112 年委託研究報告

網路電視機上盒（OTT TV 機上盒）監理法規與技術之研究

期末報告

計畫委託機關：國家通訊傳播委員會

中華民國 113 年 2 月

112 年委託研究報告
PG11207-0044

網路電視機上盒（OTT TV 機上盒）監理法規與技術之研究

受委託單位

國立臺灣科技大學

計畫主持人

查士朝 教授

協同主持人

陳曉慧 教授

研究人員

張郁婷 利文韡

研究期程：中華民國 112 年 07 月至 112 年 12 月

研究經費：新臺幣 287 萬元

中華民國 113 年 2 月

目次

表次

圖次

提要

關鍵詞：網路電視機上盒、監理法規與政策、監理技術、數位著作侵權

一、 研究緣起

近年來網路視聽多媒體發展快速，民眾的收視聽管道多元化，透過網際網路、OTT TV 平台皆可取得過往須經由傳統廣電媒體之視聽內容。基於網際網路之便利性、可取得性，不法集團透過技術截取有線電視、衛星廣播電視事業之節目訊號，再經由中繼機房將節目訊號提供給特定網路電視機上盒（下稱 OTT TV 機上盒），使得擁有該機上盒之民眾能夠無償取得未授權之影音內容，此種方式不但嚴重侵害相關視聽著作權人以及合法取得播放授權業者之合法權益，也分食合法授權之收視市場，深深影響相關產業及市場之健全發展。

為有效監理 OTT TV 機上盒之合法使用，防止合法節目內容被盜用，並釐清各主管機關之權責，規劃有效降低違法機上盒與網際網路著作權侵害之監理建議。本計畫蒐集及分析美國、英國、歐盟、韓國、日本、新加坡、中國大陸等重要國家及區域組織之網路視聽平臺發展現況，彙整其 OTT 市場現況、政府角色、政策與法規，同時探討各國 OTT TV 機上盒之監理政策、法規以及監理技術。再者，蒐集及分析我國及其他國家或區域組織 OTT TV 機上盒涉侵害智慧財產權之實際案例及應處作為。研究過程中為了解我國 OTT TV 機上盒監理法制發展需求，透過辦理兩場座談會蒐集業者與專家意見，提出實務上窒礙難行與亟需解決之問題與建議。此外，關於 OTT TV 機上盒技術分析方式、監理技術作業流程與方法，抽驗已上市的 OTT TV 機上盒，針對機上盒是否有綁定非法 App 進行檢測（檢測項目為 App 之行為

與 App 是否綁定特定機上盒)。進而分析我國 OTT TV 政策、法規及監理技術可再精進之處，並提出相關調適建議。

二、 研究方法及過程

本計畫第一部分將聚焦於 OTT TV 機上盒法制研析制度，並參酌文獻、次級資料及其他國家之規定，包括：美國、英國、歐盟、韓國、日本、新加坡、中國大陸等重要國家及區域組織之立法案例，作為本計畫後續提出政策建議之參考基礎；第二部分則透過研究團隊之技術基礎，檢測目前市面上所販售之 OTT TV 機上盒，以利進一步了解相關違法技術及破解方式。同時，為了解我國 OTT TV 機上盒監理法制發展需求，透過舉辦兩場座談會方式蒐集業者與專家意見，提出實務上窒礙難行與亟需解決之問題與建議，以座談會所蒐集之專家與產業意見為基礎，經過具體收斂之後，針對初步研究結果進行討論，提出最可行及最被認可之建議結論。

三、 重要發現

主要國家 OTT TV 機上盒規範之綜整

（一）OTT TV 目前以產業規範為主，少數會採取執照管理制度

綜整主要國家或區域組織之政策、法規：目前各國針對 OTT TV 平台產業之治理規範，相關規範相對於傳統廣播電視較少，主要仍以產業自律為主，而在內容管制部分，則以核心價值之監管為主，例如：保護兒少、著作權保護、個人資料及隱私保護等；僅有少數國家針對 OTT TV 產業採取執照管理制度（例如：中國大陸、新加坡），中國大陸甚至會介入內容產製之審查。

（二）大部分國家與地區會對 OTT TV 機上盒進行監理

關於 OTT TV 機上盒之監管，由於機上盒屬於射頻器材，大部分國家與地區皆會針對器材進行事前監管，惟監管內容略有不同，我國

主要以電波標準為主；歐盟除電波標準外，認為機上盒應被設計成保護使用者之隱私及個人資料、免於詐欺、以及維護網路安全；中國更是進一步針對機上盒所提供之內容進行相關管制。故關於 OTT TV 機上盒之監管，本計畫歸納出目前主要的三種模式：事前監理、需要執照才可以販賣機上盒設備及處罰對於機上盒裝設破解合法串流技術軟體之行為。

（三）目前世界各國/地區會不同程度訂定 OTT TV 機上盒侵權規範

每個國家/地區，幾乎都會要求 OTT TV 機上盒播放受著作權保護之內容，以維持線上行為之合法性。一般來說，從非法/未經授權的來源下載影音內容是侵犯智慧財產權的行為，受到各國著作權法之保護；至於接收串流媒體，目前主要國家也認為這樣的行為構成侵害著作權，無論是使用技術設備還是預裝附加軟體的 OTT TV 機上盒。

而各國在違法機上盒盜版侵權問題，提出多種監理、行政措施進行規範，以解決透過違法機上盒之網路盜版問題。主要可以分為三種模式，包括：行政措施、司法措施及市場機制。整體而言，主要國家對於網路盜版與違法機上盒之侵權問題相當重視，依據本計畫研究，主要國家皆可透過著作權相關民刑事法規，依據司法程序處理透過機上盒侵犯著作權之行為。不過由於網際網路之無國界性、易於隱匿等特性，雖著作權人擁有豐富的法律執行手段可以主張自身權利，但礙於各國執法時效、程序複雜度及執法有效性等問題，雖有大量可用之執法措施，並不代表實際上被廣泛運用或真正能有效打擊違法機上盒之侵權問題。

除著作權相關民刑事規定外，歸納相關司法措施尚包括：以英國、歐盟為首，逐漸透過快速、動態之司法執行措施，可針對提供侵權內容的網站進行動態封鎖，近年來，英國甚至開始以詐欺、洗錢等罪名，

透過刑事規範；以美國為首，則係以安全港作為誘因，通知網路服務提供者對侵權者及其託管或連接到侵權內容進行移除或封鎖；韓國透過專責機構處理網際網路之盜版問題等。

在技術方面，非法集團透過撰寫專屬於特定機上盒的非法 App 軟體，再利用人員線上指導或是錄製 YouTube 視訊內容進行隔空教學，指導消費者如何下載違法 App 觀看節目，使機上盒成為侵權的工具。

本計畫抽驗我國已上市的 OTT TV 機上盒，將連線過程進行分析，以瞭解該設備內容之運作方式，驗證機上盒是否有綁定可收看非法影音內容 App 之行為。而提供非法影音的機上盒業者，因為是透過販售機上盒而獲利，會進行裝置鑑別。雖然不同廠牌 OTT TV 機上盒會有不同做法，但透過攔截資料發現有以下特徵：

1. 程式通常有經過加殼或混淆，因此主要的測試手段為進行側錄，一般按照是否有使用安全連線，以及是否有綁定憑證，會有不同的做法。
2. App 啟用時常會使用認證網卡 MAC 編號、CPU-ID 及 KEY 等數值，機上盒之網卡編號 MAC 碼是唯一的認證編號，每台皆不同。
3. 在確認完裝置資訊後，會取得「gkey」、「token」等參數，以做為之後驗證之用，須提供這些參數才可取得頻道資訊。

總結來說，近年來 OTT TV 機上盒，為避免違法販售，主打販售純淨版，由消費者購買後再自行安裝特定 App。而經由本計畫之技術檢測，發現相關 App 並非單純下載即可啟用，必須要事先通過認證，類似輸入帳號密碼等機制，以限制可使用之 App 軟體，本計畫認為目前市面上可收看違法影音內容之機上盒本身可能扮演類似通行金鑰角色，而機上盒本身專屬網卡硬體編碼則為關鍵認證資訊，僅有安裝

在這些機上盒上的侵權影音程式可以收視免費影音內容，證明硬體製造商與軟體商存在一定程度的合作關係。

四、 主要建議事項

（一）強化機上盒監理

如參考歐盟《無線電設備指令》增訂事前審驗規範，建議可針對機上盒製造商、進口商與分銷商，明知或有理由可知，於銷售後再以客服方式安裝非法收視視聽內容之程式；又或購買之消費者自行至網路論壇查詢安裝此類非法收視程式，只要此類程式可危害消費者之隱私及個人資料、詐欺、以及破壞網路安全，機上盒欠缺阻止載入該軟體之設計則不予審驗通過，不可進入市場，要求製造商將隱私和個人數據、網路安全和欺詐預防之考慮因素整合至機上盒之設計中。

（二）推動後市場管理機制

為確保消費者的安全，需要迅速且可靠地通知消費者權益相關議題，因此，經營者和線上市場提供者應該利用他們手中的客戶資料，通知消費者有關已購買產品的召回和安全警告。建議可參照歐盟之回收作法，進行條文調修，包括通知義務與回收對價限制，以具體化業者之回收義務及限制。

（三）透過法規調適防治 OTT TV 機上盒侵權

1.《著作權法》之修法建議：

(1) 修訂《著作權法》第 87 條第 1 項第 8 款：為徹底杜絕「純淨版」機上盒之相關脫法行為，建議於《著作權法》第 87 條第 1 項第 8 款增訂第 4 目「製造、輸入或銷售專供匹配或綁定第一目之電腦程式之設備或器材，未預先載入者亦同。」之相關文字。

(2) 確認 OTT TV 機上盒未經授權傳送「體育賽事」直播之違法性：我國未採鄰接權制度，賽事轉播節目若欠缺視聽著作之要件，則可能無法受到保護，建議可強化體育賽事之著作權、鄰接權保護，避免違法 OTT TV 機上盒在侵害賽事轉播著作權後，相關人未能妥善獲得救濟。

(3) 研議扣押裁定之彈性：建議我國法院依個案之性質（以 OTT TV 機上盒所使用之侵權程式及其接取之 CDN 伺服器為主，OTT 平台網站、論壇、串流平台則不適用），「得」下達範圍較大之扣押裁定，在一定期間內，經過第三方驗證機構認證後，對侵權程式所接取提供侵權影像的 CDN 伺服器 IP，可向 ISP、TWNIC 提出扣押裁定。倘域名註冊人或 IP 使用者對扣押裁定不服，可依照《刑事訴訟法》第 404 條第 1 項但書第 2 款提起抗告，且依同條第 2 項規定，即使扣押已經執行終結，法院也不得因已執行無實益而駁回。抗告法院倘認為域名扣押有所不當，自得撤銷原裁定，於有必要時，並自為裁定（《刑事訴訟法》第 413 條規定參照）。並建議確認行為人違反著作權法第 87 條第 1 項第 7、8 款，除處以有期徒刑、罰金外，得擴大刑事訴訟法上「沒收」之概念，針對確認侵權之第 87 條第 1 項第 7、8 款之電腦程式，於一定期間，對其所持續連結之伺服器 IP，經第三方驗證機構確認供相同侵權行為所使用，得由主管機關命 ISP、TWNIC 停止用戶接取。

(4) 強化目前智財法中對於 ISP 業者之「安全港條款」之運用：相關規範自增訂以來已適用多年，衍生出不少法律問題，例如：網路平台業者是否適用、假藉通知取下制度而進行商業

競爭、是否僅有著作權人能進行通知 ISP 業者取下，著作權人如何認定等，建議未來可由第三方公正機構通知 ISP 業者相關盜版侵權之可能性，並告知其智財法上安全港條款之權利義務，由業者自行判斷下架相關盜版影音，並適用相關免責規定。

2.《電信管理法》之修法建議：

建議於《電信管理法》第 65 條增訂「使用電信管制射頻器材有代理權、專利權、著作權爭議者，依有關法律之規定。」

3. 廣電三法之修法建議：

(1) 新增侵權防治、訊號侵權機制：2022 年 5 月 25 日國家通訊傳播委員會（以下簡稱 NCC）通過新版《網際網路視聽服務法》（草案），外界多數期待該草案能夠處理網際網路視聽之盜版問題，惟該草案基本上仍以網路上所衍生的問題，除網際網路視聽服務事業之營運及其提供之內容服務，仍應適用各該行為之法律，故侵害智慧財產權、著作權等盜版問題，仍須回歸《著作權法》處理，但 NCC 擬透過草案針對多次侵權之業者得以糾正其相關不當營業行為之機制，後續立法進展值得持續關注。

(2) 給予自願登記納管之業者予以主張「訊號竊盜」之法律地位：民事部分可參考《有線廣播電視法》第 54 條第 1 項之規定：「未經系統經營者同意，截取或接收系統播送之內容者，應補繳基本頻道收視費用，並負民事損害賠償責任。」明訂未經合法網際網路視聽服務提供者同意，截取或接收網際網路視聽服務提供者播送之內容或訊號者，應負一定之法律責任；刑事部分則可參照《電信法》第 56 條之規範，針對「意

圖為自己或第三人不法之利益，未經網際網路視聽服務提供者同意，截取或接收網際網路視聽服務提供者播送之內容或訊號營利者」設有相關刑事處罰，或是要求連線服務提供者、電信事業或設置公眾電信網路者拒絕侵權之網際網路視聽服務提供者電信服務之請求及通信傳遞或為必要之處置。

4.《電信管制射頻器材審驗管理辦法》之修法建議：

參考歐盟於《一般產品安全規則》新增產品召回程序。

5. 通盤檢視數位產品之資安、個資規範

參考歐盟《資安韌性法》（草案）（Cyber Resilience Act）加強數位產品之資安規則，包括：網路功能損害禁止、隱私保護措施、防止詐欺、軟體之合規性等。

（四）跨部會合作行政作為之建議

1. 建立有效機上盒上架與下架流程，保護合法業者

機上盒非法侵權並非單一部會權責，涉及相關部會應建置有效事前審查、檢測上架，事中強化稽查、調查與受理檢舉機制，嚴格監督市場不法情事活動，並強化監管工作之行政檢查措施，避免不肖業者鑽漏洞，面對實際從事不法工作者，經發現屬實者，除依照法規予以裁罰之外，應建立一套有效配套措施。

2. 成立跨部會協調機制並考量設置第三方機構專責

參考韓國著作權保護署（KCOPA）之作法成立跨部門工作小組，負責著作權保護政策的制定和執行、審查與著作權保護有關的事項以及實施著作權保護所需的項目。時程上可進一步分為短、中長期規劃：

(1) 短期

短期可以成立跨部會工作小組，召集相關機關成立跨部會工作小組落實各項執法工作，完善網際網路著作權侵害之防治機制。

(2) 中、長期

若欲建立如韓國 KCOPA 集「預防→檢測→分析→行動」相關功能之推進系統並專責處理著作權侵權之第三方機構，建議仍要透過《著作權法》授權，並可參考韓國做法，負責著作權侵權之相關資訊蒐集、數位鑑定、內容鑑識等，逐步建立防護網際網路盜版之防護網。

Abstract

Keywords: OTT TV set-top box, OTT TV set-top box regulatory laws and policies, OTT TV set-top box regulatory technology, digital copyright infringement.

Ⅰ. Background

In recent years, the development of online audiovisual multimedia has been rapid, diversifying the channels through which people consume media content. Now, the content that used to be accessed through traditional broadcasting media can be obtained via the internet and OTT (Over-The-Top) TV platforms. Leveraging the convenience and accessibility of the internet, illicit groups capture program signals from cable and satellite broadcasting services, then redistribute these signals through relay server rooms to specific internet set-top boxes (referred to as OTT TV boxes). This enables individuals who possess these boxes to access unauthorized audiovisual content without cost. This practice not only severely infringes upon the legal rights of the content copyright holders and entities that have legally obtained broadcasting rights but also encroaches upon the legitimate subscription market, profoundly impacting the healthy development of the related industries and market.

To effectively regulate OTT TV set-top boxes, prevent the illicit use of legitimate program content, and delineate the responsibilities of regulatory authorities, this project aims to propose effective supervision strategies. These are designed to mitigate the use of unauthorized set-top boxes and curb copyright infringements on the internet. The project involves collecting and analyzing the development and regulatory approaches of OTT TV in major nations and regions, including the United States, the United Kingdom, the European Union, South Korea, Japan, Singapore, and China. It synthesizes the prevailing state of the OTT TV market, government roles, policies, and regulations across these jurisdictions.

Additionally, the project examines actual cases of copyright infringement involving OTT TV set-top boxes both domestically and internationally, aiming to formulate appropriate responses.

II. Research Methods and Process

The initial phase of this project is dedicated to the legislative analysis of OTT TV set-top boxes, involving a comprehensive review of literature, secondary data, and regulations from other prominent countries and regions. The legislation from these jurisdictions will inform the policy recommendations proposed in this project. The subsequent phase leverages technical expertise to scrutinize OTT TV set-top boxes, aiming to demystify the associated illegal technologies and decryption techniques.

III. Key Findings

A. Compilation of the Regulatory Frameworks for OTT TV Set-Top Boxes from Major Countries

(a) OTT TVs are now mainly regulated by the industry, with a few adopting a license management system.

An analysis of policies and regulations from prominent countries and regions indicates that governance measures for the OTT TV industry are somewhat less extensive than those for traditional broadcasting. Predominantly, the industry adheres to a model of self-regulation. In terms of content control, the emphasis largely rests on upholding core principles, which include protecting minors, ensuring copyright compliance, and safeguarding personal data and privacy. A minority of countries have implemented a Permit system for the OTT TV sector, notable examples being China and Singapore. It's worth highlighting that China takes a proactive stance by also reviewing the outcomes of content production.

(b) Most countries and regions regulate OTT TV set-top boxes.

In terms of regulating OTT TV set-top boxes, given that these devices are classified as controlled telecommunication radio-frequency devices, the majority of countries and regions implement pre-market oversight. Nevertheless, the specifics of the regulations tend to differ. In our country, the emphasis is predominantly on adhering to radio frequency standards and promoting the efficient utilization of the radio spectrum. The European Union, on the other hand, advocates for set-top boxes to be engineered with technical safeguards for privacy, personal data, anti-fraud measures, and cybersecurity. China, in addition, exercises control over the content disseminated through these set-top boxes.

Consequently, this project delineates the prevailing regulatory strategies into three primary categories: pre-market oversight, the mandate for a sales license for set-top box devices, and the imposition of penalties for the installation of unauthorized streaming software that circumvents licensed content.

(c) Currently, countries/regions around the world have set up infringement regulations for OTT TV set-top boxes at various levels.

Virtually every country or region requires OTT TV set-top boxes to distribute authorized content, reinforcing the legality of online activities. Typically, downloading audiovisual content from unauthorized sources is considered a violation of intellectual property rights. Additionally, accessing such content via streaming constitutes copyright infringement in major countries, irrespective of the use of technical devices or OTT TV set-top boxes equipped with extra software.

To combat internet copyright infringements facilitated by illegal set-top boxes, various countries have implemented a spectrum of regulations and administrative strategies. These strategies generally fall into three categories: administrative policies, judicial approaches, and market

mechanisms. Major countries place significant emphasis on preventing online copyright infringements and the distribution of illegal set-top boxes. According to this project's findings, these infringements can be addressed through both civil and criminal copyright-related regulations. However, the inherent borderless and anonymous nature of the internet means that issues such as enforcement delays, procedural complexities, and the overall effectiveness of these measures require further examination. Possessing a range of enforcement strategies and policies does not inherently ensure their widespread adoption or actual efficacy in mitigating the infringement issues associated with illegal set-top boxes.

Beyond civil and criminal copyright-related regulations, it's noteworthy that certain jurisdictions like the UK and the European Union have implemented rapid and adaptive judicial enforcement actions, particularly targeting websites distributing infringing content for dynamic blocking. The UK, for instance, has implemented stringent measures, prosecuting distributors of illegal set-top boxes under criminal law for offenses including fraud and money laundering. In contrast, the United States predominantly employs safe harbor statutes, incentivizing internet service providers to remove or block infringing content. South Korea, on the other hand, tackles the issue through specialized institutions dedicated to preventing internet copyright infringements.

Illegal groups create illegal App specifically designed for certain set-top boxes. They provide online guidance through personnel or place tutorial videos on YouTube to teach consumers how to download and install these illegal Apps on the set-top boxes for viewing unauthorized content. As a result, the set-top box becomes a tool for copyright infringement.

This project delves into the examination of OTT TV set-top boxes available in the market, employing packet capturing and analysis during

the devices' connection processes. This methodical approach aims to scrutinize the content within the devices and juxtapose it with the operations of network transmission packets. The primary objective is to ascertain whether the set-top boxes are associated with illicitly bundled applications. Providers of illegal set-top boxes often resort to device authentication mechanisms to ensure that consumers purchase exclusively from their outlets. While practices may vary across different OTT TV set-top box brands, the data intercepted and analyzed in the course of this project has yielded the following insights:

(a) The Apps use shelling or obfuscation techniques. As a result, the primary testing method involves recording and evaluating whether secure connections are utilized or if certificates are properly bound.

(b) Upon activation, Apps commonly utilize authenticated values such as the media access control address of the network card, CPU-ID, and KEY. The MAC address of the set-top box's network card serves as a unique authentication identifier for each device.

(c) Once the device information is confirmed, parameters like "gkey" and "token" are acquired for verification purposes. These parameters are essential for accessing channel information.

In summary, it's observed that providers of OTT TV set-top boxes are increasingly just selling boxes of 'clean versions' in recent years, aiming to sidestep regulations against illegal sales. Post-purchase, consumers themselves undertake the installation of specific Apps. The technical analysis conducted in this project underscores that the mere act of downloading these Apps doesn't ensure their functionality. Often, these Apps demand prior authentication, such as the entry of account credentials, as a measure to control access. This project reveals that illegal set-top boxes might operate analogously to 'access keys.' The unique hardware encoding embedded within the network card of the set-top box emerges as

critical authentication data. This observation suggests a possible collusion between the hardware manufacturers and software providers, pointing towards a more intricate ecosystem underpinning these devices.

Ⅳ. Main Recommendations

A. Recommendations for Set-top Box Regulation

Referring to the provisions of the EU's Radio Equipment Directive (RED) 2014/53/EU, we recommend amendments to the pre-market examination standards for set-top boxes. Manufacturers, importers, and distributors of set-top boxes who knowingly or have a reasonable belief that they provide customer service to install illegal Applications enabling unauthorized content viewing or listening should be subject to scrutiny. Similarly, consumers who independently seek guidance on online forums to install such illicit Applications should be considered. Any software that jeopardizes consumer privacy, personal information, fraud prevention, or compromises cybersecurity should not gain Approval from competent authorities if the set-top box lacks mechanisms to prevent the installation of such unauthorized software. Consequently, these set-top boxes should be prohibited from entering the market. Furthermore, manufacturers must incorporate considerations pertaining to privacy, personal data protection, cybersecurity, and fraud prevention into the design and development of their set-top boxes.

B. Recommendations for Post-Market Management Mechanism

Ensuring consumer safety requires timely communication. Therefore, operators and online providers should utilize customer data to inform consumers about product recalls and safety alerts related to their purchases. Possible methods include:

(a) Establishing Clear Responsibilities and Restrictions for Operators Regarding Product Recalls:

It's advisable to align with the recall procedures observed within the European Union and enact Appropriate regulatory adjustments. This involves defining the operator's obligations concerning notification and setting limits regarding the exchange or return of products.

C. Recommendations for Regulatory Amendments to Prevent Internet Copyright Infringements via OTT TV Set-Top Boxes

(a) Recommendations for Amendments to the Copyright Act

i. Amending Article 87, Section 1(8) of the Copyright Act

To eliminate illicit activities related to "clean version" set-top boxes, it is advisable to amend Article 87, Section 1(8) of the "Copyright Act." The suggested amendment would be: "To manufacture, import or sell specialized equipment or devices for loaded with the computer programs of the first item, regardless of whether it is pre-loaded."

ii. Confirm the illegality of unauthorized broadcasting of sports programs via OTT TV set-top boxes

The Copyright Act does not incorporate the concept of neighboring rights. Consequently, sports broadcasts may not possess the essential elements of "audiovisual works" as defined in the copyright act, potentially limiting their protection. Enhancing copyright or neighboring rights protection for sports programs can address this gap. This enhancement will deter illegal OTT TV set-top boxes from infringing on sports broadcasting, ensuring that right holders can pursue suitable remedies.

iii. Exploring the Flexibility of the provisional attachment

It is suggested that courts, based on the features of each case (primarily limited to specific infringing programs and CDN servers, excluding OTT platforms, forums, and streaming platforms), could issue broader seizure orders within a certain scope. After a certain period and certification by a third-party verification agency, the IP addresses of CDN servers that provide infringing content through infringing programs can be subject to

provisional seizure attachment. If the domain registrant or IP user disagrees with the provisional seizure attachment, they may appeal in accordance with Article 404, paragraph 1, subparagraph 2 of the Code of Criminal Procedure. Pursuant to the same article, even if the seizure has been completed, the court may not dismiss the case. If the appellate court finds the domain seizure improper, it may revoke the original ruling and make its own ruling (Article 413 of the Code of Criminal Procedure). Furthermore, it is recommended to confirm that the perpetrator violated Article 87, paragraphs 1, subparagraphs 7 and 8 of the Copyright Act. In addition to imprisonment and fines, the concept of "confiscation" in criminal procedure may be expanded to target computer programs confirmed to violate Article 87, paragraphs 1, subparagraphs 7 and 8. Within a certain period, upon verification by a third-party verification agency that the server IP addresses continually linked to such programs facilitate similar infringing activities, competent authorities may instruct ISPs and TWNIC to cease user access.

iv. Strengthening the Application of "Safe Harbor Provisions" for ISP Operators of the Copyright Act

The "Safe Harbor Provisions" of the Copyright Act have been applied for many years, and giving rise to numerous legal issues. These include questions such as whether internet platform operators are applicable of these clause, whether there is misuse of the takedown notification system for commercial competition, whether only copyright holders can notify ISP operators for takedown, and how copyright holders can make determinations. It is suggested that in the future, a third-party impartial organization could notify ISP operators of potential piracy and infringement, informing them of their rights and obligations under the copyright act regarding safe harbor provisions. Operators would then

independently decide to take down related pirated content and apply relevant immunity provisions.

(b) Recommendations for Amendments to the Telecommunications Management Act

The recommendation to amend Article 65 of the Telecommunications Management Act to include "In the event of disputes over the agency rights, patent rights, or copyrights of telecommunications control radio frequency equipment related thereto shall be governed by the regulations of applicable statutes."

(c) Recommendations for Amendments to the Three Broadcasting Laws

i. Amending provisions in addition to Anti-Infringement and Signal Infringement Mechanisms

On May 25, 2022, the NCC Approved a new version of the "Internet Audiovisual Service Act" (Bill). While many anticipated that this bill would address piracy concerns related to internet audiovisual content, but its primary focus remains on issues stemming from online activities. Apart from overseeing the operations of internet audiovisual service providers and the content they provide, all other matters should continue to be governed by existing regulations, particularly those concerning intellectual property rights and copyright infringement. Nevertheless, through this bill, the NCC aims to implement mechanisms to address recurrent infringements by service providers. Ongoing legislative developments in this area warrant continued attention.

ii. Granting Legal Status to Voluntarily Registered Managed Entities against "Signal Theft"

In the civil context, reference can be made to Article 54(1) of the "Cable Radio and Television Act," which stipulates: "A person who intercepts or receives content transmitted by a system without the

agreement of the system operator shall pay the basic subscription fee and be liable for civil damages compensation." This clearly defines the legal responsibility for those intercepting or receiving content signal without the consent of legitimate internet audiovisual service providers. In the criminal context, guidance can be drawn from Article 56 of the "Telecommunications Act," which imposes penalties for those intending to profit unlawfully by intercepting or receiving content without the system operator's consent. Additionally, it could require connection service providers, telecommunications companies, or public telecommunications network setters to deny requests for telecom services or necessary disposals concerning the aforementioned internet audiovisual service providers.

(d) Recommendations for Amendments to the Regulations Governing Compliance Approval for Controlled Telecommunications Radio-Frequency Devices

Reference to the EU's addition of product recall procedures in the General Product Safety Regulation.

(e) Reviewing the cybersecurity and personal data regulations of digital products

Reference to the EU's proposed Cyber Resilience Act to enhance cybersecurity rules for digital products, including: the rule of prohibition of network function impairment, privacy protection, fraud prevention, software compliance, etc.

D. Recommendations for Enhancing Collaborative Administrative Actions Among Competent Authorities

(a) Implementing an Effective Market Oversight Mechanism for Set-Top Boxes and Establishing a Removal or Takedown Process to Safeguard Legitimate Operators

Addressing the copyright infringements linked to set-top boxes demands a concerted effort, transcending the jurisdiction of any single

regulatory body. It is imperative for relevant authorities to implement robust pre-review and market surveillance mechanisms to preemptively identify potential infractions. Operational measures should include the reinforcement of inspection protocols, investigative processes, and the encouragement of whistleblower systems. A stringent monitoring regime is crucial to curb illicit market activities, necessitating enhanced administrative scrutiny to deter entities from engaging in copyright violations. In instances where illicit activities are identified and verified, it is essential to enforce regulatory penalties decisively. Moreover, the formulation and execution of a comprehensive and effective suite of measures are pivotal in addressing these challenges effectively.

(b) Establishing a Cross-Ministerial Coordination Mechanism and Considering the Establishment of a Dedicated Third-Party Organization

Drawing from the successful model of the Korean Copyright Protection Agency (KCOPA), the formation of a cross-ministerial working group is proposed. This multidisciplinary team would be tasked with discussing and strategizing on copyright protection issues and spearheading the execution of necessary initiatives. To ensure systematic progress and measurable outcomes, the timeline for this initiative should be segmented into three distinct phases:

i. Short-term

In the short term, it's crucial to establish a cross-ministerial working group. This assembly will bring together the relevant authoritative bodies, fostering a collaborative environment aimed at reinforcing the enforcement of various copyright laws and regulations. Such a unified approach is instrumental in bolstering the efforts to curb copyright infringements on the internet. By streamlining coordination and consolidating resources, this

group will lay a solid foundation for a more coherent and effective copyright protection strategy.

ii. Medium to Long-term

To establish a comprehensive system akin to the "Prevention → Detection → Analysis → Action" model of the Korean KCOPA and to entrust a third-party organization specialized in addressing copyright infringements, it is recommended to obtain authorization through copyright act. By referencing the Korean Approach, this third-party entity would be responsible for collecting relevant information on copyright infringements, conducting digital forensics, content identification, and progressively building a robust defense mechanism against internet piracy.

第一章 前言

第一節　研究動機

OTT TV 透過網際網路向用戶直接提供各項應用服務或內容，不再經過傳統電信、衛星、廣播等，同時不受網際網路連線服務業者（Internet Service Provider，ISP）介入，而非法 OTT TV 機上盒是一種透過網路連接未經授權的影音內容設備，允許消費者從非法串流媒體伺服器傳輸未經授權的影音內容，規避原先應透過付費方式觀看 OTT TV 平台之相關內容。此類設備和應用程式對不願支付訂閱費用的消費者很有吸引力，因為易於購買和使用，並且可以免費或以極低的成本觀看娛樂影音內容，多數國家針對此行為多透過智慧財產權相關法規解決內容的侵權問題，並有民事責任及刑事處罰等。

由於使用非法 OTT TV 機上盒將會對影音產業和權利人造成損害，且執法通常涉及跨境傳輸而產生障礙。當串流媒體服務內容與創新商業模式結合時，非法 OTT TV 機上盒的使用侵害了相關的創新和智慧財產權，也削弱合法串流媒體服務的商業可行性。

此外，許多消費者沒有意識到非法 OTT TV 機上盒可能成為駭客和網路入侵的載體，進而構成嚴重的網路安全威脅與資安危機，故多數國家也以此做為向民眾政策宣導不要使用非法 OTT TV 機上盒之主要理由。當非法 OTT TV 機上盒上安裝的非法應用程式含有破壞性或侵犯隱私的惡意軟體時，這些惡意軟體使網路駭客和其他不良行為者能夠藉此入侵消費者的家庭網路。物聯網（IoT）的不斷擴展，消費者、企業、醫療保健和運輸部門使用聯網設備大幅增加，再加上某些內部組織網路漏洞，可能導致安全盲點。網路犯罪分子可以利用這些盲點來攻擊物聯網設備（例如：智慧安全攝影機、網路攝影機、智慧

手機、智慧電視、智慧家電或路由器）等，而對個人、產業和公共安全造成威脅。

因此，如何援引有效監理 OTT TV 機上盒，本計畫汲取其他國家作法、相關案例等，以作為我國通訊傳播監理政策、法規及監理技術之參考依據。

第二節　委託辦理工作項目

按計畫書之規劃，本計畫應完成之委託辦理工作項目及執行進度如下表 1。

表 1：本計畫應完成之委託辦理工作項目及執行進度

項次	委託辦理工作項目	執行進度
一	蒐集及分析主要國家及區域組織（包含但不限於美國、歐盟、英國、韓國、日本、新加坡、中國大陸等）網路視聽平臺的發展現況，包含市場現況、政府角色、政策與法規等，尤其對於 OTT TV 機上盒之監理政策、法規以及監理技術。	已完成。 參閱期末報告第二章。
二	蒐集及分析我國及其他國家或區域組織 OTT TV 機上盒涉侵害智慧財產權之實際案例及應處作為（我國：經本會認可至少 3 例；其他國家或區域組織：至少包含 3 個國家或區域組織，至少 5 例）。	已完成。 參閱期末報告第三章。
三	邀集國內專家學者及相關產業舉辦至少 1 場次座談會，每場邀約產官研代表至少各 2 人（合計至少 6 人），介紹及討論 OTT TV 機上盒監理法規與技術之研究成果，並蒐集、研析各界對 OTT TV 機上盒監理法規與技術之建議。	已完成。 共舉辦座談會共 2 場： 第一場座談會：112 年 7 月 31 號下午兩點，邀請專家代表共 7 人。 第二場座談會：112 年 11 月 1 號下午兩點，邀請專家代表共 7 人。 參閱期末報告附錄。

項次	委託辦理工作項目	執行進度
四	針對我國市售可收視未經合法授權節目頻道及隨選視訊之OTT TV機上盒(至少3款，均應為不同廠牌，且款式須經本會同意）進行技術分析，並擬訂監理技術作業流程與方法。另為使本會瞭解前述OTT TV機上盒運作方式，廠商應於契約生效次工作日起第100日內，提供前述OTT TV機上盒各1台（合計至少3台）予本會進行觀測及分析。	已完成。 參閱期末報告第五、六章。
五	提出未來推動OTT TV機上盒監理法規、監理技術、型式認證審驗、後市場管理與防制非法使用智慧財產權等處理、建議、分析與因應作法，並就現行《著作權法》、《電信管理法》、廣電三法及《電信管制射頻器材審驗管理辦法》等提出修法建議，以及就如何強化政府跨部會合作之行政作為，提出具體建議。	已完成。 參閱期末報告第七、八、九章。

資料來源：本計畫整理

第三節　研究方法

一、 法規研究方法

本計畫議題聚焦於OTT TV機上盒法制研析制度作為主軸，並參酌文獻、次級資料及各相關標竿國家之規定，包括：美國、英國、歐盟、韓國、日本、新加坡、中國大陸等重要國家及區域，俾利作為本計畫之基礎；同時，為了解我國OTT TV機上盒監理法制發展需求，將透過座談會方式蒐集業者與專家意見，提出實務上窒礙難行與亟需解決之問題與建議。是故，本計畫之研究方法如下：

（一）文獻分析方法

透過蒐集相關研究文獻，檢視過往文獻並進行客觀地分析、評估。透過相關資料進行蒐集、檢驗與分析後，釐清並理解過去所獲致的結

論中，解釋 OTT TV 機上盒監理法制發展之現況與國際趨勢。本計畫期盼能從文獻資料與各項數位化資料中，進行剖析。

1. 比較法學方法

他山之石，可以攻錯。而美國、英國、歐盟、韓國、日本、新加坡、中國大陸等重要國家及區域的 OTT TV 皆有蓬勃發展，更針對 OTT TV 相關規範有所討論，透過這些標竿國家之法制研究，可作為我國 OTT TV 機上盒監理法制發展之參考。

2. 座談會意見蒐集、分析

本計畫透過專家及業者之深度訪談，蒐集研究所需之意見，並於提出初步可行性方案之後，針對初步研究結果進行討論，提出最可行及最被認可之建議結論。

二、 監理技術研究方法

本計畫議題聚焦於 OTT TV 機上盒監理技術之檢驗程序規劃，主要是對已上市的 OTT TV 機上盒，進行侵權行為之檢驗。因為目前非法機上盒為了逃避查緝，多半採用 Android TV 作業系統，並且以不事先安裝播放盜版影像之應用程式的方式來逃避查緝，而會讓購買者另外下載 App 去收看盜版影音。因此，本計畫主要分析 OTT TV 機上盒業者是否有提供專屬的 App 或應用程式，也就是說，本計畫會檢驗 OTT TV 機上盒是否綁定提供侵權影像的非法 App，並據以建立一套監理技術作業流程與方法，作為日後偵辦侵權案件之準據。

執行方式是針對 App 與機上盒之行為和是否有進行綁定，進行探討與分析，並且歸納出檢測方法。此外，為了落實檢驗管理程序標準化，也會建議在既有機上盒檢測程序外，加入 App 與機上盒之關聯分析程序。本計畫主要之研究方法如下：

（一）App 行為檢測

1. **App 行為分析**：使用動、靜態分析工具分析 App 之動態行為與靜態行為，針對該 App 之刷機、提權、存取動作，分析其侵權之行為是否確實會接收來自非法之訊號並具備播送非法來源影音之功能。而應用程式在執行過程中，可以透過側錄的方式進行傳輸內容擷取，用以分析應用程式與後端伺服器互動之情況，藉此檢驗是否與後端伺服器存在裝置鑑別或裝置綁定等機制，並且取得轉播視訊串流之來源或 CDN 服務位址。
2. **App 程式元件分析**：如透過灌載 apk-extractor.apk 等工具以取出程式。並使用 MobSF 等工具，針對取出之程式進行動靜態分析，以利分析人員針對 App 之組成進行不同的測試，強化針對 App 侵權行為之判斷。也可進一步利用逆向工程工具還原程式原始碼，以協助測試人員解析程式原始碼。惟現今多數應用程式常使用加殼工具，將應用程式加密，令分析原始碼更為困難，此時會需要透過脫殼工具去進行處理。

（二）檢測 App 是否綁定 OTT TV 機上盒

將 OTT TV 機上盒運作、連線過程以如 Wireshark 的封包側錄工具進行封包側錄與分析，以掌握 OTT TV 機上盒於網路上的傳輸使用之協定，並且確立接下來的測試布局及測試規劃。若使用 HTTPS 協定或其他加密傳輸協定，則需要設定代理伺服器，例如：Burp Suite，方能解密並探查其與後端伺服器之請求與回復。這邊要注意的是：萬一 App 有進一步採用憑證綁定等方法，則需要透過 Frida 等工具進行修改。而後，可檢測 App 啟用過程、使用期間有無綁定特定 OTT 機上盒之型號、序號、MAC address、CPUID、Key 等可識別特定機上盒特徵之識別資訊。若存在遠端之裝置鑑別機制，應使用虛擬機或其

他實體機器，安裝相同之應用程式，並觀察其遠端裝置綁定或鑑別機制是否失效，並且嘗試竄改鑑別請求，如使用相同之 MAC Address、CPUID、Key 等鑑別資訊，是否可以使用該應用程式，用以確定該應用程式確實存在裝置綁定之機制，並且不允許其他裝置執行。

第四節　研究範圍

一、 網際網路視聽服務範疇及定義

網際網路之發展已經成為我們生活不可或缺的重要組成，而網際網路的內容、應用程式和服務也爆炸式發展，推動經濟成長並促使資訊自由流動。網際網路之發展使得傳統受廣電法規所管轄之視聽媒體服務（Audiovisual media service），包括：有線電視、無線電視及電影等影音內容，皆可透過網路方式傳輸，進而形成新興視聽媒體，並影響原有視聽媒體市場及監管方向。

由於本計畫主要針對 OTT TV 機上盒之監理進行研析，因此聚焦相關議題時，有必要針對現行各種網際網路視聽服務及名詞加以釐清。目前透過網際網路提供線上影音內容的方式，約略可分為兩大類：第一類是由電信業者以其電信網絡專線（Dedicated network）提供具有品質控管（Quality of service，QoS）之 IPTV（Internet protocol TV），提供包括頻道節目、隨選視訊（Video on demand，VOD）與網路視訊內容的整合服務，使用者透過機上盒與一般電視機即可收視；第二類是由業者提供視聽媒體平臺，透過開放的網際網路傳輸不具品質控管之視聽節目服務，其平臺上之內容可能包括彙集自其他內容提供者（例如電視台、電影業者、廣告業者等）所提供之內容，或由業者自行編排使用者所上傳之內容（User generated content，UGC）[1]。該分

[1] 葉志良(2015)。我國線上影音內容管制的再塑造：從 OTT 的發展談起。資訊社會研究, 29,

類係將透過「網路」傳輸之服務，進一步區分為「電信網路專線」及「開放式網際網路」。為釐清相關架構下各國的規範模式及相關用語，本計畫試將一般常見之網際網路視聽服務之相關名詞彙整如表 2。

表 2：常見之網際網路視聽服務之相關名詞

名詞	特點	例子
網路電視（Internet TV、web TV）	Internet TV 是受許可的專業內容（包括：傳統電視節目、現場活動和電影）的視訊串流。其關鍵特色在於，控制者可以透過許可安排控制使用者的訪問權限，包括：誰可以看到內容（僅限訂閱者）以及可以在何時何地看到內容進行限制。寬頻連接的電視、遊戲機、開放式機上盒、個人電腦、智慧手機和媒體平板電腦等裝置都可以作為被視為網路電視的接收裝置[2]。	MSN TV
隨選視聽媒體服務（On-demand audiovisual media service）	由媒體服務提供商提供視聽媒體服務及節目目錄，在用戶選擇的時刻並根據其個人需求觀看節目[3]。	範圍較大，主要包括：有線電視隨選視訊系統、數位隨選視訊系統及混合式隨選視訊。
視訊分享平臺（Video-sharing platform）	依據歐盟《新視聽媒體服務指令》第 1 條（1）（b）（aa）（參見後述）。	YouTube
OTT TV	透過網際網路向用戶直接提供各項應用服務或內容，不再經過傳統電信、衛星、廣播等，同時不受網際網路連線服務業者（ISP）介入[4]。	Netflix、KK TV、Disney+、Amazon Prime

49。

[2] Gartner Glossary. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary/internet-tv

[3] Directive 2010/13/EU, art. 1(1)(g), OJ L 95.

[4] Alain Busson, Thomas Paris, & Jean Simon. (2016). The European Audiovisual Industry and the Digital Single Market: Trends. Paris: Issues and Policies. DIGIWORLD ECONOMIC JOURNAL, 101, 17.

名詞	特點	例子
		Video、YouTube 等。
IPTV	利用網際網路協定傳送包含電視、影像、聲音、文字及圖片等資料，網路環境則提供必要的服務品質（QoS）、使用體驗（QoE），並具有安全性、互動性和可靠性[5]。 *IPTV 必須建構於可管理的封閉式網路之下。	中華電信 MOD
智慧型聯網電視（Hybrid TV）	可同時連接廣播電視頻道（Broadcast channels）和寬頻網際網路（Broadband internet）、兼顧傳輸效率與資訊多元性、並讓廣播電視節目和網際網路資訊可以無縫融合的新興服務終端平台[6]。	

資料來源：本計畫整理

二、 研究範圍及限制

（一）OTT TV

本計畫主要係針對「OTT TV 機上盒」進行相關法制研析，故有必要針對 OTT TV 進行定義。OTT（Over The Top）一詞源自於籃球用語中的過頂傳球，針對 OTT 目前並未有統一且明確之法規定義，但許多文獻指出其主要透過網際網路向用戶直接提供各項應用服務或內容，而不再經過傳統電信、衛星、廣播等，也不受網際網路連線服務業者（ISP）業者介入[7]。歐盟報告認為任何透過 IP 提供的服務都可以屬於是 OTT，儘管個別服務具有非常不同的特徵[8]。也有認為 OTT 係透過網際網路傳送多樣化媒體內容的媒介，用戶無需訂閱傳統的衛

[5] ITU-T Technical Paper. (2014), Glossary and terminology of IP-based TV-related multimedia services.
[6] European broadcasting union. (n.d.). Principles for Internet Connected and Hybrid Television in Europe. https://www.ebu.ch/files/live/sites/ebu/files/News/2011/A8E39d01.pdf
[7] Supra note 4.
[8] Digital europe. (2017). Response to ITU Consultation on OTTs, Brussels: Digital Europe. http://www.itu.int/en/council/cwg-internet/Pages/consultation-june2017.aspx

星或有線服務[9]。相對於傳統廣播電視及 IPTV 的封閉式傳輸網路受到 ISP 業者之限制較多，OTT TV 則有著完全不受 ISP 業者的介入的特徵，因此，在本計畫中，OTT TV 主要指透過開放式的網際網路傳輸，提供視聽媒體服務至使用者電子終端設備的服務業者。

依據上述定義，目前 OTT TV 的商業模式相當多樣化，可依不同收費模式、經營者之所在地（境內、境外）進行區分，其大部分主要提供隨選視聽服務，但也有部分業者提供線性內容。本計畫的研究重點是將綁定機上盒的 OTT TV 運作模式歸類為 OTT TV 機上盒形式。依據不同付費及內容產製種類，初步將 OTT TV 分類如表 3。

表 3：OTT TV 之平台分類

種類		特色	例子
視訊分享平臺		由使用者自行上傳影音內容，經營者原則上不負內容編輯責任，基本上為免費。	YouTube
視聽媒體服務	訂閱制	內容為專業產製，需要使用者按月/年付費訂閱。	Netflix、Amazon Prime Video、Disney+、HBO Max、Apple TV+
	按量付費制	內容為專業產製，需要使用者按觀看需求單片付費。	Google TV
	免費廣告制	內容為專業產製，使用者可免費觀看。	Line TV、FriDay 影音的部分內容
	提供線性內容	內容為專業產製，部分頻道內容用戶無法進行隨選。	公視+

資料來源：本計畫整理

（二）OTT TV 機上盒

由於網際網路視聽服務主要由業者所提供之機上盒（Set-top box，STB）或智慧型聯網電視，抑或直接透過各種上網設備（如桌上型電

[9] Research and markets. (2016). Global OTT Devices and Services Market 2016-2020. Research and Markets. https://www.technavio.com/report/global-consumer-electronics-global-ott-devices-and-services-market-2016-2020

腦、平板電腦、手機等），隨時隨地自行選擇所欲收視之影音內容[10]。故機上盒最初設計是讓用戶傳輸合法影音內容，其傳輸方式可透過衛星通信網路、固定通信網路、有線電視及開放式網際網路等技術。

市場上普遍存在販賣者或使用者購入機上盒之後，基於機上盒的網際網路連線功能，進行軟體安裝，以接取未經權利人授權之串流媒體網站，進而收視影音內容的情況。透過此類非法串流設備（Illicit streaming devices，ISD），OTT 平臺業者、內容製播業者或權利所有人，遭受嚴重的經濟損失，成為各國亟欲解決之問題。爰此，配合上述 OTT TV 透過網際網路傳輸之特性，本計畫後續所討論之 OTT TV 機上盒均指具有網際網路傳輸功能，進而接收影像、聲音之機上盒。

三、 機上盒在網路視聽平臺非法傳輸之角色

（一）機上盒批發商可能是內容竊取者本身或其下游

依據 Digitalcitizens alliance（2020）[11]，機上盒批發商可能本身是內容的竊取者（Content thief），或者是內容的竊取者的下游進行內容之傳輸。

內容竊取者是從各種合法來源獲取內容的人，包含來自衛星電視、有線電視、OTT TV、藍光光碟或錄影機等直播或隨選內容。他們擷取內容時，可能透過物理、數位、網路等手法竊取訊號，並可能同時透過假造憑證破解來源端保護措施。但無論如何，都必須進行重新編碼、重新傳輸。也就是在擷取內容地須設置「竊訊機房」轉換 IP 數位訊號；境外斷點也須設置 IDC/CDN 機房再配送訊號至非法機上盒。

[10] 江耀國、黃銘輝、葉志良、高文崎 (2011)。多元網路平台環境下影音內容之管理思維 (PG10006-0321)。國家通訊傳播委員會。 https://www.ncc.gov.tw/chinese/files/12022/2716_120222_1.pdf

[11] Digitalcitizens Alliance. (2020). Money for Nothing : The Billion-Dollar Pirate Subscription IPTV Business, 26. https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA-Money-for-Nothing-Report.pdf

簡要圖示，請參閱視聽內容之竊取流程[12]（如圖 1）。

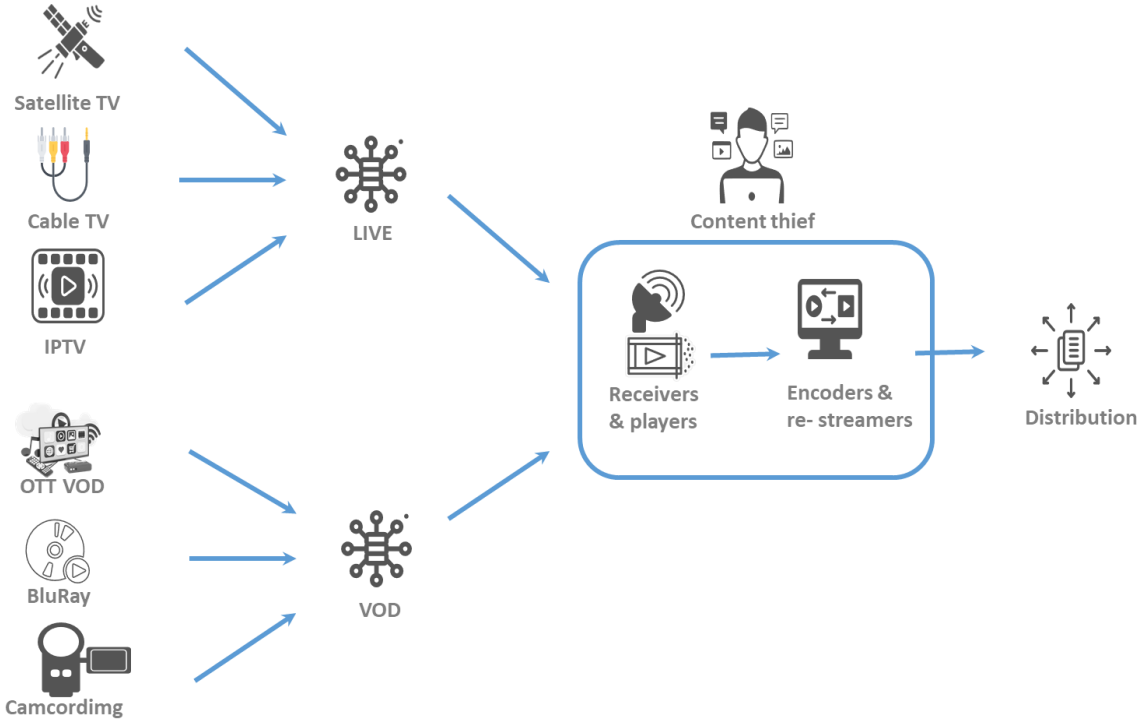

圖 1：視聽內容之竊取流程

資料來源：本計畫整理

（二）產業之利害關係人

機上盒之生產、銷售屬於整個非法視聽內容傳輸之生態系統一環，尚須搭配其他角色，才能完成服務。

1. **內容訊號擷取**：要有內容竊取者及串流訊號技術提供者等。
2. **內容訊號傳輸**：訊號透過雲端傳輸，要有主機/內容傳遞網路（Hosting/CDN）提供者、以及網路代理/虛擬私人網路（Proxies/VPNs）提供者等。
3. **註冊商、註冊管理運行機構**：註冊商（Registrar）與註冊管理運行機構（Registry operator）負責正確解析 IP 位址，而使網站得以訪問。
4. **支付服務**：如果有訂閱制，則有線上金流服務。

[12] Id.

5. 硬體、軟體開發商：設備、應用程式之開發者。

6. 線上廣告商：對線上非法視訊採取廣告獲益模式的業者，提供廣告的業者。但線上廣告商如果沒有事先的黑名單或收到來自權利人、法院之通知，通常無法得知廣告被投放於非法視聽內容中。

7. 銷售商：有批發、零售之線上或實體模式。

8. 聚合商（Aggregators）：負責蒐集非法視聽內容之超連結。

因此，當我們討論如何治理網路視聽平臺非法傳輸內容時，除了針對機上盒進行查緝外，對上述周邊各類業者如何進行調控，也會是切入點。

第二章 各國家、區域組織之網路視聽平臺發展現況

本章從打擊非法 OTT TV 網路視聽平臺和機上盒之角度出發，依據本計畫案委託機關之要求，蒐集主要國家及區域組織，包含：美國、歐盟、英國、韓國、日本、新加坡、中國大陸之網路視聽平臺發展現況，分析其市場現況、政府角色、政策與法規等，尤其對於 OTT TV 機上盒之監理政策、法規以及監理技術等進行研究分析。

第一節 美國

一、 市場現況

從全球角度來看，依據市調機構 Precedence Research 數據顯示，2023 年全球 OTT 市場規模為 2,405 億美元，到 2030 年將擴大到 12,416 億美元左右，2022 年至 2030 年複合年增長率高達 26.42%；北美地區 2022 年在 OTT 市場中佔據最大市場比例，因於 ESPN、AT&T、Crown Family Media Networks、Turner Sports 等服務對於該地區用戶產生極大吸引力[13]。

Parks Associates 國際研究機構的預測顯示，到 2027 年底，美國因盜版而損失之串流媒體收入累計可能超過 1,130 億美元；美國串流媒體電影和電視節目的盜版率預計將從 2022 年的 22%，上升至 2027 年的 24.5%[14]。市調機構 S&P Global Market Intelligence 預計 Netflix、

[13] Precedence Research. (2022). Over the Top (OTT) Market Size, Growth, Report 2022 to 2030. https://www.precedenceresearch.com/over-the-top-market

[14] Advanced Media Strategies LLC. (2023, April 18). Parks: Cumulative US Streaming Revenue Lost to Piracy May Exceed $113 Billion by 2027 Year-End. Piracy Monitor. https://piracymonitor.org/parks-associates-us-streaming-revenue-lost-to-piracy-may-surpass-113-billion-by-2027-year-end/

Amazon 和華特迪士尼公司將佔歐洲地區（包含英國）OTT 市場訂閱總收入的三分之二[15]。

網路盜版問題持續盛行的現狀，也可參閱美國雲端服務廠商 Akamai（Akamai Technologies, Inc.）發佈之研究報告[16,17]。依據美國商會全球創新政策中心近期的資料顯示，電影盜版每年在美國電視和電影業的損失估計至少為 292 億美元，最高可達 710 億美元；非法獲取數位內容消費者中，61.5%是直接通過訪問盜版資源網站以獲取資源，28.6%的人群會主動搜尋盜版內容。

二、 政府角色

美國主管廣電規範之機關為美國聯邦通訊委員會（The Federal Communications Commission，FCC）。傳統上，美國有線電視公司會將其節目與機上盒捆綁在一起提供服務，民眾透過有線電視公司租用機上盒欣賞影音節目。關於美國機上盒之規範討論已久，1990 年代初立法者和監管機構曾多次討論此議題，《1996 年電信法》（Telecommunication Act of 1996）[18]規定 FCC 應制定規則確保製造商、零售商和其他與任何多頻道視訊節目傳輸事業（Multichannel video programming distributor，MVPD）[19]提供給消費者用於訪問多頻道視頻節目的轉換器、交互式通訊設備和其他設備[20]。

為了因應市場變化，FCC 希望授予消費者權力並促進創新，讓消費者有更多選擇並提供更多的內容，FCC 於 2020 年 12 月 4 日公布

[15] S&P Global Market Intelligence. (2023, January 31). Europe: 5 Key OTT Trends to Watch in 2023. https://www.spglobal.com/marketintelligence/en/news-insights/research/europe-5-key-ott-trends-to-watch-in-2023

[16] 資安人(2022, February 11)。Akamai：5 大盜版網站訪問來源為美、俄、印、中 &巴西。https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9710

[17] VdoCipher. (2023, March 14). 12 Video Piracy Statistics, 6 Prevention Methods. https://www.vdocipher.com/blog/2020/10/stop-video-piracy/

[18] Telecommunications Act of 1996, Pub. LA. No. 104-104, 110 Stat. 56 (1996).

[19] 有關多頻道視訊節目(MVPD)請參後述。

[20] 47 U.S.C. § 549(a).

「擴大消費者的視訊訪問選擇；視訊訪問設備的商業可用性」（Expanding Consumers' Video Navigation Choices；Commercial Availability of Navigation Devices）報告和命令[21]，FCC 最初的目的是透過讓第三方公司有能力建立可以使用具有競爭性用戶介面的設備或軟體解決方案以訪問多頻道視頻節目。因此 FCC 在上述報告中提及將試圖針對視訊訪問設備訂立新的規則，包括：規定每個設備必須遵守著作權和錄製限制，以及公共利益要求（如緊急警報），消費者隱私以及兒童節目廣告限制等，同時建立一個由 FCC 監管的機構來處理搜索和安全問題，並要求 MVPD 開發應用程式。惟 FCC 此項提案遭到眾多利害關係者的批評，包括：提案沒有提供有效的方式來保護 MVPD 所擁有的內容，可能使第三方機上盒製造商能夠在沒有足夠授權金的情況下利用 MVPD 的內容；也有論者指出，該提案未解決實際問題，例如制定互操作性標準[22]。爭議至今，FCC 對於機上盒並未提出其他新的規則，針對 OTT 平台規則及 MVPD 之定義也未能更新或有具體規範。

2020 年美國政府責任署（Government Accountability Office，GAO）[23]對 FCC 機上盒監理提出分析報告[24]，從美國之有線、衛星多頻道節目分發服務之市場變化，質疑機上盒的規範之必要性，建議 FCC 從事進一步之市場分析，以評估機上盒規則之必要性。

[21] 47 CFR Part 76.
[22] In the Matter of Expanding Consumers' Video Navigation Choices Commercial Availability of Navigation Devices, Notice of Proposed Rulemaking and Memorandum Opinion and Order (2016, February 18).
[23] Government Accountability Office. (n.d.). Stli. https://stli.iii.org.tw/article-detail.aspx?no=83&tp=4&d=5524
[24] Government Accountability Office. (2017, September 29). Video Programming: FCC Should Conduct Additional Analysis to Evaluate Need for Set-Top Box Regulation. https://www.gao.gov/products/gao-17-785

三、 政策

政策(Policy)一詞並沒有明確的定義，依據 Colebatch，H.(2009)指出[25]：廣泛的方向，如開放政府政策；或常見的作法，如企業的在地採購政策；或特別的承諾，如 2010 年底將汰除類比傳輸改為數位之政策；或是一種價值宣言，如誠實是最佳政策。據此，本小節將整理分析包含來自政府、企業、團體之方向、常見作法、特別承諾或價值宣言。

（一）禁止 OTT 平台帳戶共享

美國 Netflix 2022 年採取用戶支付額外費用，才能與家庭以外的人共享 Netflix 帳戶之政策[26]。透過打擊密碼共享可能增長收入，而其阻止分享密碼的方式，是通過發送到帳戶持有人的電子郵件或短信的代碼、或使用可識別的設備登錄，以驗證用戶身分，一旦用戶無法驗證其身分，就必須支付費用，建立新的子帳戶來添加用戶[27]。

（二）OTT 產業合作、國際合作打擊非法

產業合作（Industry collaboration）與國際合作，為影視娛樂產業採取之打擊侵權政策[28]。超過 50 家的媒體與娛樂公司，包含各大著名公司如 Apple TV+、迪士尼、Fox、Netflix、amazon、BBC studios 等共同組成的「創意與娛樂聯盟」(The Alliance for Creativity and Entertainment，ACE)，在網站首頁標明其為：「世界領先的內容保護聯盟，致力於打擊危害蓬勃發展的數位生態系統的非法數位盜版行

[25] Colebatch, H. (2009). Policy. UK: McGraw-Hill Education.p.4.
[26] Netflix (n.d.)。分享您的 Netflix 帳戶。Netflix 說明中心。 https://help.netflix.com/zh-tw/node/123277
[27] VdoCipher. (2023, March 14). 12 Video Piracy Statistics, 6 Prevention Methods. https://www.vdocipher.com/blog/2020/10/stop-video-piracy/
[28] Advanced Media Strategies LLC. (2023, January 4). 2022 Highlights US: Law Suits and Shut-Downs Are Weapons of Choice. DMCA Update in Progress. Piracy Monitor. https://piracymonitor.org/2022-usa/

為。」[29]ACE 宣稱綜合採用三個方法來解決盜版問題：與世界各地的刑事執法部門合作；對大規模、以營利為目的之數位內容竊取行為，採取針對性的民事執法行動;採用策略性溝通來阻止全球數位侵權[30]。其合作伙伴，包含美國政府之智慧財產權中心（National Intellectual Property Rights Coordination Center）[31]、美國貿易代表、司法部，也及於歐洲刑警組織、歐盟執委會和國際刑警[32]、美國國土安全部和新加坡政府[33]。此外，beIN Media Group、Cavea Plus、MBC Group、United Media、FIFA 及其他媒體行業利益相關者，也是合作對象[34]。ACE 關閉全球主要盜版網站，包括：Nitro IPTV、YMovies、SPARKS Group 以及在巴西、秘魯、北非和泰國等盜版網站[35]。在臺灣，ACE 也透過刑事訴訟使 8maple 的網路營運商被判刑，在新聞稿中，ACE 特別恭賀刑事警察局和桃園地檢署成功起訴、以及桃園地方法院「具有威攝力的判決」[36]，並稱：「對 8maple 的起訴是 ACE 與當地視訊產業和執

[29] ACE (2023 年)。ACE 致力于打击数字盗版 & 保护创意市场。Alliance Creativity and Entertainment。https://www.alliance4creativity.com/zh-CN/

[30] 同註 [29]

[31] National Intellectual Property Rights Coordination Center. (n.d.). Protecting Public Health and Safety. https://www.iprcenter.gov

[32] ACE (n.d.)。关于 ACE。https://www.alliance4creativity.com/zh-CN/about-us/

[33] Advanced Media Strategies LLC. (2023, January 4). 2022 Highlights US: Law Suits and Shut-Downs Are Weapons of Choice. DMCA Update in Progress. Piracy Monitor. https://piracymonitor.org/2022-usa/

[34] 同註 [29]

[35] 同註 [33]

[36] 按本新聞稿所稱之判決為臺灣桃園地方法院 110 年度智易字第 2 號刑事判決，112 年 3 月 30 日。被告陳柏賢及莊坤憲，共同犯《著作權法》第九十二條之侵害著作財產權罪，各判處有期徒刑壹年陸月、有期徒刑壹年陸月。本案係經 Warner Bros. Entertainment Inc.（下稱華納兄弟娛樂公司）、Amazon Content Services LLC（下稱亞馬遜公司）、Disney Enterprises, Inc.（下稱迪士尼公司）、Paramount Pictures Corporation（下稱派拉蒙公司）、Columbia Pictures Industries,Inc.（下稱哥倫比亞公司）、Netflix Studios,LLC（下稱網飛公司）、Universal City Studio Production LLLP（下稱環球公司）、采昌國際多媒體股份有限公司（下稱采昌公司）、三立電視股份有限公司（下稱三立公司）、株式會社 WOWOW（下稱 WOWOW ）、日本電視放送網股份有限公司（下稱 NTV）、富士電視臺股份有限公司（下稱 Fuji TV）、株式會社 TBS 電視臺（下稱 TBS）、史坦利國際傳媒股份有限公司（下稱史坦利公司）訴由內政部警政署保安警察第二總隊、內政部警政署刑事警察局電信偵查大隊偵一隊報請臺灣桃園地方檢察署檢察官偵查起訴。另刑事附帶民事訴訟，臺灣桃園地方法院 110 年度智重附民字第 6 號刑事判決，112 年 3 月 30 日，原告史坦利國際傳媒股份有限公司就：「女力報到-小資女上班

法部門有效合作的另一個例子，它加強了我們減少盜版和保護全球創意內容法律生態系統的承諾。」[37]。同一新聞稿也指出：「在採取執法行動之前，域名 8maple.ru 每月吸引超過 3,000 萬次訪問，每月產生估計 400 萬新台幣（每月 133,000 美元）的廣告收入。當局還估計 8maple 網站給臺灣和國際娛樂業造成了 10 億新台幣(3,330 萬美元）的經濟損失。8maple 為了避免被臺灣當局發現，該網站在五個不同國家維護了 25 個伺服器：法國、烏克蘭、羅馬尼亞、美國和加拿大，該網站此前已在馬來西亞、澳大利亞和新加坡被屏蔽。」[38]由此可知，侵權網站可被多國使用者利用，營運者也會將伺服器設置在海外不同國家以逃避本國查緝，因此，國際合作實有必要，各國政府未必可以直接打擊營運商，需要其他國家協力合作採取相關屏蔽措施。

除了 ACE，國際廣播公司反盜版聯盟（The International Broadcaster Coalition Against Piracy，IBCAP）也是一個在美國由主要廣播公司組成防止未經授權串流或非法傳播國際電視內容的產業聯盟[39]。他們同樣和美國與其他國家政府主管機關合作採取執法措施；也為了識別與阻止未經授權之影視內容傳播，和網路服務提供商（ISP）、支付處理代理、內容傳遞網路（Content Delivery Networks ，CDN）、跨國科技公司以及硬體和軟體製造商合作[40]。

記（第 1 集至第 50 集）」自製之視聽著作向被告陳柏賢、莊坤憲請求損害賠償，法院判決被告連帶給付原告金額為新臺幣肆拾貳萬伍仟元。

[37] ACE (2023 年)。台湾最大盗版网络的运营商面临 18 个月的监禁和近 2 万美元的没收。Alliance Creativity and Entertainment。https://www.alliance4creativity.com/zh-CN/news/operators-of-taiwans-largest-piracy-network-face-18-month-prison-term-and-confiscation-of-almost-usd-2-million/

[38] ACE. (2023, April 11). OPERATORS OF TAIWAN'S LARGEST PIRACY NETWORK FACE 18-MONTH PRISON TERM AND CONFISCATION OF ALMOST USD $2 MILLION. Alliance Creativity and Entertainment. https://www.alliance4creativity.com/news/operators-of-taiwans-largest-piracy-network-face-18-month-prison-term-and-confiscation-of-almost-usd-2-million/

[39] IBCAP(n.d.).THE INTERNATIONAL BROADCASTER COALITION AGAINST PIRACY. IBCAP. https://www.ibcap.org/

[40] 同註 [39]

特別值得注意的是，IBCAP 所採取的「早期和頻繁的打擊行動」政策，透過「自動監控和打擊工具」，「結合 IBCAP 實驗室和法律團隊的專業知識」，使盜版服務的用戶體驗變差，而讓許多用戶轉向合法提供商，這是 IBCAP 對會員提供的重要服務[41]。例如：在今（2023）年 7 月印度板球超級聯賽 IPL 錦標賽期間，IBCAP 代表會員 Willow 和 Cricbuzz，分別在印度和美國設置人員，重點關注機上盒和 IPTV 服務、線性網路（Web linear）、社交媒體和行動應用，成功即時干擾了近 9000 個串流，其中 Facebook Live 串流的觀看次數被干擾了 360 多萬次。IBCAP 稱此次在社交媒體和移動應用上的打擊成功率是 100％！[42]。

IBCAP 對會員提供了「完整且協調」的反侵害智慧財產權服務[43]，詳如表 3。由此可以觀察到，對未經授權傳播內容採取之干預手段，不僅是技術上對各種使用者接觸內容之管道，進行監控與偵測；也須採用法律手段對各種關係人發出濫用或下架通知；並透過各種私人或公開的管道進行調查、情報交換與蒐證。此外，為了主張權利，完成在美國的著作權登記，亦屬重要。同時，也需進行消費者與經銷商的反盜版宣導活動。以上各種服務，IBCAP 可以為會員客製化；且凡是內容所有人、傳播者、體育聯盟、權利人和其他需要反盜版保護的實體都可以成為會員[44]，如表 4。

表 4：IBCAP 會員服務

可提供之服務	包含的項目
監控和偵測（線性頻道）	機上盒（STBs） 網路（Web）

[41] IBCAP(2023, July 18).IBCAP Reports Major Disruption of Piracy in Indian Premier League 2023 Tournament Coverage. GlobeNewswire. https://www.globenewswire.com/en/news-release/2023/07/18/2706474/0/en/IBCAP-Reports-Major-Disruption-of-Piracy-in-Indian-Premier-League-2023-Tournament-Coverage.html
[42] Id.
[43] IBCAP(n.d.).Membership. https://www.ibcap.org/membership
[44] Id.

可提供之服務	包含的項目
	播放清單（Playlists） 行動應用程式（Mobile Apps） Kodi 附加元件（Kodi Add-ons）
監控和偵測（VOD 隨選視訊）	機上盒（STBs） 網路（Web） 行動應用程式（Mobile Apps）
監控與偵測（銷售與行銷領域）	網上零售（Amazon、eBay 等） 社交媒體（Facebook、Twitter 等）
執法	濫用通知（由 IBCAP 實驗室發送） 向 CDN、盜版服務發送下架通知（由律師發送） 向線上零售/社交媒體發送下架通知（由律師發送） 向支付處理器發送下架通知（由律師發送）[45]
調查	私家偵探購買機上盒 本地零售（實體店鋪）調查 開源情報（Open-source intelligence，OSINT）
政府/執法部門	代表 IBCAP 成員進行協調和轉介的好處
資料/情報	可以存取 IBCAP 資料庫、鑑識工作、零售商清單等
報告	美國串流媒體盜版概述 IBCAP 通訊 會員特定報告
訴訟支援	截圖、封包檔案、證詞等。 購買機上盒/證據鏈鏈接。
著作權登記	將外國作品在美國著作權局進行登記
行銷	由 IBCAP 贊助的消費者和經銷商意識宣傳活動的好處 使用由 IBCAP 建立的行銷材料

資料來源：Membership.(n.d.). IBCAP. https://www.ibcap.org/membership

四、 OTT 平台相關法規

美國《1996 年電信法》（Telecommunication Act of 1996）[46]大幅改變了聯邦既有通訊政策及《1934 年通訊法》（Communications Act of

[45] 發送下架通知，主要是依據美國《著作權法》之相關規定，請參閱本報告「第二章第一節五、第二章第一節五、（一）安全港條款及侵權通知、取下」頁 22 以下之說明。

[46] Telecommunications Act of 1996, Pub. LA. No. 104-104, 110 Stat. 56 (1996).

1934）[47]之相關規定。《1996 年電信法》主要目標是放寬對於通訊業務之管制，促進競爭並減少監管，包括：定義「多頻道視訊節目傳輸事業」[48]；允許電話公司提供有線電視服務[49]等，作為美國視聽產業之基礎規範。

依據《1996 年電信法》對於 MVPD 之定義：「包含但不限於有線營運商（Cable Operator）、多頻道多端點經銷服務（Multichannel Multipoint Distribution Service）、直播衛星服務（Direct Broadcast Satellite Service）或僅接收衛星節目經銷商（Receive-only Satellite Program Distributor）等，讓消費者訂閱或購買多個由有線電視系統提供電視頻道之供應事業。」[50]故傳統有線電視頻道節目供應事業、電信公司及廣播衛星均屬之。

為因應網際網路之發展，MVPD 之定義隨著新興媒體之蓬勃發展而有重新定義之必要性。故 2014 年聯邦通訊委員會（Federal Communication Commission，FCC）發起了公眾諮詢（Notice of Proposed Rulemaking，NPRM），提議對 MVPD 之定義進行調整，期望納入提供線性多頻道節目（但不包括隨選視訊）的串流媒體平臺[51]，由於該提案遭到反對，導致命令未受表決，至今美國仍維持對 MVPD 相同之定義。依據現行法規解釋，針對美國 MVPD 中「頻道」（Channel）之定義認為是有線電視系統可用以承載電視頻道的部份電子頻率頻譜[52]。故多以隨選視訊（VOD）服務為主的 OTT TV 業者不在 MVPD 的涵攝範圍之內，因此相較於傳統廣播電視業者，美國對於 OTT TV 業者之管制密度較低。

---

[47] Communications Act of 1934, Pub. L. 73–416, 48 Stat. 1064 (1934).
[48] 47 U.S.C. § 522(13).
[49] 47 U.S.C. § 571-573.
[50] 47 U.S.C. § 522(13).
[51] Fcc. (2014). Commission Adopts MVPD Definition NPRM. https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-210A1.pdf
[52] Id.

五、 OTT TV 機上盒監理政策

（一）安全港條款及侵權通知、取下

「DMCA 512 條款」作為《數位千禧年著作權法》一部分，建立了一個著作權人解決線上侵權問題的系統，包括對合規服務提供商的責任限制（安全港條款），以促進網路服務的發展。立法者最初的意圖是讓著作權人和網路服務提供商合作，以偵查和處理著作權侵權行為。為了符合免受侵權責任的保護條件，服務提供商必須滿足一定的要求，通常包括採取措施來迅速處理線上著作權侵權行為[53]。

但由於服務提供商已收到超過百萬份的侵權通知及多年來發生的技術和商業模式改變，導致了網路生態系統產生變化，美國智財局認為需要進一步研究本條款之合適性，為此，2020 年 5 月 21 日該局發布了針對 DMCA 512 條款之最終報告（Section 512 Report）[54]，並確立了五項重要原則：

1. 線上著作權保護必須具有意義且有效。
2. 誠實善意的網路服務提供商應享有法律確定性和創新的自由。
3. 國會旨在鼓勵網路服務提供商與權利持有人之間的合作，但合作不能是唯一的答案。
4. 在可能的範圍內，政府的決策應該基於證據。
5. 21 世紀的網路政策不可能完全一體適用。

依據 DMCA 512 條款規定，一旦網路服務提供商接獲著作權人發送的侵權通知，在符合一定要件下配合即時移除線上侵權內容，便可進入「安全港」，即可就使用者利用其網路服務所為的侵權行為主

[53] Section 512 Study, https://www.copyright.gov/policy/section512/
[54] U.S. copyright office. (2020). Section 512 Report. https://www.copyright.gov/policy/section512/section-512-full-report.pdf

張免負共同侵權責任，藉此提供誘因，促使網路服務提供商與著作權人合作遏止網路侵權。

（二）特別 301 報告

104 年美國貿易代表署（Office of the United States Trade Representative，USTR）提出的「特別 301 報告」（Special 301 Report）[55]首度指出，包含我國、中國大陸、印尼、馬來西亞、泰國及越南等地相繼出現機上盒侵權問題，惟不僅亞洲地區如此，歐美國家亦陸續因有業者提供民眾使用連結侵權著作的第三方程式或機上盒，而屢屢發生侵權訴訟爭議[56]。

在「2023 年特別 301 報告」中特別指出，在美國提出 2017 年《惡名昭彰市場名單》（Notorious Markets List）所提及，非法串流設備繼續對內容創作者、體育聯盟、現場表演以及合法串流、隨選視訊和 OTT 媒體服務提供商構成直接威脅。同樣，非法的 IPTV 服務透過專門網站門戶和第三方應用非法重發受著作權保護的內容的電信訊號，故目前全球存在許多非法 IPTV 服務，其採取以盈利為目的的訂閱制服務，並擁有龐大而複雜的技術基礎設施。其中，值得注意的國家和地區，包括：阿根廷、巴西、加拿大、智利、中國、瓜地馬拉、香港、印度、印尼、伊拉克、約旦、墨西哥、摩洛哥、新加坡、瑞士、臺灣、泰國、突尼西亞和越南等國家，特別是中國大陸，是這些違法設備主要的製造中心[57]。

---

[55] 美國貿易代表署根據《1974 年美國貿易法》第 182 條之規定，在 301 條款規範下，進行有關智慧財產權的貿易救濟程序，美國貿易代表署都會根據保護和執法狀況進行年度審議並發行一份關於各國保護智慧財產權的狀況的年報，以讓美國政府參照決定是否對不注重智慧財產權保護的國家進行貿易報復。

[56] 張俊宏 (2020 年 8 月)。論非法機上盒侵害著作權之爭議，智慧財產權月刊。260,8。https://pcm.tipo.gov.tw/PCM2010/PCM/ebook/book/260/6/index.html?_ebooktimestamp=638276292101517078

[57] Office of the United States Trade Representative. (2023). 2023 Special 301 Report. https://ustr.gov/sites/default/files/2023-04/2023%20Special%20301%20Report.pdf

報告中列出的每個國家幾乎都能找到損害合法貿易的線上盜版例子，包括：再傳播未經授權的線上直播體育節目訊號；透過逆向工程或駭客攻擊複製基於雲端的娛樂軟體並放入用戶線上播放盜版內容的伺服器，包括盜版線上遊戲；以及線上發布允許繞過技術保護措施的軟體和設備，包括遊戲複製和修改晶片，使用戶可以在實體遊戲機上玩盜版遊戲。因網際網路之發展和線上服務促成的盜版使用，對於無法適用著作權法或未能即時更新規範之國家來說，帶來了獨特的執法和貿易挑戰[58]。

六、 OTT TV 機上盒監理法規

FCC 對於機上盒之定義較為狹隘，認為是消費者訂閱的多頻道視訊節目的主要設備[59]，這樣的解釋，造成如同 OTT TV 平台因不符多頻道視訊節目傳輸事業之定義而不適用廣電相關規範，對於現今播放 OTT TV 的第三方機上盒設備之規範也較為缺乏。

近年來，線上直播和視訊串流已成為消費者接收影音媒體的主要方式，但隨著合法串流市場的增長，也帶動非法串流的增加。而目前美國針對網路盜版和保護智財權之相關法規包括：《保護合法串流法》（Protecting Lawful Streaming Act）[60]於 2020 年通過，在美國法典第 18 章新增第 2319C 條，目的是為了打擊非法串流的盜版行為。該法案增加了對非法串流的刑事處罰，並使提供非法串流服務的供應商（而非用戶）面臨重罪指控。

[58] Id.
[59] In the Matter of Expanding Consumers' Video Navigation Choices Commercial Availability of Navigation Devices, Notice of Proposed Rulemaking and Memorandum Opinion and Order (Feb. 18, 2016).
[60] 18 U.S.C. § 2319C.

另一個主要法源依據為美國《著作權法》（Copyright Act）編入美國法典第 17 章，確保著作人對其原創著作之權利，包括重製、散布、展示、公開演播等。

美國於 1998 年通過《數位千禧年著作權法》（Digital Millennium Copyright Act，DMCA）[61]旨在保護數位環境下的著作權，並對侵犯數位著作權的行為進行懲處。其中，《網路著作權侵權限制法》（Online Copyright Infringement Liability Limitation Act）[62]也稱為「DMCA 512 條款」，為《數位千禧年著作權法》之一部分，此條款確保在網際網路平台（如網站、社交媒體等），不會因用戶上傳的侵權內容而被控侵權責任（安全港條款）。但該規範提供了通知和移除程序，以使著作權人可以要求移除侵權內容[63]。以下就美國與違法 OTT TV 機上盒相關之重要法規分述如下：

（一）《保護合法串流法》

過去針對美國非法串流之犯罪，一直被歸類為輕罪，因此長期以來一直被權利所有者視為是智慧財產權執法不足的問題。而且，該問題時常在美國對外貿易談判時被提及，而貿易談判對手國通常對這種非法串流侵害智慧財產權的違法行為設有更嚴厲的刑罰。美國網路政策工作組（The Internet Policy Task Force，IPTF）於 2013 年發表的一份綠皮書呼籲美國國會對於非法串流侵害智慧財產權之違法行為，應採取和既有《著作權法》中非法複製和傳播刑罰一致的措施[64]。

爰此，美國於 2020 年 12 月 27 日通過《保護合法串流法》，新增的美國法典第 18 章第 2397c 條（18 U.S. Code § 2319C），大幅增加對

[61] Pub. L. 105-304.
[62] Pub. L. 105-304.
[63] 17 USC § 512.
[64] Department of commerce internet policy task force. (2013). Copyright Policy, Creativity, and Innovation in the Digital Economy. https://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf

故意且出於商業優勢或私人經濟利益而非法串流侵害智慧財產權之違法行為的刑事處罰。根據本法，美國司法部可以對提供（而非使用者）此類非法服務的人士提出重罪指控。

該條主要規範內容如下，標題為「非法數位傳輸服務」（Illicit Digital Transmission Services），列舉了加重處罰的禁止行為和條件。包括：必須 1.具有故意；2.出於商業優勢或私人經濟利益的目的；以及 3.向公眾提供或提供數位傳輸服務[65]。

其中，「數位傳輸服務」被定義為「主要目的是通過數位傳輸公開演播著作的服務」（the term 'digital transmission service' means a service that has the primary purpose of publicly performing works by digital transmission）。所禁止的數位傳輸服務是下列三者之一：

1. 主要的設計或提供是為了不經著作權人或法律之授權，以數位傳輸公開演播受著作權保護的著作。
2. 除不經著作權所有人或法律之授權以數位傳輸方式公開演播受著作權保護的著作之外，沒有商業上重要的目的或用途。
3. 故意由該人或在該人指示下推廣其使用於不經著作權所有人或法律之授權以數位傳輸方式公開演播受著作權保護的著作。

刑度上與《著作權法》上侵害重製和散佈權相當。如所犯涉及「準備用於商業公開演播之著作」（works being prepared for commercial public performance），還會加重其刑。例如，預映和新上映的電影以及現場直播的體育賽事[66]。多次違法者，亦同。

---

[65] 18 U.S.C. § 2319C.

[66] Kevin madigan. (2021, January 12). Protecting Lawful Streaming Act Signed Into Law: What You Need to Know. Copyright Alliance. https://copyrightalliance.org/protecting-lawful-streaming-act-signed/

舉體之規定，在 18 U.S. Code § 2319C (c) ：「罰則——任何違反 (b) 款的人，除了根據第 17 章或任何其他法律規定的處罰外，還應處以——

(1)根據本章處以罰款，不超過 3 年監禁，或兩者併罰；

(2)根據本章處以罰款，不超過 5 年監禁，或兩者併罰，如果 ——

(A)犯罪行為與正在準備用於商業公開演播的一部或多部著作有關；和

另 18 U.S. Code § 2319C（d）明文規定，上述的處罰均不得解釋為（1）影響民事《著作權法》任何其他條款的解釋，包括第 17 章第 512 條規定的責任限制或間接責任原則；或者（2）阻止任何聯邦或州當局執行不受第 17 章第 301 條規定優先權的電纜盜竊或服務盜竊法律。

（二）著作權相關法規

美國《著作權法》確立了著作權所有人的權利，並對侵犯著作權的行為進行規範和處罰。有關非法串流可能涉及之《著作權法》相關規範，參考美國回覆 APEC 調查報告，整理如表 5；除第 506 條規範刑罰外，其他均為民事責任；而對於生產、銷售非法串流機上盒之人，美國回覆意見認為可能不構成著作權之直接侵害，但依情況可成立間接侵害[67]，參照如表 5。

表 5：非法串流可能涉及之美國《著作權法》相關規範

條號	內容
17 USC § 106（受著作權保護之客體）	除第 107 條至第 122 條另有規定外，著作權人依本法享有行使或授權下列事項之排他權： （1）重製受著作權保護的著作，包括製作複製品或音樂錄製品。 （2）基於其有著作權之著作，改作為衍生著作。 （3）以銷售或其他所有權之移轉、或出租、出借等方式，對公眾散布其有著作權之著作之重製物或影音著作。 （4）就文學、音樂、戲劇、舞蹈、默劇和電影等影音著作，公開演出其有著作權之著作。

(B)該人知道或應該知道該作品正在為商業公開演播而準備；和
(3)如果該罪行是本條或第 2319(a) 條規定的第二次或後續犯罪，則根據本章處以罰款，不超過 10 年監禁，或兩者併罰。

[67] Fowler, P. N., Office of Policy and International Affairs, & United States Patent and Trademark Office. (2021). Report on Results of Survey Questionnaire on Domestic Treatment of Illicit Streaming Devices by APEC Economies (IPEG 01 2020S). Asia-Pacific Economic Cooperation Secretariat. https://www.uspto.gov/sites/default/files/documents/APEC-DomesticTreatmentofISDs.pdf, pp.153–154.

條號	內容
	（5）就文學、音樂、戲劇、舞蹈、默劇和圖畫、圖形或雕塑著作，包括影音著作中的個別影像，在公開場所展示該受著作權保護的著作。 （6）就音樂錄製物，通過數位音頻傳輸的方式向公眾進行公開表演該受著作權保護的著作。
17 USC § 501 （侵害智慧財產權之訴因）	（a）任何違反第 106 至 122 條或違反第 106（a）條所享有之著作排他性權利，或違反第 602 條將複製品或影音著作進口到美國的行為，視情況將視為著作權或作者權利的侵權者。 （b）享有著作權排他性權利之法定權利人或其受益人，於其享有該項權利期間內，有權依第 411 條規定，就任何侵害其特定權利之行為提起訴訟。法院得命權利人依據著作權局或其他機構之檔案，以書面副本將訴訟事項通知具有或主張著作權利益之人，並應要求其將此一通知送達任何將因本案判決而利益受影響之人。法院並得准許任何主張在著作權上具有利益之人參與訴訟。 （c）有線系統在具體表現（embody）著作之表演或展出之二次播送，依第 111 條第（c）項之規定為可起訴之侵權行為。電視台擁有著作權或其他授權而播送或表演相同版本之著作，基於本條第（b）項之目的，如此二次播送係發生在該電視台之地方服務區域內，則電視台應被視為法律上之權利人或受益人。 （d）有線系統之任何二次播送，依第 111 條第（c）項第（3）款之規定，係屬可提起訴訟之侵權行為，下列之人亦得提起訴訟：（i）節目被有線系統變更之原播送者；以及（ii）二次播送發生於其地方服務區域內之該廣播電台。 （e）將具體表現著作之表演或展示之一次播送經由衛星載波台所為之二次播送，依第 119 條第（a）項第（5）款之規定，係屬可提起訴訟之侵權行為。具有著作權或其他授權而播送或表演該著作相同版本之播送網電台，當此種二次播送發生於該電台當地服務區域內時，基於本條第（b）項之目的，該電視台應被視為法律上之權利人或受益人。 （f）（1）將具體表現著作之表演或展示之一次播送經由衛星載波台所為之二次播送，依第 122 條之規定，係屬可提起訴訟之侵權行為。具有著作權或其他授權而播送或表演該著作相同版本之電視廣播電台，當此種二次播送發生於該電台當地服務區域內

條號	內容
	時，基於本條第（b）項之目的，該電視台應被視為法律上之權利人或受益人。 （2）電視廣播電台得依《1934 年通訊法》第 122 條（a）項（2）款之規定向拒絕載送電視廣播訊號之衛星載波台提起民事訴訟。
17 USC § 502 （禁制令）	（a）對依本法規定提起之民事訴訟有管轄權之法院，得依第 28 冊第 1498 條規定，在可認為合理之條件下，簽發暫時性及終局性之禁制令（injunction），以預防或制止對著作權之侵害。 （b）前項之禁制令得送達給在美國境內任何地方之禁止命令當事人；此一禁止命令在全美國境內應是有效之，並且任何對諸當事人具有管轄權之美國法院，得藉由藐視法庭罪及其他方式，使其得以強制執行。當任何其他法院要求執行禁止命令時，簽發禁止命令之法院書記官應即檢送其機關中存檔之本案所有文件副本。
17 USC § 504（b）、17 USC § 504（c）（1） （損害賠償）	（b）實際損害賠償與利益：著作權人有權利請求返還因侵權行為所生之損害，及侵權行為人因侵權行為所得且未列入實際損害計算之利益。於確定侵權行為所得之利益時，著作權人僅須舉證證明侵權行為人所得之利息，同時侵權行為人則應證明其得扣除之費用，以及源自受著作權保護著作以外之因素所生之利益。 （c）法定損害賠償額：（1）除本項第（2）款之規定外，著作權人於終局判決前之任何時間，得選擇法定損害賠償及利益，以代替實際損害賠償與利益。本訴訟所涉及之所有侵權行為之法定損害賠償，任何一位侵權行為人皆應個別負擔該項損害賠償責任，或任何兩個或兩個以上之侵權行為人應連帶或單獨負損害賠償責任。就每一件著作，法院得在總額 750 元以上 30,000 元以下之範圍內作認為適當之裁判。為實現本款所規定之目的，編輯著作與衍生著作之所有部分，構成一件著作。
17 USC § 506（a）（1）（A） （基於商業或私人經濟利益之刑事犯罪）	（a）刑事處罰 一般情況：若有人故意侵犯著作權，且侵權行為是為了商業利益或私人經濟收益，將根據《美國法典》第 18 第 2319 條之規定予以懲罰。

條號	內容
17 USC 1201(a)(2)（3）和（b）（1）（規避智財保護之技術）	（2）任何人皆不得製造、進口、允諾提供、提供或是運送任何以下規定之科技、產品、服務、裝置、組件或零件：（A）其主要設計或製造之使用目的係為規避本條所欲保護之科技保護措施（B）其主要商業價值僅於為規避科技保護措施，以取得（接觸）本條所欲保護之著作；（C）其個人及其他相關人行銷之方式，係為使他人得以規避科技保護措施，以取得（接觸）本條所預保護之著作為目的。 （3）此一條文所謂（A）規避科技保護係指在未經著作權人同意下，重組或解碼以分組或鎖碼方式保護之著作，或是以避開、移除、迴避、解除或破解著作權人之科技保護措施取得著作之方式；（B）科技保護措施，係指有效限制他人取得著作之科技方式，在著作權人同意下以資訊之透露、科技處理之方式使他人得以取得著作之裝置。 （b）其他侵權行為—（1）任何人皆不得製造、進口、允諾提供、提供或是運送任何以下規定之科技、產品、服務、裝置、組件或零件：（A）其主要設計或製造之使用目的係，為規避本條所欲保護著作權人之權利，所預備之科技保護措施；（B）其主要商業價值僅於為規避科技保護措施，以取得（接觸）本條所欲保護之著作權人之權利；（C）其個人及其他相關人行銷之方式，係為使他人得以規避科技保護措施，以取得（接觸）本條所欲保護之著作權人之權利為目的。 （2）此條文所謂（A）規避著作之科技保護方法，係指在未經著作權人同意下，重組或解碼以分組或鎖碼方式保護之著作，或是以避開、移除、迴避、解除或破解其科技保護方法以及；（B）一種有效保護著作之科技方法，係指在一般使用情況下，避免、禁止或限制使用著作權人之權利，以達到有效保護著作權人權利之方法。

資料來源：REPORT: Domestic Treatment of Illicit Streaming Devices by APEC Economies 153 Appendix 4T United States of America, pp.153-154；美國法典。

（三）其他刑事法規

非法串流機上盒還可能涉及之刑事責任，請參閱

表 6。

表 6：非法串流機上盒可能涉及之其他刑事責任

規範分類	條號及內容
刑事	18 USC § 2319（b）（3）（侵犯智慧財產權的刑事犯罪）（複製及傳播） 18 USC § 2（協助、教唆、慫恿、指揮、誘導或促成） 18 USC § 2320（販運假冒商品或服務） 18 USC § 541（錯誤分類貨物入關） 18 USC § 542（謊報貨物入關） 18 USC § 545（走私貨物）
海關	19 USC § 1595a（C）（2）（c）（協助非法進口之扣押） 19 CFR § 133.42-43（行政規則，侵權複製品或影音製品）
競爭法	15 USC § 45（a）（1）（不公平競爭）

資料來源：REPORT:Domestic Treatment of Illicit Streaming Devices by APEC Economies 153 Appendix 4T:United States of America, p.153；美國法典。

（四）案例

以下藉 Bill Omar Carrasquillo 的案例來觀察行為人應負的法律責任。本案發生在《保護合法串流媒體法》之前，合先敘明。

依據新聞報導[68]，Carrasquillo 一開始是從亞馬遜上購入預先安裝好的 Kodi 機上盒，進行轉售。之後，他自行開發 Gears TV 應用程式，提供非法 IPTV。Gears 應用程式採訂閱制，所有頻道每月 10-15 美元，雖然他之後將應用程式賣給他人，但仍然可以分潤。他提供非法 IPTV 的方法是先付費取得有線電視服務，然後，用影片編碼器（將訊號、資料、聲音、影像等訊息以特定的編碼方式轉換為數位或模擬信號），編碼器就像捕獲卡（擷取計算機或多媒體系統中的視頻或音頻信號並輸入到電腦中的硬體設備），爾後建立了一個 VPN 私人網路。他透過

[68] Maxwell, A. (2020, January 4). Omi in a HELLCAT: Selling drugs to making "$200K a day" From pirate IPTV. TorrentFreak. https://torrentfreak.com/omi-in-a-hellcat-selling-drugs-to-making-200k-a-day-from-pirate-iptv-200104/

YouTube 銷售，並與使用者透過社交媒體 Facebook、Discord 等等溝通。而帳務則是透過 Stripe、BOAMS、EMS、Nuvei 和 Worldpay 等取得，此等帳戶是透過向處理者以及在某些情況下向其銀行合作伙伴虛假申報 IPTV 服務的性質及其所有者的身分獲得的。此外，他以 YouTuber 身分報稅時，也有虛假申報等問題。在 2019 年，Gears TV 被政府關閉。

2022 年 2 月 1 日，他與政府的認罪協議，承認了如下罪名[69]：

1. 從 2016 年 3 月到 2019 年 11 月 23 日，共謀犯下重罪和輕罪侵犯著作權、規避訪問控制、訪問裝置詐欺和電信詐欺，違反了 18 U.S.C § 371。
2. 從 2016 年 3 月到 2019 年 11 月 23 日，規避訪問控制裝置，違反了 17 U.S.C § 1201（a）（1）（A）、§ 1204（a）（1）條和 18 U.S.C § 2。
3. 從 2019 年 5 月 24 日至 2019 年 11 月 20 日，重製受保護的著作，違反 17 U.S.C § 506（a）（1）（A）和《美國法典》18 U.S.C § 2。
4. 在 2019 年 2 月 11 日至 2019 年 11 月 20 日期間，公開演播三部受保護著作（透過串流），違反了 17 U.S.C. § 506（a）（1）（A） and 18 U.S.C. § 2319（b）（3）and 2（Counts 4, 13, and 18）。
5. 從 2018 年 6 月 6 日到 2019 年 6 月 5 日 8 的訪問裝置詐欺，違反 18 U.S.C. § 1029（a）（2）,（c）（1）（a）（i）and 2。

[69] Maxwell, A. (2023, February 28). U.S. govt: Omi in a Hellcat should serve 15.5 years for pirate IPTV scheme. TorrentFreak. https://torrentfreak.com/u-s-govt-omi-in-a-hellcat-should-serve-15-5-years-for-pirate-iptv-scheme-230228/

6. 2016 年 3 月至 2019 年 11 月 23 日針對受害者有線電視公司的電信詐欺計劃，違反了 18 U.S.C. § 1343。
7. 2019 年 6 月 14 日向銀行提供虛假陳述，違反了 18 U.S.C. § 1014 and 2。
8. 2018 年 12 月 20 日，參與了來自特定非法活動（洗錢）的貨幣交易，違反 18 U.S.C. § 1957。
9. 虛假陳述，違反 18 U.S.C. § 1001。
10. 逃稅，違反了 26 U.S.C. § 7201。

此外，Carrasquillo 同意沒收從他的銀行賬戶中扣押的 5,895,507.76 美元的現金，沒收 50 多輛汽車和近 50 處不動產。也同意對他從 Gears TV 收到的所有收益進行沒收金判決，並向受害者支付法院命令的賠償金[70]。

上述認罪協議所列的罪刑可達 500 多年監禁。在 2023 年 3 月，法院判處 66 個月，且認為此已足以懲罰 Carrasquillo 並向追隨者發出威懾訊息；此外，經各方同意，電視公司一起獲得 10,761,573.20 美元賠償；美國國稅局獲得 5,717,912.02 美元的賠償。[71]

七、 OTT TV 機上盒監理技術

關於美國對非法機上盒之監理技術，依據美國近期之判決[72]所示，採用了對 ISP 之封鎖禁制令、阻止第三方公司有任何業務往來等措施。

---

[70] Id.

