Research on the regulations and technologies of OTT TV set-top box

National Communications Commission

2023

I. Background

Over the last decade, the development of online multimedia has been rapid, diversifying the viewing and listening options for the public. Flexible OTT TV streaming options are more ubiquitous to a growing consumer base, replacing traditional broadcasting methods such as satellite or cable. Due to the convenience and accessibility of the internet, illicit groups intercept signals from cable television and satellite broadcasting services. They then relay these signals through intermediary facilities to specific OTT TV set-top boxes, so that users with such set-top boxes can access unauthorized audiovisual content for free. Such methods not only severely infringe upon the copyright of audiovisual holders and legally authorized broadcasting rights holders but also undermine the legitimate viewing market and hinder the healthy development of related industries and markets.

The use of illegal OTT TV set-top boxes can cause significant harm to the audiovisual industry and rights holders, with law enforcement often facing obstacles due to cross-border transmissions issue. When streaming media service content is combined with innovative business models, the use of illegal OTT TV set-top boxes undermines related innovations and copyrights, weakening the commercial viability of legitimate streaming media services.

Furthermore, many consumers are unaware that illegal OTT TV set-top boxes can serve as carriers for hackers and cyber intrusions, posing serious cybersecurity threats and information security crises. Therefore, many countries use this as a primary reason to discourage the public from using

illegal OTT TV set-top boxes. When illegal applications installed on illegal OTT TV set-top boxes contain destructive or privacy-infringing malicious software, these malware enable hackers and other malicious actors to invade consumers' home networks. With the continuous expansion of the IoT, the use of connected devices by consumers, businesses, healthcare, and transportation sectors has significantly increased, coupled with potential vulnerabilities in certain internal organizational networks, which may lead to security blind spots. Cybercriminals can exploit these blind spots to attack IoT devices (such as smart security cameras, webcams, smartphones, smart TVs, smart appliances, or routers), posing threats to individual, industrial, and public safety.

The regulations of copyright have been continuously impacted by technological advancements. The conveyance and exchange of these rights have evolved with technological progress, including various communication technologies such as telephones, recording products, television, broadcasting and cable networks, satellite communications, recorders, CDs, and the internet. These advancements have had significant implications for copyrights. The piracy issues arising from OTT TV set-top boxes discussed in this project are primarily due to consumers or viewers' constant desire to access movies and online content for free. There is a weak awareness of viewing and respecting genuine versions. Furthermore, with technological progress, such criminals become increasingly difficult to trace, and the development of Virtual Private Networks (VPNs) exacerbates the tracking challenge. Due to low costs associated with illegal dissemination and the inability to analyze and

monitor the volume of access to pirated information, online piracy continues to increase, not solely due to illegal set-top boxes. Countries are actively addressing and regulating related internet piracy issues.

To effectively regulate OTT TV set-top boxes, prevent the illicit use of legitimate program content, and clarify the responsibilities of regulatory authorities, this project aims to propose effective supervision recommendations to reduce the use of illicit set-top boxes and copyright infringements on the internet. This project collects and analyzes the development and regulatory methods of OTT TV in significant nations and regions, including the United States, the United Kingdom, the European Union, South Korea, Japan, Singapore, and China. It consolidates the current state of the OTT TV market, government roles, policies, and regulations across these countries. Furthermore, this project gathers and analyzes actual cases of OTT TV set-top boxes that infringe upon copyright in our country and other countries or regional organizations, in order to identify appropriate responses. To understand the regulatory and legislative needs for OTT TV set-top boxes, two seminars were conducted to gather opinions from industry experts and professionals. Additionally, three samples of OTT TV set-top boxes were examined to assess technical analysis methods and supervisory operational procedures. The focus was on detecting OTT TV set-top boxes that bind and activate unauthorized apps. This project examined the behavior of these apps to determine whether they are specifically bound to certain set-top boxes. Based on these analyses, recommendations are proposed to enhance the policies, regulations, and supervisory technologies related to OTT TV.

II. Research Methods and Process

The first part of this project focuses on the legislative analysis of OTT TV set-top boxes, considering literature, secondary data, and regulations from other major countries and regions. These legislations from foreign countries serve as reference for policy recommendations in this project. The second part utilizes technical expertise to examine OTT TV set-top boxes and understand related illegal technologies and decryption methods. To understand the regulatory and legislative needs for OTT TV set-top boxes in our country, two seminars were organized to collect opinions from industry experts and professionals. Using the opinions gathered from these seminars as a foundation, and after thorough consolidation, discussions will be held regarding the preliminary research findings to propose the most feasible and widely accepted recommendations and conclusions.

