數位監管的未來——論國家安全攔截法規之制定

◆ 臺灣警察專科學校兼任講師 — 蕭國振

合法攔截（Legal Interception, LI）係指在法律授權的前提下，執法機構對個人或犯罪組織的通訊進行監控和存取的行為。在毒品販運、詐欺、走私等犯罪的高度威脅下，國家安全與公民隱私的保護該如何平衡？

合法攔截的定義

網路資訊發達，使得國際恐怖組織獲得極具隱匿性通訊方式，威脅危害加乘倍增。歐洲電信標準協會（European Telecommunications Standards Institute, ETSI）於 1995 年針對合法攔截制定技術規範和標準，[1] 藉以維護國境安全及防治犯罪的治理責任。各國在保障國家利益的同時，應運制訂相關法律予以規範執法機構（Law Enforcement Agency, LEA），惟仍對人民隱私權展現相程度的尊重，確保攔截所獲方式符合比例原則，不會超出必要範圍，並規範後續所獲得資料的處理和使用，需符合法律規範和道德標準。簡言之，合法攔截雖為基於國家治權干預私人通訊存取的執法行為，但儼然成為國家安全不可或缺的一環。

隨著科技的進步，攔截信息的範圍亦逐漸廣泛，從單純電話線路的語音通訊和文字信息，發展到複雜的數據封包分析、

[1] ETSI, "INTRODUCTION," Lawful Interception (LI), https://www.etsi.org/technologies/lawful-interception.

隨著科技進步，攔截信息範圍逐漸廣泛，從單純電話線路的語音通訊和文字信息，發展到複雜的數據封包分析、加密通訊解密，甚至是人工智能驅動的行為模式識別等。

加密通訊解密，甚至是人工智能驅動的行為模式識別。執法機構必須在不侵犯公民權利的前提下，確保攔截資訊的隱蔽性，防止對象察覺監控存在，即時獲取重要情報，有效預防和打擊犯罪活動。合法攔截成為國家安全、反恐攻擊、犯罪偵查及公共安全等管理私人通訊存取之關鍵措施。

攔截方式之簡介

一、網路封包監察

網路電話（VoIP）隨著通訊軟體工具的普及，使用率已遠超過傳統電話，執法機構掛線監聽的方式顯然無用武之地，網路封包監察成為合法攔截中的重要手段。由於使用行動載具透過網路以軟體進行通訊的時候，傳輸的封包會經過網路設備機房，執法者經過法院合法授權後，可利用網路節點針對特定目標網路封包進行監察，[2] 惟現今市面上通訊軟體均提供點對點加密功能，即便在節點攔截、側錄取得傳輸的封包，所取得通訊資料都被加密而無法讀取，因此該項偵查作為在實務上仍有窒礙難行之處，對執法機構形成了新的挑戰。[3]

二、設備端通訊監察

設備端通訊監察是授權偵查機關可以侵入受監控者特定的設備（如個人電腦、智慧手機、平板電腦等）實施的監視行為，其原理係在未加密前的發話端或已解密後的受話端安裝木馬程式，記錄受監察者之語音、文字、圖片、網路瀏覽紀錄等相關資訊。[4] 例如瑞士政府與網路服務提供者（Internet Service Provider, ISP）合作，以

[2] 網路封包分析工具（Network Packet Analyzer）不會對擷取到的網路封包提出警告，也不針對任何網路封包進行阻擋的動作。如 Wireshark 等工具分析設備的入站和出站網路流量，捕獲在設備和互聯網之間傳輸的資料包。

[3] 楊貴智，〈科技偵查法讓國家成為駭客，如何確保人民的隱私〉，《法律白話文運動》，2021 年 10 月 14 日，https://plainlaw.me/posts/科技偵查法讓國家成為駭客，如何確保人民的隱私。

[4] 以色列 NSO 集團手機間諜軟體「飛馬」（Pegasus），得以監控目標的訊息、電子郵件、電話、麥克風、GPS 定位等。

使用行動載具透過網路通訊時，傳輸封包會經過網路設備機房，執法者經合法授權後可利用網路節點對特定目標進行監察，惟現今通訊軟體均提供點對點加密功能，因此偵查作為仍有窒礙難行之處。