[71] Maxwell, A. (2023, March 8). Omi in a Hellcat handed 66 months in prison for pirate IPTV, forfeits $30m. TorrentFreak. https://torrentfreak.com/omi-in-a-hellcat-sentenced-to-66-months-in-prison-for-iptv-scheme-forfeits-30m-230308/

[72] Andy Maxwell, May 2022. US Court Orders Every ISP in the United States to Block Illegal Streaming Sites. 在此文中提供了三個判決與禁制令之下載連結，分別是：UNITED KING FILM DISTRIBUTION LTD, et al. v. DOES 1-10 d/b/a ISRAEL.TV, S.D.N.Y., Case No. 1:21- cv-11024 (KPF) (RWL), April 26, 2022, https://torrentfreak.com/images/1-21-cv-11024-United-King-v-Israel-tv-judgment-injunction-220426.pdf; United King Film Distribution Ltd et al v. Does 1-10, d/b/a Israeli-TV.com, S.D.N.Y., Case No. 1:21- cv-11025 (KPF) (RWL), April 26, 2022, https://torrentfreak.com/images/1-21-cv-11025-United-King-v-Israel-tv-judgment-injunction-220426.pdf; United King Film Distribution Ltd et al v. Does 1-10 d/b/a Sdarot.com, S.D.N.Y., Case

這判決的起源是美國 United King Film Distribution、DBS Satellite Services、Hot Communication 在美國紐約南區地方法院，分別向盜版串流網站 Israel-tv.com、Israel.tv 和 Sdarot.tv 起訴著作權侵害。被告並沒有出庭，原告勝訴，除了如一般侵權判決獲得賠償金及對被告禁止侵權外，特別值得注意的是法院對 ISP 及其他第三方之禁制令。

（一）對 ISP 之封鎖禁制令

三件判決之禁制令對象是在與本案可能相關之所有的 ISP 業者、以及其他有在美國提供服務的 ISP。該禁制令將相關 ISP 業者表列於附件 B，共有 100 家，但法院於禁制令中指出命令所及之範圍包括但不限於附件 B 所列之業者，意即可觸及所有已知之違法域名之 ISP 業者皆有適用。禁制令要求此等 ISP「應透過其系統中可用的任何技術手段，封鎖對今天已知的任何域名地址的網站接取（包括但不限於附件 A 中所列）或是未來由被告使用的域名地址（新檢測到的網站）。」據此，法院並未指明或限制 ISP 所採用的技術手段，但要求達到對已知或未來由被告使用域名地址之封鎖效果。

法院並指出：「這些域名地址和任何新檢測到的網站應以一種方式進行通道管理，以使用戶無法連接和/或使用該網站，並且將被 ISP 的 DNSserver 伺服器重定向到原告經營和控制的登錄頁面（登錄頁面）。」

登錄頁面之域名與 IP 地址也被載明[73]，登錄頁面也被命令包括以下基本資訊，以 S.D.N.Y., Case No. 1：21- cv-11025（KPF）（RWL）為例：「在 2022 年 4 月 26 日，就 United King Distributors 等人對 Does1-

No. 1:21- cv-11026 (KPF) (RWL), April 26, 2022, https://torrentfreak.com/images/1-21-cv-11026-United-King-v-Israel-tv-judgment-injunction-220426.pdf.

[73] 三個案件，分別是：S.D.N.Y., Case No. 1:21- cv-11024 (KPF) (RWL): Domain: zira-usa-11024.org, IP Address: 206.41.119.64 (專用); S.D.N.Y., Case No. 1:21- cv-11025 (KPF) (RWL): Domain: http://zira-usa-11025.org, IP Address：206.41.119.81(專用); S.D.N.Y., Case No. 1:21- cv-11026 (KPF) (RWL): Domain: zira-usa-11026.org, IP Address: 206.41.119.50 (專用).

10，亦即 Israeli-tv.com（位於紐約南區聯邦地區法院，案號 1：21-cv-11025（KPF）（RWL）提起的訴訟中，美國紐約南區聯邦地區法院基於侵害著作權發布命令封鎖對該網站/服務的所有訪問。」[74]

（二）阻止第三方公司和非法營運商有任何業務往來

封鎖禁制令也禁止任何第三方公司，在其當前域名或任何新域名上與網站開展任何業務。法院「進一步命令，所有為被告的運營提供服務的第三方，包括但不限於 ISP 業者、網站託管提供商、CDN 服務提供商、DNS 服務提供商、VPN 服務提供商、域名購買服務、域名隱私保護服務、後端服務提供商、聯屬計劃提供商、網頁設計師、託運者、基於搜索的線上廣告服務（例如通過付費包含、付費搜索結果、贊助搜索結果、贊助鏈接和網際網路關鍵詞廣告）、任何銀行、儲蓄和貸款協會、商戶帳戶提供商、支付處理和提供商、發卡組織或其他金融機構，包括但不限於 PayPal，以及任何已為被告和及侵權網站（包括但不限於所附的列表並作為附件 C 展示）提供服務的服務提供商（各自稱為「第三方服務提供商」），得悉本命令，無論是透過服務、實際通知還是其他方式，均被永久禁止向該網站（通過本附件 A 中列出的任何域名，或在任何新發現的網站上）提供服務，或與本文（A）（1）至（A）（6）項所述的任何行為相關的被告提供服務。」[75]

接著，法院對註冊商與註冊處（Registrars and Registries），做出如下的命令：

1. 所有與侵權網站相關的域名，包括但不限於本附件 A 中列出的那些，以及任何新發現的網站，應轉讓給原告所有權和控制。

[74] 命令原文是:"On April 26, 2022, in the case of United King Distributors, et al. v. Does 1-10, d/b/a Sdarot.tv (S.D.N.Y., Case No. 1:21- cv-11026 (KPF) (RWL)), the U.S. District Court for the Southern District of New York issued an Order to block all access to this website/ service due to copyright infringement" 其他二件判決之頁面資訊僅案號、當事人不同。

[75] 見 S.D.N.Y., Case No. 1:21- cv-11024 (KPF) (RWL); S.D.N.Y., Case No. 1:21- cv-11025 (KPF) (RWL); S.D.N.Y., Case No. 1:21- cv-11026 (KPF) (RWL).

2. 根據本法庭的固有公平權力和強制執行合法命令的權力，由於被告持續進行其偽造活動，如果原告確認任何被告註冊或運營的新發現網站，並且與串流媒體傳輸原告的任何著作相關，包括：使用含有原告服務標誌或與之相似的域名的網站，原告將繼續有權將本命令傳遞給域名註冊處和/或個別註冊商，後者持有和/或列出與新發現網站相關的一個或多個域名；以及域名註冊處和/或個別註冊商持有和/或列出與新發現網站相關的一個或多個域名，應在本命令副本送達後的 7 天內，暫時停用與新發現網站相關的任何域名，使其失效，並以使用戶無法連接和/或使用該網站的方式進行通道管理，並將用戶重定向到上述的登錄頁面（如上文 B 段所定義）。
3. 在本命令送達後的 30 個工作日之後，註冊處和/或個別註冊商應向原告提供所有新發現網站的聯繫訊息；原告所選擇的註冊處應將與新發現網站相關的任何域名轉讓給原告所有權和控制，除非被告已向法庭提出並向原告的律師送達要求將此類新發現網站免除本命令的請求，或除非原告要求解除而非轉讓與新發現網站相關的域名。
4. 任何被告可在提前 2 個工作日書面通知法庭和原告律師的情況下，根據適當的證明，出庭並申請解除或修改有關限制轉讓屬於或受任何被告控制的新發現網站的域名的規定。

（三）原告停止對 ISP 執行禁制令

但在上述判決做成的一個多月後，2022 年 6 月，原告向法官提出一封信：「原告正在努力對（禁制令涵蓋的）非當事人之註冊商與註冊處以及每項命令中（列出的）服務提供者執行命令。」「原告希望，由於這些努力，被告侵犯原告著作權之盜版內容之串流將受到限

制。因此，可能沒有必要對 ISP 強制執行命令。」原告乃要求法院不要對美國的每個 ISP 執行封鎖令，法院因此暫停並要求等待法院進一步的命令[76]。

看來，似乎特別是針對域名註冊商和註冊商的命令已足，而沒有必要遮蔽網路和域名[77]。

第二節　歐盟

一、市場現況

依據歐洲視聽反盜版聯盟（Europe's Audiovisual Anti-Piracy Alliance，AAPA）數據顯示，2021 年歐洲非法 IPTV 提供商的年收入約 10.6 億歐元，而視訊媒體行業的年收入損失約 32.1 億歐元。其中，義大利視聽和多媒體產業保護聯合會（Italy's Federation for the Protection of the Audiovisual and Multimedia Industries，FAPAV）數據顯示，體育賽事直播的非法收益就高達 2.67 億歐元[78,79]。

歐盟智慧財產局（European Union Intellectual Property Office，EUIPO）的研究報告指出，非法的市場運營商有幾種營業方式：客戶支付每月訂閱費、經銷商利用 IPTV 經營非法業務，或是蒐集非法串流媒體網站並提供消費者；且市場上的非法 IPTV 網站有傳播惡意軟

[76] Andy maxwell. (2022, June 6). Court Orders For All US ISPs to Block Pirate Sites Have Been Suspended. TF. https://torrentfreak.com/court-orders-for-all-us-isps-to-block-pirate-sites-have-been-suspended-220606/

[77] Chris cooke. (2022, June 7). Movie Companies Who Got a US Web-Block Order Have Asked for It to Be Stayed. CMU. https://completemusicupdate.com/article/movie-companies-who-got-a-us-web-block-order-have-asked-for-it-to-be-stayed/

[78] Advanced Media Strategies LLC (2023, January 3). 2022 highlights Europe: Rights-holders lean on law enforcement. New regs passed against piracy. Piracy Monitor. https://piracymonitor.org/2022-europe/

[79] 2023 年體育廣播公司 DAZN，以 2021 年以來體育直播盜版行為增加了 26%，敦促意大利參議院投票禁止非法直播行為。但完成投票幾天後 DAZN 即調漲 2023-2024 年足球賽季價格，標準套餐上漲 1/3，Plus 套餐上漲 37%。評論認為 DAZN 漲價可能會促使消費者轉向非法網站，參見 Italy's 2023 Live Broadcast Anti-Piracy Bill: Unintended Consequences? (2023, July 24). Piracy Monitor. https://piracymonitor.org/italys-2023-live-broadcast-anti-piracy-bill-unintended-consequences/

體的技術能力，例如可在機上盒裝置惡意軟體，使非法集團蒐集用戶個人數據[80]。

二、 政府角色

歐盟智慧財產局（EUIPO）負責管理歐盟商標註冊、智慧財產權領域的歐洲和國際合作，以及侵犯智慧財產權等事項。其與歐盟刑事司法合作機構（Eurojust）合作「智慧財產權犯罪計畫」（Intellectual Property Crime Project）[81]加強合作並確保對整個歐盟智慧財產侵權行為採取更加一致和強而有力的應對措施，同時也進行打擊非法串流媒體及組織犯罪集團的工作與政策。

歐盟《執法指令》[82]要求歐盟成員國向權利人提供對中介機構終止或防止侵害之禁令，但如何執行，則由各國自行立法定之。大部分的歐盟國家都採用司法程序，但西班牙、義大利、希臘、立陶宛等採用行政程序[83]。

以義大利為例，由電信管理局 AGCOM（Autorità per le Garanzie nelle Comunicazioni，AGCOM）執行，此為一獨立的行政機構；所處理之著作權與相關權利侵權，包含：網路侵權；一般產品、元件、服務之侵權；透過廣告、促銷、說明之侵權；且對據稱存在迫在眉睫、嚴重和無法彌補的傷害威脅，有快速通道程序[84]。所採取的措施，依據託管伺服器是否位於義大利有別，如果是在境內可選擇刪除及其他防止上傳措施；如果是在境外，則於「大規模侵權」（Massive

[80] ILLEGAL IPTV IN THE EUROPEAN UNION. (2019). Economic, Legal and Technical Analysis Report, 26–27. https://doi.org/10.2814/28041
[81] Intellectual Property Crime Project. (n.d.). European Union Agency for Criminal Justice Cooperation. https://www.eurojust.europa.eu/intellectual-property-crime-project
[82] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1.
[83] Illegal IPTV in the European Union. (2019). European Union Intellectual Property Office. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf, p.47.
[84] Id., p.50.

infringement）時，AGCOM 會列出應禁止的外國網站，命在國內經營的接取供應商（Access provider）限制從義大利去訪問該著作或連結該著作；而依據 2019 年資料，已有 700 多個域名被列入黑名單，權利人對此程序的速度與執行的潛在規模，反應良好[85]。AGCOM 主要法源依據為 2013 年底發布之《電子通訊網路著作權保護規則》（Regulation on copyright protection on electronic communications networks），權利人可依規則請求 AGCOM 刪除被侵權之數位內容。AGCOM 在收到請求之日起 7 天內正式通知 ISP 業者、網站管理者和上傳者，業者可以自發性刪除該內容。對於外國網站，該規則規定，當伺服器位於義大利境內時，機構可命令託管提供者選擇性刪除內容；如果發生大規模侵權，AGCOM 可以透過命令禁止存取網頁，而非刪除[86]。2023 年 7 月 24 日，義大利通過第 93/2023 號法律[87]，並於 2023 年 8 月 8 日生效，該法旨在打擊盜版以及預防和制止透過電子通訊網路非法傳播受著作權保護的內容，該法賦予 AGCOM 有權採取緊急措施，迅速採取行動，封鎖以電影作品首映、體育賽事和社會關注活動等非法傳播直播內容的網域和 IP 位址，故 AGCOM 相關執法措施及緊急措施皆需要相關法令之支持。

[85] Illegal IPTV in the European Union. (2019). European Union Intellectual Property Office. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf, p.50.

[86] D&P Studio Legale, The Italian regulation against on line copyright piracy is valid: the decision of the Regional Administrative Court of Lazio, April 12 2017, https://www.lexology.com/library/detail.aspx?g=dffbee3b-b0a1-4a37-886d-8ab886062c19

[87] Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica. (23G00103), https://www.gazzettaufficiale.it/atto/vediMenuHTML?atto.dataPubblicazioneGazzetta=2023-07-24&atto.codiceRedazionale=23G00103&tipoSerie=serie_generale&tipoVigenza=originario&action=select-all

三、政策

（一）國際合作打擊犯罪

OTT 相關產業結合國家警察以及國際刑警組織共同執行的國際合作打擊犯罪政策。例如：義大利警察機構抓捕擁有九十萬名訂戶的非法傳播足球比賽之 OTT 網站。此外，LaLiga 西班牙足球甲級聯賽採用自行開發的反盜版平台，並與西班牙國家警察總隊（National Police Corps）與歐洲刑警組織聯合行動，逮捕了四名非法 OTT 網站營運商，這網站包含超過兩千六百個電視頻道和兩萬三千部電影和電視劇，在世界各地超過九十五家經銷商[88]。

（二）公布盜版觀察名單

歐盟執委會定期發布假冒和盜版觀察名單（Counterfeit and Piracy Watch List），提供觀察名單主要是在鼓勵服務市場以及地方執法機構和政府採取行動制止或防止智慧財產侵權行為。也期望提高歐盟公民對有問題的市場購買產品的安全和其他風險的認識[89]。

（三）採用詐欺洗錢刑罰

歐洲刑警組織支持荷蘭財政資訊和調查局（Fiscal Information and Investigation Service，FIOD）於 2023 年 5 月 23 日以詐欺洗錢取締了非法 IPTV 服務。在歐洲此服務有超過一百萬用戶，用戶只要通過零售購買串流媒體設備加上每個月大約 10 歐元的訂閱費，就可觀看迪士尼、Netflix、Viaplay、Videoland、ESPN 以及超過一萬個電視頻道

[88] Advanced Media Strategies LLC.(2023, January 3). 2022 highlights Europe: Rights-holders lean on law enforcement. New regs passed against piracy. Piracy Monitor. https://piracymonitor.org/2022-europe/

[89] European Commission. (2022, December 1). Commission Publishes Latest Counterfeit and Piracy Watch List. https://policy.trade.ec.europa.eu/news/commission-publishes-latest-counterfeit-and-piracy-watch-list-2022-12-01_en

的電影和電視節目。在取締的過程中，歐洲刑警組織的歐洲金融和經濟犯罪中心提供了數據分析，協助鎖定非法 IPTV 目標和犯罪活動[90]。

（四）交易者的可追溯性

視聽反盜版聯盟（Audiovisual Anti-Piracy Alliance，AAPA）推薦了幾種打擊盜版的技術，其中，《歐盟數位服務法》（EU's Digital Services Act）[91]所規定的了解企業客戶（Know Your Business Customer，KYBC）流程，使相關交易者具可追溯性，包括：線上代管、分發和廣告利害關係人，標示不良行為者。像是與應用程式商店運營商密切合作以識別非法應用程式及其開發人員，或是由可信的舉報者來監控和報告侵犯內容權利的應用程式。此外，Android 更有機會成為盜版應用程式的載體，除 72%市占率，非法集團常以 Android Package Kit（APK）提供非法應用程式[92]。

（五）自願措施

各成員國有關於線上著作權及相關權利執法之自願措施，茲舉丹麥、德國為例[93]。

丹麥之「處理法院或當局關於因侵權而阻止網站的決定的行為準則」是權利人和 ISP 為支援法院之域名系統（DNS）封鎖命令而採取的自願措施。當法院或公共當局對一個丹麥 ISP 所發出之網站封鎖令，可用於通知其他丹麥 ISP 封鎖訪問侵權網站。並且「最遲在『丹麥電

[90] Advanced Media Strategies LLC. (2023, May 23). Netherlands: Illegal Streaming Service Busted, Leads to Money Laundering Operation. Piracy Monitor. https://piracymonitor.org/netherlands-illegal-streaming-service-busted-leads-to-money-laundering-operation/

[91] Regulation (EU) 2022/2065.

[92] Advanced Media Strategies LLC. (2023, June 19). AAPA: Illicit Apps Leverage Every Piracy Business Model; Ad-Fraud Is the Most Lucrative. Piracy Monitor. https://piracymonitor.org/aapa-app-piracy-2023-0619/

[93] 其餘例子請參閱 Bulayenko, O., Frosio, G., Lawrynowicz-Drewek, A., & Mangal, N. (2021). Cross border enforcement of intellectual property rights in EU (PE 703.387). Policy Department for Citizens' Rights and Constitutional Affairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/703387/IPOL_STU(2021)703387_EN.pdf, pp.38-39.

信行業協會』傳達決定後的 7 個工作日內」為之。此外，如果權利人記錄到網站上出現相同內容，但該網站已被重新配置為不同的位址，也可以阻止其他 DNS 位址。[94]

在德國，依據 ISP 和權利人間之行為守則，成立了獨立的「網際網路著作權清算中心」(Clearingstelle Urheberrecht im Internet，CUII)，針對「結構性著作權侵害網站」或「以大量侵權為其商業模式主要部分之網站」，經 CUII 委員會做出一致決定，聯邦網路機關就會依據《歐盟網路中立規則》（EU Net Neutrality Regulation）審查封鎖命令的可能效果，如果聯邦網路機關並無表示疑慮，ISP 即應執行[95]。但被質疑這是一群私營公司對非法第三方採取協調一致的集體行動，可能違反競爭法，且依據歐盟法院先前案例，是否違反競爭法之判斷與第三方從事違法行為無關，因此 Bulayenko et al.（2021）建議為了避免反競爭風險，應建立安全機制，例如：(1）定義網路行為非法性質的明確門檻（依據「明顯非法內容」的概念）以及（2）自願機制必須遵守的程序性和結構性正當程序標準[96]。

四、 OTT 平台相關法規

於歐盟境內欲經營傳輸廣電網路或傳輸廣播電視訊號之服務，主要需符合《發照指令》(Authorization Directive）[97]，與《歐盟電子通

[94] Telecommunications Industry Association in Denmark, "Code of Conduct for handling decisions by the courts of law or authorities concerning blocking of websites due to rights infringements", 14 September 2014. 轉引自 Bulayenko, O., Frosio, G., Lawrynowicz-Drewek, A., & Mangal, N. (2021). Cross border enforcement of intellectual property rights in EU (PE 703.387). Policy Department for Citizens' Rights and Constitutional Affairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/703387/IPOL_STU(2021)703387_EN.pdf, pp.38-39.

[95] Bulayenko, O., Frosio, G., Lawrynowicz-Drewek, A., & Mangal, N. (2021). Cross border enforcement of intellectual property rights in EU (PE 703.387). Policy Department for Citizens' Rights and Constitutional Affairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/703387/IPOL_STU(2021)703387_EN.pdf, p.39.

[96] Id., p.41.

[97] Directive 2002/20/EC.

訊法典》[98]所規範，即取得電子通訊網路傳輸業（ECN）及電子通訊服務業（ECS）之一般許可（General authorization），會員國得對所有或特定種類的電子通訊網路與服務，課予適當義務。歐盟並未針對OTT TV 制訂一致性之平臺監理規範，有關相關業者所提供之「視聽媒體服務」主要著重在內容管制，則屬於《視聽媒體服務指令》、《新視聽媒體服務指令》之規範標的。故以下將針對「視聽媒體服務」相關定義及架構進行介紹。

（一）「視聽媒體服務」範疇

有關「視聽媒體服務」依據歐盟《新視聽媒體服務指令》（Directive 2018/1808/EU, New Audiovisual Media Services Directive, Revised AVMSD）第 1 條第 1 項（a）之定義為：「（i）負有編輯責任（Editorial responsibility）之媒體服務提供者，透過《歐盟電子通訊法典》第 2 條（a）所定義電子通訊網絡（Electronic communications networks）[99]提供《歐洲聯盟運作條約》（Treaty on the Functioning of the European Union）第 56 條與第 57 條定義下之服務，供社會大眾資訊、娛樂或教育之服務，包括電視廣播服務（Television broadcast）、隨選視聽媒體服務（On-demand audiovisual media service）。（ii）視聽廣告（Audiovisual commercial communication）。」[100]。因此，歐盟目前對於視聽媒體服務之定義相當廣泛，並主要分為線性的電視廣播服務及非線性的隨選視聽媒體服務。

[98] Directive 2002/21/EC.

[99] 電子通訊網路包含三部分：（1）傳輸系統，以及所使用之交換機或路由設備；（2）以此系統傳輸訊號；（3）以有線、無線、光或其他電磁方式，包括衛星網路、地面之固定或行動網路、電力線系統、無線廣播或無線電視網路、有線電視網路。

[100] Directive 2018/1808/EU, art. 1(1)(a), OJ L 303.

（二）「視訊分享平臺」定義

隨著全球消費者收視的習慣快速變遷，逐漸朝向網際網路匯流，民眾可透過各種連網裝置接取各式線上平臺收視各類型之影音內容，甚至可以自行產製影音內容，上傳至視訊分享平臺分享。故《新視聽媒體服務指令》將「視訊分享平臺」（Video-sharing platforms），納入專章規範。按《新視聽媒體服務指令》第 1 條（1）（b）（aa）規定有關視訊分享平臺之定義：「依《歐洲聯盟運作條約》第 56 條與第 57 條之規範，其服務或其一獨立可分的片段或服務的基本功能，為提供節目或由使用者供應視頻，或將兩者均提供予公眾，以作為資訊、娛樂或教育之用途，視訊分享平臺提供者對於節目、使用者供應視頻並無編輯責任，且該服務係透過 2002/21/EC 指令定義下的電子通訊網絡傳輸；而視訊分享平臺服務之組成，特別在陳列、標籤以及排序的方式上，是由服務提供者或演算法決定。[101]」。因此，例如：YouTube 屬本指令規範下之視訊分享平臺，雖有《新視聽媒體服務指令》之適用，惟視訊分享平臺並不屬於本指令所稱之「視聽媒體服務」，屬於特別類型的管制類型，適用第 4a 條之鼓勵自律共管的共通性規範外，其內容管制規範另規定於第 28a 條與第 28b 條。由上述規範可知，歐盟大範圍地將「視聽媒體服務」納入規管，OTT TV 也屬於視聽媒體服務之一環，並進一步區分為線性與非線性；同時，針對新興之「視訊分享平臺」則不屬於「視聽媒體服務」，但指令針對其進行特殊規管，如圖 2。

[101] Directive (EU) 2018/1808, art. 1(1)(b)(aa), OJ L 303.

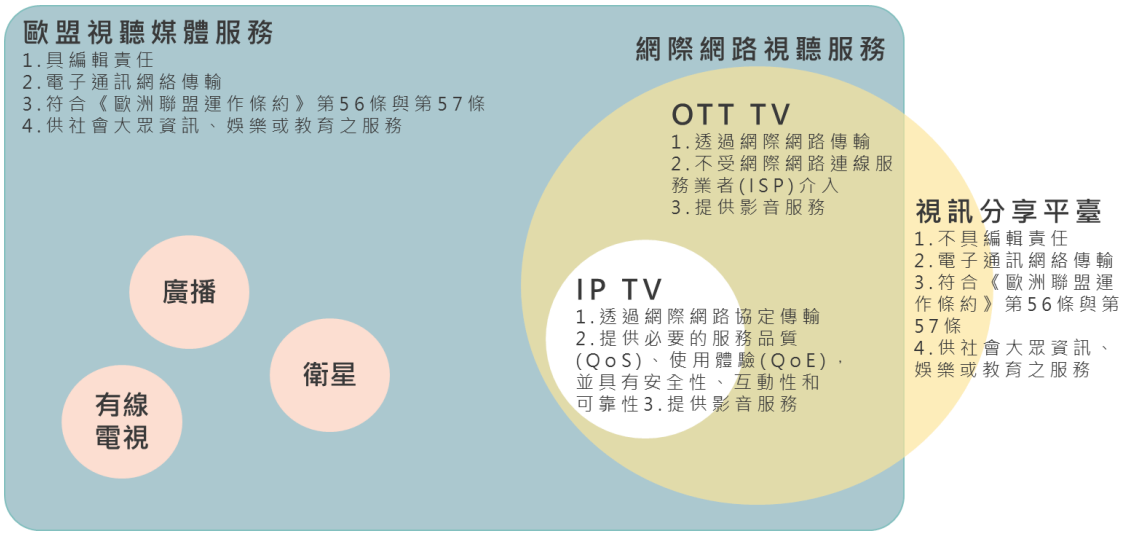

圖 2：歐盟視聽媒體服務架構

資料來源：本計畫整理

五、 OTT TV 機上盒監理政策

《歐洲電子通訊法典》（EU Electronic Communications Code，EECC）[102]第 2 條第 1 項第 7 款規定之「獨立於號碼之人際通訊服務」（Number-independent interpersonal communications service），一般稱為 OTT-1 服務，規範使用者透過網際網路之應用程式進行人際關係間通訊，自 2020 年 12 月 21 日起，必須接受和傳統電信服務受到相同的監管，違反者將面臨巨額罰款。[103]但沒有互動式通訊、通訊者不能具體選擇收件人，集中地向無限或理論上無限數量之消費者提供內容，例如新聞入口網站、部落格、論壇、推特或串流媒體等，一般稱為 OTT-2 服務，則不屬於歐盟 EECC 之監理範圍[104]。而本計畫所討論之

[102] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).

[103] 例如視訊電話服務和即時通訊，如 Skype 或 WhatsApp，以及電子郵件提供商，如 Gmail，稱為 OTT I 服務，自 2020 年 12 月 21 日起必須符合與傳統電信服務相同之服務安全性、與警察機關合作、個資保護與保密監理措施，且應具備服務透明度，否則會面臨巨額的罰款，參見：OTT REGULATION IN THE EU. (n.d.). SCHALAST. https://www.ott-regulation.com/；THE FOUR MOST IMPORTANT AREAS OF OTT REGULATION. (n.d.). SCHALAST. https://www.ott-regulation.com/regulation-of-ott-services-in-the-eu-four-areas-every-enterprise-must-review

[104] Schalast & partner. (n.d.). WHAT IS AN OTT SERVICE? SCHALAST. https://www.ott-regulation.com/what-is-an-ott-service/

OTT TV 服務一般來說屬於未進行人際關係通訊之 OTT 服務，應屬 OTT-2 之範疇，原則上不屬於歐盟 EECC 之監理範圍。

而本計畫所討論之 OTT TV 機上盒屬於 2014 年無線電設備指令（RED）[105]定義的無線電設備[106]。該指令除了規範健康及安全要求、電磁相容性、無線電頻譜之有效使用、互操作性、獲得緊急服務以及無線電設備和軟體組合的合規性；**特別值得注意的是本指令也規範了隱私及個人資料保護和防止詐欺措施[107]、以及網路安全。**

歐盟法院在 Case C-527/15 認定機上盒的銷售者，於網路上銷售多媒體播放設備，事先安裝播放視聽檔案的開源軟體，並整合第三方附加元件，使外掛可專門連結到未經著作權人授權之串流網站，同時在廣告中宣稱該設備使未經著作權人同意於電視螢幕上自由輕鬆地觀看網際網路上的視聽內容成為可能，依據第 2001/29 號指令第 3 條第 1 條，出售此類多媒體播放器構成「向公眾傳播」之侵權[108]。

對於觀看非法串流，歐盟法院在 Case C-527/15，也認為不符合重製權之例外與限制。按 2001/29 指令第 5 條第 1 項，只有在該重製是暫時的或偶然的，且為技術過程的一個組成部分，而其目的僅為透過中介之第三方網路中所進行的傳輸，或是合法使用[109]。又依同條第 5 項規定，本條前四項規定之例外和限制僅適用於不與著作或其他標的之正常利用相衝突且不無理損害他人合法利益的某些特殊情況。由於

[105] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, OJ L 153, 22.5.2014, p. 62–106.
[106] Illegal IPTV in the European Union. (2019). European Union Intellectual Property Office. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf, pp.69-70.
[107] Illegal IPTV in the European Union. (2019). European Union Intellectual Property Office. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf, pp.69-70.
[108] Judgment of 26 April 2017, filmerspeler, Case C-527/15, EU:C:2017:300, paragraphs 49-53.
[109] Directive 2001/29/EC, Art. 5 (1).

本案是故意並充分瞭解該播放器購買者接收影音資訊是免費且未經授權；且著作來自第三方串流媒體網站並未獲得著作權人同意而提供，對著作之正常利用產生不利影響；並對權利人之合法利益造成不合理之損害，這種作法通常會導致著作之合法交易減少，而對著作權人造成不合理之損害。是故，這些行為不符合 2001/29 指令第 5 條第 1、5 項之規定，亦即，在多媒體播放器上暫時重製行為，例如著作係透過未經著作權人同意之第三方的網站串流，不能主張重製權之限制與例外[110]。

六、 OTT TV 機上盒監理法規

（一）海關扣押

載有非法收視應用程式的機上盒，依據《智慧財產權執法指令》[111]、《智慧財產權海關執法條例》[112]得被海關扣押。但如果銷售的是純淨版機上盒，在歐盟稱為「香草設備」(Vanilla devices)，未經改動仍保留預設設定，「即尚未配置為接收非法流媒體的機上盒」但「最終使用者將按照經銷商提供的說明或在論壇和社交討論群組上找到的說明自行設置它們」，機上盒則無法在海關被扣押[113]。

此時，海關扣押機上盒必須另外找到法律依據，例如：該設備欠缺無線電設備指令(RED)所規定之製造商或貿易商應備之合規評定、技術檔，或產品上未標示合規性聲明、CE 標記、製造商資訊；同時，啟動向成員國市場監督當局的快速通知程序[114]。

---

[110] 同註 [108], paragraphs 59-72.
[111] Directive 2004/48/EC, Article 9(1)(b).
[112] Council Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, OJ L 196, 2.8.2003, p. 7–14.
[113] Illegal IPTV in the European Union. (2019). European Union Intellectual Property Office. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf, p.69.
[114] Id., p.70.

（二）無線電設備指令與歐盟安全標準

歐盟智慧財產局（EUIPO）認為，「由可疑企業製造的『香草』設備可能具有危險功能，根據歐盟安全標準，這些設備是非法的。」[115]此處引用的資料是 FACT 和電器安全第一（Electrical Safety First）之報告，該報告發現絕大多數非法串流裝置的電源設備，對消費者造成了巨大的火災和電氣風險[116]，並提及在 2017 年 6 月間，歐盟執委會發出對中國製造的安卓電視盒或 Kodi 盒子—OTT TV Box 4K 的召回通知，警告電擊風險嚴重[117]。該召回之依據為 2014 年《無線電設備指令》（RED）對設備安全之要求。

但不僅是安全風險，依據 2014 年《無線電設備指令》（RED），機上盒應被設計成保護使用者之隱私及個人資料、免於詐欺、以及維護網路安全；且如果有使用者、無線電設備或第三方要將軟體載入到該設備中，機上盒也必須設計為僅能安裝已證明無線電設備結合軟體具合規性之軟體（the compliance of the combination of the radio equipment and software has been demonstrated），才能將軟體載入到無線電設備中。不符合這些基本要求之無線電設備，製造商、進口商與分銷商，都不應投放至市場。此外，如果無線電裝置存在風險，進口商與分銷商都應通知製造商和市場監督當局。

因此，製造商、進口商與分銷商，明知或有理由可知，於銷售後再以客服方式安裝非法收視視聽內容之程式，將違反上開規定。又若為購買之消費者自行至網路論壇查詢安裝此類非法收視程式，只要此類程式可危害消費者之隱私及個人資料、詐欺、以及破壞網路安全（即

[115] Id., p.69.
[116] FACT. (2017, November 16). Illicit streaming devices pose fire risk. https://www.fact-uk.org.uk/illicit-streaming-devices-pose-electrical-and-fire-risk-to-users/
[117] Id.

損害網路或其功能，濫用網路資源，從而導致不可接受的服務降級，詳後述），機上盒欠缺阻止載入該軟體之設計，亦屬違反上開規定。

2014 年無線電設備指令（RED）與此相關之規定，分別說明如下：

該指令前言第 13 點指出：「無線電設備的特殊功能可以加強對使用者和無線電設備使用者的個人資料和隱私的保護，以及保護免於詐欺。因此，在適當情況下，無線電設備的設計應支持這些功能。」第 16 點指出：「某些種類的無線電設備是否符合本指令中規定的基本要求可能會受到包含軟體或修改其現有軟體的影響。使用者、無線電設備或第三方只能在不影響無線電設備隨後符合適用的基本要求的情況下，才能將軟體載入到無線電設備中。」[118]另在指令前言第 18 點提及依據《歐洲聯盟運作條約》第 290 條採取相關適當行動的權力應授權給歐盟執委會。

為此，指令第 3 條基本要求之第 3 項第 1 段 d、e、f、i 款規定，某些種類或類別之無線電設備之構造應符合以下基本要求：（d）無線電設備不可損害網路或其功能，也不可濫用網路資源，從而導致不可接受的服務降級；（e）無線電設備包含保障措施，以確保使用者和訂閱者的個人資料和隱私受到保護；（f）無線電設備支援某些功能以確保防止詐欺；（i）無線電設備支援某些功能以確保軟體只能當無線電設備和軟體組合之合規性已被證明才能載入無線電設備[119]。且，本項

[118] 原文是：The compliance of some categories of radio equipment with the essential requirements set out in this Directive may be affected by the inclusion of software or modification of its existing software. The user, the radio equipment or a third party should only be able to load software into the radio equipment where this does not compromise the subsequent compliance of that radio equipment with the applicable essential requirements.

[119] 原文是：Article 3 Essential requirements

3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;

(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

(f) radio equipment supports certain features ensuring protection from fraud;

第 2 段進一步規定：執委會應有權根據第 44 條通過授權法案，具體規定本項第 1 段（a）至（i）款所列各項要求涉及哪些種類或類別的無線電設備[120]。

據此，2022 年 1 月 12 日歐盟執委會發布《授權規則 2022/30/EU》補充了關於基本要求應用的指令 2014/53/EU，**要求製造商將隱私和個人數據、網路安全和詐欺預防之考慮因素整合到無線電設備的設計中**[121]。而規則無需等待會員國轉換成國家政策，依授權條例第 3 條規定，從 2024 年 8 月 1 日起於各國直接適用（補充：原計劃從 2024 年 8 月 1 日起強制執行，現在延期到 2025 年 8 月 1 日起強制執行）。授權規則旨在實現以下目標：提高網路恢復能力，改善個人資料保護，並降低貨幣詐欺的風險[122]。

依據授權規則第 1 條第 1 項，第 2014/53/EU 號指令第 3 條第 3 項第 1 段第 d 款規定的基本要求應適用於任何可以透過網際網路進行通訊的無線電裝置，無論是直接通訊還是透過任何其他裝置（網際網路連線之無線電裝置）。

機上盒符合本項所定義之網際網路連線之無線電裝置，其設計即應遵守 d 款所要求之不可損害網路或其功能，也不可濫用網路資源，從而導致不可接受的服務降級。所稱情況，在授權規則前言第 9 點舉例如下：攻擊者可能會惡意淹沒網際網路網路以防止合法網路流量；

(i) radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.

[120] 原文是：The Commission shall be empowered to adopt delegated acts in accordance with Article 44 specifying which categories or classes of radio equipment are concerned by each of the requirements set out in points (a) to (i) of the first subparagraph of this paragraph.

[121] Delegated Regulation (EU) 2022/30 supplements Directive 2014/53/EU with regard to the application of the essential requirements. It requires manufacturers to integrate privacy and personal data, network security and fraud prevention considerations into the design of radio equipment.

[122] Kun, E. (2022, January 18). Another Brick in the Cybersecurity Law: Data Protection by Design Requirements for Manufacturers of IoT Devices in the EU Law. KU Leuven CiTiP. https://www.law.kuleuven.be/citip/blog/another-brick-in-the-cybersecurity-law/

中斷兩個無線電產品之間的連線，從而阻止訪問服務；阻止特定人員訪問服務；中斷對特定系統或個人的服務；或中斷資訊。

授權規則第 1 條第 2 項規定第 2014/53/EU 號指令第 3 條第 3 項第 1 段第 e 款中規定的基本要求應適用於網際網路連線的無線電裝置，如果該無線電裝置能夠在歐盟 2016/679 號條例第 4 條第 1 項第 2 款的含義範圍內處理同條項第 1 款定義的個人資料，或第 2002/58/EC 號指令第 2 條第（b）項和（c）項中定義的流量資料和位置資料。所稱「處理」是指對個人資料或個人資料集執行的任何操作或一組操作，無論是否透過自動化方式，例如蒐集、記錄、組織、結構化、儲存、改編或更改、檢索、諮詢、使用、通過傳輸揭露、傳播或以其他方式提供、對準或組合、限制、刪除或銷毀[123]。「個人資料」是指與已識別或可識別的自然人（資料主體）有關的任何資訊；可識別的自然人是指可以直接或間接識別的人，特別是通過參考如姓名、身分證號、位置資料、線上標識碼等標識符或特定於該自然人的身體、生理、遺傳、心理、經濟、文化或社會身分的一個或多個因素[124]。「流量資料」是指為在電子通信網路上傳輸通信或為其計費而處理的任何資料[125]。「位置資料」是指在電子通信網路中處理的任何資料，表明公開可用的電子通訊服務使用者的終端設備的地理位置[126]。

[123] 原文是：‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[124] 原文是：‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[125] (b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

[126] 原文是：(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

機上盒業者為了營利，會限制收視對象，如綁定機器之 MAC 碼、CPU ID 及 KEY。參考歐盟對 IP 地址之見解，如果控制者在法律上得要求提供商交出其他資訊，使他能夠識別 IP 地址背後的使用者，這也是個人資料[127]。之後，在 GDPR 中明文規定「線上識別符」屬於個人資料，依據 GDPR 前言第 30 點之說明，包括 IP 地址、cookie 識別符號或如射頻（RFID）識別標籤，都可能會留下痕跡，特別是當與伺服器收到的唯一識別符和其他資訊相結合時，可用於建立自然人的配置檔案並識別他們。英國 ICO 也指出線上識別符的例子，包含 MAC 位址、廣告 ID、圖元標籤、帳戶資料和設備指紋（MAC addresses；Advertising IDs；Pixel tags；Account handles；and Device fingerprints）[128]。而機上盒所綁定機器之 MAC 碼、CPU ID 及 KEY，均屬伺服器收到之機器唯一識別符，如結合登入資料而得建立使用者之配置、識別，即為個人資料。則依據第 2014/53/EU 號指令第 3 條第 3 項第 e 款該無線電設備應包含保障措施以確保使用者和訂閱者的個人資料和隱私受到保護。

授權規則第 1 條第 3 項規定第 2014/53/EU 號指令第 3 條第 3 項第 f 款規定的基本要求應適用於任何網際網路連線的無線電裝置，如果該裝置使持有人或使用者能夠按照歐盟 2019/713 號指令第 2 條第 d 項的規定轉移貨幣、貨幣價值或虛擬貨幣。據此，當機上盒具有線上支付功能時，應支援確保防止詐欺之功能。

授權規則前言第 17 點首先指出，經濟上經營者，必須遵守 2014/53/EU 指令第 3 條之基本要求。所稱經濟上經營者，是指製造商

[127] Intersoft consulting. (n.d.). GDPR Personal Data. https://gdpr-info.eu/issues/personal-data/; CJEU Case C-582/14.

[128] Information Commissioner's Office (ICO). (2023, May 19). What are identifiers and related factors? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-are-identifiers-and-related-factors/

（指令第 10 條第 1 項）、進口商（指令第 12 條第 2 項後段[129]）、分銷商（指令第 13 條第 2 項後段[130]）。

授權規則前言第 17 點接著指出，為了便於對這些要求進行合規評定，它規定了無線電設備之符合性推定，只要符合歐洲議會和理事會法規 1025/2012/EU 規則[131]所定之自願協調標準，且該標準之目的是表達這些要求的詳細技術規格，該等規格考慮並解決與本規則所涉及之每一種類或類別之無線電設備之預期用途所相對應之風險水準，即被推定為符合這些標準或其部分所涵蓋之第 3 條規定之基本要求（指令第 16 條）。據此，歐盟執委會要求歐洲標準化組織制定必要的標準，預計統一標準將在授權規則生效前 10 個月提供，也就是在 2023 年 10 月提供[132]（註：目前預計協調標準將延於 2024 年 6 月發佈）。

第二個合規評估選項，是由製造商通知相關機構評估其產品，以證明遵守適用的法規（指令第 17 條第 4 項）。

指令前言第 70 點指出，成員國應制定適用於違反根據本指令透過的國家法律規定的處罰規則，並確保這些規則得以執行。所定之處罰應該是有效、相稱和勸阻性的。據此，第 46 條罰則規定：「（第 1 項）成員國應制定適用於經濟經營者違反根據本指令透過的國內法條

[129] 該規定為：「如果進口商認為或有理由認為無線電裝置不符合第 3 條規定的基本要求，在無線電裝置符合要求之前，他不得將無線電裝置投放市場。此外，如果無線電裝置存在風險，進口商應通知製造商和市場監督當局。」

[130] 該規定為：「如果分銷商認為或有理由認為無線電裝置不符合第 3 條規定的基本要求，則在無線電裝置符合要求之前，不得在市場上提供無線電裝置。此外，如果無線電裝置存在風險，分銷商應通知製造商或進口商以及市場監督當局。」

[131] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

[132] 在統一標準尚未制訂前，亦有若干民間機構建議之標準，可以參考，請見 Tewari, A., & Killam, T. (2022, September 28). Cybersecurity and product regulatory compliance - Part 2. OnRule - Compliance With Confidence. https://onrule.com/resources/product-regulatory-compliance-cybersecurity-part2.html

款的處罰規則，並應採取一切必要措施確保這些規定得到執行。此類規則可能包括對嚴重侵權行為的刑事處罰。（第 2 項）規定的處罰應有效、相稱且具有勸阻性。」

（三）歐盟執委員會打擊具商業規模之線上體育賽事或其他直播建議

2023 年 5 月 4 日，歐盟執委會基於《數位服務法》（Digital Services Act, 2022/2065/EU）、《執行指令》（Enforcement Directive）[133]，提出「關於打擊線上盜版直播內容的建議」（下稱建議）[134]，包含體育賽事直播和其他現場活動直播。

對現場活動之未經授權之線上再傳播，該建議首先指出其嚴重性，不僅是金額龐大，於 2019 年僅以訂閱費模式之金額就達到 5.22 億歐元；透過全球離岸主機以規避歐盟之《著作權法》及刑事責任；採取「盜版即服務」的建立、營運到金流全套服務模式；建立合法串流服務之鏡像；以及再轉播服務業者也發展了規避執法的彈性策略。（建議前言第 4 點）

其次，分析了非法再傳播流程之參與者（建議前言第 5 點）。而後指出不同類型中介服務提供者依據其可用之技術手段，刪除或禁止訪問未經授權之直播活動，實屬重要，因此，特別是應依據歐洲議會和理事會條例 2022/2065/EU 適用於中介服務提供者之不同義務，確立適合不同類型中介服務提供者各自職能之有效解決方案（建議前言第 6 點）。但並非歐盟各國都賦予體育賽事現場活動智慧財產權保護，因此，為了防止體育賽事直播造成之價值損失，應鼓勵成員國確保體育賽事主辦人能夠獲得補救措施，允許他們以非常快的方式請求禁止

[133] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157, 30.4.2004, p. 45–86

[134] Commission Recommendation (EU) 2023/1018 of 4 May 2023 on combating online piracy of sports and other live events, C/2023/2853, OJ L 136, 24.5.2023, p. 83–94.

訪問未經授權的轉播（建議前言第 8 至 11 點）。但同時也應保證必要之保障措施，保護基本權利（建議前言第 13 點）。為此，有必要促進體育賽事主辦人、權利人、中介服務提供者和主管機關之間的合作。（建議前言第 15 點）

就主機服務提供人，依據 2022/2065/EU 第 16 條有「通知和行動」（Notice and action）之義務，特別是考慮到所通知的非法內容類型和採取行動的緊迫性，應即時根據通知採取行動。於收到通知後，應即採取行動，盡量減少未經授權轉播直播活動之損害。（建議前言第 17、18 條）且建議主機服務提供人，也採取線上平台依據 2022/2065/EU 所規定之以必要的技術和組織措施，對受信任的舉報人所為之通知，優先處理且不無故拖延，但微型或小型企業則依據個案具體情況定之。（建議前言第 19 點）此外，也鼓勵開發和使用即時通知、加速處理之技術解決方案，但前提是其中也必須有補救機制。（建議前言第 20 點）

就權利人而言，應充分利用不同的方法加密或標記廣播訊號，包括取證浮水印，以便快速準確地識別未經授權的轉播來源，保護其免受未經授權之使用。（建議前言第 21 點）

就防止未經授權轉播現場體育賽事之禁制令，鼓勵廣泛地採用動態禁制令（建議前言第 28 點）。但目前僅有少數成員國提供動態禁制令，它們是由法院或某些行政當局批准，這些當局有權依職權或依申訴，命令採取封鎖或移除措施（建議前言第 26 點）。為了防止過度封鎖，必須正確識別適用動態禁制令的其他網際網路位置。其中一種可能更新禁制令所涵蓋網際網路位置清單的方式是，由權利人與禁制令對象合作，約定一種方法作為禁制令的一部分，但須受司法機關之控

制。禁制令的對象通常是 ISP（網際網路服務供應商）。（建議前言第 29 點）

對於中介服務提供者，建議採取進一步自願措施，防止所提供之服務被濫用。目前許多技術皆可達到濫用之目的，例如：內容傳遞網路（Content delivery networks，CDN）和反向代理（Reverse proxies）技術可能被用於混淆轉播訊號的來源；替代 DNS 伺服器（Alternative DNS resolvers）和虛擬專用網路（VPN）可用於接取已被封鎖的內容。（建議前言第 29 點）

對其他市場參與者，如廣告供應商以及支付服務提供者，依據其在歐盟反洗錢框架下之義務和自願行動，也可打擊線上盜版。如歐盟執委會推動一份關於線上廣告和智慧財產權的諒解備忘錄，使簽署方自願承諾盡量減少在侵犯智慧財產權（包括著作權）的網站和移動應用程式上投放廣告。（建議前言第 31 點）

對消費者而言，對其提供可用、可負擔、具吸引力、具價格競爭力之合法轉播，也有助於降低其消費侵權內容。因此，建議增進消費者對合法來源的認識。例如，某些成員國在封鎖禁制令中告知網站使用者已封鎖及合法之來源。此可指向歐盟智慧財產局觀察站也開發了 Agorateka，作為歐盟線上內容入口網站，連結到各國的入口網站。（建議前言第 32、33 點）

由於線上侵權之跨國性，因此跨國合作很重要，透過歐盟智慧財產局觀察站，各國可交流執法資訊，培訓執法人員，監測本建議採取行動之效果、提供技術專長和組織支援。（建議前言第 34-37 點）

本建議指出，應尊重基本權利、個人資料保護，要有補救機制，適當地平衡與上述措施有關人員之權利和利益，同時考慮到不同的基本權利以及這些措施在任何個案中的相當性。這些措施的適用應有嚴

格地針對性(Strictly targeted),不得對中介服務業者施加過多的義務,且不應導致一般性地監控。(建議前言第 38-40 點)

據上,本建議區分為對未經授權轉播體育賽事直播、及轉播其他現場活動。分別進一步建議:1、確保及時處理與未經授權轉播有關的通知、2、禁制令。此外建議:提高認識和主管機關之間的自願合作。最後,對本建議進行後續行動和監測。

其中,就確保及時處理與未經授權轉播有關的通知,又可區分為及時處理通知(第 4、5 點,第 22、23 點)、權利人與中介服務提供者之間的合作(第 6、7 點,第 24、25 點)。

就禁制令,對體育賽事直播先鼓勵成員國給予體育賽事主辦者尋求禁制令之法律地位(第 8 點),繼而建議禁制令對象包含未經授權轉播之營運者、以及其服務被第三方濫用於轉播未經授權轉播之中介服務提供者。且鼓勵在體育賽事前即申請禁制令,得以過去未經授權轉播類似體育賽事為證據。(第 9、10 點)

但是對於未經授權轉播其他現場活動的禁制令,並沒有上述關於主辦人法律地位、或禁制令對象之建議。

就禁制令之動態性質,分別規定在第 12 至 14 點、第 26 至 28 點。關於鼓勵成員國提供尋求對特定中介服務提供者實施禁令的可能性,這種禁令可以擴大到能夠封鎖盜版服務,即使這些服務在申請禁令時身分不明,但其涉及同一體育賽事或活動,且符合其國家程序規則,在體育賽事(第 12 點)及現場活動(第 26 點)是相同的。但在現場活動之第 26 點,更進一步要求要符合《憲章》在內之歐盟法律之適用規定,特別是言論和資訊自由權以及保護個人資料的權利。

就禁制令之動態清單,於體育賽事直播在第 13 點規定:「為了在發佈禁制令後以適當的方式識別這些盜版服務,成員國應鼓勵使用逐

案更新禁制令所涵蓋之網際網路位置清單（例如通過域名、IP 位址或 URL 來識別）之方法，包括通過在司法當局控制下之權利人和禁制令對象之間的合作。成員國可以考慮是否應由獨立的國家機關認證禁制令所涵蓋的網際網路位置清單。」但在現場活動之第 27 點規定並沒有最後一句關於設立獨立國家機構之建議。

第 14 與 28 點均規定，如果成員國授權獨立的行政機關發布禁制令或更新禁令所涵蓋的網際網路位置清單，則應有權對此決定向法院上訴。

就禁制令之保障，體育賽事規範在第 15 至 19 點，而現場活動僅有第 29 至 30 點。相同之建議是，在引入或適用有關的禁制令規則時，鼓勵成員國考慮到禁制令中規定的措施不應給對象帶來不合理的負擔。它們應嚴格針對，不應不必要地剝奪使用者合法獲取現有資訊的可能性（第 15、29 點）。鼓勵成員國確保權利人定期更新不再用於未經授權轉播之網際網路位置資訊，以便取消對這些網際網路位置之限制（第 18、30 點）。就體育賽事另外還有第 16 點：如果禁制令採取封鎖措施的形式，則應注意確保其針對由網際網路位置識別之盜版服務，該服務主要用於提供未經授權的轉播或其他類型的未經授權的內容。第 17 點：為實施此類禁制令而採用之技術措施應足以防止或至少使訪問未經授權的體育賽事轉播變得困難，並嚴重阻撓（Seriously discourage）最終使用者訪問這些未經授權的轉播。第 19 點：鼓勵成員國規定，禁制令之期限不應超過確保有效保護體育賽事直播權利人所必需之期限。鼓勵成員國規定，在這方面適用的封鎖措施只在體育賽事現場直播時生效。

就禁制令之自願合作，體育賽事直播與現場活動規定相同。應鼓勵中介服務提供者考慮適當和相當之自願措施，以防止其服務被濫用

於未經授權轉播（第 20、31 點）。應鼓勵廣告和支付服務等其他市場參與者確保其服務不會促進未經授權轉播運營商之促銷與運作（第 21、32 點）。

（四）《數位單一市場著作權指令》

歐盟《數位單一市場著作權指令》（Directive on Copyright in the Digital Single Market）[135]是歐洲議會和歐盟理事會於 2019 年通過的一項關於著作權保護重要指令，同年 6 月 6 日生效，歐盟成員國須於 2021 年 6 月 7 日前將該指令內化為國內法。該指令旨在調整和保護數位環境中的著作權和相關權利，並建立一個公平和具有可持續性的數位單一市場，同時保護創作者智慧財產權所有人的權力，尋求數位環境下不同利益者間之權衡，並特別著重受保護內容的數位與跨境使用。和 OTT TV 機上盒侵權相關之主要規範可能包括：

1. 線上內容分享服務業者的責任[136]

該指令要求線上內容分享服務業者（Online content-sharing service providers），例如：YouTube、Facebook 等，就其用戶在其平台上傳內容利用到他人著作之行為，線上內容分享服務業者應代替其用戶負責向著作權人取得「向公眾傳播」之授權。

線上內容分享服務業者如果無法替用戶取得權利人授權，則應負侵權責任，除非其達成以下三個條件，方能免除責任：A.已盡「最大努力」取得授權；B.已盡「最大努力」確保侵權內容不被上傳及 C.收到權利人侵權通知後立即移除、阻絕接觸侵權內容，以確保合法使用[137]。

[135] Directive (EU) 2019/790.
[136] Directive (EU) 2019/790, art. 17.
[137] Directive (EU) 2019/790, art. 17 (4).

線上內容分享服務業者需透過有效之機制，迅速刪除未經著作權人授權、許可之內容，同時防止未經授權之內容重新上架，以確實保障有關著作權人之權益[138]。為衡平考量，歐盟僅就大型線上內容分享服務業者課予責任，亦即若是在歐盟境內提供服務未滿三年、年營業額未滿 1,000 萬歐元的新興業者，則可免除證明前述三要件中的第二要件，不需採取措施阻止侵權內容上傳，但若該平台已達 500 萬人以上之瀏覽人次，仍不能免除[139]。

2. 適當及合理補償原則

會員國應確保當著作人及表演人授權或轉讓其著作或其他受保護內容之專屬利用權利時，有權取得適當且合乎比例之使用報酬[140]，包括線上發布、公開表演和數位傳輸等，這將有助於保護著作權所有人之權利。

（五）歐盟《資訊社會著作權及相關權利協調指令》

歐盟《資訊社會著作權及相關權利協調指令》（Directive 2001/29/EC, Information Society Directive）[141]該指令確立了著作權人之權利，包括重製、散布、展示、向公眾傳播等，並將這些權利適用於數位環境。其中和 OTT TV 較為相關的條文為：

1. 重製權[142]

各成員國應針對下列情況給予權利人複製權，以利授權或禁止直接或間接、暫時或永久地以任何方式、在任何形式中全部或部分複製：(a) 著作人之著作；(b) 表演者之表演錄製；(c) 錄音物製作人之錄音物；(d) 對於電影首次錄製製作人而言，是其

[138] Directive (EU) 2019/790, art. 13.
[139] Directive (EU) 2019/790, art. 17 (6).
[140] Directive (EU) 2019/790, art. 18.
[141] Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001 on the harmonization of certain aspects of copyright and related rights in the information society.
[142] Directive 2001/29/EC, art. 2.

電影的原版和複本；（e）對於廣播組織而言，是其廣播錄製，不論該廣播是通過電纜、衛星、有線或無線傳輸。

2. 向公眾傳播權[143]

各成員國應針對下列情況給予權利以有線或無線方式向公眾傳播（Communication to the public），包括向公眾提供（Making available to the public），使公眾成員得在他們自行選擇的時間和地點近用著作以及（a）表演者之表演錄製；（b）錄音物製作人之錄音物；（c）對於電影首次錄製製作人而言，是其電影的原版和複本；（d）對於廣播組織而言，是其廣播錄製，不論該廣播是通過電纜、衛星、有線或無線傳輸。

3. 禁制令[144]

在本指令前言第 59 點指出，特別是在數位環境中，中介人之服務可能越來越多地被第三方用於侵權。在許多情況下，此類中介人最適合制止此類侵權活動。因此，在不影響任何其他制裁和補救措施的情況下，權利人應有可能對在網路上乘載第三方侵害受保護著作或其他客體之中介人申請禁制令。即使中介人所從事之行為被第 5 條所排除，也應有這種可能性。與此類禁制令有關的條件和方式應留給成員國的國內法處理。

據此，本指令第 8 條第 3 項規定，成員國應確保權利人得對於其服務被第三人用以侵害著作權或相關權利之中介人，聲請禁制令。

（六）《廣播與電視節目智慧財產權和相關權利行使指令》

《廣播與電視節目智慧財產權和相關權利行使指令》（Directive 2019/789/EU，Directive on Television and Radio Programmes）主要是

[143] Directive 2001/29/EC, art. 3(2).
[144] Directive 2001/29/EC, art. 8(3).

補充原來第 3 條向公眾傳播解釋上之不確定性，包括：定義「傳播」（包含再傳播 IPTV 訊號）（第 2 條第 2 款）及將訊號直接傳播（Direct injection）給訊號分發者（第 8 條）是否屬於《資訊社會著作權及相關權利協調指令》指令所稱之「向公眾傳播」。

七、 OTT TV 機上盒監理技術

機上盒作為無線電設備，其經濟上經營者，包含：製造商、進口商、分銷商都必須遵守 2014/53/EU 無線電設備指令第 3 條之基本要求。歐盟執委會曾以機上盒違反此規定，有嚴重觸電危險而要呼籲盒子的所有人停止使用[145]。此外，關於第 3 條所規定之隱私及個人資料、免於詐欺、以及維護網路安全，法規要求歐洲標準化組織需於 2024 年 12 月 28 日之前制定相關標準。[146]

歐盟採取關閉網站並封鎖其域名，以阻斷 OTT TV 機上盒的視聽服務，執行技術策略，以海盜灣為例：

海盜灣（The Pirate Bay，TPB）是著名的非法 OTT 平台，2003 年成立於瑞典，是世界最大點對點檔案傳輸伺服器，過去以提供 BitTorrent 種子載點，提供各種類型的數位內容，包括自由著作權的檔案，以及盜版的電影、音樂、遊戲和軟體等[147]。2019 年海盜灣新增加一組綠色播放按鍵，讓使用者能藉由名為 BayStream 影音串流技術播放內容，直接在線上觀看影音內容，並可在實際下載前預覽內容[148]。

---

[145] FACT. (2017, November 16). Illicit streaming devices pose fire risk. https://www.fact-uk.org.uk/illicit-streaming-devices-pose-electrical-and-fire-risk-to-users/

[146] 在統一標準尚未制訂前，亦有若干民間機構建議之標準，可以參考，請見 Tewari, A., & Killam, T. (2022, September 28). Cybersecurity and product regulatory compliance - Part 2. OnRule - Compliance With Confidence. https://onrule.com/resources/product-regulatory-compliance-cybersecurity-part2.html

[147] The pirate Bay. (2023, August 14). Wikipedia, the free encyclopedia. Retrieved August 15, 2023, from https://en.wikipedia.org/wiki/The_Pirate_Bay

[148] Yeh, D. (2019, December 11). Disney+原創劇被盜得最慘！惡名昭彰「海盜灣」盜版功能再升級，還新增串流模式｜數位時代 BusinessNext. 數位時代. https://www.bnext.com.tw/article/55864/pirate-bay-torrent-streaming-baystream-piracy-file-sharing

三十多個國家和地區運用 ISP 動態封鎖海盜灣（TPB），但卻無法完全消滅，主要是因於代理網站（Proxy sites）的存在，讓非法網站在十多年的廣泛封鎖之後仍然存在。這些代理網站的特性和海盜灣（TPB）相似，但尚未列入 ISP 黑名單，所以沒有遮蔽域名。

然而，近期可將數千萬用戶引導到海盜灣代理站點的 Pirate Bay 代理索引網站從 GitHub 上消失。封鎖單位使用英國警察智慧財產權犯罪部門運營的侵權網站列表（Infringing Website List，IWL）。刪除所有重複的代理域名、任何未明確專用或針對海盜灣的域名，以及由於停機或其他原因而無法識別的任何域名，最後列出 670 至 690 個域名，所有這些代理均因出現在 IWL 黑名單將受到網站封鎖或是營運業務限制[149]。

第三節　英國

一、 市場現況

英國智慧財產局的研究估計，2022 年英國有近 400 萬人使用非法來源觀看體育賽事直播[150]。

關於英國的非法串流到底值多少錢，英國研究者約翰·盧倫茲·波奎茲 2023 年 4 月在 ESCoE 部落格發表了研究。2021 年音樂、影片（電視劇和電影）、體育直播、軟體、電腦遊戲和電子書的盜版總價值在 36 億至 75 億英鎊之間，佔家庭消費的 0.2%或通訊服務最終消費（Final consumption of communication services）的 8.8%。數位盜版總價值主要來自體育直播佔 35%，其次分別是音樂 28.3%和影片

[149] Maxwell, A. (2023, May 21). A decade of pirate Bay proxy war: Did ISP blocking slay the Hydra? TorrentFreak. https://torrentfreak.com/a-decade-of-pirate-bay-proxy-wars-did-isp-blocking-slay-the-hydra-230521/

[150] Symonds, T., & Grundy, T. (2023, May 30). TV fraud gang jailed for illegally streaming Premier League games. BBC News. https://www.bbc.com/news/uk-65697595

23.9%。作者並未完全排除 2021 年直播運動之價值可能由於 2020 年歐洲足球錦標賽而突然上升。作者認為研究顯示，數位盜版對英國經濟的影響，可能比原來想像得大，因為若將盜版內容的價值納入考慮，則 2021 年通訊服務最終消費之增長可能會慢 0.2 個百分點。[151]

二、 政府角色

英國視聽媒體主管機關為 Ofcom（Office of communications，Ofcom）。著作權主管機關為英國智慧財產局（Intellectual Property Office，IPO）。封網之禁制令是由英國法院依據權利人之申請而發布。

2016 年 12 月諾丁漢皇家法院（Nottingham Crown Court）首次對在酒吧銷售載有可在網路上搜尋非法串流之應用程式和外掛的 IPTV 機上盒的二個被告，判決犯刑法共謀詐欺罪（Conspiracy to defraud），認為他們的行為助長了大規模盜版，包括在未經授權之外國頻道上轉播英超聯賽[152]。此後，陸續有類似判決之案件[153]。

在此 2016 年刑案中，倫敦市警察局智慧財產權犯罪部門（Police Intellectual Property Crime Unit，PIPCU）進行了早期調查。然後由英超聯盟和反著作權侵權聯盟（the Federation Against Copyright Theft，FACT）聯手調查，提起自訴（Private prosecution）。倫敦市警方智慧財產權犯罪部門之偵查總督察 Pete Ratcliffe 說明了警察的角色：「這一信念表明，與行業和其他機構合作對現代警務是多麼重要。保護我

[151] Poquiz, J. L. (2023, April 21). How much is illegal streaming worth? ESCoE. https://www.escoe.ac.uk/how-much-is-illegal-streaming-worth/

[152] Premier League. (2016, December 9). Press release: Supplier of illegal iptv & Android-type boxes jailed. Home. https://www.aapa.eu/press-release-supplier-of-illegal-iptv-android-type-boxes-jailed

[153] 例如，2019 年 Steven King 被判決犯共謀詐欺罪處七年四個月徒刑，及在三個月內償還 963,000 英鎊。請參見：PA Media. (2022, June 6). Man jailed for selling illegal football streaming boxes ordered to pay £1m. the Guardian. https://www.theguardian.com/football/2022/jun/06/man-jailed-selling-illegal-premier-league-football-streaming-boxes-ordered-pay-one-million-pounds

們的創意產業對英國經濟和其中數百萬個工作崗位至關重要，此案發出了一個明確的資訊，即這是將進行調查並提交法院的犯罪。」[154]

除了各地警察之外，為了打擊非法串流，英國尚有其他政府執法人員也是功不可沒。2023 年反著作權侵權聯盟 FACT 卓越獎，表彰了 19 位在過去幾年參與成功起訴英國一些大型非法串流業務的警察與其他執法人員。由獲獎人名單，可以得知英國政府中重要的參與者，除了英國各地警察部門的警官，還有來自哈默史密斯和富勒姆委員會（貿易標準）（LB Hammersmith & Fulham（Trading Standards））、國家交易標準電子犯罪團隊（National Trading Standards e-Crime Team，NTSeCT）、和政府機構情報網路（Government Agency Intelligence Network，GAIN）的官員[155]。

哈默史密斯和富勒姆委員會是一個執行刑法以鼓勵公平交易的機關，業務範圍與商品和服務之數量、價格或描述有關；或與消費者購買的商品安全有關。他們調查投訴、與警察等其他機構合作、或採取適當行動在必要時起訴[156]。

國家貿易標準電子犯罪團隊（National Trading Standards eCrime Team，NTSeCT）由商業、創新和技能部（BIS）和國家交易標準委員會（NTSB）資助成立，為政府應對電子犯罪戰略之一部分，分為數位證據部門和調查團隊，旨在保護英格蘭和威爾斯的消費者和企業免受網際網路犯罪和線上詐欺。電子犯罪是指使用網際網路、電子郵件或手機技術實施的犯罪，廣泛來說包含線上詐騙和敲詐勒索，具體而言，仿冒商品和智慧財產權盜竊即屬之。除了對於具有國家重要性的

---

154 同註 152

155 FACT. (2023, April 20). FACT Excellence Awards. https://www.fact-uk.org.uk/police-trading-standards-recognised-for-outstanding-contributions-towards-combatting-intellectual-property-crime/

156 Trading standards. (n.d.). LBHF. Retrieved August 15, 2023, from https://www.lbhf.gov.uk/business/trading-standards

詐騙和敲詐勒索，NTSeCT 可以獨立調查外，主要是協助當地和地區貿易標準官員（Trading standards officer）[157]，提供操作和技術支援。NTSeCT 由專業鑑識分析師和網際網路調查員組成團隊 eCrime Team，以情報為主導，和情報官員、分析師和研究人員組成的團隊密切合作，蒐集並評估各種內部和外部電子犯罪情報來源。有最先進的數位證據部門，可以從幾乎任何類型的桌機、筆記本電腦、平板電腦、手機或儲存媒體中提取和分析數據。對地方執法機構提供專業的開源情報和網際網路取證培訓，使他們掌握最新的線上情報技術。調查時，他們會利用專業警察和貿易標準官員之綜合專業知識來調查，且這些官員還可以在執行搜查令時提供免費的行動支持[158]。

政府機構情報網路（GAIN）是一個由 30 多個政府機關組成的大型組織網路，為打擊嚴重及組織性犯罪，而共享資訊，並聯合執法[159]。

綜上所述，可知英國政府非常重視整合各機關之情報、以及整合各種網路調查取證專業之官員或研究者，以因應日新月異電子犯罪。對於追訴販售非法 OTT TV 機上盒或提供非法串流內容相關犯罪，發揮了重要的作用！

三、 政策

（一）消費者意識宣導

英國權利保護團體開始積極宣導因為收看盜版內容可能遭致之風險，包含詐欺、身分盜竊和惡意軟體或者參與到犯罪組織。

[157] 英國貿易標準機構主要負責執行公平貿易、監控產品安全、確保年齡限制和正確、打擊非法行為並確保所有度量衡有效執行。

[158] National Trading Standards eCrime Team. (n.d.). About us. https://www.tradingstandardsecrime.org.uk/about/

[159] Government agency intelligence network (GAIN) (2023, February 23). His Majesty's Inspectorate of Constabulary and Fire & Rescue Services. Retrieved August 16, 2023, from https://www.justiceinspectorates.gov.uk/hmicfrs/glossary/government-agency-intelligence-network/

反著作權侵權聯盟 FACT 於 2021 年發起品牌的 NothingInLifeIsFree 活動，邀請明星、網路安全專家共同拍攝影片，向群眾解釋非法串流媒體所隱藏之風險。因為，他們在 2021 年經過二次調查發現，多數人（62%）不知道上述風險，而警告會使 39%的人改變態度。且這些威脅風險很高，幾乎有接近一半的（47%）受訪者，會為使用非法串流而已經或將共享他們的個人電子郵件地址；並有三分之一的人承認，由於非法串流，他們已經被詐欺、被駭或遇到線上詐騙。[160]於 2022 年 FACT 調查 50 個知名的非法串流網站都有惡意內容；超過 90%的網站有風險，而超過 40%的網站沒有安全證書；使用者受到包括銀行木馬、加密詐騙和極端或明確的彈出視窗等威脅；還發現了許多在非法串流媒體網站上託管或連結露骨內容的例子，對兒童構成嚴重風險。[161]FACT 網站上並維持一個專區名為：「非法串流之風險」（Dangers of Illegal Streaming），除了傳統之宣傳：看未經授權的電視內容就是犯罪，還宣傳非法串流媒體或下載極其危險，可能會讓您和您的家人被惡意軟體、病毒、勒索軟體、詐騙和詐欺。[162]

Crimestoppers Trust，是一個獨立慈善機構，協助犯罪被害人匿名舉報，他們對於非法串流之網站，現在的政策是，除了告知使用者使用機上盒等收視未經授權的電影、電視、運動賽事也是犯罪之外，還特別強調使用非法串流網站會有下列風險：遭到駭客攻擊、感染病毒、詐欺或個人數據盜竊；以及這些未經授權的網站、設備、應用程式以

[160] FACT. (2022, January 17). FACT's Anti-Piracy And Content Protection Work In 2021. https://www.fact-uk.org.uk/fact-in-2021/

[161] FACT. (2022, August 19). New research finds illegal sports streaming sites expose fans to financial fraud, dangerous scams and explicit content. https://www.fact-uk.org.uk/new-research-finds-illegal-sports-streaming-sites-expose-fans-to-financial-fraud-dangerous-scams-and-explicit-content/

[162] FACT. (n.d.). Dangers of illegal streaming. https://www.fact-uk.org.uk/consumer-advice/dangers-of-illegal-streaming/

及他們可以訪問的內容，家長無法控制，可能有色情廣告和不適合年齡內容[163]。

（二）提供黑名單阻止非法網站獲得廣告收入

《英國創意行動》由倫敦市警察局智慧財產犯罪部門（PIPCU）於 2013 年發起，旨在解決非法串流媒體網站的資助問題，曾阻止非法網站獲得 600 萬英鎊廣告收入；該計劃係將非法網站列入侵權網站列表（IWL），以提醒廣告商、代理機構和其他中介機構，不會在這些網站上投放廣告或無意中資助非法網站[164]。

（三）以詐欺、共謀詐欺、洗錢論罪

除了著作權犯罪，對於提供非法串流、販售非法機上盒，近期在英國更多是以詐欺、共謀詐欺、洗錢論罪。

如前所述，2016 年 12 月諾丁漢皇家法院（Nottingham Crown Court），是首次對銷售非法機上盒之二個被告，以共謀詐欺罪（Conspiracy to defraud）判刑[165]。此後，陸續有類似判決之案件[166]。

2022 年 6 月 16 日，在曼徹斯特明舒爾街刑事法院，邁克爾·霍農（Michael Hornung）因在 2014 年至 2017 年期間三年內出售和宣傳未經授權的解碼器用於詐欺而被陪審團定罪，被判處四年零六個月的監禁。[167]

---

[163] CrimeStoppers. (n.d.). Streaming Online – Know the Risks. Online safety. https://crimestoppers-uk.org/keeping-safe/online-safety/streaming-online-know-the-risks

[164] City of London Police.(2023, June 2).Operation Creative Blocks £6 Million of UK Advertising Revenue from Funding Illegal Websites. City of London Police News. https://www.cityoflondon.police.uk/news/city-of-london/news/2023/january/operation-creative-blocks-6-million-of-uk-advertising-revenue-from-funding-illegal-websites/

[165] Premier League. (2016, December 9). Press release: Supplier of illegal iptv & Android-type boxes jailed. Home. https://www.aapa.eu/press-release-supplier-of-illegal-iptv-android-type-boxes-jailed

[166] 例如，2019 年 Steven King 被判決犯共謀詐欺罪處七年四個月徒刑，及在三個月內償還 963,000 英鎊。請參見：PA Media. (2022, June 6). Man jailed for selling illegal football streaming boxes ordered to pay £1m. the Guardian. https://www.theguardian.com/football/2022/jun/06/man-jailed-selling-illegal-premier-league-football-streaming-boxes-ordered-pay-one-million-pounds

[167] FACT. (2022, June 17). Four years and six-month jail sentence for pirate TV supplier. https://www.fact-uk.org.uk/four-years-and-six-month-jail-sentence-for-pirate-tv-supplier/

2022 年 3 月 18 日，在南安普敦刑事法院，有四人因非法串流受著作權保護的內容（如 Sky Sports 和 BT Sports）以及洗錢（因此類非法活動的收益）而被定罪：邁克爾·詹姆斯·西蒙茲（Michael James Simmonds）以及基蘭·柯林斯（Kieran Collins），依據 2006 年《詐欺法》第 9 條（為詐欺目的參與商業）和 2002 年《犯罪收益法》（洗錢）第 327 條被判刑。阿曼達·柯林斯（Amanda Collins）、羅伯特·庫裡安（Robert Kurian），根據 2002 年《犯罪收益法》（洗錢）第 327 條被判刑。另根據 2002 年《犯罪收益法》對四人提起沒收訴訟。[168]

（四）觀看非法串流構成犯罪

Paul Faulkner 因經營非法串流服務，提供英超聯賽之直播與 Sky 頻道等內容，而承認多項侵害著作權和詐欺罪被判處 16 個月監禁。但值得注意的是，法院就被告自己觀看未經授權電視之行為，認定構成犯罪，而另判處四個月的監禁。[169]英超聯盟的法務主管認為這消除了認為觀看盜版串流服務只是灰色地帶或者不構成犯罪之誤解。[170]FACT 首席執行官 Kieron Sharp 也認為法院此判決應可對消費者起到警告作用。[171]

四、 OTT 平台相關法規

英國針對廣電業者之主要法制架構為《2003 年通訊法》（Communications Act 2003）及《2009 年視聽媒體服務管制法》（The Audiovisual Media Service Regulations 2009，AVMSR 2009）、及《2020

[168] FACT. (2022, March 25). Illicit streaming fraudsters jailed. https://www.fact-uk.org.uk/illicit-streaming-fraudsters-jailed/

[169] FACT. (2021, July 8). Man jailed for illegally supplying and viewing Premier League content. https://www.fact-uk.org.uk/man-jailed-for-illegally-supplying-and-viewing-premier-league-content/

[170] Id.

[171] Maxwell, A. (2021, July 8). IPTV operator jailed for 16 months for selling & watching pirate streams. TorrentFreak. https://torrentfreak.com/iptv-operator-jailed-for-16-months-for-selling-and-watching-pirate-streams-210708/

年視聽媒體服務管制法》(Audiovisual Media Service Regulations 2020，AVMSR 2020)。

其中和 OTT TV 相關之規範主要為第 4A 章，「隨選節目服務」（On-demand progamme service，ODPS）之定義與管制類型，並設有有害內容管制、廣告與商品置入等規範；第 4B 章，「視訊分享平服務」（Video-sharing platform service，VSPS）納入規範，拉齊線性與非線性服務對於有害內容之管制密度，以對應歐盟之《新視聽媒體服務指令》，但目前英國並無針對網際網路視聽服務平臺的管制，相關規範僅針對網際網路視聽服務之內容管制。

五、 OTT TV 機上盒監理政策

（一）《無線電設備規則》

2017 年英國《無線電設備規則》(Radio Equipment regulations 2017）主要內容大致依循歐盟無線電設備指令（2014/53/EU），惟於英國脫歐之後，部分規範略有調整，例如：在歐盟受 CE 標誌之產品，未來在英國將逐步轉化為 UKCA（英國產品符合性）標誌，在商品輸入英國市場時必須貼上新的產品標誌用以證明商品符合英國法規要求。

（二）政令宣導

英國智慧財產局在網站上公布對於「非法串流設備」的建議[172]，分為六大項目，包括：1.什麼是「非法串流」以及常用的設備是什麼；2.如何識別非法串流設備；3.為什麼不應購買這些設備；4.如果您已經擁有非法串流設備該怎麼辦；5.在哪裡可以舉報非法串流設備的銷售者；6.獲取更多進一步的建議資訊。其中指出，確保著作權人獲得報酬的重要性，並警告經改裝的電視棒或「Kodi 盒子」和「Android TV

[172] Guidance Illicit streaming devices, https://www.gov.uk/government/publications/illicit-streaming-devices/illicit-streaming-devices

盒子」對兒童福利構成威脅，同時也可能對公眾帶來電氣安全隱患、為犯罪分子提供資金等。政府建議如果擁有這類設備，應立即清除其中的非法軟體，並呼籲合法訂閱觀看。

（三）封網禁制令、動態封網

在 2019 年英超聯賽，根據著作權相關法令聲請並獲得了第一個動態封鎖禁制令（2019 年令），以防止非法觀看英超聯足球比賽[173]。爾後，在相關案件中，例如：Matchroom Boxing 公司起訴英國電信等[174]案中，Matchroom Boxing（舉辦拳擊賽事的公司）申請了禁制令，以阻止對拳擊比賽進行串流媒體播放的網站侵犯著作權，該命令要求 ISP 業者採取合理措施，禁止訪問提供串流媒體的網站 IP 位置。

（四）以詐欺、共謀詐欺、洗錢論罪

自 2016 年 12 月諾丁漢皇家法院（Nottingham Crown Court），是首次對銷售非法機上盒之二個被告，以共謀詐欺罪（Conspiracy to defraud）判刑[175]。此後，陸續有類似判決之案件[176]。

2022 年 6 月 16 日，在曼徹斯特明舒爾街刑事法院，邁克爾·霍農（Michael Hornung）因在 2014 年至 2017 年期間三年內出售和宣傳未經授權的解碼器用於詐欺而被陪審團定罪，被判處四年零六個月的監禁。[177]

---

[173] [2017] EWHC 480 (Ch).

[174] Matchroom Boxing Ltd and another v British Telecommunications plc and others. (2020).EWHC 2868 (Ch). https://www.bailii.org/ew/cases/EWHC/Ch/2020/2868.html

[175] Premier League. (2016, December 9). Press release: Supplier of illegal iptv & Android-type boxes jailed. Home. https://www.aapa.eu/press-release-supplier-of-illegal-iptv-android-type-boxes-jailed

[176] 例如，2019 年 Steven King 被判決犯共謀詐欺罪處七年四個月徒刑，及在三個月內償還 963,000 英鎊。請參見：PA Media. (2022, June 6). Man jailed for selling illegal football streaming boxes ordered to pay £1m. the Guardian. https://www.theguardian.com/football/2022/jun/06/man-jailed-selling-illegal-premier-league-football-streaming-boxes-ordered-pay-one-million-pounds

[177] FACT. (2022, June 17). Four years and six-month jail sentence for pirate TV supplier. https://www.fact-uk.org.uk/four-years-and-six-month-jail-sentence-for-pirate-tv-supplier/

六、 OTT TV 機上盒監理法規

英國針對違法 OTT TV 機上盒的銷售、廣告、供應或使用，可適用以下規範：

（一）《1988 年著作權、設計和專利法》

《1988 年著作權、設計和專利法》（Copyright, Designs and Patents Act 1988）是英國針對著作權和相關權利的保護的基本規範。其與違法 OTT TV 機上盒相關執法規定摘要如下：

1. 詐欺性接收節目

當有人不誠實地接收從英國境內提供的廣播服務中的節目，且意圖逃避對該節目接收的任何費用，該人犯下罪行，一經定罪，可處以不超過標準刑度上第五級的罰金。若證明公司的犯罪行為是在董事、經理、秘書或類似職位的同意或默許下發生的，或由自稱擔任這些職位的人所犯下，該董事、經理、秘書或類似職位的人以及該公司本身都犯有該罪行，並應相應地受到追究和懲罰[178]。

2. 未經授權的解碼器

若有人執行以下行為，即構成犯罪：

（1）製造、進口、分發、銷售、出租或提供或展示未經授權的解碼器；（2）出於商業目的，持有未經授權的解碼器；（3）出於商業目的，安裝、維護或更換未經授權的解碼器；或（4）透過商業傳播方式宣傳銷售或出租未經授權的解碼器或以其他方式推廣未經授權的解碼器。犯罪者將負有以下責任：簡易判決最高可能入獄六個月或罰金不超過法定最高額，或同時兩者；若經審判法庭審判最高可能入獄十年或罰金或同時兩者。被起訴違反

[178] Copyright, Designs and Patents Act 1988, art. 297.

此條例的被告，可為自己辯護，證明他並不知道，也沒有合理理由相信該解碼器是未經授權的解碼器。

其中所謂「未經授權」指的是該解碼器旨在使加密傳輸或任何其所屬的服務以可理解的形式被訪問，而無需支付傳輸者或代表其傳輸的人收取的費用（不論如何加以課徵）；這些費用通常是用於訪問該傳輸或服務（無論是透過繞過與該傳輸或服務相關的有條件取用技術或其他方式）[179]。

3. 規避技術措施的設備和服務

若有人進行以下行為，旨在迴避保護智財權之技術措施的設備和服務，即構成犯罪：（1）為銷售或出租而製造；或（2）除了自身的私人和家庭使用之外而進口；或（3）在業務過程中：甲員銷售或出租；或乙員提供或展示銷售或出租；或丙員宣傳銷售或出租；或丁員持有；或戊員分發；或（4）其分發程度會對著作權所有人造成不利影響；以上列舉的是任何設備、產品或部件，其主要設計、製造或改裝之目的在於使迴避有效的技術措施成為可能或更容易。

若有人提供、推廣、宣傳或推銷：（1）在業務過程中；或（2）若非在業務過程中，其推銷程度會對著作權所有人造成不利影響；上述行為目的皆在迴避保護著作權之技術措施。

4. 動態禁制令

英國高等法院（The High Court）有權對服務提供者（Service provider）實際知悉另一個人利用他們的服務來侵犯著作權時[180]發出禁制令。在判定服務提供者是否實際知悉時，法院應考慮下列特定情況下，具有相關性的所有事項，包括：1.服務提供者是

[179] Copyright, Designs and Patents Act 1988, art. 297A.
[180] 此指之服務提供者依據歐盟電子商務指令(EC Directive)第 2 條之定義。

否透過依據《電子商務指令》（SI 2002/2013）第 6（1）（c）條規定所提供的聯絡方式收到通知；2.通知所提及之資訊（通知發信人的全名和地址、侵權行為的詳細資訊）等[181]。意即服務提供者雖然不是侵權人，在特定狀況下（如 ISP 業者收到侵權通知），在不知悉侵權人實際身分下，法院可命令 ISP 業者採取某些措施來阻止其客戶訪問侵權的線上內容。

（二）《2006 年詐欺法》

英國《2006 年詐欺法》（Fraud Act 2006）旨在規範和打擊各種詐欺行為，以更好地應對現代詐欺形式，該法案將不同類型的詐騙行為納入其中，其與違法 OTT TV 機上盒相關執法規定摘要如下：

1. 持有詐欺使用的物品

若持有或控制任何用於詐欺活動的物品，或者與詐欺有關，則該人將被判定有罪[182]。

2. 製造或提供用於詐欺的物品

若製造、採用、供應或提供任何物品：（1）知悉該物品是為詐欺活動而設計或適應的；或（2）意圖使用該物品來實施詐欺，或協助實施詐欺。則該人將被判定有罪[183]。

3. 不誠實的獲取服務

若有人以不誠實的行為取得自己或他人的服務，且違反了第 2 項之條件，則該人將被判定犯有本條規定下的罪行。

若有人違反以下情況取得服務，則視為違反第 2 項條件：

(1) 該服務是基於已支付、正在支付或將來會支付費用而提供的。

[181] Copyright, Designs and Patents Act 1988, art. 97A.
[182] Fraud Act 2006, art. 6.
[183] Fraud Act 2006, art. 7.

(2) 在未支付任何費用或未全額支付的情況下取得了該服務。

(3) 在取得該服務時，他知道：A.該服務是根據前述的方式提供的，或 B.他知道該服務是根據前述的方式提供的，但他故意不支付費用，或不全額支付[184]。

（三）《2007 年重罪法》

《2007 年重罪法》（Serious Crime Act 2007）旨在打擊嚴重犯罪行為，包括有組織犯罪、暴力犯罪、金融犯罪等，並增強執法機關打擊犯罪的能力。其與違法 OTT TV 機上盒相關執法規定摘要如下：

1. 故意鼓勵或協助犯罪行為[185]

行為人必須實施一個可能鼓勵或協助他人犯罪的行為。包括：直接行動或間接行動，只要這些行動具有鼓勵或協助他人犯罪的可能性。

所謂「故意鼓勵或協助」指涉及的人必須有意要鼓勵或協助他人犯罪的實施。意即行為人明確意識到自己的行為可能會導致他人犯罪，並且有意促使這種犯罪行為發生。如果鼓勵或協助犯罪只是行為人的可預見後果，而不是他故意的目的，則不應將其視為故意鼓勵或協助犯罪。

2. 間接故意鼓勵或協助犯罪行為[186]

若一人實施了可能鼓勵或協助犯罪行為的行動，並且他相信：（1）該犯罪行為將會被實施，以及（2）他的行動將鼓勵或協助該犯罪的實施。

[184] Fraud Act 2006, art. 11.
[185] Serious Crime Act 2007, art. 44.
[186] Serious Crime Act 2007, art. 45.

（四）《犯罪收益法》

《犯罪收益法》（Proceeds of Crime Act 2002）該法案的目的是削弱犯罪分子的經濟基礎，阻止他們使用非法資金進行其他犯罪活動，同時保護受害人的權益。其與違法 OTT TV 機上盒可能相關執法規定摘要如下：

1. 安排（Arrangements）

一個人進入或參與一項安排，他知道或懷疑這項安排通過任何手段促進另一個人取得、保有、使用或控制犯罪所得。若進入或參與這樣的安排，他知道或懷疑這項安排通過任何手段促進另一個人取得、保有、使用或控制犯罪所得[187]。

2. 取得、使用和持有罪（Acquisition, use and possession）

一個人犯罪，如果他（1）取得犯罪所得；（2）使用犯罪所得；（3）持有犯罪所得[188]。

七、 OTT TV 機上盒監理技術

消費者觀看非法直播主要元素：侵權錄影的來源（接收許可服務的電纜或衛星解碼器盒）、管理錄影分發的平臺、提供商的串流媒體伺服器（傳輸錄影的副本）、消費者的機上盒或媒體播放器。而英國的監理技術，以英格蘭與威爾斯高院 2017 年之英超聯盟判決[189]採用動態封網，也就是動態封鎖伺服器、變更目標 IP 和 URL，以阻斷 OTT TV 機上盒的視聽服務，以下說明其執行技術策略。

FAPL 是英超聯賽的管理機構，擁有所有英超聯賽電視鏡頭的電影著作權，以及該鏡頭中出現視訊內容的著作權。目前未經 FAPL 授權非法傳輸英超聯賽現場錄影日益嚴重的因素，包含：

---

[187] Proceeds of Crime Act 2002, art. 328.
[188] Proceeds of Crime Act 2002, art. 329.
[189] THE FOOTBALL ASSOCIATION PREMIER LEAGUE LIMITED. (2017). England and Wales High Court (Chancery Division) Decisions.

1. 用戶轉向機上盒、媒體播放器和移動裝置的應用程式來觀看侵權內容。所以封鎖網站將無法防止越來越多的侵權行為，機上盒可以透過其 IP 地址直接連線到串流媒體伺服器。
2. 機上盒和媒體播放器等裝置易於連線到家用電視，串流軟體變得更容易安裝，甚至侵權內容的來源通常會自動更新。
3. 現在可以訪問每場英超聯賽的大量高品質的侵權鏡頭串流。
4. 英國消費者認為使用機上盒和軟體訪問未經授權的串流是合法的，高於認為透過檔案共享網站訪問未經授權的內容是合法的。
5. 提供侵權串流的串流伺服器越來越多地被轉移到海外託管提供商，這些提供商不與權利人要求合作，無法即時刪除侵權內容。

（一）專有視頻指紋技術監控侵權串流

首先，FAPL 聘請的承包商在當前英超賽季的幾周內使用專有視頻指紋（Video fingerprinting）技術監控侵權串流。透過這種方式已經識別了大量侵權串流媒體伺服器所在的 IP 地址。其次，FAPL 已經確定了應該被遮蔽的侵權串流媒體伺服器，但這些命令細節都被保密，因為如果被公開，將更容易規避該命令。

（二）現場封鎖命令，運用影片監控技術、遮蔽系統

該命令是一個現場封鎖命令，僅在直播英超比賽錄影時生效。這之所以可能，是因為兩項技術進步：

1. **影片監控技術**：FAPL 使用的影片監控技術現在允許在英超聯賽比賽中以極高的準確度且即時識別侵權串流。此類串流發出的伺服器幾乎可以立即通知英國六大網際網路服務提供商（ISP）。

2. 遮蔽系統：ISP 某些遮蔽系統的進展將允許他們在英超比賽期間自動遮蔽和解鎖 IP 地址，在某些情況下會自動。如果這個過程是自動化的，或者可以在相關時間提供手動監控，那就意味著在最需要遮蔽來保護相關權利的時候，遮蔽可以配合串流媒體服務運營商使用的 IP 地址的變化，這也表示遮蔽不會在比賽時間之外發生。

（三）每個比賽週重置目標伺服器列表

儘管允許在必要時更新目標網站的 IP 地址或 URL 是標準做法，但該命令規定在英超賽季的每個比賽週重置目標伺服器列表。允許 FAPL 識別新伺服器，並通知 ISP 每週進行封鎖，並確保舊伺服器在一週結束後不會被封鎖，除非繼續被觀察到侵權錄影。

（四）命令只持續很短的時間

該命令只持續很短的時間。這是為了讓 ISP 有時間準備遵守。它只會持續到英超賽季的結束，FAPL 申請類似的要求只涵蓋賽季期間，並根據本賽季的經驗進行任何適當的調整。

（五）IP 地址被阻止要向託管提供商傳送通知

命令要求在其某個 IP 地址被阻止時，每週向每個託管提供商傳送通知，託管提供商和受該命令影響的網站或服務運營商有權申請撤銷或更改該命令。

第四節　韓國

一、 市場現況

（一）韓國非法串流媒體網站的市場現況

「Noonoo TV」非法串流媒體網站於 2021 年提供串流媒體服務，該網站免費播放電影、電視劇和動畫，並透過非法賭博網站做廣告來

盈利。截至 2023 年 2 月該網站上傳視頻的總觀看次數超過 15 億次，明顯高於韓國主要串流媒體網站的觀看次數，而每月用戶數約為 1,000 萬。非法網站利用社群媒體消息引導人們在 Noonoo TV 上免費觀看，並提供非法串流媒體網站網址，只需點擊即可輕鬆免費觀看各自的付費內容，對於 Netflix、Wavve、Tving、Coupang Play 和其他 OTT TV 服務提供商都受到 Noonoo TV 負面影響[190]。串流媒體服務提供商、廣播公司和媒體行業的其他組織聲稱因非法串流媒體網站而損失了約 4.9 萬億韓元（37 億美元），並於 2023 年 3 月 9 日對 Noonoo TV 提起刑事訴訟[191]。

（二）韓國非法種子下載網站的市場現況

韓國下載、共享種子檔案（Torrent file）並不違法，但若該種子檔案受著作權保護則被視為非法，有些國家完全禁止這種種子檔案傳輸，因這種行為常用於與其他網際網路用戶共享受保護的內容。一些國家和地區對於種子下載（包括電影、電視節目和音樂）處以罰款，包括：德國、法國、英國、芬蘭、日本和阿聯酋。此外，許多國家都有關閉種子網站的歷史，包括美國、義大利、葡萄牙、俄羅斯、拉脫維亞、中國、馬來西亞、澳大利亞和南非[192]。

二、 政府角色

就韓國視聽產業的監理架構而言，傳統的有線電視受《放送法》（방송법）所規範，主管機關為韓國通信委員會（방송통신위원회, KCC），依據《放送法》第 9 條第 1 項，任何欲從事有線廣播電視業

[190] Baek byung-yeul. (2023, March 21). OTT Service Providers Negatively Impacted by Illegal Streaming Website. Business. https://www.koreatimes.co.kr/www/tech/2023/06/129_347439.html

[191] Shin, J.S. (2023, March 16). More Koreans Using Illegal Streaming Sites Despite Police Investigation. The Korea Bizwire. http://koreabizwire.com/more-koreans-using-illegal-streaming-sites-despite-police-investigation/242954

[192] Gerald hunt. (2023, June 11). Is Torrenting Illegal in South Korea? VPN Ranks. https://www.vpnranks.com/kr/faqs/is-torrenting-illegal/

務者，需獲得 KCC 同意，同時，KCC 要求韓國科學技術資訊通訊部（Ministry of Science and ICT，MSIT）針對業者進行技術審查[193]；在這樣的規定下，有線電視的主管機關為 KCC，而執照由 MSIT 進行審查後核發。韓國智財權保護局（Korea Copyright Protection Agency，KCOPA）是韓國著作權保護機構，負責執行韓國的著作權保護和監管工作[194]。

三、 政策

（一）委員會負責監管

韓國通信委員會（KCC）負責監管廣播和電信行業，而韓國通信標準委員會（KCSC）負責監督內容和道德標準[195]。KCSC 成立於 2008 年，與 KCC 幾乎同時成立，負責監控網際網路內容並向內容託管商和其他服務提供商發出審查命令。KCSC 包括四個小組委員會，分別負責審查廣播、廣告、網際網路通信和數位犯罪。

（二）公私協力的跨部門工作小組

公私協力的保護著作權工作小組，透過立即措施、相關法規與科技改善、大眾教育等對韓國內容保護日臻完善[196]。韓國政府召集文化體育觀光部、通訊傳播委員會（KCC）、警政署、智財權保護局（KCOPA）、通訊審議委員會（KCSC），以及韓國三大網路服務供應商（ISP）包括韓國電信（KT）、LG 電信、SK 通訊等，成立跨部門工作小組。工作小組主要任務包含：

---

193 방송법, 제 9 조.

194 Purpose of Establishment·History. (n.d.). KCOPA. https://www.kcopa.or.kr/eng/lay1/S120T428C430/contents.do

195 Freedom House. (2022). South Korea. https://freedomhouse.org/country/south-korea/freedom-net/2022

196 張祐嘉 (2023 年 5 月 25 日)。捍衛正版權利，韓國抓盜版專責機構在做甚麼?。文化內容策進院。https://research.taicca.tw/article/b6aab699-81ac-326b-b916-84c9271a67af

1. **立即措施**：刑事情報共通、加重處罰要求、DNS（網域名稱系統）封鎖。
2. **相關法規與科技改善**：網站封鎖程序處理時間改善、減少已封鎖網站規避可能的科技工具發展。
3. **大眾教育**：透過名人、社群廣告、社群分享以及廣播電視等置入方式強化民眾對於著作權保護的認知。

（三）韓國非法種子下載網站的監理策略

韓國使用種子下載是合法的，但下載受著作權保護的內容卻不合法，雖然種子用戶被起訴的機會非常小，但有時他們可能會受到懲罰。著作權所有者起訴種子下載者侵犯著作權的事件數量在 2000 年代末達到頂峰。此後，在韓國的數位內容盜版者因巨額金錢而被起訴，大多數都庭外和解。1.著作權流氓（Copyright trolls）：他們的工作是識別和定位非法下載受著作權保護的材料的種子下載者。他們與著作權所有者聯繫並簽署協議，讓所有者代表自己採取法律行動。爾後負責偵查韓國的盜版行為，並通過郵件或和解信追捕種子下載者，以警告種子下載者付費而無需上法庭。2.和解函（Settlement letters）：著作權流氓識別出個人著作權盜版者的身分後，透過法院系統致電個人著作權盜版者的 ISP，並透過電子郵件對個人著作權盜版者發出法律警告，這是在韓國收到和解信的最常見方式。韓國 ISP 可能會對個人著作權盜版者採取行動，來自各個內容所有者和協會提供的報酬也可能會讓 ISP 對用戶採取任何形式行動[197]。

[197] 同註 [192]

四、 OTT 平台相關法規

在韓國 IPTV 業者受《網路多媒體放送事業法》(인터넷 멀티미디어 방송사업법)的規範,《網路多媒體放送事業法》第 4-1 條中也明定執照由 MSIT 負責審查、許可與發放;但與有線電視類似,IPTV 業者屬於《放送法》第 2 條所定義之廣播業者[198],因此主管機關屬 KCC 管轄。

而 OTT TV 業者等提供網路影音服務業者屬於在《電信事業法》(전기통신사업법)之下的「加值電信服務事業」(Value-added telecommunication service),主要受《電信事業法》所管制。有關「網路影音服務」之定義依該法規定為「依據《電影與影視著作振興法》(영화 및 비디오물의 진흥에 관한 법률)提供影視著作等數位影像物的附加通訊服務」[199]。MSIT 對於 OTT TV 之管制係採取登記報備制,業者於開始營運前須向 MSIT 進行登記[200]。

五、 OTT TV 機上盒監理政策

(一)韓國預防侵權的監理策略[201]

1. **著作權知識流通與教育**:韓國智財權保護局(KCOPA)不定期舉辦活動向大眾教育著作權保護觀念。
2. **網站資料**:提供可在網路查詢的侵權救濟流程、著作權問答集、判決案例、法律諮詢。
3. **人員培訓**:企業著作權有關領域專業人員培訓課程。
4. **認證標章**:透過 KCOPA 發行的著作權認證標章確認是否為正版商品。

198 방송법, 제 2 조.
199 전기통신사업법, 제 2 조 12.
200 전기통신사업법, 제 22 조.
201 同註 196

5. 軟體檢查工具：有單機版和網路版的檢查工具，檢查員可遠端連線下載端，依照軟體檢查列表檢視下載端的電腦是否有盜版軟體情形，或是個人電腦的網路軟體使用情形回報給網路檢查員。

（二）韓國侵權後行動的監理策略

1. 家庭監測工作者

(1) 雇用人員：雇用受培訓的身障人士、再就業婦女、多元文化家庭、低收入者監控自動爬蟲系統外的範圍，像是社群網站或反爬蟲入口網站等，範圍可擴及國外的網路來源。

(2) 發現侵權處理方式：檢查員在發現侵權行為後，可提供糾正建議、通報權利方與機構、阻斷侵權方廣告等非法收入等。

2. ICOP 平台

(1) 識別侵權內容：ICOP 平台是不中斷系統，以爬蟲和外部公共資料庫連接識別侵權的非法內容。

(2) 提供侵權報告：系統將產出監控數據與報表，提供行政單位進一步調查與分析確認是否為非法流通，並提供季度侵權報告。

六、 OTT TV 機上盒監理法規

（一）《著作權法》(저작권법)

1. 複製權

作者擁有複製其著作的權利[202]。

2. 公眾傳輸權

作者擁有將其著作進行公眾傳輸的權利[203]。

---

[202] 저작권법, 제 16 조.
[203] 저작권법, 제 18 조.