III. Key Findings

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

(a) Regulations of the OTT TV Industry

Compiling policies and regulations from major countries and regions reveals that governance regulations for the OTT TV industry are relatively limited compared to the traditional broadcasting industry. The main approach remains self-regulation within the industry.

Regarding content control, the primary focus is on regulating core values, including the protection of minors, copyright, and safeguarding personal

information and privacy. Only a few countries have been adopting a approval mode for the OTT TV industry, such as China and Singapore. Notably, China even reviews the outcomes of content production.

Figure 1. Governance Models of OTT TV Industry in Major Countries

Country	Governance Model
USA	Almost unregulated.
EU	Only regulates "video sharing platforms".
UK	Apart from regulating video-on-demand services, there is almost no regulation of internet audiovisual service platforms.
Japan	Almost unregulated.
South Korea	OTT TV operators are classified as value-added telecommunications service providers and are subject to registration and reporting. Operators must register with MSIT before commencing operations.
Singapore	Operators of television services transmitted over the internet need to obtain a Niche Television Service Licence.
China	Internet television services must have an operating license.

Source: The research findings of this project.

(b) Regulations of the OTT TV Set-Top Boxes

Regarding the regulation of OTT TV set-top boxes, since these devices are considered controlled telecommunication radio-frequency devices, most

countries and regions conduct pre-market supervision of such devices. However, the specific regulatory content varies slightly. In our country, the primary focus is on radio frequency standards and the efficient use of the radio spectrum. The European Union believes that set-top boxes should be designed to include technical features that protect privacy, personal data, guard against fraud, and maintain cybersecurity. Furthermore, China regulates the content provided by the set-top boxes. Therefore, this project categorizes the current regulatory approaches into the following three main modes: pre-market supervision, the requirement for a license to sell set-top box devices, and penalties for installing illegal streaming software that bypasses legitimate content.

i. Pre-market Supervision

OTT TV set-top boxes belong to the category of radio equipment as defined by the radio equipment directive 2014/53/EU(RED). This directive establishes a regulatory framework for placing radio equipment on the market. It ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects. These include technical features for the protection of privacy, personal data and against fraud. Furthermore, additional aspects cover interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software.

According to the radio equipment directive 2014/53/EU, set-top boxes

should be designed to protect user privacy and personal data, prevent fraud, and maintain cyber security. Moreover, if there are users, radio equipment, or third parties intending to load software into the device, the set-top box must be designed to only allow software loading if it does not compromise the subsequent compliance of the radio equipment with the applicable essential requirements. Radio equipment that does not meet these essential requirements should not be placed on the market by manufacturers, importers, or distributors.

ii. The Requirement for a License to Sell Set-top Box Devices

(i) Singapore

Set-top boxes in Singapore are classified as enhanced simplified equipment within the category of telecommunications and radio communication equipment. For the sale of telecommunications and radio communication equipment intended for local use in Singapore, it is mandatory to register the devices with the Infocomm Media Development Authority (IMDA). Before registering with the IMDA, devices must ensure compliance with relevant standards/technical specifications set forth by the IMDA regulations. Additionally, companies engaged in the import and sale of telecommunications equipment for local use in Singapore must hold a valid Telecommunications Dealer License issued by the IMDA. Therefore, entities without proper licensing are prohibited from selling related set-top box equipment.

(ii) China

The illegal distribution of OTT TV set-top boxes enables individuals to

download pirated or illegally recorded movie content, allowing viewers to access pirated audiovisual content on television or other terminal devices for free. Apart from infringing upon copyrights, this practice involves the introduction of a large amount of overseas programming without official scrutiny or permission. Consequently, it has drawn the attention of Chinese authorities, prompting the strong prohibition of the sale of illegal OTT TV set-top boxes by the National Radio and Television Administration.