木馬程式控制電腦配置之麥克風，同時記錄交談內容；德國執法機構在硬碟內植入木馬程式，錄下麥克風、網路攝影機使用紀錄，並掃描硬碟內存取得與犯罪相關之檔案；美國 FBI 使用電腦和網際網路協定位置驗證器（Computer and Internet Protocol Address Verifier, CIPAV）可記錄 IP 位址，將搜集之數據寄送回通訊監察機關。[5] 惟我國法制認為，木馬程式讓行動載具變成竊聽器時，無法擔保資訊安全，於法似有未合，故我國執法機關並未適用此種偵查作為。

三、後門程式繞行存取

所謂「後門程式」（Backdoor），係指可繞過、規避軟體安全性控制，以隱密方式取得對程式或系統的存取權，為軟體公司工程師在開發之初，設計未來方便進入系統修改和測試程式的缺口。若監察對象所使用之軟體系統設有前述之後門程式，則有心者即可藉此進入目標系統。2019 年 12 月蘋果公司公開拒絕美國政府提供解鎖犯罪者 iPhone 手機的特殊後門，[6] 因蘋果公司理解一旦開此先例，安全性及品牌信任度將大打折扣，以公司經營策略而言，斷不可能有業者願意提供後門程式，賠上企業未來的前途。

各國政府基於維護國家安全、社會治安、犯罪調查為由，使用木馬程式讀取通信內容，進而逮捕恐怖分子及重大罪犯，突破通訊監察技術無法監管之功能。惟爭議之處在於，當木馬程式取得設備端的控制權後，可以獲取整部電腦或行動載具所有資訊，如何確保最小侵害原則、保護第三人之隱私權、避免蒐集無關之資訊，似

瑞士、德國的執法機構皆有透過植入木馬程式掃描取得與犯罪相關檔案之作為。

[5] 王晴玲，《對以具加密功能之通訊軟體之通訊監察之理論與實務》，法務部，頁 49。

[6] Zack Whittaker, "Apple, in refusing backdoor access to data, may face fines," *ZDNET*, September 11, 2015, http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/.

後門程式為軟體工程師在開發之初，設計未來方便進入系統修改和測試程式的缺口，可規避軟體安全性控制，以隱密方式取得對程式或系統的存取權。

乎在執行層面無法採取合宜的措施，依然陷入人權與法治無法取捨的難題。[7]

外國法制研析

隨著進入 21 世紀，資訊科技日新月異，網際網路的發展使得傳統通訊監察失去效用。網路通訊封包加密技術的變革，嚴重威脅到國家安全層面。全球為了應對這一挑戰，《執法機關通訊協助法》（Communications Assistance for Law Enforcement Act, CALEA）被設計來確保電信運營商能夠在其網路中實施技術修改，以便執法機構能夠執行法庭授權的電子監控。茲就各國立法情形，分述如下。

一、1994 年美國國會通過《通訊協助法》（CALEA）

此法由時任總統威廉 · 傑佛遜 · 柯林頓（William Jefferson Clinton）簽署。明文要求通訊服務業者，須具備協助執法機關進行通訊監察的能力，該法案旨在執行法律授權電子監控活動的合法性；2005 年 8 月擴大適用範圍，範圍涵蓋「網路寬頻服務提供者」及「與傳統電話業者互連之網路電話業者」，即包括傳統電話通信、網際網路、VoIP 通信等在內的現代通信服務，確保電信運營商有義務協助執法機關的需求。[8]