3. 同步廣播權

廣播業者擁有將其廣播進行同步廣播的權利[204]。

4. 禁止透過技術讓保護措施失效

任何人不得以正當授權之外的方式，故意或過失地移除、修改或規避技術保護措施等方式來使其無效。然而，符合下列各項情況之一除外：

(1) 從事加密領域研究的人，以正當方式取得著作等的副本，或為了研究著作等所應用的加密技術的缺陷或漏洞，在必須的範圍內使其技術無效的情況。然而，僅限於已經竭盡努力獲得權利人同意進行研究，但未獲得同意的情況。

(2) 防止未成年人接觸在線上有害的著作所為之技術、產品、服務或設備中的無效化技術保護措施組件或零件。然而，僅限於根據第 2 項所不禁止的情況。

(3) 確認可私下蒐集和傳播個人識別資訊以追蹤個人在線上的行為，並為了使其無效化而需要的情況。然而，不包括影響他人接觸著作等的情況。

(4) 為了國家的執法、合法資訊蒐集或安全保障等所必需的情況。

(5) 根據第 25 條第 3 項和第 4 項的規定，為了決定學校、教育機構和課程支援機構，以及根據《公共記錄管理法》的記錄管理機構是否購買著作等所必要的情況。然而，僅限於無法在不無效化技術保護措施的情況下進行接觸的情況。

(6) 在有正當授權的情況下，使用程序的人在需要與其他程序兼容的範圍內進行程序碼逆向分析的情況。

---

[204] 저작권법, 제 85 조.

(7) 在有正當授權的情況下，由於檢查、調查或校正計算機或資訊通信網路的安全性所需要的情況。

原則上任何人不得製造、進口、分發、傳輸、銷售、租賃、為公眾提供訂閱或為出售或租賃而廣告或分發，或者以提供服務的方式來保存或擁有下列裝置、產品或零件。包括：以無效化技術保護措施為目的進行宣傳、廣告或促銷的物品；具有商業目的或僅有商業用途之無效化技術保護措施物品；用於發明、製造、改造或運作以使無效化技術保護措施成為可能或便利化為主要目的物品[205]。

5. 損害賠償及處罰

違反上述規定或侵害著作權人權利，可依據《著作權法》第第 104-8 條請求停止侵權、第 123 條請求損害賠償及銷毀、第 125 條請求損害賠償、第 126 條損害數額的認定及第 136 條、第 137 條、第 141 條處罰。

七、 OTT TV 機上盒監理技術

關於韓國的監理技術，以下案例採用線上監控、數位著作權侵權科學調查、著作權侵權綜合應對系統，以阻斷 OTT TV 機上盒的視聽服務，執行技術策略如下：

[205] 저작권법, 제 104 조의 2.

（一）線上監控

韓國智財權保護局（KCOPA）成立線上監控小組，僱用弱勢群體作為家庭監測工作者，對國內外網站的非法複製行為進行監控，以應對國內外廣泛的智慧財產權侵權行為。主要工作內容有，24 小時監控、分析智財權侵權資訊，進行糾正建議（警告和刪除/暫停傳輸等）和公私合作應對措施、提供必要的資訊；阻止非法網站搜尋和阻止廣告等以消除收入來源；調查非法傳播韓流內容的海外網站，向權利公司提供資訊支持自救[206]。

（二）數位著作權侵權科學調查

智財權保護局與文化體育旅遊部特別司法警察合作開展著作權侵權取證調查，按照規範的程序和方法，對著作權侵權人的數位存儲設備進行調查、收集、傳輸、存儲、分析和報告等一系列過程，使數據作為數位證據而具有法律效力[207]。

（三）著作權侵權綜合應對系統

建立綜合情報室，全年 365 天、每天 24 小時，當侵權發生時，作為控制塔，實時掌握情況，確保對應侵權的黃金時間，迅速採取行動，自動蒐集與公共數據相關的著作權資訊並支持著作權保護。包括：音樂、電影、廣播、出版、遊戲、動漫、軟體之侵權資訊及慣犯之即時分析[208]。

---

[206] 온라인 모니터링. (n.d.). KCOPA. https://www.kcopa.or.kr/lay1/S1T10C222/contents.do 。
[207] Id.
[208] Id.

第五節　　日本

一、 市場現況

串流媒體平臺 MUVI[209]研究發現，2023 至 2027 年，亞洲地區（包含韓國、日本、新加坡、中國大陸）OTT 市場和視頻串流媒體行業將以 10.75%的複合年增長率增長，如果增長速度符合預期，市場規模將在 2023 年增長至 1076 億美元，而到 2027 年，預計將達到 1619 億美元。Statista[210]發布數據，2023 年至 2027 年，日本 OTT 市場將以 10.24%的複合年增長率增長。2022 年日本 OTT 市場規模為 87 億美元，到 2023 年底，預計將增長至 101.1 億美元，預計到 2027 年底將增長至 149.6 億美元。

日本非法水蛭網站（Leech websites）的市場現況[211]，2020 年 6 月，日本通過修訂《著作權法》及《節目作品登記特別規定法》的部分修正（著作権法及びプログラムの著作物に係る登録の特例に関する法律の一部を改正する法律），禁止非法下載音樂和視頻等，這項新法律還對帶有盜版下載鏈接的水蛭網站進行監管，這些網站造成的損失估計高達 3000 億日元或 27.5 億美元。東京監管機構的一項研究顯示，漫畫、動漫和視頻遊戲等日本娛樂的在線盜版在 2021 年造成了約 2 萬億日元（150 億美元）的損失，比 2019 年增加了 5 倍[212]。

日本內容網站的市場現況，B9GOOD 是在中國運營的最大日本盜版動漫發行網站之一。是日語網站，但也含有部分中國著作，根據

[209] Debarpita banerjee. (2023, February 21). OTT Market Projections (2023 – 2027) – Asia Pacific. MUVI. https://www.muvi.com/blogs/ott-market-projections-for-apac-2023-2027

[210] OTT Video – Worldwide. (2023). Statista. https://www.statista.com/outlook/amo/media/tv-video/ott-video/worldwide

[211] Fahim Ahmed. (2020, August 17). Streaming Sites Taken Down As Japan Exerts Stricter Piracy Laws. Search Medium. https://medium.com/the-crown-writer/streaming-sites-taken-down-as-japan-exerts-stricter-piracy-laws-131ee8403013

[212] Online Anime and Manga Piracy Caused ¥2 Trillion Loss in 2021, Watchdog Says. (2023, April 22). Thejapantimes. https://www.japantimes.co.jp/news/2023/04/22/business/tech/online-piracy-japan-losses/

網路分析工具 SimilarWeb 資訊，從 2021 年 3 月至 2023 年 2 月，總共吸引了超過 3 億人次的觀看。然而，即使 B9GOOD 網站已經於 2023 年 3 月 27 日被關閉，還是有許多替代網站出現。B9GOOD 的日本使用者佔 95%比例，也就是在中國境內開的盜版動漫網站，卻是針對日本人為收視對象而經營的。盜版網站通常是通過刊載廣告來確保運營費和收益，日本國內的廣告業界團體加強自主約束，但國外廣告公司等一直是漏洞。日本持續與各國警察和業界團體共享訊息，在國內外查處盜版網站，同時強化措施制止企業在盜版網站上發佈廣告。

二、 政府角色

日本廣電主管機關為總務省，負責傳統廣播電視發照業務；而針對非法串流媒體設備之主要執法機關為跨部會執行，包括：內閣府、警察廳、總務省、法務省、文部科學省、經濟產業省。

三、 政策

（一）中國首例取締日本動畫盜版網站

因應六家日本動漫相關公司（Aniplex、Toei Animation、Toho、Namco Bandai Filmworks、TV Tokyo、NHK）的要求，內容產品海外流通促進機構（CODA）[213]代表相關方向中國相關部門投訴日本動畫盜版網站 B9GOOD，這也是日本首例此類型案件被揭發，也是查處海外運營者的示範案例。

2023 年 2 月 14 日至 3 月 21 日，中國江蘇省公安廳對相關人員進行拘留並搜查違法者之住所。經營者為重慶男性，透過盜版發行獲得了 600-700 萬元人民幣。另外有兩名上傳盜版內容的經營者，以及其他盜版內容分佈伺服器而賺取廣告費者也被審訊。

[213] The Operator of “Manga BANK” Was Exposed. Administrative Penalties Have Now Been Confirmed in China. (2022, July 14). CODA. https://coda-cj.jp/en/news/179/

四、 OTT 平台相關法規

日本法制目前並未納管 OTT TV 平台，相應的內容規範則全數劃歸網際網路內容之規範為之，主要規範法源為：適用《青少年網際網路環境整備法》（青少年インターネット環境整備法）及《特定電信業務提供者之損害賠償責任限制暨發訊者資訊開示法》（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律），主要針對規範網際網路服務提供者的相關作為義務，同時也明確規範發訊人、送訊人及相關權利人間之權利義務。

五、 OTT TV 機上盒監理政策

自 2019 年 4 月起，日本總務省開始舉辦有關對抗網路盜版方針相關檢討會議（インターネット上の海賊版サイトへのアクセス抑止方策に関する検討会），並陸續提出相關對策及報告，除對應網路盜版之政策外，同時考慮使用者之通訊隱私和確保網路自由使用等因素。

2020 年 12 月，總務省與相關政府機關、團體和業者協調合作，公布「總務省網絡盜版對策清單」（インターネット上の海賊版対策に係る総務省の政策メニュー）。目前，根據這份政策清單，持續推進相關措施。總務省打擊盜版相關措施主要包括下列四大項：

1. 提高使用者的數位素養。
2. 推動使用安全軟體。
3. 努力公開盜版者資訊。
4. 推動反盜版措施的國際合作[214]。

[214] 事務局. (2022, May 31).インターネット上の海賊版サイト対策に関する現状とりまとめ骨子. https://www.soumu.go.jp/main_content/000816832.pdf

六、 OTT TV 機上盒監理法規

隨著數位和網路技術的進步，各種音樂、動畫、電影、漫畫等多樣的內容在網際網路上越來越跨國流通。同時，網際網路上也出現大量流通未經授權的著作權侵害內容，這些內容讓使用者可以在未支付權利擁有者合理報酬的情況下使用。由於盜版造成的損害日益嚴重，日本政府於 2019 年 10 月制定了「對抗網路上盜版的綜合對策和時間表」（インターネット上の海賊版に対する総合的な対策メニュー及び工程表について）[215]（於 2022 年 4 月更新），旨在推動全體政府通力合作，提出有效的對策措施。其與違法 OTT TV 機上盒相關執法規定摘要如下：

（一）《著作權法》

1. 複製權

著作者擁有對其著作物進行複製的專有權利[216]。

2. 公開傳輸權

著作者專有對其著作物進行公開傳輸（包括自動公開傳輸的情況，其中包括將其送達至公開傳輸的狀態。）的權利。著作者專有透過接收裝置公開傳輸其著作物的權利[217]。

3. 非法下載侵權內容

著作物的目的是供個人、家庭或其他有限範圍內的使用（以下稱為「私人使用」），除下列情況，使用者可以複製著作物。意即在符合下列情況，即使為「私人使用」仍為侵權行為：

---

[215] 内閣府、警察庁、総務省、法務省、外務省、文部科学省、経済産業省. (2021, April 9). インターネット上の海賊版に対する 総合的な対策メニュー及び工程表について. https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2020/pdf/kaizoku_taisaku.pdf

[216] 著作権法第 21 条。

[217] 著作権法第 23 条。

(1) 使用自動複製機器（具有複製功能，且相關裝置全部或主要部分實現自動化的機器）進行複製，以供公眾使用為目的。

(2) 使用者透過規避技術保護手段或者經特殊轉換後的著作物、表演、唱片或廣播或有線廣播中的音頻或影像進行復原，使得能夠進行技術保護手段防止的行為或者阻止技術保護手段防止的行為的結果失去作用，並在明知該情況下進行複製。

(3) 使用者透過接收侵犯著作權的自動公眾傳輸（包括在國外進行的自動公眾傳播，如果在國內進行則構成著作權侵犯）進行數位方式錄音或錄像，在明知該情況下進行複製。

(4) 使用者通過接收侵犯著作權的自動公眾傳輸（包括在國外進行的自動公眾傳輸，如果在國內進行則構成著作權侵犯）而進行的數位方式複製，在明知該情況下進行複製（除非該著作物的類型和用途以及特定侵犯複製的方式與不會不當地損害著作權人的利益等特殊情況）[218]。

4. 停止侵權請求

著作者、著作權者、出版權者、演出家或著作隣接權者有權要求侵害其著作者人格權、著作權、出版權、演出家人格權或著作隣接權的人或可能侵害其權利的人停止或預防侵害。著作者、著作權者、出版權者、演出家或著作隣接權者在提出上述請求時，也有權要求銷毀侵害行為所涉及的物品、侵害行為所產生的物品，或是專供侵害行為使用的機器或器具等，以及其他必要的措施來停止或預防侵害[219]。

[218] 著作権法第 30 条。
[219] 著作権法第 112 条。

5. 規避技術保護措施

以下各項中的任何一個符合者，將受到三年以下的有期徒刑或三百萬日元以下的罰金，或二者合併處罰：（1）銷售、出租、製造、進口、擁有、提供或公開傳輸技術保護措施的迴避裝置（包括能夠容易組裝的該裝置的全部零件）或迴避技術保護措施的功能程式的複製物給公眾，或進行公開傳輸或使其可傳輸的行為（若該裝置或程式的功能包含侵犯著作權等之行為，以技術保護措施迴避實現侵權或依第 113 條第 6 項之規定視為侵犯著作權、出版權或著作隣接權而供特定迴避利用目的者除外）。（2）業者以業務為目的，按照公眾需求提供技術保護措施的迴避或技術利用制限手段的迴避者。（3）依照第 113 條第 2 項之規定被視為侵犯著作權、出版權或著作隣接權的行為者。（4）依照第 113 條第 7 項之規定被視為侵犯技術保護措施相關著作權等或技術利用限制手段相關著作權、出版權或著作隣接權的行為者。（5）以營利為目的，依照第 113 條第 8 項之規定被視為侵犯著作者人格權、著作權、出版權、表演者人格權或著作隣接權的行為者。（6）以營利為目的，依照第 113 條第 10 項之規定被視為侵犯著作權或著作隣接權的行為者。

（二）《提供者責任限制法》

《提供者責任限制法》（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律）於 2001 年制定，針對特定的通信服務提供者，例如：網際網路服務供應商（ISP）和電信業者，在特定條件下可限制其對於損害賠償責任，並強制揭露違法發信者的資訊。其主要規範內容如下：

1. 損害賠償責任的限制（安全港條款）

特定的通信服務提供者除非符合特定要件，即使第三方進行著作權侵害等非法行為，該提供者對於此類行為引起的損害不負責任[220]。

2. 發信者資訊的揭露

特定的通信服務提供者有義務揭露從事著作權侵害、誹謗等非法行為的發信者的資訊。法院可透過命令要求 ISP 業者提供發信者的 IP 位置、姓名等資訊[221]。

過去，向外國企業要求揭露發信者資訊的請求需要透過大使館並等待很長的時間，但新修法將使相關資訊請求之提出更簡單，例如透過 EMS 向外國企業發送投訴表格。因此，預計盜版網站侵犯著作權的案件將能得到更快的處理。

惟上述損害賠償責任的限制和發信者資訊的揭露僅在特定條件下適用。具體而言，ISP 業者平時還是必須對從事非法行為的用戶進行警告，並採取措施以警示其不再進行相同行為[222]。

七、 OTT TV 機上盒監理技術

關於日本的監理技術，以下案例採用跨國共同合作，打擊犯罪跟關閉機房，以阻斷 OTT TV 機上盒的視聽服務，執行技術策略如下：

因應六家日本動漫公司的要求，日本內容產品海外流通促進機構（CODA）[223]代表，向中國相關部門投訴動畫盜版網站「B9GOOD」，這是日本查處海外運營者跨國合作的首例。

---

[220] 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律，第 3 条。

[221] 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律，第 5 条、第 6 条。

[222] 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律，第 4 条。

[223] The Operator of “Manga BANK” Was Exposed. Administrative Penalties Have Now Been Confirmed in China. (2022, July 14). CODA. https://coda-cj.jp/en/news/179/

1. **白帽駭客（White Hacker）技術人員的協助：**運營者訊息難以鎖定，營者通常會借助海外網路服務等來隱藏身分。這次是經由白帽駭客技術人員的協助，對網站進行分析，才得以成功獲取了訊息。此外，非法網站常有規避技術，像是 Leech 網站引導公眾非法上傳侵權內容的網站，網站的運營商將影片資料上傳到海外伺服器，它們提供連結，而不是直接非法上傳檔案，並且不負責刪除內容或聯絡非法上傳的來源。
2. **與海外當地相關部門進行直接交涉：**日本方面以「國際調查互助」程序要求海外相關部門進行調查，但這種方法涉及多個機構，需要花費大量的時間和精力，本案主要是因為 CODA 在中國有辦事處才得以申訴。

第六節　新加坡

一、市場現況

從事新加坡本地使用的電信設備進口和銷售的公司必須是持有新加坡資通訊媒體發展局（Infocomm Media Development Authority，IMDA）有效電信經銷商許可證的設備供應商/經銷商。故未取得許可證之業者不可任意銷售相關機上盒設備。新加坡刑事調查部門官員於 2022 年突擊搜查森林電子購物廣場（Sim Lim Square）的幾家零售商店，共查獲超過 2,500 套非法 OTT TV 機上盒，其中廣場中價格較高的機型提供英超聯賽足球比賽等體育內容。這次的打擊行動，是在封鎖了九十九個網址之後進行的，這些網址允許用戶非法瀏覽韓劇內容和體育賽事[224]。

[224] Ang Qing.(2022, October 4).17 People Arrested for Suspected Involvement in Selling Illegal Streaming Devices. The Straits Times. https://www.straitstimes.com/singapore/courts-crime/17-people-arrested-for-suspected-involvement-in-selling-illegal-streaming-devices

二、 政府角色

新加坡廣播電視與視聽服務內容之主管機關為新加坡資通訊媒體發展局（Infocomm Media Development Authority，IMDA），隸屬於新加坡資訊與通訊部（Ministry of Communication and information）。

三、 政策

（一）封鎖網站和應用程式

這些網址允許使用者非法串流傳輸內容和體育節目，包括：英超聯賽。新加坡屏蔽了近 200 個跨網站域和侵權應用程式。

（二）抓零售業者和 IT OEM 廠商

刑事調查局查獲至少有七家商店在 Sim Lim Square 出售可訪問盜版線上串流媒體或內容的非法 Android 機上盒。分發和銷售非法串流媒體設備是嚴重的違法行為。

IT OEM 廠商 Synnex Trading 因銷售非法 Android 機上盒而在法庭上被罰款 160,800 美元（詳如後續新加坡判決說明）。

（三）跨國國際合作

新加坡的大多數球迷合法觀看熱門聯賽，FAPL 地方當局合作，針對那些提供非法訪問的人採取行動。

四、 OTT 平台相關法規

新加坡與視聽服務相關之法規包括：《廣電法》（Broadcasting Act）、《電子傳輸法》（The Electronic Transactions Act）、《電影法》（Film Act）、《公共娛樂法》（Public Entertainments Act）、《通訊法》（Telecommunication Act）與《不良出版法》（Undesirable Publications Act）等。

依據新加坡《廣電法》第 2 條第 1 項定義，廣播服務（Broadcasting service）為：「其傳輸的標誌或信號（無論是否加密）包括：（a）任何

能夠以視覺圖像的形式接收、或接收並顯示的節目，無論是動態的還是靜態的；(b) 任何可供接收之音訊節目；(c) 任何可供接收或接收並顯示由視覺圖像（無論是動態的還是靜態的）和聲音組合而成的節目。[225]」換言之，無論傳遞技術為何（無線、有線、衛星），只要提供影音訊號之服務皆屬於廣播服務，故提供影音服務之 OTT TV 平台也屬於新加坡廣電法下之「廣播服務」。

又依據該法第 8 條第 1 項規定，所有「須照廣電服務」均應取得「廣電執照」(Broadcasting Licence)：「未經管理局根據本條或第 9 條所授予的廣播許可證，任何人不得在新加坡提供任何需要許可的廣播服務或從新加坡提供這類廣播服務[226]」。依據本法之附件二，提供 20 項需要在新加坡取得執照之廣播服務[227]，包括：免費全國電視服務（Free-to-Air Nationwide Television Services）、免費地區電視服務（Free-to-air localized television service）、免費國際電視服務（Free-to-air international television service）、國內訂閱電視服務（Subscription nationwide television services）等。

依據上述規定，在新加坡境內和/或從新加坡向特定小眾市場提供電視服務以及通過網路傳輸的電視服務的運營商需要取得小眾電視服務執照（Niche Television Service Licence），其許可期限五年，服務中所提供之內容需要符合「OTT、VOD 與小眾服務內容規則」（Content Code for Over-the-Top（OTT）, Video-on-Demand（VOD）and Niche Services）及《2019 線上不實內容與操控防止法》(Protection from Online Falsehoods and Manipulation Act 2019）等相關規範[228]。

---

[225] Broadcasting Act, Art. 2(1).
[226] Broadcasting Act, Art. 8(1).
[227] Broadcasting Act, SECOND SCHEDULE Licensable broadcasting services.
[228] Over-the-Top (OTT) TV (Niche) Licence. (2023, July 13). Infocomm Media Development Authority. https://www.imda.gov.sg/regulations-and-licensing-listing/over-the-top-tv-niche-licence

五、 OTT TV 機上盒監理政策

新加坡和臺灣，都是在《著作權法》中明訂對非法 OTT TV 機上盒之相關處罰，作法上警察積極查緝市場上的非法 OTT TV 機上盒，併用靜態封網[229]。

六、 OTT TV 機上盒監理法規

（一）《著作權法》

新加坡《著作權法》（Copyright Act）規定了保護著作權和打擊盜版行為的相關規定，確保原創著作受到適當的保護。和非法 OTT TV 機上盒侵權之條文包括下列幾項：

1. 侵犯著作權的行為

按《著作權法》第 146 條規定，在新加坡境內進行或授權在新加坡境內進行著作權所涵蓋的任何行為而不擁有著作權或未取得授權即為侵權；在廣播或有線節目的情況下，進行包括接收廣播或節目和透過任何物品或物件使用包含的視覺圖像和聲音的行為，皆屬著作權之侵害[230]。

2. 透過裝置或提供服務等方式獲取未經授權著作侵權

按《著作權法》第 150 條規定，下列行為構成著作權侵權：

(1) 未經著作權人之授權，將該著作傳輸給公眾。

(2) 在著作傳輸給公眾前或之後進行以下任何行為：

i. 製造用於獲得商業利益的裝置。

ii. 在商業上交易該裝置。

iii. 進口用於商業交易的裝置。

iv. 銷售裝置，對著作權人造成損害。

[229] 新加坡 2021 年《著作權法》之修正重點及評析.(2022).智慧財產權月刊.

[230] Copyright Act, Art. 146.

v. 向公眾提供服務，包括：以付費方式提供服務；或與裝置的銷售一同提供服務；該裝置或服務能夠促進對該著作的訪問；知道或理應合理地知道該裝置或服務能夠促進未經著作權所有人授權的著作被公眾訪問，並基於商業利益[231]。

3. 禁止訪問公然侵權的線上位置

按《著作權法》第 325 條到第 328 條規定，當權利擁有人發現某個網絡位置明顯侵犯其著作權著作或受保護表演的權利，並且該網絡位置是由網絡通訊服務供應商提供的，權利擁有人可以向法院申請下達「訪問禁用令」（Access disabling order），要求該網絡通訊服務供應商採取合理步驟禁止對該網路位置的訪問。

在申請禁用訪問令前，權利擁有人需向相關網路位置的所有者和網絡通訊服務供應商發出通知，告知其侵權情況並表明將申請禁用訪問令。但在一些情況下，如果權利人無法找到該網絡位置的所有者或無法提供通知，法院可以免除這一要求。法院在做出禁用訪問令的決定時，必須考慮多方面的因素，包括：對權利人可能造成的損害、網絡通訊服務供應商執行的負擔、技術可行性、有效性、對網絡通訊服務供應商業務運營的可能影響等。

七、 OTT TV 機上盒監理技術

關於新加坡的監理技術，以下案例採用網站封鎖、跨國共同合作，抓零售商和 IT OEM 廠商，以阻斷 OTT TV 機上盒的視聽服務，執行技術策略如下：

[231] Copyright Act, Art. 150.

（一）定期網站屏蔽[232]

依據反盜版聯盟（Coalition Against Piracy）2023 年針對盜版情況之消費者調查，新加坡在經過近十年的網站封鎖後，新加坡的消費者盜版率是亞太地區最低的，只有 39%的消費者觀看盜版。新加坡是最早允許權利人透過司法措施屏蔽網站，保護其內容的國家之一。

調查顯示，定期網站屏蔽不僅可以阻止消費者線上訪問盜版內容，還可以促使他們轉向合法來源，平均有 20%的消費者訂閱付費服務，平均超過 40%的消費者會訪問合法的免費內容服務。

人們對網絡盜版相關風險的認識也不斷增強，該地區每個市場中至少 80%的消費者明確表示盜版會帶來負面後果。而消費者意識到、感知到的損害會因失業、對創意產業的影響以及個人計算機和設備上惡意軟體感染的風險而異。

（二）IT OEM 廠商銷售非法 OTT TV 機上盒被鉅額罰款[233]

盜版是英超聯賽自 2019 年在新加坡設立辦事處以來一直致力於解決的問題之一。英超聯賽已與警方密切合作，支持突襲行動以強化當局打擊盜版的承諾，並且支持《著作權法》的修訂，清楚訴求盜版是非法的。新加坡大多數球迷都是合法觀看熱門聯賽，英超聯賽將繼續與地方當局合作，針對那些提供非法觀看機會的業者採取法律行動。

2019 年英超聯賽和其他權利持有者，在打擊未經授權的賣家取得里程碑的勝利。IT OEM 廠商 Synnex Trading 因銷售非法 OTT TV Android 電視盒而在法庭上被罰款 160,800 美元，此次判決是在 2018 年開始的長達 22 個月法庭鬥爭之後做出的。

---

[232] Advanced Media Strategies LLC.(2023, May 15). Asia Pacific Consumer Surveys Show Benefits of Effective Site Blocking: AVIA-CAP. Piracy Monitor. https://piracymonitor.org/asia-pacific-consumer-surveys-show-benefits-of-effective-site-blocking-avia-cap/

[233] Ang Qing.(2022, October 4).17 People Arrested for Suspected Involvement in Selling Illegal Streaming Devices. The Straits Times. https://www.straitstimes.com/singapore/courts-crime/17-people-arrested-for-suspected-involvement-in-selling-illegal-streaming-devices

有了法律先例以及之後向其他OTT TV供應商發送的通知，FAPL發現在新加坡透過非法串流媒體設備提供其內容的賣家減少了80%。到目前為止，它已在新加坡屏蔽了近200個網站和侵權應用程式的域名。

第七節　中國大陸

一、市場現況

第一次有人為日本市場經營漫畫盜版網站的人在海外受到懲罰[234]。2022年6月15日，中國重慶市文化市場執法總局以違反《資訊網路傳輸權保護條例》，對居住在重慶經營多個盜版網站、漫畫網站、漫畫銀行並且未經權利人許可分銷漫畫著作的男子處以沒收犯罪收益（約33萬日元）的行政處罰，及3萬元人民幣的罰款。

前述所提美國貿易代表署（Office of the United States Trade Representative，USTR）發布最新《2023特別301報告》點名「非法網路協定電視（IPTV）」猖獗的國家包括臺灣、中國、香港、泰國、越南、墨西哥、加拿大和巴西等。報告指出，伊拉克是生產預裝盜版IPTV 應用程式之衛星接收器的重鎮，**而中國大陸則是相關設備的製造中心。**

此外，將中國大陸、印度、阿根廷、智利、印尼、俄羅斯和委內瑞拉7個國家繼續列為優先觀察名單；被列入觀察名單的22個國家則包括保加利亞、加拿大、哥倫比亞、越南、泰國，而白俄羅斯是唯一新增的國家。報告指出，中國大陸在保護智慧財產權方面的改革步

[234] The Operator of “Manga BANK” Was Exposed. Administrative Penalties Have Now Been Confirmed in China. (2022, July 14). CODA. https://coda-cj.jp/en/news/179/

伐放緩，目前仍未解決其技術轉讓、商業機密、惡意商標、假冒、網路盜版等長期問題。

二、 政府角色

中國大陸之媒體制度相當特殊，主管機關為國家廣電總局、國家工信部、國家市場監督管理總局和國家發改委等，國家廣電總局主要負責制定數位電視行業管理規章和發展規劃，同時對數位電視網路運營、數位電視節目內容製作、數位電視有關技術政策和行業標準的制定及實施、數位電視設備器材的入網認定[235]等方面進行監督管理。

三、 政策

大陸的媒體制度特殊，媒體所有權主要由國家所有，內容部分也有嚴密控管，根據《國務院關於授權國家網路資訊辦公室負責網際網路資訊內容管理工作的通知》（国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知），自 2014 年 8 月 26 日起，國家網路資訊辦公室（国家互联网信息办公室）負責全國網際網路資訊內容管理工作，並負責監督管理執法，中國政府對網路內容進行審查的方式採取多樣、多層次、跨部門之作法。

2015 年廣電總局發出《關於依法嚴厲打擊非法電視網絡接收設備違法犯罪活動的通知》（关于依法严厉打击非法电视网络接收设备违法犯罪活动的通知），明文規定所有透過 USB 等方式，安裝程式後就可以收看非官方許可之內容的設備，都屬於非法設備，此一禁令頒布後，已有效控制了某些機上盒的販售與流通。

[235] 「入網認定」指在某些網路或系統中，確認或驗證一個設備、使用者或應用程式是否被允許連接或訪問該網路或系統的過程。這個過程通常涉及到身份驗證和授權措施，以確保只有合法的設備、使用者或應用程式能夠進入網路或系統，從而保障網路的安全性和可靠性。

四、 OTT 平台相關法規

中國大陸透過各種政策法規，逐漸把 OTT TV 等新興媒體納入了原本的廣電媒體體制之下，需要取得執照並接受嚴密的管制才能提供服務。有關 OTT TV 之主要規範包括：《廣播電視管理條例》（广播电视管理条例）、《網際網路視聽節目服務管理規定》（互联网视听节目服务管理规定）、《網際網路等資訊網路傳播視聽節目管理辦法》（互联网等信息网络传播视听节目管理办法）。2011 年 7 月《關於嚴禁通過網際網路經機上盒向電視機終端提供視聽節目服務的通知》（关于严禁通过互联网经机顶盒向电视机终端提供视听节目服务的通知）、10 月《關於持有網際網路電視牌照機構運營管理要求的通知》（持有互联网电视牌照机构运营管理要求）等，重申網路電視需有營運牌照，而且網路電視內容服務只能接入廣電總局批准設立的 OTT TV 平台。包括 CNTV、BesTV、Wasu、SMC、CIBN、MangoTV、CNR 等，只有這些牌照持有者才可以合法經營 OTT 視訊媒體，其他業者只能跟這些業者合作[236]。

五、 OTT TV 機上盒監理政策

（一）制定標準

為進一步加強對中國大陸網際網路電視接收設備的管理，保障資訊安全和整體利益，防範和抵制不良文化的影響，保證經營者和消費者的合法權益，2016 年中國大陸工業和資訊化部（工业和信息化部）發布《網際網路電視接收設備技術規範》標準，規定了網際網路電視接收設備的技術要求，描述了相應的測試方法。還適用於支援通過網際網路接收廣播電視等視聽節目的電視接收設備的開發、測試和生產；國家廣播電視總局於 2021 年 1 月 20 日發布《網際網路電視總體技術

[236] 賴祥蔚. (2018). 中國大陸管制下的網路視訊媒體策略. 展望與探索月刊, 16(16), 119.

要求》（互联网电视总体技术要求）[237]、《網際網路電視集成平台技術要求》（互联网电视集成平台技术要求）[238]、《網際網路電視內容服務平台技術要求》（互联网电视内容服务平台技术要求）[239]和《網際網路電視集成平台節目集成系統技術要求及接口規範》（互联网电视集成平台节目集成系统技术要求及接口规范）[240]等四項標準文件，現為中華人民共和國廣播電視和網絡視聽推薦性行業標準。

（二）「劍網 2020」行動

中國大陸智財局、工業和資訊化部、公安部、國家網路資訊辦公室於 2020 年 6 月至 10 月聯合開展第 16 次打擊網路侵權盜版「劍網」行動。此行動的工作目標是強化著作權執法監管力度，嚴厲打擊盜版視聽著作、電商平台、社交平台、線上教育等領域的侵權盜版行為，著力規範網路遊戲、網路音樂、知識分享等平台。行動包括：網路視聽著作著作權整治：強化對互動式網路電視（IPTV）、智慧電視機上盒（OTT）、智慧終端機、視頻播放機等串流媒體軟硬體的著作權監管，嚴厲打擊通過串流媒體傳播侵權盜版著作行為；集中關閉、封堵「三無」侵權盜版網站，深挖透過境外伺服器傳播盜版著作的國內源頭，切斷灰色產業鏈[241]。

其他行動包括：鞏固重點領域著作權治理成果，通知要求各相關部門查辦案件，擴展宣傳教育，並加強組織領導，要求各組織及時報送工作報告，持續鞏固網路文學、動漫、應用市場等專項治理成果，營造良好的網路著作權環境。

[237] GYT 342-2021.
[238] GYT 343-2021.
[239] GYT 344-2021.
[240] GYT 345-2021.
[241] 整理自「国家版权局等关于开展打击网络侵权盗版“剑网 2020”专项行动的通知」。

六、 OTT TV 機上盒監理法規

由於非法 OTT TV 機上盒可以幫助民眾下載盜版或是盜錄的電影內容，讓民眾可在電視機等終端上免費觀看盜版影音，除對智慧財產權之侵害外，也涉及了大量未經官方審查與許可之境外節目的引入，因此引起中國大陸官方的注意，非法 OTT TV 機上盒之販賣被廣電總局強力禁止。其相關規範包括：

（一）《中華人民共和國著作權法》

1. 播放視聽作品、錄像製品應取得許可

按《中華人民共和國著作權法》(中华人民共和国著作权法）第 48 條規定：「電視台播放他人的視聽作品、錄像製品，應當取得視聽作品著作權人或者錄像製作者許可，並支付報酬；播放他人的錄像製品，還應當取得著作權人許可，並支付報酬。[242]」

2. 規避保護技術措施

按《中華人民共和國著作權法》第 49 條規定：「為保護著作權和與著作權有關的權利，權利人可以採取技術措施。未經權利人許可，任何組織或者個人不得故意避開或者破壞技術措施，不得以避開或者破壞技術措施為目的製造、進口或者向公眾提供有關裝置或者部件，不得故意為他人避開或者破壞技術措施提供技術服務。但是，法律、行政法規規定可以免除的情形除外。本法所稱的技術措施，是指用於防止、限制未經權利人許可瀏覽、欣賞作品、表演、錄音錄像製品或者通過資訊網路向公眾提供作品、表演、錄音錄像製品的有效技術、裝置或者部件。[243]」

[242] 中华人民共和国著作权法第 48 条。
[243] 中华人民共和国著作权法第 49 条。

3. 侵權民事責任

按《中華人民共和國著作權法》第 53 條規定相關之侵權態樣及民事責任，包括：

(1) 未經著作權人許可，複製、發行、表演、放映、廣播、彙編、透過資訊網路向公眾傳播其作品的，本法另有規定除外。

(2) 出版他人享有專有出版權的圖書的。

(3) 未經表演者許可，複製、發行錄有其表演的錄音錄像製品，或者透過資訊網路向公眾傳播其表演的，本法另有規定除外。

(4) 未經錄音錄像製作者許可，複製、發行、透過資訊網路向公眾傳播其製作的錄音錄像製品的，本法另有規定的除外。

(5) 未經許可，播放、複製或者透過資訊網路向公眾傳播廣播、電視的，本法另有規定的除外。

(6) 未經著作權人或者與著作權有關的權利人許可，故意避開或者破壞技術措施的，故意製造、進口或者向他人提供主要用於避開、破壞技術措施的裝置或者部件的，或者故意為他人避開或者破壞技術措施提供技術服務的，法律、行政法規另有規定的除外。

(7) 未經著作權人或者與著作權有關的權利人許可，故意刪除或者改變作品、版式設計、表演、錄音錄像製品或者廣播、電視上的權利管理資訊，知悉或者應當知悉作品、版式設計、表演、錄音錄像製品或者廣播、電視上的權利管理資訊未經許可被刪除或者改變，仍然向公眾提供的，法律、行政法規另有規定除外。

(8) 製作、出售假冒他人署名的作品。

有上述侵權行為，應當根據情況，承擔本法第 52 條規定的民事責任[244]；侵權行為同時損害公共利益的，由主管著作權的部門責令停止侵權行為，予以警告，沒收違法所得，沒收、無害化銷毀處理侵權複製品以及主要用於製作侵權複製品的材料、工具、設備等，違法經營額五萬元以上的，可以並處違法經營額一倍以上五倍以下的罰款；沒有違法經營額、違法經營額難以計算或者不足五萬元的，可以並處二十五萬元以下的罰款；構成犯罪的，依法追究刑事責任[245]。

中國大陸人民法院審理著作權糾紛案件，應權利人請求，對侵權複製品，除特殊情況外，責令銷毀；對主要用於製造侵權複製品的材料、工具、設備等，責令銷毀，且不予補償；或者在特殊情況下，責令禁止前述材料、工具、設備等進入商業管道，且不予補償[246]。

（二）《中華人民共和國刑法》

1. 侵犯著作權[247]

按《中華人民共和國刑法》（中华人民共和国刑法）第 217 條規定著作權相關之侵權態樣及刑事責任。主要行為有，以營利為目的，有下列侵犯著作權或者與著作權有關的權利的情形之一，違法所得數額較大或者有其他嚴重情節的，處三年以下有期徒刑，並處或者單處罰金；違法所得數額巨大或者有其他特別嚴重情節的，處三年以上十年以下有期徒刑，並處罰金：

[244] 根據情況承擔停止侵害、消除影響、賠禮道歉、賠償損失等民事責任。
[245] 中华人民共和国著作权法第 53 条。
[246] 中华人民共和国著作权法第 54 条第 5 項。
[247] 中华人民共和国刑法第 219 条。

(1) 未經著作權人許可，複製發行、透過資訊網路向公眾傳播其文字作品、音樂、美術、視聽作品、計算機軟體及法律、行政法規規定的其他作品。

(2) 出版他人享有專有出版權的圖書。

(3) 未經錄音錄像製作者許可，複製發行、透過資訊網路向公眾傳播其製作的錄音錄像。

(4) 未經表演者許可，複製發行錄有其表演的錄音錄像製品，或者透過資訊網路向公眾傳播其表演。

(5) 製作、出售假冒他人署名的美術作品。

(6) 未經著作權人或者與著作權有關的權利人許可，故意避開或者破壞權利人為其作品、錄音錄像製品等採取的保護著作權或者與著作權有關的權利的技術措施。

犯第 219 條規定之罪，對單位判處罰金，並對其直接負責的主管人員和其他直接責任人員，依照相關規定處罰[248]。

2. 未經許可販賣違法物品（非法經營罪）[249]

按《中華人民共和國刑法》第 225 條規定，違反國家規定，有下列非法經營行為之一，擾亂市場秩序，情節嚴重處五年以下有期徒刑或者拘役，並處或者單處違法所得一倍以上五倍以下罰金；情節特別嚴重的，處五年以上有期徒刑，並處違法所得一倍以上五倍以下罰金或者沒收財產：

(1) 未經許可經營法律、行政法規規定的專營、專賣物品或者其他限制買賣的物品。

(2) 買賣進出口許可證、進出口原產地證明以及其他法律、行政法規規定的經營許可證或者批准文件。

[248] 中华人民共和国刑法第 220 条。
[249] 中华人民共和国刑法第 225 条。

(3) 未經國家有關主管部門批准非法經營證券、期貨、保險業務的，或者非法從事資金支付結算業務的。

(4) 其他嚴重擾亂市場秩序的非法經營行為。

按相關規定，販賣違法機上盒之行為屬於違反國家規定，從事生產、銷售非法電視網路接收設備（含軟體），以及為非法廣播電視接收軟體提供下載服務、為非法廣播電視節目頻道接收提供連結服務等營利性活動，擾亂市場秩序，個人非法經營數額在五萬元以上或違法所得數額在一萬元以上，單位非法經營數額在五十萬元以上或違法所得數額在十萬元以上[250]，按照非法經營罪追究刑事責任。

3. 利用計算機實施詐騙

按《中華人民共和國刑法》第 287-2 條規定，明知他人利用資訊網路實施犯罪，為其犯罪提供網路接入、伺服器託管、網路存儲、通訊傳輸等技術支持，或者提供廣告推廣、支付結算等幫助，情節嚴重的，處三年以下有期徒刑或者拘役，並處或者單處罰金。單位犯前款罪的，對單位判處罰金，並對其直接負責的主管人員和其他直接責任人員，依照第一款的規定處罰[251]。

（三）《資訊網路傳播權保護條例》

1. 資料提供

按《資訊網路傳播權保護條例》(信息网络传播权保护条例）第 13 條:「著作權行政管理部門為了查處侵犯資訊網路傳播權的行為，可以要求網路服務提供者提供涉嫌侵權的服務物件的姓名（名稱）、聯繫方式、網路位址等資料。」

[250] 「關於依法嚴厲打擊非法電視網路接收設備違法犯罪活動的通知」，新廣電發（2015）229 號文。

[251] 中华人民共和国刑法第 287-2 条。

2. 刪除、封鎖權

權利人若認為受到侵權可向 ISP 業者請求刪除及封鎖提供侵權作品之網路位置，主要依據為《資訊網路傳播權保護條例》第 14 條前段:「對提供資訊存儲空間或者提供搜索、連結服務的網路服務提供者，權利人認為其服務所涉及的作品、表演、錄音錄影製品，侵犯自己的資訊網路傳播權或者被刪除、改變了自己的權利管理電子資訊的，可以向該網路服務提供者提交書面通知，要求網路服務提供者刪除該作品、表演、錄音錄影製品，或者斷開與該作品、表演、錄音錄影製品的連結。」

ISP 業者在收到通知後，依據同條例第 15 條規定應當立即刪除涉嫌侵權的作品、表演、錄音錄影製品，或者斷開與涉嫌侵權的作品、表演、錄音錄影製品的連結，並同時將通知書轉送提供作品、表演、錄音錄影製品的服務物件；服務物件網路位址不明、無法轉送的，應當將通知書的內容同時在資訊網路上公告。但若服務物件接到網路服務提供者轉送的通知書後，認為其提供的作品、表演、錄音錄影製品未侵犯他人權利的，可以向網路服務提供者提交書面說明，要求恢復被刪除的作品、表演、錄音錄影製品，或者恢復與被斷開的作品、表演、錄音錄影製品的連結（同條例第 16 條）。

3. 侵權的民刑事責任、沒收

按《資訊網路傳播權保護條例》第 18 條:「違反本條例規定，有下列侵權行為之一的，根據情況承擔停止侵害、消除影響、賠禮道歉、賠償損失等民事責任；同時損害公共利益的，可以由著作權行政管理部門責令停止侵權行為，沒收違法所得，並可處以 10 萬元以下的罰款；情節嚴重的，著作權行政管理部門可以沒收

主要用於提供網路服務的電腦等設備；構成犯罪的，依法追究刑事責任：

(1) 通過資訊網路擅自向公眾提供他人的作品、表演、錄音錄影製品的。

(2) 故意避開或者破壞技術措施的。

(3) 故意刪除或者改變通過資訊網路向公眾提供的作品、表演、錄音錄影製品的權利管理電子資訊，或者通過資訊網路向公眾提供明知或者應知未經權利人許可而被刪除或者改變權利管理電子資訊的作品、表演、錄音錄影製品的。

(4) 為扶助貧困通過資訊網路向農村地區提供作品、表演、錄音錄影製品超過規定範圍，或者未按照公告的標準支付報酬，或者在權利人不同意提供其作品、表演、錄音錄影製品後未立即刪除的。

(5) 通過資訊網路提供他人的作品、表演、錄音錄影製品，未指明作品、表演、錄音錄影製品的名稱或者作者、表演者、錄音錄影製作者的姓名（名稱），或者未支付報酬，或者未依照本條例規定採取技術措施防止服務物件以外的其他人獲得他人的作品、表演、錄音錄影製品，或者未防止服務物件的複製行為對權利人利益造成實質性損害的。」

按《資訊網路傳播權保護條例》第 19 條:「下列行為之一的，由著作權行政管理部門予以警告，沒收違法所得，沒收主要用於避開、破壞技術措施的裝置或者部件；情節嚴重的，可以沒收主要用於提供網路服務的電腦等設備，並可處以 10 萬元以下的罰款；構成犯罪的，依法追究刑事責任：

(1) 故意製造、進口或者向他人提供主要用於避開、破壞技術措施的裝置或者部件，或者故意為他人避開或者破壞技術措施提供技術服務的。

(2) 通過資訊網路提供他人的作品、表演、錄音錄影製品，獲得經濟利益的。

(3) 為扶助貧困通過資訊網路向農村地區提供作品、表演、錄音錄影製品，未在提供前公告作品、表演、錄音錄影製品的名稱和作者、表演者、錄音錄影製作者的姓名（名稱）以及報酬標準的。」

（四）其他規範

有效遏制非法電視網路接收設備違法犯罪活動，確保國家安全、社會穩定和民眾的利益，中國最高人民法院、最高檢察院、公安部及新聞出版廣播電影電視總局等主管機關陸續提出許多通知及規範性文件。簡述如下：

1.「持有網際網路電視牌照機構運營管理要求」（持有互联网电视牌照机构运营管理要求）對網路集成業務、內容業務、業務運營、終端產品管理進行細部規定和要求。

2.「專網及定向傳播視聽節目服務管理規定」（专网及定向传播视听节目服务管理规定）。

3.「關於嚴禁透過網際網路經機上盒和向電視機終端提供視聽節目服務的通知」（关于严禁通过互联网经机顶盒向电视机终端提供视听节目服务的通知）。

4.「關於不得超範圍安裝網際網路電視客戶端軟體的通知」（关于不得超范围安装互联网电视客户端软件的通知）。

5. 2015 年公布《關於依法嚴厲打擊非法電視網路接收設備違法犯罪活動的通知》(关于依法严厉打击非法电视网络接收设备违法犯罪活动的通知)：強調將嚴厲打擊非法電視網路接收設備違法犯罪活動，明確化有關非法電視網路接收設備的種類，包括「電視棒」等網路共享設備、非法網際網路電視接收設備以及用於收看非法電視、收聽非法廣播的網路軟體和行動網路客戶端軟體等，對於從事生產、銷售非法電視網路接收設備、提供非法廣播電視接收軟體下載服務、提供連結服務等營利性活動的，將依法追究刑事責任。
6. 「關於做好網際網路電視整頓改革工作的通知」(关于做好互联网电视整改工作的通知)。
7. 「關於進一步強化網際網路電視集成平台管理和規範傳播秩序的通知」(关于进一步强化互联网电视集成平台管理和规范传播秩序的通知)。
8. 「關於推進網際網路電視業務 IPv6 改造的通知」(关于推进互联网电视业务 IPv6 改造的通知)。
9. 「關於對網際網路電視集成平台開展年度內容安全檢查的通知」(关于对互联网电视集成平台开展年度内容安全检查的通知)。
10. 「最高人民法院關於審理侵犯網絡傳播權民事糾紛案件適用法律若干問題的規定」(最高人民法院关于审理网络侵权民事案件若干问题的规定)。

解釋有關網路民事侵權之相關疑義。與 OTT TV 相關侵權規範包括：

1. 網路使用者、網路服務提供者未經許可，透過資訊網路提供權利人享有資訊網路傳播權的作品、表演、錄音錄影製品，除法律、行政法規另有規定外，中國大陸人民法院應當認定其構成侵害資訊網路傳播權行為。透過上傳到網路伺服器、設置共享文件或者利用文件分享軟體等方式，將作品、表演、錄音錄影製品置於資訊網路中，使公眾能夠在個人選定的時間和地點以下載、瀏覽或者其他方式獲得，法院應當認定其實施了提供行為。
2. 有證據證明網路服務提供者與他人以分工合作等方式共同提供侵權內容，構成共同侵權行為的，法院應當判令其承擔連帶責任。網路服務提供者能夠證明其僅提供自動接入、自動傳輸、資訊存儲空間、搜索、連結、文件分享技術等網路服務，不構成共同侵權行為。

七、 OTT TV 機上盒監理技術

關於中國大陸的監理技術，中國大陸對於 OTT TV 採取嚴密的管制措施，廣電媒體更是只限於政府機構才能開辦，相關內容也有嚴密控管，必須經過嚴格的申請與審批程序，才能獲得拍攝與播出的審批。可運用嚴密管制阻斷 OTT TV 機上盒的視聽服務[252]。

[252] 賴祥蔚. (2018). 中國大陸管制下的網路視訊媒體策略.展望與探索月刊, 16(6), 117–118.

第三章 OTT TV 機上盒涉侵害智慧財產權之案例及應處作為分析

本章蒐集及分析我國及其他國家或區域組織 OTT TV 機上盒涉侵害智慧財產權之實際案例及應處作為。依據本計畫案委託機關之要求，蒐集我國 3 例，以及其他 3 個國家或區域組織 5 例。

1. 我國 3 例：

(1) 110 年度刑智上更（一）字第 6 號。

(2) 110 年度民著訴字第 81 號。

(3) 臺灣新北地方法院 110 年度聲扣字第 19 號（淨頻專案）。

2. 其他國家或區域組織 5 例：

(1) 英國：

i. The Football Association Premier League Ltd v British Telecommunications Plc & Ors（英超對 ISP 業者提出禁制令）

ii. R v William O'Leary & Terence O'Reilly

(2) 美國：

i. UNITED KING FILM DISTRIBUTION LTD, D.B.S. SATELLITE SERVICES （1998） LTD, HOT COMMUNICATION SYSTEMS LTD, RESHET MEDIA LTD, KESHET BROADCASTING LTD, v. DOES 1-10 d/b/a SDAROT.COM

ii. Joint Stock Co. Channel One Russ. Worldwide v. Infomir LLC。

(3) 新加坡：

i. Neil Kevin Gane v. Jia Xiaofeng and Synnex Trading Pte Ltd。

第一節　我國

一、110 年度刑智上更（一）字第 6 號

（一）案例事實

被告王○遠明知聯利等公司[253]各自經營頻道，並分別在頻道內播放自行製播而享有著作財產權或取得重製權、公開傳輸權之專屬授權之視聽著作，非經聯利等公司同意或授權與位於中國大陸真實姓名年籍不詳之成年人何○寧共同基於意圖銷售，而擅自以重製、公開傳輸之方法侵害他人著作財產權之犯意聯絡。由王○遠自民國 104 年 1 月間起，自何○寧取得設置機房之設備及費用後，由王○遠在其位在新北市之住處設置機房，並安裝電腦主機、數據機、解碼器、路由器、訊號強波器及電視盒等，接續在機房擷取由中華電信公司、全國數位公司、臺灣大寬頻等業者提供之電視盒傳遞至電視機之前開聯利等公司自行製播或受有專屬授權之視聽著作之有線電視頻道訊號，經由解碼器轉換為網路封包形式而重製，並即時藉由網際網路上傳至何○寧所架設之雲端伺服器，前開上傳至雲端伺服器之轉換為網路封包之影像聲音，再經由網際網路提供不特定消費者在安○盒子上安裝 App（軟體）觀看即時節目，而侵害聯利等公司之著作財產權。王○遠則自 104 年 1 月起至 107 年 6 月 21 日止，每月向何○寧請領款項。

（二）主要爭點及法律依據

1. 爭點：本案是否符合《著作權法》中所稱之公開傳輸及其對第 87 條第 1 項第 7 款之主觀犯意。

[253] 包括：聯利媒體股份有限公司、東森電視事業股份有限公司、超級傳播股份有限公司、緯來電視網股份有限公司、年代網際事業股份有限公司、壹傳媒電視廣播股份有限公司、中天電視股份有限公司、民間全民電視股份有限公司、八大電視股份有限公司、三立電視股份有限公司、飛凡傳播股份有限公司等 11 家公司。

2. 法律依據：《著作權法》第 91 條第 2 項之意圖銷售而擅自以重製之方法侵害他人之著作財產權罪、同法第 92 條擅自以公開傳輸之方式侵害他人之著作財產權罪、同法第 87 條第 1 項第 7 款。

（三）分析

1. 本案屬公開傳輸

《著作權法》第 26 條之 1 之立法說明及《著作權法》關於「公開傳輸」之定義「經以有線電、無線電之網路或其他通訊方法，藉聲音或影像向公眾提供或傳達著作內容，即屬公開傳輸」，而非只有限定公眾於其各自選定之時間或地點，只要以上述方法接收著作內容，始屬公開傳輸。

本案透過安○盒子即時節目之影音傳輸架構採用 P2P 技術，先由 MS 伺服器發佈串流媒體直播來源，再由各個 P2P 節點互相分享各影音片段。又本案起訴及告訴內容所涉及之特定節目僅限於直播觀看部分前開過程全然經由網際網路運行，不特定消費者更經由網際網路與著作提供者處於互動式關係，應評價為「公開傳輸」。

2. 法院認本案被告針對涉犯《著作權法》第 87 條第 1 項第 7 款無主觀犯意

本案安○盒子觀看即時節目之技術設定，已對公眾提供可公開傳輸著作之電腦程式或其他技術，然無證據顯示被告明知利用安○盒子之 App（軟體）之不特定消費者係透過 P2P 方式觀看即時節目，又經由網際網路傳遞聲音影像之方式並非僅有 P2P，傳統的網路資料傳送模式尚有 C/S（Client/Server）模式，故難認為被告對於利用安○盒子之 App(軟體)之不特定消費者係透過 P2P

方式觀看即時節目一事有所預見，故縱本案安○盒子安裝之 App 觀看即時節目之技術，客觀上係《著作權法》第 87 條第 1 項第 7 款規定之行為，然被告主觀對此毫無認識，難認屬於共同正犯之合同意思範圍。

（四）法院結論

王○遠共同意圖銷售而擅自以重製之方法侵害他人之著作財產權，係犯《著作權法》第 91 條第 2 項之意圖銷售而擅自以重製之方法侵害他人之著作財產權罪、同法第 92 條擅自以公開傳輸之方式侵害他人之著作財產權罪。處有期徒刑壹年，緩刑肆年，並應支付損害賠償。扣案之物均沒收，未扣案之犯罪所得沒收，於全部或一部不能沒收或不宜執行沒收時，追徵其價額。

二、 110 年度民著訴字第 81 號

（一）案例事實

被告銘淳公司等 4 人明知未獲原告授權，卻本於意圖銷售而擅自重製、公開播送、意圖供公眾網路重製、公開傳輸之故意，而向香港普視科技有限公司委託製造內建收視功能及可下載安裝播放程式之「元博普視 PV BOX」臺灣版數位電視機上盒（下稱 PVBOX 機上盒），並由銘淳公司負責進口，再由元博公司或鄭○銘自 108 年 1 月起自行或將系爭機上盒出售予被告金豐收公司等 5 人，再以每台約 3,580 元之價格轉售予不特定之消費者。

當消費者於購得系爭機上盒後，再由被告鄭○銘、李○晉、邱○博、蘇○森、陳○杰等人，未經原告同意分別指導或協助消費者下載安裝由銘淳公司所提供之「PV 直播」、「臺灣直播」電腦程式 App，或由消費者以 LINE、WeChat 方式聯繫被告鄭○銘並告知系爭機上盒之 MAC 碼後，由其協助聯絡大陸地區合作之業者開通系爭機上盒之

臺灣直播收視功能，使消費者得以使用系爭機上盒直接收看原告所有之電視頻道及節目，而共同侵害原告所示節目之公開播送及公開傳輸權，並違反《著作權法》第 87 條第 1 項第 7 款、第 8 款規定而侵害原告之著作權。

（二）主要爭點及法律依據

1. 爭點：被告是否侵害原告之公開傳輸權。

2. 法律依據：《著作權法》第 91 條第 2 項之意圖銷售而擅自以重製之方法侵害他人之著作財產權罪、同法第 92 條擅自以公開傳輸之方式侵害他人之著作財產權罪、《著作權法》第 87 條第 1 項第 7 款、第 8 款第 1 至 3 目。

（三）分析

1. 公開播送、公開傳輸及向公眾提供之定義

(1) 公開播送：指基於公眾直接收聽或收視為目的，以有線電、無線電或其他器材之廣播系統傳送訊息之方法，藉聲音或影像，向公眾傳達著作內容。由原播送人以外之人，以有線電、無線電或其他器材之廣播系統傳送訊息之方法，將原播送之聲音或影像向公眾傳達者，亦屬之。

(2) 公開傳輸：係指以有線電、無線電之網路或其他通訊方法，藉聲音或影像向公眾提供或傳達著作內容，包括使公眾得於其各自選定之時間或地點，以上述方法接收著作內容。著作人專有公開播送或公開傳輸其著作之權利，《著作權法》第 3 條第 1 項第 7 款、第 10 款、第 24 條第 1 項、第 26 條之 1 第 1 項分別定有明文。

(3) 向公眾提供：不以利用人有實際上之傳輸或接收之行為為必要，只要處於可得傳輸或接收之狀態為已足。

「公開傳輸」係指消費者透過網路，在各自選定之時間或地點，接收著作內容為其特色，與「公開播送」係由播送方基於公眾直接收聽或收視為目的，以有線電、無線電之廣播系統，向公眾傳達著作內容，消費者係居於被動之地位，無法選擇在何時何地接收，有所不同。現今網路發達與頻寬增加，科技發展之技術使得機上盒內得安裝設定相關之 App 應用程式，當機上盒連接網路執行該程式後，使用者即得與網路平台業者相連結，而接收觀賞其提供的影音內容，故機上盒為使用者與網路平台間之媒介，已非單純與第四台業者之連結，此種服務類型可使使用者不用限定時間而自行選定所需要的影音內容，而非受限於傳統第四台廣播系統僅得單向接受觀看之方式，該隨選影音之傳送方式應屬公開傳輸之行為。電視頻道及節目，並非居於被動地位，此種隨選影音之傳送方式即與《著作權法》所稱公開播送之方式有所不同，自無須再論原告所謂被告有侵害其公開播送權之主張，應認系爭機上盒固可公開傳輸原告所示之節目著作無誤。

提供「超連結」之行為是否符合《著作權法》第 3 條第 1 項第 10 款「公開傳輸」定義，基於技術中立原則，應以其技術本身客觀上之運作方式茲為認定。而所謂「超連結」，乃使用者藉由點選連結路徑開啟、新增外部網站，將使用者帶至該經連結之網頁為瀏覽，是超連結之技術手段只是「提供」外部原始已經存在足以供不特定大眾瀏覽、播放各該著作之「路徑」，事實上向公眾提供或傳達著作內容者為將節目影片上傳之外部影音平台之人，並不是提供超連結之人，故而單純提供超連結即與「公開傳輸」之構成要件不該當。

2. 第 87 條第 1 項第 7 款之構成要件

(1) 未經著作財產權人同意或授權。

(2) 圖供公眾透過網路公開傳輸或重製他人著作，侵害著作財產權。

(3) 對公眾提供可公開傳輸或重製著作之電腦程式或其他技術，而受有利益。該款所稱「對公眾提供可公開傳輸或重製著作之電腦程式或其他技術」，固不限於點對點（Peer to Peer）技術，任何對公眾提供可公開傳輸或重製著作之電腦程式或其他技術，均應包含在第 7 款範圍內，然無論係採用何種技術，行為人所提供之電腦程式或技術，仍需使得公眾本身得以「透過網路公開傳輸或重製他人著作」，始會構成本款視為侵害著作權之行為。使用者僅得透過系爭機上盒單純觀看節目，並無法透過網路「公開傳輸」或「重製」他人之著作，自不該當《著作權法》第 87 條第 1 項第 7 款之要件。

3. 第 87 條第 1 項第 8 款之構成要件

按《著作權法》第 87 條第 1 項第 8 款：「八、明知他人公開播送或公開傳輸之著作侵害著作財產權，意圖供公眾透過網路接觸該等著作，有下列情形之一而受有利益者：（一）提供公眾使用匯集該等著作網路位址之電腦程式。（二）指導、協助或預設路徑供公眾使用前目之電腦程式。（三）製造、輸入或銷售載有第一目之電腦程式之設備或器材。」渠等在銷售系爭機上盒之後，即可透過 Line 指導、協助購買系爭機上盒之使用者下載開通該機器專用可觀看臺灣電視直播頻道之應用程式，實質上亦等同於透過系爭機上盒提供 PV 直播、臺灣直播等應用程式之方式，供使用者透過網路接觸該等節目著作。為吸引消費者購買系爭機上

盒，已在該公司架設之「OTT 購物中心」網頁及「銘淳國際」臉書粉絲專頁等，以前揭廣告：「免費觀看 1500＋全球直播頻道、海量影視資源」、「第四台月租費 OUT」等文字，積極誘使公眾購買該公司之系爭機上盒而獲有利益，顯然具備侵害他人著作財產權之意圖。

（四）結論

本件原告依前揭規定請求被告銘淳公司等 4 人、金豐收公司、李○晉、邱○博、蘇○森連帶給付相關賠償金額准許。

三、 臺灣新北地方法院 110 年度聲扣字第 19 號（淨頻專案）

（一）案例事實

刑事局電信偵查大隊於 110 年 2 月起執行淨頻專案，並透過國家通訊傳播委員會協調中華電信股份有限公司、愛爾達電視股份有限公司、LiTV 及四季線上等國內大型 OTT 平台共同追查非法訊號來源。查出臺灣安○企業股份有限公司（亦為進口國內安○機上盒射頻審驗認證廠商）負責人黃○詮涉嫌夥同犯嫌洪○喬、犯嫌徐○揚分別向愛爾達、LiTV 等合法 OTT 影視平臺業者註冊會員，再透過○○科技網路有限公司（負責人：張○）及彼○○網路資訊股份有限公司（負責人:蔡○生)架設伺服主機，竊取 OTT 影視平臺業者訊號源憑證(m3u8 檔案)，然後透過破解視訊串流技術將合法影視轉傳到非法安○機上盒中[254]。

犯罪嫌疑人與美國網際網路服務供應商承租網址及 IP，明知緯來電視網股份有限公司等 63 家公司所經營之頻道，所播放視聽節目享

[254] 經濟部智慧財產局。(n.d.)。破獲非法機上盒違反《著作權法》，執行網域扣押案例。https://www.tipo.gov.tw/tw/dl-281050-34f6849d32e146d19906a6421c83f360.html

有著作權，設法使安◯盒子連結至未取得著作權之特定網址，公開傳輸上開視聽著作供安◯盒子使用者收看，而侵害著作財產權。

（二）主要爭點及法律依據

1. 爭點：域名是否可以成為形式強制處分制度下的扣押標的。

2. 法律依據：刑法第 38 條第 2 項規定，供犯罪所用、犯罪預備之物或犯罪所生之物，屬於犯罪行為人者，得沒收之。

（三）分析

本案於二波搜索結束之後，向臺灣新北地方法院聲請網域扣押。以往執法機關逮到犯罪網站之主嫌，通常都會要求被告配合主動關閉網站，但若找不到主嫌，或網站又是架設在國外時，往往無法達到阻絕之效果，但透過網域扣押之執行，即可停止臺灣使用者與設在國外網站伺服器連線，對涉案網站進行停止解析，而限制接取該等網站及 IP，以達到特定網站斷訊之目的[255]。

實務上已普遍接受域名為「無形財產」（Intangible property）的一種形式[256]，而與其他財產權一樣，得成為扣押之標的，核與財產權之特性並無相違。為了因應網路犯罪與網路安全威脅增加，「財團法人臺灣網路資訊中心」（Taiwan Network Information Center，TWNIC）整合國內網路服務提供者，共同建構 DNS RPZ（Response Policy Zone）[257]。在執行上，分為二種，第一種是法院及行政命令裁定攔阻者（稱為 RPZ 1.0），任何人可以執法院判決或行政命令提出；對 TWNIC 之攔阻，不得申訴[258]。第二種是犯罪防治緊急案件處理（稱為 RPZ 1.5 版），限於五種緊急事由：選舉期間執法機構緊急申請、重大金融犯

[255] Id.
[256] Kremen v. Cohen, 337 F.3d 1024,1030 (9th Cir. 2002).
[257] DNS RPZ 機制採取主從架構，如將不當網域名稱或 IP 位址寫入主節點 DNS RPZ 時，所有參與 DNS RPZ 的次級節點，會同時限制接取此不當網域名稱或 IP 位址。
[258] 財團法人臺灣網路資訊中心. (n.d.). RPZ 治理機制：法院及行政命令裁定攔阻者. https://rpz.twnic.tw/d.html

罪緊急申請、假冒政府公務機關網站緊急申請、詐騙網站緊急申請、賭博網站緊急申請；受害單位必須先向高檢署、警察單位、調查局、數位部產業發展署提出，再由高檢署等向 TWNIC 提出；對 TWNIC 攔阻，可申訴[259]。

由於審判權的限制，非屬.tw 的域名，例如 www.amazon.com 等網域名稱,其域名管理業務並非由 TWNIC 所管轄,處理頂級域名.com 的根伺服器（Root server）亦非位在我國境內，因此，TWNIC 無法在其業務職掌範圍內，命令 Verisign 等註冊管理機構限制或剝奪域名持用人的權限。所以對於非屬 TWNIC 管理權限內的域名，僅能透過司法互助的方式，以我國法院所核發的裁定，向該管國家請求協助執行域名扣押[260]，參照如表 7。

表 7：本案所封網域清單

列入 RPZ 黑名單事由	聲請年度	聲請依據文件	涉及網域數	網域
法院裁判或行政機關命令停止解析	110 年 12 月	臺灣新北地方法院 110 年度聲扣字第 19 號	20	f01.twtv0100.com
				f02.twtv0200.com
				f15.twtv1500.com
				f03.twtv0300.com
				f04.twtv0400.com
				f05.twtv0500.com
				f06.twtv0600.com
				f09.ub1900.com
				f10.twtv1000.com
				f11.twtv1100.com
				f12.twtv1200.com
				f13.twtv1300.com

[259] 財團法人臺灣網路資訊中心. (n.d.). RPZ 治理機制：犯罪防治緊急案件處理 (RPZ 1.5 版). https://rpz.twnic.tw/d_2.html

[260] 陳昱奉。(2022)。網路犯罪與資訊安全的未來─從網域名稱扣押談網路治理. 刑事政策與犯罪防治研究專刊, 32, 248.

列入 RPZ 黑名單事由	聲請年度	聲請依據文件	涉及網域數	網域
				f14.twtv1400.com
				f17.twtv1700.com
				f18.pp18000.com
				f20.twtv2000.com
				ub1234.com
				qqqqwwww.com
				ooooppppp.com
				ww.apps1688.com

資料來源：TWNIC 財團法人臺灣網路資訊中心

（四）結論

法院裁定扣押的方式，向法院聲請扣押涉犯《著作權法》的網域名稱，並以 DNS RPZ 的方式執行獲准，而就涉外域名部分，透過國際司法互助模式，向該管國家司法機關協助執行我國的扣押裁定。

第二節　英國

一、 The Football Association Premier League Ltd v British Telecommunications Plc & Ors（英超對 ISP 業者提出禁制令）[261]

（一）案例事實

原告英格蘭足球超級聯賽（FA Premier Leagu，下稱 FAPL）是足球比賽組織機構，擁有包含所有英格蘭足球超級聯賽的電視鏡頭影片以及出現在其中的作品的著作權；被告是英國六家主要的網路服務提供商（ISP）。FAPL 依據英國《1988 年著作權、設計和專利法》第 97A

[261] [2017] EWHC 480 (Ch), [2017] ECC 17.

條向被告提出禁制令，要求被告採取措施封鎖或至少阻礙其客戶訪問向英國消費者提供侵權直播英超聯賽鏡頭的串流媒體伺服器。

禁制令的主要目的是解決未經授權在網路上直播英超聯賽影片的問題。直播串流的關鍵是串流媒體伺服器，該伺服器將未經授權的影片傳輸給消費者。FAPL 識別了一組應該被封鎖的侵權串流媒體伺服器，並要求被告每週更新封鎖名單。

禁制令只在英超聯賽比賽直播時有效，由於技術進步，原告可以即時識別侵權直播，被告的封鎖系統也允許他們在比賽期間自動封鎖和解鎖 IP 位址。禁制令的有效期為 2017 年 3 月 18 日至 2017 年 5 月 22 日，為期短暫，以利後續評估其效果和遇到的問題。

（二）主要爭點及適用法條

1. 爭點：FAPL 對於比賽影片是否擁有著作權，法院是否可依上述法規同意原告系爭禁制令之聲請。

2. 適用法條：《1988 年著作權、設計和專利法》第 97A 條。

（三）法院理由

1. FAPL 對於比賽影片有著作權

FAPL 每場比賽的都會錄製乾淨實況，且根據 FAPL 提交的證據，法院認為這些作品擁有著作權。

2. 允許禁制令之條件

允許禁制令應該受到相應保障措施，原告應每週向串流媒體伺服器主機提供通知，並允許伺服器的操作者以及聲稱受到封鎖影響的任何客戶向法院申請撤銷或修改禁制令。根據《1988 年著作權、設計和專利法》第 97A 條，高等法院有權對服務提供商進行禁制令，如果該服務提供商實際知悉另一個人使用他們的服務來侵犯著作權。法院同意該禁制令前，必須確立四個要件：

(1) 被告是服務提供商。

(2) 使用者和/或目標伺服器的操作者侵犯了英超聯賽的著作權。

(3) 使用者和/或目標伺服器的操作者使用被告的服務進行侵權行為。

(4) 被告實際知悉侵權事實。

3. 侵害重製權：在串流媒體的過程中，訪問串流媒體的使用者會在其電腦、行動設備或機上盒這些設備的記憶體中建立作品的副本，如果使用者流傳比賽的相當部分影片，這部分影片很可能被複製。這種複製行為顯然發生在使用者位於英國的情況下。

4. 目標伺服器的操作者進行向公眾傳播權之侵害：串流媒體伺服器的操作者透過電子傳輸向每個在比賽期間訪問串流媒體伺服器的使用者進行作品的公開傳播。操作者之所以有這種公眾傳播行為，是因為他們故意介入，並充分知曉其行為的結果，以利用戶在本來無法享受作品的情況下給予對作品的訪問。證據顯示，雖然這些串流媒體的觀眾數量無法確定，但實際上有大量人觀看。

串流媒體伺服器的操作者的公開傳播對於FAPL所提供的最初公眾傳播形式（例如：廣播和付費串流媒體服務的授權用戶）來說是另一群「新的公眾」。因此，使用串流媒體伺服器向網路用戶免費提供作品的情況，很明顯違反業者之使用條款，同時需要進行規避內容保護措施（例如：限制訪問、加密和用戶名稱和密碼）。目標伺服器的操作者通常不僅只有連接到英超聯賽鏡頭，通常還透過廣告取得收入，因此推定他們有必要進行這種公眾傳

播。而這些向公眾傳播的行為是針對英國的群眾，故應該被視為在英國發生。這一結論係基於下列多個因素：

(1) 在英國前三大網路服務提供業者在英超比賽期間記錄到非常大的流量。這些流量的變化情況與每場比賽的時間表有密切關聯性，以及所消耗的原始頻寬數量，只有大量的消費者從這些伺服器接收英超轉播內容才能解釋這一現象。

(2) 這些流量的高峰期一直持續到每場英超比賽結束。大體上，頻寬持續的時間與比賽的時間相同，之後立即下降。這種有意識的消費者活動強烈表明相當大比例的英國公眾認為這些伺服器上的英超內容是提供給他們的。

(3) 觀察到的英國流量的其他高峰期是在訂閱平台上播放其他體育賽事期間（例如世界錦標賽飛鏢和英格蘭足球冠軍賽），這些賽事對英國觀眾也是有興趣的。

(4) 雖然無法確定全球對目標伺服器的流量狀況，但合理假設這些大量流量的通訊與目標伺服器佔有很大關係。

(5) 在許多情況下，目標伺服器提供的頻道是複製英國需要訂閱的頻道，而這些頻道本身是專門針對英國消費者。

(6) 在將串流媒體嵌入網站時，這些媒體經常有針對英國消費者的廣告。

（四）結論

法院認為FAPL沒有其他有效且不繁瑣的替代措施來應對這些著作權侵權行為，目前禁制令在保護FAPL權益的同時，也兼顧了其他相關權益，因此符合合理性和比例性的要求。

二、 R v William O'Leary & Terence O'Reilly

（一）案例事實

倫敦市警察局打擊智慧財產權犯罪小組（The Police Intellectual Property Crime Unit，PIPCU）對非法 IPTV 設備進行偵查，隨後，O'Reilly 和 O'Leary 被發現向酒吧和消費者銷售非法 IPTV 設備，該設備已安裝非法串流媒體的應用程式和其他附加零組件，使消費者可以收看未經授權在外國頻道上轉播的英超聯賽[262]。

（二）本案爭點及適用法條

1. **爭點**：本案是否適用英國普通法下的串謀詐欺罪（Conspiracy to defraud）[263]。
2. **適用法條**：《2007 年重罪法》第 44 條中的鼓動或協助組織違法行為、《1988 年著作權、設計和專利法》第 107 條（2）（a）、普通法下的串謀詐欺罪。

（三）本案分析

1.《1988 年著作權、設計和專利法》第 107 條（2）（a）

本規定主要規範行為人在明知或有理由認為某物品將被用於製作侵權複製品以供銷售或出租或用於商業過程的情況下製作專門設計或改造用來複製某特定著作權作品的該物品的行為屬於犯罪。但依據第 107 條（2）款（a）項提起訴訟非常複雜，且和被指控串謀詐欺罪的最高量刑有所不同。由於在陪審團面前舉證違反上述著作權案件相當困難，但串謀詐欺罪相對簡單，陪審團更易接受。

---

[262] Illegal IPTV Box Seller Jailed for Four Years over Piracy. (2016, December 12). Trademarks and Brands Online. https://www.worldipreview.com/illegal-iptv-box-seller-jailed-for-four-years-over-piracy-12719

[263] Intellectual Property Office. (2017). Illicit IPTV Streaming Devices – Call for Views. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594048/illicit-IPTV-streaming-devices-call-for-views.pdf

法院認為 William O'Leary 和 Terence O'Reilly 在 2011 年 3 月 17 日至 2013 年 12 月 3 日之間，與已知和未知的人串謀詐欺付費電視服務，對付費電視內容感興趣的人透過提供便利付費電視觀看的設備和服務而無需向所述廣播公司支付適當費用。

串謀詐欺罪之要件為「指兩人或以上協議用不誠實的手段欺騙他人，有目的造成他人經濟損失或導致他人有經濟損失的風險，或意識到可能會造成這種損失或風險。」，未經兩人或兩人以上的同意、合意或聯合，串謀詐欺罪不能成立[264]。

本案為第一起涉及 IPTV 設備賣家遭起訴判刑之英國案件，這些違法機上盒設備使人們能夠觀看非法內容。法院認為銷售允許人們觀看未經授權的英超聯賽轉播的設備是大規模盜版的一種形式且為違法，其嚴重程度足以導致監禁。

（四）結論

諾丁漢皇家法院以串謀詐欺罪判處 William O'Leary 和 Terence O'Reilly4 年監禁，緩刑 2 年。

第三節　美國

一、 Uuited King Film Distribution Ltd, D.B.S. Satellite Services （1998） Ltd, Hot Communication Systems Ltd, Reshet Media Ltd, and Keshet Broadcasting Ltd v. Does 1-10 d/b/a sdarot.com[265]

[264] Attorney general's office. (2012). Guidance-Use of the Common Law Offence of Conspiracy to Defraud. https://www.gov.uk/guidance/use-of-the-common-law-offence-of-conspiracy-to-defraud--6

[265] No. 21 Civ. 11025.

（一）案例事實

原告是電影、電視、體育和新聞內容製作者和以色列的影音服務提供商，在以色列各地擁有數千名訂閱戶，透過有線或衛星廣播並在自己的平台線上提供數百個受著作權保護的節目（該節目有被原告加密）。被告透過網站重新播送原告僅被授權在以色列境內播送、觀看的原創內容、廣播頻道和電視服務串流影音等；被告透過各種服務和硬體允許最終消費者繞過原告加密以查看原告的內容。

（二）本案爭點及適用法條

美國法典 17 USC § 504（c）。

（三）本案分析

法院若不採取禁制令救濟，是否對原告造成不可挽回的傷害。

（四）結論（禁制令內容）

1. 對被告的禁制令

(1) 禁止透過網站或任何其他網域、伺服器、網站、設備、應用程式、服務或流程，執行、連接、託管、推廣、廣告，傳播、串流式傳輸、分發、向公眾提供、廣播、公開直接或間接侵權或展示任何包含任何原告的頻道或網站或任何原告的內容。

(2) 禁止包括但不限於：複製、串流媒體或以其他方式分發、提供或出售（透過網際網路或其他方式）任何原告擁有專有權利的作品（包括電影、電視、體育賽事和新聞廣播），無論是否註冊、現在存在或後來創作的作品。

(3) 禁止運營或託管被告的侵權行為網站。

(4) 禁止誘導或促使任何人進行上述（1）至（3）的行為。

(5) 禁止銷售、租賃、許可、轉讓、轉讓、分配、出借、抵押、質押或以其他方式轉讓，無論是否有報酬或補償，其侵權業務的任何部分或資產。

(6) 禁止移除、銷毀或以其他方式處置和被告侵權網站、資產和營運相關之任何計算機文件、電子文件、業務記錄或相關文件。

2. 針對網路服務提供商（ISP）

所有 ISP 以及在美國提供服務的任何其他國家之 ISP 阻止對當今已知的被告任何侵權網域及未來新發現的網域，禁止透過任何技術在 ISP 系統上使用。ISP 業者應使用戶以無法訪問網域的方式，進行引導連接至另外一個頁面。

3. 針對第三方服務商

禁止包括但不限於 ISP 業者、網路託管提供商、CDN 服務提供商、DNS 服務提供商、VPN 服務提供商、域名購買服務、後端服務提供商、聯屬計劃提供商、網頁設計師、託運者、基於搜索的線上廣告服務、任何銀行、儲蓄和貸款協會、商戶帳戶提供商、支付處理商和提供商、發卡組織或其他金融機構等，向被告及侵權網站提供服務。

4. 針對註冊服務商和註冊管理機構

所有與侵權相關的域名網站，轉讓所有權給原告並且控制；應暫時禁用該命令相關的任何域名網站，使其處於非活動狀態，並引導用戶無法連接和/或使用網站。

5. 針對被告的貨幣帳戶

發現屬於被告或由其控制的資金或帳戶，禁止該被告擁有或控制的所有帳戶，及轉移或處置該被告的任何金錢、股票或其他財產資產，並應防止此類資金被轉移或提取。

二、 Joint Stock Co. Channel One Russ. Worldwide v. Infomir LLC

（一）案例事實

原告是由 Joint Stock Company Channel One Russia Worldwide 等幾個俄羅斯電視廣播公司所組成（下稱原告），起訴糾正被告之「盜版」行為，透過網路將其電視節目轉售給美國消費者（未支付任何授權費用）。被告 Infomir 是一家紐約的有限公司，原告認為被告在未經許可的情況下侵入、攔截或以其他方式獲取原告頻道的加密訊號並傳輸至其伺服器，並以串流方式透過 IPTV 機上盒向該司法管轄區的客戶傳輸訊號。

（二）本案爭點及適用法條

1. 爭點：本案原告使用「Wireshark」網絡協議分析軟體來確定與被告 Infomir 的 IPTV 機上盒相關視頻串流來源，關於該證據是否有證據能力。

2. 適用法條：《聯邦通訊法》§ 605（a）[266]、《著作權法》17 U.S.C. § 1201 等、15 U.S.C. § 1125、《紐約一般商業法》（The New York General Business Law）§ 349。

（三）本案分析

本案原告聘用一位名叫 Christopher Vidulich 的法律助理進行調查，他使用「Wireshark」網路協議分析器來確定與被告 Infomir 的 IPTV

[266] 42 U.S.C. §605(a).

機上盒相關視頻串流之來源。Christopher Vidulich 於 2016 年 5 月進行 Wireshark 調查，並且證詞與結果皆支持原告最初之訴之聲明。

但原告反復未能提供使用 Wireshark 調查中一項被稱為「Channel One Capture.pcapng」（Channel One PCAP）完整紀錄之電子文件，儘管法院已多次發出要求、命令和傳票；且 Vidulich 最初證稱 Wireshark 數據「未保存」，後來也再次重申了這一虛假證詞。然而，後來發現他確實擁有這些數據，並將其轉移到另一台電腦上。而上述 Channel One PCAP 電子檔最終於 2018 年 10 月才被提供，原告聲稱這是「不慎」的遺漏。

Infomir 要求對原告進行制裁，聲稱原告發表了虛假陳述，並採取阻礙性策略，以阻止發現與 Vidulich 證詞相矛盾的證據。同時，Infomir 提供了可信的專家證據，顯示 Wireshark 調查並不如 Vidulich 所描述的那樣進行。雙方專家都同意 Vidulich 關於未經授權的 IPTV 串流的來源的主張是不準確的。

（四）結論

法院同意 Infomir 之動議，禁止原告引入或依賴 Vidulich 之證詞及關於 Wireshark 調查的相關證據。並命原告償還 Infomir 的律師費、專家費和其他相關費用。

第四節　新加坡

一、 Neil Kevin Gane v. Jia Xiaofeng and Synnex Trading Pte Ltd[267]

[267] Neil.Kevin.Gane.v.Jia.Xiaofeng.and.Synnex.Trading.Pte.Ltd [2019] SGMC 73

（一）案例事實

被告 Synnex Trading Pte Ltd 是一家銷售違法串流設備的新加坡公司及其董事賈曉峰。被告自 2015 年以來一直在銷售違法串流設備並將其供應給其他零售商。

Synnex 的員工向客戶表示該設備是完全合法的，並幫助他們下載和啟動非法串流媒體應用程式，突擊檢查販售違法串流設備商店的場所後發現總共擁有 255 個違法串流設備，其中 104 個預裝了侵犯著作權的串流媒體應用程式。一旦買家啟動設備，這些應用程式就能夠播放未經授權的電視頻道以及其他娛樂和體育內容。

（二）本案爭點及適用法條

新加坡《著作權法》第 136（3A）和 137（4）條（舊法），「持有專門用於侵害著作權之物」，對於提供可連結侵權影音之非法串流裝置／服務，以獲取商業利益。

（三）本案分析

本案主要是被告與原告達成和解並認罪，故法院認定賈曉峰作為 Synnex 的控制者負有重大罪責，且其犯後行為和態度不佳，在權利所有人向他送達了各種停止、終止信函以及在他收到了此次起訴的指控之後，他仍然沒有表現出悔意，並堅持透過 Synnex 銷售串流媒體設備。

（四）結論

Synnex 因故意侵犯著作權而被罰 4,800 新元，並因擁有 104 個預裝侵權應用程式的違法串流設備而被罰 156,000 新元（每個違法串流設備 1,500 新元），被告董事被判監禁 12 週併罰款 5,400 新元。

第四章 未來推動 OTT TV 機上盒監理之評估概要

本章第一節分析我國現有法制制度以及綜整主要國家及區域組織對 OTT TV 機上盒之監理政策、法規，就法規面及執行面，提出未來推動 OTT TV 機上盒監理之評估概要。第二節提出 OTT TV 機上盒監理技術之構想與方式，以及評估監理技術需使用之軟體及硬體工具。

第一節　法規面與執行面

一、 我國現有法制制度分析

（一）網路視聽平台及廣播視聽相關規範

現行我國管制視聽媒體服務，主要依據「廣電三法」，依傳輸方式之屬性不同而分別立法，包括：以無線電波頻率傳輸為主之《廣播電視法》、有線電纜傳輸之《有線廣播電視法》以及衛星頻率傳輸之《衛星廣播電視法》。由於技術與立法先後順序不同，長期有管制規範寬嚴不一與落差之爭議；再加上網際網路技術與新興媒體之發展，網際網路視聽媒體之規管也成為主要討論之議題，故國家通訊傳播委員會（以下簡稱通傳會或 NCC）近年有整合相關法律及管制規範逐步齊一化等相關草案之提出。

我國目前尚無將 OTT TV 網路視聽平台納管之專有法律，部分得以依據既有法規治理，但仍有規範不足之處。爰此，通傳會於 109 年 7 月公告《網際網路視聽服務管理法》（草案），草案主要採取輕度之自願「登記制」方式（111 年草案改採行為管理機制），就網際網路視聽服務進行必要事項管理；但為考量公眾視聽權益保護，主管機關得公告一定經營規模以上之網際網路視聽服務提供者應辦理登記，以納入管理，並採取業者自律及公私協力之治理模式，以維護諸如個人資

訊、隱私、智慧財產權、兒少身心健康、消費者權益、市場公平競爭等個人與社會法益[268]。惟相關立法工作仍在進行中，仍待後續觀察。

惟目前較為特殊之情況為 IPTV 服務，在我國多由電信業者提供相關服務，而電信業者（如中華電信）因有政府機關作為股東，需要受到較多法令之限制。由於中華電信有交通部之持股，依據廣電三法中所謂「黨政軍條款」，中華電信原則上不得經營廣電媒體。而目前中華電信經營 IPTV 服務，主要依據《電信管理法》授權之《公眾電信網路設置申請及審查辦法》第 6 條有關經營多媒體內容傳輸平臺服務[269]規定申請。故中華電信目前在經營 MOD 服務時，因上述規範不得提供頻道節目內容外，也不得干預頻道節目內容服務提供者之內容服務與組合、銷售方式與費率訂定，同時需要事先將用戶機上盒規格及提供方式載明於營運計畫。

（二）OTT TV 機上盒監理法規

OTT TV 機上盒因具備無線射頻功能（Wi-Fi 或藍牙），屬電信管制射頻器材。按《電信管理法》第 65 條第 2 項規定「為維持電波秩序，經主管機關公告之電信管制射頻器材，應經核准，始得製造、輸入。」另依同法第 66 條第 1 項：「電信管制射頻器材除經主管機關專案核准外，應符合技術規範，經審驗合格，始得販賣。」故通傳會針對電信管制射頻器材的目的在於避免使用者受電波不當干擾，對無線機上盒之強制審驗範圍，僅限於硬體之無線射頻功能（如 WiFi 或藍牙等），未包括其所載軟體及其後端或雲端提供之影音內容[270]。

---

[268] 《網際網路視聽服務管理法》草案總說明. (2020, July 22). https://www.ncc.gov.tw/Chinese/news_detail.aspx?site_content_sn=5306&sn_f=43455

[269] 《公眾電信網路設置申請及審查辦法》第 6 條第 3 項：「第一項所稱多媒體內容傳輸平臺服務，指利用公眾電信網路視聽媒體互動介面及視聽內容儲存設備所架構電信事業可控制非開放環境之平臺上，供用戶藉由寬頻接取電路及用戶機上盒，接取該平臺上由內容服務提供者所提供之多媒體內容服務。」

[270] 國家通訊傳播委員會. (112 C.E.). 國家通訊傳播委員會業務概況報告. 立法院第 10 屆第 7 會期交通委員會, 15.

通傳會在評估各種類、項目之射頻器材對於國內電波秩序之影響程度後，將可能產生干擾電波秩序者，公告為管制的電信管制射頻器材，必須透過取得審驗合格或專案核准等方式，才得以在國內製造、輸入或在市場上販賣，防止後續該等器材之使用發生電波干擾情形。爰此，依據《電信管理法》第 66 條第 5 項授權訂立《電信管制射頻器材審驗管理辦法》規範有關電信管制射頻器材之審驗；並依《電信管理法》第 65 條第 3 項及《電信管制射頻器材製造輸入及申報作業管理辦法》公告將規管之電信管制射頻器材分為「第一級電信管制射頻器材」與「第二級電信管制射頻器材」，明定各級器材所包含之項目，進行分級管理措施。

如販賣未經審驗合格之電信管制射頻器材，涉及違反上述《電信管理法》第 66 條第 1 項規定，主管機關可依同法第 81 條第 1 項規定：「違反第六十六條第一項規定，販賣未經審驗合格之電信管制射頻器材者，處警告或新臺幣一萬元以上二十萬元以下罰鍰，並通知限期改正；屆期未改正者，得按次處罰。」通傳會針對機上盒除事前審驗外，也加強市場抽驗，並要求申請審驗者須出具所提供軟體不違反《著作權法》之切結書；對於常態違反規定之申請者與器材加強審驗要求；並請財政部關務署及網路平臺業者加強查核，阻卻違法無線機上盒流通[271]。

技術規範部分，106 年 10 月 13 日通傳會公告「固定通信多媒體內容傳輸平臺機上盒技術規範」於 107 年 10 月 1 日生效；108 年 1 月 10 日則公告《具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引》，協助數位機上盒業

[271] Id.