According to the " Notice on the strict crackdown on unlawful and criminal activities of illegal television network receiving equipment in accordance with law," the sale of illegal set-top boxes constitutes a violation of national regulations. Engaging in profit-making activities such as producing and selling illegal TV network receiving equipment (including software), providing download services for illegal broadcast TV reception software, and offering link services for illegal broadcast TV program channels disrupts market order. Individuals found operating illegally with amounts exceeding RMB 50,000 or illegal gains exceeding RMB 10,000 will face criminal prosecution, while entities engaging in illegal businesss operations with amounts exceeding RMB 500,000 or illegal gains exceeding RMB 100,000 will also be held accountable for criminal offenses.

iii. Penalties for Installing Illegal Streaming Software that bypasses Legitimate Content

According to the United States Code 17 USC 1201(a)(2)“ No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any

technology, product, service, device, component, or part thereof, that—(A)is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;(B)has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or(C)is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.".

(c) Regulations for Prevent Internet Copyright Infringements via OTT TV Set-Top Boxes

Almost every country or region mandates that OTT TV set-top boxes play authorized content to uphold the legality of online activities. Generally, downloading audiovisual content from unauthorized or illegal sources constitutes an infringement of intellectual property rights. Furthermore, accessing unauthorized audiovisual content via streaming is recognized as copyright infringement by major countries, regardless of whether it involves the use of technical devices or OTT TV set-top boxes pre-loaded with additional software.

Various countries have proposed a range of regulations and administrative policies to address the issue of preventing internet copyright infringements via illegal set-top boxes. These approaches can be primarily categorized into three types: administrative policies, judicial approaches, and market mechanisms. Overall, major countries take the prevention of online

copyright infringements and illegal set-top boxes very seriously. According to the finding of this project, these countries can address copyright infringements through both civil and criminal regulations related to copyright. However, considering the borderless and anonymous nature of the internet, even though copyright holders have ample legal approaches at their disposal, the issues such as enforcement delays, procedural complexities, and effectiveness still need to be reconsidered. Having various enforcement approaches and policies available does not guarantee widespread implementation or true effectiveness in combating the infringement issues related to illegal set-top boxes.

In addition to civil and criminal regulations related to copyright, summarizing relevant judicial approaches, examples from the UK and the European Union stand out. Both regions have gradually adopted rapid and dynamic judicial enforcement measures targeting websites that offer infringing content for dynamic blocking. Notably, the UK has taken stringent measures, prosecuting providers of illegal set-top boxes under criminal law, citing offenses like fraud and money laundering. Conversely, the United States primarily leverages safe harbor statutes as incentives, prompting internet service providers to remove or block infringing content. Meanwhile, South Korea addresses the prevention of internet copyright infringements through specialized institutions.

Figure 2. Comparison of OTT TV Copyright Regulation and Policies

Category	Regulation and Policies	Area
Administrative Measures	Pre-equipment inspection	UK, EU, Japan, South Korea, China, Singapore, Taiwan
	Publication of blocking watch lists	USA, EU, Taiwan
	Border control, customs seizure	USA, UK, Japan
	International cooperation	EU, UK, Japan, Korea, China
	Notification and information sharing	UK, Korea, Japan
	Prohibition of unlicensed sales	Singapore, China
Judicial measures	Copyright regulations	All
	Penalties for circumvention of technological measures, equipment, and services	USA, UK, Singapore, China, Japan, Korea, Taiwan
	Safeharbor provisions	USA, EU, China, Taiwan

Category	Regulation and Policies	Area
	Injunctions	EU, UK, USA, Singapore, Taiwan
	Dynamic blocking	EU, UK
	Regulations on fraud and money laundering	UK
Market mechanisms	Financial flow and advertising mechanism cooperation	USA, UK
	Self-regulatory measures	Japan, Singapore
	Technical filtering	Korea, Netflix
	Consumer regulatory advocacy and education	EU, UK, Taiwan

Source: The research findings of this project.

B. The Detection by Technical Approach

Illegal groups create illegal app specifically designed for certain set-top boxes. They then 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 investigates OTT TV set-top boxes available in the market. We conduct packet capturing and analysis during the connection process to

understand the device's content and compare it with network transmission packet operations. This process helps determine whether the set-top boxes are linked to illicitly bundled applications. Illegal set-top box providers employ device authentication to ensure consumers buy from their company. While various OTT TV set-top box brands may have distinct practices, based on the data intercepted in this project, we have found the following:

(a) The software frequently uses 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, OTT TV set-top box providers have increasingly focused on selling "clean versions" in recent years to circumvent illegal sales. Subsequently, consumers install specific apps on their own post-purchase. Based on the technical analysis of this project, it's evident that merely downloading relevant apps does not guarantee their activation. These apps often require prior authentication, such as entering account credentials, to restrict their usage. This project find that illegal set-top boxes may function similarly to access keys. The distinct hardware encoding of the set-top

box's network card acts as vital authentication information, indicating a potential collaboration between hardware manufacturers and software providers.