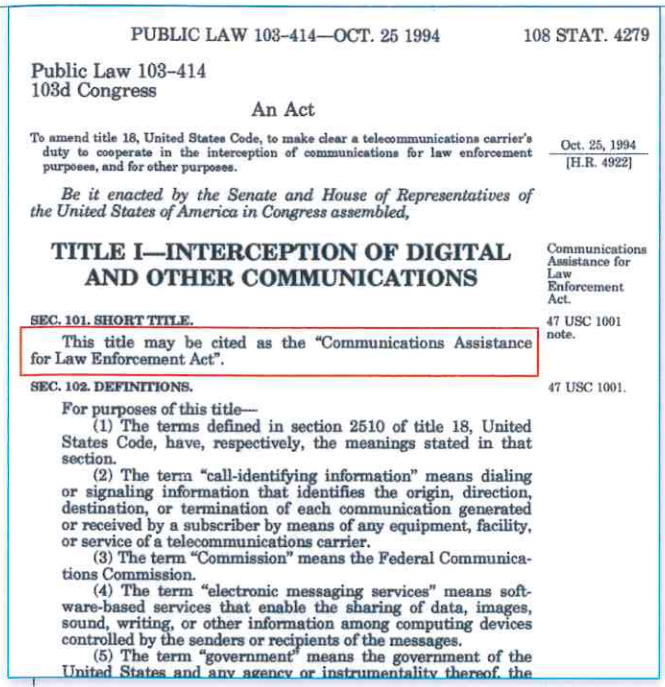
二、2005 年加拿大司法部合法存取常見問題解答（Department of Justice Lawful Access FAQ）提出

加拿大政府在問題解答中提出合法截取通信並搜查及扣押電腦資料，主要用於調查重大犯罪及國家安全威脅等情形。在受《加拿大權利與自由憲章》（Canadian Charter of Rights and Freedoms）的約束下，法官得以核發令狀，授權執法機關合法截取通信資料（範圍包括固網技術、無線技術，如手機、衛星通信；互聯網技術，如電子郵件和網路）。惟目前並無規範所有電信服務業者，都需要在其網路中設計攔截功能，這給執法機構帶來執法上額外的負擔。[9]

[7] 蕭國振，《「視覺辨識」科技偵查措施之適法性－以隱私權為核心－》，國立政治大學法學院碩士在職專班碩士論文，頁 116-117。

[8] CONGRESS.GOV, "H.R.4922 - Communications Assistance for Law Enforcement Act," https://www.congress.gov/bill/103rd-congress/house-bill/4922.

[9] Government of Canada, "Summary of Submissions to the Lawful Access Consultation," 2005, https://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html.



PUBLIC LAW 103–414—OCT. 25 1994 108 STAT. 4279

Public Law 103–414
103d Congress

An Act

To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes. Oct. 25, 1994 [H.R. 4922]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TITLE I—INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS

Communications Assistance for Law Enforcement Act.

SEC. 101. SHORT TITLE. 47 USC 1001 note.

This title may be cited as the "Communications Assistance for Law Enforcement Act".

SEC. 102. DEFINITIONS. 47 USC 1001.

For purposes of this title—

(1) The terms defined in section 2510 of title 18, United States Code, have, respectively, the meanings stated in that section.

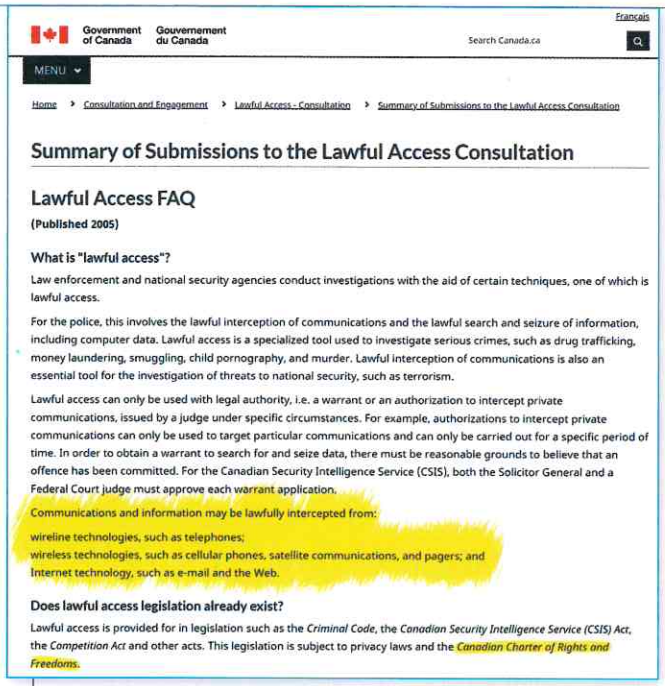
(2) The term "call-identifying information" means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.