者建立完善的資通安全防護機制，帶動相關產品之自主性資安檢測及驗證，以保護消費者權益並協助業者強化產品之安全。

標準部分，通傳會委託財團法人電信技術中心（Telecom Technology Center，TTC）參考國際標準、規範與指引，在臺灣資通產業標準協會（Taiwan Association of Information and Communication Standards，TAICS）標準制定平臺，聚集產、官、學、研，依產業標準制定程序制定「機上盒資安標準」[272]，依（1）可用性、（2）身分識別、（3）隱私加密、（4）安全功能等四安全構面規定機上盒之資訊安全要求，並依此區分為三級安全要求；並同時提出「機上盒資安測試規範」[273]，具體明列測試項目、測試方法及結果等來驗證產品所能達到之資安要求。

（三）OTT TV 機上盒侵害著作權相關法規

我國有關機上盒之侵權主要透過《著作權法》處理，法律上可採取通知取下機制、民刑事相關救濟程序以及法院命令。

1. 通知取下機制

網路服務提供者可按《著作權法》第 90-4 條至第 90-12 條的「網路服務提供者之民事免責事由」相關規範適用安全港條款，符合一定條件下，配合著作權人之通知取下侵權資訊，即可主張賠償責任之免除，藉此鼓勵網路服務提供者與著作權人合作。而《著作權法》有關「網路服務提供者」將之分為四個類別，包括：連線服務提供者[274]、快速存取服務提供者[275]、資訊儲存服務提供者[276]及搜尋服務提供者[277]而有不同之免責要件。

[272] 台灣資通產業標準協會. (2022). 機上盒資安標準. TAICS TS-0049 v1.0, 15.
[273] 台灣資通產業標準協會. (2022). 機上盒資安測試規範. TAICS TS-0049 v1.0.
[274] 《著作權法》第 90-5 條。
[275] 《著作權法》第 90-6 條。
[276] 《著作權法》第 90-7 條。
[277] 《著作權法》第 90-8 條。

按第 90-6 條第 3 款、第 90-7 條第 3 款及第 90-8 條第 3 款規定快速存取服務提供者、資訊儲存服務提供者及搜尋服務提供者之通知取下機制：「經著作權人或製版權人通知其使用者涉有侵權行為後，立即移除或使他人無法進入該涉有侵權之內容或相關資訊。」，但通知取下機制並不適用於連線服務提供者。

通知取下機制，分為「通知」以及「取下」兩階段。當著作權人發現網路上有侵害其著作權之內容時，依《著作權法》第 90-4 條第 1 項第 3 款上之聯繫資訊，通知網路服務提供者侵權情事並載明權利人聯絡方式、侵權著作、請求移除聲明、涉及侵權內容之相關資訊及存取路徑、係基於善意相信有侵權情事、如通知有不實權利人願負法律責任之聲明等相關資訊，即完成「通知」程序；資訊儲存服務提供者接收來自著作權人之通知後，若立刻移除或讓他人無法存取該涉及侵權資訊；或在從其他管道知悉侵害情事後，善意取下該涉及侵權資訊者，未來在訴訟上，可對著作權人及網路使用者主張不負賠償責任。

經上述通知取下機制後，涉及侵權的使用者如認其無侵權情事，可向移除其內容的資訊儲存服務提供者發送回復通知（Counter Notice），要求回復被移除之著作[278]；此時資訊儲存服務提供者會轉達予權利人，要求其於 10 個工作日內提出訴訟，若權利人在轉送回復通知之 14 天內未提起出訴訟，資訊儲存服務提供者就應該回復被移除之資訊[279]，以兼顧受通知取下機制所影響的網路服務使用者之程序權益。

[278] 《著作權法》第 90-9 條第 3 項。
[279] 《著作權法》第 90-9 條第 4 項、第 5 項。

2. 著作權民刑事責任

《著作權法》於 2019 年 4 月 16 日增訂第 87 條第 1 項第 8 款，第 87 條主要規範各種被視為侵害著作權或製版權之行為，凡實施該條規定之行為者，須負侵害著作權的民事責任。其中，第 87 條第 1 項第 8 款規定:「明知他人公開播送或公開傳輸之著作侵害著作財產權，意圖供公眾透過網路接觸該等著作，有下列情形之一而受有利益者：（一）提供公眾使用匯集該等著作網路位址之電腦程式。（二）指導、協助或預設路徑供公眾使用前目之電腦程式。（三）製造、輸入或銷售載有第一目之電腦程式之設備或器材。」

另經濟部智慧財產局 110 年 8 月 11 日電子郵件字第 1100811c 號有針對「欲請經濟部智慧財產局提供平台辨識非法機上盒之指引」之問題進行回復，內容略以:「銷售網路機上盒之業者（包含代理商）是否成立《著作權法》第 87 條第 1 項第 8 款規定，應視其是否「明知公開傳輸之著作侵害著作財產權」而定，如銷售業者明知有上述情形而仍為販售行為，即有該當違法之可能，例如：廣告行銷機上盒以明示或暗示使用者可影音看到飽、終身免費、不必再付月租費等廣告文字號召誘使或煽惑使用者利用該電腦程式連結至侵權網站（相關內容可參考本局網站「《著作權法》修正第 87 條、第 93 條修正 Q&A」，路徑：本局首頁/著作權主題網/工具資源/著作權 FAQ）；另外，新法通過後，臺灣線上影視產業協會（https://www.taiwanott.org）已公布數款非法機上盒或 App 應用程式名單，而國家通訊傳播委員會也會不

定期公告違法機上盒型式名單，敬請至該協會或國家通訊傳播委員會網站查詢，避免因販售非法機上盒，而生訴訟爭端。[280]」

3. 法院判決、裁定封鎖網站

2013 年經濟部智慧財產局為了保護文創產業，擬修改《著作權法》，以行政權模式要求 ISP 業者以 IP 位址或 DNS 封鎖技術，阻斷國內網路使用者連結至國外侵權網站，卻引發外界高度反彈，認為恐有擴張行政權致侵害言論自由及資訊接觸自由之虞，而後決定不再推動由行政機關介入封鎖侵權網站之認定，回歸由司法機關認定之原則[281]。相關爭議後，我國目前針對封鎖網站之作法，主要仍需要取得法院之判決或裁定方得據以執行。

為了因應網路犯罪與網路安全議題「財團法人臺灣網路資訊中心」（Taiwan Network Information Center，TWNIC）整合國內網路關鍵基礎設施提供者，共同建構 DNS RPZ（Response Policy Zone）限制境內外惡意網域名稱或 IP 位址接取，限制惡意域名接取依據包含法院判決、裁定或行政機關命令，或有資安疑慮且影響資安重大者[282]。

TWNIC 得以根據法院判決、裁定，將預計停止解析之網域名稱，載入 DNS RPZ 資料庫後，同步更新至國內電信業者 DNS 資料庫，全國統一停止解析[283]。前述臺灣新北地方法院 110 年度聲扣字第 19 號裁定，即是向法院聲請扣押涉犯《著作權法》的網域名稱，並以 DNS RPZ 的方式執行獲准，由 TWNIC 執行阻斷訊號接取，停止使用者連上違法網站。

---

[280] 經濟部智慧財產局 110 年 8 月 11 日電子郵件字第 1100811c 號。

[281] Newtalk 新聞. (2013, June 3). 政策逆轉 智財局：不推動行政權封網. https://newtalk.tw/news/view/2013-06-03/37020

[282] 黃勝雄. (2020, September 23). DNS RPZ 摘要說明. TWNIC. https://blog.twnic.tw/2020/09/23/15311/

[283] 前揭註 [260]，頁 123。

二、 綜整主要國家或區域組織之政策、法規

（一）OTT TV 產業之治理模式

目前各國針對 OTT TV 平台產業之治理規範，相關規範相對傳統廣播電視少，主要仍以產業自律為主，而在內容管制部分，則主要以核心價值之監管為主，例如：保護兒少、著作權保護、個人資料及隱私保護為主；僅有少數國家針對 OTT TV 產業採取執照管理制度（例如：中國大陸、新加坡），甚至中國大陸會介入內容產製之審查。以下就各國針對 OTT TV 之治理模式，制表如下表 8。

表 8：主要國家 OTT TV 治理模式

國家	產業治理模式
美國	幾乎未管制。
歐盟	僅規管「視訊分享平臺」。
英國	英國除管制隨選節目服務外，幾無針對網際網路視聽服務平臺的管制。
日本	幾乎未管制。
韓國	OTT TV 業者屬加值電信服務事業，採取登記報備制，業者於開始營運前須向 MSIT 進行登記。
新加坡	透過網路傳輸的電視服務的運營商需要取得小眾電視服務執照（Niche Television Service Licence）。
中國大陸	網路電視需有營運牌照。

資料來源：本計畫整理

（二）OTT TV 侵權管制規範及政策比較

在 OTT TV 規範議題中，各國目前主要關注重點在於盜版侵權問題，並提出多種監理、行政措施進行規範，以解決透過違法機上盒之網路盜版問題。主要可以分為三種模式，包括：行政措施、司法措施及市場機制，如表 9。

表 9：OTT TV 侵權管制規範及政策比較

分類	採取措施	國家
行政措施	事前設備檢驗	英國、歐盟、日本、韓國、中國大陸、新加坡、臺灣
	公布觀察、封鎖名單	美國、歐盟、臺灣
	邊境管制、海關扣押	美國、英國、日本
	國際合作	歐盟、英國、日本、韓國、中國大陸
	通報與資訊分享	英國、韓國、日本
	禁止無執照販賣	新加坡、中國大陸
司法措施	著作權民刑事規範	各國皆有
	規避技術措施的設備和服務處罰	美國、英國、新加坡、中國大陸、日本、韓國、臺灣
	安全港條款	美國、歐盟、中國大陸、臺灣
	禁制令	歐盟、英國、美國、新加坡、臺灣
	動態封鎖	歐盟、英國
	詐欺、洗錢規範	英國
市場機制	金流及廣告機制合作	美國、英國
	自律措施	日本、新加坡
	技術過濾	韓國、Netflix
	消費者政令宣導、教育	歐盟、英國、臺灣

資料來源：本計畫整理

整體而言，由於世界各國對於網路盜版問題之重視，依據前述研究，目前主要國家皆可透過著作權相關民刑事法規，依據司法程序處理透過機上盒侵犯著作權之行為。雖著作權人擁有豐富的法律執行手段，可以主張自身權利，但主要關鍵點在於時效、程序複雜度及執法有效性等問題，故大量可用之執法措施，並不代表實際上被廣泛運用或真正有效。

除著作權相關民刑事規定外，歸納相關司法措施，以英國、歐盟為首，逐漸透過快速、動態之司法執行措施，可針對提供侵權內容的網站進行動態封鎖；以美國為首，則係以安全港作為誘因，通知網路服務提供者對侵權者及其託管或連接到侵權內容進行移除或封鎖。儘管執行措施眾多，但執法效果尚難確定，各國仍積極尋找解決網路盜版的方式，期望以合理且便捷的合法途徑來保護受著作權保護的內容。而近年來，英國甚至開始以詐欺、洗錢等罪名，透過刑事規範。

三、 對未來推動 OTT TV 機上盒監理之評估概要

（一）主要問題現況

比對我國與主要國家之行政措施、司法措施及市場管理機制，可以發現我國關於透過機上盒之網路影音侵權之相關規範及行政措施並未較他國少，但仍被美國的 2023 年特別 301 報告點名為「非法網路協定電視」猖獗的國家。為進行後續規範評估，將前述所提及之主要打擊機上盒盜版之相關措施細部問題分述如下表 10。

表 10：我國打擊機上盒盜版之相關措施細部問題分析

分類	問題描述	變化和發展推估	利害關係人	主要原因
行政措施	事前監理之規範要求不足	強化事前監理	◆ 主管機關 ◆ 機上盒設備商	可參考、對應歐盟RED之規範要求
	技術過濾	增加技術過濾機制	◆ 主管機關	可透過事前技術規範要求設

分類	問題描述	變化和發展推估	利害關係人	主要原因
			◆ 機上盒設備商	備業者具一定技術、規格，降低盜版侵權之可能性
	後市場管理不足，回收機制仍待強化	增加回收機制之細節性規範	◆ 主管機關 ◆ 機上盒設備商、經銷商 ◆ 使用者	可參考、對應歐盟RED之規範要求
司法措施	法律仍有不確定性（智財法）	明確相關規範解釋	◆ 主管機關 ◆ 立法機關 ◆ 相關業者 ◆ 使用者	司法適用仍有解釋不同之處，以至於效果不確定
	禁制令之範圍及時效	基於法官保留原則，於法制規範內實行	◆ 司法機關 ◆ OTT TV業者 ◆ ISP 業者 ◆ TWNIC	目前法院扣押裁定未能產生動態封鎖之效果
市場機制	宣導教育不足	強化宣導，增加不同面向之說明（例如：資安、防詐騙等）	◆ 主管機關 ◆ 司法機關	目前宣導反盜版對於使用者無法產生共鳴及嚇阻效力
	產業合作仍待強化	鼓勵產業合作、增加廣告商之配合	◆ 相關業者 ◆ 廣告商 ◆ 公協會	透過市場力量禁止相關違法行為

資料來源：本計畫整理

（二）對策方案研擬及影響預評估

在對策方案之研擬上，主要可分為管制型工具和非管制型工具兩大類。管制型工具主要透過法規及公權力，由政府機關對於人民自由行使憲法基本權利或自由從事經濟商業活動，施予一定程度的限制，違反限制者必然受到行政處罰或刑罰；非管制型之對策方案則是依賴

經費補助、獎勵、教育宣導、資訊提供、技術協助、價值訴求等等方式，鼓勵人民達成某項目標。

總結主要國家在機上盒違法侵權之政策作法上，主要以管制型工具為主，透過各項刑事、行政手段，發現、處罰侵害著作權之行為人。而就上述相關細部問題分析而言，未來針對違法機上盒之監管主要也將以管制型工具為主（詳細建議請參後述），而針對可能之發展方向及監管手段之收緊對於利害關係人之立即性或未來可見的重大顯著影響項目，包括正面（效益）和負面（成本負擔等），分析如下表 11。

表 11：強化機上盒違法侵權之管制型工具之影響評估

	角色	效益	成本
利害關係人	主管機關	降低民眾違法風險 提升我國國際聲譽	增加行政成本
	ISP 業者	減低觀看盜版帶來之流量成本	增加執行成本
	內容產製者	增加使用者觀看正版意願 提高授權收入	增加協助執法成本
	機上盒設備商/經銷商	提高產品聲譽	降低原有意違法觀看者之購買意願 增加設備成本 增加違法設備回收成本
	OTT TV 平台業者	增加使用者訂閱意願 提高訂閱收入	增加協助執法成本
	使用者	降低資安侵害風險 降低違法觀看侵權風險[284]	增加合法平台之訂閱費

資料來源：本計畫整理

[284] 使用者觀看違法影音，主要視是否涉及「重製」行為，若為種子下載則涉及重製行為而觸法，例如過去「成功大學 MP3 事件」；但若單純觀看非法機上盒之影音內容，使用者通常僅涉及《著作權法》第 22 條第 3 項及第 4 項之暫時性重製行為，單純網路瀏覽排除於所規範「重製」行為態樣之外，而不違反《著作權法》。

第二節　技術面

一、OTT TV 機上盒監理技術之構想

OTT TV 機上盒因具備無線射頻功能（Wi-Fi 或藍牙），屬電信管制射頻器材，通傳會對無線機上盒之強制審驗範圍，如前所述僅限於硬體之無線射頻功能，未包括其所載軟體及其後端或雲端提供之影音內容[285]。

非法集團常撰寫專屬於特定機上盒的非法 App 軟體，再利用人員線上指導或是錄製 YouTube 視訊內容進行隔空教學，指導消費者如何下載違法 App 觀看節目，使機上盒成為侵權的工具。因此，本計畫將針對我國市售可收視未經合法授權節目頻道及隨選視訊之 OTT TV 機上盒進行技術分析，並提出有助於 OTT TV 機上盒監理技術相關事項，以期有效防止合法節目內容被盜用散播。

（一）技術規範與標準之構想

前述提及臺灣 OTT TV 機上盒技術規範，包括：通傳會公告「固定通信多媒體內容傳輸平臺機上盒技術規範」、「具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引」，協助數位機上盒業者建立完善的資通安全防護機制，帶動相關產品之自主性資安檢測及驗證，以保護消費者權益並協助業者強化產品之安全。

關於 OTT TV 機上盒技術標準，通傳會則在臺灣資通產業標準協會（TAICS）標準制定平臺「機上盒資安標準」[286]，依可用性、身分識別、隱私加密、安全功能等四安全構面規定機上盒之資訊安全要求，

[285] 國家通訊傳播委員會. (112 C.E.). 國家通訊傳播委員會業務概況報告. 立法院第 10 屆第 7 會期交通委員會, 15.

[286] 台灣資通產業標準協會. (2022). 機上盒資安標準. TAICS TS-0049 v1.0, 15.

並同時提出「機上盒資安測試規範」[287]，具體明列測試項目、測試方法及結果等來驗證產品所能達到之資安要求。

歐盟智慧財產局（EUIPO）認為，由可疑企業製造的相關設備可能具有危險功能[288]。又依據 2014 年無線電設備指令（RED），機上盒應被設計成保護使用者之隱私及個人資料、免於詐欺、以及維護網路安全；且如果有使用者、無線電設備或第三方要將軟體載入到該設備中，機上盒也必須設計為僅能在不影響無線電設備之基本要求的情況下，才能將軟體載入到無線電設備中。不符合這些基本要求之無線電設備，製造商、進口商與分銷商，都不應投放至市場。此外，如果無線電裝置存在風險，進口商與分銷商都應通知製造商和市場監督當局。

因此，OTT TV 機上盒建議可參照歐盟相關規範檢測非法 App 軟體有無綁定特定 OTT TV 機上盒，如果機上盒欠缺阻止載入該 App 軟體之設計，可以於銷售後再以客服方式安裝收視非法視聽內容之程式，或是購買之消費者自行至網路論壇查詢安裝此類非法收視程式，只要此類程式可危害消費者之隱私及個人資料、詐欺、以及破壞網路安全（即損害網路或其功能，濫用網路資源，從而導致不可接受的服務降級）皆屬違反規定，而不應投放至市場。

（二）收視權限檢驗機制之構想[289]

若欲證明某機上盒為專用於侵犯著作權之主要工具，則需要證明專用於侵犯著作權之非法 App 僅可用於特定之機上盒。本計畫將抽驗我國已上市的 OTT TV 機上盒，驗證是否有這種綁定啟動的非法

[287] 台灣資通產業標準協會. (2022). 機上盒資安測試規範. TAICS TS-0049 v1.0.

[288] Illegal IPTV in the European Union. (2019). European Union Intellectual Property Office. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf, p.69.

[289] 我國 110,民著訴,81,20230424,1 App 綁定盒子案

App 的機上盒。參酌實務上警方勘驗非法 OTT TV 機上盒，檢驗該特定機上盒是否具有「**收視權限檢驗機制**」，即：

1. 機上盒之網卡編號 MAC 碼是唯一的認證編號，每台皆不同。這邊要說明的是：也有機上盒會採用其他唯一的識別編號。
2. 使用該機上盒觀看直播必須向伺服器傳送鑑別參數，例如「gkey」、「token」等，做為驗證後方可收視直播頻道。
3. 收視權限為機上盒業者控制收視者之方法，透過綁定機上盒之 MAC 碼或其他編碼，侷限可使用之 App 軟體，避免未購買系爭機上盒者卻使用 PV 直播、臺灣直播收視免費第四台。

核與 OTT TV 機上盒之封包側錄報告所載結論相符：以 PVBOX 為例，直播功能於啟動時，授權畫面中的認證機制需要 MAC 編碼作為參數使用，證明硬體製造商與軟體商存在一定程度的合作關係。

二、 OTT TV 機上盒監理技術之方式[290]

OTT TV 機上盒之啟用須於開啟機上盒後下載第三方 App 軟體方可觀覽相關影片、節目，故本計畫分別針對 App 之行為與 App 是否綁定機上盒規劃監理技術。

（一）App 行為檢測—App 本身之功能分析

OTT TV 機上盒要取得根目錄權限就須取得 root 控制權，以及對 Android 系統進行提權動作，常見方式就是透過刷機等方式進行，或是利用機上盒作業系統之漏洞進行。

（二）App 行為分析—分析 App 有無綁定特定 OTT 機上盒

將 OTT TV 機上盒運作、連線過程進行封包側錄與分析，進一步瞭解該設備內容並同步比對網路傳輸封包運作狀況，檢測 App 啟用

[290] 莊明雄、林俊賢 (2017).OTT 機上盒侵權與資安數位鑑識架構初探. Communications_of_the_CCISA, 23(3), 49–64.

過程、使用期間有無綁定特定 OTT TV 機上盒之型號、序號、MAC 等可識別特定機上盒特徵之機制。目前來講，如果機上盒封包本身沒有加密機制，則可直接透過 Switch port mirror 或 Hub Sniffer 等技術取得傳輸資料內容來驗證有無事前認證及綁定機上盒特殊專屬編碼（例如常見的 MAC 編號），如下圖 3 所示，檢測人員可以透過連接 Hub 並使用 Port Mirror 的方式或使用 Hub Sniffer 進行側錄，取得機上盒連線至網際網路的封包資訊。

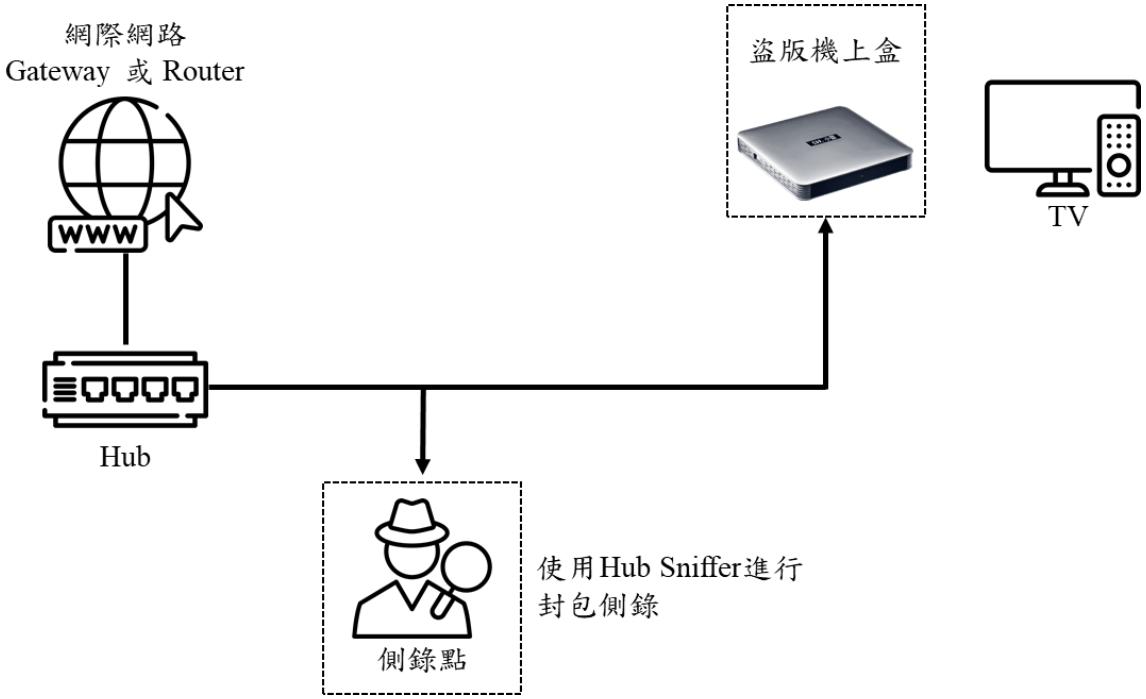

圖 3：封包 port mirror 或 sniffer 側錄方式
資料來源：本計畫整理

下圖 4 顯示，App 啟用時認證網卡 MAC 編號、CPU-ID 及 KEY 等數值會於封包資料留下紀錄。紅色框所標示的為 MAC、CPU-ID 及 KEY。

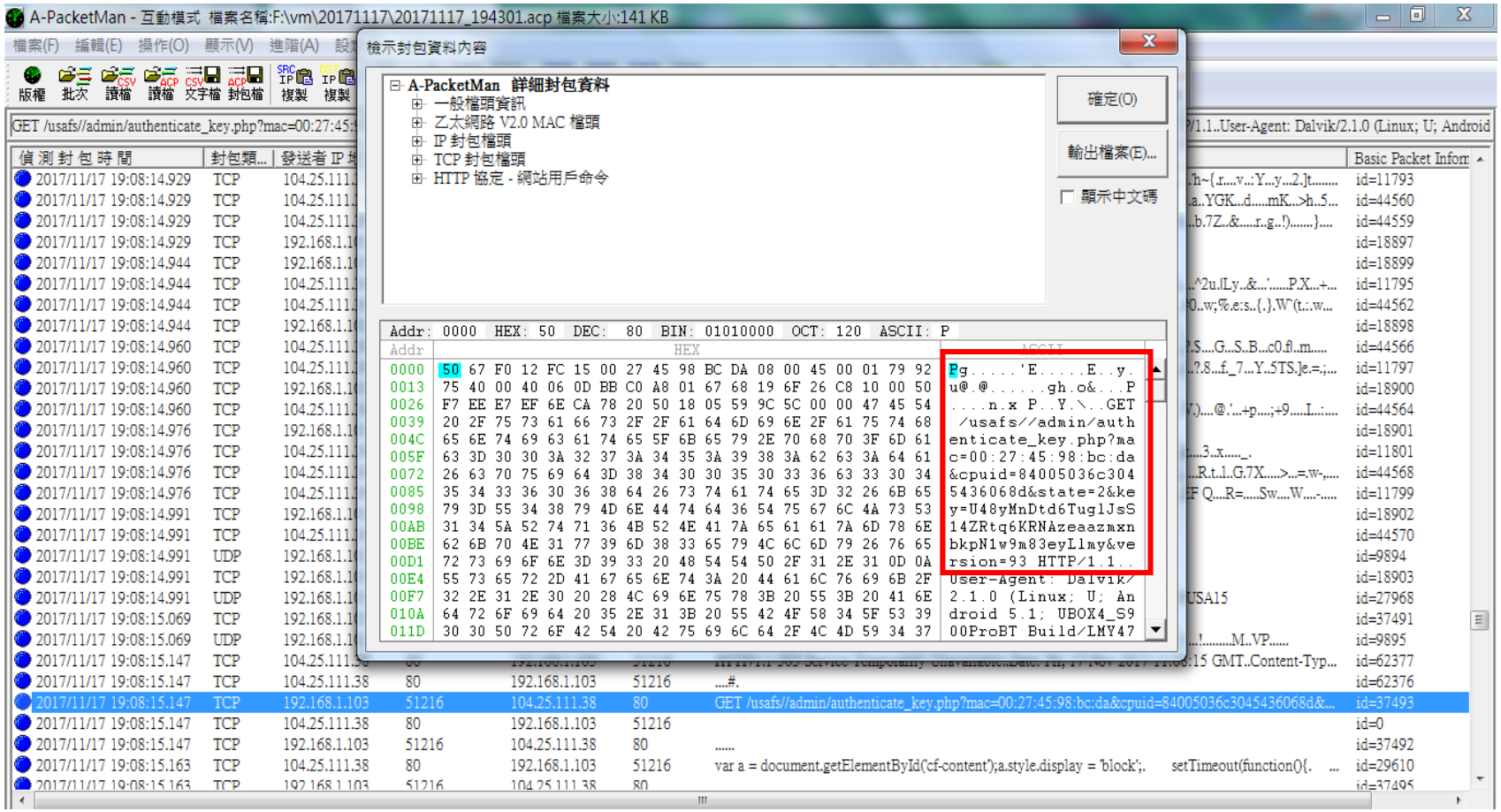

圖 4：App 啟用時會在封包資料留下紀錄

資料來源：本計畫整理

但觀察近期出產之機上盒，封包內容均使用 HTTPS 等協定傳輸加密，主要避免過程中被揭露或數位鑑識出業者刻意綁定相關機上盒硬體資訊，意圖透過機上盒販售牟取不法利益，因此為能順利取得機上盒關鍵資訊，並且繞過不法業者刻意加密保護機制，故必須使用中間人攻擊手法（Man-in-the-middle attack，縮寫：MITM）來取得加密之內容，從下圖 5 可見，針對側錄 A 點使用筆記型電腦分享網路熱點讓機上盒連線，然後進行封包側錄與 Burp Suite 軟體攔截封包，來找出是否有刻意綁定資訊，並在 B 點同步進行封包側錄，掌握完整網路通訊行為與模式，如下圖 6，從 A 點分析出確實機上盒須綁定網卡 MAC 等資訊才能收視。

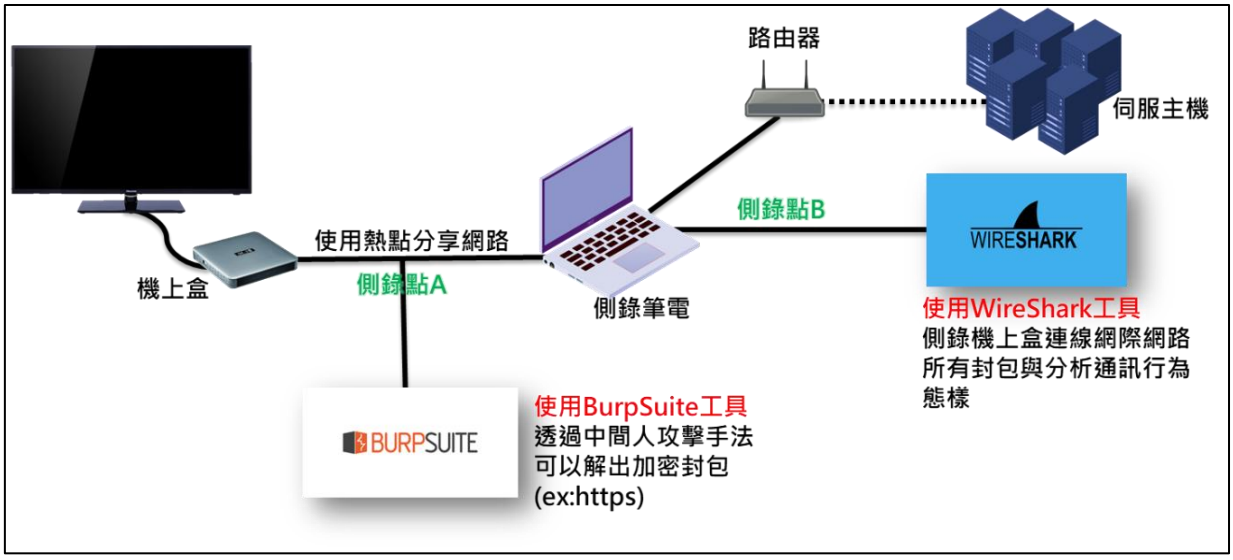

圖 5：機上盒本身封包進行加密，需要透過中間人攻擊手法取得加密內容
資料來源：本計畫整理

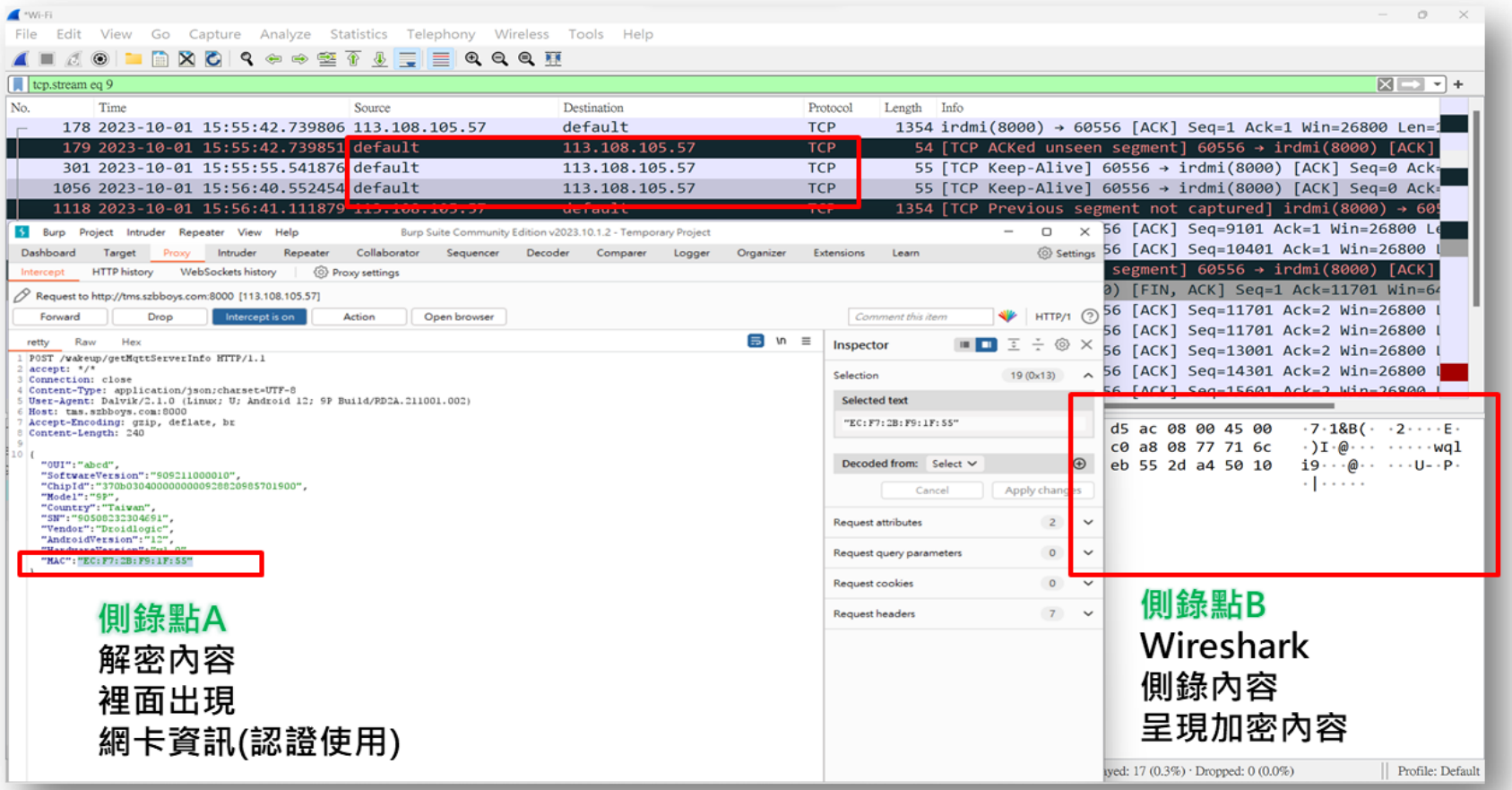

圖 6：從 A 點分析出確實機上盒有綁定網卡 MAC 等資訊才能收視

資料來源：本計畫整理

此外，透過 Mobsf 平台分析非法機上盒使用之專屬 APK，進行靜態分析。如圖 7 所示，發現 App 是需要進行認證程序，並非單純下載即可啟用，必須要事先通過認證，類似輸入帳號密碼等機制，因此與前述動態分析（Burp Suite）發現的模式相同，透過這樣的方法可以驗證機上盒本身可能扮演類似通行金鑰角色，而機上盒本身專屬網卡硬體編碼則為關鍵認證資訊。

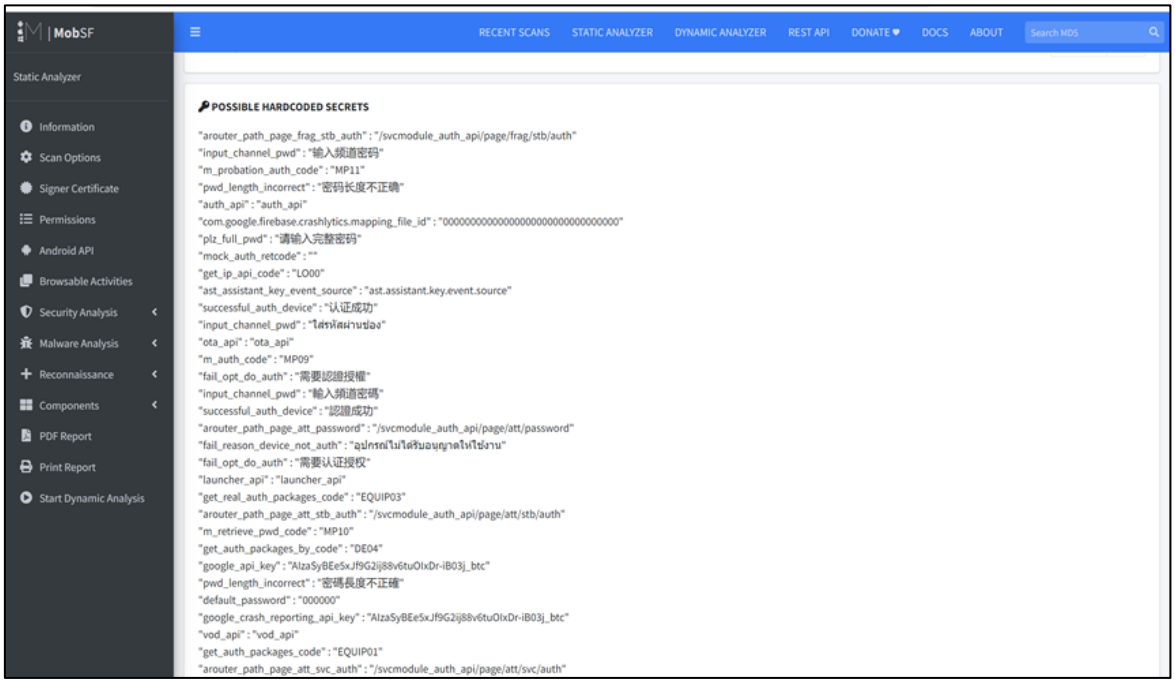

圖 7：Mobsf 靜態分析機上盒 App 必須預先輸入認證碼才能使用
資料來源：本計畫整理

三、 評估監理技術需使用之軟體及硬體工具

（一）軟體工具

1. 封包側錄工具

Wireshark：使用封包側錄工具 Wireshark 對 OTT TV 機上盒運作、連線過程進行封包側錄與分析，進一步瞭解該設備內容並同步比對封包運作狀況，檢測 App 啟用過程、使用期間有無綁定特定 OTT TV 機上盒之型號、序號、MAC 等可識別特定機上盒特徵之機制。

2. TLS 代理服務

Burp Suite：是一個用於測試網路應用程式安全性的圖形化工具，可透過加掛 proxy 分析網頁或用戶端 App 行為，用於分析其侵權之行為是否進行認證封包傳輸及非法訊號傳輸等運作機制。

3. 靜態分析工具

(1) apk-extractor.apk

透過在受測裝置上安裝 apk-extractor.apk，可以在不更動 App 內容的前提下取出 APK 程式。確保檢測之 APK 檔是能夠執行於機上盒之應用程式，而非仿冒之 APK。

(2) Mobile Security Framework[291]

透過分析工具 MobSF，針對 App APK 進行解析，並分析原始碼（Code Analysis），該工具可於報告呈現 App 之功能、風險分析、檔案位置，以利分析人員針對 App 之組成進行不同的測試，強化針對 App 侵權行為之判斷。

[291] Mobile Security Framework: https://mobsf.live/

（二）硬體工具

1. 測試用 OTT TV 機上盒

用於測試 OTT TV 機上盒實際運作情形，並進行 App 行為分析與檢測。受測之機上盒規格如下：

(1) A 機上盒：【CPU：Intel H618】、【記憶體：4GB】、【快閃記憶體：32GB】。

(2) B 機上盒：【CPU：ARM Cortex A35】、【記憶體：4GB】、【快閃記憶體：64GB】。

(3) C 機上盒：【CPU：ARM Mali G31 MP2】、【記憶體：4GB】、【快閃記憶體：32GB】。

2. Hub 或 Switch（具 Port Mirror 功能）

以有線方式連接測試主機與待測之機上盒，利用具備 Port Mirroring 功能之集線器或交換器收集 OTT TV 機上盒與外界通訊之封包，藉此分析封包資訊。

3. 鑑識工作站

作為分析 App、OTT TV 機上盒運作之鑑識工作站。安裝測試所必要之軟體，並以適當之方式對待測物之測試布局進行設置。

（三）符合 ISO 17025 實驗室品質管理系統的檢測程序

1. 確保封包過濾偵測證據的有效性

前述檢測 App 有無綁定特定 OTT TV 機上盒，是採用封包側錄工具 Wireshark 進行封包側錄與分析，為了確保封包過濾偵測證據的有效性，建議建立符合 ISO 17025 的程序。因此，目前，我國對於機上盒已建立技術檢驗標準，並要求符合 ISO 17025 的檢測實驗室進行檢測。未來，可更進一步擴充檢測範圍，發展 App 靜態測試、封包動態測試的監理技術，若有採用 Wireshark 封包

過濾等偵測措施時，建議參酌韓國智財權保護局數位著作權取證中心，建立採用符合 ISO/IEC 17025 精神之檢測程序，而更進一步擴充既有檢測實驗室之範圍。像是韓國智財權保護局負責執行韓國的著作權保護和監管工作，其在 2020 年啟動數位著作權取證中心，並取得數位鑑識領域 ANAB ISO/IEC 17025 認證[292]。支援數位著作權取證[293]是按照標準化程序和方法進行調查、蒐集、傳輸、儲存、分析和報告等系列流程，以確保資料具備作為侵犯著作權案件的數位儲存設備數位證據的法律能力，數位取證程序如下[294]：

(1) 初步調查：識別版權侵權案件、收集材料（包括螢幕截圖）、找到伺服器位置、識別操作者。

(2) 數位證據的收集：複製並鏡像磁碟、扣押特定物品、轉儲資料庫、準備 hash 證書。

(3) 數位證據的轉移：封裝裝置以屏蔽電磁波和衝擊、封存證據、移交證據。

(4) 數位證據分析：恢復數據、分析資料庫、分析原始碼、分析日誌和時間表。

(5) 數位證據報告：回顧分析過程、驗證分析結果、計算著作權侵權損失、撰寫分析報告。

(6) 數位證據的銷毀：退回或銷毀數位儲存設備、抹除硬碟和記憶體。

---

[292] Purpose of Establishment·History. (n.d.). KCOPA. https://www.kcopa.or.kr/eng/lay1/S120T428C430/contents.do

[293] Support for Digital Copyright Infringement Forensics. (n.d.). KCOPA. https://www.kcopa.or.kr/eng/lay1/S120T435C441/contents.do

[294] Id.

2. 符合 ISO17025 之檢測程序

針對技術項目之檢測，建立符合 ISO17025 之標準化流程，確保檢測結果之一致性。初步草擬如下圖 8 所示：

(1) 機上盒送驗。

(2) 記錄 OTT TV 機上盒型號與所需安裝之 App。

(3) 檢測 App 是否有盜取訊號之侵權功能。

(4) 若 App 存在侵權功能，進一步檢測判斷分析 App 是否在啟用或運作期間有綁定 OTT TV 機上盒型號、序號、MAC number 等資訊之機制。

(5) 《電信管制射頻器材審驗管理辦法》增列有關電信管制射頻器材之審驗規範，例如不得安裝非法軟體等類似歐盟之規範。若可證明 App 存在侵權功能，且 App 於啟用或運作期間有綁定 OTT TV 機上盒之機制，則該機上盒可視為非法侵權之工具，也就是販賣未經審驗合格之電信管制射頻器材，涉及違反上述規範，將處理回收、廢除機制。

(6) 通傳會針對 OTT TV 機上盒除事前審驗外，同時應加強市場抽驗，要求申請審驗者須出具所提供軟體不違反《著作權法》之切結書；對於常態違反規定之申請者與器材加強審驗要求。

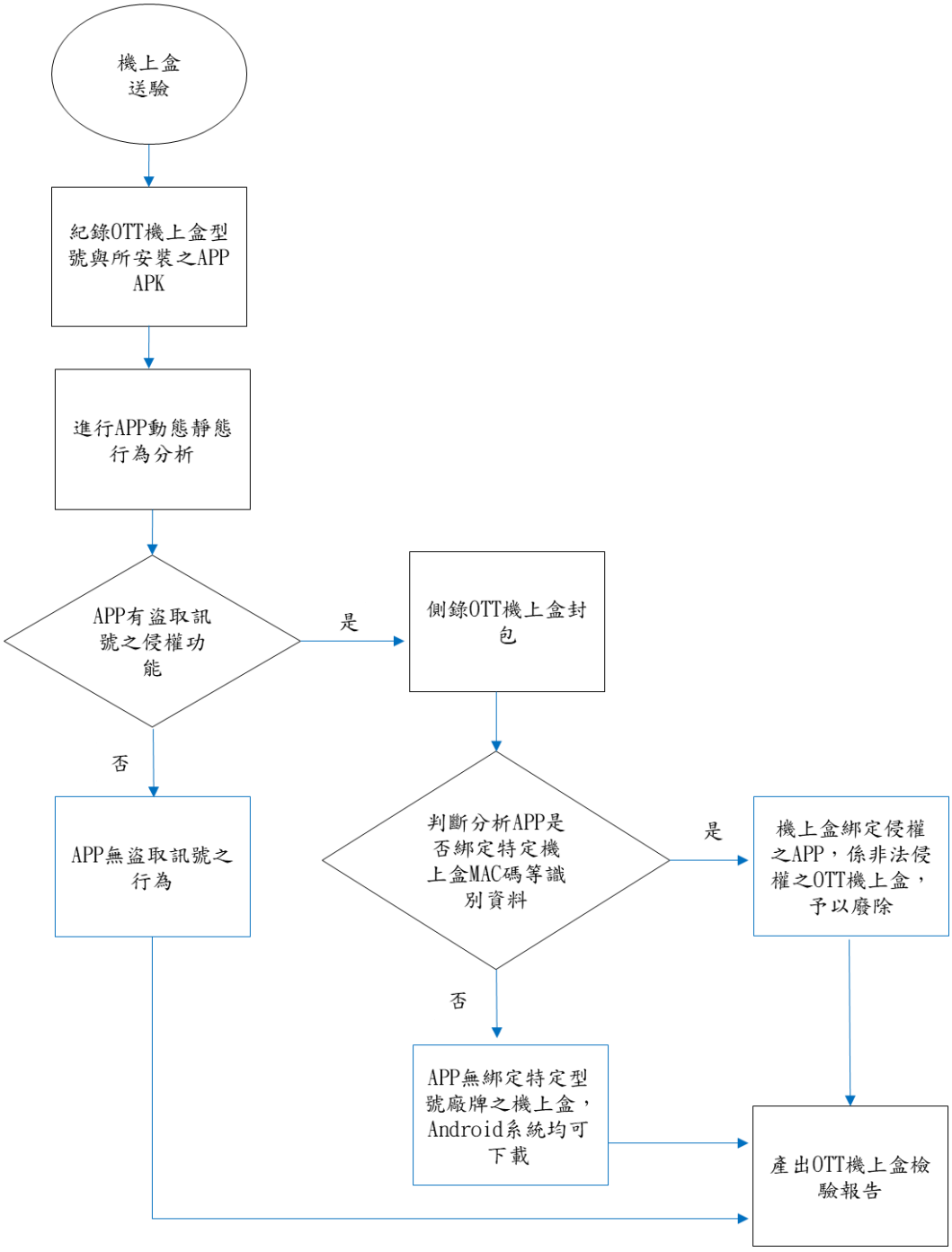

圖 8：OTT TV 機上盒檢驗作業流程圖

資料來源：本研究繪製

第五章 市售可收視未經合法授權視訊之 OTT TV 機上盒技術分析

本研究案選定目前國內市售 3 款 OTT TV 機上盒進行技術研究與內容分析，上述 OTT TV 機上盒均可收視未經合法授權節目頻道及隨選視訊，以下茲就相關檢測過程與測試結果進行相關說明：

第一節　機上盒初次連上網路之條件及程序

本次針對市售某 A 品牌機上盒進行檢測，從下圖 9 可簡略觀察該機上盒外觀相關硬體組成，包含電源器、傳輸線及遙控器，並且連結孔為 RJ45 規格網路傳輸線，並且可透過 Wifi 進行網路連線後，下載非法授權 App 收視，顯見為透過網際網路傳輸影音作為收視。

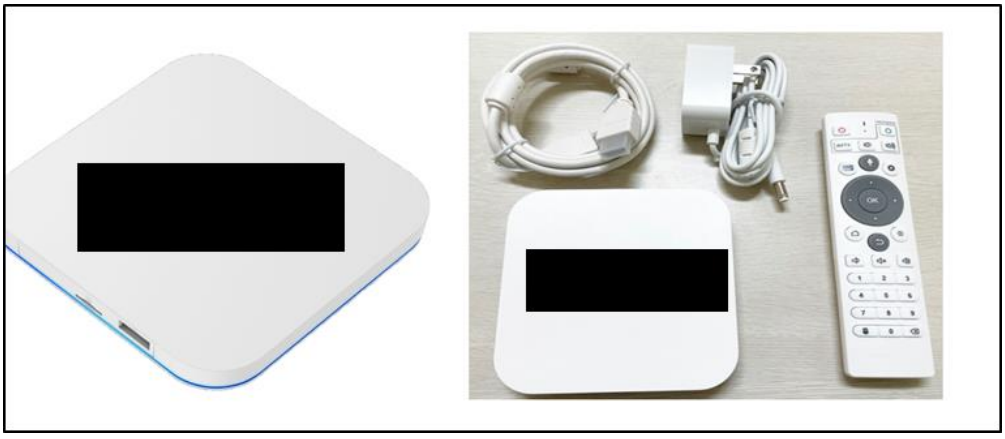

圖 9：某 A 品牌機上盒外觀
資料來源：本計畫整理

第二台受測之市售某 B 品牌機上盒，從下圖 10 可簡略觀察該機上盒外觀亦僅為一硬體包覆之機上盒，也包含電源器、傳輸線及遙控器，連結孔為 RJ45 規格網路傳輸線，與其他機上盒相同可透過 Wifi 進行網路連線後收視，確認均透過網際網路傳輸影音作為收視。

圖 10：某 B 品牌機上盒外觀
資料來源：本計畫整理

第三台受測之市售某 C 品牌機上盒，從下圖 11 可簡略觀察該機上盒外觀為一硬體包覆之機上盒，也包含電源器、傳輸線及遙控器，連結孔為 RJ45 規格網路傳輸線，與其他機上盒相同可透過 Wifi 進行網路連線後，下載非法授權 App 收視，確認均透過網際網路傳輸影音作為收視。

圖 11：某 C 品牌機上盒外觀
資料來源：本計畫整理

上述三台 OTT TV 機上盒均為 Android 作業系統，在開機之後，都必須先設定有線網路或無線網路：進入主頁面後，點選「網路」連接 Wifi 或者插入 RJ45 網路線連上網路，透過系統中的設定選擇網路連線方式，如圖 12 所示。

初次開啟三台機上盒，發現其中皆無預設安裝侵權影音程式，符合其所稱為純淨版機上盒。

圖 12：機上盒網路設定操作畫面
資料來源：本計畫整理

第二節　分析說明機上盒中播放未經合法授權節目頻道及隨選視訊軟體之取得管道與運作方式

一、3 款機上盒取得非法 App 之途徑

（一）A 品牌機上盒取得非法 App 之途徑

透過 google 直接搜尋 A 品牌機上盒相關安裝說明指引(如圖 13)，會找到安裝指南，並取得安裝資訊，起先會提供 ub1234.com，如圖 14。但由於此網域名稱已被 TWNIC 封鎖解析，因此查詢後發現，可以透過 ub6789.com 此域名下載應用程式。依照指示開啟機上盒到進入系統主畫面時，開啟瀏覽器並搜尋 ub6789.com，下載「uptv」並依照指示安裝即可開啟 App 觀看盜版節目，如圖 15 所示。

圖 13：網路上可以搜尋 A 品牌機上盒之 App

資料來源：截取自 Google 搜尋結果，本研究整理

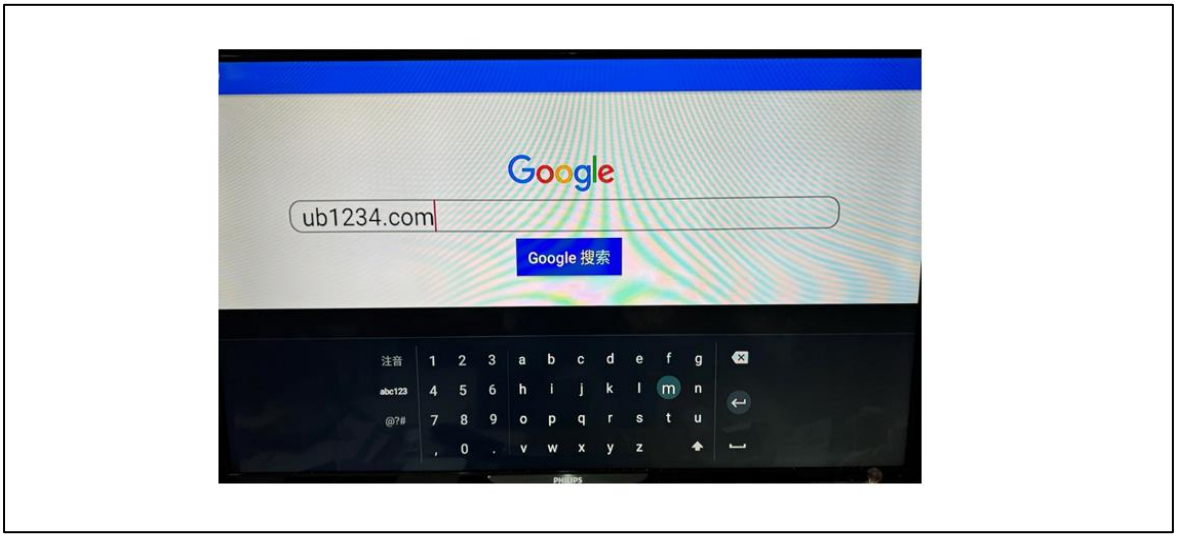

圖 14：A 品牌機上盒 App 下載網址

資料來源：截取自 Google 搜尋結果，本研究整理

圖 15：A 品牌機上盒之備用之 App 下載網址

資料來源：本研究整理

（二）B 品牌機上盒取得非法 App 之途徑

如下圖 16 所示，可先透過 google 搜尋到 B 品牌機上盒教學，並從該文章中得知 B 品牌機上盒 App 係從第三地網站 8686c.cc 下載。圖 17 說明 B 品牌機上盒之安裝非法侵權影視應用程式之流程。使用該機上盒預設瀏覽器輸入 8686c.cc 後，便可以下載 Yogurt TV App，安裝完成後即可觀看盜版節目，無須輸入帳號密碼或註冊帳號。

圖 16：B 品牌機上盒網路搜尋下載 App 之教學

資料來源：截取自 Google 搜尋結果，本研究整理

圖 17：從第三方網站下載非法親權之影視 App

資料來源：本研究整理

（三）C 品牌機上盒取得非法 App 之途徑

如圖 18 所示，使用 Google 搜尋 C 品牌盒子安裝教學，可以找到一個 43066.cc 的網站，如圖 19，可點選欲下載使用之非法影視 App，安裝完成後即可使用應用程式觀看盜版節目，無須其他認證方式。

圖 18：搜尋 C 品牌機上盒之安裝教學

資料來源：截取自 Google 搜尋結果，本研究整理

圖 19：透過專屬網址下載非法影視 App

資料來源：截取自網路搜尋結果，本研究整理

二、 3 款機上盒 App 運作與機上盒認證之關聯

（一）A 品牌機上盒驗證機制

A 品牌機上盒啟動非法影音 UBTV App 時，以 HTTPS 協定進行加密傳輸，並採用 POST 方法與後端伺服器取得節目資訊。因此，檢測時必須透過 Burp Suite 建立 TLS 代理伺服器，方能取得明碼網址傳輸內容，如下圖 20 所示。網路傳輸認證資訊，如圖 21，因其資訊經過加密，無法得知確切之認證資訊為何。而後才開始下載.m3u8 檔案取得節目索引，並以此向伺服器取得.ts 檔案讓機上盒使用者收視。

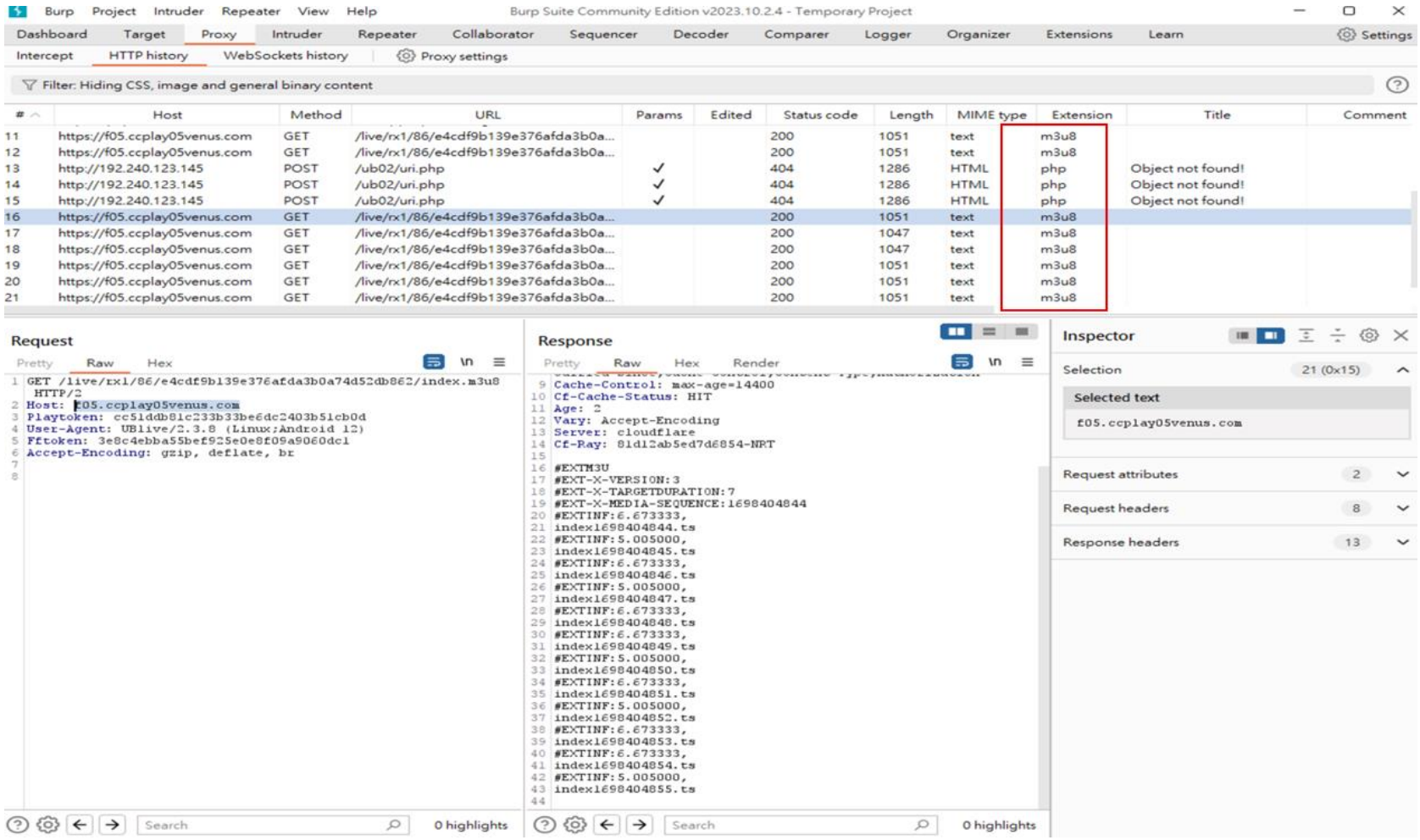

圖 20：透過 Burp Suite 解析 A 品牌機上盒之 HTTPS 請求

資料來源：本研究整理

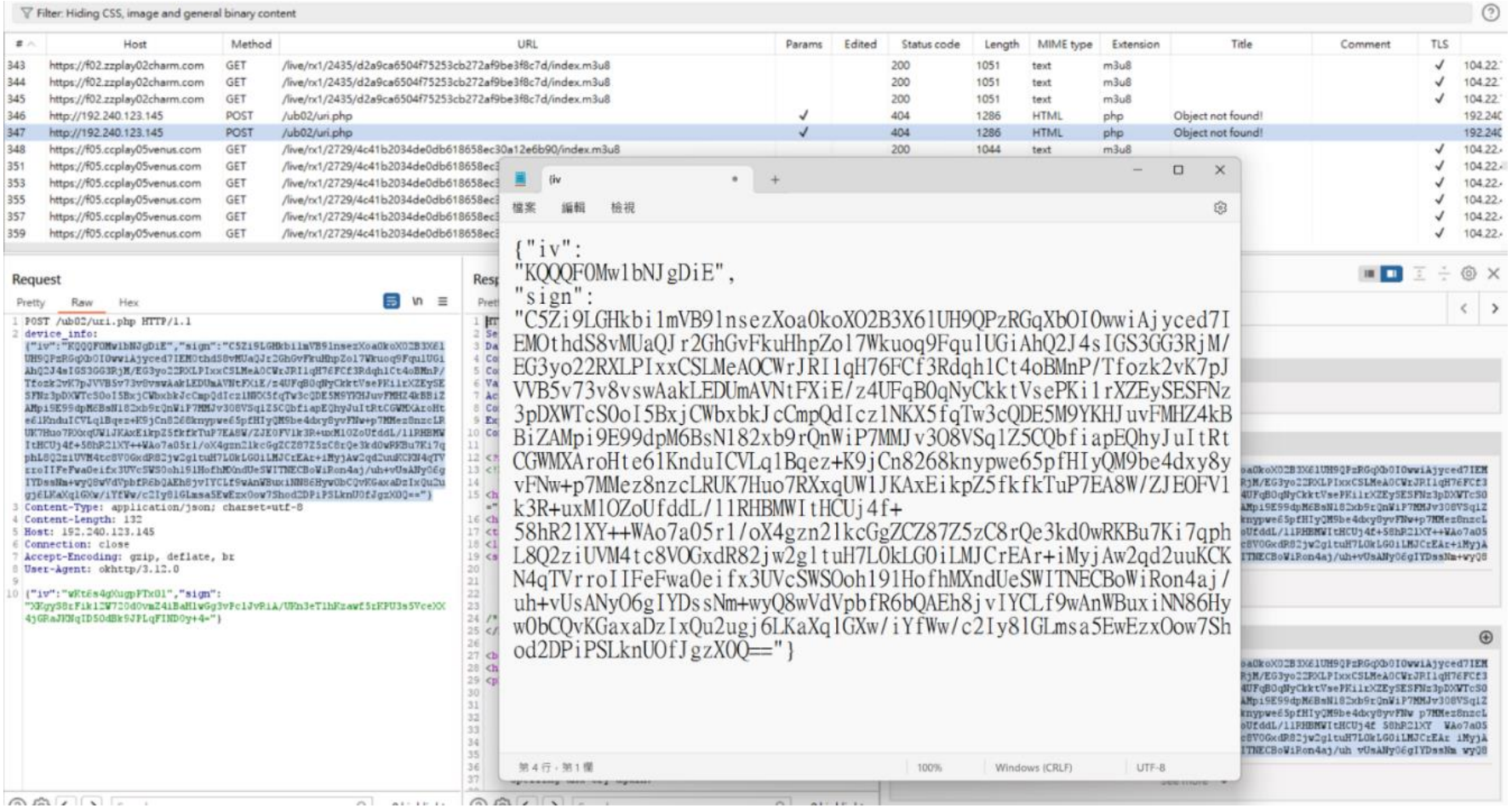

圖 21：A 品牌機上盒疑似經過加密的認證機制

資料來源：本研究整理

（二）B 品牌機上盒驗證機制

B 品牌機上盒透過封包與網址分析，確認會認證機上盒晶片、SN 序號、網卡 MAC 等資訊，透過機上盒硬體資訊做為驗證，亦用為控管使用者使用相關服務，如圖 22 所示。

圖 22：B 品牌機上盒認證機制

資料來源：本研究整理

（三）C 品牌機上盒驗證機制與影音傳輸方式

C 品牌機上盒當開啟「享悅 TV」App 時，會主動連向 http://fd10d586.ockeyo.com/api/wbtj5hmx，然後認證 C 品牌機上盒主機上之網路卡編號，確認後才開啟影視瀏覽畫面，如圖 23。

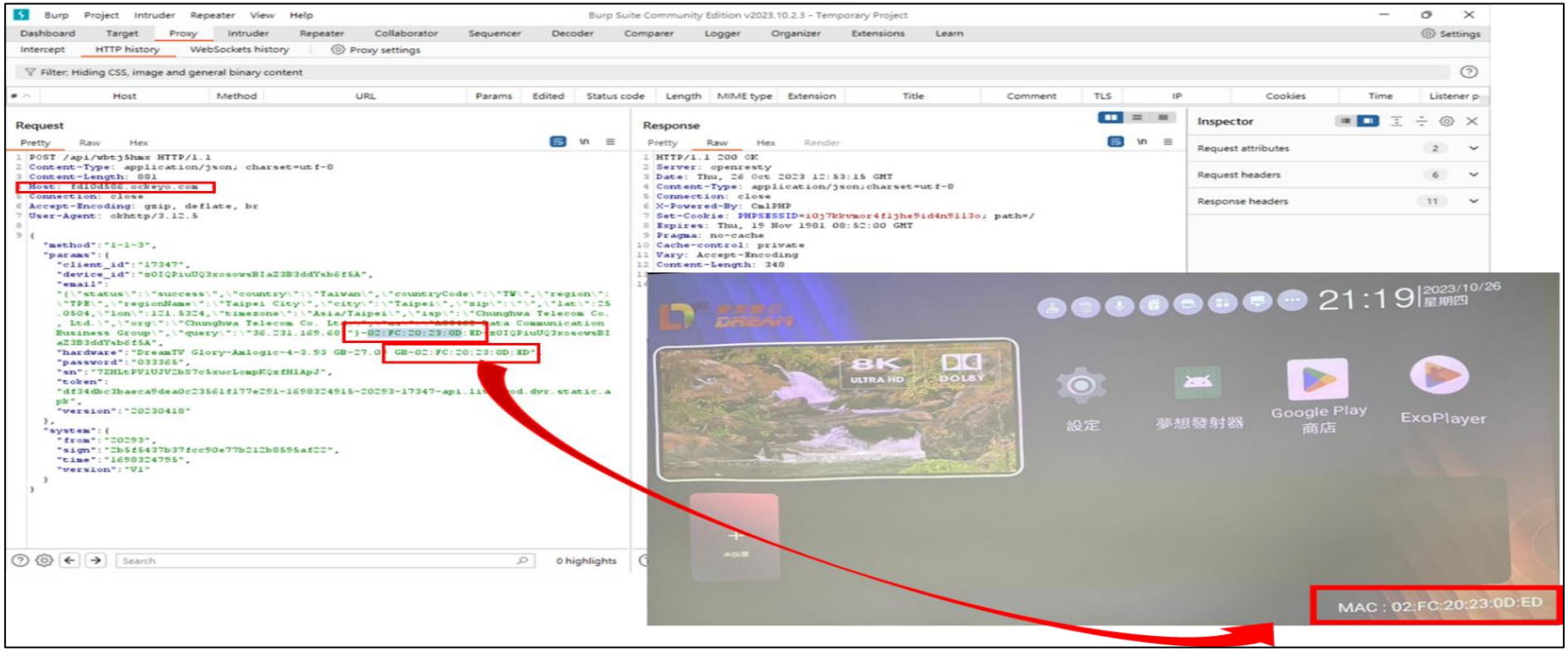

圖 23：C 品牌機上盒開啟 App 後便執行認證機制

資料來源：本研究整理

三、 使用 Mobsf 工具對於 APK 程式進行靜態分析

Mobsf 為一個用於分析行動裝置應用程式框架之程式。提供了靜態分析與反組譯之功能，並提供應用程式安全性分析之功能。本研究使用此工具分析盜版影視應用程式，發現在原始程式中使用了加殼程式 libshell-super 進行混淆，因此需要進一步使用逆向加密演算法來取出金鑰，方能檢視完整之程式碼。然而，在程式中所儲存的字串，如圖 24 所示，包含認證相關之提示字詞，推斷應用程式可能存在認證機制。但是在測試過程中，並未發現任何需要使用者輸入認證資訊的地方，因此可能是藉由綁定裝置資訊於伺服器端進行驗證。

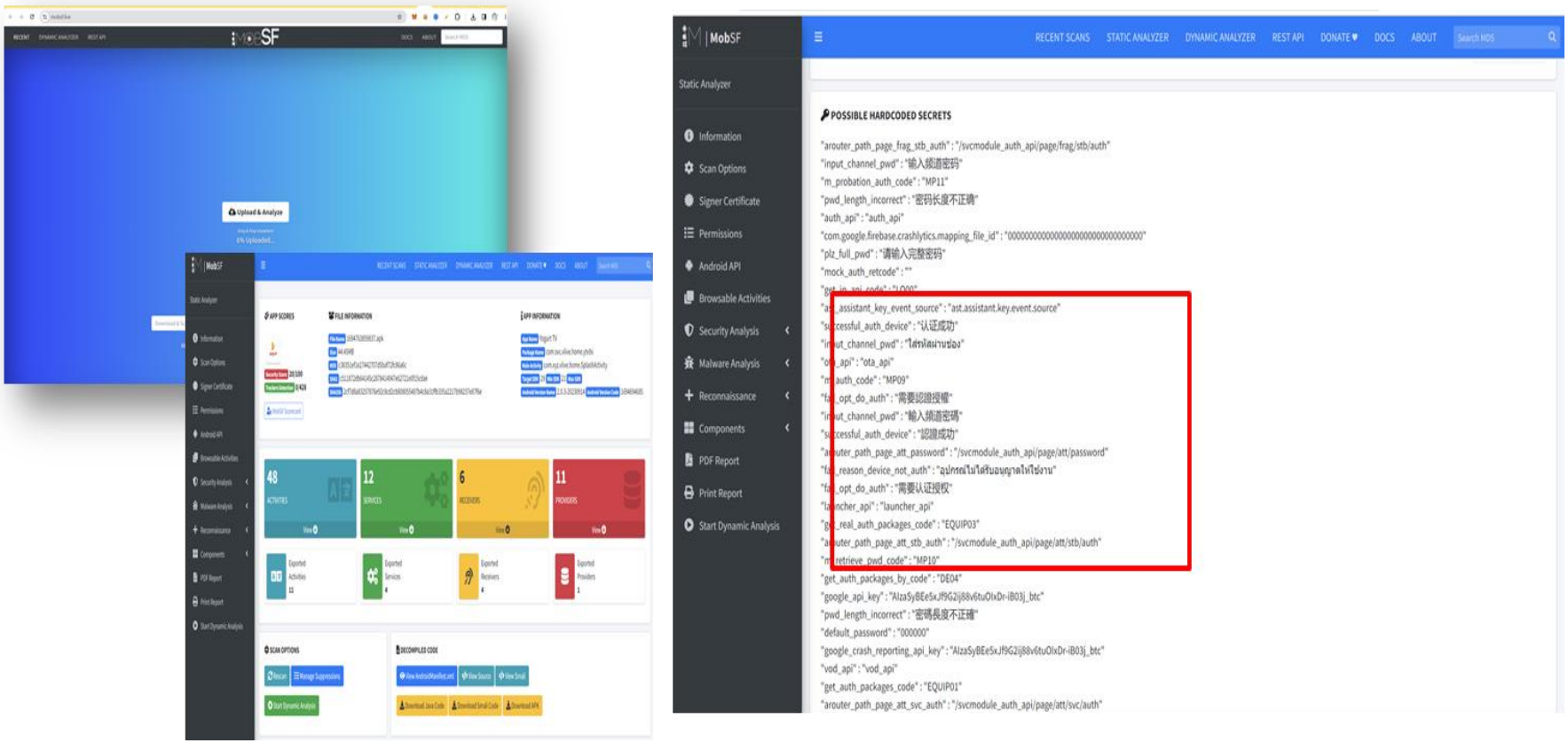

圖 24：使用 Mobsf 靜態分析之結果

資料來源：本研究整理

四、 小結

上述 3 款機上盒均有認證機制，透過綁定機上盒相關硬體資訊限制使用者僅能於特定裝置執行盜版影視應用程式。而裝置綁定之資訊多半以網卡 MAC 為主，因為網卡 MAC 常被認為是唯一識別碼，目前主流的裝置綁定機制多使用此資訊做為裝置認證之資訊，如表 12。

表 12：比較 3 款機上盒認證機制異同性

機上盒種類	有無認證	認證方法
A 品牌機上盒	有	加密（無法解出）
B 品牌機上盒	有	網卡編號等資訊
C 品牌機上盒	有	網卡編號等資訊

資料來源：本研究整理

第三節　機上盒播放未經合法授權節目頻道及隨選視訊之操作方式

一、 A 機上盒 OTT TV 頻道與隨選視訊操作方式

A 機上盒主要係以「UBTV」及「UB 影視」等 2 個 App 進行收視，UBTV 主要負責提供臺灣或其他國家的直播節目，相關頻道號碼與有線電視業者均相同（如圖 25），如果沒有告知為非法機上盒的情況下，幾乎與現有有線電視業者使用同軸電纜進行傳輸的節目內容差異不大，另外目前因為網路盜版訊號品質日益提升，幾乎也能達到標榜 4K 畫質，如圖 26，對合法業者的智慧財產權侵害極大。

圖 25：A 機上盒節目頻道名稱與播放內容

資料來源：截取自 A 機上盒畫面，本研究整理

圖 26：A 機上盒網路販售標榜可達 4K 畫質

資料來源：截取自市售電子商務平台，本研究整理

二、 B 機上盒 OTT TV 頻道與隨選視訊操作方式

B 機上盒操作方式主要以「Yogurt TV」為主要播放各式直播節目之 App，操作上大致上也與其他市售與有線電視業者機上盒相同，具備完整節目頻道編號、名稱，如圖 27，直接使用遙控器操作就可以觀看節目內容。

圖 27：B 機上盒節目頻道名稱與播放內容

資料來源：截取自 B 機上盒畫面，本研究整理

三、 C 機上盒 OTT TV 頻道與隨選視訊操作方式

C 機上盒主要透過「享悅 TV」與「享悅影視」2 個 App 來負責播放國內直播頻道及隨選影劇內容，當開啟「享悅 TV」App 時，可以看到非常明顯的頻道名稱，也會出現其他國家的頻道在最左邊可以選擇，全數頻道可以使用遙控器來操作，節目的畫質也與目前有線電視業者提供內容差距不大，如圖 28，顯然盜版影視的來源品質可能很好，操作上之直覺性且與目前合法有線電視者或 OTT 業者頻道內容非常接近。

圖 28：C 機上盒節目頻道名稱與播放內容

資料來源：截取自 C 機上盒畫面，本研究整理

第四節　機上盒可收視節目頻道數量、類別、來源國家之統計及說明

一、 各機上盒可收視頻道數量

統計 3 款機上盒，均能提供超過 200 台以上的國內頻道，而且非侷限於台灣本土，且所有訊號均透過網際網路提供，但穩定度仍有落差，有時頻道內容會有不穩定及闕漏狀況。整理各機上盒頻道狀況如表 13。

表 13：各機上盒頻道列表

機上盒類別	頻道數（台灣頻道）	有無其他國家
A 品牌機上盒	203 台	有
B 品牌機上盒	225 台	有
C 品牌機上盒	200 台	有

資料來源：本研究整理

二、 機上盒收視頻道來源國家類別

比較 3 款機上盒頻道來源國家，以 A 品牌機上盒最多，其次為 B 品牌機上盒，最後是 C 品牌機上盒，不難發現 3 款機上盒幾乎擁有相同的頻道別，合理推測應有專屬集團從事買賣這些遭竊取的頻道，並提供機上盒業者進行內容整合，如表 14。

表 14：機上盒頻道來源國家別統計

機上盒	頻道來源統計
A 品牌機上盒（18 國別）	臺灣 港澳大陸 日本 韓國 美國 加拿大 英國 法國 義大利 新馬 馬來新 菲律賓 泰國 印尼 越南土耳其 巴西 印度
B 品牌機上盒（15 國別）	臺灣 港澳大陸 美國 英國 加拿大 韓國 日本 新馬 印度 印尼 越南 泰國 菲律賓 澳大利亞 柬埔寨
C 品牌機上盒（13 國別及區域）	臺灣 香港大陸 國際 日本 韓國 印度 歐美 印尼 菲律賓 新馬 泰國 越南 新加坡

資料來源：本研究整理

第五節　封包側錄與追蹤

從上述分析可知目前市面上之機上盒會使用硬體資訊來確認該機上盒為應用程式可運作之載體。認證完成後，應用程式會透過 HTTPS 取得影片索引檔（通常為 m3u8 檔案格式）。在取得影片索引檔之後，當使用者選擇節目時，App 會抓取影片來源（存放於 ts 檔），連線至影片所在之 CDN（Content Distribution Network，內容傳遞網路），即可播放影片，如圖 29。

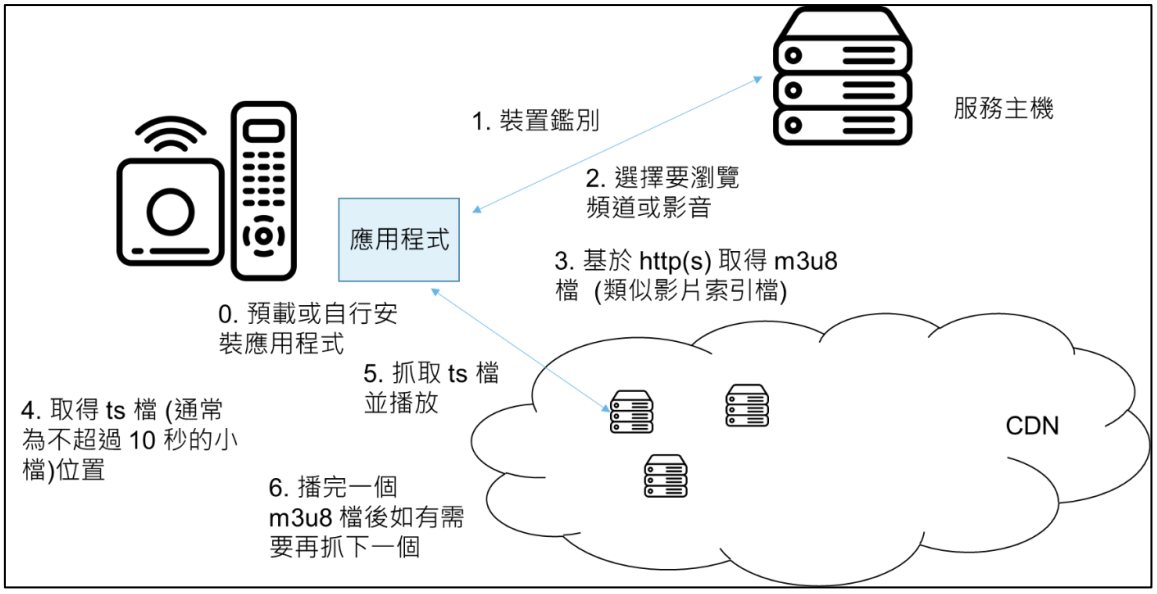

圖 29：OTT TV 機上盒播放技術概念，以 HLS[295]為例
資料來源：本研究整理

而本研究將測試環境中以側錄主機連上網路後，開啟熱點並分享網路給待測之機上盒，同時側錄主機開啟封包側錄軟體 Wireshark 以及代理伺服器 Burp Suite。WireShark 可側錄機上盒連線網際網路的所有封包並分析通訊行為樣態，Burp Suite 則是設定代理伺服器，利用中間人攻擊手法繞過機上盒的 HTTPS 加密，從中取得認證資訊、影片來源、傳輸路徑等內容。合併兩者分析結果可取得非法影音之來源，並識別其為境內或境

[295] 什麼是 HTTP 即時串流 (HLS，HTTP Live Streaming) https://www.cloudflare.com/zh-tw/learning/video/what-is-http-live-streaming/

外之傳輸路徑，溯源機上盒連接對應 CDN 機房之位址，以下就三個機上盒結果作個別呈現。

一、 傳輸模式分析

（一）A 品牌機上盒傳輸模式分析

如圖 30，分析 A 品牌機上盒 UBTV 中「幸福空間居家」等頻道影音來源，發現 f05.ccplay05venus.com 等多個網址，會提供機上盒用戶下載 m3u8 檔案，然後開始串流式傳輸，透過下面影片與封包檔案分析就可以佐證該機上盒有連線境外 CDN 主機來進行侵權收視行為（提取 m3u8 檔案，內含.ts 視訊檔案）。

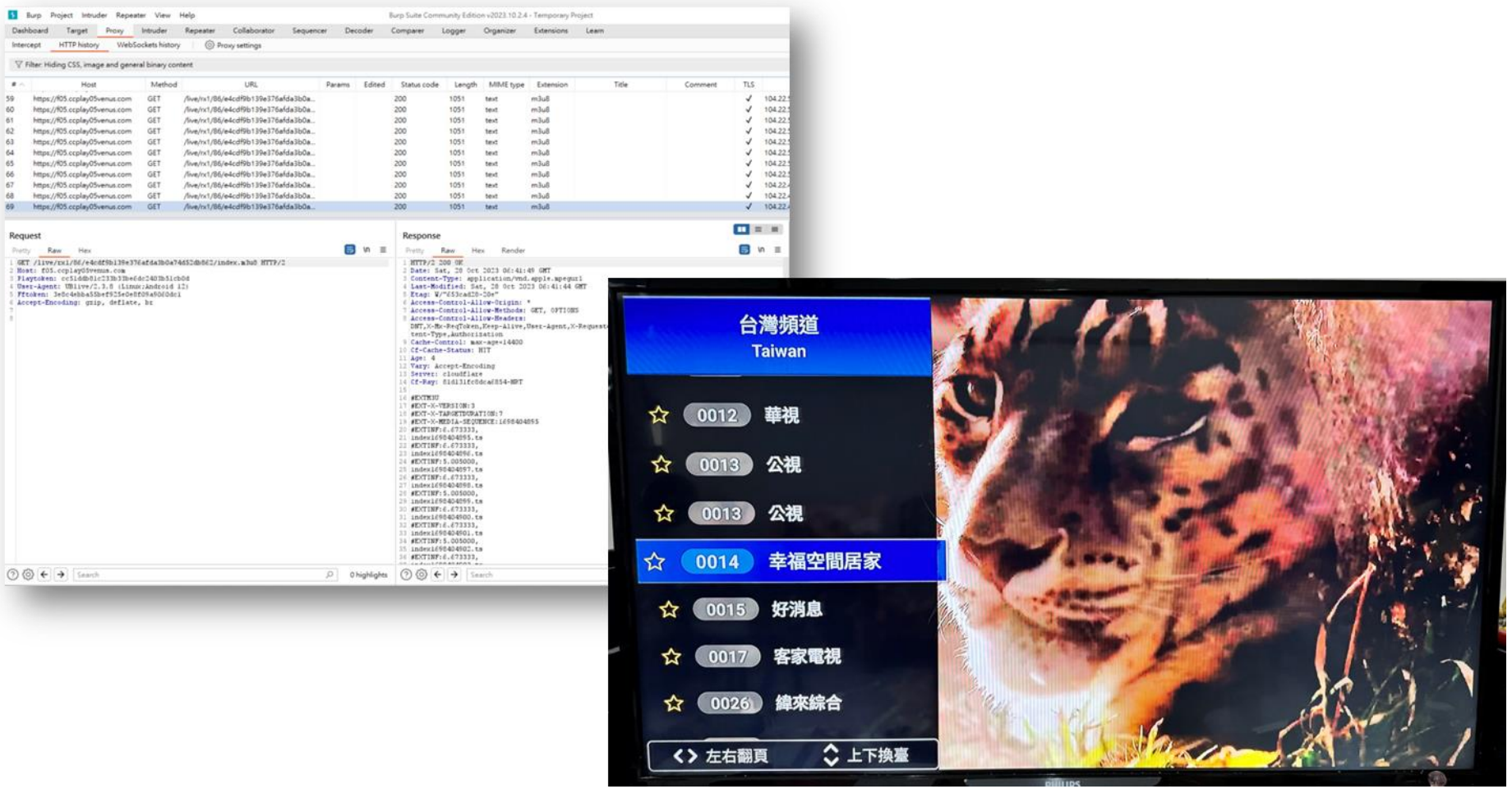

圖 30：分析 A 品牌機上盒之幸福空間居家頻道來源

資料來源：截取自 A 機上盒畫面，本研究整理

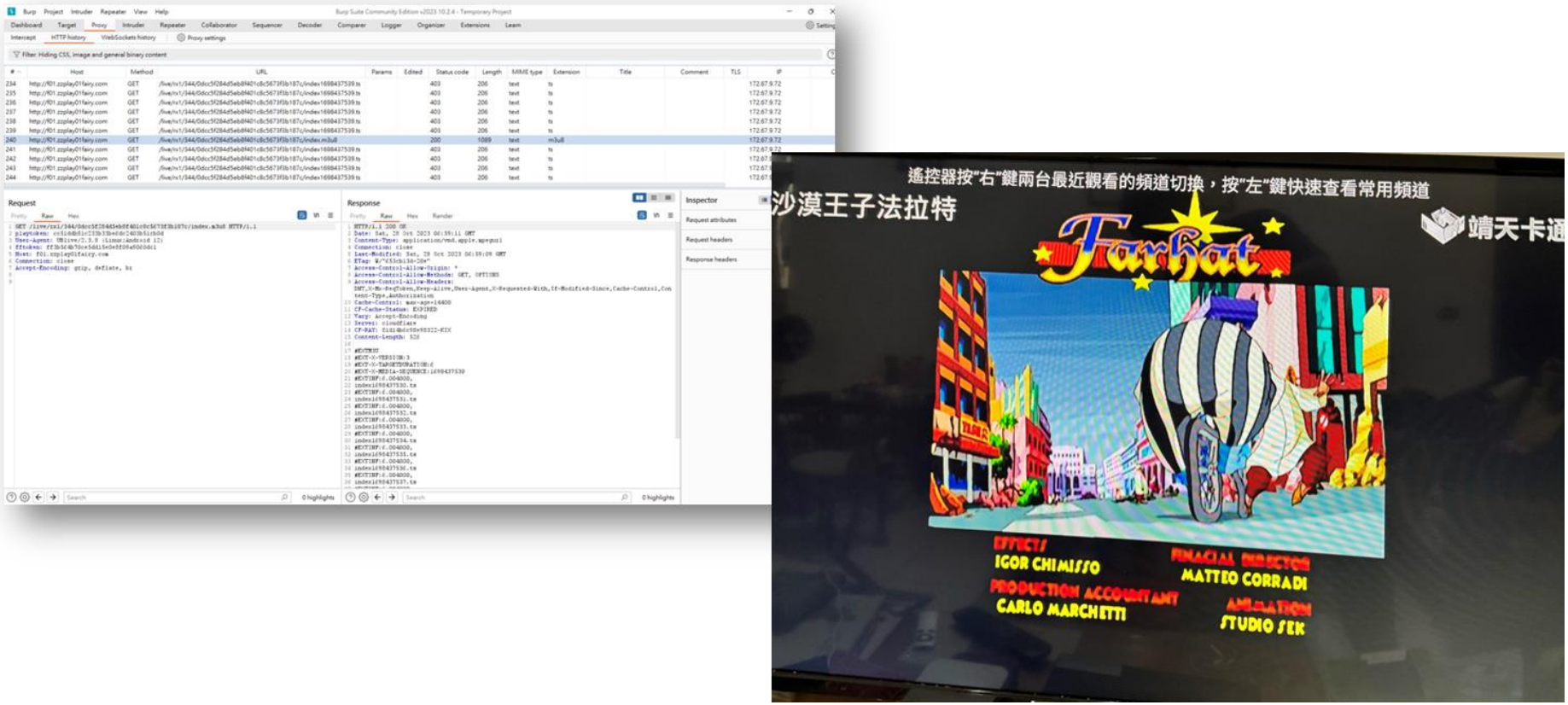

圖 31：分析 A 品牌機上盒「靖天卡通台」頻道來源

資料來源：截取自 A 機上盒畫面，本研究整理

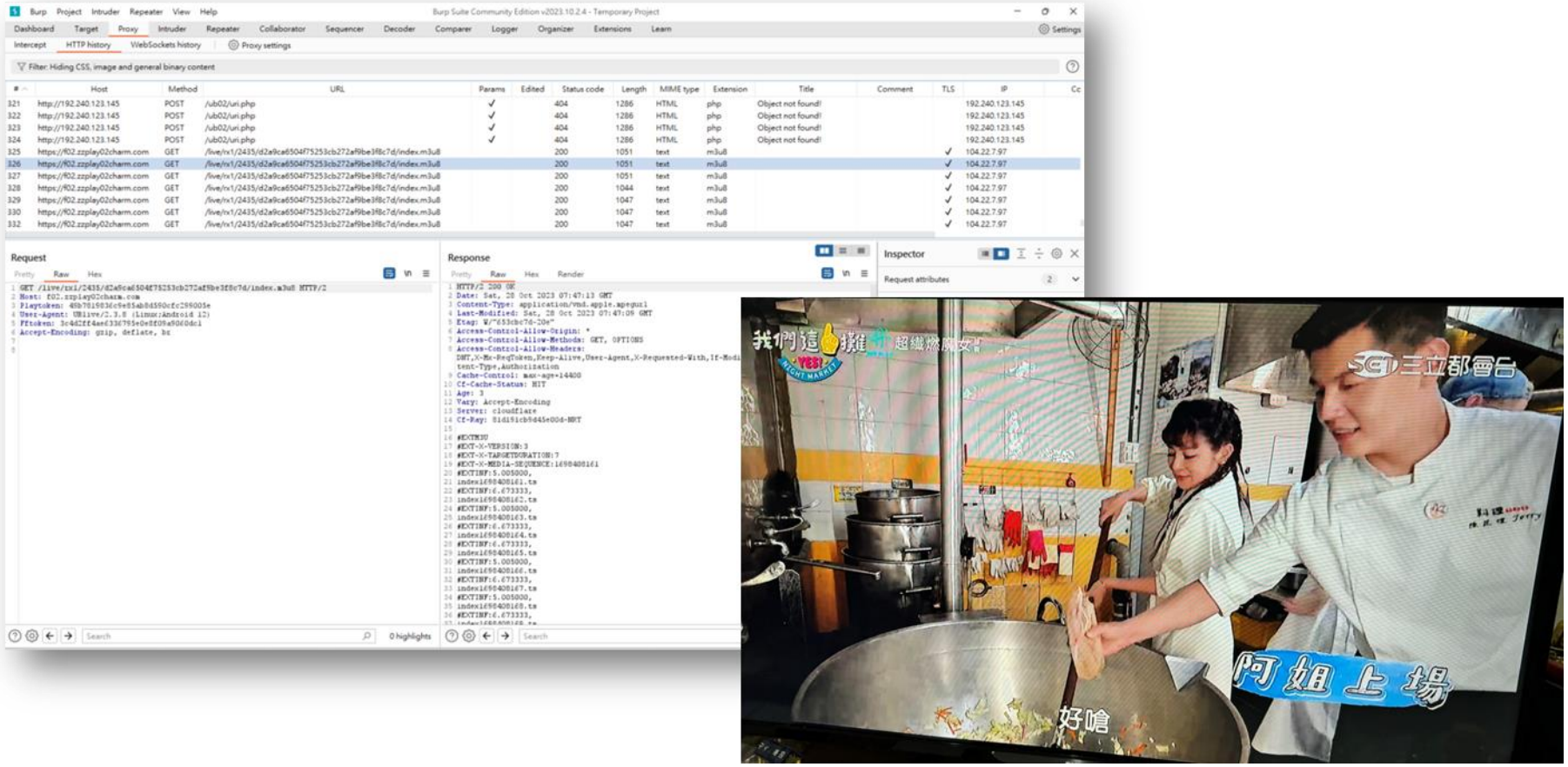

圖 32：分析 A 品牌機上盒「三立都會台」頻道來源

資料來源：截取自 A 機上盒畫面，本研究整理

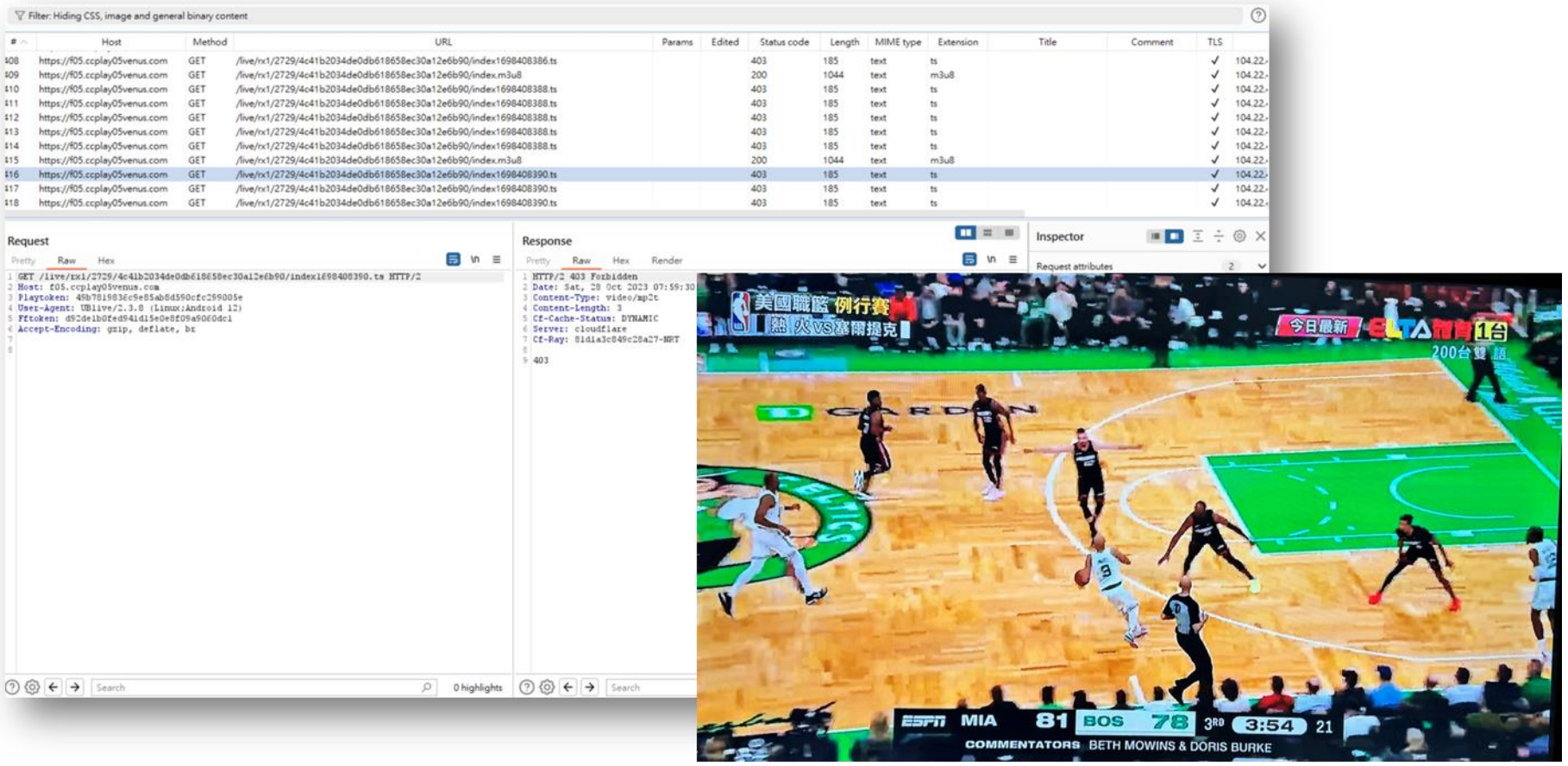

圖 33：分析 A 品牌機上盒「愛爾達體育一台」頻道來源

資料來源：截取自 A 機上盒畫面，本研究整理

上述分析結果，A 機上盒相關影視檔案來自於 f05.ccplay05venus.com（2 組）、f01.zzplay01fairy.com、f02.zzplay02charm.com 等網址，如圖 31、圖 32、圖 33，經查網址均為雲端反向代理 CDN 主機，均使用美國 Cloudflare 作為域名管理服務供應商，如圖 34，後端主機真實來源尚無法確認是否位於境內，仍需透過管道向業者取得資訊。

	IP	域名	国家	Region	城市	ISP	ASN
■	104.22.5.43	f05.ccplay05venus.com				CLOUDFLARENET	13335
■	104.22.38.162	f01.zzplay01fairy.com				CLOUDFLARENET	13335
■	104.22.6.97	f02.zzplay02charm.com				CLOUDFLARENET	13335

3 out of 3 hosts successfully processed. Have a nice day!