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. Referring to the recycling practices of the European Union, amendments will be made to the articles, including:

i. Notification Obligation

Require operators to notify downstream manufacturers and consumers as much as possible. Reference can be made to other legislative examples in our country. The relevant text should be added to Article 23(2) of the " Regulations Governing Compliance Approval for Controlled Telecommunications Radio-Frequency Devices," stating "shall announce in mass media and notify consumers through other effective means."

ii. Restrictions on Recycling Prices

In accordance with EU regulations, relevant text should be added to Article 23(2) of the "Regulations Governing Compliance Approval for Controlled Telecommunications Radio-Frequency Devices," stating that equipment with discontinued inspection certificates may require operators at fault to reasonably and fairly recycle illegal set-top boxes circulating in the market.

The main point is that the operator's illegal behavior has been confirmed by a final judgment, so it is reasonable to require them to recycle illegal set-top boxes at a fair price. However, it is appropriate to explicitly specify this requirement in the relevant regulations.

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

According to Article 87(1)(8) of the Copyright Act: " Knowing that the works broadcast or transmitted publicly by another person infringe economic rights, with the intent to provide the public to access such works by the Internet, acting as follows, and to receive benefit therefrom: (1) To provide the public with computer programs which have aggregated the Internet Protocol Addresses of such works. (2) To direct, assist or preset paths to the public for using computer programs in the preceding item. (3) To manufacture, import or sell equipment or devices preloaded with the computer programs of the first item." Therefore, according to the above provisions, the sale of set-top box devices must not include pre-installed or default computer programs for viewing unauthorized audiovisual content, nor should they instruct or assist consumers in installing such illegal computer programs. If illegal operators are caught, they shall be subject to criminal liability under Article 93 of the Copyright Act, with a maximum imprisonment term of less than 2 years or a fine of up to NT$500,000. Furthermore, according to Article 22(2)(8) of the Regulations Governing

Compliance Approval for Controlled Telecommunications Radio-Frequency Devices, "Prohibition to sell a CTRFD or non-plug-and-play radio-frequency module（component）that has been approved due to a dispute over authority of agency, patent or copyright which has been decided by the court of law against seller;"

To comply with the above regulations, some illegal set-top boxes may be marketed as "clean versions," meaning that the set-top box devices are initially sold without pre-installed computer programs for viewing illegal or unauthorized audiovisual content, nor do they contain default illegal links. Sales personnel generally do not instruct users to view illegal content, so they are considered legal for sale. However, after purchasing such set-top box devices, consumers often install the aforementioned computer programs through internet searches, making it difficult to effectively prevent the circulation of illegal set-top boxes in the market.

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

Our judicial enforcement units execute "application for court domain name seizure and implementation of DNS RPZ" through TWNIC, successfully seizing domain names and stopping the resolution of illegal audiovisual source URLs. Therefore, through court ruling for provisional attachment, the implementation of DNS RPZ to block signal reception ensures that infringing content cannot be accessed by visitors through the website. This approach is legally and operationally sound, and has been recognized in judicial practice in Taiwan.

Regarding the seizure of infringing websites, it is primarily based on the provisions of Articles 122 and following of the Code of Criminal Procedure, as well as Articles 133 and following regarding search and seizure. Judicial enforcement authorities can confirm the operators behind the scenes through investigation procedures, then proceed with regular search and seizure procedures to seize their computers and phones. With interrogation, search, and telecommunication investigation capabilities, law enforcement can directly access the account credentials such as usernames and passwords of the website, enabling the closure of infringing websites or replacement of their entry pages.

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

i. Integrating Pre-Market Review Criteria Based on the EU Radio Equipment Directive:

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.

The act covers all products with digital elements, except for those already subject to specific regulations (e.g., medical equipment, aviation, or automotive). Different security requirements will apply to products with varying levels of risk, with a few requiring third-party assessment. Products with digital elements are defined as those where the device or network is expected or can reasonably be expected to directly or logically connect data. Two main objectives were identified aiming to ensure the proper functioning of the internal market: (1) create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously

throughout a product's life cycle; and (2) create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements. Four specific objectives were set out: (i) ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle; (ii) ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers; (iii) enhance the transparency of security properties of products with digital elements, and (iv) enable businesses and consumers to use products with digital elements securely.