(3) The term "Commission" means the Federal Communications Commission.

(4) The term "electronic messaging services" means software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages.

(5) The term "government" means the government of the United States and any agency or instrumentality thereof, the

美國早在 1994 年就通過《通訊協助法》，旨在執行法律授權電子監控活動的合法性。（Source: Congress.gov, https://www.congress.gov/103/statute/STATUTE-108/STATUTE-108-Pg4279.pdf）



Government of Canada / Gouvernement du Canada — Search Canada.ca — Français

MENU

Home > Consultation and Engagement > Lawful Access - Consultation > Summary of Submissions to the Lawful Access Consultation

Summary of Submissions to the Lawful Access Consultation

Lawful Access FAQ

(Published 2005)

What is "lawful access"?

Law enforcement and national security agencies conduct investigations with the aid of certain techniques, one of which is lawful access.

For the police, this involves the lawful interception of communications and the lawful search and seizure of information, including computer data. Lawful access is a specialized tool used to investigate serious crimes, such as drug trafficking, money laundering, smuggling, child pornography, and murder. Lawful interception of communications is also an essential tool for the investigation of threats to national security, such as terrorism.

Lawful access can only be used with legal authority, i.e. a warrant or an authorization to intercept private communications, issued by a judge under specific circumstances. For example, authorizations to intercept private communications can only be used to target particular communications and can only be carried out for a specific period of time. In order to obtain a warrant to search for and seize data, there must be reasonable grounds to believe that an offence has been committed. For the Canadian Security Intelligence Service (CSIS), both the Solicitor General and a Federal Court judge must approve each warrant application.

Communications and information may be lawfully intercepted from:

wireline technologies, such as telephones;
wireless technologies, such as cellular phones, satellite communications, and pagers; and
Internet technology, such as e-mail and the Web.

Does lawful access legislation already exist?

Lawful access is provided for in legislation such as the *Criminal Code*, the *Canadian Security Intelligence Service (CSIS) Act*, the *Competition Act* and other acts. This legislation is subject to privacy laws and the *Canadian Charter of Rights and Freedoms*.

在受加拿大權利與自由憲章的約束下，加拿大法官得以核發令狀，授權執法機關合法截取通信資料。（Source: Department of Justice Canada, https://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html）

三、2000 年英國政府通過《調查權力法案》（Regulation of Investigatory Powers Act 2000, RIPA）

此法旨在規範政府機構進行電子監控和資料收集的合法授權，包括通信攔截、設備干擾、使用祕密情報來源和獲取通訊資料等活動。[10] 面對技術進步和不斷變化的威脅環境，2016 年通過了更為全面的《調查權法案》（Investigatory Powers Act），旨在保護國家安全、預防犯罪活動和保護公眾免受恐怖襲擊的同時，確保對個人隱私權的尊重和保護。新法增加要求 ISP 業者保留用戶連接記錄（ICR）長達一年，供執法機構獲得授權時得以調閱，並允許在一定條件下進行大數據分析，藉以識別恐怖威脅和行為模式。[11]

Regulation of Investigatory Powers Act 2000

2000 CHAPTER 23

An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes.

[28th July 2000]

Investigatory Powers Act 2016

2016 CHAPTER 25

An Act to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

[29th November 2016]

英國陸續通過《調查權力法案》、《調查權法案》，旨在保護國家安全、預防犯罪活動和保護公眾免受恐怖襲擊的同時，確保對個人隱私權的尊重和保護。（Source: UK Legislation, https://www.legislation.gov.uk/ukpga/2000/23/introduction/2022-03-25; https://www.legislation.gov.uk/ukpga/2016/25/introduction/enacted）

[10] Legislation.gov.uk, "Regulation of Investigatory Powers Act 2000," https://www.legislation.gov.uk/ukpga/2000/23/contents.