圖 34：A 品牌機上盒使用之 CDN

資料來源：本研究整理

（二）B 品牌機上盒傳輸模式分析

透過封包分析找出 B 機上盒使用 xml 進行收視內容傳輸，如圖 35。另外透過分析發現 B 品牌機上盒後臺為 tms.szbboys.com:8000，位於中國境內，如圖 36 及圖 37。

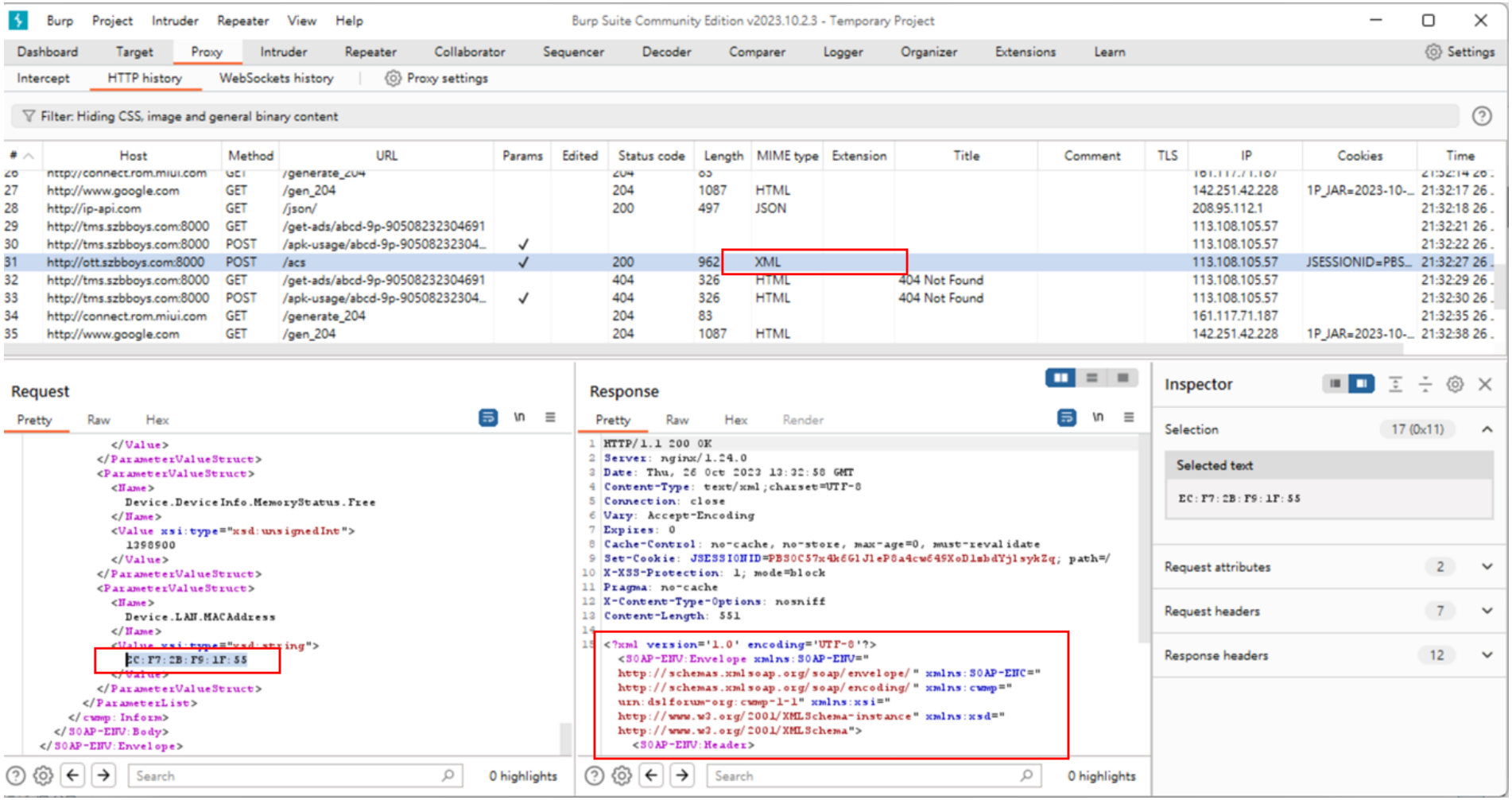

圖 35：B 品牌機上盒透過 xml 傳輸節目資訊

資料來源：本研究整理

圖 36：B 品牌機上盒後臺管理系統畫面

資料來源：截取自 B 機上盒後臺畫面，本研究整理

	IP	域名	国家	地区	城市	互联网服务供应商	ASN
[redacted]	113.108.105.57	tms.szbboys.com	中国			Chinanet	4134

圖 37：B 品牌後台主機位置

資料來源：本研究整理

（三）C 品牌機上盒傳輸模式分析

當 C 品牌機上盒開始點選直播影視畫面時，會先從主機下載 m3u8 索引檔，然後播放影音，如圖 38。另外測試享悅 TV 開啟「華視新聞」之 m3u8 索引檔，使用能支援解析之影片播放器，可以自動下載其中的.ts 檔案，看到 CDN 上影音片段檔案，如圖 39。

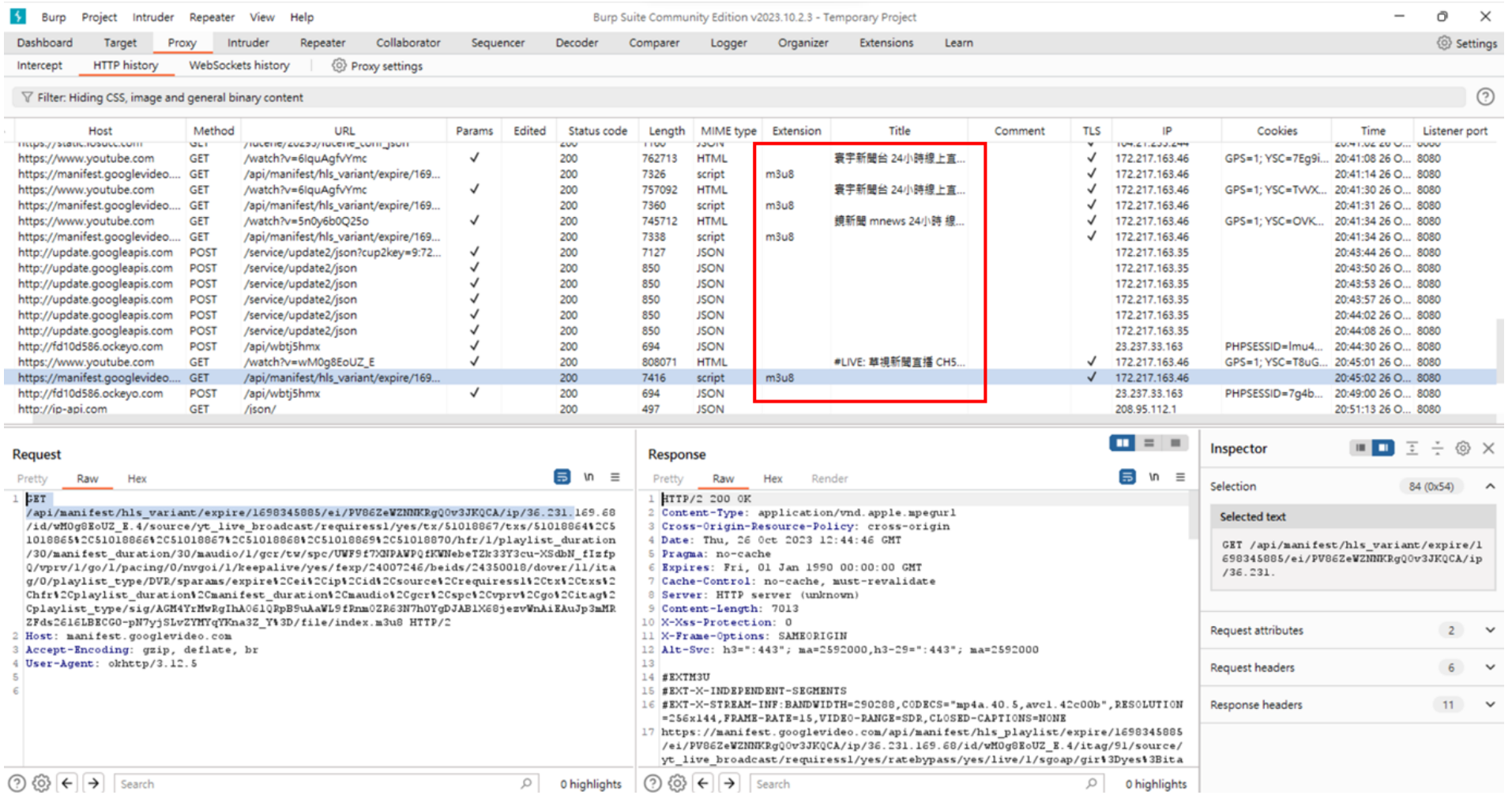

圖 38：享悅 TV 開始播放時會下載 m3u8 格式目錄檔取得節目影片索引

資料來源：本研究整理

圖 39：透過支援 m3u8 之影片播放器，可以自動取得影音內容

資料來源：截取自 C 機上盒畫面，本研究整理

影音提供之主機 http://fd10d586.ockeyo.com，主要提供認證後影音內容，經查來自於美國，如圖 40。

IP	域名	国家	地区	城市	互联网服务供应商	ASN
23.237.33.163	fd10d586.ockeyo.com	美国	加州	洛杉矶	COGENT-174	174

圖 40：提供 m3u8 索引檔之伺服器位置

資料來源：本研究整理

二、 小結

整理 3 款機上盒傳輸機制與影音訊號來源如表 15，3 款機上盒皆將相關主機或代理伺服器放置於境外，主要是為了提高隱匿度，避免遭到查緝或干預。

表 15：彙整 3 款機上盒傳輸機制與影音訊號來源

機上盒種類	有無加密	IP（含 CDN）來源
A 品牌機上盒	有	境外
B 品牌機上盒	有	境外
C 品牌機上盒	有	境外

資料來源：本研究整理

第六節　其他有助於 OTT TV 機上盒監理技術事項

本研究經由側錄結果顯示發現多數市售非法機上盒於封包傳輸過程中，封包內容均有加密，故提出下列建議事項，有助於機上盒監理技術之分析。

一、 繞過憑證綁定機制

綁定憑證的方式可能包括數位簽章、訪問金鑰或其他安全控制機制。綁定憑證是指將特定的數位憑證（Digital certificate）與特定的設備、應用程式或用戶帳戶關聯起來，確保僅有具有相應憑證的設備可以訪問服務，以實現安全性和身份驗證的目的。OTT TV 機上盒可能會使用憑證或其他形式的身份驗證來確保僅有被授權的用戶可以取得對應的服務與內容，這種授權機制有助於侵權者管控僅向購買機上盒的消費者提供侵權影音內容。

因此在檢測過程中於測試環境中安裝有效之憑證，可有助於 OTT TV 機上盒之技術監理，取得更完整之服務、連線、資料傳遞過程等內容。同時，綁定憑證過程須倚靠破解程式或其他破解工具，故可透過憑證之破解，深入了解機上盒之內容，更加符合機上盒之使用設定（如圖 41）。

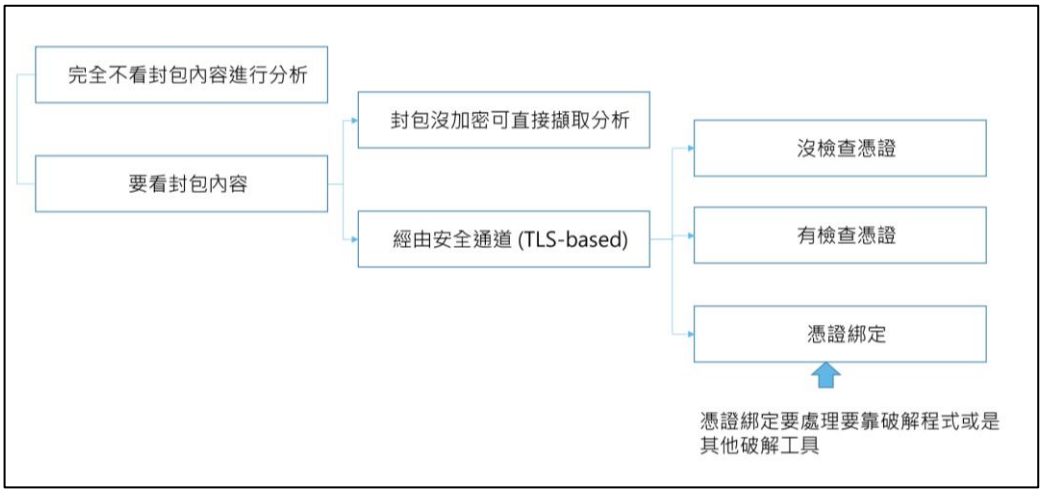

圖 41：封包分析處理過程建議流程　資料來源：本研究整理

二、 Proxy 代理伺服器設定

Proxy（代理伺服器）設定是在網頁伺服器或應用程式中配置的一種網路設定，用來通過中介伺服器轉發網路請求，可增加隱私、改進性能、實施內容篩檢或繞過特定網路限制。故透過手動修改 Proxy 之埠號及代理伺服器位址，可達成中間人攻擊（Man-in-the-Middle Attack，簡稱 MITM 攻擊）之效果，取得更加完整之 OTT TV 機上盒傳輸內容。

中間人攻擊係指一種攻擊手法，攻擊者在通信的兩端之間插入自己的位置，能夠截取、修改或監控通訊內容。故利用 Proxy 手動修改，直接攔截並可讀取未經加密之封包內容，更有利於非法來源之溯源，並監理 OTT TV 機上盒與 App 間的認證關係。

三、 建置虛擬機環境

針對 Android 程式行為進行分析，將測試 OTT TV 機上盒使用之侵權影音程式 App，其 APK 是否可在其他安卓系統環境下正常安裝使用，若可以在其他安卓環境下正常安裝使用、觀覽節目，則該 App 與 OTT TV 機上盒本身可能不存在認證或綁定關係；相反地，若 APK 無法在虛擬機環境之系統下順利安裝、使用，僅在所對應機上盒才可正常安裝、開啟使用，則可進一步證明機上盒與瀏覽盜版影音程式存在關聯性。

（一）A 品牌機上盒使用之特定 App 放入虛擬機檢測

將下載之 A 品牌機上盒之專屬 APK（圖 42）放入安卓虛擬機（LDPlayer 或 Vmware），會發現雖然可以順利開啟 APK 程式，但是卻無法收視到影音內容，如圖 43。顯見 App 如果未經過實體機上盒機碼驗證機制，將無法進行影音收視行為，可證明該 App 與硬體存在綁定關係。

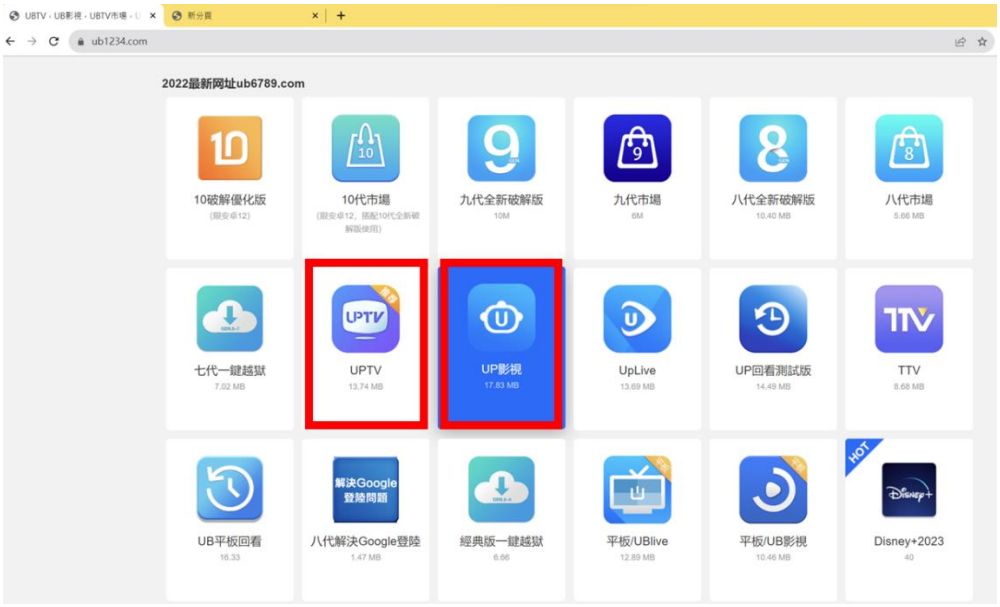

圖 42：下載 A 品牌機上盒之 APK 程式

資料來源：本研究整理

圖 43：使用虛擬機無法收視

資料來源：本研究整理

（二）B 品牌機上盒使用之特定 App 放入虛擬機檢測

將下載之 B 品牌機上盒之專屬 APK（圖 44）放入安卓虛擬機（LDPlayer 或 Vmware），發現無法開啟 APK 程式，並顯示認證失敗，顯見脫離了實體機上盒機碼驗證機制，就無法進行影音收視行為，足見該 App 與硬體應係綁定，如圖 45。顯見該 App 如果未經過實體機上盒機碼驗證機制，將無法進行影音收視行為，可證明該 App 與硬體存在綁定關係。

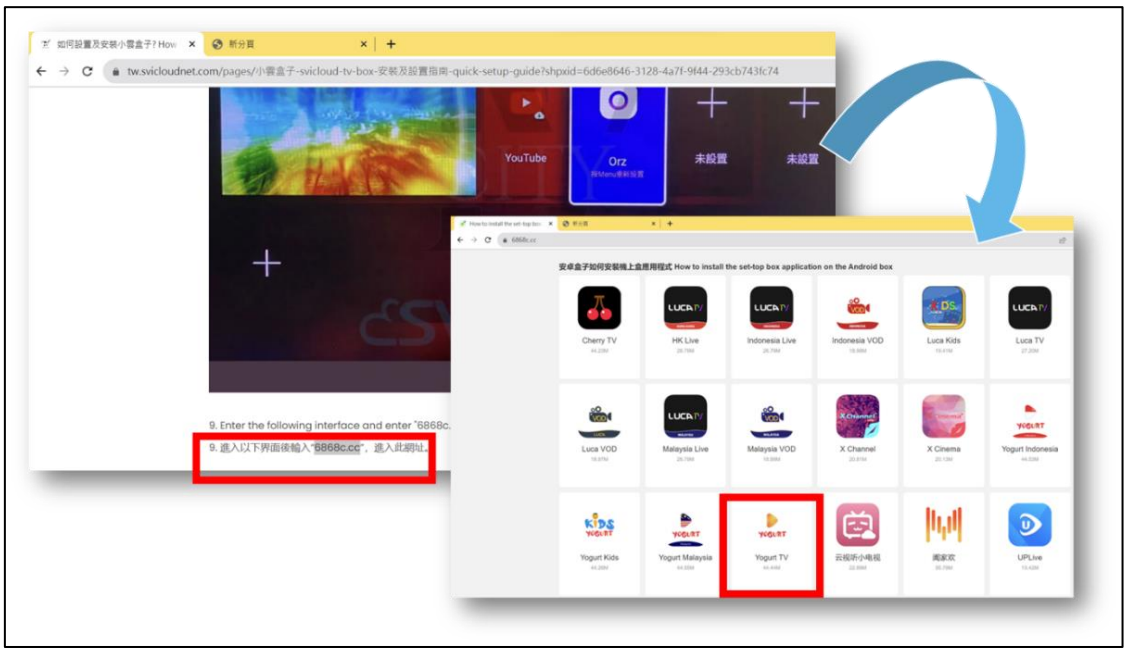

圖 44：下載 B 品牌機上盒專屬應用程式

資料來源：本研究整理

圖 45：使用虛擬機無法執行

資料來源：本研究整理

（三）C 品牌機上盒使用之特定 App 放入虛擬機檢測

將下載之 C 品牌機上盒之專屬 APK（圖 46）安裝於安卓虛擬機（LDPlayer 或 Vmware），發現無法開啟 APK 程式，並顯示認證失敗，如圖 47。顯見該 App 如果未經過實體機上盒機碼驗證機制，將無法進行影音收視行為，可證明該 App 與硬體存在綁定關係。

圖 46：下載 C 品牌機上盒專屬應用程式

資料來源：本研究整理

圖 47：使用虛擬機無法執行

資料來源：本研究整理

第六章 OTT TV 機上盒監理技術之作業流程、方法與所需軟硬體

第一節 OTT TV 機上盒監理技術之作業流程及方法

OTT TV 機上盒係透過取得 m3u8 檔，獲得節目索引目錄與來源位置後，根據使用者觀覽之節目抓取非法來源之影片，因此以下列作業流程及方法進行技術監理：

一、 建立測試布局

於測試主機中安裝必要之測試軟體，如 Wireshark、Burp Suite 後，建構 OTT TV 機上盒測試布局。將測試主機與測試用路由器進行連接，並將受測裝置與測試用路由器進行連線，並設定代理伺服器，確認 Wireshark 以及 Burp Suite 等軟體能擷取受測裝置之封包資訊，如圖 48、圖 49。兩種不同布局在於對於待測物是否透過有線網路連接測試用路由器，對於測試結果並無不同，僅提供本研究案不同測試布局之參考。

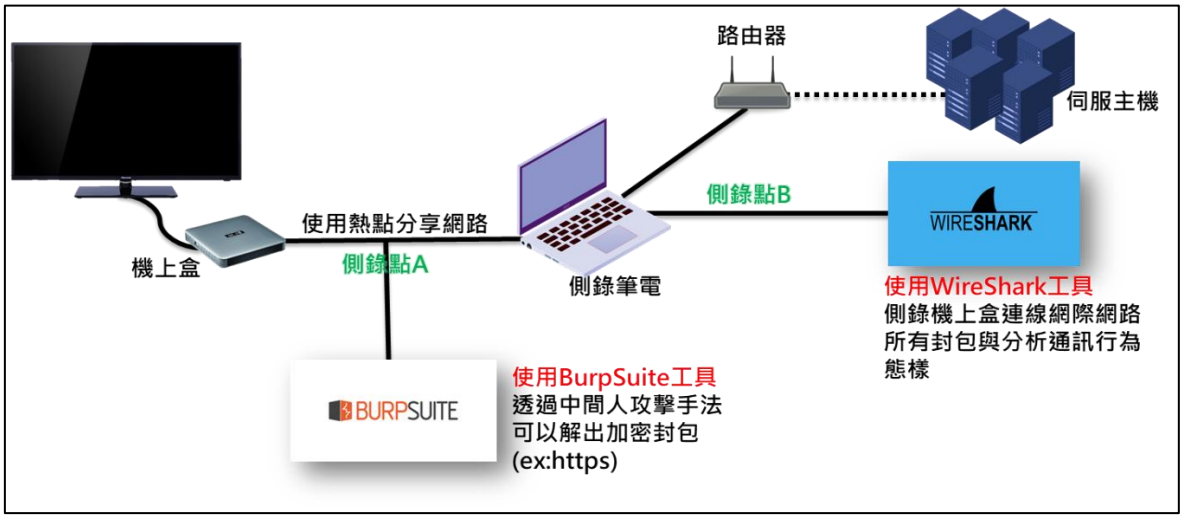

圖 48：測試布局 1

資料來源：本研究整理

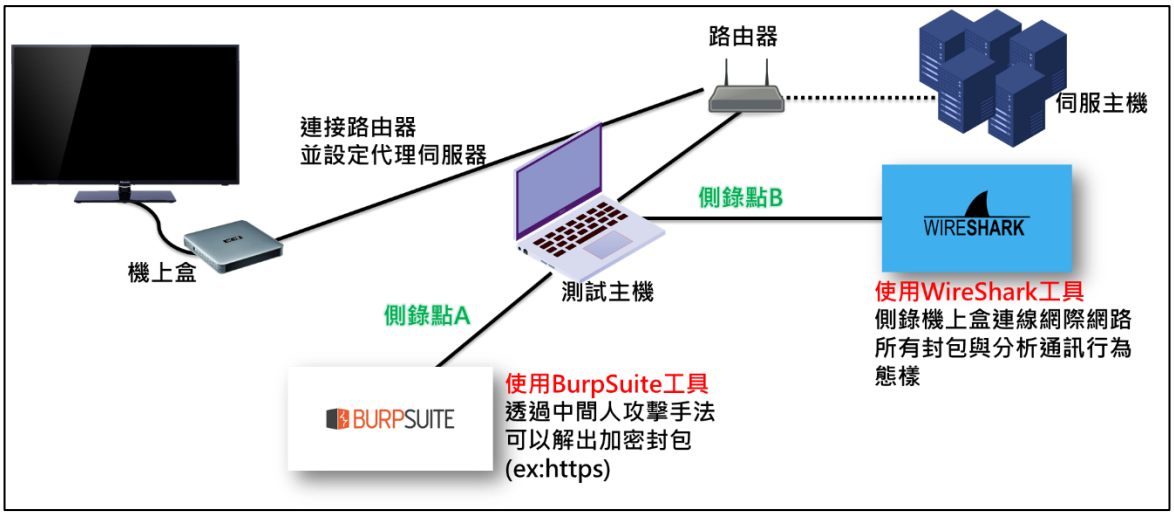

圖 49：測試布局 2

資料來源：本研究整理

二、 確認測試樣品是否預載應用程式

開啟測試樣品電源，進入主選單，並檢視其系統是否預載相關盜版影視應用程式。

三、 設定測試樣品之系統代理伺服器

如第一步驟，確定好測試布局時，應建立代理伺服器之主機環境，在此步驟中，設定測試樣品之系統代理伺服器之 IP 地址指向測試主機之 IP 地址。

四、 下載影視應用程式

由於純淨版之測試樣品並無預載盜版影視應用程式，測試人員應依據測試樣品提供之操作指示或是自行上網搜尋，透過瀏覽器開啟應用程式下載網頁，並下載影視應用程式。此時可以記錄下載地址之服務器位址。

五、 使用動靜態掃描工具分析應用程式

下載完成後，使用 AppExtractor 取得完整之應用程式 APK，便可以使用 MobSF 動靜態掃描工具分析此應用程式。

六、 透過 Wireshark 分析應用程式與伺服器協定

測試樣品連網時，機上盒所對外發送之網路封包都應經過測試主機之網路介面卡，因此我們可以利用 Wireshark 來監看網路介面卡之封包，並透過來源 IP 過濾出來自機上盒之網路封包。藉此分析封包傳輸內容，訊號傳遞方式、協定，來源與目標 IP 等，以 Wireshark 分析測試樣品與遠端伺服器之封包與協定，如圖 50 所示。

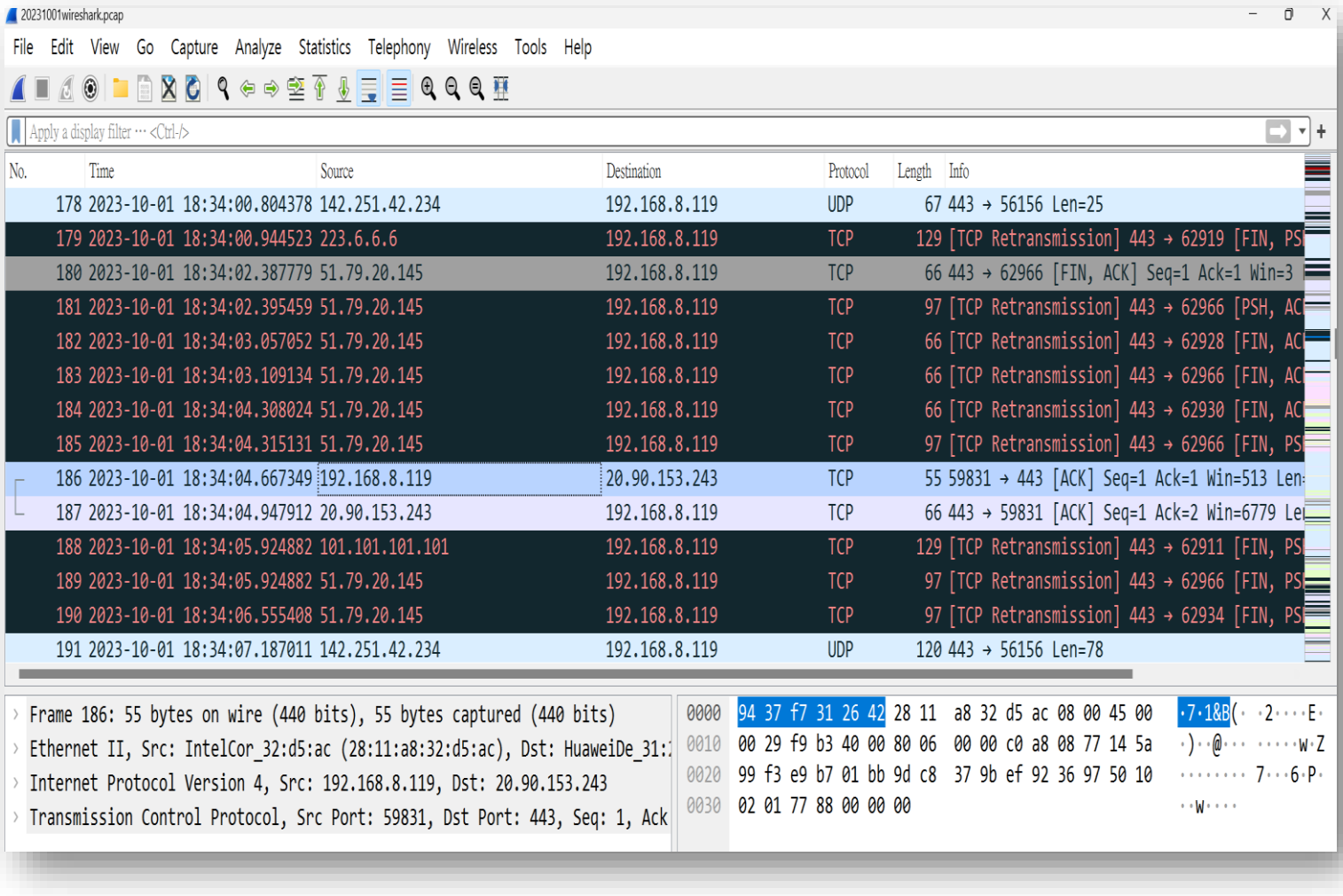

圖 50：Wireshark 攔截封包內容

資料來源：本研究整理

七、 若加密，使用 Burp Suite 代理伺服器並安裝憑證

由於測試樣品與遠端伺服器之通訊協定可能採用 HTTPS 加密通道，使用 Wireshark 無法解析出 HTTPS 之加密內容。透過設定 Burp Suite 作為 TLS（Transport Layer Security）代理伺服器，如圖 51 所示安裝憑證。

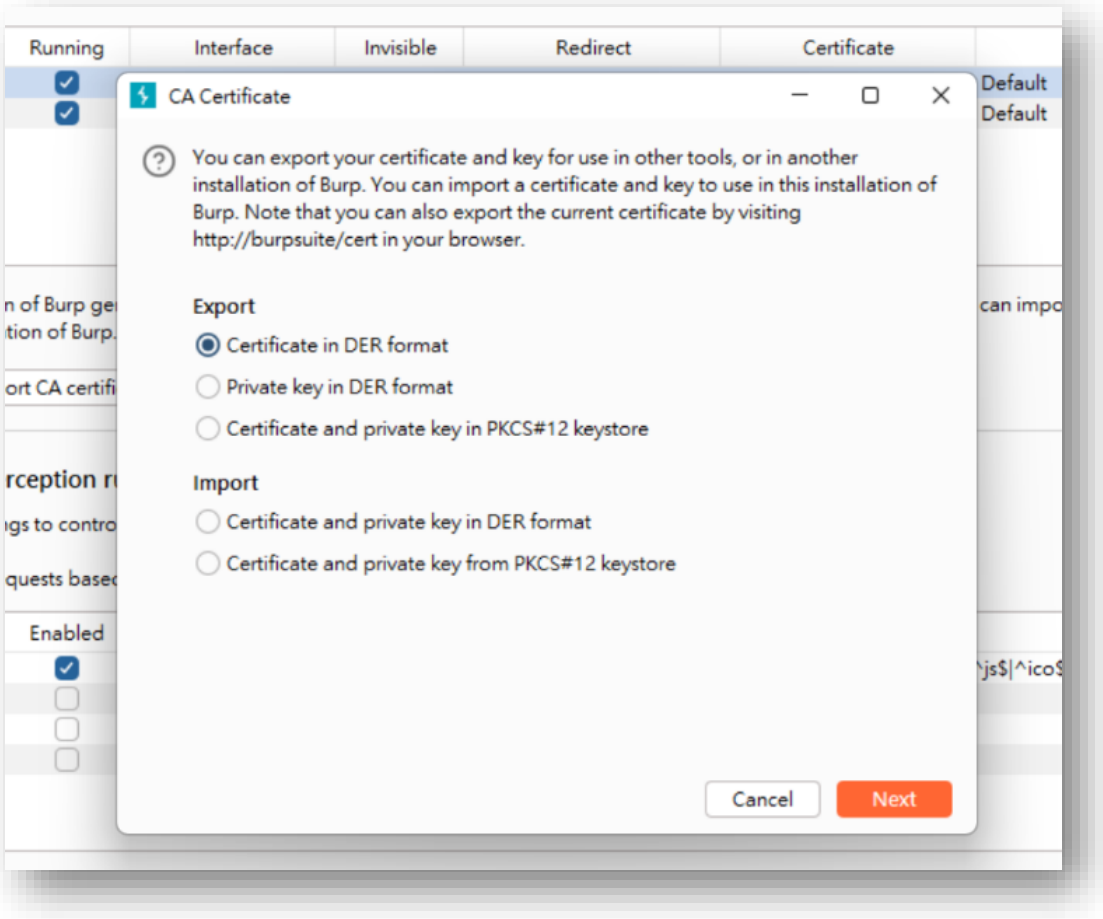

圖 51：Burp Suite 安裝憑證

資料來源：本研究整理

八、 使用 Burp Suite 分析應用程式與伺服器之間之通訊內容

在完成 Burp Suite 設定以及安裝憑證後，便可以成功解析出 HTTPS 加密內容，如圖 52 所示。

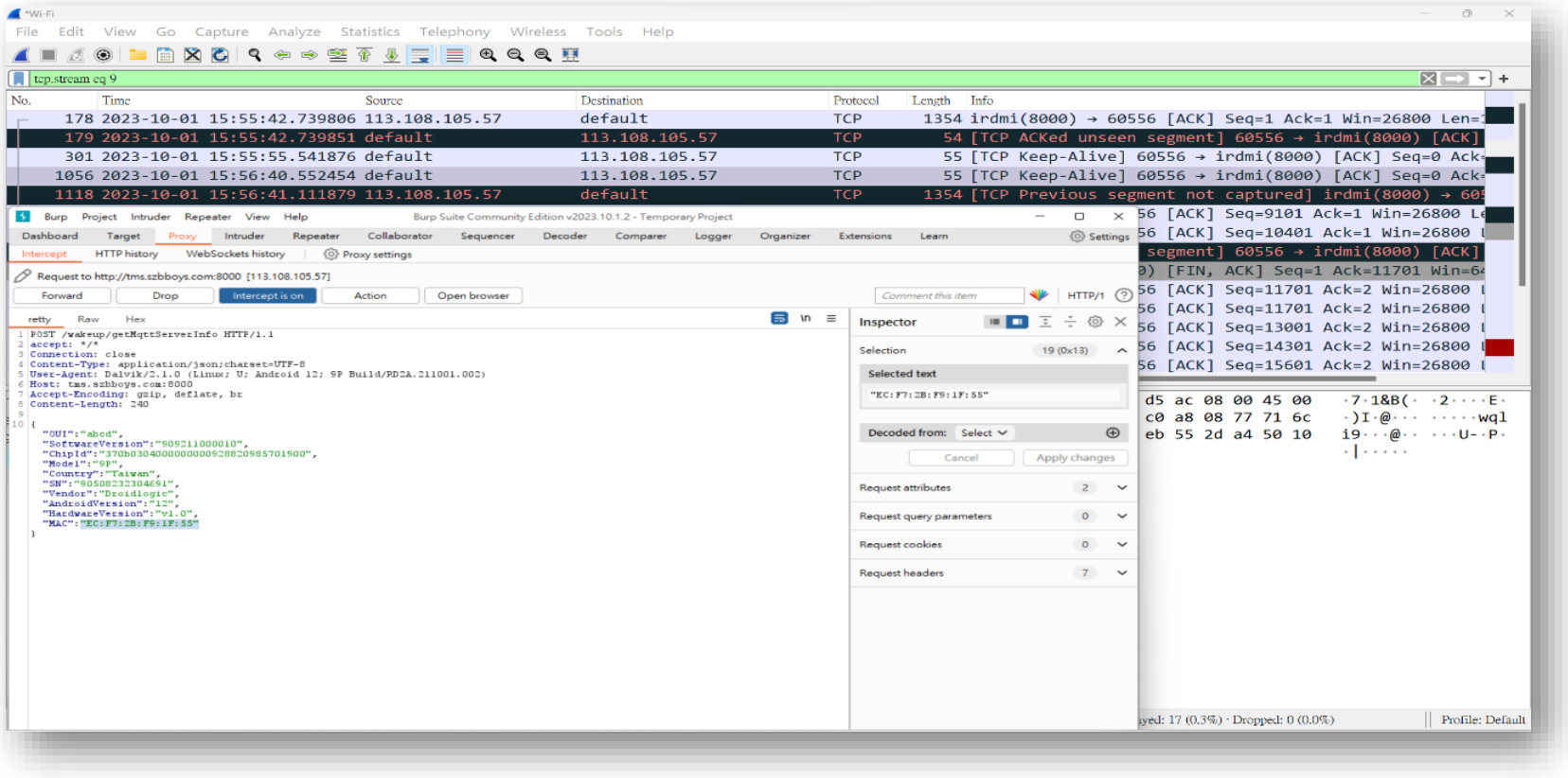

圖 52：Burp Suite 解析 HTTPS 請求資訊

資料來源：本研究整理

九、 檢查是否存在裝置綁定驗證之請求與回覆

在初次啟動測試樣品時，觀察是否存在可能與遠端服務驗證裝置綁定之請求。如圖 53 所示，測試樣品將硬體相關資訊，例如：硬體序號與網卡編號作為裝置綁定之依據，向遠端服務要求認證。

```
POST /wakeup/getAcsServerInfo HTTP/1.1
accept: */*
Connection: close
Content-Type: application/json;charset=UTF-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 12; 9P Build/RD2A.211001.002)
Host: tms.szbboys.com:8000
Accept-Encoding: gzip, deflate, br
Content-Length: 240

{
  "OUI":"abcd",
  "SoftwareVersion":"909211000010",
  "ChipId":"370b030400000000092882098570l900",
  "Model":"9P",
  "Country":"Taiwan",
  "SN":"905082323046 91",
  "Vendor":"Droidlogic",
  "AndroidVersion":"12",
  "HardwareVersion":"v1.0",
  "MAC":"EC:F7:2B:F9:1F:55"
}
```

圖 53：裝置綁定之請求

資料來源：本研究整理

十、 確認裝置綁定使用之硬體資訊是否與硬體本身相符

檢查裝置綁定之網卡編號，是否與硬體本身之網卡編號相符合。如圖 54 所示，其向遠端服務之請求中的網卡編號確實與測試樣品顯示出的網卡編號相符合。

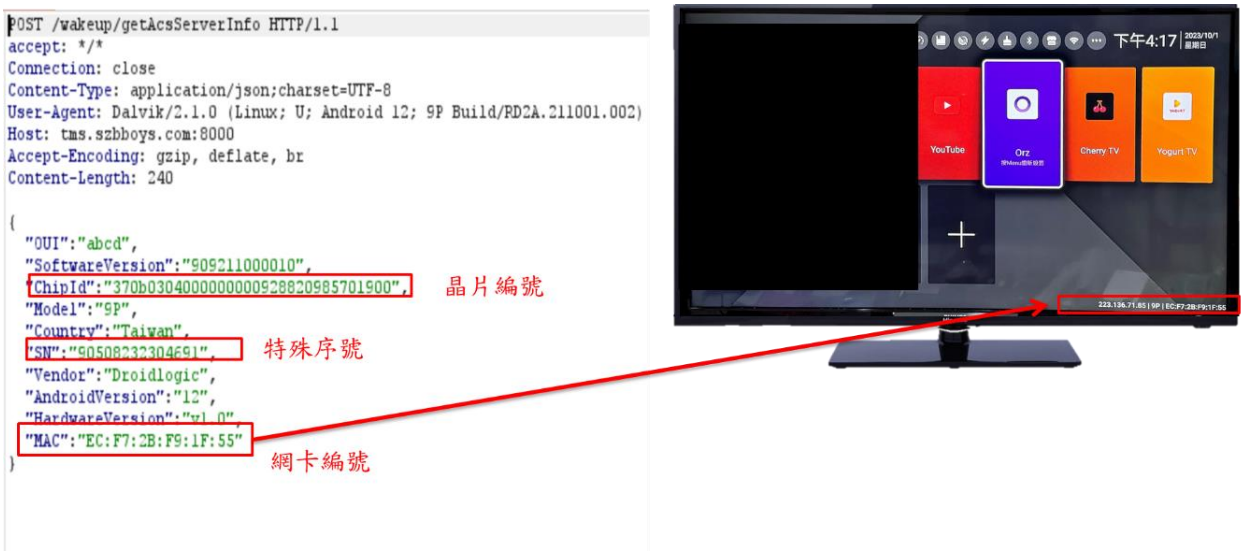

圖 54：裝置綁定驗證資訊與實體主機相符

資料來源：本研究整理

十一、 證明 m3u8 檔之傳輸

經攔截封包後，證明在 App 播放節目過程中，可直接看見 m3u8 檔之傳輸，分析該檔案內容後，可發現.ts 索引檔，並可直接連線至 CDN 快取發現盜版節目畫面，進而溯源同時證明非法盜取影音之過程（圖 55）。

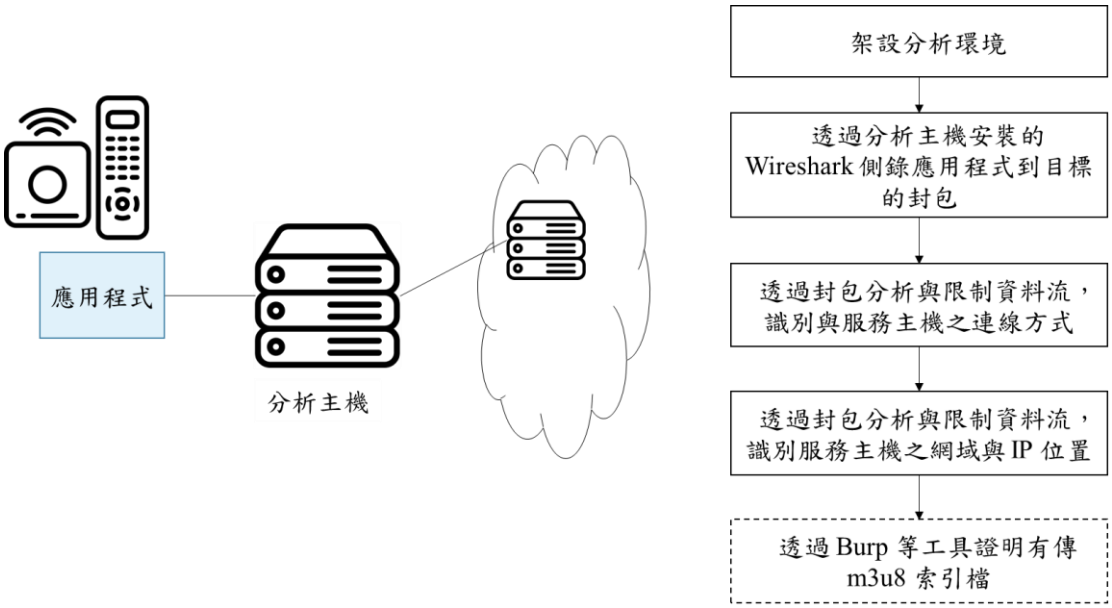

圖 55：OTT TV 機上盒監理技術之作業流程
資料來源：本研究整理

第二節　OTT TV 機上盒監理流程

一、 發現盜版與確認

若發現 OTT TV 機上盒有盜版之疑慮，需確認其合法性與訊號來源，並啟動 OTT TV 機上盒之檢測調查程序。

二、 調查機上盒與瀏覽盜版影音程式之關聯性

針對機上盒與瀏覽盜版影音程式之關聯性，進行下列分析：

（一）檢測機上盒與侵權影音程式之綁定行為

透過檢測 OTT TV 機上盒在開機與開啟 App 過程中是否讀取、認證 OTT 機上盒之 MAC 碼、網卡、ID 等資訊，判斷機上盒與侵權影音程式之綁定行為。

（二）辨識侵權影音的源頭與傳送方式

在 OTT TV 機上盒上使用侵權影音程式，並對封包進行側錄與分析，觀察其 M3U8 檔、.ts 檔之來源、存放 CDN 位置，再針對影片之來源進行溯源，並釐清訊號之傳送方式、途徑，追查不法。

三、 後續監理方法

（一）對機上盒進行禁售

目前法規尚不允許直接禁售，建議可於《著作權法》第 87 條第 1 項第 8 款增訂相關裝置綁定之條文，針對純淨版之機上盒，即便是預設並無應用程式，在使用者下載特定應用程式後，有裝置綁定等機制，可認定純淨版機上盒為盜版影視應用程式之載體。並針對《著作權法》第 93 條，增加禁止販售或其他處罰條款，將能透過下載影視應用程式且有裝置綁定之機上盒視為違法並禁售。

（二）針對盜版影音進行封阻或下架

針對 OTT TV 盜版影音之來源位址、網域進行適當之封阻或下架，避免未經授權之訊號來源持續侵害著作權，將損害與風險降至最低。

（三）對行為人進行處罰

針對盜取非法影音訊號來源並透過 OTT TV 機上盒播送之行為人，採取刑事之追訴程序，進行處罰。

（四）下架侵權影音程式

因非法訊號需透過 App 方能播放，故應一併下架應用程式，以杜絕不法，整理如圖 56。

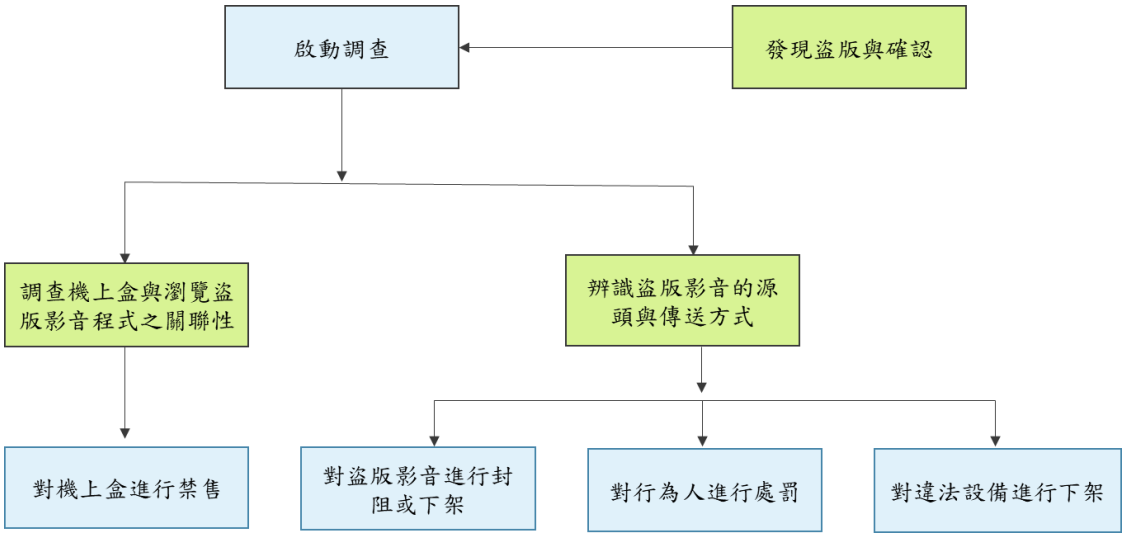

圖 56：OTT TV 機上盒監理技術之方法流程圖

資料來源：本研究整理

第三節　OTT TV 機上盒監理技術的軟硬體工具

一、 軟體工具

（一）Burp Suite

1. 軟體功能說明

Burp Suite 是一個用於測試網路應用程式安全性的圖形化工具，可透過加掛 proxy 分析網頁或用戶端 App 行為，可攔截封包讀取 App 傳輸內容，並分析非法訊號來源以及是否進行認證封包等運作機制。

2. 安裝流程

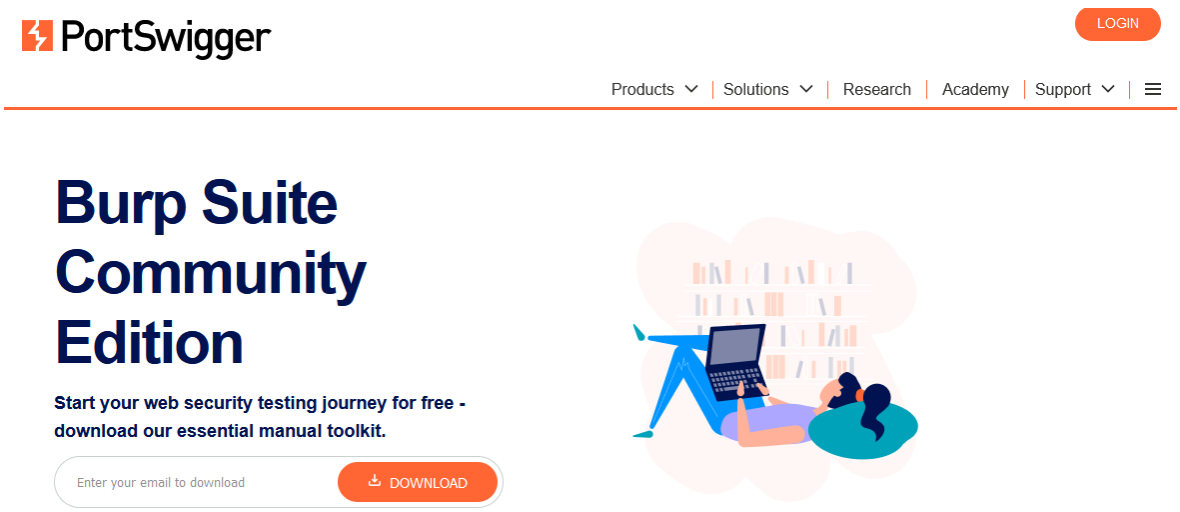

圖 57：Burp Suite 下載頁面

資料來源：本研究整理

前往 PostSwigger 網站（https://portswigger.net/customers），下載 Burp Suite Community Edition，如圖 57、圖 58。

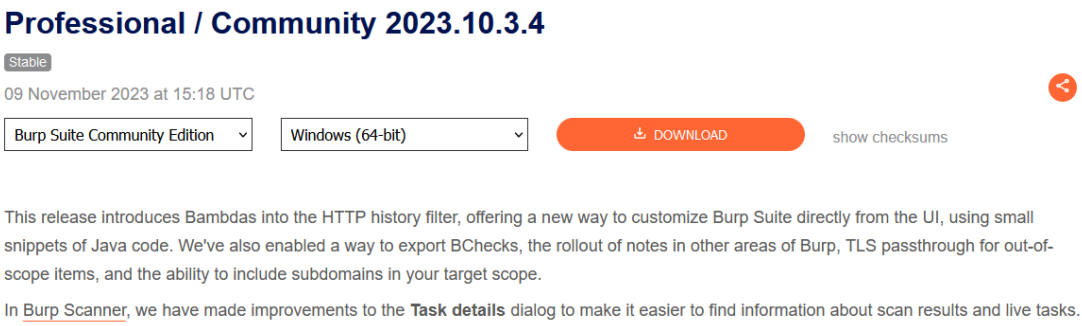

圖 58：選擇下載版本

資料來源：本研究整理

下載完成後，進行安裝，如圖 59、圖 60、圖 61。

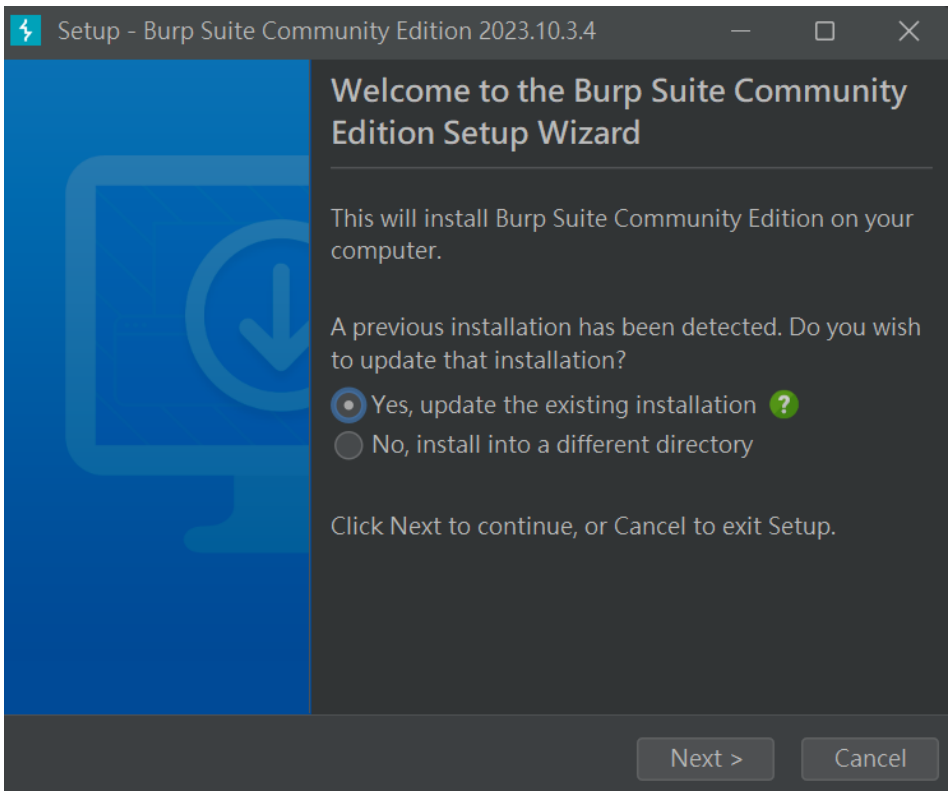

圖 59：開始安裝 Burp Suite

資料來源：本研究整理

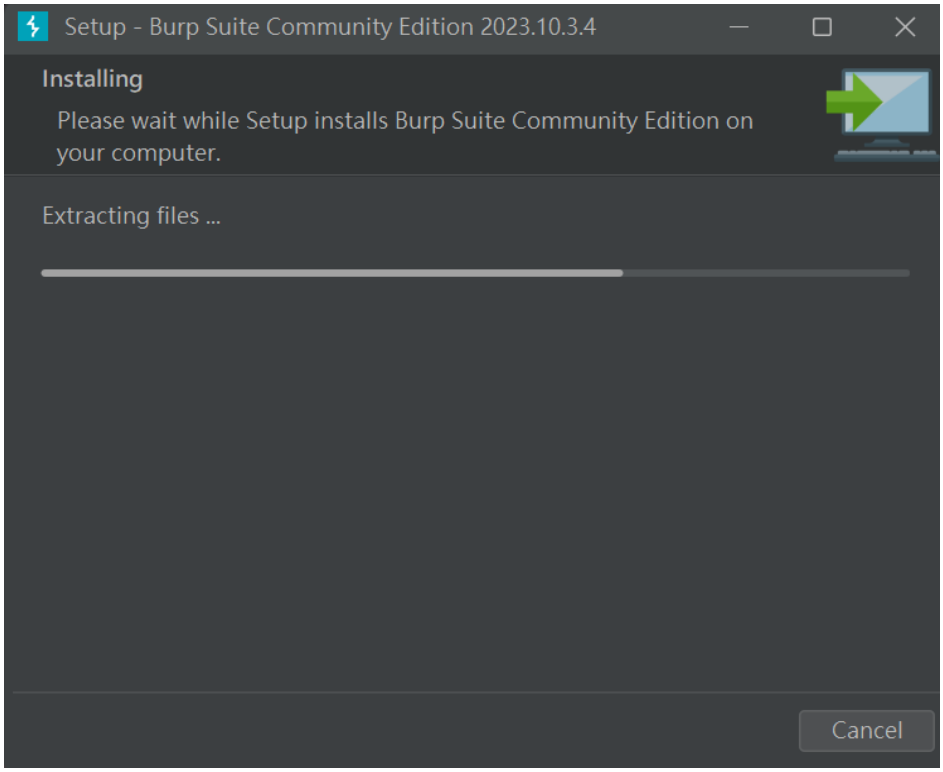

圖 60：安裝進行中

資料來源：本研究整理

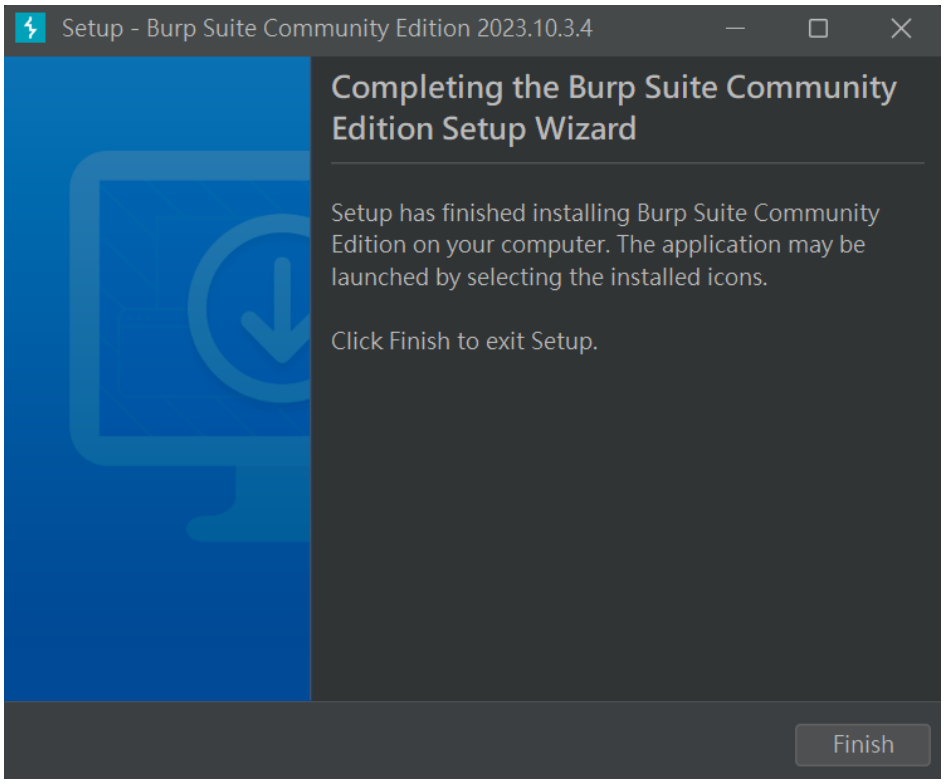

圖 61：Burp Suite 安裝完成

資料來源：本研究整理

創建或開啟專案，如圖 62、圖 63。

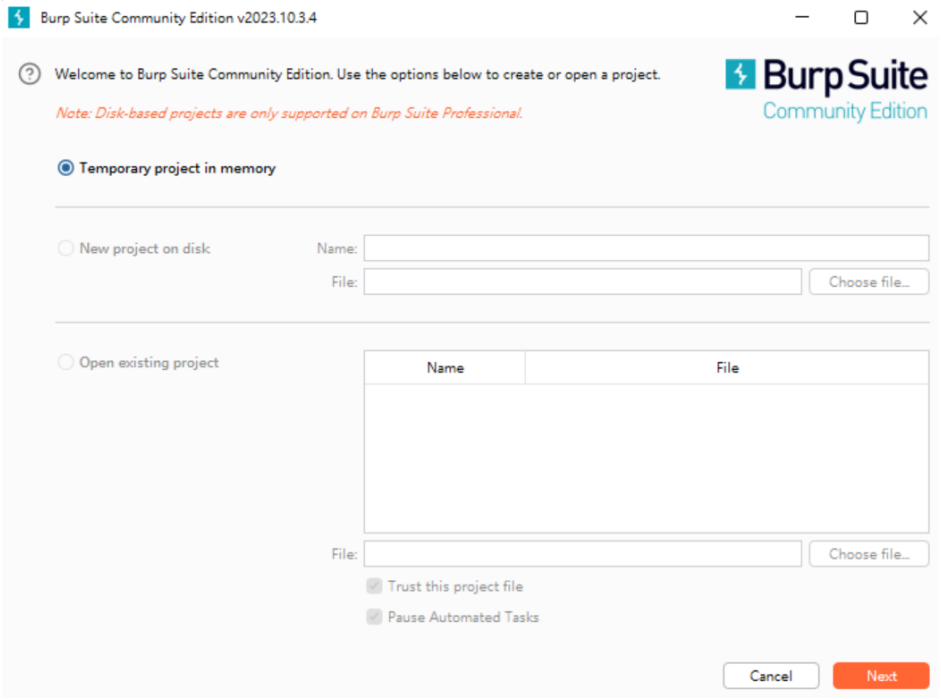

圖 62：開啟或建立新的專案

資料來源：本研究整理

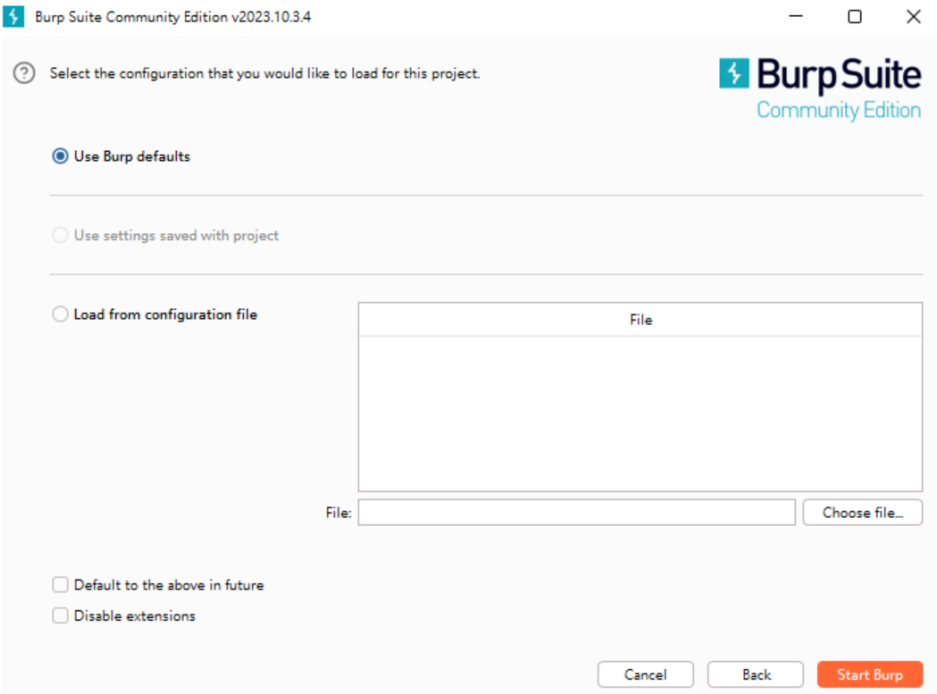

圖 63：選擇新專案設定

資料來源：本研究整理

Burp Suite 主要功能介面，如圖 64。

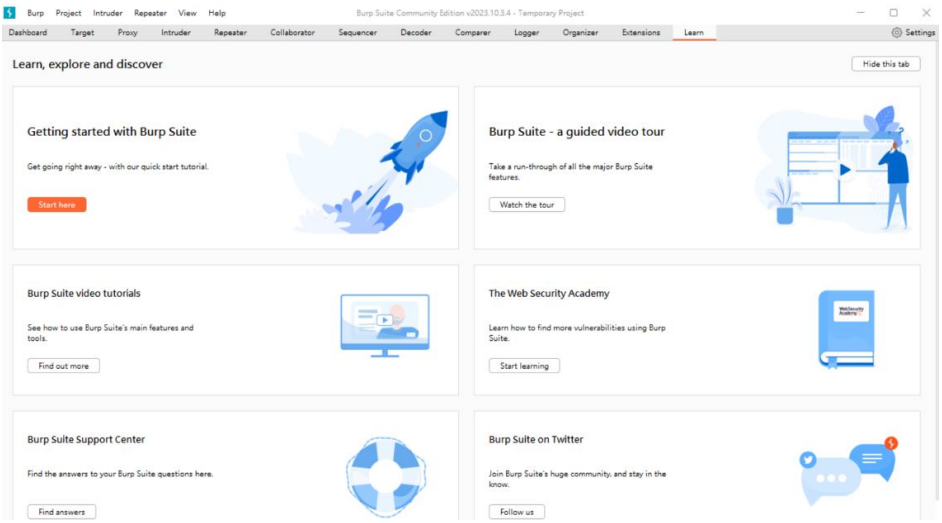

圖 64：Burp Suite 主要功能介面

資料來源：本研究整理

（二）APK Extractor

1. 軟體功能說明

APK Extractor 是一款 Android 的應用程序，其主要功能是從裝置中提取任何已安裝應用的 APK（Android Package Kit）文件。這款工具能夠有效地識別和複製系統或第三方應用的 APK 文件，並將它們儲存於用戶指定的存儲位置。其操作不需要裝置的 Root 權限，確保了廣泛的可用性和用戶安全。APK Extractor 特別適用於應用程序的備份、移植和安全分析。

2. 安裝流程

APK Extractor 可以由以下不同網站進行安裝，如表 16。

表 16：APK Extractor 安裝來源

Website	Description
http://apkpure.com/	APK Extractor 版本 4.21.08 可在 APKPure.com 上找到。此版本允許您從 Android 設備上提取已安裝的應用程序並將它們保存到 SD 卡上。
http://uptodown.com/	也可以從 Uptodown 下載 Android 的 APK Extractor。可以從手機上安裝的工具中提取 APK 文件。這裡提供的版本是 1.0.5，由 Kim Heeseok 開發。
http://digitaltrends.com/	另一個選擇是從 Digital Trends 下載 APK Extractor。

資料來源：本研究整理

（三）Mobile-Security-Framework（MobSF）

1. 軟體功能說明

Mobile-Security-Framework（MobSF）可以針對 App APK 進行解析，並分析原始碼（Code Analysis），該工具可於報告呈現 App 之功能、風險分析、檔案位置，以利分析人員針對 App 之組成進行不同的測試，強化針對 App 侵權行為之判斷。

2. 安裝流程

執行 docker 指令 docker pull opensecurity/mobile-security-framework-mobsf:latest，如圖 65。

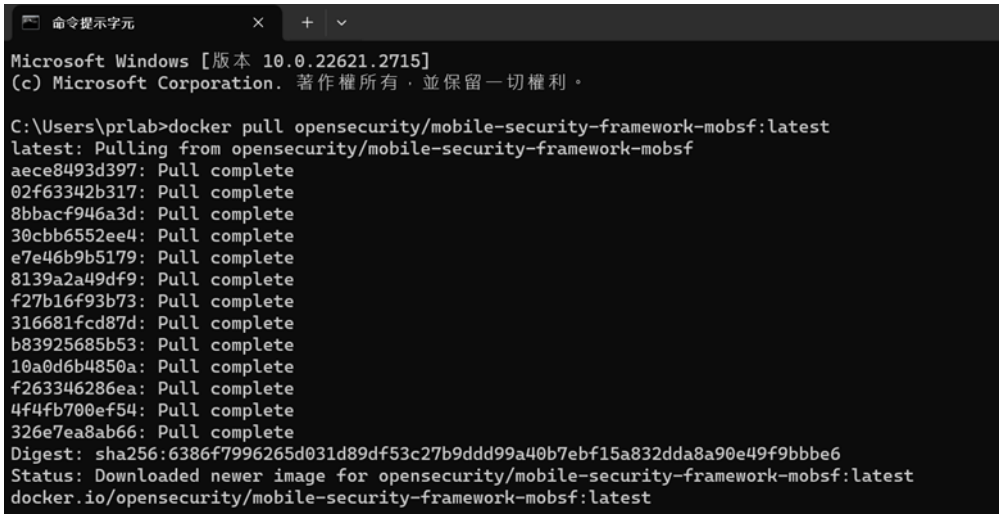

圖 65：下載容器映像檔

資料來源：本研究整理

執行 docker 指令 docker run -it --rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest，如圖 66。

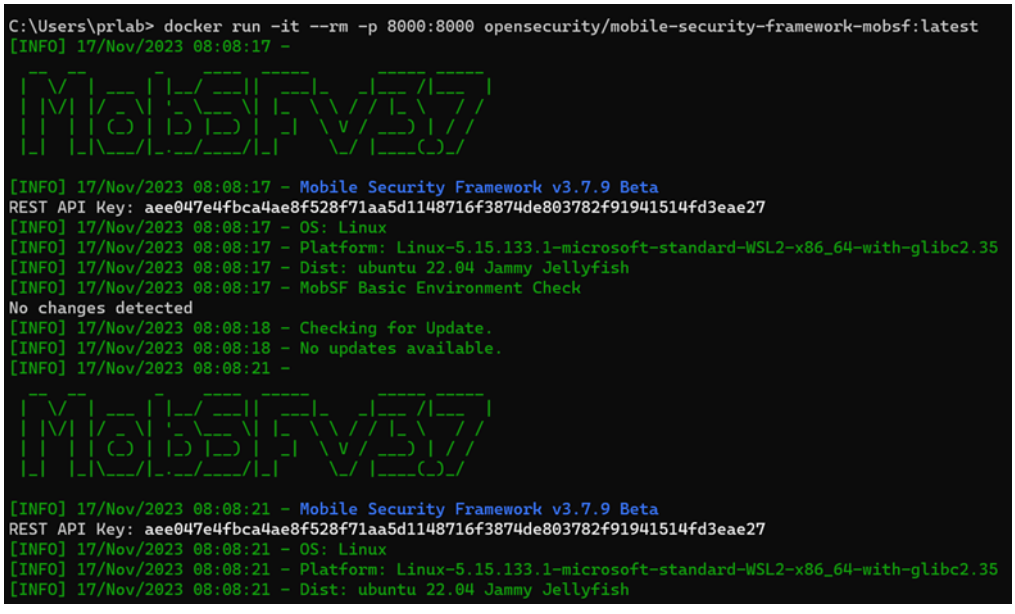

圖 66：執行容器映像檔

資料來源：本研究整理

前往 http://127.0.0.1:800 查看 MobSF 網站頁面，如圖 67。

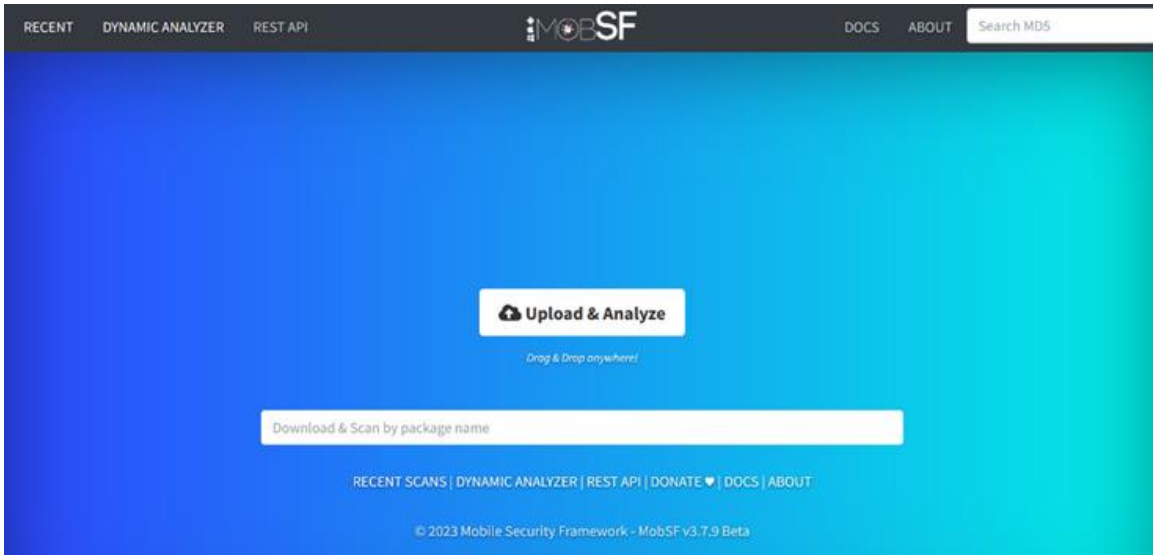

圖 67：首頁介面

資料來源：本研究整理

（四）Wireshark

1. 軟體功能說明

Wireshark 是款封包側錄工具，可以對 OTT TV 機上盒的運作和連線過程進行深入分析。此過程包括側錄和解析數據封包，以識別該設備的特定運作模式。透過 Wireshark，專業人員能夠檢測 App 啟動和使用過程中，是否存在與 OTT TV 機上盒型號、序號或 MAC 地址等獨特識別標誌相關聯的機制，從而更全面地分析設備的行為和數據傳輸特性。

2. 安裝流程

至 Wireshark 網站（https://www.wireshark.org/download.html）選擇欲下載的作業系統規格，如圖 68。

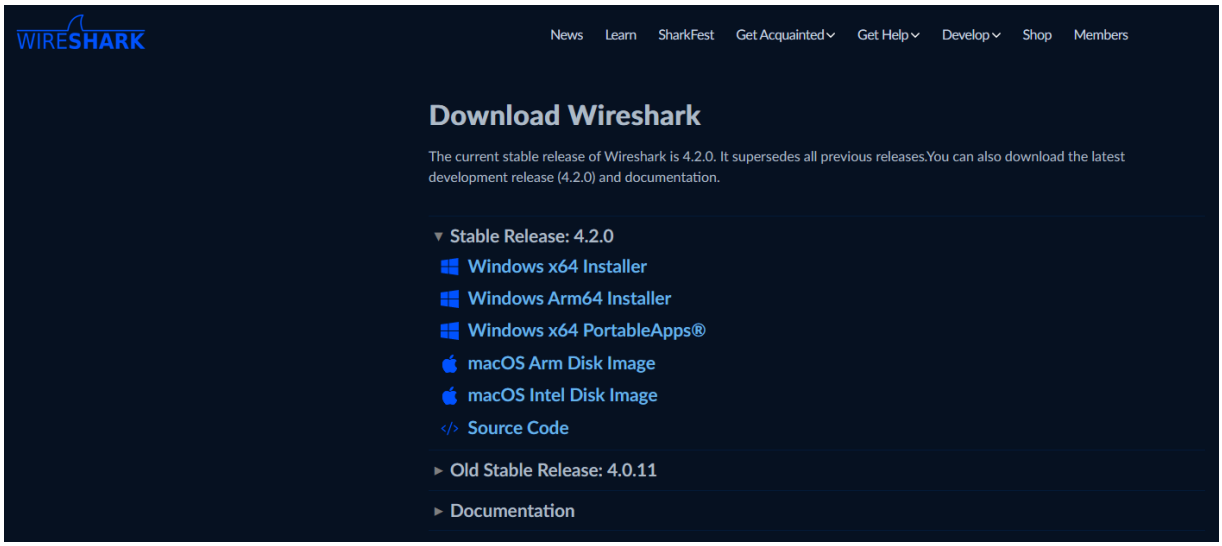

圖 68：Wireshark 下載頁面

資料來源：本研究整理

下載完畢後，即可開始安裝，如圖 69。

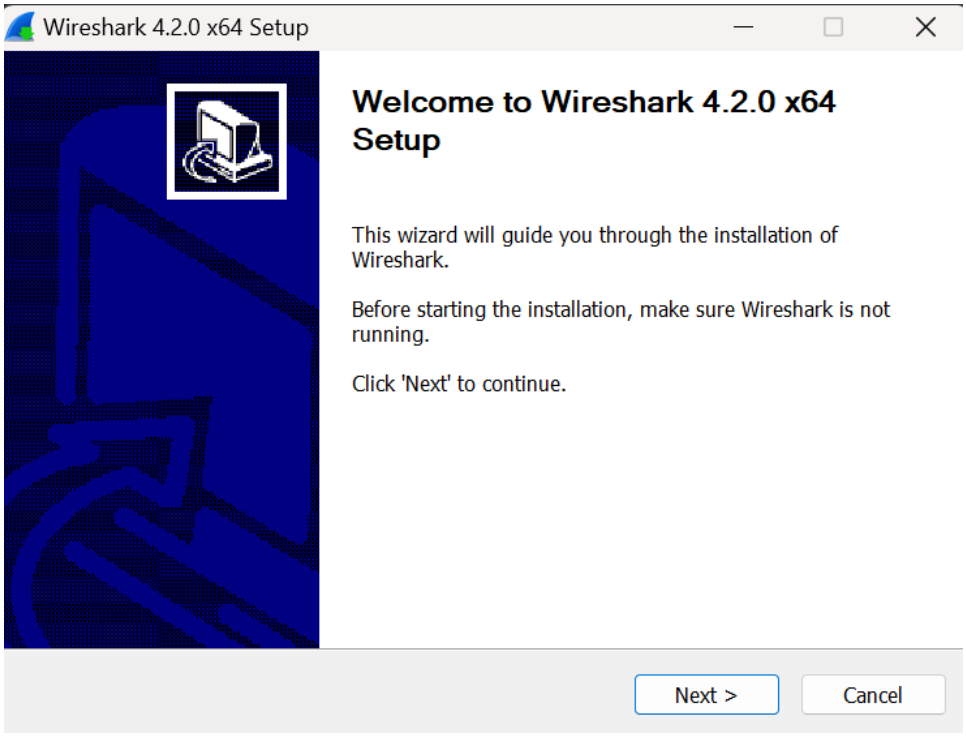

圖 69：Wireshark 安裝程序

資料來源：本研究整理

安裝完畢後，即可開啟 Wireshark 介面，進行封包側錄與分析，如圖 70。

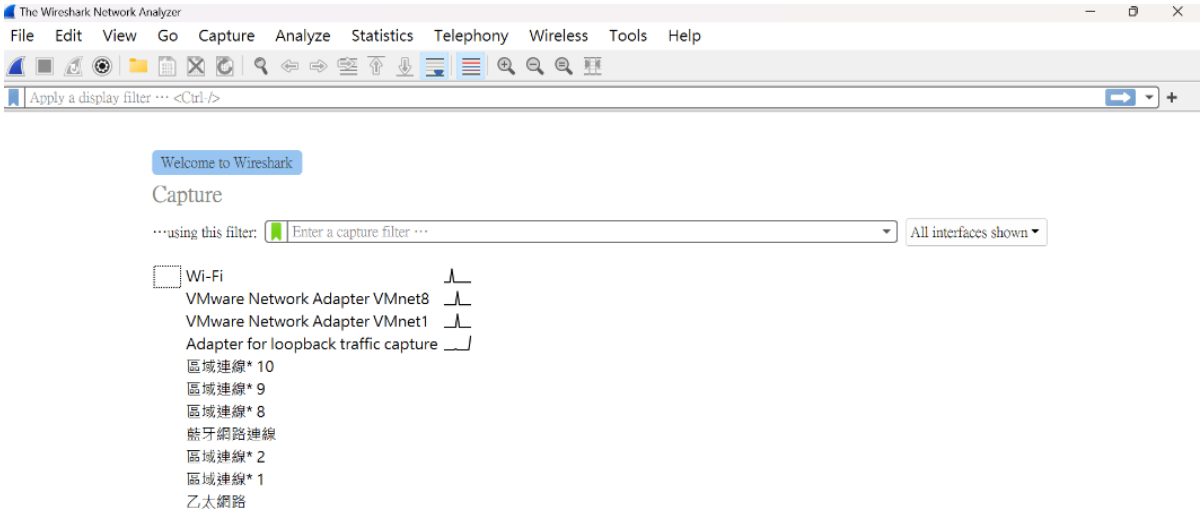

圖 70：Wireshark 介面

資料來源：本研究整理

二、 硬體工具

（一）測試用 OTT TV 機上盒

OTT TV 機上盒通常具備 RJ45 有線網路連接埠以及 WIFI 無線網路介面卡，且多為 Android 系統。本計畫分別使用了 A、B、C 牌的 OTT TV 機上盒，用於測試 OTT TV 機上盒實際運作情形，並進行 App 行為分析與檢測。

（二）Hub 或 Switch（具 Port Mirror 功能）

具備 Port Mirror 功能的網絡設備 Hub 或 Switch 是關鍵所在，可用於監控和分析網絡流量。Port Mirroring 允許將特定網路連接埠的流量鏡像轉移到機器上的另一網路連接埠。

在本研究計畫中，透過 Port Mirroring 可以收集流經該機上盒的網路封包。檢測人員能夠透過軟體來分析封包，瞭解網路流量的目的地與來源、傳輸協定等，以便進行檢測。

（三）鑑識工作站

鑑識工作站是專門設計用於分析和檢測 OTT TV 機上盒之工作站。其應透過標準化流程建立檢測環境，並針對不同待測物建立相關測試布局。在每次檢測時應確認鑑識工作站之測試環境與測試軟體的版本，並依測試流程進行測試，確保測試結果的一致性。

（四）虛擬機

用於安裝 APK 檔案，測試 OTT TV 專屬 App 是否可在其他安卓系統環境下正常安裝使用，若可以在其他安卓環境下正常安裝使用、觀覽節目，則該 App 與 OTT TV 機上盒本身可能不存在認證或綁定關係；相反地，若 APK 無法在虛擬機環境之系統下順利安裝、使用，僅在特定機上盒上能運作，即可證明機上盒為驗證資訊之關鍵所在。

第四節　具有公信力實驗室之必要性

透過建立 OTT TV 機上盒檢測實驗室，建置鑑識認證實驗室框架，可確保檢測流程之完整性，建立檢測品質與技術之保證，作為檢測 OTT TV 機上盒之標準實驗室環境。藉由實驗室之建立，評估並確保實驗室能夠提供符合特定測試和校準要求之準確與可靠結果。具體明列測試項目、測試方法及結果等來驗證機上盒之認證綁定行為及追溯節目訊號來源端。而因為目前已經有對機上盒之 ISO 17025 技術檢測實驗室，可進一步擴充範圍，加入對於機上盒是否綁定侵權 App 之標準檢測程序。具體的好處有以下：

一、 科學嚴謹性

在 ISO 17025 檢測實驗室標準的框架下，必須採用科學化的方法與程序，證明待測物是否符合檢測項目所訂定之規範。

二、 檢測一致性

透過標準化的程序，確保測試人員對測試樣品進行檢測的結果有其一致性，減少檢測人員的主觀偏見造成結果偏差，增加檢測結果的可信度。

三、 人才專業性

在 ISO 17025 檢測實驗室標準的框架下，測試人員必須滿足一定的要求，並通過能力試驗活動，確保測試人員之專業能力及檢測過程與結果滿足檢測實驗室之要求。

四、 獨立性

政府若訂立相關檢測標準與測試規範，則國內檢測實驗室可以申請檢測項目之增項，屆時法院或相關檢調單位可以委由不同實驗室進行測試，以確保檢測結果之獨立性，確保檢測結果用於作為證據之證據力與提升可信度。

五、 合規性

由於檢測實驗室出具檢測報告須滿足相關規範，例如每三年必須通過 TAF 重新驗證，確保檢測實驗室出具報告之檢測能力，令檢測結果能維持品質。

就目前制度上，不管是要提起訴訟，或是要封鎖 IP 與使用 DNS RPZ 去限制域名解析，都會需要經過審查。若有通過認證，則因為有上述的好處，更容易通過審查。

總結來說，建立一適用於 ISO 17025 檢測實驗室之檢測規範，能夠令受稽單位取得更客觀公正之結果，並讓其檢測報告之證據力更為充分，對於後續監理之措施與裁罰有更客觀之依據。

第七章 研究發現

第一節　研究成果分析

一、 綜整各國及區域組織之 OTT TV 機上盒之監理政策、法規

串流媒體以壓縮形式透過網路發送並立即播放內容，不需要保存到硬碟上，媒體是以連續的資訊流形式發送，因此用戶不必等待下載完畢，即可在資訊到達時播放、觀賞。其中，OTT TV 機上盒就是提供資訊串流分發的實體設備，在合法的用途中，消費者可受益於可靠安全的、全球可訪問的架構享受到影音娛樂服務。機上盒設備會發生違法問題在於犯罪分子使用相同技術非法傳播受著作權保護的影音內容。

因此，非法 OTT TV 機上盒會配置軟體，使消費者能夠從非法 OTT TV 機上盒透過串流傳輸視聽內容，此類軟體可透過多種方式（應用程式商店、促銷網站、員工協助等）獲取「專有」應用程式。以這種方式配置的非法 OTT TV 機上盒可以讓消費者以遠低於合法服務的價格輕鬆訪問訂閱電視、體育和電影，其費用可能包含設備的購買價格，又或者透過定期「訂閱」支付。

關於 OTT TV 機上盒之監管，目前主要可以分為下列三種模式：

（一）事前監理—歐盟

OTT TV 機上盒屬於《2014 年無線電設備指令》（RED）定義的無線電設備。該指令除了規範健康及安全要求、電磁相容性、無線電頻譜之有效使用、互操作性、獲得緊急服務以及無線電設備和軟體組合的合規性；也規範了隱私及個人資料保護和防止詐欺措施、以及網路安全。

依據《2014 年無線電設備指令》，機上盒應被設計成保護使用者之隱私及個人資料、免於詐欺、以及維護網路安全；且如果有使用者、無線電

設備或第三方要將軟體載入到該設備中，機上盒也必須設計為僅能在不影響無線電設備隨後符合適用的基本要求的情況下，才能將軟體載入到無線電設備中[296]。不符合這些基本要求之無線電設備，製造商、進口商與分銷商，都不應投放至市場。

（二）需要執照才可以販賣機上盒設備—新加坡、中國大陸

1. 新加坡

機上盒在新加坡屬於電信和無線電通信設備中的強化型簡易設備（Enhanced Simplified Equipment），而在新加坡出售供當地使用的電信和無線電通信設備必須在新加坡資通訊媒體發展局（Infocomm Media Development Authority，IMDA）進行設備註冊，設備在向 IMDA 註冊設備之前，須確保符合 IMDA 法規的相關標準/技術規格。另外，從事新加坡本地使用的電信設備進口和銷售的公司必須是持有 IMDA 有效電信經銷商許可證的設備供應商/經銷商[297]。故未取得許可證之業者不可任意銷售相關機上盒設備。

2. 中國大陸

非法 OTT TV 機上盒可以幫助民眾下載盜版或是盜錄的電影內容，讓民眾可在電視機等終端上免費觀看盜版影音，除對智慧財產權之侵害外，也涉及了大量未經官方審查與許可之境外節目的引入，因此引起大陸官方的注意。非法 OTT TV 機上盒之販賣被廣電總局強力禁止，按「關於依法嚴厲打擊非法電視網路接收設備違法犯罪活動的通知」販賣違法機上盒之行為屬於違反國家規定，從事生產、銷售非法電視網路接收設備（含軟體），以及為非法廣播電視接收軟體提供下載服務、為非法廣播電視節目頻道接收提供連結服務等營利性

[296] Directive 2014/53/EU, Sec. 3 (3)(i)
[297] Equipment Registration. (n.d.). IMDA. https://www.imda.gov.sg/regulations-and-licensing-listing/equipment-registration

活動，擾亂市場秩序，個人非法經營數額在五萬元以上或違法所得數額在一萬元以上，單位非法經營數額在五十萬元以上或違法所得數額在十萬元以上，按照非法經營罪追究刑事責任。

（三）處罰對於機上盒裝設破解合法串流技術軟體之行為—美國

按美國法典 17 USC 1201（a）（2）規定「（2）任何人皆不得製造、進口、允諾提供、提供或是運送任何以下規定之科技、產品、服務、裝置、組件或零件：（A）其主要設計或製造之使用目的係為規避本條所欲保護之科技保護措施；（B）其主要商業價值僅於為規避科技保護措施，以取得（接觸）本條所欲保護之著作；（C）其個人及其他相關人行銷之方式，係為使他人得以規避科技保護措施，以取得（接觸）本條所欲保護之著作為目的。」[298]。

二、 綜整各國及區域組織之監理技術

英國從內容源頭、伺服器直接動態封鎖；網路視聽平臺的連線監理技術，像是韓國每日頻繁自動封鎖非法 IP，阻斷串流網站的內容傳播；網路視聽平臺的端點監理技術，像是臺灣和新加坡，持續掃蕩非法的機上盒。

廣義的監理技術含括搭配政策、法規、國際合作以達到遏制侵權歪風之效果，像是《著作權法》明文處罰，甚至改採以詐欺洗錢刑罰，達到恫嚇效果；動用團體策略，如韓國公私協力與行政監理，或是中日跨國合作打擊策略；此外，阻斷市場金流收入也是重要策略，像是美國的封鎖禁制令也附加阻止任何第三方公司和盜版營運商有任何業務往來。整理各國及區域組織之監理模式，如圖 71。

[298] 17 USC 1201(a)(2).

圖 71：網路視聽平臺的監理模式

資料來源：本計畫整理

（一）《著作權法》明文處罰非法 OTT TV 機上盒模式[299]

各國皆可運用著作權法，對於透過非法 OTT TV 機上盒傳播未經授權之違法內容進行處罰，其中，新加坡透過警察積極查緝市場上的非法 OTT TV 機上盒併用靜態封網。

1. 模式內容

透過《著作權法》中針對非法 OTT TV 機上盒傳播未經授權之違法內容進行處罰，例如：我國《著作權法》第 87 條第 1 項第 8 款，以及新加坡模仿我國所新增的《著作權法》第 150 條，但這種模式必須併用封網才能阻斷非法串流，但是臺灣和新加坡都還是採取靜態封鎖，即僅針對網址封鎖，對於更改網址或 IP 後另外衍生的標的則無法後續處理。

2. 模式案例

臺灣：由新北地檢署向新北地院聲請網域扣押獲准，交由財團法人臺灣網路資訊中心（TWNIC）執行「聲請法院扣押域名並執行停止解析（DNS RPZ）」，將安◯盒子全面斷訊。之後，TWNIC 發展出 RPZ 1.0 治理規範。

新加坡：2019 年 High Court 做出第一個對非法盒子業者的刑事判決。該案主要係因被告認罪而定讞，若被告未認罪，依據相關規定未必可將被告定罪。而後新加坡修改《著作權法》，直接規範販賣盒子業者的責任。

3. 模式問題點

(1) 以臺灣封鎖的執行者是 TWNIC，依據國際 RPZ（MANDR）自律規範，有三種情況：

i. RPZ 1.0：阻斷要有法院判決和行政機關命令，所以耗時久。

[299] 新加坡 2021 年《著作權法》之修正重點及評析. (2022). 智慧財產權月刊.

ii. RPZ 1.5：阻斷以高等檢察署、法務部調查局、刑事警察局提出犯罪防治緊急申請，而被質疑欠缺法律依據。

iii. RPZ 2.0：網域名稱係有資安疑慮且影響資安重大者。

3 種情況之共同問題都是效用很差。因為（a）機上盒業者只要更換視聽來源網址便能繼續提供非法收視；(b)目前臺灣盜版停止解析只能處理「.tw」結尾的網址，實務上很多是「.com」網站（位於海外）無法解決；(c) 靜態封網的缺點需要靠動態封網解決。

(2) App 綁定盒子案[300]，臺灣判決中的陳○杰先生案例，陳先生是不知情經銷商，不法集團利用經銷商販售機上盒，然後以 YouTube 視訊內容進行隔空教學，指導消費者如何下載違法 App 觀看節目。我國現行《著作權法》規定無法解決利用無知經銷商侵權情況。

（二）封網技術模式

各國採用不同的動態封網技術：動態封鎖、變更目標 IP 或 URL、採取禁用盜版網站域名、在網站首頁顯示禁用訊息、阻止任何第三方跟盜版商有業務往來、自動檢測以驗證新版本和替代網站。

1. 英國的模式內容[301]

動態封鎖、變更目標 IP 或 URL：(1) 現場封鎖命令，僅在直播英超比賽錄影時生效；(2) 允許在必要時更新目標網站的 IP 地址或 URL；(3) 指令只持續很短的時間，只維持英超賽季的結束；(4) 當違法 IP 地址被阻止存取，每週會向 ISP 傳送通知。

封鎖技術：(1) 影片控制技術：在英超聯賽（FAPL）比賽中以極高準確度即時識別侵權串流，出現違法串流伺服器可立即通知；(2)

[300] 我國 110,民著訴,81,20230424,1 APP 綁定盒子案

[301] THE FOOTBALL ASSOCIATION PREMIER LEAGUE LIMITED. (2017). England and Wales High Court (Chancery Division) Decisions.

遮蔽解鎖技術：允許英超比賽期間自動遮蔽和解鎖 IP 地址，自動化遮蔽以保護相關權利，遮蔽或改變串流媒體營商使用的 IP 地址，這阻擋技術不必在比賽時間之外發生。

技術好處：即時封鎖非法直播、封鎖目標精準、處理時間短、影響性小。

2. 美國的模式內容[302]

封鎖禁制令：位於美國的網際網路服務提供商名單，他們不僅需要阻止盜版網站目前使用的域名，還需阻止他們將來可能使用的任何域名。

域名地址和任何新檢測到的網站，應以使用者無法連線和/或使用本網站的方式進行，並將由 ISP 的 DNS 伺服器轉移到原告運營和控制的登入頁面。

封鎖禁制令的附加功能：阻止任何第三方公司（包括 ISP、網站主機、CDN 提供商、DNS 提供商、域名公司、廣告服務、金融機構、支付服務等）在其當前域名或任何新域名上與網站展開任何業務。

技術好處：採取禁用盜版網站域名、在網站首頁顯示禁用訊息、阻止任何第三方跟盜版商有業務往來。

3. 韓國的模式內容[303]

透過增加頻率持續封鎖非法服務：伺服器放置在海外的韓國盜版網站 Noonoo TV 對於 OTT 產業造成的損害與日俱增，去年科學和資訊通訊技術部、韓國線上影片服務業、ISP 和韓國廣播協會（RAPA）共同合作，透過增加頻率持續阻止封鎖服務，導致 Noonoo TV 服務在 2023 年 4 月終止。此外，原始盜版網站是每天封鎖一次存取，近

[302] Andy Maxwell, May 2022. US Court Orders Every ISP in the United States to Block Illegal Streaming Sites.

