n.d.). Retrieved December27, 2017, from The Federal Communications Commission website: https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

Corpuz, J. (2021, May 17). The best encrypted messaging apps in 2021. Retrieved July3, 2021, from tom's guidewebsite: https://www.tomsguide.com/reference/best-encrypted-messaging-apps

David J. Wetherall, &Andrew S. Tanenbaum. (2010). *Computer Networks* (5th ed.). Retrieved from https://www.oreilly.com/library/view/computer-networks-fifth/9780133485936/

Diffie, W., &Landau, S. (2009). Communications surveillance : Privacy and security at Risk. *Communications of the ACM*, *52*, 42–47. https://doi.org/10.1145/1592761.1592776

Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. (2020a, July 2). Retrieved July3, 2021, from EUROJUST website: https://www.eurojust.europa.eu/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. (2020b, July 2). Retrieved July4, 2021, from EUROJUST website: https://www.eurojust.europa.eu/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

Equipment Interference Code of Practice. (2018). Retrieved from http://www.gov.uk/government/collections/investigatory-powers-bill

ETSI TS 102 232-1 Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery,.

(2017). ETSI TS 102 232-1.

Goodwin, B. (2021a, March 10). Police crack world's largest cryptophone network as criminals swap EncroChat for Sky ECC. Retrieved July4, 2021, from ComputerWeekly.com website: https://www.computerweekly.com/news/252497565/Police-crack-worlds-largest-cryptophone-network-as-criminals-swap-EncroChat-for-Sky-NCC

Goodwin, B. (2021b, March 29). UK courts face evidence 'black hole' over police EncroChat mass hacking. Retrieved July4, 2021, from ComputerWeekly.com website: https://www.computerweekly.com/news/252498544/UK-courts-face-evidence-black-hole-over-police-EncroChat-mass-hacking

Guidelines for law enforcement. (n.d.). Retrieved August2, 2018, from Twitter website: https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support

Hoffmann, P., &Terplan, K. (2006). *Intelligence support systems : technologies for lawful intercepts*. Auerbach Publications.

Hymas, C., &Kirk, A. (2019, January 13). Crime victims wait half an hour for police to respond to 999 calls as response times double. *Telegraph*. Retrieved from https://www.telegraph.co.uk/news/2019/01/13/crime-victims-wait-half-hour-police-respond-999-calls-response/

Information for Law Enforcement Authorities. (n.d.). Retrieved August2, 2018, from Facebook website: https://www.facebook.com/safety/groups/law/guidelines/

Intelligence Committee Leaders Release Discussion Draft of Encryption Bill. (2016, April 13). Retrieved from https://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649

Joint meeting of Five Country Ministerial and quintet of Attorneys-General: communiqué, London 2019. (2019, October 23). Retrieved July4, 2021, from GOV.UK website: https://www.gov.uk/government/publications/five-country-ministerial-communique/joint-meeting-of-five-country-ministerial-and-quintet-of-attorneys-general-communique-london-2019

Judgment in investigatory powers legal challenge. (2019, July 29). Retrieved July4, 2021, from The Home Office website: https://homeofficemedia.blog.gov.uk/2019/07/29/judgment-in-investigatory-powers-legal-challenge/

Karantzoulidis, S. (2018, November 20). The Best and Worst Police Response Times of 10 Major U.S. Cities. *Security Sales & Integration*. Retrieved from https://www.securitysales.com/news/best-worst-police-response-times/

Koops, B.-J. (1995, July). Crypto Law Survey. Retrieved from ftp://ftp.cerias.purdue.edu/pub/doc/cryptography/Crypto_Law_Survey/CryptoLawSurvey.html

Kravets, D. (2015, January 13). UK prime minister wants backdoors into messaging apps or he'll ban them. *Ars Technica*. Retrieved from https://arstechnica.com/tech-policy/2015/01/uk-prime-minister-wants-backdoors-into-messaging-apps-or-hell-ban-them/

L'enquête EncroChat en France. (n.d.).

Landau, S. (2005). CALEA and Network Security: Security, wiretapping, and the Internet. *IEEE Security & Privacy*, *52*(11), 26–33. Retrieved from http://ieeexplore.ieee.org/document/1556533/

Law Enforcement Guidelines Us. (n.d.). Retrieved January11, 2018, from https://www.documentcloud.org/documents/4254995-Law-Enforcement-Guidelines-Us.html#document/p10/a3

Lawful Interception (LI); Requirements of Law Enforcement Agencies. (2017). Retrieved from http://www.etsi.org/standards-search

LINE responding to law enforcement agencies. (n.d.). Retrieved December10, 2019, from https://linecorp.com/en/security/article/35

Marquis-Boire, M., Marczak, B., Guarnieri, C., &Scott-Railton, J. (2013, March 13). You Only Click Twice: FinFisher's Global Proliferation - Citizen Lab. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Meister, A. (2018, June 26). Geheime Dokumente: Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen. Retrieved July4, 2021, from Netzpolitik.org

website: https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/

New major interventions to block encrypted communications of criminal networks. (2021a, March 10). Retrieved July3, 2021, from EUROPOL website: https://www.europol.europa.eu/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

New major interventions to block encrypted communications of criminal networks. (2021b, March 10). Retrieved July4, 2021, from EUROPOL website: https://www.europol.europa.eu/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

NIST Proposes Voluntary Federal Standard for Key Escrow Encryption. (1993, July 29). *NIST*. Retrieved from https://www.nist.gov/news-events/news/1993/07/nist-proposes-voluntary-federal-standard-key-escrow-encryption

Quellen-TKÜ und Online-Durchsuchung. (n.d.). Retrieved July4, 2021, from Bundeskriminalamt website: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html

Quinlan, S., &Wilson, A. (2016, September). A brief history of law enforcement hacking in the United States. Retrieved December30, 2017, from New Ameirca website: https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf

Snap Law Enforcement. (n.d.). Retrieved December10, 2019, from https://www.snap.com/en-US/safety/safety-enforcement

Surveillance Devices Act 2004 Annual Report 2019-20. (2020). Retrieved from https://www.pmc.gov.au/government/commonwealth-coat-arms.

Telecommunications security; Lawful Interception (LI); Requirements for network functions. (n.d.).

The Assistance and Access Act 2018. (n.d.). Retrieved July3, 2021, from The Department of Home Affairs website:

https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

Thomson, I. (2021, April 8). Belgian police seize 28 tons of cocaine after “cracking” Sky ECC’s chat app encryption. Retrieved July4, 2021, from The Register website: https://www.theregister.com/2021/04/08/sky_ecc_drugs/

Tumblr Law Enforcement Guidelines. (n.d.). Retrieved August2, 2018, from Tumblr website: https://www.tumblr.com/docs/en/law_enforcement

VonPatrick Beuth, &Kai Biermann. (2017, June 23). Staatstrojaner: Dein trojanischer Freund und Helfer. *Zeit*. Retrieved from http://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss

WeChat law enforcement data request guidelines. (n.d.). Retrieved December10, 2019, from https://www.wechat.com/en/law_enforcement_data_request.html

WhatsApp FAQ - Information for Law Enforcement Authorities. (n.d.). Retrieved August2, 2018, from WhatsApp website: https://faq.whatsapp.com/en/26000050/?category=5245250

Wray, C. (2019, October 4). Finding a Way Forward on Lawful Access: Bringing Child Predators out of the Shadows. Retrieved July2, 2021, from https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access