[11] Legislation.gov.uk, "Investigatory Powers Act 2016," https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

四、1998 年荷蘭政府通過《電信法》（Telecommunicatiewet）

此法旨在規範電信網路和服務的許可、提供和使用，以及相關的用戶隱私保護。內容明文規範電信網路業者有義務配合該國的《刑事訴訟法》（Wetboek van Strafvordering）及《2017 年情報和安全服務法》（Wet op de inlichtingen- en veiligheids-diensten 2017），並需具備必要的技術能力和科技設施，攔截或記錄透過其電信網路傳輸的電信資訊。[12] 透過上揭規範，不但能有效保護國家安全和公共利益，亦能維護人民的隱私權益。

他山之石，審視我國法規不足

2021 年國家洗錢及資恐風險評估報告指出，我國受到高度威脅的犯罪共有 10 大類型，包含毒品販運、詐欺、走私、稅務犯罪、組織犯罪、證券犯罪、地下匯兌、網路博弈、貪污賄賂及智慧財產犯罪等。[13] 面對「科技犯罪」不能只是一味傾倒於人權之維護，而忽略社會治安的維穩，消極的鴕鳥心態將導致治安的惡化，比例失衡所帶來的衝擊，都是全民所要承受的苦果。

全球執法機構為了突破通訊軟體加密機制，在「設備端」監察採取之手段已經無所不用其極，嚴重侵犯秘密通訊自由、資訊隱私權及個人資料自主權，本文認為，除非已達危及國家安全層級需求，方可適用此種新型態的偵查作為，一般犯罪偵查不宜採用植入木馬程式的偵查方式取證，以維護權益均衡。普羅大眾對於科技偵查措施產生的疑慮，立法機關應審慎面對，並儘快制定相關規範，授權給予執法者使用科技偵查措施的依據，衡平公益訴追與保障人權，方能面對將來科技犯罪帶來的嚴峻挑戰。

洗錢威脅評等表

低	中	高	非常高
1.性剝削 Sexual Exploitation	1.非法販運武器 Illicit Arms Trafficking	1.第三方洗錢 Third-Party ML	1.毒品販運 Drug Trafficking
2.人口販運 Trafficking in Human Beings (Migrant Smuggling)	2.贓物 Illicit Trafficking in Stolen and other Goods		2.詐欺 Fraud
3.搶奪、強盜 Abrupt Taking, Robbery	3.竊盜 Theft		3.走私 Smuggling
4.恐嚇取財(含勒贖軟體) Extortion (including Ransomware)	4.環保犯罪 Environmental Crime		4.稅務犯罪 Tax Crime
5.偽造貨幣 Counterfeiting Currency	5.偽造文書 Forgery		5.組織犯罪 Organized Crime
6.殺人、重傷害 Murder, Grievous Bodily Injury	6.綁架、拘禁等妨害自由 Kidnapping, Illegal Restrain		6.證券犯罪 Securities Crime
7.海盜 Piracy			7.地下匯兌 Underground Banking
			8.非法賭博(含網路博弈)(新增) Illegal Gambling (including Online Gambling)(newly-added)
			9.貪污賄賂 Corruption and Bribery
			10.智慧財產犯罪 IPR Infringement

2021 年國家洗錢及資恐風險評估報告指出，我國受到高度威脅的犯罪共有 10 大類型。（資料來源：行政院洗錢防制辦公室，https://www.amlo.moj.gov.tw/1461/31062/1482/37161/post）

[12] Overheid.nl, "Telecommunicatiewet," https://wetten.overheid.nl/BWBR0009950/2024-01-01.

[13] 林俊宏，〈2021 洗錢資恐風險報告發表　10 大洗錢犯罪手法曝光〉，《鏡周刊》，2021 年 12 月 29 日，https://www.mirrormedia.mg/story/20211229inv002/。