[303] Baek byung-yeul. (2023, March 21). OTT Service Providers Negatively Impacted by Illegal Streaming Website. Business. https://www.koreatimes.co.kr/www/tech/2023/06/129_347439.html

期又出現的冒名網站，將採取強化封鎖措施，執行一日多次的干擾措施。

自動檢測以驗證新版本和替代網站：目前對非法網站的檢測和封鎖主要依靠人力資源的手動工作，為了克服這限制，韓國計劃開發 AI 能夠自動檢測以驗證新版本和冒名網站的技術。

技術好處：自動檢測以驗證新版本和替代網站可節省人力。

4. 三個國家的模式問題點

英國的問題點：動態封鎖、變更目標 IP 或 URL 的技術，可即時封鎖非法直播、封鎖目標精準、處理時間短、影響性小。動態如此有效，取決於先進的技術，如果欠缺這些技術，將無法採用此模式。

美國的問題點：採取禁用盜版網站域名、在網站首頁顯示禁用訊息、阻止任何第三方跟盜版商有業務往來，極有可能會發生關站內容不一定全部非法，或是可能無侵權內容卻被認違法的問題，會使 ISP 業者不清楚要如何執行。

韓國的問題點：ISP 封鎖很快被反擊，於 NooNoo TV 從賭博廣告中創造了大量收入，極大利益讓非法網站部署了數十個域名來規避封鎖措施。甚至藏匿伺服器放置在海外的地點，阻擋韓國以外存取者。

（三）跨國合作打擊模式

跨國共同合作，打擊犯罪跟關閉機房。例如：日本與中國合作，中國地方政府依據《著作權法》下的行政規定，執行查緝機房的行政罰。

1. 模式內容[304,305]

日本與中國大陸合作：因應六家日本動漫公司的要求，日本內容產品海外流通促進機構（CODA）代表，向中國相關部門投訴動畫盜

[304] Lim jeong-won. (2023, March 27). Korea to Bolster Efforts to Protect Korean Copyrights Overseas. Korea JoongAng Daily. https://koreajoongangdaily.joins.com/2023/03/27/culture/gamesWebtoons/Korea-Korea-Copyright-Protection-Agency-Kcopa/20230327132905320.html

[305] The Operator of "Manga BANK" Was Exposed. Administrative Penalties Have Now Been Confirmed in China. (2022, July 14). CODA. https://coda-cj.jp/en/news/179/

版網站 B9GOOD，是日本查處海外運營者跨國合作的首例。中國重慶市政府以民眾違反《資訊網路傳輸權保護條例》，對居住在重慶經營多個盜版網站，且並未經權利人許可傳輸動漫作品的男子處以罰款。

韓國跟泰國的合作：韓國政府機構和企業請求泰國政府提供政策支持和實際合作，以保護韓國內容。泰國政府承諾為此目的，在韓國機構和企業與泰國著作權保護當局之間建立密切的溝通管道。

2. 模式問題點

日本跟中國大陸共同合作，打擊犯罪跟關閉機房，落實方式就是在中國《著作權法》下加了一項行政的規定，讓政府可以去執行這個行政處罰。然而，這種措施對於臺灣是有困難的，因為需要中國的配合。

放置原創影音內容的機房未必只建置在中國，不法集團很大的可能性是將蒐集的影音資料放置世界各地機房，對於司法合作的難度跟時效性都是挑戰，國際合作是需要時間，以及合作國家的善意。

（四）公私協力與行政監理模式

韓國組成跨部門工作小組、以行政監理處理線上侵權。著作權主管部門補助成立公共機構雇用就業弱勢民眾進行居家線上侵權監控，依據監控結果，確定著作權人後，提供相關資訊給權利人，讓權利人提出相關救濟以執行停止解析侵權網址。

1. 模式內容[306]

成立跨部門工作小組、侵權防禦系統之監控計畫。韓國保護著作權工作小組執行措施：

[306] 同註 [304]

(1) 公私協力的保護著作權工作小組，透過立即措施、相關法規與科技改善、大眾教育等對韓國內容保護日臻完善。

(2) 將措施分為預防與侵權後行動，前者注重教育與監控，後者注重高效率行動與司法偵查活動。且不論措施內容、程序，以及各案件審查過程都以公開透明為原則。

(3) 韓國智財權保護局（KCOPA）[307]所建立的著作權侵權防禦系統。

2. 模式問題點

(1) KCOPA 為 100%政府補助的公立機構，但人民權利若未經法院判決，容易引起爭議，例如：KCOPA 所關站的內容不一定全部非法，或是可能無侵權內容卻被認違法定，當民眾要取用原本合法內容而未能取用，則有侵犯資訊自由的可能性。

(2) 跨政府機構、跨產業之計畫，動員各界耗時費力。

（五）詐欺洗錢刑罰模式

近年英國對於非法機上盒，多改以詐欺洗錢進行查緝、判決。這項重要變化也影響了歐盟其他國家。

1. 模式內容[308,309]

英國：5 名任職於非法串流運營商（Illegal streaming operators）在該國頂級足球聯賽因非法直播遭起訴，被法院判處總共超過 30 年的監禁。英超聯賽的法律團隊表示，他們現在將追查其他非法串流運營商。

荷蘭：荷蘭的財政資料和調查局（FIOD）取締了歐洲最大的盜版 IPTV 服務。該服務通過零售購買的非法串流媒體設備加上每月約

[307] Purpose of Establishment·History. (n.d.). KCOPA. https://www.kcopa.or.kr/eng/lay1/S120T428C430/contents.do

[308] Pinsent Masons,2017.英國案件突出了檢察官在供應改裝電視機頂盒時採取的不同路線

[309] Advanced Media Strategies LLC. (2023, May 23). Netherlands: Illegal Streaming Service Busted, Leads to Money Laundering Operation. Piracy Monitor. https://piracymonitor.org/netherlands-illegal-streaming-service-busted-leads-to-money-laundering-operation/

10 歐元的訂閱費，用戶可以觀看迪士尼、Netflix、Viaplay、Videoland、ESPN 以及 10,000 多個電視頻道的電影和系列電視節目。

2. 轉成詐欺洗錢刑罰以及模式問題點

2016 年開始，英國對於非法機上盒，多改以詐欺洗錢進行查緝、判決。這項重要變化也影響了歐盟其他國家。主要轉變理由是：由於在陪審團面前舉證違反著作權案件相當困難，但串謀詐欺罪相對簡單，陪審團更易接受。臺灣目前還未曾使用過這個模式。

三、 第一場與第二場座談會意見蒐集與研析

（一）第一場座談會意見蒐集與研析

依照專家回饋之意見，整理市場現況與困難點，如表 17。

表 17：第一場座談會專家回饋（市場現況與困難點）

主題	市場現況與困難點
非法視聽內容的盜竊、傳播、訂閱流程	◆ **OTT 影音侵權產業範圍：**這個議題牽涉到 OTT 影音的侵權問題，而不僅僅是機上盒的問題。機上盒僅是整個侵權產業中的末端終端裝置。（郭聯彬 法務組長） ◆ **正途是阻止非法公開傳輸：**MAC 號碼類似身分證號碼，用於識別設備。儘管設備能夠辨識，但設備本身是中性的。從非法機上盒的角度來看，針對這問題的切入似乎不太正當。正途應該是如何防止非法的公開傳輸。（郭聯彬 法務組長） ◆ **非法機上盒導致頻道慘重損失：**A 品牌機上盒近年銷售超過百萬台，對頻道造成嚴重損失。其內部頻道完全相同，且盒子使用行為與有線電視一致，包括遙控器和頻道排列。（陳依玫 秘書長）
《著作權法》明文處罰非法機上盒模式	◆ **司法訴訟程序冗長：**本公會七年內提出三十餘起訴訟案，司法訴訟流程冗長，期望加快停損程序。在 A 品牌盒子第三代和 A 品牌盒子第四代時，已在地方法院的初審取得成效，對於涉及機房的被告判處一年以上有期徒刑，禁止易科罰金。（陳依玫 秘書長） ◆ **機上盒鑑識報告規避違法：**A 品牌的製造商或業主在臺灣都有網頁回答問題，聲稱 A 品牌是合法的理由在於盒子是空

	的。法院上被告也提供鑑識報告，聲稱未開封且開封後連接網路後盒子內真的是空的。（陳依玫 秘書長） ◆ **機上盒本身是中性設備**： 機上盒應該是中立的裝置，雖然 A 品牌盒子盒子有一些綁定功能，但在監理制度下，應能實現完全不需要綁定。僅將焦點放在機上盒管理上無法完全解決問題，只能增加犯罪成本。（張友寧 主任檢察官） ◆ **中性設備難以處理著作權問題**：如果機上盒具有非侵權功能，它可以視為中性設備，因此從業者的角度難以處理著作權問題。（林宜柔 助理教授） ◆ **機上盒不綁定不預載不算違法**：針對機上盒，查緝時法源至關重要。若未預載，則不構成侵權的違法範圍，需要考慮改成綁定或專屬綁定。要先處理這部分的違法先決條件。（王翔正 副隊長） ◆ **機上盒採用網際網路連線**：衛星公會和頻道協會都是被害者。目前的機上盒使用網際網路 Bus，而有線電視使用 Cable 的 Bus，其訊號不透過網路傳輸，而是透過訊號傳遞。因此，在 OTT 方面，臺灣相對落後，而不法份子的工具卻比我們更先進。（莊明雄 代理科長） ◆ **切結書讓業者保證無違反智財權**：透過切結書的方式，業者可以提高確保其取得的內容未侵犯著作權或其他智慧財產權的機制。根據審驗辦法第 22 條第 3 項，如果切結書內容被違反，可先要求業者改正，若未改正則可考慮廢止。（楊采文 律師）
技術封網模式	◆ **機櫃機房會是個重點**：中華電信機房裡有很多機櫃，機櫃內容涵蓋各種業者。因此，機櫃機房實際上是一個重要的運作中心。（陳依玫 秘書長） ◆ **非法影音機房難尋**：要有效防止，應著重於傳輸源頭，採用封鎖網路的方法。基本上，要封鎖非法影音的來源，必須追蹤其所在的機房。然而，最大的挑戰在於是否能即時阻擋非法影音的傳播，若等到確認判斷，將無法及時制止。（郭聯彬 法務組長） ◆ **業者需提供證據以免被封鎖**：警方通知電信業者哪些是非法行為，若能協助封鎖，可達到相似效果。為避免誤封，可配

	合監管措施，要求業者在特定條件下提供無侵權證明。檢舉者指控侵權時，業者需提供證據以免被封鎖。（郭聯彬 法務組長） ◆ **封網技術成效有限：**目前在學界中，尚未找到有效封鎖 CNC server 的方法。封網技術成效有限，由於網路上的電腦和域名眾多，透過 IP 或域名的方式逐漸變得困難。（紀博文 副教授） ◆ **動態封網目前有法規問題：**目前在動態封網方面，主要問題存在於法規方面。透過刑事手段扣押的法律條文尚不足夠，因為無法以單一命令不斷變更扣押對象，而是以個案為基準。這造成法規上的困境，因此建議修法明確規範。另一主要問題是法院如何接受這樣的做法。（張友寧 主任檢察官） ◆ **審驗標準認定：**要快速取得證明，證明傳輸的內容是違法的，特別是在動態阻擋方面，關鍵在於是否符合審查標準，若未顯示違規字眼，即認定為不合規。（王翔正 副隊長）
跨國合作打擊模式	◆ **非法集團用跨國分工規避：**被告公司分割成多家，軟體也拆分成多家，未來要如何證明彼此之間的關係變得相當困難，尤其是在非法集團中，分工並跨足跨國，使得追查變得極具挑戰性。臺灣目前正面臨這樣的問題。（張友寧 主任檢察官）
公私協力與行政監理模式	◆ **NCC 可以把責任課予在業者：**NCC 是否有行政裁量權來針對合資的製造業者或 OTT 業者加強監理？將更大的監理權賦予這些業者，使其在使用者利用其平台或盒子進行非法或侵權行為時有更多行政裁量的權利，將責任歸給業者，要求他們進行糾正。（林宜柔 助理教授） ◆ **收費機制管理比較容易阻斷發展：**若以收費機制進行管理，可能更容易阻止其發展。至於如何扣押帳戶，這可能不在 NCC 的管理範疇內，而是由辦案人員處理金流帳戶。這些業者可能採取賣斷式的方式規避檢查，因為在訂閱前會有固定帳戶進行扣款，容易被追查。（張友寧 主任檢察官）
詐欺洗錢刑罰模式	◆ **用詐欺判罪國內不可行：**英國使用詐欺的方式，但在國內實施可能有困難。對詐欺罪的定義，不容易僅因違反某特定標準而判定為詐欺。（張友寧 主任檢察官）
非法機上盒有安全威脅	◆ **機上盒成為統戰的一環：**大家可能想到的是盜版的問題，但在實務中，我們看到當盜版機上盒啟動時，內容通常是中央

	電視台，指的是中國台北。這在某種程度上可以視為一種統戰手段，而機上盒則成為統戰的一環。（莊明雄 代理科長）
綁定啟動的非法 App 的機上盒	◆ **線上教學綁定非法 App：**A 品牌第六代後，現在轉向雲端服務，透過在 Google 購買廣告或合作夥伴，利用網紅開箱文指導觀眾或透過經銷商提供的方式，教導購買者如何從雲端下載 APK。然而，僅有 A 品牌盒子可執行此操作，因其本身即是犯罪工具，是打開盜版倉庫的鑰匙。目前更新版的 APK 已更名為 UPTV。（陳依玫 秘書長） ◆ **Root 技術控管機上盒**：從機上盒入手，無論是否有綁定，我們都能對盒子進行 root 或 JB，甚至直接刷入其他映像檔。（紀博文 副教授） ◆ **行政訴訟來處理舉證責任是困難：**機上盒監理的主要挑戰在於 App 和盒子之間的綁定關係。這一問題在民事或行政訴訟中都是核心議題，牽涉到舉證責任是否可轉換。然而，若以行政訴訟處理舉證責任，可能面臨極大困難，因為刑事訴訟架構中，以國家為唯一的舉證方。（張友寧 主任檢察官） ◆ **NCC 無法拒絕去幫機上盒背書：**NCC 為何無法拒絕背書機上盒呢？原因在於 NCC 必須接受人民的射頻設備審驗申請，無法拒絕此職責。（王翔正 副隊長） ◆ **以蒐集連結理由規避違法：**在法庭上的抗辯大多聲稱只是蒐集連結，沒有進行公開傳輸。他們主張未實施公開傳輸，因為公開傳輸涉及伺服器，而非他們的應用程式。（王翔正 副隊長）
修改《著作權法》、管制辦法等	◆ **利用射頻器材審議的行政作業疑慮：**研究案提出了巧妙的方法，透過射頻器材審議的行政程序，迂迴地使業者難以盈利，這想法相當有創意。然而，射頻器材的目的是管理通訊，主要處理無線電發射技術的規範和可能的電磁波強度對人健康的影響，而非管理智慧財產權。透過這種方法懲罰智慧財產權侵權並非正規途徑，可能會面臨未來的挑戰，也可能涉及違反法律保留原則的問題。（郭聯彬 法務組長）
市場回收機制	◆ **業者無利可圖：**利用宣告機上盒廢止確實可能導致業者無利可圖，但也會使合法經銷商因全額退費而猶豫出售，降低合法通路。結果可能導致地下市場的興起，使購買者難以退款。

	儘管這種方法可能對非法業者造成一定打擊，但是否能根治問題仍有疑慮。（郭聯彬 法務組長） ◆ **經銷商不願負責盜版問題：**經銷商繼續販售，因為他們宣稱已經得知 A 品牌通知各大通路商，每次被通知時，他們都表示 A 品牌告訴他們的盒子是空的、沒有不合法。（陳依玫 秘書長）

依照專家回饋之整理分類，建議如表 18。

表 18：第一場座談會專家回饋（建議）

主題	建議
修改《著作權法》、管制辦法等	◆ **修改射頻法：**在處理著作權時，無論是透過訴訟程序還是舉證，都是一條漫長的道路。或許可以考慮從射頻法方面進行修正。（林宜柔 助理教授） ◆ **修改《著作權法》、管制辦法：**第一個可能需要修訂《著作權法》。對於管制辦法和審驗辦法，我們需要確定相應的法源，以明確審查內容的認定標準。針對特定目標的違法行為，應根據相應的審查標準，包括母法和其他法規。在開機訊息方面可能有助於第二點。（王翔正 副隊長） ◆ **審驗辦法修法注意事項：**審驗辦法原旨在規範電信傳輸的安全，禁止電波干擾。將額外考量如資通安全、智慧財產權納入其中，可能引起違法和明確性的問題，需要進行進一步的評估。若採用切結書方式，即業者自願承諾，可能是一種解決方法。（楊采文 律師） ◆ **修法專屬綁定理由撤照：**撤照的理由仍需回歸至著作權部分，可能需要調整過程，例如加入專屬綁定的用語。在進行技術審驗時，同樣需要確定相應的法源。（王翔正 副隊長）
建立符合 ISO17025 檢驗實驗室	◆ **期望成立 ISO 測標準實驗室：**NCC 計劃借鑑 ISO 的概念，建立一個實驗室，針對機上盒制定檢測標準，類似物聯網的檢測標準。刑事局最近也在進行相關工作，包括如何擷取相關日誌。（莊明雄 代理科長） ◆ **支持成立 ISO 標準實驗室：**被告可提供鑑識報告，檢方自然也會呈上相對應的報告。因此，我支持建立實驗室的研究標準，這將使我們能夠在 App 與盒子綁定的相關性建立上，採取標準化措施，並生成標準化的鑑識報告。這樣的標準化

	作業將有助於在法庭上更容易說服法官，以取得更有利的結果。（張友寧 主任檢察官）
機上盒開機訊息	◆ **提醒民眾下載收視內容的風險性：**NCC 負責行政管控許可證的發放。此外，在開箱文的第一頁中，明確顯示 NCC 所授權的是射頻器材，符合安全標準，但對於所下載的任何收視內容，必須遵守《著作權法》。NCC 的公告應針對此類觀眾，提醒其存在相應的法律風險。（陳依玫 秘書長） ◆ **使用警語提醒違法使用的安全風險：**除了告知審定合格的字號外，我們是否能夠與政府其他部門合作，在法規中加入一些警語，授權禁止盒子使用盜版內容。至少應通知使用者這樣的行為存在風險，以提高他們的警覺。（張友寧 主任檢察官） ◆ **NCC 可公布撤照理由：**過去，NCC 通常因硬體性能未達標準或認證標示不合格而撤照。針對潛在的侵權內容，為了維護市場秩序，NCC 似乎在這方面的措施相對勉強，缺乏堅實的立足點。若畫面顯示無法連接 NCC 網站，則可清楚判定設備不符技術審驗標準，NCC 可向民眾宣告此設備已被撤照。（王翔正 副隊長）
市場回收機制	◆ **臺灣的回收體系涵蓋產品安全：**臺灣的回收體系主要涵蓋產品安全，例如商品檢驗法和公路法中的汽車召回措施，以及環保體系中的廢棄法。因此，在考慮基礎回收體系時，我們實際上需要深入考慮刑事、行政和民法層面。（楊采文 律師） ◆ **用消費關係的方式去做回收：**在行政程序中，我們建議考慮專案查緝，尤其是對販售未經審驗合格的 OTT TV 機上盒，是否可直接以沒收方式處理。行政方面，目前汽車召回體系為何選擇民法途徑，即透過消費者關係來實施回收，而非採用行政方式監督，或許是因為行政機關成本高，且環保署在廢棄處理上已著墨很多。（楊采文 律師） ◆ **製造商是最終的回收責任業者：**製造和經銷有明確的分工，審驗辦法規範的對象是申請人，通常為製造商或主要臺灣廠商。然而，退費機構的規範並未涵蓋到經銷商，使得回收計畫的主體仍然是申請人。申請人需要負責如何處理退費，這是回收計畫的一部分，也是最終的回收責任業者。（楊采文 律師）

座談會第一場之專家代表提出多面向綜合建議：

首先，在技術分析上，強調對盒子技術的深入研究，特別關注 MAC number，以增強對盒子犯罪工具性質的理解。其次，機房調查應更加嚴謹，特別針對盒子可能在境外機房中操作，以深入了解盜版行為的背後結構。在法庭上，強調技術論證，針對盒子特殊性質提供鑑識證據，有助於消除法官的疑慮。同時，透過教育觀眾，加強 NCC 公告中的盒子使用風險，提高觀眾對法律及資安風險的認識。此外，強調標準化許可發放流程，以迅速處理問題，確保合法盒子獲得許可並快速應對非法行為。密切與 NCC 合作、強化法務手段、加強行業合作和進行媒體宣傳，共同應對盜版問題。總體而言，這些建議針對法律、技術、合作和宣導等多方面，期望能有效解決或減緩相關問題。

（二）第二場座談會意見蒐集與研析

依照專家回饋之意見，整理市場現況與困難點，如表 19。

表 19：第二場座談會專家回饋（市場現況與困難點）

主題	市場現況與困難點
A 品牌盒子的收益來源	◆ **A 品牌盒子就是現金所在：**斷開 A 品牌盒子的財源是關鍵，目前 NCC 缺乏法源依據。從公務人員的行政作業規定來看，它主要檢驗射頻器材，而在處理著作權問題時，法律方面仍需進一步處理。（彭淑芬 秘書長） ◆ **營運商將頻道做成免費形式：**A 品牌盒子主要透過硬體銷售賺取收入，而後不收取其他訂閱費用。類似的合法操作已被許多運營商採用，後續線性頻道即將擴大成為免費提供是極有可能的。（盧信儒 資深經理） ◆ **A 品牌盒子結合廣告收益：**A 品牌盒子若規模擴大，可能會整合廣告、進行置入廣告，進而取得額外的資金，使得中斷其運作變得更加困難。（盧信儒 資深經理）
浮水印技術	◆ **政府補助浮水印機制：**若成本允許，可以考慮引入浮水印機制，用於偵測網路上傳遞的內容。然而，這需要相當大的投入成本，可能需要業者和政府的補助，或者進行相關討論方能實現。（盧信儒 資深經理）

	◆ **系統廠商浮水印技術**：我們先前在機上盒機房使用浮水印，但由於需要龐大的系統商才能處理，我們實際上並無法檢視浮水印。此外，我們也利用一些線上 App 軟體的授權碼來擷取 m3u8 檔案並進行下載。從法規角度來看，如果針對機上盒本身進行處理，可能會更為有效。（王翔正 副隊長）
憑證綁定技術難處	◆ **憑證綁定的技術有難度**：憑證綁定技術使中間人攻擊變得困難，因此我們難以攔截封包。然而，這可能導致成本效益的問題，因此在技術方面，我們需考慮尋找更快速的方法，因為 App 的修改速度相當迅速。（紀博文 副教授）
臺灣封網作法	◆ **停止解析網址**：我們採用了全球 39 個國家的做法，即所謂的「site blocking」。在台灣我們不能提封網，而是停止解析網址，即通知對方取下。（彭淑芬 秘書長）
機上盒認證註銷困境	◆ **切結書之法源依據**：NCC 要求機上盒業者簽署切結書，承諾不侵犯著作權。如果違反切結書，行政單位是否能有法源處理權，這是需要澄清的問題。（彭淑芬 秘書長） ◆ **認證註銷還可以申請**：A 品牌盒子曾多次被註銷 NCC 認證，卻仍能再次進行認證申請。為何不禁止其再次認證，特別是考慮到他的歷史記錄？此外，各種地下論壇提供了檢舉和利益相關信息的管道。（盧信儒 資深經理） ◆ **廠商黑名單的適用性**：將這家廠商列入黑名單是一種方法，但實際上他們可能只需更改名稱，就能迴避這項制裁。（林宜柔 助理教授） ◆ **下架機上盒依據**：《著作權法》80 條之一，轉到 88 條之一可不可以作為下架機上盒的依據，只把我用錄影機這種方式錄下來的東西，再傳輸來那後面傳輸的行為雖然是違法的，但他有沒有影響到權利保護措施，權利管理電子資訊，這個部分可能會有一些問題，如果沒有，實際上就不可能以這個條文的規定來處理。（張友寧 主任檢察官） ◆ **抽測手段查緝**：查緝的過程，這個是抽測的手段，可以單一路徑去抽測。在一般的《著作權法》案件上，民間權利人抽測的時候，確實是有這樣的做法，那基本上法院也都接受。違法蒐證，大部分都是針對國家違法蒐證，那如果說是這個民間，就是權利人他利用自己私人蒐證的手段。（張友寧 主任檢察官）

法律面狀況	◆ **司法程序緩慢**：處理智慧財產權侵害通常需要透過司法程序，但這可能過於緩慢。是否可以在法律設計中採用行政手段來更有效處理這些問題呢？（張友寧 主任檢察官） ◆ **《著作權法》84 條**：《著作權法》84 條的部分，雖然我不是民事的專家，但是我們一般法院，在解釋這一條，所謂的請求方式，其實是說請法院以裁判的方法，決定一個方式來避免侵害，那當然透過這個假處分方式，或者是假扣押的方式來進行。（張友寧 主任檢察官）

依照專家回饋之整理分類，建議如表 20。

表 20：第二場座談會專家回饋（建議）

主題	建議
審驗增加測項	◆ **審驗增加綁定測項**：審驗時，當廠商申請射頻機台合格證明時，加入一項測試，要求有一個實時的 Live 狀態。如果發現綁定了 App，則無法通過該測項。（彭淑芬 秘書長） ◆ **公正第三方審核**：App 發展迅速，如果要建立公正的第三方審核機制，需特別關注時效性。（紀博文 副教授）
虛擬機是否能執行檢測	◆ **採用虛擬機模擬器做為證據**：建議使用虛擬機的方式，在模擬器中下載 App，觀察其執行情況。由於無法執行的理由眾多，為確保法律上的證據足夠，App 在**虛擬機模擬器下**有時可執行有時不可執行足以作為對照確認有綁定違法行為，以避免非法業者狡辯。（紀博文 副教授） ◆ **模擬 A 品牌盒子和非 A 品牌盒子的環境**：透過模擬 A 品牌盒子與非 A 品牌盒子的環境，比較兩者的不同，以確保法院相信在 A 品牌盒子環境下可觀看，而在非 A 品牌盒子環境中則無法觀看。這種證明方法在確保環境相似的前提下是相對有效的。（張友寧 主任檢察官） ◆ **模擬 A 品牌盒子訊號**：能否完全模擬 **A 品牌盒子**的訊號，包括其內部機碼，以及能否辨識其關鍵機碼，需要進一步探討。有時候無法成功仿效可能是由於序號不符合，若非正確合法序號可能會成為挑戰。是否能夠達到完全模擬的環境，仍需深入研究。（王翔正 副隊長）
封網技術	◆ **DNS 封不住要封 IP**：我們長期與 **A 品牌盒子**對抗，如今他已成為台灣最大的運營商，各種 DNS RPZ 已無法封鎖他。雖然在 2021 年台北地方法院的刑事裁定中封鎖了數十個 URL，但 **A 品**

	牌盒子仍有 IP 地址，中華電信不願、不敢、也無法封鎖 IP，擔心誤封。然而，當 DNS 無法封鎖時，封鎖 IP 就成為必然的選擇。（彭淑芬 秘書長） ◆ **封網行政措施依據**：可以參考刑法的電腦犯罪專章-刑法 362 條，提及製作專供犯本章之罪之電腦程式，《著作權法》87 條第 1 項第 8 款這 3 目裡面提及，若是他可以專供綁定使用這個電腦違反本法的相關的行為的電腦程式的設備，或者是器材，若針對這部分執行可斷他的金流。後續相關包括封網這些行政措施較有依據可行。（王翔正 副隊長） ◆ **臨時封鎖機制擴大**：TWNIC 最新的 RPZ 策略是一旦接到通報，就立即封鎖，不過這僅限於特定案例。未來是否可能透過 TWNIC 或政府相關法規的調整，將臨時封鎖機制擴大至更多案件類型。（張友寧 主任檢察官）
教育宣導	◆ **教育宣導是重要的**：針對教育宣導，我們需要讓民眾認識到這不僅是經濟問題，但政府目前的困境涉及選票和選民壓力。（彭淑芬 秘書長） ◆ **提供獎勵及從教育面做起**：要打擊侵權，我們需提升著作權的獎勵，始於教育。（盧信儒 資深經理） ◆ **先下警語後處理**：使用《著作權法》87 第一項第 8 款來處理，通常需要有一個前置的直接侵權行為。在先前的會議中提到的方法之一是在盒子啟動時發出警告。另一種方式可能是將一個監理的 App 內建於其中。（林宜柔 助理教授） ◆ **使用機上盒的機制**：雖然使用 A 品牌盒子的人難以直接追蹤，但我們需要找到更有效的機制。修法的一方面應該考慮符合業者應有的權利，同時建立一個更清晰的施力點。（林宜柔 助理教授）
機上盒認證註銷	◆ **前科業者的處置方式**：有前科的業者為何能再次驗證？我們可以設立法條，例如在違規記錄中加入黑名單制度，參考採購法的相關條規，限制其在特定年限內無法申請驗證。這樣一來，我們就能在一段時間內切斷他的金流，對其業務產生實質影響。（張友寧 主任檢察官）
常設第三方公正機構	◆ **未來能夠有一個常設機制**： 建立一個固定的機制，特別推崇的韓國案例啟發，即 KCOPA 雛

	型。期望能有一個類似 iWIN（網路內容防護機構）的組織，具備法源基礎，開始推動類似 KCOPA 的進程。（彭淑芬 秘書長） ◆ **第三方公正單位進行鑑定：**透過第三方公正機構的鑑識，可在案件後進行處理。然而，鑑定的時間可能成為一個問題。個人認為最有效的監護方法是直接禁止機上盒的銷售。一旦發現違規，表示該機上盒已有侵權紀錄，主管機關可據權限撤銷許可，同時啟動下架程序。（張友寧 主任檢察官）
修法方向	◆ **數位問題、數位解決：**在數位時代，透過法院程序處理數位問題已經不切實際。網路犯罪案件過多已經使法院難以應付，有可能導致法院運作癱瘓。因此，檢察官和法官普遍認同應該採用數位方式解決這些問題。（彭淑芬 秘書長） ◆ **提案修法草案精神：**草案的精神是：在網路內容牽涉侵權時，透過網路侵權內容爭議處理機構，即第三方認證機制，依循處理程序確定後，向通訊傳播主管機關報告，通知網路服務提供者執行限制、擷取或移除相關內容。（彭淑芬 秘書長） ◆ **通知取下：**《著作權法》第 84 條規定權利人有權防止著作物的侵害，而修法通常針對此進行調整，如第 84 條之一。因為權利人可行使防止權，因此所謂的通知取下和限制擷取實際上類似於一種暫時性的假扣押。（彭淑芬 秘書長） ◆ **法條構成要件：**以執法單位來講，剛剛最重視的就是法條、構成要件，那現在目前狀況大概就是《著作權法》87 第一項第八款，這三目裡面講到就是上次修法就是說針對預載的才有違法，那其實這部分確實有要再修的必要性。（王翔正 副隊長）
跨部會行政流程建議	◆ **機上盒從資安管理著手：**讓 OTT TV 盒子與有線電視盒子一樣受到規範，包括獲得 ISO 資安標準，以確保其符合相關的資安規定。（彭淑芬 秘書長） ◆ **射頻器材審驗增加智慧局簽名：**未來射頻器材審驗應新增智慧局簽名的要求，即在提出文件或通過特定階段時，需取得智慧局的簽名。雖然這具有相當的難度，但我認為新增測項是一個實行可行的方案。（彭淑芬 秘書長） ◆ **擴展成為著作權保護機制：**目前，我們仰賴射頻管制器材來監管這個盒子，期望將其擴展成為主要的著作權保護機制。未來，這個盒子可能轉變為一個 App，而數位部成立後，將成為 App 的主管機關。（紀效正 簡任視察）

	◆ **執法單位需要授權**：我們的執法單位需要相應的授權，未來所有法規都應包含這一項，這應該是數位發展部的責任之一。我們需要確保法律跟上數位時代的發展，同時讓第三方公正單位擁有法源依據，以執行宣導。（彭淑芬 秘書長）

座談會第二場之專家代表提供數位犯罪和侵權問題的多項建議，主要分為法律修訂、技術應對、合作機制和宣導教育等四個方向。首先，建議建立常態化的研究機制，參考韓國的 KCOPA 模式，以深入了解盒子技術並提高法官對盒子犯罪工具的理解。其次，強調法院程序的數位化，以迅速應對數位犯罪和侵權案件，並提出加強政府跨部會合作，參考韓國政府在解決數位侵權問題上的成功經驗。同時，建議修法授權成立第三方認證機構，以加強在數位犯罪和侵權案件中的法律制裁。

在技術層面，提出加強對認證主機的監控，優化封鎖機制，並加強監測效能，以應對安◯盒子等不斷演進的解析機制。同時，強調提高技術應對的速度，迅速適應數位犯罪工具的演進，並加強國際合作，特別針對侵權機上盒等工具已轉向使用境外 DNS 的情況，加強與國際監理機構和其他國家的合作。

在法律和合作方面，建議修法強化機上盒管理，加強法院封網程序，擴大 RPZ 通報機制，並強化智慧財產權保護。同時，建議強化 CDN 業者的法源依據與合作機制，並建立台灣 ISP 業者協同機制，以協同阻斷非法內容。

在宣導和教育層面，建議提升著作權獎勵，討論非法機上盒的 NCC 認證問題，建立更有效的地下論壇及檢舉機制，導入浮水印機制，並影響非法機上盒的收入金流，探討影響其硬體收入或限制進行額外訂閱費用等方法。

此外，對於法條的修訂，建議針對《著作權法》第 87 條第 1 項第 8 款進行修訂，特別是針對侵權程式綁定特定機上盒的部分，加強法條的明

確性。同時，提出多項具體的法源依據修正、建立第三方認證機制、強化機上盒處理等措施，以因應技術發展所帶來的挑戰。

總體而言，這些建議綜合考慮了法律、技術、合作、宣導和教育等多方面，旨在更有效地應對數位犯罪和侵權問題，同時加強政府和相關機構之間的協作。

第二節　未來推動監理法規、監理技術、型式認證審驗、後市場管理與防制非法侵害智慧財產權之處理、建議、分析與因應作法

一、 監理法規

（一）強化機上盒監理

如參考歐盟《無線電設備指令》增訂事前審驗規範，建議可針對機上盒製造商、進口商與分銷商，明知或有理由可知，於銷售後再以客服方式安裝非法收視視聽內容之程式；又或購買之消費者自行至網路論壇查詢安裝此類非法收視程式，只要此類程式可危害消費者之隱私及個人資料、詐欺、以及破壞網路安全，機上盒欠缺阻止載入該軟體之設計則不予審驗通過，不可進入市場，要求製造商將隱私和個人數據、網路安全和欺詐預防之考慮因素整合至機上盒之設計中。

（二）推動後市場管理機制

為確保消費者的安全，需要迅速且可靠地通知消費者權益相關議題，因此，經營者和線上市場提供者應該利用他們手中的客戶資料，通知消費者有關已購買產品的召回和安全警告。建議可以參照歐盟之回收作法，進行條文調修，包括通知義務與回收對價限制，以具體化業者之回收義務及限制。

建議可以參照歐盟之回收作法，進行條文調修，包括通知義務與回收對價限制。

（三）透過法規調適防治 OTT TV 機上盒侵權（細節詳第八章）

1.《著作權法》之修法建議：

(1) 修訂《著作權法》第 87 條第 1 項第 8 款：為徹底杜絕「純淨版」機上盒之相關脫法行為，建議於《著作權法》第 87 條第 1 項第 8 款增訂第 4 目「製造、輸入或銷售專供匹配或綁定第一目之電腦程式之設備或器材，未預先載入者亦同。」之相關文字。

(2) 確認 OTT TV 機上盒未經授權傳送「體育賽事」直播之違法性：我國未採鄰接權制度，賽事轉播節目若欠缺視聽著作之要件，則可能無法受到保護，建議可強化體育賽事之著作權、鄰接權保護，避免違法 OTT TV 機上盒在侵害賽事轉播著作權後，相關人未能妥善獲得救濟。

(3) 研議扣押裁定之彈性：建議我國法院依個案之性質（以 OTT TV 機上盒所使用之侵權程式及其接取之 CDN 伺服器為主，OTT 平台網站、論壇、串流平台則不適用），「得」下達範圍較大之扣押裁定，在一定期間內，經過第三方驗證機構認證後，對侵權程式所接取提供侵權影像的 CDN 伺服器 IP，可向 ISP、TWNIC 提出扣押裁定。倘域名註冊人或 IP 使用者對扣押裁定不服，可依照《刑事訴訟法》第 404 條第 1 項但書第 2 款提起抗告，且依同條第 2 項規定，即使扣押已經執行終結，法院也不得因已執行無實益而駁回。抗告法院倘認為域名扣押有所不當，自得撤銷原裁定，於有必要時，並自為裁定（《刑事訴訟法》第 413 條規定參照）。並建議確認行為人違反著作權法第 87 條第 1 項第 7、8 款，除處以有期徒刑、罰金外，得擴大刑事訴訟法上「沒收」之

概念，針對確認侵權之第 87 條第 1 項第 7、8 款之電腦程式，於一定期間內，對其所持續連結之伺服器 IP，經第三方驗證機構確認供相同侵權行為所使用，得由主管機關命 ISP、TWNIC 停止用戶接取。

(4) 強化目前智財法中對於 ISP 業者之「安全港條款」之運用：相關規範自增訂以來已適用多年，衍生出不少法律問題，例如：網路平台業者是否適用、假藉通知取下制度而進行商業競爭、是否僅有著作權人能進行通知 ISP 業者取下，著作權人如何認定等，建議未來可由第三方公正機構通知 ISP 業者相關盜版侵權之可能性，並告知其智財法上安全港條款之權利義務，由業者自行判斷下架相關盜版影音，並適用相關免責規定。

2.《電信管理法》之修法建議：建議於《電信管理法》第 65 條增訂「使用電信管制射頻器材有代理權、專利權、著作權爭議者，依有關法律之規定。」

3. 廣電三法之修法建議：

(1) 新增侵權防治、訊號侵權機制：2022 年 5 月 25 日國家通訊傳播委員會（以下簡稱 NCC）通過新版《網際網路視聽服務法》（草案），外界多數期待該草案能夠處理網際網路視聽之盜版問題，惟該草案基本上仍以網路上所衍生的問題，除網際網路視聽服務事業之營運及其提供之內容服務，仍應適用各該行為之法律，故侵害智慧財產權、著作權等盜版問題，仍須回歸《著作權法》處理，但 NCC 擬透過草案針對多次侵權之業者得以糾正其相關不當營業行為之機制，後續立法進展值得持續關注。

(2) 給予自願登記納管之業者予以主張「訊號竊盜」之法律地位：而未來在討論《網際網路視聽服務法》（草案）時，關於侵權部

分，民事部分可參考《有線廣播電視法》第 54 條第 1 項之規定：「未經系統經營者同意，截取或接收系統播送之內容者，應補繳基本頻道收視費用，並負民事損害賠償責任。」明訂未經合法網際網路視聽服務提供者同意，截取或接收網際網路視聽服務提供者播送之內容或訊號者，應負一定之法律責任；刑事部分則可參照《電信法》第 56 條之規範，針對「意圖為自己或第三人不法之利益，未經網際網路視聽服務提供者同意，截取或接收網際網路視聽服務提供者播送之內容或訊號營利者」設有相關刑事處罰，或是要求連線服務提供者、電信事業或設置公眾電信網路者拒絕為侵權之網際網路視聽服務提供者電信服務之請求及通信傳遞或為必要之處置。

4.《電信管制射頻器材審驗管理辦法》之修法建議：參考歐盟於《一般產品安全規則》新增產品召回程序。

5. 通盤檢視數位產品之資安、個資規範：參考歐盟《資安韌性法》（草案）（Cyber Resilience Act）加強數位產品之資安規則，包括：網路功能損害禁止、隱私保護措施、防止詐欺、軟體之合規性等。

（四）跨部會合作行政作為之建議（細節詳第九章）

1. 建立有效機上盒上架與下架流程，保護合法業者

機上盒非法侵權並非單一部會權責，涉及相關部會應建置有效事前審查、檢測上架，事中強化稽查、調查與受理檢舉機制，嚴格監督市場不法情事活動，並強化監管工作之行政檢查措施，避免不肖業者鑽漏洞，面對實際從事不法工作者，經發現屬實者，除依照法規予以裁罰之外，應建立一套有效配套措施。

2. 成立跨部會協調機制並考量設置第三方機構專責

參考韓國著作權保護署(KCOPA)之作法成立跨部門工作小組，負責著作權保護政策的制定和執行、審查與著作權保護有關的事項以及實施著作權保護所需的項目。時程上可進一步分為短、中長期規劃：

(1) 短期

短期可以成立跨部會工作小組，召集相關機關成立跨部會工作小組落實各項執法工作，完善網際網路著作權侵害之防治機制。

(2) 中、長期

若欲建立如韓國 KCOPA 集「預防→檢測→分析→行動」相關功能之推進系統並專責處理著作權侵權之第三方機構，建議仍要透過《著作權法》授權，並可參考韓國做法，負責著作權侵權之相關資訊蒐集、數位鑑定、內容鑑識等，逐步建立防護網際網路盜版之防護網。

二、 監理技術

（一）侵權影音程式綁定特定機上盒之檢測

監理技術之運作以受檢舉有侵害著作權的 OTT TV 機上盒為前提，杜絕非法 OTT TV 對於現行電視業者之著作權侵害，調查機上盒與瀏覽盜版影音程式之關聯性，處理方式可分為以下 2 部分進行：

1. 架設模擬機上盒

於虛擬機或是他牌機上盒中安裝侵權影音程式，若可安裝、可執行，則代表該收看影音應用程式並未綁定特定機上盒；相反地，若該盜版影音程式不可安裝或不可於虛擬機上盒上正常執行運作，則需釐清原因、溯源影音來源，以茲證明機上盒與侵權影音程式具有關聯性，應提報相關單位進行後續處理。而機上盒之技術分析應以政府單位宣告之檢測標準監理之，並透過符合 ISO 17025 之檢測實驗室出具最終檢測報告，以確保檢測結果的正確性。

2. 直接辨識機上盒與瀏覽盜版影音程式之綁定方式

透過封包側錄、逆向工程等方法，確認應用程式在開啟、執行、運作的過程中確實有鑑別裝置特徵之認證行為，且透過修改該裝置特徵，確認在其他裝置無法正常運作，證明機上盒與侵權影音程式確認具有關聯性，提報相關單位進行後續處理。

故建議針對機上盒綁定行為、侵權影音程式是否可在虛擬機上盒上安裝執行進行監理，判斷侵權影音程式是否僅可在特定機上盒上收視，再進一步進行後市場管理、禁售等程序，如圖 72。

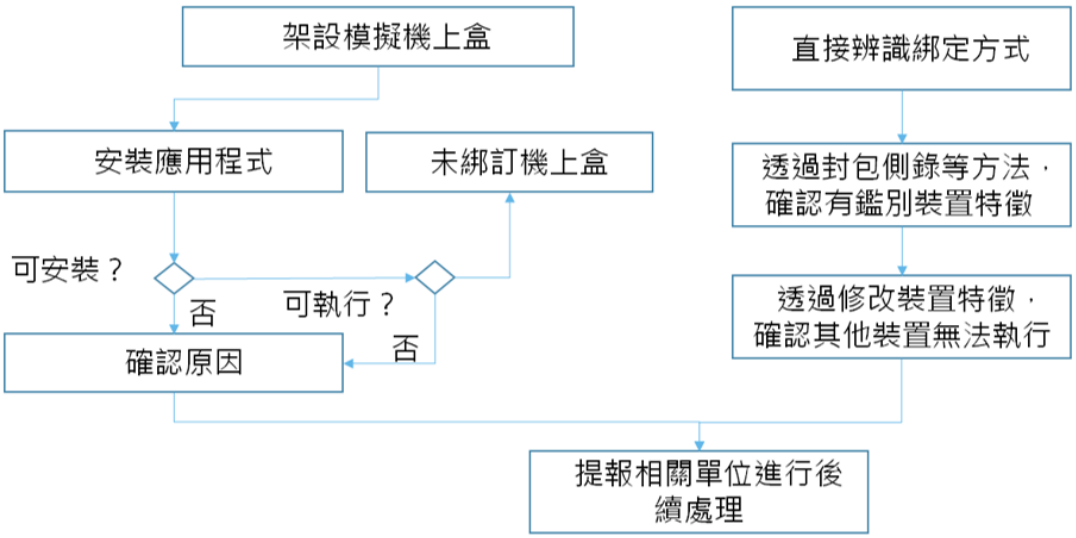

圖 72：OTT TV 機上盒技術監理之處理程序規劃
資料來源：本計畫整理

（二）封網技術建議

透過網頁連線紀錄、IP 位址伺服器，溯源機房或我國的網路服務公司，追查最終資料是否放在國內，若位於國內可直接進行查扣或請網路服務業者中止服務。

若來源係來自國外，可從連線紀錄中找到本國嫌疑人，並請求對方刑事單位協助查緝，向國外網路服務業者檢舉。若國外單位不配合，依法規由數位部進行審查與執行或使用 DNS RPZ 等技術禁止查詢，達成封網與溯源管理之成效，杜絕非法觀覽影音之來源，如圖 73。

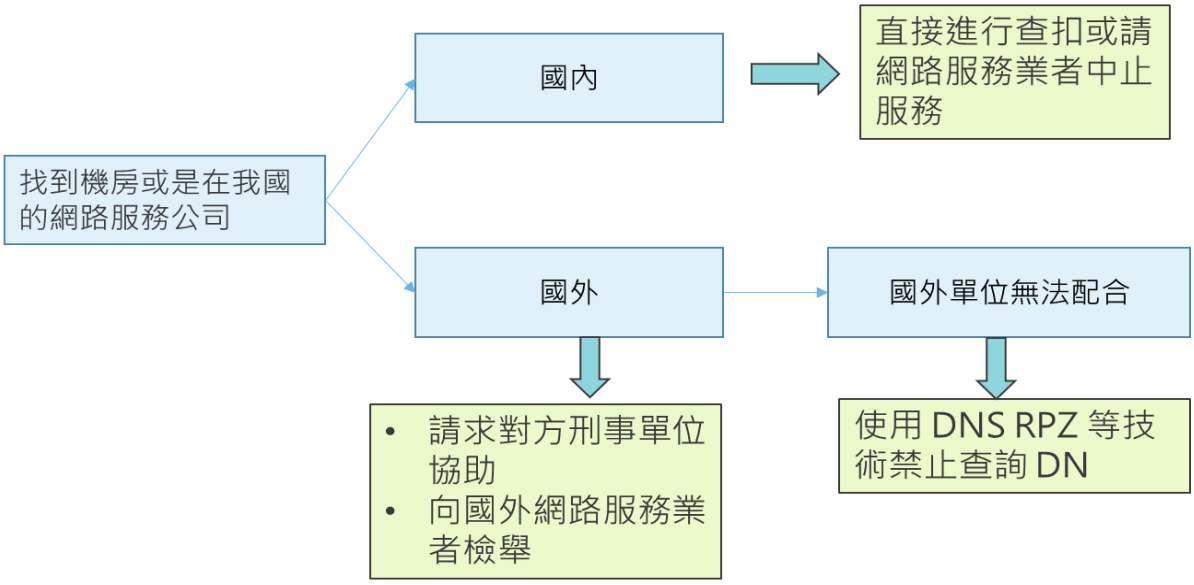

圖 73：OTT TV 機上盒封網技術建議

資料來源：本計畫整理

三、 型式認證審驗

對於型式認證審驗之處理，建議於實驗室檢測及驗證機構審驗時，應納入「侵權影音程式是否綁定特定機上盒」之檢測項目，以確保審驗程序更全面。具體建議如下：

（一）認證審驗之處理

於 OTT TV 機上盒上市前進行技術審驗，包括架設模擬機上盒、辨識機上盒與侵權影音程式之綁定方式，有助於確保機上盒未綁定可觀覽未經授權的影音 App，避免業者蓄意將侵權程式綁定至特定機上盒硬體，以謀取不法利益。透過這樣的審驗步驟，可以提高整體系統的安全性和合法性。

（二）禁止販售

一旦確認機上盒與侵權影音程式具有關聯性，應立即向相關單位報告，並採取後續處理措施，包括但不限於禁止相關機上盒的販售。這種積極的應對措施有助於遏制侵權行為，維護市場秩序，並保護消費者的權益。

禁止販售是一種有效的手段，可加強對不當行為的制止，使市場更加公平和透明。

四、 後市場管理

（一）參考歐盟作法：

歐盟於 2023 年 5 月 10 日公告《一般產品安全規則》（Regulation on General Product Safety，GPSR）（Regulation（EU）2023/988）對一般產品安全規範進行大幅修正，並於 2023 年 6 月 12 日生效，由《一般產品安全規則》取代原《一般產品安全指令》（Directive 2001/95/EC），並新增部分管制措施，包括一般產品之事故、產品召回和市場監督程序。

在新的《一般產品安全規則》前言第 85 點也提及：「當已售予消費者的產品被證實存在危險時，為保障歐盟內的消費者，可能需要進行產品召回。消費者可能不知道自己擁有一個被召回的產品，為了增加召回的效力，聯繫相關消費者是非常重要的。直接聯繫是提高消費者對召回的認知並促使採取行動的最有效方法，也是所有消費者群體中首選的溝通途徑。為確保消費者的安全，迅速可靠地通知他們是很重要的。因此，經營者和線上市場提供者應該利用他們手中的客戶資料，通知消費者有關已購買產品的召回和安全警告。因此，需要法律義務要求經營者和線上市場提供者使用他們手中已有的客戶資料，通知消費者有關召回和安全警告的消息。在這方面，經營者和線上市場提供者應確保他們在現有的客戶忠誠計畫和產品註冊系統在有召回或安全警告時，有可以直接聯繫客戶之可能。故客戶將被要求在購買產品後自願向製造商提供一些資訊，例如：姓名、聯絡資訊、產品型號或序列號。召回是針對消費者的，故不應阻止經營者和線上市場提供者讓所有客戶意識到產品召回通知，也不應阻止他們為其他終端用戶提供解決方案。應鼓勵經營者和線上市場提供者採取此類行

動，特別是在微型和小型企業。[310]」依據新《一般產品安全規則》主要召回程序及內容如下：

1. 通知

按新《一般產品安全規則》第 35 條第 1 項規定：「在產品安全召回，或需要向消費者提供特定資訊以確保產品的安全使用（安全警告）時，經營者應根據本規則第 9 條、第 10 條、第 11 條和第 12 條的相關義務，以及線上市場提供者應根據本規則第 22（12）條的相關義務，確保所有受影響的消費者能夠被直接且不延遲地通知。經營者及線上市場提供者若有蒐集客戶個人資料，應利用該資料進行召回和安全警告。[311]」；第 4 項規定：「若根據第 1 項規定無法聯繫所有受影響的消費者，經營者和線上市場提供者應根據各自的責任，在其他適當的管道傳播清晰可見的召回或安全警告，確保通知至最廣泛的覆蓋範圍，包括：公司網站、社交媒體管道、通訊和零售門店，並在適當情況下，在大眾媒體和其他通訊管道進行公告。這些資訊對於弱勢族群可觸及。[312]」。另外，召回通知應滿足本規則所訂之格式和內容要求[313]。

2. 產品安全召回之補救措施

(1) 基本補救措施

新《一般產品安全規則》第 37 條規定有關產品安全召回之補救措施，當產品安全召回由經營者發起或由國家主管當局下令，負責產品安全召回的經營者應向消費者提供有效、免費且及時的補救措施[314]。經營者應向消費者提供以下至少兩種解決方案之選擇，包括：(a) 召回產品的修理；(b) 用同類型且至少具有相同價值和品質的安全替

[310] Regulation (EU) 2023/988, Recitals (85).
[311] Regulation (EU) 2023/988, Sec. 35 (1).
[312] Regulation (EU) 2023/988, Sec. 35 (4).
[313] Regulation (EU) 2023/988, Sec. 36.
[314] Regulation (EU) 2023/988, Sec. 37 (1).

代品取代召回產品；或（c）適當退還召回產品的價值，前提是退款金額至少應等於消費者支付的價格[315]。

(2) 其他補救措施

i. 退貨

當負責產品安全召回的經營者未能在合理時間內且對消費者造成重大不便的情況下才能完成修理或更換時，消費者始終有權退貨[316]。

ii. 消費者的自行維修

消費者的自行維修僅在消費者能夠輕鬆、安全地進行並在召回通知中考慮到的情況下被視為有效的救濟措施。在此種情況下，負責產品安全召回的經濟營運者應向消費者提供必要的指示、免費的替換零件或軟體更新[317]。

iii. 消費者的處置

消費者的處置只有在消費者能夠輕鬆、安全地進行並在第 36(2)（d）下進行的行動中，並且不會影響消費者根據本條第 1 項之規定享有退款或召回產品替換的權利[318]。

救濟措施不應對消費者造成重大不便。消費者不應承擔運送或退回產品的費用。對於其性質不便攜的產品，經濟營運者應安排收回該產品[319]。

（二）我國規範與建議作法

按我國《電信管制射頻器材審驗管理辦法》第 23 條第 2 項：「審驗證明經撤銷或廢止時，原取得審驗證明者、經授權使用審驗合格標籤或符合性聲明標籤者，應依主管機關指定期限回收已販賣之電信管制射頻器

[315] Regulation (EU) 2023/988, Sec. 37 (2).
[316] Regulation (EU) 2023/988, Sec. 37 (2).
[317] Regulation (EU) 2023/988, Sec. 37 (3).
[318] Regulation (EU) 2023/988, Sec. 37 (4).
[319] Regulation (EU) 2023/988, Sec. 37 (5).

材或非隨插即用射頻模組（組件），若他人權益因而受損，並應負損害賠償責任。」；第 3 項：「依前項應辦理回收而拒不辦理回收或有回收不確實情形時，原取得審驗證明者自主管機關通知日起六個月內，不得就同一電信管制射頻器材或非隨插即用射頻模組（組件）向驗證機關（構）申請審驗。」已有規定有關回收之相關作法，故目前實務作法主要為通傳會將審驗證明廢止名單公告於官網，並請廠商提報回收計畫，說明回收處理情形，同時請網路平臺及實體通路業者配合下架處理等方式進行。

為使審驗證明經撤銷或廢止之機上盒回收更有效率，建議參照歐盟之回收作法，進行條文調修，包括：

1. **通知義務**：要求業者盡可能的通知所有下游廠商及消費者，可參照我國其他立法例[320]於《電信管制射頻器材審驗管理辦法》第 23 條第 2 項新增「應於大眾傳播媒體公告並以其他有效方式通知消費者」相關文字。
2. **回收對價限制**：器材被廢止審驗證明者，可參照歐盟規範，於《電信管制射頻器材審驗管理辦法》第 23 條第 2 項新增相關文字，要求違法有責之業者，以適當、合理之對價回收市面上流通之違法機上盒。主要在於業者違法事實已經判決確定，故要求其以合理對價回收違法機上盒並無不妥，但應於相關法規中明確規定為宜。

綜上所述，可將《電信管制射頻器材審驗管理辦法》第 23 條第 2 項調整為「審驗證明經撤銷或廢止時，原取得審驗證明者、經授權使用審驗合格標籤或符合性聲明標籤者，應依主管機關指定期限回收已販賣之電信管制射頻器材或非隨插即用射頻模組（組件），**並應於大眾傳播媒體公告並以其他有效方式通知消費者，回收對價應適當、合理**，若他人權益因而受損，並應負損害賠償責任。」

[320] 參照《汽車安全性調查召回改正及監督管理辦法》第 13 條、第 15 條之文字。

五、 防制非法侵害智慧財產權

對於每個國家/地區，幾乎都會要求 OTT TV 播放受著作權保護之內容，以維持線上行為之合法性。一般來說，從非法/未經授權的來源下載影音內容是侵犯智慧財產權的行為，受到重製權的保護；至於接收串流媒體，目前主要國家也認為這樣的行為構成侵害著作權，無論是使用技術設備還是預裝附加軟體的 OTT TV 機上盒。

各國針對 OTT TV 機上盒之智慧財產侵權皆設有許多執法措施、程序、補救措施和制裁，包括：行政措施（例如：事前監理、回收）、司法措施（例如：民事禁制令、刑事處罰等）。執法措施可能有針對受保護內容的使用者或中間機構（例如：網路服務提供商、機上盒設備製造商），或是針對使用者和中介機構的執法措施；國際上打擊 OTT TV 機上盒之智慧財產侵權的民事、行政和刑事等執法措施並不缺乏。下列對應各國作法後，分析我國可能需要精進之問題如下，並提出初步建議方向如表 21。

表 21：未來推動防制非法侵害智慧財產權之分析

分類	問題描述	變化和發展推估	建議方向
行政措施	事前監理之規範要求不足	強化事前監理	可比照歐盟《無線電設備指令》、《資安韌性法》（草案）強化個資、資安事前審驗規範。
	技術過濾	增加技術過濾機制	比照歐盟《無線電設備指令》、《資安韌性法》（草案）增訂事前審驗規範（個資、資安等）。
	後市場管理不足，回收機制仍待強化	增加回收機制之細節性規範	考慮增訂回收機制之細節性規範，包含:通知及產品安全召回之補救措施。
司法措施	法律仍有不確定性（智財法）	明確相關規範解釋	➢ 修訂《著作權法》第 87 條第 1 項第 8 款。

分類	問題描述	變化和發展推估	建議方向
			➢ 明確「訊號竊盜」之訴訟主體。 ➢ 確認體育賽事之直播是否擁有著作權。
	假處分之範圍及時效	基於法官保留原則，於法制規範內實行	➢ 考量扣押裁定之彈性。 ➢ 強化目前智財法中對於 ISP 業者之「安全港條款」之運用。
	違法機上盒造成資安、個資漏洞	基於數位元素產品的資安進行監管法案	參考《資安韌性法》（草案）數位產品之相關安全法規，建立清晰且明確的規範。
市場機制	宣導教育不足	強化宣導，增加不同面向之說明（例如：資安、防詐騙等）	參考英國作法，以不同面向向消費者進行宣導。
	產業合作仍待強化	鼓勵產業合作、增加廣告商之配合	鼓勵產業合作、參考韓國資訊共享之作法。

資料來源：本研究整理

第八章 防治 OTT TV 機上盒侵權之修法建議

第一節　《著作權法》之修法建議

一、修訂《著作權法》第 87 條第 1 項第 8 款

按現行《著作權法》第 87 條第 1 項第 8 款規定：「明知他人公開播送或公開傳輸之著作侵害著作財產權，意圖供公眾透過網路接觸該等著作，有下列情形之一而受有利益者：（一）提供公眾使用匯集該等著作網路位址之電腦程式。（二）指導、協助或預設路徑供公眾使用前目之電腦程式。（三）製造、輸入或銷售載有第一目之電腦程式之設備或器材。」故依上開規定目前銷售機上盒設備不得內建、預設可觀看未授權影音內容之電腦程式或指導、協助消費者安裝上開違法電腦程式，違法的業者一旦被查獲，依《著作權法》第 93 條之規定將處以 2 年以下有期徒刑之刑事責任，或併科最高新臺幣 50 萬元以下罰金；同時，依據《電信管制射頻器材審驗管理辦法》第 22 條第 2 項第 8 款「因代理權、專利權、著作權爭議，經法院判決敗訴確定，致不得販賣經審驗合格之電信管制射頻器材或非隨插即用射頻模組（組件）。」可作為主管機關或原驗證機構得廢止其設備審驗證明之事由。

為符合上開法規，有些銷售商會標榜所販賣的為「純淨版」機上盒，此機上盒設備內在販售時並無安裝觀看非法、未授權之影音內容的電腦程式，也無預設非法連結、販售人員基本上也不會指導觀看非法影音，故屬合法販售。但消費者購買相關機上盒設備後，往往可以自行透過網路搜尋方式安裝上開電腦程式，導致相關規範仍無法有效防堵違法機上盒於市面上流通。

為徹底杜絕上開「純淨版」機上盒之相關脫法行為，建議於《著作權法》第 87 條第 1 項第 8 款增訂第 4 目「製造、輸入或銷售專供匹配或綁

定第一目之電腦程式之設備或器材，未預先載入者亦同。」鑒於目前許多電腦程式皆可與多種設備相容，為限縮處罰範圍，以「專供匹配或綁定第一目之電腦程式之設備或器材」之具特定意圖之違法設備或器材為主，且為防止消費者可自行搜尋安裝違法程式，即使未預先載入者也應列為處罰對象，而本款前段設有「知悉」、「意圖」及「受有利益」等要件，如此增訂應不至於將處罰範圍過於擴大。

二、 確認 OTT TV 機上盒未經授權傳送「體育賽事」直播之違法性

體育賽事透過網路即時盜播成為許多違法 OTT TV 機上盒違法「轉播」之形式之一，而體育賽事直播是否受到著作權保護也成為法律爭點之一。就目前學者見解認為，若不是專屬授權，賽事轉播的被授權人，僅取得自己得轉播比賽的權利，但對於轉播內容，自己並沒有權利。因此，當他人盜播時，被授權人無權出面主張權利，必須通知著作財產權人或專屬授權之被授權人，由他們出面主張權利。除非著作財產權人或專屬授權之被授權人知悉盜播而怠於主張權利，被授權人始有在民事上代位追償之可能，但被授權人終究不是權利人，無從對盜播者進行刑事告訴或自訴[321]。

在司法實務中，愛爾達體育台在 2018 年取得世界盃足球賽轉播權，賽事轉播畫面卻遭盜用在手機 App 上直播，愛爾達自行蒐證找到電視直播 App「亞視」，檢警獲報後調查起訴亞視 App 負責人，其於桃園機房及臺北機房架設網路、伺服器、影像擷取、編碼及傳送系統[322]，旋利用中華電信 MOD、凱擘數位機上盒及中嘉數位機上盒收受節目訊號，再藉由上開機房內之電腦設備、影像擷取及編碼系統、伺服器將所收受之電視節目

[321] 章忠信. (2023). 運動賽事之轉播授權實務. http://www.copyrightnote.org/ArticleContent.aspx?ID=9&aid=3139

[322] 偷愛爾達訊號直播世足賽　亞視 APP 負責人違反《著作權法》起訴. (2019, August 27). ETtoday. https://www.ettoday.net/news/20190827/1522469.htm

儲存、編碼、重製後，透過「亞視 App」之伺服器提供前揭電視節目給購買「亞視 App」之消費者觀賞[323]。判決認為被告未經愛爾達公司同意或授權，先擅自重製系爭電視節目，繼而公開傳輸之，除成立《著作權法》第 91 條第 2 項之罪外，另亦應成立《著作權法》第 92 條之擅自公開傳輸侵害他人著作財產權罪[324]。但並未針對愛爾達是否擁有轉播內容之著作權進行深究。

針對體育賽事是否有著作權按我國目前現行法解釋，無法一概而論。《著作權法》第 5 條第 1 項第 7 款規定「視聽著作」為被保護之著作類型之一，而「視聽著作」包括電影、錄影、碟影、電腦螢幕上顯示之影像及其他藉機械或設備表現之影像，不論有無附隨聲音而能附著於任何媒介物上之著作[325]。享有重製權（第 22 條第 1 項）、公開播送權（第 24 條第 1 項）、公開上映權（第 25 條）、公開傳輸權（第 26-1 條）、改作與編輯權（第 28 條）、散布權（第 28-1 條）及出租權（第 29 條），但並無公開演出之使用報酬請求權。

經濟部智慧財產局 92 年 12 月 22 日電子郵件 921222a 號函釋內容略以：「廣播電台播出的節目，有可能是包含著作之節目（例如播出錄音、音樂、小說、短文精選等），也有可能是與著作無關的節目（例如實況轉播的運動比賽、報導選情造勢活動等）。...部分歐陸法系國家在其《著作權法》中設有專章，對於廣播機構之節目，不論是否具有創意，一律加以保護，通稱「鄰接權制度」。」由相關函釋可以看出，智財局認為實況轉播的運動比賽是與著作無關的節目，但我國未採鄰接權制度，賽事轉播節目若欠缺視聽著作之要件，則可能無法受到保護，建議可強化體育賽事之

[323] 臺灣臺北地方法院 108 年度智易字第 55 號刑事判決。
[324] 臺灣臺北地方法院 108 年度智易字第 55 號刑事判決。
[325] 中華民國八十一年六月十日台(81)內著字第八一八四〇〇二號公告。

著作權、鄰接權保護，避免違法 OTT TV 機上盒在侵害賽事轉播著作權後，相關人未能妥善獲得救濟。

三、 研議扣押裁定之彈性

（一）實務作法

我國司法及執法單位透過 TWNIC 執行「聲請法院扣押域名並執行 DNS RPZ（停止解析域名）」，成功扣押域名並停止解析非法視聽來源網址。故藉由法院核發扣押裁定，對於域名實施 DNS RPZ 用以阻斷訊號接取的方式，讓侵權內容無法繼續由造訪者透過該網站取得，在法制面及執行面上係屬有據且可行，在我國司法實務上已獲得肯認[326]。

而針對侵權網站之扣押，主要係依據我國《刑事訴訟法》第 122 條以下以及第 133 條以下關於搜索、扣押之規定，我國警方可藉由偵查程序確認幕後經營者後，再依一般搜索扣押程序扣押其電腦、手機，並憑藉警方訊問、搜索及電信偵查能力，直接掌握該網站的帳號、密碼等管理權限，進而執行關閉侵權網站、置換網站的入口頁面[327]。

按《刑事訴訟法》第 133 條第 1 項：「可為證據或得沒收之物，得扣押之。」又按第 133-1 條第 1 項為獨立扣押程序「非附隨於搜索之扣押，除以得為證據之物而扣押或經受扣押標的權利人同意者外，應經法官裁定。」檢警得不需搜索侵權行為人，即直接扣押該侵權網站之網域；第 133-2 條第 1 項「偵查中檢察官認有聲請前條扣押裁定之必要時，應以書面記載前條第三項第一款、第二款之事項，並敘述理由，聲請該管法院裁定。司法警察官認有為扣押之必要時，得依前項規定報請檢察官許可後，向該

[326] 陳昱奉. (2022). 網路犯罪與資訊安全的未來—從網域名稱扣押談網路治理. 刑事政策與犯罪防治研究專刊, *32*, 248.

[327] 由楓林網事件探討我國刑事程序扣押網站及網域名稱之可能方式. (n.d.). 聖島國際法律事務所. https://www.saint-island.com.tw/Tw/Knowledge/Knowledge_Info.aspx?IT=Know_1_1&CID=586&ID=1758

管法院聲請核發扣押裁定。」故依據上開規定，非以搜索為前提的扣押，得以循上開規定，向法院聲請裁定獲准後執行扣押。

扣押為強制處分之一種，《刑事訴訟法》並未限定其執行態樣，因此，以扣押之意思而對欲扣押之標的執行扣押，即產生扣押效果。一旦扣押之意思達到扣押標的之持有人或所有人，並將應扣押標的移至公權力之下，扣押行為即告完成，法律上即為國家所占有，其原有運作之功能亦即因扣押而中止[328]。藉由網站和域名涉犯違反《著作權法》等犯行的情形，對於任何網站而言，網站訊息的進出與傳遞，來自於對其網域名稱的解析，所以透過域名扣押方式，將域名支配權限移轉於公權力之下，由公權力決定該網站營運與否，或者透過前述 DNS RPZ 的方式為之，將系爭網域名稱列在「黑名單」之中，以停止解析的方式，讓一般大眾無法接取，實際上與扣押的本質並無不同，屬《刑事訴訟法》第 133 條第 1 項所稱之扣押。檢警或亦可直接扣押網域，使侵權行為人無法繼續使用侵權網域為非法行為[329]。

依據現行實務作法，檢警按《刑事訴訟法》第 133 條第 1 項以及第 133-1 條向法院聲請扣押裁定，並於取得法院核發之裁定後，透過目前 DNS RPZ 的運作框架，TWNIC 得以根據法院判決、裁定，將預計停止解析之網域名稱，載入 DNS RPZ 資料庫後，同步更新至國內電信業者 DNS 資料庫，全國統一停止解析。惟執法機關依據《刑事訴訟法》之規定，其實沒有辦法採取類似「動態封網」的作法，就目前司法實務上沒有辦法不斷的變更同一個扣押裁定上的被扣押標的。

（二）行政封網修法易引發爭議

對於「行政封網」之修法，往往會遭受民眾之強烈反彈。2013 年經濟部智慧財產局發表新聞研擬修法，將由智慧財產局直接下令 ISP 業者，

328 同註 325

329 同註 325

以 IP 位址或 DNS 技術等方式封鎖「一望即知重大侵權的境外網站」，後來因外界強烈批評而撤案。由於「重大明顯的侵權行為」難以認定，由國家行政機關自行界定恐有濫權之可能，引起民眾對行政封網認定的質疑，更引發網路輿論譁然，甚至被解讀為 2013 年台灣網路的白色恐怖，網友群起串聯抗議，原本預計於 2013 年第二立法院院會期間審查，後來停止推動修法。故行政封網在我國之修法推動往往會受到極大反彈。

（三）建議作法

建議我國法院可參考英國之作法，依個案之性質（以 OTT TV 機上盒所使用之侵權程式及其接取之 CDN 伺服器為主，OTT 平台網站、論壇、串流平台則不適用），「得」下達範圍較大之扣押裁定，在一定期間內，經過第三方驗證機構認證後，對侵權程式所接取提供侵權影像的 CDN 伺服器 IP，可向 ISP、TWNIC 提出扣押裁定。

倘域名註冊人或 IP 使用者對扣押裁定不服，可依照《刑事訴訟法》第 404 條第 1 項但書第 2 款提起抗告，且依同條第 2 項規定，即使扣押已經執行終結，法院也不得因已執行無實益而駁回。抗告法院倘認為域名扣押有所不當，自得撤銷原裁定，於有必要時，並自為裁定（《刑事訴訟法》第 413 條規定參照）。

並建議確認行為人違反著作權法第 87 條第 1 項第 7、8 款規定，除處以有期徒刑、罰金外，得擴大刑事訴訟法上「沒收」之概念，針對確認侵權之第 87 條第 1 項第 7、8 款之電腦程式，於一定期間內，對其所持續連結之伺服器 IP，經第三方驗證機構確認供相同侵權行為所使用，得由主管機關命 ISP、TWNIC 停止用戶接取。

參考前述英國《1988 年著作權、設計和專利法》第 97A 條，英國高等法院（The High Court）有權對服務提供者（Service provider）實際知悉另一個人利用他們的服務來侵犯著作權時發出禁制令，且近年相關案例

已於英國法院判決中認為相關禁制令合乎比例原則，故為使法院判決有所依循，建議可於《著作權法》中，參考上揭作法作成相關修法。

四、 強化目前智財法中對於 ISP 業者之「安全港條款」之運用

若欲在執行面有效將盜版影音下架，或可強化目前智財法中對於 ISP 業者之「安全港條款」之運用，按《著作權法》第六章之一規範「網路服務提供者之免責事由」其立法目的是為網路服務提供者提供與著作權人合作打擊侵權之誘因，透過安全港制度之設計，降低網路服務提供者因為其使用者之著作權侵害行為而產生被訴之風險，並訂有《網路服務提供者民事免責事由實施辦法》主要內容在規範《著作權法》第 90 條之 4 第 1 項第 3 款所稱的聯繫窗口資訊、第 90 條之 6 至第 90 條之 9 所稱的通知及反通知格式。著作權人一旦發現網路上有侵害其著作權之內容時，只需依相關規定通知 ISP，即可經由 ISP 之配合取下而迅速排除侵權行為，並避免損害範圍之擴大。ISP 對於網路使用者利用其服務從事著作權侵權之行為，只要依著作權人通知，立即取下該涉嫌侵權之內容；或 ISP 因其他管道知悉該等侵害情事，善意取下該涉嫌侵權之內容者，該 ISP 對著作權人及網路使用者均不負賠償責任。另外，《著作權法》第 90 條之 4 第 1 項第 2 款也規定了所謂「三振條款」，ISP 應於提供服務前向使用者明確「告知」，使用者於涉有侵權情事達三次時，ISP 將終止全部或部分之服務。依該款規定，ISP 有告知使用者違反規定之法律效果之義務，至於使用者是否涉有侵權情事達三次以上，ISP 是否終止全部或部分之服務，則屬於自由裁量之範圍。

相關規範自增訂以來已適用多年，衍生出不少法律問題，例如：網路平台業者是否適用、假藉通知取下制度而進行商業競爭、是否僅有著作權人能進行通知 ISP 業者取下，著作權人如何認定等，建議未來可由第三方公正機構通知 ISP 業者相關盜版侵權之可能性，並告知其智財法上安全

港條款之權利義務，由業者自行判斷下架相關盜版影音，並適用相關免責規定。

第二節　《電信管理法》之修法建議

任何科技如果沒有特別強調可以使用於侵害著作權之行為，基於技術中立原則，應不能認為該科技構成侵害著作權。至於使用該等科技之人是否應負侵害著作權責任，應視使用者之使用行為而定[330]。為了平衡著作權保護與技術發展之間的法益，仍要回歸《著作權法》等相關規範，判斷行為人是否執行侵害著作權之行為，或是對於他人之侵害著作權行為予以幫助、引導或誘使。因此，建議於《電信管理法》第 65 條增訂「使用電信管制射頻器材有代理權、專利權、著作權爭議者，依有關法律之規定。」[331]

第三節　廣電三法之修法建議

通訊傳播相關產業並非單一產業，包括電信、網際網路接取、無線廣播、無線電視、有線電視、衛星電視，其中《廣播電視法》、《有線廣播電視法》及《衛星廣播電視法》合稱為「廣電三法」，主要以不同傳輸方式規範廣播和電視行業的運作、監管和內容管理（穀倉模式）。

隨著網際網路之發展，一個傳輸網路可以提供多個原本由不同產業所提供的服務。這使得不同產業得以跨越藩籬而進入其他產業之中，打破了垂直立法模式預設的界限。由於穀倉模式遭受衝擊，為因應匯流趨勢及調整立法模式，「水平架構」之理論及思維被提出[332]。NCC 於 2020 年 7

[330] 章忠信，開發或提供軟體或平台讓民眾免費上傳與下載盜版是否違法，http://www.copyrightnote.org/ArticleContent.aspx?ID=3&aid=1840

[331] 相關文字對應《電信管制射頻器材審驗管理辦法》第 22 條第 2 項第 8 款之文字。

[332] 江耀國. (2014). 論水平架構之通訊傳播法制革新—層級模式、馬來西亞及英國法制與臺灣之革新草案. 月旦法學雜誌, 214. http://lawdata.com.tw/tw/detail.aspx?no=204067

月 22 日公告《網際網路視聽服務法》草案，擬將透過網際網路提供視聽服務的事業納管。2021 年 9 月 30 日 NCC 宣布暫緩立法；2022 年 5 月 25 日 NCC 通過新版《網際網路視聽服務法》（草案），主軸為提升網際網路視聽服務健全環境、保障我國消費者權益，並帶動我國內容產業發展；本次草案新增網際網路視聽服務提供者經法院判決確定其提供之視訊內容違反《著作權法》，NCC 得針對多次侵權之業者糾正其相關不當營業行為之機制[333]。NCC 得命連線服務提供者、電信事業或設置公眾電信網路者拒絕該網際網路視聽服務提供者電信服務之請求及通信傳遞或為必要之處置[334]。

外界多數期待該草案能夠處理網際網路視聽之盜版問題，惟該草案基本上仍以網路上所衍生的問題為限，除網際網路視聽服務事業之營運及其提供之內容服務，仍應適用各該行為之法律，故侵害智慧財產權、著作權等盜版問題，仍須回歸《著作權法》處理。

但除此之外，或許可考量給予自願登記納管之業者予以主張「訊號竊盜」之法律地位。民事部分可參考《有線廣播電視法》第 54 條第 1 項之規定：「未經系統經營者同意，截取或接收系統播送之內容者，應補繳基本頻道收視費用，並負民事損害賠償責任。」明訂未經合法網際網路視聽服務提供者同意，截取或接收網際網路視聽服務提供者播送之內容或訊號者，應負一定之法律責任；刑事部分則可參照《電信法》第 56 條之規範，針對「意圖為自己或第三人不法之利益，未經網際網路視聽服務提供者同意，截取或接收網際網路視聽服務提供者播送之內容或訊號營利者」設有相關刑事處罰；或是要求連線服務提供者、電信事業或設置公眾電信

[333] NCC 通過「網際網路視聽服務法」草案架構，完整草案條文將於近期公布. (2022, May 25). 國家通訊傳播委員會新聞稿. https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=47561

[334] 國家通訊傳播委員會公布「網際網路視聽服務管理法」草案架構. (2022, May 30). 理律法律事務所. https://www.leeandli.com/TW/NewslettersDetail/6888.htm

網路者拒絕為侵權之網際網路視聽服務提供者電信服務之請求及通信傳遞或為必要之處置。

第四節　《電信管制射頻器材審驗管理辦法》之修法建議

一、 增訂回收機制之細節性規範

參考歐盟於《一般產品安全規則》新增產品召回程序。包括：

（一）通知

經營者及線上市場提供者若有蒐集客戶個人資料，應利用該資料進行召回和安全警告，或在其他適當的管道傳播清晰可見的召回或安全警告，確保通知至最廣泛的覆蓋範圍，包括：公司網站、社交媒體管道、通訊和零售門店，並在適當情況下，在大眾媒體和其他通訊管道進行公告。

（二）產品安全召回之補救措施

負責產品安全召回的經營者應向消費者提供有效、免費且及時的補救措施：包括：1.召回產品的修理；2.用同類型且至少具有相同價值和品質的安全替代品取代召回產品；3.適當退還召回產品的價值，前提是退款金額至少應等於消費者支付的價格；4.消費者自行維修、處置（向消費者提供必要的指示、免費的替換零件或軟體更新）。

如前所述，為使回收機制更有效率，可進一步參考歐盟相關規範將《電信管制射頻器材審驗管理辦法》第 23 條第 2 項之回收機制調整為「審驗證明經撤銷或廢止時，原取得審驗證明者、經授權使用審驗合格標籤或符合性聲明標籤者，應依主管機關指定期限回收已販賣之電信管制射頻器材或非隨插即用射頻模組（組件），**並應於大眾傳播媒體公告並以其他有效方式通知消費者，回收對價應適當、合理，**若他人權益因而受損，並應負損害賠償責任。」

第五節　通盤檢視數位產品之資安、個資規範

違法機上盒除了造成著作權侵害外，也形成資安、個資漏洞，對於使用者造成莫大威脅。故英國政府在打擊違法機上盒方面，也不斷呼籲民眾不要使用這些違法機上盒產品，以免造成個資外洩以及相關資安問題。

在數位時代下，許多聯網數位產品皆應具有相關資安及個資保護措施，以利民眾安心使用，許多國家也開始進行數位產品個資及資安之相關規範。例如：歐盟近期有對於具有數位元素的產品的資安進行監管的法案《資安韌性法》（草案）（Cyber Resilience Act）[335]加強了數位產品之資安規則，以確保更安全的硬體和軟體產品於市面上流通。該法案之目的有四，包括：1.確保製造商從設計和開發階段整個生命週期中，提升帶有數位元素產品的安全性；2.確保一致的資訊安全框架，促進硬體和軟體生產商的合規；3.提高具有數位元素的產品安全的透明度，以及 4.使企業和消費者能夠安全地使用具有數位元素的產品。

該法案除部分已有特殊規範之產品（例如：醫療器材、航空或汽車）範圍涵蓋所有具有數位元素的產品，因應不同等級風險的產品將有不同的安全要求，少數產品須接受第三方評估。所謂數位元素之產品，包括：「該設備或網絡（Network）預期或可預期直接連接或邏輯性地間接連接數據資料」。而該法案主要規範架構為：1.規定帶有數位元素的產品投放市場的規則，確保此類產品的資訊安全；2.具有數位元素的產品的設計、開發和生產的基本要求，以及與這些產品相關的運營商在資訊安全方面的義務；3.製造商為確保帶有數位元素的產品在整個生命週期內的資訊安全，需要制定漏洞處理流程的基本要求，以及運營商與這些流程相關義務；4.市場監督規則以及執法規則。製造商必須確保符合在歐盟市場提供數位

[335] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 .

產品的安全性要求，如：隱私及資料保護，製造商在發生資訊安全攻擊時，必須及時通報當局和消費者，並能夠快速應對事件。有鑑於國外立法趨勢，國內資安及個資主管機關也應通盤檢視所有關於數位產品之相關安全法規，建立清晰且明確的規範，有助於企業更有方向地投資於資訊安全與個人資料保護，並使消費者能更安心的使用所有聯網數位產品，接軌國際趨勢。同時建議可針對下列事項進行細部規定[336]：

一、 網路功能損害禁止

數位產品不可損害網路或其功能，也不可濫用網路資源，從而導致服務降級。

二、 隱私保護措施

數位產品包含確保使用者和訂閱者的個人資料和隱私受到保護之保障措施。設備製造商必須採取措施防止未經授權的訪問或傳輸消費者的個人數據。

三、 防止詐欺

數位產品支援某些功能以確保防止詐欺。設備製造商必須提供用戶身分驗證控制等功能，以最大限度地減少詐欺性電子支付和貨幣轉帳。

四、 軟體之合規性

需要確保數位產品和軟體組合後之合規性，該軟體才能載入數位產品。

[336] Directive 2014/53/EU, Sec. 3.

第九章 跨部會合作行政作為建議

第一節　遏止非法 OTT TV 機上盒流通販售之強化政府跨部會合作行政作為建議

一、 建立有效機上盒上架與下架流程，保護合法業者

機上盒非法侵權並非單一部會權責，涉及相關部會應建置有效事前審查、檢測上架，事中強化稽查、調查與受理檢舉機制，嚴格監督市場不法情事活動，並強化監管工作之行政檢查措施，避免不肖業者鑽漏洞，面對實際從事不法工作者，經發現屬實者，除依照法規予以裁罰之外，應建立一套有效配套措施，例如公告撤照之後的快速下架機制，與產業合作方針，以提升國內智慧財產保障，如圖 74。

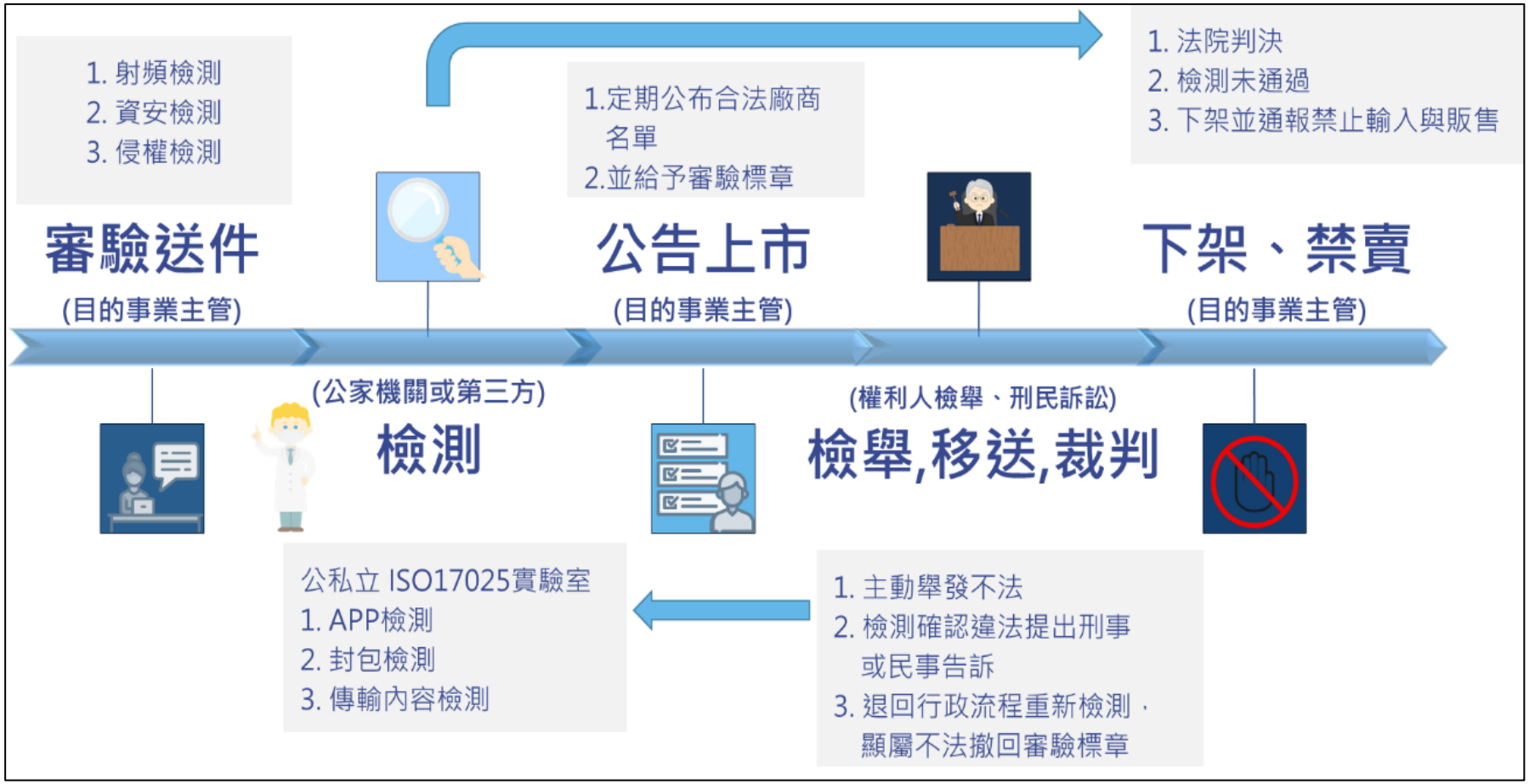

圖 74：本研究規劃之下架流程

資料來源：本研究整理

二、 成立跨部會協調機制並考量設置第三方機構專責

由於關於著作權之保護涉及各機關職權，以本研究案為例，由經濟部智財局為《著作權法》之主管機關、負責相關政策、法規、制度之研究、擬訂及執行事項等；由警政署負責受理關於著作權侵害之檢舉、刑事偵查等事項；NCC 則是負責關於機上盒設備之檢驗；TWNIC 則是負責 RPZ 治理機制、網域停止解析；數位部則負責資訊安全；國發會為《個人資料保護法》之主責機關；法院則負責核發扣押命令及裁判等，盤點可能涉及機關之權責如表 22。

表 22：違法機上盒可能涉及之各機關權責盤點

單位	所涉之相關權責
經濟部智財局	➢ 《著作權法》主管機關。 ➢ 智慧財產權政策、法規、制度之研究、擬訂及執行事項。
數位發展部	➢ 推動國家資通安全發展方案，落實資通安全管理法。 ➢ 確認通傳關鍵基礎設施提供者落實資安法遵、深化通傳資安情資分享。
國家發展委員會	➢ 《個人資料保護法》之主責機關。
內政部警政署	➢ 保安警察第二總隊刑事警察大隊執行保護智慧財產權工作。
國家通訊傳播委員會	➢ 通訊傳播系統及設備之審驗。 ➢ 違反通訊傳播相關法令事件之取締及處分。
文化部	➢ 電影、廣播、電視、流行音樂等產業之規劃、輔導、獎勵及推動。
法院	➢ 核發扣押命令。 ➢ 關於智慧財產之民事訴訟、刑事訴訟、行政訴訟及商業之民事訴訟與非訟事件審判事務。
TWNIC	➢ 統籌網域名稱註冊及 IP 位址發放。 ➢ 執行封鎖網域。

資料來源：本研究整理

由於網際網路之發展，間接助長網際網路侵權之狀況，透過機上盒觀看未授權之影音內容僅是網際網路著作權侵害之一種態樣，未透過機上盒之網路盜版影音在所多有，並非單一機關之權責，由於網路著作權侵害之各項事務涉及不同機關之權責，仍需要政府透過跨部會機制共同討論、處理。例如前述日本於 2019 年 10 月制定了「對抗網路上盜版的綜合對策和時間表」，就是透過日本內閣府、警察廳、總務省、法務省、外務省、文部科學省、經濟產業省等部會共同合作，依據機關執掌進行不同工作規劃，全面性的防治網路盜版侵權行為。

故短期可以成立跨部會工作小組，目前我國針對特定事務之成立跨部會小組之前例在所多有，通常由行政院主導，召集相關機關成立跨部會工作小組落實各項執法工作，完善網際網路著作權侵害之防治機制。

若要有效、快速且動態的解決網際網路所面臨之智慧財產侵害問題，並長期進行網際網路著作權侵害之防治，可考慮成立第三方機構專責協調合作及數位鑑定等相關事項，惟該專責機構須要有法令授權，方可發揮較大效益與功能。而相關機構之組成在我國也並非特例，例如依據兒少法第 46 條授權成立之 iWIN，即由國家通訊傳播委員會邀請各目的事業主管機關，如衛生福利部、教育部、文化部、內政部警政署及數發部等共同籌設，專責防止兒童及少年接觸有害其身心發展之網際網路內容。

以韓國為例，韓國著作權保護署（KCOPA）召集文化體育觀光部、通訊傳播委員會（KCC）、警政署、通訊審議委員會（KCSC），以及韓國三大網路服務供應商（ISP）包括韓國電信（KT）、LG 電信、SK 通訊等，成立跨部門工作小組，負責著作權保護政策的制定和執行、審查與著作權保護有關的事項以及實施著作權保護所需的項目。對應著作權侵權之作法，包括：主動分析著作權侵權資訊，並提出糾正建議（警告和刪除/停止傳輸請求等）和公私合作提供必要的資訊；同時也執行防止搜尋非法網

站和阻止廣告等任務，以消除盜版之利潤來源；並調查非法傳播韓流內容的海外網站，將相關資訊提供給著作權人等，透過規劃和監測行動應對新的國內外著作權侵權行為並調查和分析相關問題，透過這樣的機構建立集「預防→檢測→分析→行動」相關功能之推進系統[337]。

而本研究認為，若我國要建置專責處理著作權侵權之第三方機構，建議仍要透過《著作權法》授權，並可參考韓國做法，負責著作權侵權之相關資訊蒐集、數位鑑定、內容鑑識等，逐步建立防護網際網路盜版之防護網，如圖 75。

[337] https://www.kcopa.or.kr/lay1/S1T10C224/contents.do

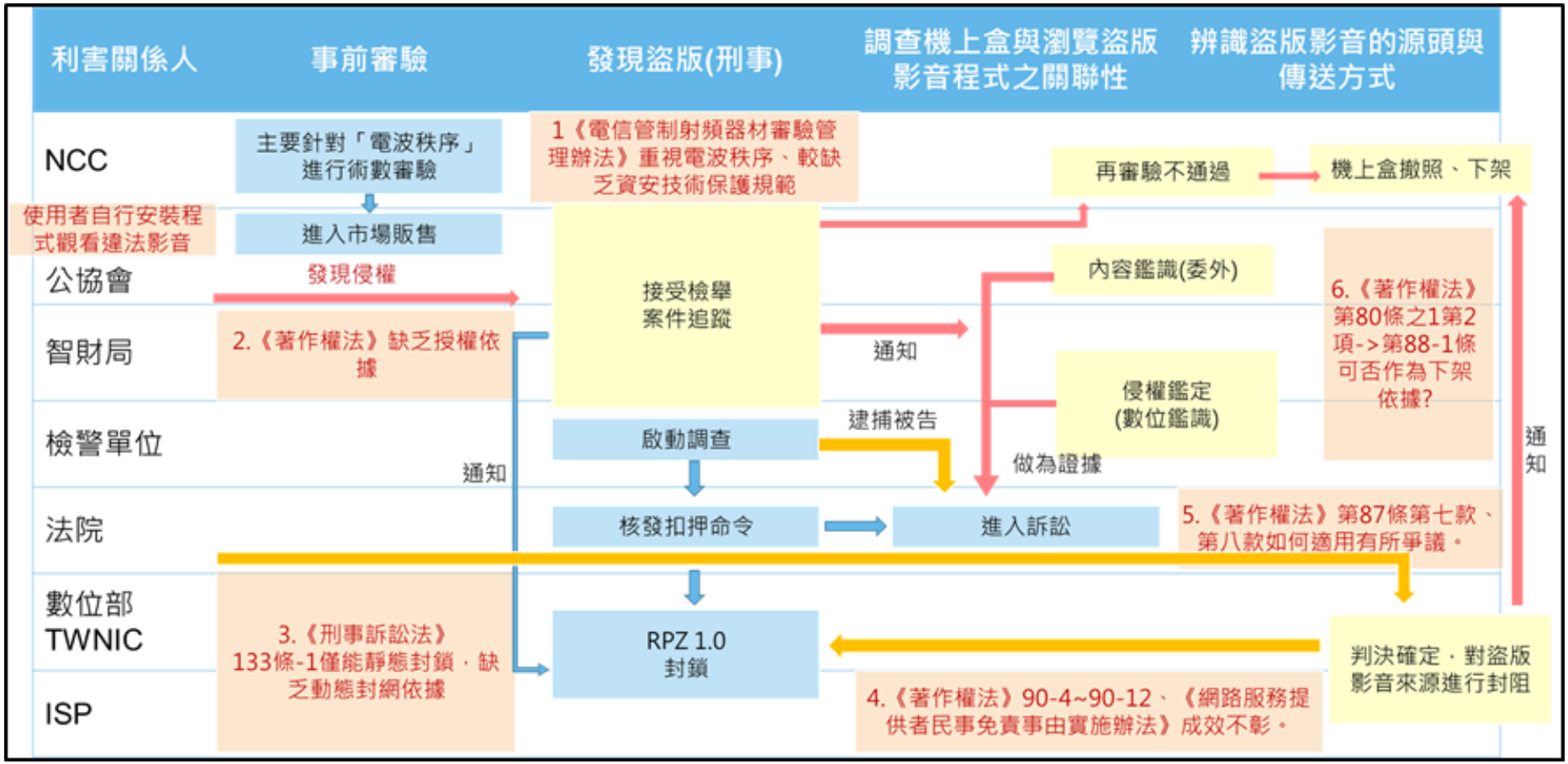

圖 75：本研究規劃之跨部會機制

資料來源：本研究整理

第二節　其他

一、借鏡國外 OTT 產業合作、國際合作打擊非法

（一）創意與娛樂聯盟

接續本報告第 16 頁，美國案例，產業合作（Industry collaboration）與國際合作，為影視娛樂產業採取之打擊侵權政策。

超過 50 家的媒體與娛樂公司，包含各大著名公司如 Apple TV+、迪士尼、Fox、Netflix、amazon、BBC studios 等共同組成的「創意與娛樂聯盟」（The Alliance for Creativity and Entertainment，ACE），在網站首頁標明其為：「世界領先的內容保護聯盟，致力於打擊危害蓬勃發展的數位生態系統的非法數位盜版行為。」[338]ACE 宣稱綜合採用三個方法來解決盜版問題：（1）與世界各地的刑事執法部門合作；（2）對大規模、以營利為目的之數位內容竊取行為，採取針對性的民事執法行動；（3）採用策略性溝通來阻止全球數位侵權[339]。其合作伙伴，包含美國政府之智慧財產權中心（National Intellectual Property Rights Coordination Center）[340]、美國貿易代表、司法部，也及於歐洲刑警組織、歐盟執委會和國際刑警[341]、美國國土安全部和新加坡政府[342]。此外，beIN Media Group、Cavea Plus、MBC Group、United Media、FIFA 及其他媒體行業利益相關者，也是合作對象[343]。ACE 關閉全球主要盜版網站，包括：Nitro IPTV、YMovies、SPARKS Group 以及在巴西、秘魯、北非和泰國等盜版網站[344]。在臺灣，ACE 也透

[338] ACE (2023 年)。ACE 致力于打击数字盗版 & 保护创意市场。Alliance Creativity and Entertainment。https://www.alliance4creativity.com/zh-CN/
[339] Id.
[340] National Intellectual Property Rights Coordination Center. (n.d.). Protecting Public Health and Safety. https://www.iprcenter.gov
[341] ACE (n.d.)。关于 ACE。https://www.alliance4creativity.com/zh-CN/about-us/
[342] Advanced Media Strategies LLC. (2023, January 4). 2022 Highlights US: Law Suits and Shut-Downs Are Weapons of Choice. DMCA Update in Progress. Piracy Monitor. https://piracymonitor.org/2022-usa/
[343] 同註 [338]
[344] 同註 [338]

過刑事訴訟使 8maple 的網路營運商被判刑，在新聞稿中，ACE 特別恭賀刑事警察局和桃園地檢署成功起訴、以及桃園地方法院「具有威攝力的判決」[345]，並稱：「對 8maple 的起訴是 ACE 與當地視訊產業和執法部門有效合作的另一個例子，它加強了我們減少盜版和保護全球創意內容法律生態系統的承諾。」[346]。同一新聞稿也指出：「在採取執法行動之前，域名 8maple.ru 每月吸引超過 3,000 萬次訪問，每月產生估計 400 萬新台幣（每月 133,000 美元）的廣告收入。當局還估計 8maple 網站給臺灣和國際娛樂業造成了 10 億新台幣（3,330 萬美元）的經濟損失。8maple 為了避免被臺灣當局發現，該網站在五個不同國家維護了 25 個伺服器：法國、烏克蘭、羅馬尼亞、美國和加拿大，該網站此前已在馬來西亞、澳大利亞和新加坡被屏蔽。」[347]由此可知，侵權網站可被多國使用者利用，營運者也會將伺服器設置在海外不同國家以逃避本國查緝，因此，國際合作實有必要，各國政府未必可以直接打擊營運商，需要其他國家協力合作採取相關屏蔽措施。

---

[345] 按本新聞稿所稱之判決為臺灣桃園地方法院 110 年度智易字第 2 號刑事判決，112 年 3 月 30 日。被告陳柏賢及莊坤憲，共同犯《著作權法》第九十二條之侵害著作財產權罪，各判處有期徒刑壹年陸月、有期徒刑壹年陸月。本案係經 Warner Bros. Entertainment Inc.（下稱華納兄弟娛樂公司）、Amazon Content Services LLC（下稱亞馬遜公司）、Disney Enterprises, Inc.（下稱迪士尼公司）、Paramount Pictures Corporation（下稱派拉蒙公司）、Columbia Pictures Industries,Inc.（下稱哥倫比亞公司）、Netflix Studios,LLC（下稱網飛公司）、Universal City Studio Production LLLP（下稱環球公司）、采昌國際多媒體股份有限公司（下稱采昌公司）、三立電視股份有限公司（下稱三立公司）、株式會社 WOWOW（下稱 WOWOW ）、日本電視放送網股份有限公司（下稱 NTV）、富士電視臺股份有限公司（下稱 Fuji TV）、株式會社 TBS 電視臺（下稱 TBS）、史坦利國際傳媒股份有限公司（下稱史坦利公司）訴由內政部警政署保安警察第二總隊、內政部警政署刑事警察局電信偵查大隊偵一隊報請臺灣桃園地方檢察署檢察官偵查起訴。

另刑事附帶民事訴訟，臺灣桃園地方法院 110 年度智重附民字第 6 號刑事判決，112 年 3 月 30 日，原告史坦利國際傳媒股份有限公司就：「女力報到-小資女上班記（第 1 集至第 50 集）」自製之視聽著作向被告陳柏賢、莊坤憲請求損害賠償，法院判決被告連帶給付原告金額為新臺幣肆拾貳萬伍仟元。

[346] ACE (2023 年)。台湾最大盗版网络的运营商面临 18 个月的监禁和近 2 万美元的没收。Alliance Creativity and Entertainment。https://www.alliance4creativity.com/zh-CN/news/operators-of-taiwans-largest-piracy-network-face-18-month-prison-term-and-confiscation-of-almost-usd-2-million/

[347] ACE. (2023, April 11). OPERATORS OF TAIWAN'S LARGEST PIRACY NETWORK FACE 18-MONTH PRISON TERM AND CONFISCATION OF ALMOST USD $2 MILLION. Alliance Creativity and Entertainment. https://www.alliance4creativity.com/news/operators-of-taiwans-largest-piracy-network-face-18-month-prison-term-and-confiscation-of-almost-usd-2-million/

（二）國際廣播公司反盜版聯盟

國際廣播公司反盜版聯盟（The International Broadcaster Coalition Against Piracy，IBCAP）也是一個在美國由主要廣播公司組成防止未經授權串流或非法傳播國際電視內容的產業聯盟[348]。他們同樣和美國與其他國家政府主管機關合作採取執法措施；也為了識別與阻止未經授權之影視內容傳播，和網路服務提供商（ISP）、支付處理代理、內容傳遞網路（Content Delivery Networks，CDN）、跨國科技公司以及硬體和軟體製造商合作[349]。

特別值得注意的是，IBCAP 所採取的「早期和頻繁的打擊行動」政策，透過「自動監控和打擊工具」，「結合 IBCAP 實驗室和法律團隊的專業知識」，使盜版服務的用戶體驗變差，而讓許多用戶轉向合法提供商，這是 IBCAP 對會員提供的重要服務[350]。例如：在今（2023）年 7 月印度板球超級聯賽 IPL 錦標賽期間，IBCAP 代表會員 Willow 和 Cricbuzz，分別在印度和美國設置人員，重點關注機上盒和 IPTV 服務、線性網路（Web linear）、社交媒體和行動應用，成功即時干擾了近 9000 個串流，其中 Facebook Live 串流的觀看次數被干擾了 360 多萬次。IBCAP 稱此次在社交媒體和移動應用上的打擊成功率是 100%！[351]

IBCAP 對會員提供了「完整且協調」的反侵害智慧財產權服務[352]，詳如表 3。由此可以觀察到，對未經授權傳播內容採取之干預手段，不僅是技術上對各種使用者接觸內容之管道，進行監控與偵測；也須採用法律手段對各種關係人發出濫用或下架通知；並透過各種私人或公開的管道

[348] IBCAP(n.d.).THE INTERNATIONAL BROADCASTER COALITION AGAINST PIRACY. IBCAP. https://www.ibcap.org/

[349] Id.

[350] IBCAP(2023, July 18).IBCAP Reports Major Disruption of Piracy in Indian Premier League 2023 Tournament Coverage. GlobeNewswire. https://www.globenewswire.com/en/news-release/2023/07/18/2706474/0/en/IBCAP-Reports-Major-Disruption-of-Piracy-in-Indian-Premier-League-2023-Tournament-Coverage.html

[351] Id.

[352] IBCAP(n.d.).Membership. https://www.ibcap.org/membership

進行調查、情報交換與蒐證。此外，為了主張權利，完成在美國的著作權登記，亦屬重要。同時，也需進行消費者與經銷商的反盜版宣導活動。以上各種服務，IBCAP 可以為會員客製化；且凡是內容所有人、傳播者、體育聯盟、權利人和其他需要反盜版保護的實體都可以成為會員[353]，如表 23。

表 23：IBCAP 會員服務

可提供之服務	包含的項目
監控和偵測(線性頻道)	機上盒（STBs） 網路（Web） 播放清單（Playlists） 行動應用程式（Mobile Apps） Kodi 附加元件（Kodi Add-ons）
監控和偵測（VOD 隨選視訊）	機上盒（STBs） 網路（Web） 行動應用程式（Mobile Apps）
監控與偵測(銷售與行銷領域)	網上零售（Amazon、eBay 等） 社交媒體（Facebook、Twitter 等）
執法	濫用通知（由 IBCAP 實驗室發送） 向 CDN、盜版服務發送下架通知（由律師發送） 向線上零售/社交媒體發送下架通知（由律師發送） 向支付處理器發送下架通知（由律師發送）[354]
調查	私家偵探購買機上盒 本地零售（實體店鋪）調查 開源情報（Open-source intelligence，OSINT）
政府/執法部門	代表 IBCAP 成員進行協調和轉介的好處
資料/情報	可以存取 IBCAP 資料庫、鑑識工作、零售商清單等
報告	美國串流媒體盜版概述 IBCAP 通訊 會員特定報告
訴訟支援	截圖、封包檔案、證詞等。

[353] IBCAP(n.d.).Membership. https://www.ibcap.org/membership

[354] 發送下架通知，主要是依據美國《著作權法》之相關規定，請參閱本報告「第二章第一節五、第二章第一節五、(一) 安全港條款及侵權通知、取下」頁 22 以下之說明。

可提供之服務	包含的項目
	購買機上盒/證據鏈鏈接。
著作權登記	將外國作品在美國著作權局進行登記
行銷	由 IBCAP 贊助的消費者和經銷商意識宣傳活動的好處 使用由 IBCAP 建立的行銷材料

資料來源：Membership. (n.d.). IBCAP. https://www.ibcap.org/membership

（三）建議我國模式

台灣模式也可循此方向建立業界聯盟和進行國際合作，列入打擊盜版的重要策略之一。以下是一些具體的建議和說明，可以用於台灣影視娛樂業者：

1. 建立業界聯盟：

(1) 確立聯盟目標：定義清晰的聯盟目標，例如減少盜版影響、保護智慧財產權、提升合法市場份額等。確保所有成員共享相同的核心價值觀。

(2) 吸引各方參與：積極邀請台灣的主要媒體和娛樂公司參與，包括製片公司、發行商、影視平台等。聯盟的實力取決於成員的多樣性和數量。

(3) 建立合作機制：創建工作小組，專門處理盜版問題，例如技術專家、法律專家、宣傳與宣導專家等。這些小組可以協同合作，制定具體的對策。

(4) 共同制定政策：創建聯盟政策，規範成員的行為和義務。這可能包括共同的監測標準、盜版行為應對程序等。

(5) 資源共享：進行資源共享，包括技術工具、法律資源、監測系統等。這可以幫助提高整個行業的打擊盜版的效率。

2. 國際合作：

(1) 建立國際聯絡點：在國際上建立合作的聯絡點，與其他國家的相關機構、業界聯盟進行積極的溝通。在美國、歐洲、亞洲等地設立代表處。

(2) 加入國際組織：台灣的業界可以考慮加入國際盜版打擊組織，例如國際電影影片協會（MPA）或相關的地區性組織。這樣可以取得更多的資源和合作機會。

(3) 舉辦國際會議：積極參與國際性的會議、研討會，分享經驗、學習先進國家的成功經驗，並拓展國際聯繫。

(4) 與國際執法機構合作：與國際刑警組織（Interpol）等執法機構合作，分享情報、共同打擊跨境盜版。

(5) 推動國際法律合作：與其他國家簽署合作協議，共同推動制定和修改有助於打擊盜版的法律。

(6) 參與國際案例：參與國際盜版案例，支援他國打擊盜版行為，建立良好的國際形象。

這些建議旨在促使業界共同行動，同時與國際社群合作，以全方位的方式打擊盜版問題。在執行上，需要密切注意法規要求，確保所有行動符合當地和國際法律。

二、 強化獎勵及大眾教育

接續本報告第 145 頁提及：非管制型之對策方案可依賴經費補助、獎勵、教育宣導、資訊提供、技術協助、價值訴求等等方式，鼓勵人民達成某項目標。參考國外之教育面相關做法，分述如下：

（一）大眾教育

韓國 KCOPA 除了前述針對著作權侵害之技術作法，也積極透過教育讓大眾認知影音內容、數位作品及軟體之著作權的重要性。主要作法包括：

1.向全國各機構之軟體負責人進行教育和諮詢，強化對軟體使用的著作權認識；2.透過教育諮詢，預防著作權糾紛，並創造正確的使用環境；3.透過教育諮詢診斷非法軟體侵害情況及改善使用環境;4.針對代表性的著作權侵權案例及類型進行說明、相關法令、懲罰條款；5.進行軟體管理及活用軟體檢查工具，提出有效的軟體資產管理指南。

KCOPA 所建立的著作權侵權防禦系統，不論音樂、影視、廣播、出版、遊戲、動畫與漫畫、軟體都涵蓋在保護傘下。且系統為廣布海外的韓流內容提供著作權保護支援，整體系統更為主動，也透過人工、自動化系統達成全面的著作權保護。

另外 KCOPA 也與韓國國內商業團體合作推動音樂作品權利保護，在網漫部分則與 KOCCA、Kakao、漫畫家協會商討倡議著作權保護作法。除了與不同產業公司單位合作，因應風靡國際的韓流，KCOPA 也陸續在泰國、越南、菲律賓等國家開設駐點辦公室，並透過 MOU、研討會與專題會議討論相關措施，以及倡議著作權保護。

KCOPA 目前所進行的措施大致分為兩類：預防侵權以及當侵權行為發生時所採取的行動。預防侵權措施包含：

1. 著作權知識流通與教育

在大眾教育的部分，KCOPA 以不同形式例如邀請專業人士拍攝影片，提供著作權保護相關知識。例如：網路漫畫形式，用幽默的表現形式與對白達到效果。如前所述，KCOPA 不定期舉辦展覽、研討會、發布著作權指南、邀請名人宣傳、社群廣告等向大眾教育著作權保護觀念。

2. 資訊公開

其他像是侵權救濟流程、著作權問答集、判決案例、法律諮詢也都在 KCOPA 網站上提供。另外也有企業著作權有關領域專業人員培訓課程。

（二）消費者意識宣導、專線服務

英國權利保護團體開始積極宣導因為收看盜版內容可能遭致之風險，包含詐欺、身分盜竊和惡意軟體或者參與到犯罪組織。例如：反著作權侵權聯盟 FACT 於 2021 年發起品牌的 Nothing In Life Is Free 活動，邀請明星、網路安全專家共同拍攝影片，向群眾解釋非法串流媒體所隱藏之風險。

英國智慧財產局透過網站公開宣導違法機上盒之危險性，包括說明為何民眾不應該購買這些裝置，理由包括：這些裝置通常缺乏家長控制，使用它們可能會讓兒童或年輕人接觸到露骨或年齡不適當的內容。從電氣安全的角度來看，部分裝置及其電源未通過歐盟安全標準，有可能對公眾構成真正的危險，導致使用場所發生火災。

另外，民眾若看到這些裝置正在出售，英國政府提供專線讓民眾匿名檢舉，他們會將此轉交給適當的組織進行調查，電話是 0800-555-111。

（三）其他做法建議

政府相關單位可透過多種獎勵的方式鼓勵民眾使用正版機上盒，同時拒絕購買盜版機上盒，以保障智慧財產權。包括：

1. **補助計畫**：推出補助計畫，對選擇正版機上盒的家庭提供一定金額的補助或折扣，鼓勵正版機上盒的購買。
2. **合法內容優先**：在公共機構、學校、社區中優先提供合法授權的影音內容，降低違法機上盒之使用誘因。

3. **資訊分享與互動**：建立正版機上盒使用者的社群平台，促進資訊分享和互動，並在社區中舉辦相應的社群活動，以增強使用正版的社會認同感。
4. **合法業者合作**：合法有線電視和網路提供商合作，共同推廣正版機上盒的優勢，例如高畫質、穩定服務、法律合規性等。
5. **資訊透明**：提供民眾易於理解的資訊，解釋使用盜版機上盒的風險和潛在後果。可透過官方網站、宣導手冊、和其他教育資源。
6. **合法服務優惠**：鼓勵業者提供使用合法機上盒的用戶一些特殊優惠，例如價格折扣、贈品、忠誠度點數特殊節目或高速網路服務等，以提高使用正版服務的動機。

透過以上方式，政府和合法業者可以共同努力，建立一個正面的環境，提升民眾對盜版機上盒風險的認知，進而鼓勵他們選擇合法、正版的機上盒或線上服務。

第十章 結論

第一節　法規面、執行面

長期以來，智慧財產權因為技術的進步而不斷受到影響，這些權利的傳達和交換方式隨著技術進步而不斷變化，包括：電話、錄音製品、電視、廣播和有線網路、衛星通訊、錄音機、光碟和網際網路等通訊技術，不斷對智慧財產權產生重大影響。而在本研究所討論之OTT TV 機上盒所產生之盜版問題，主要是因為消費者或觀眾不斷渴望透過免費方式存取電影和網路連續劇，對於觀看、尊重正版之意識薄弱，有龐大的需求驅動；再加上隨著技術進步，此類犯罪分子難以追蹤，虛擬私人網路（VPN）的發展更是加劇了追蹤難度，由於非法傳播成本低廉，而且無法分析和監控訪問盜版資訊的數量，導致線上盜版影片不斷增加，而並非單僅有非法機上盒所致。各國也積極針對相關網際網路盜版問題進行處理、規範，歸納本研究所觀測之國家，關於 OTT TV 機上盒之監管模式、法規、跨部會建議總結如下：

一、 監理模式

（一）事前監理

本模式以歐盟為主，由於 OTT TV 機上盒屬於《2014 年無線電設備指令》（RED）定義的無線電設備。該指令除了規範健康及安全要求、電磁相容性、無線電頻譜之有效使用、互操作性、獲得緊急服務以及無線電設備和軟體組合的合規性；同時也必須符合相關規範中，有關隱私及個人資料保護和防止詐欺措施、以及網路安全等規定。惟此規範主要仍是針對整體「無線電設備」而設，而非僅針對智慧財產權進行處理。

（二）需要執照才可以販賣機上盒設備

本模式以新加坡、中國為主，在該二國出售供當地使用的電信和無線電通信設備必須在主管機關進行設備註冊，業者須確保符合相關法規的相關標準/技術規格。另外，從事本地使用的電信設備進口和銷售的公司必須是持有有效電信經銷商許可證的設備供應商/經銷商許可證。故未取得許可證之業者不可在該二國任意銷售相關機上盒設備，因此管制上較為嚴格，一般民眾無法從合法經銷商購買非法機上盒商品。機上盒在我國雖屬電信管制射頻器材，但對於經銷商並無特別關於執照之規定，仍屬可以自由流通之商品，我國較難參照。

（三）處罰對於機上盒裝設破解合法串流技術軟體之行為

本模式主要透過《著作權法》規範關於破解智財保護之科技保護措施之產品或服務，主要國家之《著作權法》皆有規定。我國《著作權法》第 80-1 條、第 80-2 條皆有針對權利管理電子資訊及防盜拷措施進行規範。

二、 法規建議

針對 OTT TV 機上盒之智慧財產侵權之執法措施、程序、補救措施和制裁，本研究認為就法規面可再精進之處，如表 24。

表 24：本研究法規建議綜整

主要問題	建議修法方向
《著作權法》之修法建議	➢ 修訂《著作權法》第 87 條第 1 項第 8 款。 ➢ 確認 OTT TV 機上盒未經授權傳送「體育賽事」直播之違法性，或考量增訂鄰接權制度。 ➢ 研議扣押裁定之彈性。 ➢ 強化目前智財法中對於 ISP 業者之「安全港條款」之運用。 ➢ 授權第三方專責處理著作權侵害、數位鑑定等事宜。

《電信管理法》之修法建議	➢ 於《電信管理法》第 65 條增訂「使用電信管制射頻器材有代理權、專利權、著作權爭議者，依有關法律之規定。」
廣電三法之修法建議	➢ 於新版《網際網路視聽服務法》（草案）增訂針對多次侵權之業者得以糾正其相關不當營業行為之機制（可包括：下架、回收等）。 ➢ 民事部分可參考《有線廣播電視法》第 54 條第 1 項之規定：「未經系統經營者同意，截取或接收系統播送之內容者，應補繳基本頻道收視費用，並負民事損害賠償責任。」明訂未經合法網際網路視聽服務提供者同意，截取或接收網際網路視聽服務提供者播送之內容或訊號者，應負一定之法律責任。 ➢ 刑事部分則可參照《電信法》第 56 條之規範，針對「意圖為自己或第三人不法之利益，未經網際網路視聽服務提供者同意，截取或接收網際網路視聽服務提供者播送之內容或訊號營利者」設有相關刑事處罰；或是要求連線服務提供者、電信事業或設置公眾電信網路者拒絕該網際網路視聽服務提供者電信服務之請求及通信傳遞或為必要之處置。
《電信管制射頻器材審驗管理辦法》之修法建議	➢ 增訂回收機制之細節性規範。
通盤檢視數位產品之資安、個資規範	➢ 參考歐盟《資安韌性法》(草案)強化數位產品之資安規則，以確保更安全的硬體和軟體產品於市面上流通。國內資安及個資主管機關通盤檢視所有關於數位產品之相關安全法規，建立清晰且明確的規範。

資料來源：本研究整理

第二節　技術面

在技術面，本研究針對現今主要非法機上盒進行分析，並且將分析方法進行彙整，以供相關單位進行相關工作時參考，而作為以下用途：

一、 建立播放侵權影像 App 與機上盒關聯之事後審驗機制

科技日新月異，不法分子為意圖牟利，不斷演進犯罪手法，從最早會在機上盒中內建應用程式，到現在採用不先預載的形式，繞過現行事前審驗機制。而因為目前這些機上盒廠商，是以販售機上盒做為主要的營利來源，因此需要有技術去證明機上盒與播放侵權影像 App 之關聯性。

本研究透過檢驗市面上 3 款機上盒，發現：

1. 3 款款機上盒之播放侵權影像 App 均無預先下載，需透過指定網頁另外下載。
2. 3 款盒子均有認證機制，其中 B 牌及 C 牌機上盒可以直接解析網卡認證行為；A 牌機上盒則將認證資訊加密。
3. 3 款盒子均有可收看臺灣頻道之盜版功能。
4. 3 款盒子之影音網址均來自境外 IP Address，並將傳輸過程加密。
5. 3 款機上盒皆有透過主機，去鑑別機上盒是否為相對應產品的方法。

而本研究也透過中間人側錄的方法，去驗證這些機上盒是否搭配專屬綁定的侵權影音 App，做為證明專供機上盒侵權使用之憑據。

二、 追蹤來源以採取更進一步措施

環顧各國對於類似侵權影音行為做法，最雷厲風行就是快速、準確與動態偵測不法網路串流來源，透過阻斷、封鎖或減速流量，讓不法訊號消失或遞減其效能，避免劣幣驅逐良幣，不應讓瞟竊者甚囂塵上。

本研究在分析機上盒當中播放侵權影音 App 行為時，發現相關的認證主機與侵權影像資料的位置，該資訊可做為證據。除了於提交

法院審理時提高公信力之外，未來透過成立專責技術單位檢測不法訊號來源，並建立一套聯防機制，快速通報相關管理單位（例如數發部、臺灣網路資訊中心 TWNIC 或電信公司），消耗盜版者資源，讓網路治理發揮正確效果，進一步遏止不法流量形成另一股洗錢風氣，保障合法業者，不僅營造政府與民間互利環境，也提升我國之國際形象。

第三節　結語與展望

本計畫主要針對 OTT TV 機上盒，從法律與技術層面，研究監理的方法與作為，從而對我國現行制度進行建議。而法規與技術密不可分，法規訂定如果不考慮到技術可行性，則可能無法執行，而造成實際效益不彰的情況。就這部分來說，本計畫從落實法規的方向，從技術面找出支援法規執行的做法。從另一方面，也從技術面，從分析非法 OTT TV 機上盒的運作方式，去對法規面做出回饋，而提供建議做為參考。

目前我國對於非法機上盒是採用被動式偵測的做法，如要更進一步發揮效果，可以更進一步採取主動式防禦的方式。畢竟影音應用需要鄰近使用者，影像通常會置於國內網路服務業者的機房，若能向網路服務業者提出要求，以便利的搜查與封鎖方式來處理影音服務的委託需求，以便在侵權行為發生後，可以快速因應，即便侵權影音源頭來自國外，仍可發揮封鎖或禁止的效果，乃至於可以遏止侵權行為的發生。

展望未來，非法機上盒業者可能更加進化，甚至會採用不綁定機上盒的做法，也就是說，監理的對象不是針對「OTT TV 機上盒」，而是更進一步針對整體「OTT TV」。此時需透過官民合作，更快速地發現侵權行為，並且透過主動式防禦的做法，來加強因應措施的有效性。

然而，監理行為是兩面刃，可能造成箝制言論自由的爭議，故需要進行更進一步的研究，以擬定更細緻的規範。

附錄一 OTT TV 機上盒監理法規與技術座談會

第 1 場

- 本計畫第一場座談會已於 2023 年 07 月 31 日(一)14：00–16：00，假國立臺灣科技大學研揚大樓 TR-829 舉辦。
- 邀請來自產、官、學界專家，共七人與會。專家名單（依姓氏筆畫排列）如下：

  王翔正 副隊長 刑事警察局電信偵查大隊

  林宜柔 助理教授 中信金融管理學院科技金融研究所暨財經法律系

  紀博文 副教授 國立臺灣師範大學 資訊工程學系

  莊明雄 代理科長 刑事局科技研發科

  張友寧 主任檢察官 台北地檢署

  郭聯彬 法務組長 中華網路頻道事業協會

  陳依玫 秘書長 中華民國衛星廣播電視事業商業同業公會

  楊采文 律師 創拓國際法律事務所

第一節　　會議現場照片及簽到表


專利研究所


王翊正

【OTT TV 機上盒監理法規與技術之研究座談會第一場】 會議簽到表			
計畫編號：		會議日期：	112 年 7 月 31 日
主席：	查士朝老師/陳曉慧老師	地點/會議室：	臺科大 - 研揚大樓八樓 T829

姓　　名	簽　　名
中華民國衛星廣播電視事業商業同業公會 陳依玫 秘書長	
中華網路頻道事業協會 郭聯彬 法務組長	
台北地檢署 張友寧 主任檢察官	
刑事警察局 電信偵查大隊 王翔正 副隊長	
中信金融管理學院科技金融研究所暨財經法律系 林宜柔 助理教授	
創拓國際法律事務所 楊采文 律師	
國立臺灣師範大學 資訊工程學系 紀博文 副教授	

第二節　　摘要稿

陳依玫 秘書長發言：

- 本公會一步一腳印走了七年，期間已經提出了三十幾個訴訟案，但很不幸的，司法訴訟程序非常冗長，謝謝 NCC 委託貴單位來做這樣的研究案，然後就是希望能夠有快速停損。
- 本公會從第三代就開始提告，但沒有一個有定讞，也就是說沒有一個已經終審。但其實已經有很不容易的成果，就是我們在安 O 三、安 O 四的時候，已經在地方法院的一審有達到效果，就是機房這幾位嫌犯，被判一年以上的有期徒刑、不可以易科罰金。
- 中華電信機房裡面的機櫃有很多，機櫃裡面當然有各種各樣的業者，所以其實機櫃機房會也會是一個重點，一個出力重點。
- 查處的過程中有了解到，安 O 盒子他們是越做越狡詐，因為它的 DNA 就是要來犯罪的，所以它一定在境外。
- 安 O 現在它從安 O 六就開始採用話術，這個完全不合常情，如果是空的，為什麼會有消費者願意用四千塊買一個空的，作為一個安 O 盒子的製造商或業主，他甚至在臺灣都有光明正大的網頁，就是說我在網頁上，還可以回答非常多問題，你對我提出來的法律意見，他還有律師可以回答，所以我一切合法為什麼，因為盒子是空的。
- 法院上被告也提鑑識報告，他就說我這個是從沒有開封的，然後開封完之後，打開接上網，空的就沒有真的沒有東西就空的，我覺得這是我們研究案上，要幫助我們怎麼突破。
- 從安 O 六之後，它就不會預設內建在盒子裡，之前叫一鍵安裝，他現在就是在雲端服務，在 Google 買廣告，或者是透過他的合作對象，利用網紅開箱文的方式教觀眾，或者是經銷商提供小紙條，教購買機上盒的人，如何從雲端把這個 APK 抓下來 。但只有安 O 打得開，他本身就是犯罪工具，他是鑰匙，他就是開盜版倉庫的鑰匙 。現在更新版的 APK 改名叫 UPTV。
- 我覺得還是要回到 NCC 的盒子所謂的許可證發放的這個部分，有沒有可能因為這個可能在行政手段，他會比較快一點。另，我們應該在開箱文的第一頁，顯示 NCC 所許可的是射頻器，用一些白話，我許可的是電磁波，是

沒有溢波、符合安全標準，但你裡面所要下載的任何收視內容，必須要符合著作權。 NCC 的公告內容應該是針對這樣的觀眾，去告知他，你有這個法律的風險。

- 非法機上盒的話術，還有導致一個效果，就是經銷商就繼續賣，因為經銷商就說反正我們公會已經去函給各大通路商，每一次通知經銷商，經銷商他就踢皮球，他就說安 O 告訴我說他的盒子是空的。
- 安 O 確實是這幾年在盜版機上盒裡面最頭痛的，而且它的銷售情況真的是上百萬台，然後甚至真的造成了頻道的慘重損失，和所謂訂戶所謂的移轉，這都是因為它裡面的頻道一模一樣，還有它的關鍵，因為盒子裡面的使用行為跟有線電視一模一樣，它也是按遙控器也是頻道排列的方式。

陳曉慧 教授 回覆：

- 投影片第 31 頁，如果要加註就是收看著作權的問題，這個比較不是 NCC 的權限，不過我們會斟酌，因為如同剛剛講的，其實不是只有這個，還有色情等問題。
- 就是這個盒子是空的，然後如何透過特殊的綁定，變成一個犯罪工具，這件事情確實是可以再說明，然後剛剛那個判決，其實有認可過這件事情，那個判決在投影片 21 頁的左下角。

郭聯彬 法務組長發言：

- 其實這整個問題，是一個 OTT 影音侵權的問題，不是只有機上盒的問題，機上盒是整個侵權產業一個末端的終端裝置而已。
- 以往的安 O 盒子，的確在它的盒子裡面，使用了簡單的方式，你可以一點就把那個軟體裝進去。它現在為了迴避這個問題，它可能就透過網路教學的方式，讓它這個盒子真的是空的，所以今天你說這個盒子是一個非法機上盒，我其實不太贊成，我相信到時候這個東西在訴訟上，法官也很難說它是一個非法機上盒，因為它是一個中性的東西，它是透過跟違法的東西結合以後才變成違法。
- MAC number，就類似身分證號碼一樣，它認得你這個設備，所以我讓你這個設備可以讀，但是這個設備本身還是中性的，今天從非法機上盒的這個

角度，去切入這個問題，我覺得是比較不是正途，真正的正途還是它怎麼去做非法的公開傳輸這件事情。

- 研究案提了一個，我覺得是一個滿別出心裁的方法，利用射頻器材審議的行政作業的方式，迂迴的來讓這個業者無利可圖，我覺得這個想法是滿有創意的。然而，因為所謂射頻器材它的目的，它其實是通訊主管機關，在管理這些無線電發射的技術規範，它是在管理的這個技術有沒有可能電波太強、或者說傷害人健康的問題，它不是在管智慧財產權的，我們透過這個方法，來處罰智慧財產權的侵權，它其實就不是一個正途，這個東西很可能以後會受到挑戰，它可能也會有比如說違反法律保留原則的問題。
- 利用宣告機上盒廢止，這個方法的確有可能產生讓業者無利可圖的情況，但是我們不要期待消費者會乖乖的去按照我們想的方式去做，消費者他們都知道那是盜版的。這個方法的確有一定的可行性，但是我預想它最後會產生的就是，合法的經銷商不敢賣，因為要全額退費，他不會賣，因為他賣了會無利可圖。所以到時候一定是走入地下，你只能透過網路才買得到，然後你買得到然後退不了錢。我覺得非法的業者不會無利可圖，但是他的通路會減少很多，我相信這個方法會有一定的效果，但是不是根治。
- 真的要防，應該還是要從傳輸的地方來防，也就是封網的方式。原則上，今天我們要封這個非法影音的來源的話，就是找到它的機房在哪裡。其實最大的問題，就是我們有沒有辦法即時的去阻止這個非法的影音來傳遞，那你如果要等到判別確定，那一定是來不及的。
- 警政機關告訴電信業者，哪一些業者是非法的，他也可以擋的話，就可以達到類似的效果。如果要防止錯殺太多的話，其實可以配合一些監理的做法，在一定的條件下，要求業者來舉證他沒有侵權，只要有人檢舉你是侵權，你要證明你沒有侵權，否則我們把你封起來。

陳曉慧 教授 回覆：

- 我們這次要處理的是在投影片第 21 頁，就是這個機器本身，被特別寫了一個觀看的程式，這種特殊的專屬關係，來證明它是一個犯罪侵權工具。

- 我們現在講的是一個端的問題，當然封線絕對是有效的，否則不會歐洲他們都去發展即時封網技術，由警方去進行封網的 RPZ1.5 現在有法律上的所謂依據欠缺的爭議存在，這個問題它不是我們這個研究案的重點。

紀博文 副教授發言：

- 如果我開兩到三家公司，App 一家公司、安 O 盒子一家公司，可能請教一下，這樣子他們還有綁定的能力嗎。
- 我們說會在那個畫面上，放上本機上有沒有獲得許可字號，然後我們用經濟的方式去處理它，我剛剛想到一個對抗的方式，誰敢退貨，我就告誰。
- 三個月內可以退費，免費退費，某種程度也對盒子的廠商不公平，因為你還是看了三個月，反正我就說買什麼東西，一個月花錢，那我就每個月定時回去拿錢回來，我再買一台，一個月我再回去拿回來。
- 駭客組織會養很多的殭屍網路，而殭屍網路他們必須要聽令一個司令官，我們叫他做 CNC server，但是他們就會一直變。以目前來講即便在學界，我們也沒找到很好的方式，去封鎖 CNC server 的這件事情。封網技術目前成效依然不彰，沒有一個很好的方式，因為現在網路上電腦太多，域名也太多，所以我們越來越難透過一些 IP，或是 Domain name 的方式。
- 抓到某一個，這個到底是誰去申請的，這到底是誰擁有這個 IP 的位置，能不能用這個當作一個紀錄來說，來去究責那家公司呢。
- 曾經犯過錯或者是曾經被抓到過，那是不是那時候再請他，提供更多的證據去處理，真的還是要從源頭起，比較有道理，因為從機上盒的話，其實不管有沒有綁定或是什麼，就是很多那些盒子，我們都可以去 root 他 JB 他，或者是我就直接在燒其他的印象檔進去，這一類網路上的教學都很多。

陳曉慧 教授 回覆：

- 英國怎麼封，他們其實是有幾個標準，但是有些標準他們不講，為了講了以後就怕封網失效。
- 新加坡現在開始有，不算是動態封網，其實最大的目的還是從正常的管道，就讓他不容易取得這件事情，其實就讓盜版就可以消失掉很多，運用很多不同的管道，從一般的狀況增加這種盜版的難度。

莊明雄 代理科長發言：

- NCC 希望臺科大這邊用一個 ISO 的概念，去建立一個實驗室，去針對這個所謂的機上盒有一個檢測標準出來，有點像物聯網檢測標準，其實我們刑事局最近也在做這個，包含怎麼樣把那些 log 取出來。
- 事實上如果 iPhone 能夠做 NCC 的刑事審驗的話，那是不是機上盒也可以這麼做，我覺得這是一個概念。
- NCC 會找臺科大做的研究，是希望透過學界的整理，在端末這一邊看能不能做一些方法，我覺得我們可能封不住，可是起碼目前來講，在主管機關的部分，沒有太多配套的法令。
- 衛星公會跟所謂的頻道協會，你們都是被害人，我們現在的機上盒是一個網際網路的 Bus，可是我們現在的有線電視，是一個 Cable 的 Bus，他們的訊號不是靠網路傳的，是靠訊號傳的，所以我們臺灣在 OTT 這一塊蠻落後的，反而壞人的工具比我們好很多。很早以前臺灣很多山寨機，後來手機做得很好，沒有人要買山寨機，我相信那一天會來，不然就是有線電視，包含我們臺灣電視台都掰掰。
- 各位想的可能都是盜版的問題，可是我們在實務上看到，當盜版機上盒打開都是中央電視台，我說中國台北，其實某種程度上它是個統戰，機上盒是個統戰。
- 提供一個監理的技術，就是包含學校這邊，是不是有一些技術性的 SOP，我們不能說我這個研究，就是叫你 NCC 去跟智財局講，你法律技術都不好，或者是 NCC 去跟文化部講你就是文化涉管（涉及管轄），這次研究案，重點是強調監理的東西要加強。

張友寧 主任檢察官發言：

- 我個人也認為，機上盒應該是個中立的東西，基本上如果安 O 盒子，它是有一些綁定的功能，這個監理制度下去以後，它一定有辦法做到完全不用綁定。我們如果只把重心放在機上盒的管理，其實沒有辦法完全的解決問題，只能增加他們犯罪的成本而已。

- 我們這個案子討論的是有可能可以預載，或者說它在機器裡面有一些設備跟機制，讓這個程式可以自動下載，或者說綁定它機器的 Mac 之類的東西，然後再來做非法的影音傳輸。
- 檢查官的角度來講，可能就是怎麼查，或者說怎麼樣去增加他的犯罪成本。如果從收費的機制來做管理的話，我覺得比較容易阻斷他們的發展。然後帳戶要怎麼樣扣押，那當然這可能不是 NCC 要管的事情，辦案的人員，去處理他收錢的金流帳戶，他們會用賣斷式的方法，也是在規避這個，因為你訂閱之前會有固定帳戶會收錢，就會被查緝。
- 英國的方法，他是不是用詐欺，我覺得其實在國內有點困難，就是說以我們對詐欺罪構成要件的定義來講，你很難說因為他違反一定的標準，他就是詐欺。
- 動態封網的部分，目前的問題，還是在法規上的問題，因為現在如果是要透過刑事的手段去扣押的話，執法機關你透過刑事作法的規定，其實沒有辦法採取這樣的作法，它是個案式的，沒有辦法用同一個命令，去不斷的變更被扣押的標的，所以這個是會有一個問題，所以他的結論是建議要修法要明訂。另一項最大的問題是在於，法院怎麼接受這樣的一個東西。
- 關於機上盒的監理的部分，比較大的問題，是 App 跟盒子之間綁定的關係，因為這個不管是在民事訴訟或者是行政訴訟上，都是最核心的問題，舉證責任可不可以轉換的問題，但是，如果是以行政訴訟來處理舉證責任的問題，我想基本上會非常非常困難，因為我們刑事訴訟的架構，就是以國家就是舉證方唯一的這個舉證方。
- 很容易證明有盜版的盒子有 App，App 有綁定盒子，這個都可以證明，接下來被告到底有沒有知道這件事，被告到底有沒有參與這件事，他拆分成好幾個公司，軟體也拆分成好幾個公司，將來我們要怎麼證明彼此之間的關係，這個都很難。尤其是非法集團，分工化以後，然後再跨國，你就查不到，臺灣目前就是碰到這樣的問題。
- 除了審定合格的字號要告知以外，我們是不是配合政府其他單位，有些警語的加註能夠在法規裡面給予一個授權，盒子不可以使用盜版的內容物，至少你要告訴他這件事情，讓他知道說你這樣做是有危險的，多少增加一些用戶的警覺這樣子。

- 站在執法單位的角度來講，如果真的要告使用者的話，我們可能會受不了，應該會崩潰。
- 被告能夠拿出鑑識報告，當然檢查這邊也一定會拿出相對應的鑑識報告，也就是說所以我滿贊同，就是實驗室能夠建立一個研究的標準，因為有這樣的標準，我們能夠在 App 跟盒子綁定的關聯的建立上，能夠做出一個標準化的動作，然後產出標準化的鑑識報告，日後就比較容易說服法院，取得比較有利的結果。動態那邊，只要有法院的授權，我想要取得法院的支持，也會比較容易。

林宜柔 助理教授發言：

- 他們其實就是想要可以看到盜版的東西，所以他們才會去買這樣子的一個盒子。然而，我們不太可能就是一直不斷地去找這些使用者，然後找這些直接侵權行為人，來去處理他，因為那處理不完，而且那個數量真的很龐大。
- 機上盒有非侵權的功能的話，它就可以被認定為是中性的一個設備，所以你也很難從業者的這個部分來去處理著作權的問題。
- 著作權在處理上，我們不管是走訴訟的程序也好，然後或者是你要去做舉證這方面也好，我們這真的是漫漫長路或許可以從射頻法這邊來下去做修正。
- NCC 有沒有辦法可以有這樣子的一個行政裁量，然後針對這些合資的製造業者，或是 OTT 的這些業者，來去有更高的一個監理的權利，然後去做行政裁量。當把這個責任課予在業者上，就是當他們的使用者，會利用他們的平台或者是利用他們盒子來去做非法的事情的時候，或是侵權的行為的時候，那這些業者有義務要去做糾正。這樣可以互相分擔掉某一部分的風險跟責任。

陳曉慧 教授 回覆：

使用者有沒有侵權，就是如果你是 P2P，後面傳輸技術是 P2P 的話，本身就是一個點，那你可能就一定會有侵權的問題。可是現在直接是從雲端抓下來的，

有的國家確實也認為說，串流的暫時性重置仍然是一種重置，而美國的學者並不認為這種短暫看串流的重置，是屬於需要處罰的行為。

楊采文 律師發言：

- 是否可以透過這機上盒的一些取締，或是它審驗規範，去達到我們打擊違法內容或是下架的一些目的。如果我們要透過修改這個審驗規範，來達到我們想要達到的目的的話，其實我會建議就是做一個可以考量短長程的一個評估。
- 透過切結書的方式，來提升業者去確保，他們連取的內容是沒有違反著作權，或是沒有違反其他的智慧財產權的，如果透過切結書的內容的話，目前對應到的是審議辦法第 22 條第 3 項，如果有違反切結書聲明的內容，是可以先要求業者改正，然後之後改正不成，才會廢止。
- 如果未來修法的話，真的修了這個審議辦法，把它沒有通過 App，或是沒有通過這樣的一個遵循權限驗證的做法，列為它一個廢止或是撤銷的一個聲明的做法的話，那跟違反切結書的中間的關聯性會是什麼，我們可以了解一下，就是法規適用的一些基本的問題。
- 審議辦法，它原本是要規範電信的傳輸安全的，是禁止電波的干擾，那我們把這樣的一個附加的，譬如說資通安全、智慧財產權的考量，納入這樣的辦法裡面，會不會有違法跟明確性，可能也是另外的一些評估，那我們如果用切結書的方式來做，用業者自願承諾的方式。
- 現在未來可能就是裝置它是純潔的、純淨的、沒有任何綁定的一些問題。那還有到犯罪體系，它變成是產品製造者，跟經銷商還有它的推廣團隊是分開的。
- 如果它就算綁定了一個 App，那 App 當時檢驗的時候，我們說它是盜取訊號，或是連結到非法網站，但它當時給的網站是合法的呢，合法網站它已經取得授權，但授權之後中止了，或者是它之後變更增加它的內容，那你到時候要罰它，是要用它聲明不實，還是要用它跟原取一樣的樣品不符去罰它，那這也是一個基礎上需要考量的地方。
- 臺灣的回收體系，你可能認為就是產品安全，還有就是產品安全的譬如說就像是商品檢驗法，或是公路法有一些汽車召回的措施，那另外就是環保

體系有廢棄法，那所以我們在考量基礎上的回收體系的時候，其實可能要從刑事、行政跟民法下去重度考量。

- 行政程序，我們建議是譬如說專案查緝，然後販賣未經審驗合格 OTT 機上盒，是否直接用沒收的方式去處理。行政的部分，其實現在的汽車召回體系，為什麼我們今天採取是民法，就是消費關係的方式去做回收，而不是用行政的方式去督促，我們當然知道行政機關成本很高，然後環保署在廢棄處理這一塊，其實著墨很多。
- 製造跟經銷它有一個明確的一個分工，它是著作在經銷商要退費，可是因為今天的審議辦法，它的規範對象是申請人，申請人是製造商，或是它主要的臺灣的廠商，為什麼退費的機構會被規範到這個法律沒有規範到的經銷商，所以整個回收計畫的主體，應該還是申請人，只是申請人要如何辦理退費，這是它回收計畫的一部分，它還是最終的回收的責任業者。

陳曉慧 教授 回覆：

提到幾個角色，一個就是申請人，審驗證明的申請人，一個是審驗證明的被授權人，還有一個販賣者這樣，所以是有三個人，所以我們到時候再來看看，這個法律的部分的責任的建立的問題。

王翔正 副隊長發言：

- 關於公開傳輸或重置的問題，上法庭的抗辯大部分都是講說，我就是蒐集連結，我沒有公開傳輸，都可以抗辯說，我沒有做公開傳輸，因為公開傳輸是伺服器，不是我 App。
- 針對機上盒部分，當然我們在查緝的時候重要的是法源，他如果不預載，就不在於違法的侵權、不在違法的範圍裡面，就是構成要件是不符的，應該是要改成綁定或是專屬綁定，應該是把這個部分違法的先決的要件，先把它處理好。
- 我如何幫助 NCC 不去幫機上盒背書，為什麼 NCC 不能夠拒絕去幫機上盒背書呢，那當然是沒有辦法，因為它也是利用了就是 NCC 必須要去接受人民來申請審驗射頻設備。

- 瀏覽過去新聞的時候，發現 NCC 的撤照理由，那不合格的案件裡面，硬體性能檢驗不合技術規範，或者是認證標示不合格，針對可以看到這些侵權的內容的這些，為了維護設備器材的市場秩序，我覺得 NCC 它其實很勉強地在做這件事情，它其實沒有有力的立足點。
- 公佈訊息的這個畫面，就是我沒有辦法去連接 NCC 網站，那我就可以很明確地認定，這個就是不合我的技術審驗規範。如果你可以去連的話，NCC 一定可以跟民眾講，這個就是已經被撤照了。
- 用什麼理由去撤照，必須還是一樣回歸到著作權那部分，可能過程要修，就是說你要可能有專屬綁定，或是綁定之類的用語，我們可能前面要做技術審驗的時候，那我也要有一個法源。
- 怎麼樣去快速取得，證明這個傳輸的內容是違法的，我們說剛剛講到動態的那個阻擋的問題。它只要沒有達到審驗標準，然後沒有把那個字秀出來，我就認為你就違法，你就是不合規範。
- 第一個可能前面就是要去修《著作權法》，第二個管制辦法的部分，審驗辦法的部分，你必須要有一個法源，怎麼樣去認定這個審驗的內容，我只能要去針對這個標的，我能夠去認定他違法，我是依據本身的這個審驗標準的辦法，還是母法還是說其他的法規，那他也要有一個法源，他開機訊息的部分，當然就是我覺得可以幫助到第二點。

陳曉慧 教授 回覆：

英國作法，你如果使用非法機上盒，你的盒子就有很高的資安風險，然後會有讓色情甚至竊盜、洗錢等等的問題，當然如果後面還是 P2P 的話，毫無疑問的，就已經是一個侵權的問題。或許去強化從端點的這個器材的安全，會更加容易的去建立。

查士朝 教授發言：

- 我們知道它到底是怎麼樣子去做認證之後，我們其實就把認證的方式在 YouTube 上公布出去，大家都可以看違法的這個 App 之後，它就無利可圖，大家也不用花幾千塊買了，這個或許也是一種方式。

- 機上盒封網相對難度比臉書高一點 它動態在改的時候，幾乎很難去做封網，但是如果說是以這個我們能夠知道有問題，然後知道有哪些位置，如果說能夠未來提供一些形式。目前刑事機構在封網的時候，沒有一個標準。
- 我們在這個計劃裡面，第一個我們會做核心的部分，就是先把怎麼找到問題，問題的源頭先把它識別出來，到底哪個 App 有問題，或是哪一個這個機上盒有問題，我們先能夠做鑑識 我們也會跟法律的這個團隊共同來想，有沒有一些更好的一些方法。

第三節　逐字稿

各位專家可以從法規面、市場面跟技術面，提供我們進行後續研究的建議跟指正，謝謝大家，從陳秘書長開始。

陳依玫 秘書長發言：

今天報告資訊非常多、很充實，非常感謝研究團隊這麼認真跟用心，我也在沒有盡頭的隧道中看到了一線光明。我身為受害者，我們電視台每天花非常多的人力物力來製作內容，可是我們卻不斷的被盜版。這幾年，我們也很感謝警方跟檢方都非常努力打擊盜版，**本公會一步一腳印走了七年，期間已經提出了三十幾個訴訟案，但很不幸的，司法訴訟程序非常冗長**，他有一定要走的程序，確實是比較長。我們現在終於有看到、也很**謝謝 NCC 委託貴單位來做這樣的研究案，然後就是希望能夠有快速停損**。因為我們的受害已經發生了，就是要快速停損的效果。

然後，在這邊先跟大家致謝，由於這個盜版的業者，在現在數位匯流全媒體的環境之下，盜版的成本是非常低的，不論他在各種成本都比我們做正版的低很多，所以警察也很辛苦，檢方也很辛苦，我們做內容也很辛苦。我就先回來這邊，因為報告資訊很多，我希望能夠有正確理解，也分享一些我的看法。

第一個就我在技術面上的認知，我會建議這個研究案裡面，包括像第 10 頁、11 頁所提到的封網，我們可能要先釐清他封的是網站還是盒子裡面的那個 URL 或 IP 或網域。就我在技術面上的了解，我們臺灣最惡質的就是安 O 盒子，他從第三代已經產生到第十代到現在第十一代都出來。**本公會從第三代就開始提告**，三代、四代、五、六、七、八、九、十，我全部都有告，**但沒有一個有定讞，也就是說沒有一個已經終審。但其實已經有很不容易的成果，就是我們在安 O 三、安 O 四的時候，已經在地方法院的一審有達到效果，就是機房這幾位嫌犯，被判一年以上的有期徒刑、不可以易科罰金。**這結果當時就是空前的，真的很少見，之前我們訴訟就判三個月，然後五萬、六萬這樣子，我們都欲哭無淚。

我們有個節目被盜了三年，最近的判決一個節目賠十萬，十萬對於年製作費而言，連百分之幾都沒有。就我技術面的了解，就是盒子的 IP 第一層其實是假的，如果我們透過一些技術性技術的動作去跟網站其實是不一樣的，尤其是盒子他是不能走 Hinet。尤其他的服務量這麼大，一定會在近端就在地會有 CDN，所

以他一定會放在我們的機房，這個機房就是中華電信機房，**中華電信機房裡面的機櫃有很多，機櫃裡面當然有各種各樣的業者，所以其實機櫃機房會也會是一個重點，一個出力重點。**

首先，我們過去在這個**查處的過程中有了解到，安 O 盒子他們是越做越狡詐，因為它的 DNA 就是要來犯罪的，所以它一定在境外。**然後，它一定在機房做了很多層，它不會只有一層，所以可能那跟這個封網站是不太一樣，那我看起來這個好像有些資訊，比較是偏向於在處理網站。

第二點，想要提醒就是說，**安 O 現在它從安 O 六就開始採用話術，這個完全不合常情，如果是空的**，為什麼一個可以賣四千塊，**為什麼會有消費者願意用四千塊買一個空的**，就是說那當然這中間，業者有規避掉一些法律責任，就是說我今天**作為一個安 O 盒子的製造商或業主，他甚至在臺灣都有光明正大的網頁，就是說我在網頁上，還可以回答非常多問題，你對我提出來的法律意見，他還有律師可以回答，所以我一切合法為什麼，因為盒子是空的。**

然後我們在法庭上，我提供些資訊，我們最近在因為很多案件，我們已經從七年前就開始提告，很多案件一審完業者現在進入法院的二審的階段，**法院上被告也提鑑識報告，他就說我這個是從沒有開封的，**然後從開封也是找鑑識報告，**然後開封完之後，打開接上網，空的就沒有真的沒有東西就空的**，所以他說你不要再講我什麼盜版，問題是他現在就是有做了一個動作，**我覺得這是我們研究案上，要幫助我們怎麼突破**，實際上就我們在技術面的證明他不是空的。報告剛剛有一頁，就是說 MAC number 已經燒在他的盒子裡。他盒子本身，我講一個比較聽得懂的，就是說他今天有在本地端雇用了一些協助盜版的員工，他就去盜版訊號後，成立一個機房，通常我們警方能破的都是機房，然後機房一定要破，因為目前法院只認機房，然後機房破獲之後，他們就把這些訊號傳到境外的雲端之後，運用 APK。盜版 APK，過去叫 UBTV，而且**從安 O 六之後，它就不會預設內建在盒子裡，之前叫一鍵安裝，他現在就是在雲端服務，在 Google 買廣告，或者是透過他的合作對象，利用網紅開箱文的方式教觀眾，或者是經銷商提供小紙條，教購買機上盒的人，如何從雲端把這個 APK 抓下來**，抓到盒子裡面之後，因為這個 APK 是量身打造，他等於是一個存放贓物的倉庫，存放在境外的雲端，但是拉下來之後，今天我如果是其他盜版盒子，像是我們做過實際的測試，千尋、兔子都盜版，正版的也有很多機上盒，LINETV 也有盒子，我們都可以下載這個

UBTV 的這個 APK，**但只有安 O 打得開**，為什麼，因為只有他有鑰匙，這個鑰匙就已經在盒子裡面，就是剛剛講那個 MAC number，所以說他盒子怎麼會是空的，他的盒子本身就是一個犯罪工具，所以他盒子，他把等於導引到一個錯的方向，他盒子本身我們要去主張的，不是他空不空，而是**他本身就是犯罪工具，他是鑰匙，他就是開盜版倉庫的鑰匙，**只有他開得開，然後他現在因為在法院上，法院他被挑戰，法院就說，他現在就不承認，他說這個 UBTV 跟我這個盒子不相干，法官說沒有，你叫 Unblock 那個盒子，那你這個 UBTV 也叫 Unblock，就你家的他說好那我現在改名，所以他**現在更新版的 APK 叫 UPTV**，我也不曉得這個有這麼好騙，反正他現在法庭上已經有改說這個 UBTV 不是我生的，你沒有辦法證明 UBTV 就是，我也不知道接下來會怎樣，所以我的建議就是，這個部分我不曉得，我們用剛剛講這些，我們提供的這個技術建議，或者在法律上見解，有沒有辦法在法庭上，可以說服那個法官，或是說讓他們覺得很放心，就是不要被對方的話術所騙。

最後一點，投影片第 31 頁，**我覺得還是要回到 NCC 的盒子所謂的許可證發放的這個部分，有沒有可能因為這個可能在行政手段，他會比較快一點**，如果今天開機真的我覺得我也沒想到，確實開機畫面會有一個訊號訊息公布的畫面的話，是不是應該是要在開機畫面打開的時候，不是寫本盒子或許可，因為這樣反而誤導了。因為那個安 O 的業者，我們在 106 年，Google 隨便查詢，我們就查詢安 O 三還是安 O 四，輸入後馬上幾秒鐘就幾千筆的開箱文，其中有一個網紅，他就在開箱文裡面就是寫說，我這個就是 NCC 許可的，其實我們應該在開箱文的第一頁，顯示 **NCC 所許可的是射頻器**，用一些白話，我許可的是電磁波，是沒有溢波、符合安全標準，但你**裡面所要下載的任何收視內容，必須要符合著作權**。否則你看的人，因為就目前的法律，我不曉得請問專家就目前看起來法律上可以究責，目前觀看節目的人，我們不敢去究責他而已，今天其實要告要告黑人陳建州才對，因為盒子的廠商做了一個陷阱給陳建州，是陳建州自己下載 APK，我盒子是空的，我盒子是合法的，我覺得他們已經下了一個套給買盒子的人，我賣給你的時候是空的，是你陳建州下載了 UBTV 之後，看到了奧運，看到了海爾達的轉播內容，但是就是說目前好像只能這樣子，所以我們是不是 **NCC 的公告內容應該是針對這樣的觀眾，去告知他，你有這個法律的風險，**另外當然你今天盒子上，他有 Mac number 這件事情，我們可以在法律上怎麼主張，或怎麼樣在

技術上，讓他能夠被曝光。而不是在法庭上被他的話術所牽引，然後甚至於就是說，**因為他這個話術，還有導致一個效果，就是經銷商就繼續賣，因為經銷商就說反正我們公會已經去函給各大通路商**，很多次，就是說這個安 O 盒子我們其實也很節制，就是我只要必須要到警方破獲之後，或者是有這個起訴，我們破案記者會跟起訴的時候，判刑的時候，我們就公函去，不會說今天他 NCC 核准了一款 11、12 代，我就去函，我不是這樣子，我們一定有伴隨就是我承擔的叫司法責任，我提告，然後警方也破案了，然後也起訴了，或一審定讞了，我就**每一次通知經銷商，經銷商他就踢皮球，他就說安 O 告訴我說他的盒子是空的**，沒轍，沒有辦法做到剛剛講快速停損，就一直流血，所以就是說可能這幾個，幫我們可以解決一下，以上先這樣，謝謝。

陳曉慧 教授 回覆：

第一件事情，投影片第 31 頁，**如果要加註就是收看著作權的問題，這個比較不是 NCC 的權限，不過我們會斟酌，因為如同剛剛講的，其實不是只有這個，還有色情等問題**。

第二件事情，**就是這個盒子是空的，然後如何透過特殊的綁定，變成一個犯罪工具，這件事情確實是可以再說明，然後剛剛那個判決，其實有認可過這件事情，那個判決在投影片 21 頁的左下角**，非常感謝您剛剛提供了很多重點，讓我們都記下來。

郭聯彬 法務組長發言：

各位先進，我有一些可能還不太成熟的想法，可能跟這個研究案的想法也不太一樣，請各位參考、也請各位指教。首先，我看到這個主題覺得好像有點偏離正軌，**其實這整個問題，是一個 OTT 影音侵權的問題，不是只有機上盒的問題，機上盒是整個侵權產業一個末端的終端裝置而已**。整份報告裡面，其實研究裡面也有講到，他怎麼樣去擷取這些內容，然後怎麼樣建立機房，怎麼樣把這個東西傳出去，那機上盒其實是最後末端的那個終端裝置而已。

同樣身為受害人的業者協會，關於技術方面的理解，我跟陳秘書長不太一樣，因為我是贊成機上盒的確是空的，因為機上盒它其實就跟手機一樣。用手機舉例大家就很好理解，手機本來是中性的，今天它之所以可以看侵權內容，是因為那

個 App，App 是軟體，今天這個軟體沒有裝到硬體裡面，這個硬體真的就是空的。**以往的安 O 盒子**，的確在它的盒子裡面，使用了簡單的方式，**你可以一點就把那個軟體裝進去，那它現在為了迴避這個問題，它可能就透過網路教學的方式，讓它這個盒子真的是空的，所以今天你說這個盒子是一個非法機上盒，我其實不太贊成，我相信到時候這個東西在訴訟上，法官也很難說它是一個非法機上盒，因為它是一個中性的東西，它是透過跟違法的東西結合以後才變成違法**。

我想舉個例子，今天詐騙集團讓車手去拿錢，那這個車手騎了一台摩托車去拿錢，這台摩托車會變成他的犯罪工具，但是我們不能說這台機車是一台違法機車，它只是這個犯罪過程中，使用到一個東西而已，那今天這個安 O 盒子這個模式，它其實真的就把這個盒子做成一個很中性、很合法的狀態，那在技術方面，剛剛提到把 MAC number 燒進盒子裡，其實不是這個樣子的，因為 MAC number 是所有的聯網設備都有的，它是在那個聯網的晶片上。據我所知，它應該是在晶片設計的業者，生產晶片的時候就已經做上去的，不是機上盒的業者去做的。等於說，每一個聯網設備都有一個身分證，所以今天並不是那個 MAC number 有什麼特別，它就是一個中性的東西。只是以安 O 盒子來說，它會記錄它自己所有出廠的設備，有哪些 MAC number，然後它知道哪些是我的同志，所以它有辦法去辨認，哪一些盒子可以讀取我的非法內容，盒子本來是中性的。

我再舉一個例子，比如說悠遊卡，我們悠遊卡為什麼可以騎 UBIKE，因為每個悠遊卡都有一個獨特的 IP，然後今天你告訴 UBIKE 說，我這張卡我記了名，所以 UBIKE 就認得了你這張卡，其實它只是認得你這張卡而已，就好像你告訴它，你的身分證字號是多少，它就認你是會員一樣，所以這個 **MAC number，就類似身分證號碼一樣，它認得你這個設備，所以我讓你這個設備可以讀，但是這個設備本身還是中性的，今天從非法機上盒的這個角度，去切入這個問題，我覺得是比較不是正途，真正的正途還是它怎麼去做非法的公開傳輸這件事情。**

當然，這個老師出的題目，學生當然要照這個題目回答，題目說的是機上盒，當然這個研究案就是怎麼做機上盒，只是說這個機上盒去處理這個問題，其實是已經繞了一個彎，**尤其是研究案提了一個，我覺得是一個滿別出心裁的方法，利用射頻器材審議的行政作業的方式，迂迴的來讓這個業者無利可圖，我覺得這個想法是滿有創意的**，但是其實這個方式，我覺得可能在法律上會有點問題，如果今天我們在認定這個有沒有侵權這件事情，必須透過法律或者透過訴訟，緩不濟

急。然後，我們卻繞過這個訴訟的程序，讓行政的程序就可以去制裁它，這個其實可能會涉及法律保留原則違反的問題，或者是不當連結。因為**所謂射頻器材它的目的是什麼，它其實是通訊主管機關，在管理這些無線電發射的技術規範，它是在管理的這個技術有沒有可能電波太強、或者說傷害人健康的問題，它不是在管智慧財產權的，我們透過這個方法，來處罰智慧財產權的侵權，它其實就不是一個正途，這個東西很可能以後會受到挑戰，它可能也會有比如說違反法律保留原則的問題。**

就好像今天以前有一個社會新聞，檳榔西施穿的太辣，民眾反應要管，結果警察不知道怎麼管，因為法律沒有這項處罰，結果他就用這個檳榔攤非法佔用人行道，或非法佔用的這個規則來罰，其實他不是在罰檳榔西施，所以像這種方式都不是正途。我覺得今天我們如果真的要處理智慧財產權，還是要從智慧財產權的方式來處理，**剛剛提到利用宣告機上盒廢止，這個方法的確有可能產生讓業者無利可圖的情況，但是我們不要期待消費者會乖乖的去按照我們想的方式去做，消費者他們都知道那是盜版的，**那他為什麼要付錢，因為比較便宜，他付的錢還是比買正版的便宜，所以他會願意去做這個事情。有一個可能讓消費者會去做，讓業者無利可圖的事情就是，他還是會去買，可是他買了以後發現如果今天我可以全額退費的話，我就可以一直換，我第一代買了，然後退費，然後因為第一代會被廢止，第二代又會被廢止，所以我就買一次，然後一直換可以吃到飽。如果吃到飽的話，**業者的確無利可圖，所以從這個角度來說，這個方法的確有一定的可行性，但是我預想它最後會產生的就是，合法的經銷商不敢賣，因為要全額退費，他不會賣，因為他賣了會無利可圖，**然後因為他的上游不會讓他全額退費的，如果全額退費他也無利可圖，所以上游給下游一定不會讓他全額退費，這個零售商要允許你全額退費，除非他腦袋壞掉，**所以到時候一定是走入地下，你只能透過網路才買得到，然後你買得到然後退不了錢，**到時候一定是這樣子。就是說，今天我們不要把業者跟我們都想得很善意，大家都會唯利是圖，結果就會是這個樣子，所以這個東西我覺得會有一定程度的作用，就是到時候正牌的零售業者可能會不賣，比如說那個 PChome 或者是 Momo，他們一定不敢賣這個東西，因為可以全額退費，那上游不會讓他全額退費他也不會賣，所以到時候光華商場的長期經營的店家他也不會賣，會賣的就是那種隨時會落跑的，那觀眾買不買得到、還是買得到，但是只買得到那種會落跑的，到時候退不了費的，那會完全嚇阻嗎，

不會，**我覺得業者不會無利可圖，但是他的通路會減少很多，我相信這個方法會有一定的效果，但是不是根治。**

再來我想提比較正面的角度就是說，**真的要防，應該還是要從傳輸的地方來防，也就是封網的方式**。我是不太理解剛剛講說這個機上盒出去的網路跟網站有什麼不同，就我的理解，網域 IP 它都是一樣的東西，你封了網域封了 IP，連不到就是連不到，不管你是透過什麼裝置。所以**原則上，今天我們要封這個非法影音的來源的話，就是找到它的機房在哪裡**。在技術上，網域換來換去，有沒有辦法即時追蹤，這可能就要請比較懂技術的人員來解答，如果今天我們有辦法這樣跟著去綁的話，技術上，我們現在不管法律程序上的問題，技術上它應該是有辦法檔。我一個粗淺的想法，今天我買了一個機上盒，我放在家裡，或者我今天就是這個主管機關，我這個機上盒能夠連到哪裡，我有辦法監控的話，它連到哪裡我就擋哪裡，難道有那麼困難嗎，我不太確定，但是如果我今天有個機上盒，這個機上盒它總要知道有什麼網域，它才知道去哪邊拿非法的影音，那這個網域是什麼，這個機上盒上一定有，我覺得應該是有辦法查到，那這些東西我就全部封起來就好，那我們要怎麼樣及時擋，我覺得這個問題，其實大家討論了很久。**其實最大的問題，就是我們有沒有辦法即時的去阻止這個非法的影音來傳遞，那你如果要等到判別確定，那一定是來不及的**。那據我所知，目前警方有一些跟電信業者合作，去 block 掉一些詐騙的訊息，當警政機關告訴電信業者，這個是詐騙電話的時候，這個電信業者是可以配合把這些詐騙電話全部封掉，所以所有電話使用者，他不會收到這些詐騙的來源，只要被警政機關指定，如果用類似的思維，**警政機關告訴電信業者，哪一些業者是非法的，他也可以擋的話，就可以達到類似的效果**，這當然有舉證的問題，侵權可不可以做呢，說不定是可以思考的方向。

那另外就是，今天我們**如果要防止錯殺太多的話，其實可以配合一些監理的做法**，比如說我先講一個東西，舉證責任的問題，今天我們要證明這個內容是侵權的話，如果要由受侵害者來，那就比較麻煩，我們是不是可以**在一定的條件下，要求業者來舉證他沒有侵權**，那你全部的業者舉證可能是個太沉重的負擔，我現在出幾個想法：也許可以區分，比如說，今天你是登記有案的 OTT 業者，你就沒有這個問題，你就沒有舉證責任倒置的問題。但是如果你不是登記有案的業者，你是國外的網站營運者，你連公司在哪裡，我們都不知道的，對不起，臺灣不保護你，舉證責任在你，**只要有人檢舉你是侵權，你要證明你沒有侵權，否則我們**

把你封起來，技術上可以封的話，現在就是法律上，我們在法律上賦予比如說某一個機關有權利，通知電信業者把某一個業者封起來，那這個只要在科技上是做得到的話，我覺得是可以比較快，把侵權的東西擋住的，先到這裡，謝謝。

陳曉慧 教授 回覆：

第一件事情，關於 MAC 這件事情，請大家看一下投影片第 22 頁，就是這一次，我們其實並沒有打算要處理，就是當一個機器它其實就只是一個機器，然後大家要裝什麼都可以的狀況，它並不是這次要處理的。**我們這次要處理的是在投影片第 21 頁，就是這個機器本身，被特別寫了一個觀看的程式，這種特殊的專屬關係，來證明它是一個犯罪侵權工具**。

第二件事情，就是如同您剛剛所講的，其實**我們現在講的是一個端的問題，當然封線絕對是有效的，否則不會歐洲他們都去發展即時封網技術**，非常的有效這樣，因此臺灣的問題，其實是您剛剛提到的，**由警方去進行封網的 RPZ1.5 現在有法律上的所謂依據欠缺的爭議存在，這個問題它不是我們這個研究案的重點**，就要請您在這部分要諒解這樣子。

感謝您剛剛的建議，我們都會把它記下來，然後再做個回應。

陳依玫 秘書長發言：

我也回應一下，其實剛剛我的說明，我也滿贊成法務組長的說法，但是就是要釐清一下，就是說安 O 盒子，他就是剛剛老師講的，我們所在意的跟應該要究察的，就是他就是特定的綁定關係，他特別為了這個盒子，而這個盒子就是透過剛剛講的，就算這個 MAC number 不是盒子業者去燒，而是晶片的業者，但他確實也是透過這個 MAC number 的認識，就是套用剛剛法務組長講的話，他其實就是一個描述的說法，就是透過這個出廠的時候，已經認識了他這一批盒子，所以他才能打得開他自己做的綁定好的那個特製的 APK，所以我們還是認為應該是要在這個部分，因為這個部分而導致，當然他不認同，但我認為因此而這個盒子裡面的 MAC number，就是特定化，就是我們在 22 頁寫到，就是一般的機器要去安裝非法 App 的時候為了要跟你收錢的金流，也一定要綁你的 MAC，就是非綁不可能，沒錯，可是他並沒有去特製化一個盜版的 APK，所以拿手機來類比，

我是不能同意的，因為今天我買 ASUS iPhone，沒有綁定一個特定的盜版 APK，然後是用我的這個手機的 MAC number 可以打開的，這完全不成為一個類比。

郭聯彬 法務組長發言：

不好意思我可以再補充一下，剛剛也有提到韓國的案例，韓國案例我們很清楚看到，它的那個商業模式是廣告。商業模式是廣告的時候，在我們這個案子就完全無法解決了，因為它可以透過瀏覽器，透過自己下載的 App，它不是用機上盒的獲利模式，所以在這個案子就沒有辦法處理，那其實我蠻贊成。

就這個整個它的商業結構來說，它整個商業結構就是違法的，可是他很刻意的把機上盒切出來，讓它變得合法的外觀，那其實說我剛剛提到說，手機的類比不適用，其實我再補充一下，手機在什麼情況下可以適用，比如說今天它是一個侵權的 App，這個 App 它不是鎖安 O 的盒子，它同時也可能開放給手機用，你只要付了錢，你就把你的手機的 MAC number 傳給它，它就開放給你用，那這個手機就是違法手機嗎，我想不是這樣，所以今天用手機類比，是在強調它其實就是一個硬體而已，那今天這個違法業者，他要開放哪個裝置來看，他都是做得到的，他也可以開放給你手機看，他是可以的。

陳依玫 秘書長發言：

沒關係，我補充一下，就是說有一個叫，另外一種盒子，就是它的 App 不綁定它的盒子，但是那個盒子可能就賣很便宜就一兩千塊而已，可是安 O 從剛開始出來是五千多塊，綁了 PAD 加上車機，因為我有一次搭一個計程車司機告訴我，車機 PAD 加上他家電視上的 BOX 加起來八千塊，就一次買八千塊，那他這幾年因為競爭者多，所以他當然就降價。

我意思是說，因為**安 O 確實是這幾年在盜版機上盒裡面最頭痛的，而且它的銷售情況真的是上百萬台，然後甚至真的造成了頻道的慘重損失，和所謂訂戶所謂的移轉，這都是因為它裡面的頻道一模一樣，還有它的關鍵，**為什麼我們覺得網站跟盒子不一樣，是因為**盒子裡面的使用行為跟有線電視一模一樣，它也是按遙控器也是頻道排列的方式**，所以它確實對整個產業的，既有的正版產業的衝擊是非常大，所以安 O 它實際上就是剛剛講綁定的，所以今天另外一種，它就不是我們剛剛講的另外那一種，我不是一個 APK，然後你手機也可以用，哪裡也可以用，因此就說手機是盜版，不是這個意思，我拉回來來講，安 O 就是安 O，安 O 就是一個非常期待處理的議題，也不能說，因為剛剛那個邏輯，就不處理安 O 了，我覺得這樣子太可惜，因為回頭來講，我現在比較希望就是說，我們還是要來處理，市場上實際上已經發生，而且影響很慘重，不然因為我們不是坐在象牙塔裡面，我們今天做的這個研究，就是來解決問題的，問題最大，不好意思就是安 O，如果它這個模式很成功，而且還有它為什麼叫自產自銷，因為它才可以賣貴，牛自己養，盜版的網站倉庫自己做，所以它才能夠賣 4 千塊 5 千塊，別的盒子就用不了它自己做的 APK，所以它可以賣 4、5 千塊，其他的盒子不綁特定的，它就便宜，而且還有再講一個，警方破壞機房後，這個盒子就不見了，就是剛剛講的那個沒有自產自銷不是自己養牛的這一種盒子，它在市場上生命真的比較短暫，也比較容易在透過我們的這個犯罪打擊是比較容易消滅的，安 O 它從 3 已經到 10 我覺得這已經非常嚴重，就以上是我的想法，謝謝。

陳曉慧 教授 回覆：

謝謝兩位在技術上分別做了兩個闡述，既然這樣我想先邀請紀博文副教授來給我們一些建議。

紀博文 副教授發言：

好謝謝，先聲明我沒有買安 O 盒子，但是我剛剛第一次查了安 O 盒子，然後發現在柏克萊有在賣，而且它也真的在上面說了本盒子什麼都沒有，空的，但更好玩的是，它居然的敢在下面放一個廣告，說我們有完善的 CTN 你裡面是空的，你要 CTN 幹什麼，但是我要講一件事情，就是你要知道，做資安的都是壞人，我們就是要有壞人才會有警察，所以我其實剛剛一直在想，**如果我開兩到三家公司，App 一家公司、安 O 盒子一家公司**，然後剛剛說還是有一對一綁定，沒關係，對我就不綁定，我有兩三家公司，然後盒子我也開兩三家公司，我甚至還去稀釋他們的利潤，把它拆到四五家公司，不好意思，我不是法律專家，等一下**可能請教一下，這樣子他們還有綁定的能力嗎**，我覺得很好玩，可是以今天的這個，因為我們剛剛說，假設它是綁定的，這個是這個案子的前提。

然後，**我們說會在那個畫面上，放上本機上有沒有獲得許可字號，然後我們用經濟的方式去處理它，我剛剛想到一個對抗的方式，誰敢退貨，我就告誰**。因為剛剛我們說了要告的是黑人對吧，所以誰敢做這件事情，代表我是空的盒子，是誰去下載的，是使用者自己，所以你敢來退費，我就告你，這第一個恐嚇看有沒有用，因為理論上他被告坦白說收視戶也是活該，應該要被告的，但是如果我用這種方式，這個制裁還有沒有效果。

第二件事情，坦白說，假設我們今天不考慮被告的問題，可能大家有看過一些新聞，就是我買了，譬如說**三個月內可以退費，免費退費**，就有人真的我買了什麼東西，三個月，衣服穿了三個月覺得不合身，我真的拿去，我跟你講衣服大概是七天，但可能有一些東西有比較長，我就真的退了，可是這樣子，**某種程度也對盒子的廠商不公平，因為你還是看了三個月，反正我就譬如說買什麼東西，一個月花錢，那我就每個月定時回去拿錢回來，我再買一台，一個月我再回去拿回來所以這種經濟的導向**，是不是真的能夠阻止這件事情，其實我可能有一點點問號。

最後以技術的角度，我稍微回答一件事情，就是封網，其實我剛剛本來一直很期待聽到，就是英國超級聯賽到底是怎麼做的，然後我只聽到說他們有強大的技術，但是我沒聽到技術是什麼，不好意思，沒錯，但我先說那個很難抓。以目前我們在資安的世界裡頭，確實有一些駭客組織，我們先不要機上盒，**駭客組織的話，他們會養很多的殭屍網路，而殭屍網路他們必須要聽令一個司令官，我們**

叫他做 CNC server，那怎麼阻止他，很簡單的我們把 CNC server 封起來就對了，**但是他們就會一直變**，所以坦白說以目前來講即便在學界，**我們也沒找到很好的方式，去封鎖 CNC server 的這件事情**。

曾經我有一些朋友，他們在做相關的研究，但是研究的成果，**目前成效依然不彰**，沒有一個很好的方式，因為坦白說現在**網路上電腦太多，域名也太多**，長得亂七八糟的也很多，而且他們可能還是合法的，所以我們**越來越難透過一些 IP，或是 Domain name 的方式**，去說我說誰是壞人。但是，也許可以反過來說，就是假設我們真的**抓到某一個，這個到底是誰去申請的，這到底是誰擁有這個 IP 的位置，能不能用這個當作一個紀錄來說，來去究責那家公司呢**，就是我不是法律的專家，也許這還有其他法律的議題。譬如說我在四方電信我租了，然後有人真的查到我身上，就是你，你曾經被查過一次，資料是從這邊出來的，那當然可能只有那邊是壞的，但是以後我要做什麼事情，有沒有一個類似像 credit 的概念，如果我曾經做過壞事，那麼以後我在提供什麼服務的時候，我需要更多的去更多的去舉證，就是一般假設大家都是好人的話，那可能不用，但是如果你**曾經犯過錯或者是曾經被抓到過，那是不是那時候再請他，提供更多的證據去處理**，其實我滿贊同剛剛法務組長說的，真的**還是要從源頭起，比較有道理，因為你從機上盒的話**，其實不管有沒有綁定或是什麼，我講難聽一點，就是很多那些盒子，**我們都可以去 root 他 JB 他，或者是我就直接在燒其他的印象檔進去，這一類網路上的教學都很多**，那這些教學甚至還可以告訴你，剛剛你把 Mac address 燒在晶片裡，沒關係我這邊寫了一個軟體，模擬那個晶片讓你去讀它，你放到其他人可能也會做，而且坦白說這些教學，網路上還有那種，來我教你 Step by step 第一步、第二步、第三步，坦白說就是我們老師做的教學網站都沒有那些好了，我告訴你我曾經看過中過勒索，我有認識人中過勒索病毒，上面很完整的告訴你，比特幣是怎麼一回事，你要怎麼買，第一步、第二步、第三步、多國語系都有，我沒有看過比那個更好的，比特幣的教材，這個也是一樣其實現在叫人家破解盒子，然後教人家下載 APK 去安裝，去做各樣的手腳，其實網路上的資訊真的非常非常的多，所以其實我滿贊成，就是要管應該是從源頭開始管，在後面的那些，我剛剛也提出了一些，一些顧慮或者一些可能的攻擊的方式，目前還沒有比較好的一些解法，再請各位專家們指教，謝謝。

陳曉慧 教授 回覆：

我看一下就是他剛剛提到，就是**英國怎麼封，他們其實是有幾個標準，但是有些標準他們不講，為了講了以後就怕封**，所以有一些他們就不講，他們有公布一部分沒有多公布，這個部分我們會在後面的報告再補充。

第二件事情就是，剛剛有數位專家都提到就是說，這不是一個最有效的方法。但是事實上，之前就算英國他們在封網，還沒有做到動態封的時候，其實大家最重要的目的就是，包含**新加坡**現在開始有這種，也**不算是動態封網**，其實**最大的目的還是從正常的管道，就讓他不容易取得這件事情，其實就讓盜版就可以消失掉很多**，所以運用很多不同的管道，從這個一般的狀況增加這種盜版的難度，其實它還是有實際上的效用，大概是先暫時這樣子回答。

剛剛就是紀老師有提到，就是如果就是我透過分散很多家，不同家之後，那如何來認定綁定這件事情，莊科長這裡有什麼樣技術上的建議，或者覺得侵權者會怎麼樣來做這件事。

莊明雄 代理科長發言：

我先回頭來講一下我們這一次的研究案，其實是 NCC 派的，當然有蠻多專家認為說，你可能從端末，中端這邊處理效果不大，畢竟來講，其實我聽說在智財局跟文化部那邊也有類似研究，他們可能也會把問題丟到這邊來，所以我們應該要把大家拉回來，其實在這邊或許做的方法不是那麼精準，可是我們裡面也提到，在這個研究案裡面，**NCC 希望臺科大這邊用一個 ISO 的概念，去建立一個實驗室，去針對這個所謂的機上盒有一個檢測標準出來，這個有點像物聯網檢測標準，其實我們刑事局最近也在做這個，包含怎麼樣把那些 log 取出來**，投影片第 31 頁，這個概念應該從勒索軟體來的，為什麼這些綁架勒索軟體願意付錢，因為它的頁面就不能再看了，就一直在最上層，所以這個是不是在審驗的部分，未來要求他們要做這件事情。他們有這個概念，是因為最近那個 iMessage 最近不是很多詐騙信件，NCC 副主委做了一件很偉大的事情，他說只要你的 iPhone 裡面，沒有辦法過濾釣魚網站的釣魚簡訊，我就讓你在臺灣不能賣 iPhone，所以他們要求好像在 16 點幾的版本裡面要多出一個版本，upgrade 一個版本，for 臺灣或亞太地區，**事實上如果 iPhone 能夠做 NCC 的刑事審驗的話，那是不是機上盒也可以這麼做**，我覺得這是一個概念。

NCC 會找臺科大做的研究，是希望透過學界的整理，在端末這一邊看能不能做一些方法，我覺得我們可能封不住，可是起碼**目前來講，在主管機關的部分，沒有太多配套的法令**，那我們從學者專家這邊，現在也找到主任檢察官，看能不能找到一些想法。而且也不見得要照委託研究案去做，因為委託研究案在實務單位，我們單位也派過，可能十本裡面一兩本就參考了沒辦法做。所以這部分我覺得以學校來看，我今天看了一下，我覺得學校做得很好，所以這是我們覺得，應該大家要拉回來想，我們在監理技術這一塊能夠做什麼，那基本上另外一個部分，**衛星公會跟所謂的頻道協會，你們都是被害人，我們現在的機上盒是一個網際網路的 Bus，可是我們現在的有線電視，是一個 Cable 的 Bus，他們的訊號不是靠網路傳的，是靠訊號傳的，所以我們臺灣在 OTT 這一塊蠻落後的**，反而壞人的工具比我們好很多，那是不是透過相關的研究，能讓 NCC 對於這一塊或者是未來主管對這一塊，能夠有新的思維，或者產業還沒升級之前，我覺得這一塊是很難處理的。這跟山寨機的概念一樣，**很早以前臺灣很多山寨機，後來手機做得很好，沒有人要買山寨機，我相信那一天會來，不然就是有線電視你們全部都要掰掰，包含我們臺灣電視台都掰掰**。

所以我回頭來講一件事，**其實各位想的可能都是盜版的問題，可是我們在實務上看到，當盜版機上盒打開都是中央電視台，我說中國台北，其實某種程度上它是個統戰，機上盒是個統戰**，比如說它的首頁第一頁都是中央電視台，它的新聞都是，所以國安會顧立雄他特別開了四次會邀集國安單位去研究，怎麼樣打擊非法機上盒，我覺得這一塊如秘書長所講的，智財局應該也有類似的會，提供我們蒐證的報告。

陳依玫 秘書長發言：

他的頻道每天都在罵臺灣。

莊明雄 代理科長發言：

所以我們回頭，警政單位我算代表之一，以目前來看，我們應該想盡比較好的方法，**提供一個監理的技術**，就是包含學校這邊，**是不是有一些技術性的一個 SOP**，另外一部分法令的部分，就是說能不能在現有的法令部分，尤其在 NCC 的主政法，因為畢竟是 NCC 是主管機關，他委託我們研究，**我們不能說我這個研究，就是叫你 NCC 去跟智財局講，你法律技術都不好，或者是 NCC 去跟文化部講你就是文化涉管（涉及管轄）**，回頭來講，這次研究案，為什麼曉慧老師

一直在講監理的東西要加強，這部分是我覺得他整個研究是對的，以下我的建議到此，謝謝。

陳曉慧 教授 回覆：

謝謝科長，講了 **iPhone 的這個做法，有很好的建議**，接下來我想邀請就是主任檢察官這裡，不知道是不是從法律面上，還有您犯案的經驗給我們指導。

張友寧 主任檢察官發言：

其實我心裡還滿害怕的，因為這個部分，其實我覺得很大的問題是法律上的問題，其實剛剛的討論裡面有提到，機上盒綁定的問題，其實我滿贊同郭法務組長的這個意見，因為**我個人也認為，機上盒應該是個中立的東西，基本上如果安 O 盒子，它是有一些綁定的功能，這個監理制度下去以後，它一定有辦法做到完全不用綁定**，我們的法令永遠都是追在壞人的後面，查緝的手法也是一樣的，就是我們通常都是跟在被告的後面，成長的這樣，被告都一定跑得比我們快，所以在這個機上盒的管理上面，我覺得**我們如果只把重心放在機上盒的管理，其實沒有辦法完全的解決問題，只能增加他們犯罪的成本而已**，這個是我的第一個想法，尤其在看投影片跟提問報告，以及剛剛討論過程中，我都一直在想一個問題，**就是我們這個案子討論的是有可能可以預載，或者說它在機器裡面有一些設備跟機制，讓這個程式可以自動下載，或者說綁定它機器的 Mac 之類的東西，然後再來做非法的影音傳輸**，但是我在網路上，其實我今天來之前，我也在網路上 Google 一些 YouTuber 的介紹，他就在介紹我所謂的純淨版的機上盒，就是空的什麼都沒有，他就像剛剛那個紀老師講的，他就是一步一步的教你怎麼樣安裝軟體，怎麼樣綁定這個盒子，然後怎麼樣看，那開箱文就是在介紹這個，所以其實我會覺得，如果安 O 現在還不是這樣，那他其實應該算是落伍的，那因為效能小的，大概都是可以控的這樣，那接下來站在**檢查官的角度來講，可能就是怎麼查，或者說怎麼樣去增加他的犯罪成本**，那其實我覺得可以換另外一個角度講，就是除了這個剛剛講到的封網的技術以外，封網當然我們再來談，但是我覺得除了封網技術以外，因為他的收費，他一定會有一個收費機制，那**如果從收費的機制來做管理的話，我覺得比較容易阻斷他們的發展**，就是說就像詐欺集團，他一定要人頭帳戶一樣，他還會有一個你錢要匯進去的帳號，我的意思是說你針對那個帳號去

處理，就是透過英美的方法，應該說**英國的方法，他是不是用詐欺，我覺得其實在國內有點困難，就是說以我們對詐欺罪構成要件的定義來講，你很難說因為他違反一定的標準，他就是詐欺**，那但是不是洗錢，就是說他這個錢收進來，或者說他這個犯罪所得要怎麼沒收，**然後帳戶要怎麼樣扣押**，這個部分對於犯罪者的成本來講，我覺得是一個可以出發的角度，**那當然這可能不是 NCC 要管的事情**，就可能在這個研究計畫裡面沒有辦法去處理，但是我會建議，就是實際上在**辦案的人員，去處理他收錢的金流帳戶**，可能對於被告的傷害，以及後續犯罪的影響，查緝會比較有幫助，因為你扣掉他的犯罪所得，他短時間內他可能有一些傷害，他是零售的嗎，不是，如果他 OTT 他要裝軟體，或者是要收費的話，他可能會另外的，他只有賣盒子為止，只有賣盒子的話可能就沒辦法，安 O 是這樣，其他家都是這樣。（**陳依玫 秘書長：**他靠這樣賺翻了）其實我覺得**他們會用賣斷式的方法，也是在規避這個，因為你訂閱之前會有固定的帳戶會收錢，就會被查緝。**

接下來回來**動態封網**的部分，其實我也個人認為，這個是**目前比較可行的做法**，不過我在出來之前，我有查了一下，前一次我們高檢署的智慧財產權會報，就這個議題，智財局有提出一個提案，這邊大概跟各位稍微說明一下，當次會議的結論，就是說其實高檢署跟智財局那邊，在這個會報上面討論結論是認為說，**目前最大的問題，還是在法規上的問題**，因為**現在如果是要透過刑事的手段去扣押的話，執法機關你透過刑事作法的規定，其實沒有辦法採取這樣的作法，它是個案式的，沒有辦法用同一個命令，去不斷的變更被扣押的標的，**所以這個是會有一個問題，所以他的**結論是建議要修法要明訂**，那至於要修在哪裡，我想是可以考慮的。

動態封網的部分，這邊給各位的一個建議，我也基本上認為**動態封網最大的問題還是在於，法院怎麼接受這樣的一個東西**，其實技術上我覺得幾位老師也講得很清楚，你封什麼，其實我覺得你封 Domain Name 跟封 IP 其實差別沒有很大，因為你封 Domain Name 的話，它 IP 掛了你就擋掉，如果兩邊都封，那就是比較完整，我的想法是這樣。

關於機上盒的監理的部分，我覺得比較大的問題，就是說這個研究案，我建議一定要處理清楚的是怎麼樣去建構，這個 **App 跟盒子之間綁定的關係，因為這個不管是在民事訴訟或者是行政訴訟上，都是最核心的問題**，剛剛老師們有提到就是說，**舉證責任可不可以轉換的問題**，我想這個可能民事或者是行政訴訟上，

比較有可能達成。**但是，如果是以行政訴訟來處理舉證責任的問題，我想基本上會非常非常困難，因為我們刑事訴訟的架構，就是以國家就是舉證方唯一的這個舉證方**，負有完全的舉證責任，所以在刑事案件裡面，我們不可能不負責舉證，被告自己負有侵權而且他還知情這件事情，而這個其實是在我們一般刑事案件裡面最痛苦的問題。因為**客觀的形容，都很容易證明有盜版的盒子有 App，App 有綁定盒子，這個都可以證明，接下來被告到底有沒有知道這件事，被告到底有沒有參與這件事**，或者像紀老師提的更進一步，**他拆分成好幾個公司，軟體也拆分成好幾個公司，將來我們要怎麼證明彼此之間的關係，這個都很難**，因為其實詐欺集團的模式，就是長期被追溯以後，他慢慢發展出來，所以他就把稅房，收帳本，詐騙組，金主什麼，全部都拆開來，**分工化以後，然後再跨國，你就查不到，臺灣目前就是碰到這樣的問題**，這個我們真的是很困難，在臺灣的國際處境之下，要跟國際合作也有很大的困難，至於說 Mac 網卡，這個本身有沒有綁定，我想綁定是他們的一個機制，但是是不是只會綁網卡，其實我覺得倒不一定，因為從這個研究案，其實剛剛資料裡面也提到，比如說有 CPYD，因為只要這些東西是他可以掌握的，他自己建的資料庫，他就可以拿來綁定，**所以將來他要做，如果我們處理 Mac 綁定，他就會換其他的方式來綁定**，我會覺得這其實都只是，我們就是要 follow 他一直在改變我們的做法，我會覺得比較有意義的。

加註警語的部分，我也滿贊同，就是剛剛兩位被害人代表有提到的，這個警語其實不要告訴他，只有審定合格，其實我們如果能夠在辦法裡面增加，就是說**除了審定合格的字號要告知以外，我們是不是配合政府其他單位，有些警語的加註能夠在法規裡面給予一個授權**，這樣子的話，我們就可以在授權的網頁，警語的網頁裡面告訴他說，**盒子不可以使用盜版的內容物**，至少你要告訴他這件事情，讓他知道說你**這樣做是有危險的，多少增加一些用戶的警覺這樣子**。

至於告使用者這個部分，當然單純從法律的角度來講，使用者是下載的人，他也是實際上有看的人，好像應該是有法律責任，但是這個**站在執法單位的角度來講，如果真的要告使用者的話，我們可能會受不了，應該會崩潰**，如果只處理一個人，這個東西就是一樣，就像我今天處理黑人以後，別的人就會來告所有的使用者，就像早期有一陣子 P2P 下載，早年我們都沒處理，對不對，突然不知道哪一天有一個人，就想到了，然後就找了某個分局就來做，其實我在早期還在智財局的時候，我就碰過，當時我第一個做法，就是我先在程序上先刁難他，等到

把他都教會了，你就擋不住了，現在我們處理的智慧產權案件，大眾都是在告 P2P 下載，可是那個使用者，你就是看他一臉無辜，那很多人就是下載來看，那處理這個東西法律上我覺得是沒有問題，只是說我們政策上，是真的要這樣處理嗎，另外就是查緝機關負擔得了負擔不了的問題，對，檢查官有一點點小小的私心這樣。

陳依玫 秘書長發言：我覺得時機滿成熟的從黑人開始

張友寧 主任檢察官發言：

剛剛秘書長也提到就是說那個鑑識報告的部分，其實這就是舉證的問題，那我想這個，**被告能夠拿出鑑識報告，當然檢查這邊也一定會拿出相對應的鑑識報告，也就是說所以我滿贊同，就是實驗室能夠建立一個研究的標準，因為有這樣的標準，我們能夠在 App 跟盒子綁定的關聯的建立上，能夠做出一個標準化的動作，然後產出標準化的鑑識報告，日後就比較容易說服法院，取得比較有利的結果**。那我想鑑識報告如果做得夠完整的話，事實上在**動態那邊，只要有法院的授權，我想要取得法院的支持，也會比較容易**，那這個可能是我以上小小的建議，如果有的話，我們再另外跟各位報告，謝謝。

陳曉慧 教授 回覆：

謝謝檢察官給我們這麼多的指導，那接下來我想邀請林宜柔教授，是不是也從法律面上給予建議。

林宜柔 助理教授發言：

各位專家跟先進大家午安，有機會可以來參加這個活動，滿榮幸的。因為聽到很多平常沒有接觸到的一些經驗，那我有一點點小小的想法，想要跟大家來分享一下。其實在這之前，我對 OTT TV 機上盒的認識，其實最多就是 OVO，在 OVO 第一代出來的時候，就曾經他還在做群募的時候我就已經去買過了，然後我很討厭那家公司，因為他們客服做得很糟，我曾經問過一次問題，然後他們把那個放在他們內部的群信裡面，然後他們最高的 CTO，回信時他也講說又是一個 iOS 的使用者，然後想要用蘋果的角度，來看我們這個盒子，然後我從此以後

把它列為拒往，這是一個題外話。然後他們後來其實把他們的盒子改得就是完全不一樣，跟他們剛開始出來的時候。

陳依玫 秘書長：後來就被我們告了以後，就改成現在合法的，他原始版真的是盜版。

林宜柔 助理教授發言：

那現在因為大部分都是 Smart TV，所以我會覺得會去買這個盒子的使用者，基本上他們都是有特別的想法，就是**他們其實就是想要可以看到盜版的東西，所以他們才會去買這樣子的一個盒子。**要不然像我們就是用 Smart TV，或者是 MOD 也好，然後或者是我們其他這些合法的來源，我們都可以看得很愉快了，那當然我們先就著作權的部分，就也算有一點點回答。剛剛秘書長這邊提到的，的確就是我們直接侵權行為人，當然是使用者，剛剛那個主任檢察官這邊也有提到，可是**我們不太可能就是一直不斷地去找這些使用者，然後找這些直接侵權行為人，來去處理他，因為那處理不完，而且那個數量真的很龐大**，剛剛說到那個安 O 盒子賣了 100 萬台，那可能就有 100 萬個，或許就有 100 萬個這樣子一個侵權行為人。

可是吵了非常非常多年，等於是從上個世紀，吵到這個世紀，從美國的那個 Sony 跟 Universal Studio，開始在講的輔助侵權行為，或者是代理侵權行為這件事情，那他們又把它界定，就是從 Sony Doutring 裡面，又把它界定說只要這個設備，它是中性的，它有除了侵權以外其他的功能，它也不是說它完全就是沒有侵權的功能的話，**它只要它有非侵權的功能的話，它就可以被認定為是中性的一個設備，所以你也很難從業者的這個部分來去處理著作權的問題**。

第三個方面是，因為**著作權在處理上，我們不管是走訴訟的程序也好，然後或者是你要去做舉證這方面也好，我們這真的是漫漫長路**，然後而且處理的效率其實也沒有那麼的好，那當然就是曉慧老師她在那個簡報檔當中裡面已經有提到，**或許可以從射頻法這邊來下去做修正**，然後或許是像我們剛剛提到，那個警語的部分，因為我們現在去看電影它上面也都會，我們在看電影的前面，正片開始播放的時候，它也都會放那個警語告訴你說，你不可以做任何錄音錄影，或是拍照的行為，那這個部分的話，其實我認為在技術上不是很困難。

另外的話，就是我們的題目是監理，然後又講到英國他們在處理這方面，可能用反洗錢的那個方式，那我就有一個有趣的想法，因為監理這對金融業來講不是很陌生，金融業的話有他們所謂的監理科技，主管機關就是金管會他會要求這些金融業者，因為他們畢竟是特許的一個行業，然後去有高度的 compliance，就是法令遵循的一個責任，那反過頭來用在我們這一個產業的話，**NCC 有沒有辦法可以有這樣子的一個行政裁量，然後針對這些合資的製造業者，或是 OTT 的這些業者，來去有更高的一個監理的權利，然後去做行政裁量**，要求我們這些業者，來去做這方面的法令遵循，也就是說**當把這個責任課予在業者上，就是當他們的使用者，會利用他們的平台或者是利用他們盒子來去做非法的事情的時候，或是侵權的行為的時候，那這些業者有義務要去做糾正**，或是有義務要去發現這樣子一個事情，那這樣是不是層層下來的話，**可以互相分擔掉某一部分的風險跟責任**，那這樣子的話會不會侵權的行為反而會少一點，因為其實起碼我們現在看金融業的用這樣子的方式來去處理，打擊反洗錢是有一定的成效的，那用這樣子的東西反過頭來考的話，這其實是另外一個思考的角度，我幾點小小的分享，謝謝。

陳曉慧 教授 回覆：

非常謝謝林老師，就是剛剛有非常多的專家，有提到**使用者有沒有侵權**，這裡也跟各位分享一下，我目前的發現，就是**如果你是 P2P，後面的那個傳輸技術是 P2P 的話，本身就是一個點，那你可能就一定會有侵權的問題。可是現在的案子**，絕大部分不用 P2P 了，就是**它直接是從雲端抓下來的**，那在這個狀況下，你變成一個純粹接收串流的人，**有的國家確實也認為說，串流的暫時性重置仍然是一種重置**，就是我為了看串流，它會有短暫的重置，那個你還會構成重置。但是以美國的一些文章看起來，**美國的學者並不認為這種短暫看串流的重置，是屬於需要處罰的行為**，所以如果不是透過 P2P 的話，使用者會不會一直就構成侵權，我覺得這件事是還有討論的可能性，那這是第一個回答大家，就是我們現在的一個發現，對於這個法律的部分，不知道是不是也請這個楊律師這邊，給我們建議，謝謝。

楊采文 律師發言：

感謝各位專家學者剛剛熱烈的討論，我這邊只是稍稍補充比較技術性的一些說明。首先，我必須要釐清，因為今天我們討論的是機上盒的問題，那**是否可以透過這機上盒的一些取締，或是它審驗規範，去達到我們打擊違法內容或是下架的一些目的**。那必須就是要進行一些成本效益的評估。那我們當然了解，其實機上盒這件事情，只能打擊到一些願意在臺灣生存的合法業者，我們沒有辦法就是根絕所有任何從海外進來的一些境外，他們就是一些產品平時出入到臺灣的業者，那所以如果繼續在這個架構之下，願意達到我們這個目標的話，我們才有去討論的一些可行性。那我們也必須要了解就是，其實 NCC 的說法它有一定的時程，那**如果我們要透過修改這個審驗規範，來達到我們想要達到的目的的話，其實我會建議就是計畫團隊，做一個可以考量短長程的一個評估**。

先前 NCC 的新聞報導，裡面有提到說，它想要**先透過切結書的方式，來提升業者去確保，他們連取的內容是沒有違反著作權，或是沒有違反其他的智慧財產權的，那如果透過切結書的內容的話，目前對應到的是審議辦法第 22 條第 3 項，那如果有違反切結書聲明的內容的話，是可以先要求業者改正，然後之後改正不成，才會廢止**，那所以這邊我們也可以考慮到，**如果未來修法的話，真的修了這個審議辦法，把它沒有通過 App，或是沒有通過這樣的一個遵循權限驗證的做法，列為它一個廢止或是撤銷的一個聲明**的做法的話，**那跟違反切結書的中間的關聯性會是什麼**，我們可以了解一下，就是法規適用的一些基本的問題。

我們也了解到其實現在，我們把它定在審議辦法裡面，會有一個限制，也就是**這個審議辦法，它原本是要規範電信的傳輸安全的，它其實是禁止電波的干擾，那我們把這樣的一個附加的，譬如說資通安全、智慧財產權的考量，納入這樣的一個辦法裡面，會不會有違法跟明確性，那可能也是另外的一些評估**，那當然我們**如果用切結書的方式來做，用業者自願承諾的方式**，會不會比較是一個柔軟的手段，那可能也是一個考慮的方式，

另外技術團隊是比較著重在用 App 綁定特殊的那個代碼來開通，然後去做它的一個驗證方式，因為技術它變遷很快速，我們也必須考量到，**現在未來可能就是裝置它是純潔的、純淨的、沒有任何綁定的一些問題**。那還有到**犯罪體系，它變成是產品製造者，跟經銷商還有它的推廣團隊是分開的**。我們是不是還可以去證明，它有一個綁定的功能，或是它是不是還有一個 App 的存在，那都可能是會影響到，我們要怎麼去做這個檢驗，或是透過這個檢驗，去排除非法機上盒的

一個做法的適當性。那另外還有一個就是，**如果它就算綁定了一個 App，那 App 當時檢驗的時候，我們說它是盜取訊號，或是連結到非法網站，但它當時給你的網站是合法的呢**，它如果就算沒有盜取訊號，然後給你一個合法網站它已經取得授權，**但授權之後中止了，或者是它之後變更增加它的內容，那你到時候要罰它，是要用它聲明不實，還是要用它跟原取一樣的樣品不符去罰它**，那這也是一個基礎上需要考量的地方。

那另外就是**臺灣的回收體系**，你可能認為就是產品安全，還有就是產品安全的譬如說就像是**商品檢驗法**，或是公路法有一些**汽車召回的措施**，那另外就是**環保體系有廢棄法**，那所以我們在**考量基礎上的回收體系的時候，其實可能要從刑事、行政跟民法下去重度考量**。

刑事的部分，因為在場有檢察官在，我們不便表示意見，我們當然了解，如果起訴就是一般的客人的話，其實大家早些時候的同業會很容易互相告，那我們法律負擔很大，尤其刑事程序的浪費是公帑，那我們也知道檢察官壓力會變很大，所以我們**行政程序，我們建議是譬如說專案查緝，然後販賣未經審驗合格 OTT 機上盒，是否直接用沒收的方式去處理。**

行政的部分，其實**現在的汽車召回體系**，可能可以考慮一下，我們今天可能要解釋一下，**為什麼我們今天採取是民法，就是消費關係的方式去做回收，而不是用行政的方式去督促，我們當然知道行政機關成本很高，然後環保署在廢棄處理這一塊，其實著墨很多**，但廢棄這一塊，它譬如說廢棄的電池，或是車輛的這些回收機制，它會有一個回收基金來處理，當業者執行不能，業者必須先提繳、提撥部分他們的銷售，然後之後用這筆基金來去回填，他們日後需要由機關代執行的費用，其實**在汽車召回的體系，在商品經營體系，它還有一個回報的進度**，你必須在回報的時候，你必須先跟主管機關，申報你每月的銷售量，然後之後回報的時候，你要說如果機關讓你去召回，你就要跟他講你的執行率多高。如果不高，沒有超過九成，或機關約定比例的話，你就要提供改善計畫，這是可能可以相互配合的機制。

另外這邊我看到還有一個小小的疑慮是，因為我們**現在製造跟經銷它有一個明確的一個分工**，我們剛剛看到計畫團隊，它是著作在**經銷商要退費，可是因為今天的審議辦法，它的規範對象是申請人，申請人是製造商，或是它主要的臺灣的廠商，為什麼退費的機構會被規範到這個法律沒有規範到的經銷商，所以整個**

回收計畫的主體，應該還是申請人，只是申請人要如何辦理退費，這是它回收計畫的一部分，它還是最終的回收的責任業者，好，這邊是我簡單的一些評論，謝謝大家。

陳曉慧 教授 回覆：

謝謝楊律師，在這個辦法裡面，其實是有**提到幾個角色，一個就是申請人，審驗證明的申請人，一個是審驗證明的被授權人，還有一個販賣者這樣**，所以是有三個人，所以我們到時候再來看看，這個法律的部分的責任的建立的問題。

最後其實我想要請教一下，就是行政警察局的王副隊長，因為現在看起來就是如同剛剛很多專家跟楊律師所提到，就是他們都是一個分工的狀態，從這個生產、製造、銷售，這樣的一個分工的狀態，然後會不會很不容易去調查跟認定，就是我們所說的綁定?所以我們今天所提供的這個措施，會不會很容易就被逃脫?

王翔正 副隊長發言：

兩位主持人，各位先進大家好。我這邊想要談的，也是剛剛主持人講的，我們在查緝這類案件的困難點，其實一開始我們不管是針對機上盒或者是 App 來講，我們大概都會遇到修法前的一個問題，**就是想到公開傳輸或重置的問題，上法庭的抗辯大部分都是講說，我就是蒐集連結，我沒有公開傳輸**，就算是 App，那有影像從伺服器傳到我 App 上面去看，我用 App 來看，**都可以抗辯說，我沒有做公開傳輸，因為公開傳輸是伺服器，不是我 App。**

當然現在修法之後，也有針對這部分去修，但是無論他怎麼修，犯罪者就怎麼去規避他。現在我們再回來**針對機上盒部分**，我覺得第一個部分，當然**我們在查緝的時候重要的是法源**，所以我第一個想提的就是說，在 87 條第一項第八款裡面講到說，宅有這個部分，就是宅有侵權的程式，當然我們原先要攻擊的標的，是講說他如果有預載，那結果現在說沒有預載，那如果他沒有，等於說他**如果不預載，就不在於違法的侵權、不在違法的範圍裡面，就是構成要件是不符的**，那我覺得第一個部分，我們是應該要針對這個部分，**應該是要改成綁定或是專屬綁定，應該是把這個部分違法的先決的要件，先把它處理好。**

再來的話，我才會回歸到說，我們今天要討論，我覺得我白話去理解，我個人理解不知道對不對，因為這是 NCC 委託案，那 NCC 其實它在針對這個機上盒

部分，其實它的工具很少，那在我理解我看起來感覺像是說，**我如何幫助 NCC 不去幫機上盒背書**，那我會覺得是這樣，因為我一開始的疑惑也是這樣，就之前在討論這個問題的時候，**為什麼 NCC 不能夠拒絕去幫機上盒背書呢，那當然是沒有辦法，因為它也是利用了就是 NCC 必須要去接受人民來申請審驗射頻設備，**這個沒有辦法，NCC 沒有辦法去拒絕，你只要是機上盒，我就不接受你審驗。

那在這個狀況下，我們的研究人員很好，又想到了，是不是在前面能夠加上警語那這個部分，我就想到技術上是有一個問題，就是說，當然我可以要求你要去連結 NCC 網站，但是我只要下載了程式之後，我可以把它改掉，但是事實上，這樣也不是完全沒有幫助。我想到的另外一個部分就是說，縱使它後面去改，但是沒關係，我第一次開機還是看得到，那看得到的狀況下，就可以幫助到我去做射頻審驗，你有沒有照我的審驗規範，去做了這件事情上面去。因為我在看**過去新聞的時候，發現 NCC 的撤照理由**，它是用到說我在 107 年的 3 月 28 號的時候，NCC 抽驗了 14 項的機上盒，那不合格有 11 項，**那不合格的案件裡面**，在新聞稿上面寫到的，**硬體性能檢驗不合技術規範，或者是認證標示不合格**有 2 款，那技術規範 7 款，那我現在我不曉得剩下是什麼，就這樣 9 嘛，它 11，那剩下 2，我不知道它是怎樣，那在中間又特別講到說，**針對可以看到這些侵權的內容的這些，為了維護設備器材的市場秩序**，可是在我看起來，我覺得 **NCC 它其實很勉強地在做這件事情，它其實沒有有力的立足點**。

那我就想要說，那是不是可以把這一個**公佈訊息的這個畫面**，當作我的一個條件，如果你要去改，那我開機一定就沒有這個東西，就是我**沒有辦法去連接 NCC 網站**，那我就可以很明確地認定，**這個就是不合我的技術審驗規範**。如果你**願意去連**，就是說你沒有辦法規避這一塊，你可以去連的話，NCC 一定可以跟民眾講，**這個就是已經被撤照**了，那這個我相信這部分，它可能比較難規避掉。

可是這個還是要回歸到說，我怎麼**用什麼理由去撤照**，那當然撤照理由可能就是我前面講的，**必須還是一樣回歸到著作權那部分，可能過程要修，就是說你要可能有專屬綁定，或是綁定之類的用語**，當然法律用語不是那麼的知道，說該過相關的法規用的用語是什麼，但是我覺得就是在這個部分，也是就又回歸到，我們團隊所提出的內容是一樣，就是說我們可能**前面要做技術審驗的時候，那我也要有一個法源**，就是說我怎麼去認定說這個，如果你做這樣的綁定是違法的，那這個就可以回應到這一塊，就是說我可以接得起來。

因為我在聽計畫單位報告的時候，我有想到，對他的技術上做得到，可是你怎麼樣去跟人家講，如果有綁定的行為就是屬於違法，或者是說，這個內容是不是違法，這個也是一個部分的問題，**怎麼樣去快速取得，證明這個傳輸的內容是違法的，又回到後面我們說剛剛講到動態的那個阻擋的問題**。因為機上盒這邊是一個部分，那另外一個部分當然就是非法訊源，訊源當然就是透過很多層的伺服器跳進來到臺灣，那其實在 DSRPD 這個阻斷，我覺得是一個目前可行的做法，應該說不得已的做法，如果假設我們當然可以，把境外的伺服器都抄掉，那當然是沒有問題，可是現在是做不到，那做不到的狀況，比較能夠選擇的工具可能就是這個，就跟前面機上盒的侵權認定是一樣的，NCC 當你收到一個空的機上盒的時候，我裡面也沒載軟體，然後我怎麼樣去認定它是違法的，而且他們那時候也還沒賣掉，那我有想到剛剛教授有提到，臺灣廣告可能就講說，我可以看侵權內容，但是問題是你送審驗的時候，它都還沒開始賣，那 NCC 到底能夠怎麼認定，我最好的方法就是你只要叫安 O，你就是違法，但是這一定不行，可能它會改名字，所以我能夠很明確的，對我們查緝的單位來講，越明確是越好，當然對審驗也是一樣，越明確越好，**它只要沒有達到審驗標準，然後沒有把那個字秀出來，我就認為你就違法，你就是不合規範**，那如果我們只要能夠有權力的單位，很明確的告訴我們，這個內容就是違法的，那當然後續要做，就相對會容易很多，因為畢竟剛剛教授會講到誤殺，就是我如果有 block 掉，那我會不會誤殺到不是的。那像剛剛那個我覺得英國那邊的做法，我個人認為也有可能就是，他必須要去，任何一個放出來的頻道，我怎麼樣去直接認定，這個頻道是沒有權力的，這個是我覺得認定很麻煩，除了權力人以外，沒有任何人能夠知道，他到底他的權力的狀況是怎麼樣，到底是過期了還是沒有，原本就沒有還是怎樣，這個我們警察也不知道。

我覺得就是這兩個部分，就是說我只能要把這個前面研究團隊提出來投影片 20 頁的這個整個機制要怎麼聯想，這是**第一個可能前面就是要去修《著作權法》，那第二個管制辦法的部分，審驗辦法的部分，你必須要有一個法源，怎麼樣去認定這個審驗的內容，我只能要去針對這個標的，我能夠去認定他違法，我是依據本身的這個審驗標準的辦法，還是母法還是說其他的法規，那他也要有一個法源，他開機訊息的部分，當然就是我覺得可以幫助到第二點**，那機制這邊的話就比較沒有建議，謝謝。

陳曉慧 教授 回覆：

非常感謝副隊長給我們的建議，各位剛剛都提示了我們，就是其實大家一致認為從著作權來證明，我想這也是為什麼，因為最後**英國**他們現在抓的大部分，甚至於是抓盜版的組織，對外的宣傳也是不再是只是單純的說，你不要看這個盜版網站，對你不好，而是他們會告訴你說，就是**你如果使用非法機上盒，你的盒子就有很高的資安風險，然後會有讓色情甚至竊盜、洗錢等等的問題，當然如果後面還是 P2P 的話，那你毫無疑問的，就已經是一個侵權的問題**。

在不知不覺的情況下，我想從 NCC 他可以介入的角色來講，或許去**強化從端點的這個器材的安全，會更加容易的去建立**，他為什麼可以建立這個監理機制的一個重點，我們會在適當的地方加以說明，非常感謝各位。

剛剛各位也提出了很多，就是如何逃脫或者是被稀釋等等，我們還是請這個構想原始人，查士朝老師來做一個總結。

查士朝 教授發言：

謝謝 NCC 長官以及各位來參加的貴賓，基本上我今天從各位的身上聽到很多的想法。我稍微舉個例子來講，之前很多人就有問我很多個資已經掉了怎麼辦，我建議不斷的放一些假個資出去，可以把外面的個資都洗成是假的。

其實我們在這邊看的時候，比較技術的地方，首先第一個來講，我們要知道說到底這個有問題的 App 或是有問題的機上盒，它到底問題是在哪，我可以去證明說它有問題。實際上來說，我們知道說它有問題之後，有很多的手段可以做這樣子的一些處理，當然有一些不太合法。例如說，我剛剛也有想到說，**我們知道說它到底是怎麼樣子去做認證之後，我們其實就把認證的方式在 YouTube 上公布出去，大家都可以看違法的這個 App 之後，它就無利可圖**，大家也不用花幾千塊買了，這個或許也是一種方式。但這種其實就是說，用這種方式，要死一起死，不過我想基本上我們會針對這個技術為基礎，其實我們第一個，是要證明說它的這個問題，當然後續怎麼樣做這個查緝的這個部分。

當然這個封網，當然大家各位剛剛有提到這個封網，封網跟之前臉書去做封網來講，其實已經有很多人抗議說，你去封 IP 的封 Domain 來講這個問題，其實以**機上盒封網相對難度比臉書高一點**，因為臉書來講它是一個 Domain Name，那

這個你如果說像它的 IP 位置，然後其實它是如果是走 CPM 的話，相對來講那個**它動態在改的時候，幾乎很難去做封網，**但是如果說是以這個我們能夠知道有問題，然後知道有哪些位置，如果說能夠未來提供一些形式。

因為大家其實現在很擔心，**刑事機構在封網的時候，沒有一個標準，**然後我們如果說能夠提供它說，今天來講這個單位，它在連網的時候，那個 IP 的位置其實就是有問題，或者它在封的時候，有相關的鑑識的紀錄，那他們在做這件事情，或許會有更好的一個手段。所以我想我們在這邊來講，至少**我們在這個計劃裡面，第一個我們會做核心的部分，就是先把怎麼找到問題，問題的源頭先把它識別出來，到底哪個 App 有問題，或是哪一個這個機上盒有問題，我們先能夠做鑑識**，那至於之後的手段，那當然這邊可能就是，**我們也會跟法律的這個團隊共同來想，看說有沒有一些更好的一些方法**，來跟大家最後來產生一些這個建議，那非常謝謝各位給的一些建議，今天非常謝謝大家的出席，今天會議就到這裡，謝謝大家。

附錄二 OTT TV 機上盒監理法規與技術座談會

第 2 場

- 本計畫第一場座談會於 2023 年 11 月 1 日（三）14：00–16：00，假集思台大會議中心-亞歷山大廳舉辦。
- 邀請來自產、官、學界專家，共九人與會。專家名單（依姓氏筆畫排列）如下：

  王翔正 副隊長 刑事警察局電信偵查大隊

  林宜柔 助理教授 中信金融管理學院科技金融研究所暨財經法律系

  紀博文 副教授 國立臺灣師範大學 資訊工程學系

  張友寧 主任檢察官 台北地檢署

  張銘巖 處長 CBIT 台灣有線寬頻產業協會

  彭淑芬 秘書長 CBIT 台灣有線寬頻產業協會

  楊育麒 副處長 CBIT 台灣有線寬頻產業協會

  蔡銘財 協理 中嘉有線電視業者

  盧信儒 資深經理 中嘉有線電視業者

第一節　　會議現場照片及簽到

【OTT TV 機上盒監理法規與技術之研究座談會第二場】
會議簽到表

計畫編號：	112QD127	**會議日期：**	112 年 11 月 1 日
主席：	查士朝老師/蔡文玲律師	**地點/會議室：**	集思台大會館-亞歷山大廳

姓　　名	簽　　名
CBIT 台灣有線寬頻產業協會 彭淑芬 秘書長	
CBIT 台灣有線寬頻產業協會 張銘巖處長	
CBIT 台灣有線寬頻產業協會 楊育麒副處長	
中嘉數位股份有限公司 蔡銘財 協理	
中嘉數位股份有限公司 盧信儒資深經理	
中信金融管理學院科技金融研究所暨財經法律系 林宜柔 助理教授	
刑事警察局 電信偵查大隊 王翔正 副隊長	
台北地檢署 張友寧 主任檢察官	
國立臺灣師範大學 資訊工程學系 紀博文 副教授	

第二節　　摘要稿

彭淑芬 秘書長發言：

- 2016 年安 O 三代和四代在台灣，就有侵權問題，2021 年有判重刑就是兩年四個月，罰一千多萬的案例，法院終於認可侵權是一個重罪，但是到 2023 年還沒有定讞，所以「數位問題、數位解決」，在數位時代走法院程序是已經來不及。
- 數位時代同樣都有網路犯罪的問題，太多案件已經讓法院已經沒有辦法負荷，會癱瘓法院的作業，所以現在檢察官、法官也認為，應該要從數位方式來解決。
- 未來能夠有一個常設機制，在這麼多國際案例，我最推崇的就是韓國的案例，那就是 KCOPA 雛型。有一個法源依據讓這個常設機構，就像 iWIN（網路內容防護機構）這樣子的一個組織，有法源依據就開始像 KCOPA 這樣開始往前跑。
- 安 O 盒子就是它的現金所在，斬斷這個盒子就是重點， 目前 NCC 沒有法源依據，以公務人員的這個行政作業的規定來講，它是檢驗射頻器材，當講到說著作權的部分的時候，法的部分還是要處理。
- 我們早就有兩個法，一個是《著作權法》，一個是電信法，都是比照 iWIN（網路內容防護機構）的模式，有個第三方認證機構，因為沒有法源所以沒有辦法執行。
- 關於教育宣導的部分，就是讓民眾來了解說，這件事情是重要的，他不是只是一個經濟問題，政府目前困難點在於選票、選民壓力。
- 韓國的 KCOPA 經理有談過，韓國也不是一蹴可擊，在 2017 年之前修了二三十次的法，三十次的法律修訂，才到今天這個稍微可以接受的程度，是很機動性的，可以立即來做處理。
- 我們已經對抗安 O 很久了，他現在已經變成台灣最大的 operator，各 DNS RPZ 已經封不到他。當初 2021 年的台北地方法院的刑事裁定還扣押五十幾個 URL 網址，其實他還有 IP address，中華電信他不願意也不敢也不行封 IP，他覺得會錯封，但當 DNS 封不住的時候，當然要封 IP。

- 我們的執法單位需要授權，未來所有的法令都要具備這一部分，這應該是數位發展部的職責之一，怎麼樣讓我們法律也是跟上世代數位化，怎麼樣讓第三方的公正單位，他有個法源依據可以來做我們剛剛所講的執行宣導。
- 韓國努力的軌跡，關於如何強化政府跨部會合作行政作為，這個就是所有的事情的重點、關鍵。韓國政府，有不得不做的壓力，使命來講，當然要想方設法去修法去跟民眾溝通。今天第三方認證機構，主張網路防範侵權。防範國安的重要角色來講，怎麼可以不成立，像是安 O 盒子曾經被中國那邊做統戰宣導。
- 我們用全世界 39 個國家所做的，他們叫做這個 site blocking。台灣不能講封網，是停止解析網址，就是先停損，就是通知取下。
- 機上盒的部分， NCC 現在用了大批的人力在做抽測，我覺得那個是浪費人力。事實上 NCC 他沒有著作權的管理權限，可是為什麼你有一個切結書，切結書裡面寫的是，我發誓我這個盒子沒有侵犯著作權。你的行為不符切結，我難道行政單位沒有權利可以去處理嗎，如果說沒有這個法源依據，那為什麼會有這個切結呢。
- 還是要修法，講三管齊下，就是第一個 site blocking、第二個盒子，第三個修法，賦予法源依據。
- 最後問三個問題，第一個，我們長期間看，就是說安 O 盒子一直在進化，DNS RPZ 已經封不了它，它現在已經境外 Server 了，所以最後還是要封 IP 或其他的做法。第二個，有沒有可能讓這個 OTT TV 的盒子比照過跟我們有線廣播電視現在有盒子的規管，還有一個資安的部分，我們都必須要去拿 ISO，就是說中華民國資安管理協會所發給我們的資安，就是說我這個盒子是符合資安規定，所有的盒子基於資安管理，拉近跟有線電視一樣的規管水平。最後一個是，安 O 盒子現在還有四百多萬，是一樣的使用行為，將來可能沒有盒子，它可能是 App，可能內建到電視機。

楊育麒 副處長發言：

- 開始解析是從國內 ISP 業者去做解析，前一個階段已經改變為 Google，最近應該是用 OpenDNS 就是 System of Bingo 的驗證。

- 因為都已經改為境外的 DNS，所以我們在第一次做 RPZ，做 URL 的封鎖的時候，其實大概時效大概是幾個小時之後就已經全部都解開了。那現在在這個機制，RPZ 的機制基本上是已經無效了，現在唯一還沒有變化的，只有認證主機的 URL 還是用國內的 DNS。

紀博文 副教授發言：

- 像憑證綁定的技術，其實用上去以後就會發現，這個會很難去做中間人攻擊，所以我們也很難去攔截到封包，能不能略過它。但是一支 App 運氣好的話，兩個禮拜，運氣不好一個月，那這個是他每天的工時都花在這個上面，所需要的時間，所以這可能會導致我們這樣做合不合成本，所以我們在技術上在考慮的時候，可能要先考慮，我們要找比較快速的方式，因為 App 的那個改動速度其實非常快。
- 現在各位的銀行的 App 打開，如果偵測到有 Frida，銀行的 App 連開都不讓你開，如果未來就是這些安 O 盒子的 App，把這一套偵測技術也拿過來以後，那會不會就是說，它也合法說我本來就不應該執行，因為這個是不安全的環境。
- 我比較建議我們可以採用虛擬機的方式，我今天要模擬的是，我能不能模擬安 O 盒子，我覺得這個就是一個很強的證據，可以證明說，你今天這個 App 是綁定安 O 盒子的，因為剛剛看到了其實很多參數，那些參數我大概掃過去，我覺得這些參數應該在模擬系統裡模擬得出來，我把 App 下載下來在模擬器，發現不能看，說真的我覺得法律上證據不是很夠，因為 App 不能執行的理由有太多了，所以我們一定要讓它可以執行跟不能執行，都同時存在，這樣它比較沒有理由狡辯。
- App 確實它的演變是很快速的，如果我們要成立這個 App 的公正第三方的審核機制的話，可能時效性這邊還要特別注意。

張銘巖 處長發言：

- 針對盜版內容的擷取，這幾年其實一直在配合電信警察這邊來做，就是從源頭端發機卡號，然後從收視的機卡號去反查，也是從它的訊源端，然後下去把它做阻斷，這個提供給研究單位做參考。

楊育麒 副處長發言：

- 封完之後幾個小時之後，它就變成是其他的裡面 Domain Name，通常它的內容會是快取（cache）在 CDN 業者，那個快取（cache）就隱藏在裡面，而且那個快取（cache）是會動態的變的，如果我們封了，比如說 Cloudflare 的 SPAWN 機房裡面的，那它可能這邊認證到說這邊是順暢，它會動態移除到另外一個 IDCC 裡面去，某程度我們是不是可以立馬說要求 CDN 業者，是要能夠協助把這個阻斷掉，它的動態能夠分配這個內容的部分，它的法源夠不夠。
- 我們 ISP 業者，都會受傷，只要我們封了這個 Domain Name，率先封網之後，那我們的寬頻用戶（客戶）就會來 complain，因為我這邊中華電信可以用啊，可是在你這邊不能用，下個月就退租了，然後中華電信又是比較屬於半國營事業，沒有法源依據的話，不會去執行。
- 技術面應該是在 CDN 業者那邊的，那邊封的話會更有效，因為它的內容是在那邊，前面那個只是認證而已，認證完了，取得那個認證的 key 之後，它真正的 content 都在快取（cache）那裡，而且它的快取（cache）是真的跑來跑去的。

楊育麒 副處長發言：

- CDN 業者是要有一個怎麼樣封它的一個法源依據，必須我們台灣裡面要一起 ISP 業者一起阻斷掉，才不會還是有漏洞可以跑。
- 如果它跑到境外的話，通常它的收訊品質不好，那中端收訊人，不會再去收這種非法資料。CDN 業者應該要慢慢納入加強管制。

盧信儒 資深經理發言：

- 第一點：我們在教育上面，要打擊這個侵權，但是我們應該要提升著作權的獎勵，這個我覺得從教育做起。
- 第二點：修法相關的部分，安 O 他已經有很多拿到 NCC 認證的被註銷，可是他還是可以依舊繼續去做認證，為什麼不讓他去做認證的申請，或者是

他明明就有前科，為什麼還可以這樣做。然後再來，其實有很多地下論壇，或哪裡都可以取得這個資訊，就是檢舉跟利益相關的部分。

- 第三點：如果成本允許的話，是其實可以導入一個所謂的浮水印的機制，在網路上傳遞的內容，其實是有辦法去做偵測，但這個投入的成本會相對大，需要業者政府補助，或是相關的討論才有辦法去做。
  - 第四點：安 O 他他在賺錢的部分，賣那個硬體來賺錢，之後他沒有收其他的訂閱（subscription）的費用，那他們現在很多 operator 已經開始在走類似安 O 的這種做法，就是合法的安 O，就是他們會把很多接下來線性頻道都做成免費的形式。
  - 第五點：安 O 他數量如果多，他可能會結合廣告，置入廣告，他就有額外的金援，這時候如果要再斷他就更困難。

查士朝 教授回覆：

- 有一些時候有一些的影片被盜錄，的確是都要加一些能夠識別自己來源的，這個影片來講如果是被盜錄的時候，的確是比較容易避免誤抓的情況。

張友寧 主任檢察官發言：

- 要模擬安 O 的環境，跟非安 O 的環境，去比較兩者不一樣，這樣子就可以讓法院相信，在安 O 的時候才可以看，然後在不是安 O 的環境下，不能看，那這個我覺得是比較有效的證明方法，這個就是可能在做的過程裡面一定要確認跟安 O 的環境是一樣的才可以，這樣法院才會相信。
- 我們在走法院的程序，的確是相當的慢，那我也看了一些 RPZ 的案例，基本上都是透過刑事訴訟的扣押裁定去做，TWNIC 出來的新版的 RPZ 的做法是，只要有通報就先封，它只限定在特別類型的案件，那將來是不是有可能在 TWNIC 或者是說透過政府的一些立法的設計，暫時封鎖的一個機制能夠擴散到比較多類型的案件。
- 基本上是在有第三方公正單位，做了一些鑑識或鑑定以後，再來做後面的案件或者是做封網的處理。這個鑑定的時間，我想這的確是一個問題。另外就是關於監護方法，我個人認為直接禁賣機上盒是最好的方法，但

是因為器材管理就是只有以電波為主，那我個人的想法可能跟剛剛幾位先進講的不太一樣，就是說其實我覺得在智慧財產權這個領域，就是只要 NCC 准，你就可以判過，就是智財局也給他一個許可，但是一旦他有案件，智財局就可以依照這個案件紀錄撤銷他的許可。如果一旦有發案件，就表示你這個機器已經有違規侵權的紀錄，那我主管機關就可以依照我的權限，對於有侵權的這個機上盒撤銷許可，同時他就可以開始下架。

- 智慧財產權侵害的一個處理的模式，大部分都是走司法程序，那實際上因為走司法程序就是緩不濟急。主管機關都不介入的話，其實就跟詐欺一樣，就是甲方跟乙方檢察官都累死，然後查了很多但是效果不佳，日後把這些相關的訊息，轉給經濟部、智慧局他們這邊再考慮一下，是不是可以在法律的設計上面，利用一些行政的手段來做處理會比較好。
- 《著作權法》80 條之一，轉到 88 條之一可不可以作為下架機上盒的依據，只把我用錄影機這種方式錄下來的東西，再傳輸來那後面傳輸的行為雖然是違法的，但他有沒有影響到權利保護措施，權利管理電子資訊，這個部分可能會有一些問題，如果說沒有，那實際上就不可能用這個條文的規定來做這個處理。
- 有前科的業者為何可以再驗證?其實可以提供一個法條的規定，既然已經有違規的紀錄，就乾脆在這幾個裡面就有這種黑名單的制度，採購法的規定就可以做，譬如說限制他多少年內不可以來送，那你就在這幾年內就斷他金流，因為他沒辦法賣盒子就會有影響，所以我覺得這個其實是一個可以考慮的方向。

王翔正 副隊長發言：

- 以執法單位來講，剛剛最重視的就是法條、構成要件，那現在目前狀況大概就是《著作權法》87 第一項第八款，這三部裡面講到就是上次修法就是說針對預載的才有違法，那其實這部分確實有要再修的必要性。
- 綁定這個用語在其他法律上是不是有用過，法律的話可能沒有，但是行政規則是有用到綁定這個字，就是在 5 倍券的那個發放辦法裡面有用到綁定這兩個字，那我覺得如果可以用。

- 可以參考那個刑法的電腦犯罪專章- 刑法 362 條，他有講到製作專供犯本章之罪的電腦程式,《著作權法》87 條第 1 項第八款這 3 部裡面講的，如果他可以綁定使用專攻綁定使用這個電腦違反本法的相關的行為的電腦程式的設備，或者是器材這樣子，那如果針對這部分去做可以去斷他的金流。那對後續的相關有提到，包括封網這些行政措施，我覺得比較有依據可以做。
- 我們之前有用那個機上盒機房做浮水印，因為比較大系統商才有辦法去處理那些事，我們去下浮水印其實也都看不到。那另外，是用線上的一些 App 軟體的授權碼，去抓 M3U8 的檔案，然後做下載的動作，，那這基本上我們法規的部分，如果說針對機上盒本身去處理的話，那是比較好。
- 我們有沒有辦法完全模擬一個安 O 的訊，他的裡面的機碼之外，那是不是能夠知道說他的關鍵的機碼是什麼，還必須要講得出來，就是你可能不能仿，那可能原因只是因為序號不對，不是他合法的序號，那是不是也會有這種問題，那這個完全模擬的環境是不是我們都做得出來。

張友寧 主任檢察官發言：

- 法院目前的解釋都是，你只要是專供，他就認為基本上是不存在的，像我們毒品條例裡面講到，專供適用毒品的東西，那不能扣玻璃球，你說這個玻璃球不是專供適用的，所以他就不會扣， 所以我們建議就不要用專供，用供就可以了。

林宜柔 助理教授發言：

- 《著作權法》87 第一項第八款這個部分來去做處理，那因為間接侵權的這個概念上面的話，我們通常還是要有一個直接侵權的行為在前面，我們在上一次開會的時候有提到一個就是你在盒子的一開頭的時候，先下個警語。
- 另外一個方式，有沒有可能我們也放了一個 App 在裡面，然後來去做一個監理的那樣子一個機制。

- 使用安 O 盒子的人的立場來講的話，我們沒有辦法直接去找到這些人，或是一個比較有效一點的機制，我覺得可能也比較沒有一個明確一點的施力點在，就是我們怎麼去真正的來去做修法，一方面來符合業者他們應該要擁有的一個權利。
- 直接把這個廠商被調的話，可以把他放進去黑盒子黑名單，但是其實實際上大家在運作的方式，就是他只要換一個名稱，然後這件事情好像就解套了。

紀效正 簡任視察發言：

- 事情現在就依靠這個射頻管制器材在管這個盒子，希望把它擴大成為著作權保護的一個主要的機制，將來這個盒子可能會變成一個 App，然後目前數位部成立以後，App 的主管機關是數位部。

查士朝 教授回覆：

- 解決純定版的問題，看看說我們能不能夠在法條或者是一些相關的監理機制上面去做一些補充，當然我們在技術上面會提供一些相關的程序作為鑑識，到時候可以成為一個 SOP 的做法。
- 如何建立成立第三方的機制，然後仿照韓國 KCOPA 的方式 ，英國來講，英國好像在針對一些英超期間，他們有一些動態封網的行為，我們也會去看有沒有辦法有更速度化的做法。

彭淑芬 秘書長發言：

- 在做審驗的時候，就是當有廠商來申請射頻機台審驗合格證明的時候，增加一個測項，就是設法有一個 Live 的狀態，測項當有發現它綁定一個 App 的時候，就是不行通過。
- 將來在做射頻器材審驗的時候，加一個要求，就是要智慧局簽名，就是說射頻器材審驗的時候，加一個必須要提據的文件或是說有一個關卡，智慧局要簽名就對了，我認為這一點困難度也不下於第一點，但我覺得加測項這個很可行。

- 我們已經付委的這兩套法律，有沒有可能再讓它透過各位的專業來修改它，讓它是比較可行的，草案精神是：網際網路內容涉及侵害著作權，經網路侵權內容爭議處理機構，就是這個第三方認證機制，這個機構，依網路侵權內容爭議處理程序確定，報請通訊傳播主管機關，通知網路服務提供者，那就執行限制擷取瀏覽移除，大概是這個精神。
- 《著作權法》84 條，有講到說權利人對於著作物有被侵害之虞者得防止之，得防止之，所以修法都是在 84 之一，既然可以防止之，那我們這個所謂的，叫做通知取下，限制擷取，它其實是一個有點類似假扣押是一個暫時性的，它不是一個永久的，它的效果是一個暫時性的停損的動作，並不是一個判決。

查士朝 教授回覆：

- 當然比較難一點的就是禁止下載一些不明來源的程式，那個程式就會去檢查黑名單，或是如果下載下來，我們可以直接做一些 remote wiping，就是直接遠端抹除的做法。

張友寧 主任檢察官發言：

- 在《著作權法》上面，因為是告訴乃論，所以就只有權利人能告，應該說節目、頻道的業者，就是提供內容的業者，他們才有權利來提告。
- 查緝的過程，這個是抽測的手段，可以單一路徑去抽測。在一般的《著作權法》案件上，民間權利人抽測的時候，確實是有這樣的做法，那基本上法院也都接受。違法蒐證，大部分都是針對國家違法蒐證，那如果說是這個民間，就是權利人他利用自己私人蒐證的手段。
- 《著作權法》84 條的部分，雖然我不是民事的專家，但是我們一般法院，在解釋這一條，所謂的請求方式，其實是說請法院以裁判的方法，決定一個方式來避免侵害，那當然透過這個假處分方式，或者是假扣押的方式來進行。

蔡文玲 律師回覆：

- 我覺得第三方機構，這是一個很好的建議，我們也會再參考一下韓國他們的一個相關的一個做法。
- 《著作權法》84 條，其實相關的部份我們確實都會透過假處分、假扣押，或者是一個確定的判決，才能夠去做後續的一些強制執行，或者是就是那個一些那個預防機制的一個部分，所以在目前我們可能比較常遇到的問題是說，在整個訴訟的程序上面，可能確實會有一些緩不濟急的一些情況。

第三節　逐字稿

彭淑芬 秘書長發言：

各位長官、各位委員大家好，我感謝第一個發言，我爭取過我有 10 分鐘的時間，謝謝。感謝研究團隊，其實都有抓到重點，然後也非常的專業，那我們就不從頭說起了，現在直接找解決方案，我首先要回應一下，很高興，第一個有這麼專業的研究團隊，來做今天這樣的一個研究案心有戚戚焉，看法是滿一致的，很有構思。

那我說明一下，從 2016 年安 O 三代和四代在台灣，就是有這樣的一個侵權問題，然後我們開始訴諸於法院到現在，雖然 **2021 年已經有判重刑**就是兩年四個月，罰一千多萬的案例。可是對不起，2023 年還沒有定讞喔，2012 年開始有訴訟 2021 年判重刑，法院終於能夠認可侵權是一個重罪，不是像以前罰四萬塊五萬塊，是罰一千多萬，然後徒刑兩年多個月。那對不起，法院有共識啊，政府也支持啊，但是到 2023 年還沒有定讞啊， 三審還在二審耶，所以這就是如同陳玉鳳檢察官所講的「**數位問題、數位解決**」，在數位時代走法院程序是已經來不及，這個當然會有今天的研究案，我們就從頭說起就是說必須要有這樣的。

簡報這個架構，就是如同我們這個簡報裡面，老師簡報裡面講的這個流程機制，怎麼樣來因應數位時代的挑戰，那法院現在也已經有共識，就是說我們這麼多的詐騙案件封了幾萬個網址，其實跟侵權這個事情是一樣的，在數位時代同樣都有這個網路的犯罪的問題，就是說太多的案件已經讓法院已經沒有辦法負荷了，會癱瘓法院的作業，**所以現在檢察官、法官也認為，應該要從數位方式來解決**，所以今天這個研究案是很有意義的，我很建議這個只是起頭。

未來希望這個研究的架構能夠常態化，變成實際將來運作，就像韓國的這個 KCOPA 這樣的一個角色，這是第一點，我很期待就是說這個研究案未來能夠化成一個常設機制。那像在這麼多國際案例裡面，**我最推崇的就是韓國的案例，那就是 KCOPA 這個雛型，這是第一個重點**。我們努力至少七年來，各種方法都試過了，包括剛剛老師所講的這個可行方案。我很同意我們其實後來終於了解到，的確這個**盒子就是它的現金所在，斬斷這個盒子就是重點**，所以盒子一定是很重要的，NCC 也都很幫忙很願意配合，可是很抱歉都幫不上忙，為什麼，**沒有法源依據，以公務人員的這個行政作業的規定來講，它是檢驗射頻器材**，雖然 NCC

很願意幫忙，但當講到說著作權的部分的時候，就是要還是要法，**所以法的部分恐怕還是要處理**。

不過我覺得有兩條路，第一個**有一個法源依據讓這個常設機構**，就像 iWIN（網路內容防護機構）這樣子的一個組織，有法源依據就開始像 KCOPA 這樣開始往前跑，需不需要修法我們打個問號，那現在當然不可能修法，一定要選後 1 月 26 號之後，跟各位報告，我們努力了這麼多年，我們早就有兩套版本，兩個法，**一個是《著作權法》，一個是電信法**都有了，都是比照 iWIN （網路內容防護機構）的模式，有個第三方認證機構，因為我就直接講，智慧局、NCC、文化部都很想幫忙，可是對不起都幫不上忙，也都不願意負責，不是啦，我是說**因為沒有法源所以沒有辦法**，愛莫能助。當我們想修法的時候，我就必須講這兩套法在 2022 年，去年的 3 月就已經覆文了，一讀然後直接覆文，已經在交通委員會跟經濟委員會，一年多了沒辦法審，我今天講的會後可以提供相關資料，這個法規都在了，這就是 iWIN 模式，有個第三方公證單位，這個單位可以做什麼，我們都把它列執掌，列了六項執掌，主要就是什麼呢？做溝通協調，跟 ISP 介接，當有這樣的合於法規所規定的侵權案件，或者說網路犯罪案件的時候，當然是以侵權為主。

他怎麼去設立這個機制，就是如同我們這個上面所講的，怎麼去討論出一個機制，怎麼發動、怎麼執行，這是第一個，執行面。第二個他要做**教育宣導**的部分，就是讓民眾來了解說，這件事情是重要的，他**不是只是一個經濟問題**，他還牽涉到很多層面，當然我知道政府的困難點在於，就是說為什麼這個法不敢修，就是所謂的**選票-選民壓力**。所以就像我們之前有跟韓國的 KCOPA 經理有談過，**韓國也不是一蹴可擊**的，他在 2017 年之前修了二三十次的法，三十次的法律修訂，才到今天這個稍微可以接受的程度，就是說他可以很機動性的，可以立即來做處理。那有沒有人反對，當然有人反對啊，那就是一直溝通，所以這個單位他做執行，做教育宣導，還有一個很重要研究，為什麼，對不起，我先講法規面，技術面由我們兩位專家待會再補充，我們其實已經對抗安 O 很久了，他現在已經**變成台灣最大的 operator**，我們所有人中華電信誰都比不上他，可能 Netflix 都比他小，為什麼要研究，他在進化中，各 **DNS RPZ 已經封不到他**了，所以我們現在想方設法，事實上當初 2021 年的台北地方法院的刑事裁定還扣押五十幾個 URL 網址，其實他還有一排叫做 IP address，可是為什麼中華電信不曉得上一

場有沒有來，中華電信也沒有來，中華電信他不願意也不是說不願意，他不願意也不敢也不行封 IP，他覺得會錯封，可是當我們初步研究，等一下再進一步跟各位講，就是說**當你 DNS 封不住的時候，當然要封 IP**，還有得選嗎，那當我們知道這一段就是他的 IP address，為什麼不敢封，所以我講這麼多意思就是說，大家都很有心，可是都幫不上忙，需要什麼，我覺得我們公務體系，我們的**執法單位，他可能還是需要有一個授權**，一個法律的部分，那我的法已經在立法院了，剩下三個月吧，就要休會了，那就換屆了，換屆不連續，這個法從頭來過了，那現在是名氣可用，就是說我們這個叫做防制性侵無法，還有動物防疫的相關法令，都是採數位時代、數位問題、數位解決都是採網路的技術的做法，因為等法院等行政，已經來不及了， 一定是直接用網路的工具去做。

我相信未來，所有的法令可能都要具備這一部分， 這應該也是**數位發展部的職責之一** ，怎麼樣讓我們**法律也是跟上世代數位化** ，法的部分我們來想想，我這邊就是說只提說已經有兩套法已經在立法院，怎麼樣讓第三方的公正單位，他有個法源依據 可以來做我們剛剛所講的執行，宣導，然後研究未來，我現在講結論，我提出一個建議，然後提出三個問題。

第一個就是，我們去看韓國努力的軌跡，我必須講，這邊我們本來提到說，**如何強化政府跨部會合作行政作為**，這個就是所有的事情的重點、關鍵。韓國政府他有韓流，他沒有任何的本錢可以不防止數位侵權，他的韓流就靠這個，我們台灣呢，我要問政府你真的想要解決網路侵權的問題嗎，我懷疑，如果你是韓國政府，你有不得不做的壓力，使命來講，你當然要想方設法去修法去跟民眾溝通，我問台灣政府選後願不願意處理，再加上另外一節，我們改天再來講，就是說他絕對有國安問題的，絕對有資安國安問題的，這個我們掛保證，這個已經有專家認證了，如果需要提供資訊也是可以回頭提供，今天這個第三方認證機構，他主持的是一個**網路防範侵權**，防範國安的重要的角色來講，怎麼可以不成立呢，就算台灣不重視著作權好了，那麼重視國安吧，國安跟資安 講到這裡，我們之前 OTT 交流平台會議，其實在上一次的時候就有提到這個，很可惜文化部又改組了，所以重視的長官已經不在位置上了，但是我真的必須講選後，輕則我聽說國安會其實也很在意安 O 盒子，**安 O 盒子曾經被中國那邊做統戰宣導**，大家都知道，這個怎麼可以不處理呢，所以就是說剛剛講要讓這個第三方認證機構能夠常態化，如果這個團隊可以蛻變到這個常識的機構是更好，那就是法律看怎麼樣來，

給他這樣的一個依據，對不起我再兩分鐘，建立好解方沒有一種單一方法，立刻就處理就可以解決了，叫多管齊下，三管齊下，第一個就是我們用全世界 39 個國家所做的，他們叫做這個 site blocking。台灣不能講封網，台灣講 site blocking 會被抓去關，因為要講 講得很複雜，停止解析網址，類似這樣，第一個封網，就是封阻，這個是必須做的，我覺得什麼其他的方法很多都緩不濟急，就是先停損，就是通知取下，下架這件事情，就像 iWIN 跟防制性侵無法的做法，這是第一個。

第二個是盒子的部分，我講說 NCC 這個事情，其實 NCC 也是很幫忙，他剛剛所講的就是說，他沒有著作權的這個法源依據，那很抱歉，我要講的是說，剛剛那個老師有一個問題說，**怎麼樣讓他下架，就是 NCC 現在用了大批的人力在做抽測，我覺得那個是浪費人力**。不是這樣子，我建議以盒子來講，盒子也很重要，現行如果不動不修法或不修管理規則，我想請教就是說，**事實上 NCC 他沒有著作權的管理權限**，可是為什麼你有一個**切結書**，切結書裡面寫的是，我發誓我這個盒子沒有侵犯著作權。你竟然有切結書，**你的行為不符切結，我難道行政單位沒有權利可以去處理嗎**，如果說沒有這個法源依據，那為什麼會有這個切結呢，那如果切結不實該怎麼辦，所以我認為 NCC 也不是沒有工具可用。那很高興就是說我們今天這個圖表裡面，**除了射頻以外，還有一個資安加侵權部分的檢測**，這個如果未來，能夠讓他有一個依據，這個是最完美的，那這個又要再走到法律，我剛剛講的是盒子。

第三個就是說，剛剛講的就是說，**還是要修法**。所以剛剛講**三管齊下，就是說第一個 site blocking、第二個盒子，第三個修法，賦予法源依據。**那我最後問三個問題，提出一個比較未來可能面對的。第一個，我們長期間看，就是說**安 O 盒子一直在進化**，就剛剛所講的，DNS server，DNS server 用不了它，**DNS RPZ 已經封不了它，它現在已經境外 Server 了，第一個，所以最後還是要封 IP 或其他的做法，我相信絕對有方法封的，就是可不可以做而已。**第二個，盒子來講，就是剛剛已經給你報告過了，NCC 這個也是一個很好用的工具，怎麼強化，**有沒有可能讓這個 OTT TV 的盒子比照過跟我們有線廣播電視現在有盒子的規管**，有線電視的規管方式，列下來應該有十幾個吧，我念一下，有線電視中端設備審驗辦法、有線電視中端設備機構認證管理辦法、有線電視中端設備中規範、有線電視中端設備技術規範、審驗有線電視終端設備，還有一個最重要的，還有一個

資安的部分，我們都必須要去拿 ISO， 就是說**中華民國資安管理協會所發給我們的資安，就是說我這個盒子是符合資安規定**，它的側項是很多的，有沒有可能，**所有的盒子基於資安管理，拉近跟有線電視一樣的規管水平**，這個請 NCC 長官考慮一下。

最後一個是：安 O 盒子一直不斷的在進化中，它現在是有盒子是因為民眾是因為它現在還有四百多萬，是一樣的使用行為，**將來可能沒有盒子**囉，**它可能是 App，可能內建到電視機**喔，是不是，所以漸行，就是說我們這個第三方公正單位，今天就是開始籌備的第一天，開始可以研究未來下一步，安 O 一定會變形的啦，那我以上先報告到這邊，謝謝。

查士朝 教授回覆：

好那謝謝彭秘書長，那接下來請楊副處長先，就先順著這樣，大概請楊副處長先講一下這個部分。

楊育麒 副處長發言：

各位大家好，我今天大概都是從技術面上看到的，其實在整個的技術面上的監理機制，其實從剛剛的報告裡面都已經講得很詳細了，對於我們自己在做這方面的建立，其實跟剛剛的報告裡面大同小異，基本上我們都可以看到所謂的認證主機，那從我們的觀察裡面的話，安 O 盒子的確如剛剛講的一直在進化。一開始的解析是從國內的 ISP 業者去做解析，慢慢的前一個階段已經改變為 Google 那最近應該是用 OpenDNS 就是 System of Bingo 的驗證，那現在除了認證主機還是用所謂的國內的 ISP 所發放的 DNS 在解析以外，那整個在剛剛有特別提到，**因為他們都已經改為境外的 DNS**，所以我們在第一次做 RPZ，做 URL 的封鎖的時候，其實大概時效大概是幾個小時之後就已經全部都解開了，那現在在這個機制，RPZ 的機制基本上是已經無效了，現在唯一還沒有變化的，只有認證主機的 URL 還是用國內的 DNS，以上大概是這樣子的一個，其他的部分的話，整個監測的部分大概是大同小異。

紀博文 副教授發言：

不好意思，跟各位委員說聲抱歉，因為 3 點半有課，要回去學校。 感謝張老師這樣詳細的介紹，那因為我本人我不太懂法律學或這種技術。 所以我當我們在研究資安或者相關議題的時候，我第一個做法就是把自己當壞人，就是我今天看了這一連串，我如果是案過後，就不要怎麼避開它，那剛剛其實那個查老師

他其實講了很多，包含了像憑證綁定的技術，其實用上去以後就會發現，這個會很難去做中間人攻擊，所以我們也很難去攔截到封包，能不能略過它。其實可以，但是這會產生另外一個問題，就是我有問過做這些事的人，他說一支 App 運氣好的話，兩個禮拜，運氣不好一個月，那這個是他每天的工時都花在這個上面，所需要的時間，所以這可能會導致下一個問題就是，我們這樣做合不合成本，所以我們在技術上在考慮的時候，可能要先考慮，我們要找比較快速的方式，因為 App 的那個改動速度其實非常快。所以我建議就是，我可能要看一下有沒有什麼比較快速的一些方式，來做這件事。

那剛剛那個查老師有特別提到那個 Frida 那個工具，那個工具有用，可是它會有另外一個問題，就是現在各位的銀行的 App 打開，如果偵測到有 Frida，對不起銀行的 App 連開都不讓你開，而且這是我們現在要求銀行的 App，就要做到的事情，如果未來就是這些安 O 盒子的 App，把這一套偵測技術也拿過來以後，那會不會就是說，它也合法說我本來就不應該執行，因為這個是不安全的環境，那我們還有什麼方式。

查老師剛剛有提到一個很有趣的概念，就是我們能不能用虛擬機的方式來偵測，其實**我比較建議我們可以採用虛擬機的方式**，為什麼，只是我們虛擬機會有一個比較麻煩的點，就是我們要如何模擬，我不是要模擬一個 Andriod 的平台，我今天要模擬的是，我能不能模擬安 O 盒子，我會不會說我設定好換成安 O 盒子，我就可以看了，然後我今天設定好一改我就不能看了，我覺得這個就是一個很強的證據，可以證明說，你今天這個 **App 是綁定安 O 盒子的**，**因為剛剛看到了其實很多參數，那些參數我大概掃過去，我覺得這些參數應該在模擬系統裡模擬得出來**，如果它模擬得出來的話，那我就把我的虛擬機變成安 O 盒子，跟變成不是安 O 盒子，就會發現一會兒可以看，一會兒不能看，那我認為這樣算是一個足夠的證據，來讓我們說這個 App 是綁安 O 盒子的，不然如果我們剛剛只是說，我把 App 下載下來在模擬器，發現不能看，說真的我覺得法律上證據不是很夠，因為 App 不能執行的理由有太多了，所以我們一定要讓它可以執行跟不能執行，都同時存在，這樣它比較沒有理由狡辯。

但是還是那句話，就是 **App 確實它的演變是很快速的**，所以這整套的檢測流程我們不可能說一個 App 出來，我們就要花上一個月的時間，一個月可能 App 都改了三版，那我之前好不容易產生一份報告出來，它可能已經失去它的時效性，

以我建議就是**如果我們要成立這個 App 的公正第三方的審核機制**的話，可能**時效性這邊還要特別注意**一下，以上，謝謝， 不好意思，因為我還有課，可能要先行離席。

查士朝 教授回覆：

好，謝謝。那我們就繼續，請張處長發言，謝謝。

張銘巖 處長發言：

查教授、各位先進好，其實這個機上盒的監理建議已經做得很完整，那我這邊再補充一個是數位源頭，針對盜版內容的擷取，其實我們這幾年其實一直在配合電信警察這邊來做，就是從源頭端發機卡號，然後從收視的機卡號去反查，也是從它的訊源端，然後下去把它做阻斷，這個提供給研究單位做參考。

楊育麒 副處長發言：

中間再講一下，我們在 2020 年左右，就開始就在封那個認證的時期， 就是剛剛查老師簡報的那個 1.1234，封完之後幾個小時之後，它就變成是其他的裡面 Domain Name，那如果真的要阻絕的話，其實就算是它 IP 註冊是在境外，但是它為了要讓它的連接會比較順暢，通常它的內容會是快取（cache）在 CDN 業者，那這 CDN 業者通常是在各大的 IDCC 網，像是 SPAWN 機房或比較大的，那個快取（cache）就隱藏在裡面，而且那個快取（cache）是會動態的變的，如果我們封了，比如說 Cloudflare 的 SPAWN 機房裡面的，那它可能這邊認證到說這邊是順暢，它會動態移除到另外一個 IDCC 裡面去，那有些比較大的 ISP 機房 也是有 Cloudflare 的快取（cache）在裡面，所以說真的如果偵測出來，第三方認證出內容是有侵權的，那要去也知道它的網址的內容的話它的 IP 的話，**某程度我們是不是可以立馬說要求 CDN 業者，是要能夠協助把這個阻斷掉，它的動態能夠分配這個內容的部分，它的法源夠不夠**，不然我們 ISP 業者，通常都會受傷，就是說現在法源不足，通常只要我們封了這個 Domain Name 之後，率先封網之後，那我們的寬頻用戶（客戶）就會來 complain，因為我這邊中華電信可以用啊，可是在你這邊不能用，下個月就退租了，然後中華電信又是比較屬於半國營事業，沒有法源依據的話，不會去執行，對我們來講，在執行面上面是真的是比較困難。

那我個人認為是，就技術面要打的話，**應該是在 CDN 業者那邊的，那邊封的話會更有效**，因為它的**內容是在那邊，前面那個只是認證而已**，認證完了，取得那個認證的 key 之後，它真正的 content 都在快取（cache）那裡，而且它的快

取（cache）是真的跑來跑去的。

查士朝 教授回覆：

其實像您講的，其實我那時候是有想過可能的一些方向是說，如果說是，像是四方例如你要借機房的時候，是要要求放 CDN 上來的業者。

楊育麒 副處長發言：

數位認證完之後，確定要堅持說這個連結的是不合法，那就應該把那個連結要處決掉，而且是要求當時任何 CDN 業者，或是 Cloudflare 都要看，因為我們機房其實也都有 Cloudflare 進駐到，機房裡面的快取（cache），但是我們並沒有法源依據，我可以阻攔它。大概建議是，CDN 業者也是要有一個怎麼樣封它的一個法源依據，而且必須我們台灣裡面要一起 ISP 業者一起阻斷掉，才不會還是有漏洞可以跑。

如果它跑到境外的話，通常它的收訊品質不好，因為頻寬要更大，那中端收訊人，時間久的時候會轉圈圈，慢慢慢慢，某種程度上，它不會再去收這種非法資料。CDN 業者應該要慢慢納入加強管制，以上我的建議。

盧信儒 資深經理發言：

大家好，我是中嘉代表，剛剛前面各位都分享了比較有效的做法跟自訂方向，那我這邊有幾個跳 TONE 的想法，就是在這個裡面，我是覺得。

第一點：我們在教育上面，應該要雖然說，我們要打擊這個侵權，但是我們應該要**提升著作權的獎勵**，這個我覺得**從教育做起**，這是第一個

然後第二點：是剛剛討論到修法相關的部分，那我是覺得有一個好奇的點，就是安 O 他已經有很多拿到 NCC 認證的被註銷，可是他還是可以依舊繼續去做認證，那這個部分為什麼針對這個品牌，我不可以把它 ban 掉，不讓他去做認證的申請，或者是他明明就有前科，為什麼還可以這樣做，是不是這個方向是可以做討論。然後再來，其實**有很多地下論壇**，或哪裡都可以取得這個資訊，那這些是不是要，那這有點言語的恐怖，但是是不是針對這個部分，需要做處理或是什麼方式，就是檢舉跟利益相關的部分。

那再來第三點：在科技的做法的部分，如果成本允許的話，是其實可以導入一個所謂的**浮水印的機制**，就是在網路上傳遞的內容，其實是有辦法去做偵測，但這個投入的成本會相對大，就是需要業者政府補助，或是相關的討論才有辦法去做。

那再來第四點：就是其實安 O 他他在賺錢的部分，**賣那個硬體來賺錢**，之後他沒有收其他的訂閱（subscription）的費用，那其實我們以前好像也有討論過，就是斷絕他的收入，其實他就可以或是讓他的收入變緩，他可能會可能會有問題，這樣子。所以這個是在九月底的時候我有去看了一個展，那他們現在很多 operator 已經開始在走類似安 O 的這種做法，就是合法的安 O，就是他們會把很多接下來線性頻道都做成免費的形式，其實跟安 O 是一樣，我覺得走到最後，我猜測過幾年後可能會有很多的頻道是免費， 那這個其實是會跟安 O 一樣的狀況，所以那個數量會更多。

第五點：我是覺得這是需要小心的，就是安 O 他現在的數量如果多，或是類安 O 的這種服務多了，他可能**會結合廣告，置入廣告，他就有額外的金援**，這時候如果要再斷他就更困難，我目前想到的補充的部分。

查士朝 教授回覆：

謝謝，我想這邊其實有幾個部分，可能大概之前我們有在 NCC 開會的時候，上次我們報告的時候，有委員提到，因為有一些時候有一些的影片被盜錄，的確是我們自己大家**都要加一些能夠識別自己來源的**，這個影片來講如果是被盜錄的時候，的確是比較容易避免誤抓的情況，這其實是我們也會多評估一下。那當然另外的話，有一些的這個議題來講的話，我們大概也會做一些的參考。那接下來，我們想請主任檢察官來跟我們做一些分析。

張友寧 主任檢察官發言：

主持人好、查老師好，還有各位在場的先見好。我因為是法律人，所以其實對技術並不是非常的了解。那看這個報告，我們可能一開始也是用法律人的角度來看，那像剛剛報告 其實前面提到監視機器的那個程序跟手法，我第一個反應是，只有用虛擬機來做 OK 嘛? 結果剛剛紀老師已經有解釋了，那我覺得紀老師提的這個方法， 我覺得是在法院出重招會比較有意義的，第一個，就是你用同樣的一個，你都用模擬器做就可以了，但是你要模擬安 O 的環境，跟非安 O 的環境，去比較兩者不一樣，這樣子就可以**讓法院相信**，在安 O 的時候才可以看，然後在不是安 O 的環境下，不能看，那這個我覺得是比較有效的證明方法，或者原來報告上面所提的這個 這個檢測的方法就是你裝在安 O 上可以看，然後用虛擬機不能看，或者是說你裝在別的盒子上不能看，那對方一定就會抗議說，第一個虛擬機跟我的環境不一樣，第二個，別家的盒子，我們測三家不能看，他就可

以舉出第四家第五家可以看，所以這個其實會講不完，那就是用同一個環境去模擬，那當然這個模擬的環境的參數，這個就是可能在做的過程裡面一定要確認跟安 O 的環境是一樣的才可以，這樣法院才會相信。

那其實剛秘書長也有提到，我們在走法院的程序，的確是相當的慢，那我也看了一些 RPZ 的案例，基本上都是透過刑事訴訟的扣押裁定去做，那個其實都是在案件已經進行到一段期間以後有相關的證據，我們才有可能向法院去申請 RPZ，那拿到裁定其實封的時間 就像各位剛一提到大概就是幾個小時而已，而且其實，其實在看報告的時候，我自己也想到，因為我自己的 DNS 就是設戶口的，所以就算台灣的業者全部封了，我還是看得到，那所以我想這個連我不是統計系的人都會用，那業者應該也想得到，那果然你確實有聽到這樣的一個狀況，所以其實 RPZ 可能不是那麼有效率，但是 RPZ 我想也不是完全沒有效，因為其實 TWNIC 出來的新版的 RPZ 的做法是，只要有通報就先封，那這個目前，我看一下，它只限定在特別類型的案件，那將來是不是有可能在可能 TWNIC 或者是說透過政府的一些立法的設計，到這種通報就不封，暫時封鎖的一個機制能夠擴散到比較多類型的案件，譬如說這個侵權案件，那我想對那個會對侵權的人來影響會比較大，因為他就需要去調整，短時間就需要調整，而我們封網的速度會相對比現在要快很多，所以這個部分可能對他們犯罪的成本我想是應該會有增加的。

那我想報告裡面都有提到，就是基本上是在有第三方公正單位，做了一些鑑識或鑑定以後，再來做後面的案件或者是做封網的處理。 那剛剛紀老師提到的這個鑑定的時間，我想這的確是一個問題。另外就報告裡面有提到的一些問題，那我想做一些回應，就是關於監護方法，我個人認為直接禁賣機上盒是最好的方法，但是因為器材管理就是只有以電波為主，那我個人的想法可能跟剛剛幾位先進講的不太一樣，就是說其實我覺得在智慧財產權這個領域，就是只要 NCC 准，你就可以判過，就是智財局也給他一個許可，但是一旦他有案件，智財局就可以依照這個案件紀錄撤銷他的許可。那我們為什麼一開始要給他許可的原因，是因為如果我們直接要實際去審查這個機器有沒有內容上違法，會有違反言論自由的問題，但是如果一旦有發案件，就表示你這個機器已經有違規侵權的紀錄，那我主管機關就可以依照我的權限，對於有侵權的這個機上盒撤銷許可，同時他就可以開始下架。

那當然其實就我們的觀察，就算這些被下架的盒子，應該說被撤銷許可的盒子 能不能在外面買得到，還是買得到，但是我想這個就是增加他們流通的管道，那要怎麼樣的去減少這些非法的機上盒在外面流通，可能也需要各個主管機關更加的努力，去查才可以。

那因為我覺得我們目前對於這個智慧財產權侵害的一個處理的模式，大部分都是走司法程序，那實際上因為走司法程序就是緩不濟急。主管機關都不介入的話，其實就跟詐欺一樣，就是甲方跟乙方檢察官都累死，然後查了很多但是效果不佳，然後也沒有辦法真正解決問題，所以我會建議其實這個部分，NCC 代表也可以考慮一下，或者說日後把這些相關的訊息，轉給經濟部、智慧局他們這邊再考慮一下，是不是可以在法律的設計上面，利用一些行政的手段來做處理會比較好。

那另外報告裡面有提到，《著作權法》80 條之一，轉到 88 條之一可不可以作為下架機上盒的依據，那其實我想到的第一個問題是，所有權利人的內容，他都有做權利的管理電視資訊嗎，因為我們看電視好像很少看到，也許有，但是我們可能一般人沒有辦法理解吧，那假設都有，那我側錄的行為，因為其實我們現在如果是用錄影機把它錄下來，原則上還是合法的，那我先只把我用錄影機這種方式錄下來的東西，再傳輸來那後面傳輸的行為雖然是違法的，但他有沒有影響到權利保護措施，權利管理電子資訊，這個部分可能會有一些問題，如果說沒有，那實際上就不可能用這個條文的規定來做這個處理，那當然如果說能夠舉證證明確實有影響到權利保護電子資訊的話，那我覺得透過程序來請求法院判決下來當然是可以，只是說一樣還是會有時效性的問題，沒有辦法馬上解決，我想就是權利人被侵害的一個馬上可以處理的狀況，那以上大概是初步的想法。

剛剛盧經理這邊有提到過，有前科的業者為何可以再驗證?這個我們其實可以提供一個法條的規定，就是說我覺得 NCC 其實可以考慮就是說，你既然已經有違規的紀錄，就乾脆在這幾個裡面就有這種黑名單的制度，採購法的規定就可以做，譬如說限制他多少年內不可以來送，那你就在這幾年內就斷他金流，因為他沒辦法賣盒子就會有影響，所以我覺得這個其實是一個可以考慮的方向，應該在某種程度來講也是會有效的，至少我斷他金流，就沒辦法再繼續做下去，可能會比較好， 謝謝。

王翔正 副隊長發言：

主持人、各位先進大家好，其實以我們執法單位來講，剛剛最重視的就是法條、構成要件，那現在目前狀況大概就是《著作權法》87 第一項第八款，這三部裡面講到就是上次修法就是說針對預載的才有違法，那其實這部分確實有要再修的必要性，因為如果你修得不是很好，他就是會一直載。

那現在來講的話，以我們研究內容講到綁定，那其實之前我在想過，綁定這個用語在其他法律上是不是有用過，然後稍微找一下就是法律上，法律的話可能沒有，但是行政規則是有用到綁定這個字，就是在 5 倍券的那個發放辦法裡面有用到綁定這兩個字，那我覺得如果可以用。

那另外一部分其實可以參考那個刑法的電腦犯罪專章- 刑法 362 條，他有講到說製作專供犯本章之罪的電腦程式，那這個部分是不是針對我們剛講的，《著作權法》87 條第 1 項第八款這 3 部裡面講的，是不是可以做一些參考這兩個去修訂，那可能就是去講說，如果他可以綁定使用專攻綁定使用這個電腦違反本法的相關的行為的電腦程式的設備，或者是器材這樣子，那如果針對這部分去做可以去斷他的金流，其實我們很多犯罪就是這樣子，因為他其實如果是財產犯罪的話，他一定就是要有賺錢，那當然如果可以從這邊去看的話，那我們去讓他們閃不掉，可能會對我們執法來講，會比較明確一點。那對後續的相關有提到，包括封網這些行政措施，我覺得比較有依據可以做，那我覺得第 1 點應該比較重要的是這個。

那另外我想要回應一下張處長，張處長剛有講到說，我們之前有用那個機上盒機房做浮水印，這些事情去查緝的案例，那其實現在的狀況，主要他們那些截錄機房其實他也不去用，因為比較大系統商才有辦法去處理那些事，那現在我發現就是，我們去下浮水印其實也都看不到。那另外還有之前我們有用過，他是用線上的一些 App 軟體的授權碼，去抓 M3U8 的檔案，然後做下載的動作，那其實這個我們當然也有抓人，那其實這些方法，我只要講說，就算我們想要最好的方法，人都會閃都可能會閃，那我們其實也不想去揭露這些方法。但是，最近我們有同仁去出庭，然後法官就問他說，你這個浮水印怎麼做，就現場叫我們同仁講，然後他說這個可以講嗎?就是再怎麼樣，他們就會想辦法去刺探我們怎麼知

道這件事情，那所以我覺得不是說人閃掉他就不能做，那這基本上我們法規的部分，如果說針對機上盒本身去處理的話，那是比較好。

那第二個的話，就是有講到模擬那部分，之前有一個訊息，安 O 的部分，他其實會針對機器的一些序號，他其實是可以改的，所以如果提到模擬這件事，就變成說，我們有沒有辦法完全模擬一個安 O 的訊，他的裡面的機碼之外，那是不是能夠知道說他的關鍵的機碼是什麼，還必須要講得出來，就是你可能不能仿，那可能原因只是因為序號不對，不是他合法的序號，那是不是也會有這種問題，那這個完全模擬的環境是不是我們都做得出來，我覺得這個是要去考慮的，大概這樣子。

張友寧 主任檢察官發言：

想補充兩件事情：第一個就是，他有提到專供這個概念，那當時立法的確有這個，就是說他立法的目的的確是很好，但是法院目前的解釋都是，你只要是專供，他就認為基本上是不存在的，像我們毒品條例裡面講到，專供適用毒品的東西，那不能扣玻璃球，你說這個玻璃球不是專供適用的，所以他就不會扣， 所以我們建議就不要用專供，用供就可以了，這樣子就是說立法的時候，你用專攻大概就是不可能用，那個條文就會沒用。第二個就是，我忘記了，我就先講這個，謝謝。

林宜柔 助理教授發言：

各位先進、大家午安，其實剛剛大家都已經分享過，我很多很專業的部分包含法律跟技術面，那我有一點小小的疑問是，因為其實剛剛不管是那個主任檢察官 還是副座這邊，大家都有提到，那個《著作權法》上面，我們用《著作權法》87 第一項第八款這個部分來去做處理，那因為間接侵權的這個概念上面的話，我們通常還是要有一個直接侵權的行為在前面，那我比較疑惑一點的地方，是因為我們今天整個討論的過程當中，前面是先有一個前提，要有人先去檢舉，那也一定要先有一個不法行為在前面，可是我們現在在處理的，這些技術手段，大概都是在之後，就是當事情已經發生了，那我們現在的這些技術手段，都是在處理事情已經發生之後，那我們前面的那個部分，怎麼去找出來?那個問題怎麼去找

出來?那這個問題怎麼去找出來的方式，當然就是可能，我們在上一次開會的時候有提到一個就是你在盒子的一開頭的時候，先下個警語。

然後另外一個方式是，有沒有可能我們也放了一個 App 在裡面，然後來去做一個監理的那樣子一個機制，那只是去做監理的機制的話，我們是要預防不法的行為在前面，那跟我們現在討論，就是已經有一個實質不法的行為在，或是我們認為它是實質不法的行為在，然後我們再去進行解決，好像是兩個不一樣的概念，那我們去做預防的這件事情的話，目前就我來看，其實大概沒有比較明確一點的法源依據，因為法律永遠走在技術的後面，然後又回到我們剛剛提到說，你要有一個直接侵權的行為在前面，那現在安 O 盒子它明顯的情況就是，剛剛那個查教授這邊也有提到，我們現在在市面上賣的它都是一個所謂的純淨版，所以你也很難說，它是造成直接侵權行為，雖然業者大概就是大家都恨得牙癢癢，就覺得你們為什麼不趕快去處理這件事情，那我剛剛在會前的時候，有跟紀簡任視察有稍微小聊了一下，就是權力人有沒有把這件事情帶到法院裡面來，然後實際上再去進行檢舉的這件事情，到底是應該由誰來做?

那我覺得這個可能大概都是目前各方面遇到的一個問題,還有一個困難的存在， 那就那個使用安撫盒子的人的立場來講的話，我們沒有辦法直接去找到這些人，或是一個比較有效一點的機制，不管是去讓他們沒有辦法再看，像舉一個比較有趣一點點的例子,我大概前兩個禮拜去美國開會,然後去拜訪我國中老師,他非常得意的跟我講說，他從台灣帶了安 O 盒子來，然後他可以在美國就可以看到台灣的那幾個他很喜歡看鄭宏儀的《朕來》還是什麼的節目，然後他可以選擇在任何時間點去看，他就非常的開心，他可以因為有這個安 O 盒子，那我就尷尬了，因為我也參加過這個會，也知道這中間可能會產生的問題，可是就使用者來講的話，他們就是很開心有這樣子的一個東西，所以他更不可能擔任檢舉人這樣子一個角色,所以我才會覺得我們如果要從修法面來下去的話，我覺得可能也比較沒有一個明確一點的施力點在，就是我們怎麼去真正的來去做修法，一方面來符合業者他們應該要擁有的一個權利。

然後另外一方面，讓這個壞人就怎麼把他去下架，剛剛主任檢察官也有針對盧經理這邊提到說，直接把這個廠商被調的話，可以把他放進去黑盒子黑名單，但是其實實際上大家在運作的方式，就是他只要換一個名稱，然後這件事情好像就解套了，所以這個其實大概都是後續執行上面的一些問題，那少少回應一下剛

剛彭秘書長有提到說，既然他們都有簽著作權的切結書裡面的話，那其實這其實有點類似像契約行為，然後但是你如果沒有去定他違反的法律效果的話，其實就是那樣，我只要講了，但是你沒有跟我講說我沒有做到，我會得到什麼樣子的懲罰，大概也是可能是切結書上面會產生的問題。好，謝謝。

紀效正 簡任視察：

今天還是來聆聽大家的意見，我想這個問題，彭秘書長在這邊存在非常久遠，我們畢竟是行政機關監理機關，我們也曾經想過帶著秘錄器，像司法警察一樣 ，剛剛查教授也講了，他去買的時候，這樣子就《刑事訴訟法》上面能不能作為佐證依據，透過秘錄器一個不具司法和警察的人，在買安 O 盒過程中，透過對話詢問他，說想看，所以畢竟還是政府有分工的。

以著作權的執法或是解釋《著作權法》的適用，還是經濟部，然後智財局我們也跟他開會過多次，他就比較說要尊重智財法院法官的判決，也不是他能夠主張很多事情的，所以事情現在就依靠這個射頻管制器材在管這個盒子，希望把它擴大成為著作權保護的一個主要的機制，現在大家也提到了所以我們這個委託案，剛才查教授也講了，但是我們也知道，隨著這個科技的進步，將來這個盒子可能會變成一個 App，然後目前數位部成立以後，App 的主管機關是數位部，TWNIC 剛才大家也知道，現在主管機關由原來的 NCC 變成了數位部，所以將來現在也講解壓縮等等的，全部已經都到數位部了，所以數位部又界定它是產業輔導機關，所以它並沒有太多的願意去，我不知道啦，就是執法， 所以這個問題，彭秘書長也講，我們畢竟是行政機關，這一部分就法定主義， 剛才講了就不准安 O 盒，叫他改名，剛才也講了，切結書的法律效力，我想在座不管是律師或是檢察官，或是執法的司法警察，都了解切結書的法律效力，所以這邊還有很多我們希望從產、官、學，特別是我們 NCC，對《著作權法》了解不如智財局的情況下，聆聽大家的高見，所以我就先發言到這邊，還是多留時間聆聽大家，說不定有第二輪更好的意見，謝謝各位。

查士朝 教授回覆：

首先謝謝各位剛剛發言的部分，我們目前的計畫比較會先針對的是解決純定版的問題，看看說我們能不能夠在法條或者是一些相關的監理機制上面去做一些補充，當然我們在技術上面會提供一些相關的程序作為鑑識，到時候可以成為一

個 SOP 的做法，那當然另外一個方面來講，可能未來我們在後面寫報告，我們會研擬討論，看看如何建立成立第三方的機制，然後仿照韓國 KCOPA 的方式 ，乃至於能夠去看對於 Akamai 或者是 Cloudflare 來說，能不能做一些更進一步的限制，像我以前在念書的時候，那時候的分散式創業，是我們分散式創業的典範，那個時間來講它是一個 MIT 的銷售所來開的一家公司，後來它又不行，後來又因為這個影音產業起來，它又開始做的不錯，所以當然我們其實有很多認識的人都在這個產業裡面，所以我們當然也會在試圖去從技術跟法律上面看有沒有一些方式。另外其實我們也會更進一步，因為我們知道說英國來講，英國好像在針對一些英超期間，他們有一些動態封網的行為，我們也會去看有沒有辦法有更速度化的做法，因為目前看起來大概也都可以知道問題在哪，但是檢舉了之後，有效多久?速度多快? 都是問題，所以我們會再去參考國外的做法。那不知道說還有沒有哪一位先進，想要再給我們一些的這個建議的部分，謝謝。

彭淑芬 秘書長發言：

謝謝主席，我再補充一兩點，就是剛剛所講的這一次的研究主軸在講說這個盒子的部分，射頻審驗有什麼可以分享的部分，那我這邊提出兩個想法。第一個，是我們協會 CBIT 跟衛星公會陳依玫秘書長，我們兩個有一個建議，看可不可以提出來，請教各位專家。

就是在做審驗的時候，就是當有廠商來申請射頻機台審驗合格證明的時候，增加一個測項，就是設法有一個 Live 的狀態，我不知道如何有這樣的情境，因為我提出這個做法的時候，被很多技術專家挑戰說，安 O 就跟你講它是清淨版嗎? 就是沒有啊，你又要它是 Live 的狀況，這個測項的環境如何實現，這是各位的專長。測項當有發現它綁定一個 App 的時候，就是不行通過，我不知道我這樣解釋，各位看不看得清楚，Live 的狀況如何實現，它一定有綁定，綁定就是不行，就不要過了，這是一種解方之一，選項之一，明天我們要去 NCC 年度座談會，我也會提這一件，可能會被很多人攻擊，不過就是說，有沒有可能測試項目加這一個。

第二個，是有一位受尊敬的 NCC 委員的倡議，他還有那個條文草案，我想朱老知道是誰，他建議將來在做射頻器材審驗的時候，加一個要求，就是要智慧局簽名，我大致描述這位長官委員的想法，他也有這個版本，他已經分享給大家，我想可以分享給研究團隊，就是說射頻器材審驗的時候，加一個必須要提據的文

件或是說有一個關卡，智慧局要簽名就對了，我認為這一點困難度也不下於第一點，但我覺得加測項這個很可行。

最後講就是說可不可以建議研究團隊，我們這個已經付委的這兩套法律，有沒有可能再讓它透過各位的專業來修改它，讓它是比較可行的，我們這個草案大概是長這樣，這個精神是這樣：網際網路內容涉及侵害著作權，經網路侵權內容爭議處理機構，就是這個第三方認證機制，這個機構，依網路侵權內容爭議處理程序確定，報請通訊傳播主管機關，通知網路服務提供者，那就執行限制擷取瀏覽移除，大概是這個精神。

請各位參考看，如何能夠精進，我再次的補充，就回應一下老師們剛剛的這個意見，就是說《著作權法》84 條，它是有講到說權利人對於著作物有被侵害之虞者得防止之，得防止之，所以我們這個修法都是在 84 之一，既然可以防止之，那我們這個所謂的，叫做通知取下，限制擷取，它其實是一個有點類似假扣押是一個暫時性的，它不是一個永久的，它的效果是一個暫時性的停損的動作，並不是一個判決，既然我 84 條可以防止之，那我這個假扣押也是一個防止的動作，非常合情合理，所以就這樣一個修法技術，是否是可行，也就這樣各位老師，謝謝。

查士朝 教授回覆：

謝謝彭秘書長，就第一個部分來講，我們在這上面正面去看的話，是有一點點難的部分，但是有這個可能性來做類似的事情。舉個例子來講，現在的那一些 Android 的 App 都可以要求，禁止下載不明來源的位置，或是要求禁止下載一些有害的內容，所以某種程度上如果說是我們要求，像是我們國家裡面要販售的機上盒，它都要安裝某一個程式，它會去檢查。第一個當然比較難一點的就是禁止下載一些不明來源的程式，所以我們幾乎所有的東西都會一定去從那個架上下來，那架上下來就一定通常可以去管這個東西，這個就是一個做法。那當然另外一個更進階一點的話，可能就是說，我們可以要求它去裝一些的程式，那裝一些程式的話，那個程式就會去檢查黑名單，就像我們跑出來的一樣，那至少一定可以檢查問題，如果是在清單上，清單我們可以定期更新，那於是乎一發生問題，那種 App 就沒辦法直接下載進來，或是如果下載下來，我們可以直接做一些 remote wiping，就是直接遠端抹除的做法，這個或許是一個技術上面可行的方式，不過

這個可能就會牽涉到一些實際上執行的一些難度，這個可能到時候還是再研究一下相關的部分。不知道有沒有哪一位先進，就這幾個議題有沒有可以再建議。

張友寧 主任檢察官發言：

不好意思那我再補充，老師有提到查緝的部分，那其實在《著作權法》上面，因為剛剛是告訴乃論，所以就只有權利人能告，應該說節目、頻道的業者，就是提供內容的業者，他們才有權利來提告。

第二個就是查緝的過程，其實我覺得這個是抽測的手段，那剛剛處長這邊也有提到，可以單一路徑去抽測。其實我們在一般的《著作權法》案件上，民間權利人抽測的時候，確實是有這樣的做法，那基本上法院也都接受。所以我覺得這個部分應該法律上不會有太大的問題，因為我們一般來講，你說違法蒐證，大部分都是針對國家違法蒐證，那如果說是這個民間，就是權利人他利用自己私人蒐證的手段，而且他是在對話的過程中，他自己是對話的當事人一方，那法院基本上是接受這個東西，就是說他會接受這個是合法的蒐證手段，那以上做一點補充。

另外就是剛剛秘書長也提到《著作權法》84 條的部分，雖然我不是民事的專家， 但是我們一般法院，在解釋這一條，所謂的請求方式，其實是說請法院以裁判的方法，決定一個方式來避免侵害，那當然透過這個假處分方式，或者是假扣押的方式來進行，當然是可以。只是其實因為我們過去的經驗也是，像我剛分發當檢查官的時候，我們處理過那個 ezPeer，跟那種很早期的 P2P 下載的案子，當時業者也是花了很大筆錢，去做了假扣押， 結果就像大家講的幾個小時以後又換了，那個錢就打水漂了，所以其實對權力人士來講，這是一個很大的成本，因為你只封得了一時，你封不了一世，而且他很快就變化，所以最後沒有用這個管道，就是因為這是成本太高的做法，大概是這樣的意思，謝謝。

查士朝 教授發言：

是，謝謝，不知道還有沒有先進想要提供一些建議，不過原本的時間也是到三點半左右，不知道蔡律師有什麼一些要討論?

蔡文玲 律師發言：

謝謝各位專家的建議，研究團隊會把它納入，那只是我們再回應一下，其實我們不見得很常遇到的困境，就是因為技術中立性的一個問題，就像販售道德這個問題，那包括說我覺得第三方的一個機構，這是一個很好的建議，但是我們遇到的困境，常常都是說，我們要怎麼樣去認定，它確實是侵權的內容的過程，這

個可能會是比較重要的,所以這個部分可能就是我們也會再參考一下韓國他們的相關的做法，再看看是不是能夠提供一些相關的結果。

像我們講《著作權法》84 條，其實相關的部份我們確實都會透過假處分、假扣押，或者是一個確定的判決，才能夠去做後續的一些強制執行，或者是預防機制的部分,所以在目前我們可能比較常遇到的問題是說,在整個訴訟的程序上面,可能確實會有一些緩不濟急的一些情況，那我們再看看，是不是有辦法，參考一些國外的做法，來提供一些相關的建議，謝謝。

查士朝 教授：

好，其實我們的計畫一開始是都是法律一開始在做，那我們大概技術也是一開始在談，但接下來我們會把兩邊再結合起來，再做一些討論，所以我會希望說提供一個更完整更周全的方式，以上謝謝各位今天的參加，謝謝各位，謝謝。

參考文獻

中文文獻

ACE（2023 年）.*台湾最大盗版网络的运营商面临 18 个月的监禁和近 2 万美元的没收*。Alliance Creativity and Entertainment. https://www.alliance4creativity.com/zh-CN/news/operators-of-taiwans-largest-piracy-network-face-18-month-prison-term-and-confiscation-of-almost-usd-2-million/

ACE （2023 年）.*ACE 致力于打击数字盗版 & 保护创意市场* .Alliance Creativity and Entertainment 。https://www.alliance4creativity.com/zh-CN/

ACE （n.d.）。*关于 ACE*. https://www.alliance4creativity.com/zh-CN/about-us/

Yeh, D.（2019 年 12 月 11 日）.*Disney+原創劇被盜得最慘！惡名昭彰「海盜灣」盜版功能再升級，還新增串流模式*。數位時代。https://www.bnext.com.tw/article/55864/pirate-bay-torrent-streaming-baystream-piracy-file-sharing

Netflix （n.d.）.*分享您的 Netflix 帳戶* .Netflix 說明中心. https://help.netflix.com/zh-tw/node/123277

江耀國、黃銘輝、葉志良、高文崎 （2011）.*多元網路平台環境下影音內容之管理思維*（PG10006-0321）.國家通訊傳播委員會。http://www.ncc.gov.tw/chinese/files/12022/2716_120222_1.pdf

財團法人臺灣網路資訊中心.（n.d.）.*RPZ 治理機制：法院及行政命令裁定攔阻者*. https://rpz.twnic.tw/d.html

財團法人臺灣網路資訊中心.（n.d.）.*RPZ 治理機制：犯罪防治緊急案件處理 （RPZ 1.5 版）*. https://rpz.twnic.tw/d_2.html

莊明雄、林俊賢（2017）。*OTT 機上盒侵權與資安數位鑑識架構初探*。Communications_of_the_CCISA, 23（3）, 49–64。

張祐嘉 （2023 年 5 月 25 日）.*捍衛正版權利，韓國抓盜版專責機構在做甚麼?*。文化內容策進院。https://research.taicca.tw/article/b6aab699-81ac-326b-b916-84c9271a67af

張俊宏 （2020 年 8 月）.*論非法機上盒侵害著作權之爭議*。智慧財產權月刊，260。https://pcm.tipo.gov.tw/PCM2010/PCM/ebook/book/260/6/index.html?_ebooktimestamp=638276292101517078

陳昱奉 （2022）.*網路犯罪與資訊安全的未來—從網域名稱扣押談網路治理*.刑事政策與犯罪防治研究專刊, 32, 248.

智慧財產權月刊.（2022）.新加坡 2021 年《著作權法》之修正重點及評析.

經濟部智慧財產局.（n.d.）.*破獲非法機上盒違反《著作權法》，執行網域扣押案例*。 https://www.tipo.gov.tw/tw/dl-281050-34f6849d32e146d19906a6421c83f360.html

葉志良 （2015）.*我國線上影音內容管制的再塑造*：從 OTT 的發展談起。資訊社會研究, 29, 49。

資安人 （2022, February 11）.Akamai：5 大盜版網站訪問來源為美、俄、印、中 &巴西. https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9710

賴祥蔚.（2018）. *中國大陸管制下的網路視訊媒體策略. 展望與探索*月刊, 16（16）

日文文獻

事務局.（2022, May 31）.*インターネット上の海賊版サイト対策に関する現状とりまとめ骨子*. https://www.soumu.go.jp/main_content/000816832.pdf

閣府、警察庁、総務省、法務省、外務省、文部科学省、経済産業省.（2021, April 9）. *インターネット上の海賊版に対する 総合的な対策メニュー及び工程表について*. https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2020/pdf/kaizoku_taisaku.pdf

英文文獻

ACE.（2023, April 11）. *OPERATORS OF TAIWAN'S LARGEST PIRACY NETWORK FACE 18-MONTH PRISON TERM AND CONFISCATION OF ALMOST USD $2 MILLION*. Alliance Creativity and Entertainment. https://www.alliance4creativity.com/news/operators-of-taiwans-largest-piracy-network-face-18-month-prison-term-and-confiscation-of-almost-usd-2-million/

Advanced Media Strategies LLC.（2023, May 15）. *Asia Pacific Consumer Surveys Show Benefits of Effective Site Blocking： AVIA-CAP*. Piracy Monitor. https://piracymonitor.org/asia-pacific-consumer-surveys-show-benefits-of-effective-site-blocking-avia-cap/

Advanced Media Strategies LLC.（2023, April 18）. *Parks： Cumulative US Streaming Revenue Lost to Piracy May Exceed $113 Billion by 2027 Year-End*. Piracy Monitor. https://piracymonitor.org/parks-associates-us-streaming-revenue-lost-to-piracy-may-surpass-113-billion-by-2027-year-end/

Advanced Media Strategies LLC.（2023, January 4）. *2022 highlights US： Law suits and shut-downs are weapons of choice. DMCA update in progress*. Piracy Monitor. https://piracymonitor.org/2022-usa/

Advanced Media Strategies LLC. （2023, January 3）. *2022 highlights Europe： Rights-holders lean on law enforcement. New regs passed against piracy.* Piracy Monitor. https://piracymonitor.org/2022-europe /

Advanced Media Strategies LLC. （2023, July 24）. *Italy's 2023 Live Broadcast Anti-Piracy Bill： Unintended Consequences?* Piracy Monitor. https://piracymonitor.org/italys-2023-live-broadcast-anti-piracy-bill-unintended-consequences/

Advanced Media Strategies LLC. （2023, May 23）. Netherlands： Illegal Streaming Service Busted, Leads to Money Laundering Operation. Piracy Monitor. https://piracymonitor.org/netherlands-illegal-streaming-service-busted-leads-to-money-laundering-operation/

Advanced Media Strategies LLC. （2023, June 19）. *AAPA： Illicit Apps Leverage Every Piracy Business Model； Ad-Fraud Is the Most Lucrative.* Piracy Monitor. https://piracymonitor.org/aapa-app-piracy-2023-0619/

Alain Busson, Thomas Paris, & Jean Simon. （2016）. *The European Audiovisual Industry and the Digital Single Market： Trends*. Paris： Issues and Policies. DIGIWORLD ECONOMIC JOURNAL, 101, 17.

Ang Qing. （2022, October 4）. *17 People Arrested for Suspected Involvement in Selling Illegal Streaming Devices.* The Straits Times. https://www.straitstimes.com/singapore/courts-crime/17-people-arrested-for-suspected-involvement-in-selling-illegal-streaming-devices.

Attorney general's office. （2012）. *Guidance-Use of the Common Law Offence of Conspiracy to Defraud*. https://www.gov.uk/guidance/use-of-the-common-law-offence-of-conspiracy-to-defraud--6

Asia Video Pulse. （2023, June）. *AIVA*. https://avia.org/

Baek byung-yeul. （2023, March 21）. *OTT Service Providers Negatively Impacted by Illegal Streaming Website.* Business. https://www.koreatimes.co.kr/www/tech/2023/06/129_347439.html

Bulayenko, O., Frosio, G., Lawrynowicz-Drewek, A., & Mangal, N.（2021）. *Cross border enforcement of intellectual property rights in EU*（PE 703.387）. Policy Department for Citizens' Rights and ConstitutionalAffairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/703387/IPOL_STU（2021）703387_EN.pdf

Busson, A., Paris, T., Simon, J.P., *The European Audiovisual Industry and the Digital Single Market： Trends*. Paris： Issues and Policies,（2016）.

Chris cooke.（2022, June 7）. *Movie Companies Who Got a US Web-Block Order Have Asked for It to Be Stayed*. CMU. https://completemusicupdate.com/article/movie-companies-who-got-a-us-web-block-order-have-asked-for-it-to-be-stayed/

City of London Police.（2023, June 2）.*Operation Creative Blocks £6 Million of UK Advertising Revenue from Funding Illegal Websites*. City of London Police News. https://www.cityoflondon.police.uk/news/city-of-london/news/2023/january/operation-creative-blocks-6-million-of-uk-advertising-revenue-from-funding-illegal-websites/

CODA.（2022, July 14）. *The Operator of "Manga BANK" Was Exposed. Administrative Penalties Have Now Been Confirmed in China*. Copyright Infringement. https://coda-cj.jp/en/news/179/

Colebatch, H.（2009）. Policy. UK： McGraw-Hill Education.

Commission Recommendation （EU） 2023/1018 of 4 May 2023 on combating online piracy of sports and other live events, C/2023/2853, OJ L 136, 24.5.2023.

CrimeStoppers.（n.d.）. *Streaming Online – Know the Risks. Online safety*. https://crimestoppers-uk.org/keeping-safe/online-safety/streaming-online-know-the-risks

Department of commerce internet policy task force. （2013）. *Copyright Policy, Creativity, and Innovation in the Digital Economy*. https://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf.

Debarpita banerjee.（2023, February 21）. *OTT Market Projections（2023 – 2027） – Asia Pacific. MUVI*. https://www.muvi.com/blogs/ott-market-projections-for-apac-2023-2027

Digital europe.（2017）. *Response to ITU Consultation on OTTs, Brussels：Digital Europe*. http://www.itu.int/en/council/cwg-internet/Pages/consultation-june2017.aspx.

Digitalcitizens Alliance. （2020）. *Money for Nothing ： The Billion-Dollar Pirate Subscription IPTV Business*, 26. https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA-Money-for-Nothing-Report.pdf

European broadcasting union. （n.d.）. Principles for Internet Connected and Hybrid Television in Europe. https://www.ebu.ch/files/live/sites/ebu/files/News/2011/A8E39d01.pdf

European Commission. （2022, December 1）. Commission Publishes Latest Counterfeit and Piracy Watch List. https://policy.trade.ec.europa.eu/news/commission-publishes-latest-counterfeit-and-piracy-watch-list-2022-12-01_en

FACT. （2017, November 16）. *Illicit streaming devices pose fire risk*. https://www.fact-uk.org.uk/illicit-streaming-devices-pose-electrical-and-fire-risk-to-users/

FACT. （2021, July 8）. *Man jailed for illegally supplying and viewing Premier League content*. https://www.fact-uk.org.uk/man-jailed-for-illegally-supplying-and-viewing-premier-league-content/

FACT. （2022, January 17）. *FACT's Anti-Piracy And Content Protection Work In 2021*. https://www.fact-uk.org.uk/fact-in-2021/

FACT. （2022, August 19）. *New research finds illegal sports streaming sites expose fans to financial fraud, dangerous scams and explicit content*. https://www.fact-uk.org.uk/new-research-finds-illegal-sports-streaming-sites-expose-fans-to-financial-fraud-dangerous-scams-and-explicit-content/

FACT. （n.d.）. *Dangers of illegal streaming*. https://www.fact-uk.org.uk/consumer-advice/dangers-of-illegal-streaming/

FACT.（2022, June 17）. *Four years and six-month jail sentence for pirate TV supplier*. https://www.fact-uk.org.uk/four-years-and-six-month-jail-sentence-for-pirate-tv-supplier/

FACT. （2022, March 25）. *Illicit streaming fraudsters jailed.* https://www.fact-uk.org.uk/illicit-streaming-fraudsters-jailed/

FACT. （2023, April 20）. *FACT Excellence Awards.* https://www.fact-uk.org.uk/police-trading-standards-recognised-for-outstanding-contributions-towards-combatting-intellectual-property-crime/

Fahim Ahmed.（2020, August 17）. *Streaming Sites Taken Down As Japan Exerts Stricter Piracy Laws. Search Medium*. https://medium.com/the-crown-writer/streaming-sites-taken-down-as-japan-exerts-stricter-piracy-laws-131ee8403013

Fcc. （2014）. *Commission Adopts MVPD Definition NPRM*. https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-210A1.pdf.

Fowler, P. N., Office of Policy and International Affairs, & United States Patent and Trademark Office. （2021）. *Asia-Pacific Economic Cooperation Secretariat.* https://www.uspto.gov/sites/default/files/documents/APEC-DomesticTreatmentofISDs.pdf

Freedom House. （2022）. *South Korea*. https://freedomhouse.org/country/south-korea/freedom-net/2022

Gartner Glossary. （n.d.）. Gartner. https://www.gartner.com/en/information-technology/glossary/internet-tv

Gerald hunt. （2023, June 11）. *Is Torrenting Illegal in South Korea?* VPN Ranks. https://www.vpnranks.com/kr/faqs/is-torrenting-illegal/

Government Accountability Office. （n.d.）. Stli. https://stli.iii.org.tw/article-detail.aspx?no=83&tp=4&d=5524

Government Accountability Office. （2017, September 29）.*Video Programming： FCC Should Conduct Additional Analysis to Evaluate Need for Set-Top Box Regulation*. https://www.gao.gov/products/gao-17-785

Guidance Illicit streaming devices, https://www.gov.uk/government/publications/illicit-streaming-devices/illicit-streaming-devices

Government agency intelligence network（GAIN）（2023, February 23）. *His Majesty's Inspectorate of Constabulary and Fire & Rescue Services*. Retrieved August 16, 2023, from https://www.justiceinspectorates.gov.uk/hmicfrs/glossary/government-agency-intelligence-network/

The Operator of “Manga BANK” Was Exposed. Administrative Penalties Have Now Been Confirmed in China. （2022, July 14）. CODA. https://coda-cj.jp/en/news/179/

IBCAP（n.d.）.*THE INTERNATIONAL BROADCASTER COALITION AGAINST PIRACY*. IBCAP. https://www.ibcap.org/

IBCAP（2023, July 18）.*IBCAP Reports Major Disruption of Piracy in Indian Premier League 2023 Tournament Coverage*. GlobeNewswire. https://www.globenewswire.com/en/news-release/2023/07/18/2706474/0/en/IBCAP-Reports-Major-Disruption-of-Piracy-in-Indian-Premier-League-2023-Tournament-Coverage.html

IBCAP（2023, July 18）.*IBCAP Reports Major Disruption of Piracy in Indian Premier League 2023 Tournament Coverage*. GlobeNewswire. https://www.globenewswire.com/en/news-release/2023/07/18/2706474/0/en/IBCAP-Reports-Major-Disruption-of-Piracy-in-Indian-Premier-League-2023-Tournament-Coverage.html

IBCAP（n.d.）.*Membership*. https://www.ibcap.org/membership

ITU-T Technical Paper. （2014）, *Glossary and terminology of IP-based TV-related multimedia services* , approved at the ITU-T Study Group 16 meeting held in Sapporo, Japan, 30 June – 11 July 2014.

ILLEGAL IPTV IN THE EUROPEAN UNION. （2019）. *Economic, Legal and Technical Analysis Report*, 26–27. https://doi.org/10.2814/28041

Intellectual Property Crime Project. （n.d.）. *European Union Agency for Criminal Justice Cooperation*. https://www.eurojust.europa.eu /intellectual-property-crime-project

Illegal IPTV in the European Union.（2019）. *European Union Intellectual Property Office*. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf.

Illegal IPTV Box Seller Jailed for Four Years over Piracy.（2016, December 12）. *Trademarks and Brands Online.* https://www.trademarksandbrandsonline.com/news/illegal-iptv-box-seller-jailed-for-four-years-over-piracy-4889

Intellectual Property Office.（2017）. Illicit IPTV Streaming Devices – Call for Views. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594048/illicit-IPTV-streaming-devices-call-for-views.pdf

Intersoft consulting.（n.d.）. GDPR Personal Data. https://gdpr-info.eu/issues/personal-data/； CJEU Case C-582/14.

Information Commissioner's Office（ICO）.（2023, May 19）. *What are identifiers and related factors?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-are-identifiers-and-related-factors/

Kevin madigan.（2021, January 12）. *Protecting Lawful Streaming Act Signed Into Law： What You Need to Know*. Copyright Alliance. https://copyrightalliance.org/protecting-lawful-streaming-act-signed/

Kun, E.（2022, January 18）. *Another Brick in the Cybersecurity Law： Data Protection by Design Requirements for Manufacturers of IoT Devices in the EU Law. KU Leuven*

CiTiP. https://www.law.kuleuven.be/citip/blog/another-brick-in-the-cybersecurity-law/

Lim jeong-won. （2023, March 27）. *Korea to Bolster Efforts to Protect Korean Copyrights Overseas. Korea JoongAng Daily*. https://koreajoongangdaily.joins.com/2023/03/27/culture/gamesWebtoons/Korea-Korea-Copyright-Protection-Agency-Kcopa/20230327132905320.html

Maxwell, A. （2023, May 21）. *A decade of pirate Bay proxy war： Did ISP blocking slay the Hydra?* TorrentFreak. https://torrentfreak.com/a-decade-of-pirate-bay-proxy-wars-did-isp-blocking-slay-the-hydra-230521/

Maxwell, A. （2021, July 8）. *IPTV operator jailed for 16 months for selling & watching pirate streams. TorrentFreak*. https://torrentfreak.com/iptv-operator-jailed-for-16-months-for-selling-and-watching-pirate-streams-210708/

Matchroom Boxing Ltd and another v British Telecommunications plc and others.（2020）.EWHC 2868（Ch）. https://www.bailii.org/ew/cases/EWHC/Ch/2020/2868.html .

Maxwell, A. （2022, June 6）. *Court Orders For All US ISPs to Block Pirate Sites Have Been Suspended*. TF. https://torrentfreak.com/court-orders-for-all-us-isps-to-block-pirate-sites-have-been-suspended-220606/

Maxwell, A.（2022, May）. *US Court Orders Every ISP in the United States to Block Illegal Streaming Sites*.

Maxwell, A. （2020, January 4）. *Omi in a HELLCAT： Selling drugs to making "$200K a day" From pirate IPTV*. TorrentFreak. https://torrentfreak.com/omi-in-a-hellcat-selling-drugs-to-making-200k-a-day-from-pirate-iptv-200104/

Maxwell, A. （2023, February 28）. *U.S. govt： Omi in a Hellcat should serve 15.5 years for pirate IPTV scheme*. TorrentFreak. https://torrentfreak.com/u-s-govt-omi-in-a-hellcat-should-serve-15-5-years-for-pirate-iptv-scheme-230228/

Maxwell, A. （2023, March 8）. *Omi in a Hellcat handed 66 months in prison for pirate IPTV, forfeits $30m*. TorrentFreak. https://torrentfreak.com/omi-in-a-hellcat-sentenced-to-66-months-in-prison-for-iptv-scheme-forfeits-30m-230308/

National Intellectual Property Rights Coordination Center. （n.d.）. Protecting Public Health and Safety. https：//www.iprcenter.gov

National Trading Standards eCrime Team. （n.d.）. *About us*. https://www.tradingstandardsecrime.org.uk/about/

Netflix, Disney Battle Pirate Sites That Rip Off Their Content. （2021, March 18）. AIVA. https://avia.org/netflix-disney-battle-pirate-sites-that-rip-off-their-content/

Office of the United States Trade Representative. （2023）. 2023 Special 301 Report. https://ustr.gov/sites/default/files/2023-04/2023%20Special%20301%20Report.pdf

Online Anime and Manga Piracy Caused ¥2 Trillion Loss in 2021, Watchdog Says. （2023, April 22）. Thejapantimes. https://www.japantimes.co.jp/news/2023/04/22/business/tech/online-piracy-japan-losses/

Over-the-Top （OTT） TV （Niche） Licence. （2023, July 13）. Infocomm Media Development Authority. https://www.imda.gov.sg/regulations-and-licensing-listing/over-the-top-tv-niche-licence

OTT REGULATION IN THE EU. （n.d.）. SCHALAST. https://www.ott-regulation.com

OTT Video – Worldwide. （2023）. Statista. https://www.statista.com/outlook/amo/media/tv-video/ott-video/worldwide

PA Media. （2022, June 6）. *Man jailed for selling illegal football streaming boxes ordered to pay £1m. the Guardian*. https://www.theguardian.com/football/2022/jun/06/man-jailed-selling-illegal-premier-league-football-streaming-boxes-ordered-pay-one-million-pounds

Precedence Research. （2022）. Over the Top （OTT） *Market Size, Growth, Report 2022 to 2030.* https://www.precedenceresearch.com/over-the-top-market

Protecting Public Health and Safety.（n.d.）. National Intellectual Property Rights Coordination Center. https://www.iprcenter.gov

Poquiz, J. L. （2023, April 21）. *How much is illegal streaming worth? ESCoE*. https://www.escoe.ac.uk/how-much-is-illegal-streaming-worth/

Premier League.（2016, December 9）. *Press release： Supplier of illegal iptv & Android-type boxes jailed. Home*. https://www.aapa.eu/press-release-supplier-of-illegal-iptv-android-type-boxes-jailed

Purpose of Establishment·History. （n.d.）. KCOPA. https://www.kcopa.or.kr/eng/lay1/S120T428C430/contents.do

Premier League.（2016, December 9）. *Press release： Supplier of illegal iptv & Android-type boxes jailed*. Home. https://www.aapa.eu/press-release-supplier-of-illegal-iptv-android-type-boxes-jailed

Research and markets.（2016）. *Global OTT Devices and Services Market 2016-2020*. Research and Markets. https://www.technavio.com/report/global-consumer-electronics-global-ott-devices-and-services-market-2016-2020

S&P Global Market Intelligence.（2023, January 31）. *Europe： 5 Key OTT Trends to Watch in 2023*. https://www.spglobal.com/marketintelligence/en/news-insights/research/europe-5-key-ott-trends-to-watch-in-2023

Schalast & partner.（n.d.）. *WHAT IS AN OTT SERVICE?* SCHALAST. https://www.ott-regulation.com/what-is-an-ott-service/

Section 512 Study, https://www.copyright.gov/policy/section512/

Shin, J.S.（2023, March 16）. *More Koreans Using Illegal Streaming Sites Despite Police Investigation*. The Korea Bizwire. http://koreabizwire.com/more-koreans-using-illegal-streaming-sites-despite-police-investigation/242954

Support for Digital Copyright Infringement Forensics.（n.d.）. KCOPA. https://www.kcopa.or.kr/eng/lay1/S120T435C441/contents.do

Symonds, T., & Grundy, T.（2023, May 30）. *TV fraud gang jailed for illegally streaming Premier League games. BBC News*. https://www.bbc.com/news/uk-65697595

Telecommunications Act of 1996, Pub. LA. No. 104-104, 110 Stat. 56（1996）.

Tewari, A., & Killam, T.（2022, September 28）. *Cybersecurity and product regulatory compliance* - Part 2. OnRule - Compliance With Confidence. https://onrule.com/resources/product-regulatory-compliance-cybersecurity-part2.html

The pirate Bay. （2023, August 14）. Wikipedia, the free encyclopedia. Retrieved August 15, 2023, from https://en.wikipedia.org/wiki/The_Pirate_Bay

THE FOOTBALL ASSOCIATION PREMIER LEAGUE LIMITED. （2017）. England and Wales High Court （Chancery Division）Decisions.

THE FOUR MOST IMPORTANT AREAS OF OTT REGULATION. （n.d.）. SCHALAST. https://www.ott-regulation.com/regulation-of-ott-services-in-the-eu-four-areas-every-enterprise-must-review

Trading standards. （n.d.）. LBHF. Retrieved August 15, 2023, from https://www.lbhf.gov.uk/business/trading-standards

U.S. copyright office. （2020）. *Section 512 Report.* https://www.copyright.gov/policy/section512/section-512-full-report.pdf

VdoCipher. （2023, March 14）. *12 Video Piracy Statistics, 6 Prevention Methods*. https://www.vdocipher.com/blog/2020/10/stop-video-piracy/