Given the legislative trends abroad, domestic authorities responsible for cybersecurity and personal data should comprehensively review all relevant security regulations concerning digital products, establish clear and explicit standards, facilitate businesses' targeted investments in information security and personal data protection, and enable consumers to use all interconnected digital products with greater peace of mind, aligning with international trends.

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 illegal infringements associated with set-top boxes is not the sole responsibility of a single competent authority. Relevant authorities must establish robust pre-review and detection mechanisms for market

oversight. During operations, it is essential to strengthen inspection, investigation, and whistleblower mechanisms. Strict oversight of illicit market activities should be implemented, enhancing administrative inspection measures to deter entities engaged in copyright infringements. Upon detecting and confirming any illicit activities, regulatory sanctions should be applied accordingly. Furthermore, a comprehensive and effective set of measures needs to be established to tackle these issues effectively.

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

Drawing inspiration from the practices of the Korean Copyright Protection Agency (KCOPA), a cross-ministerial working group should be established. This group would be responsible for deliberating on matters of copyright protection, and implementing projects required for copyright protection. The timeline for this initiative can be further divided into short-term, medium-term, and long-term plans:

i. Short-term

In the short term, a cross-ministerial working group should be formed. This group will convene relevant competent authorities to establish a collaborative approach to enforce various copyright act and regulations, thereby enhancing the prevention of copyright infringements on the internet.

ii. Medium to Long-term

To establish a comprehensive system akin to the "Prevention → Detection → Analysis → Action" model of the 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.

In analyzing the behavior of playing infringing video apps on set-top boxes, this project has identified the relevant authentication hosts and the location of infringing video data. This information can serve as evidence, not only to enhance credibility when submitted to the court for trial but also for the establishment of a dedicated technical unit in the future to detect illegal signal sources. Establishing a joint defense mechanism and promptly notifying relevant regulatory authorities will deplete the resources of pirates. This ensures that internet governance achieves the intended effect. It also safeguards legitimate businesses, fosters a mutually beneficial environment between the government and the private sector, and enhances the international image of our country.

(c) OTT Industry Collaboration and International Cooperation in Combating Illegitimate Activities

Taiwanese entities can establish industry alliances and engage in international cooperation as part of a key strategy to combat piracy. This includes:

i. Establishment of Industry Alliances:

Clearly define alliance objectives, such as reducing the impact of piracy, protecting intellectual property rights, and increasing legal market share. Ensure that all members share the same core values. Actively invite major media and entertainment companies in Taiwan to participate, including production companies, distributors, and streaming platforms. The strength of the alliance depends on the diversity and quantity of its members.

Create working groups dedicated to addressing piracy issues, including technical experts, legal experts, and publicity specialists. These groups can collaborate to develop specific strategies. Develop alliance policies to regulate the behavior and obligations of members. This may include common monitoring standards and procedures for addressing piracy. Share resources, including technical tools, legal resources, and monitoring systems. This can help improve the efficiency of piracy prevention across the entire industry.

ii. International Cooperation:

Establish collaborative contact points internationally and engage in active communication with relevant agencies and industry alliances in other countries. Establish representatives in the United States, Europe, Asia, and other regions. Taiwanese industries can consider joining international anti-piracy organizations such as the Motion Picture Association (MPA) or relevant regional organizations to access more resources and cooperation opportunities.

Actively participate in international conferences and seminars to share

experiences, learn from successful experiences in advanced countries, and expand international contacts. Collaborate with law enforcement agencies such as Interpol to share intelligence and jointly combat cross-border piracy. Participate in international piracy cases, support other countries in combating piracy, and establish a positive international image.

(d) Strengthening Incentives and Public Education

Government agencies can encourage the public to use legitimate set-top boxes and refrain from purchasing pirated ones through various incentive programs, thereby safeguarding intellectual property rights. These include:

i. Subsidy Programs

Introduce subsidy programs that provide a certain amount of financial assistance or discounts to families choosing legitimate set-top boxes, encouraging their purchase.

ii. Priority for Legal Content

Prioritize the provision of legally authorized audiovisual content in public institutions, schools, and communities to reduce incentives for using pirated set-top boxes.

iii. Information Sharing and Interaction

Establish a community platform for legitimate set-top box users to promote information sharing and interaction. Organize corresponding community activities to enhance social identity with the use of legitimate set-top boxes.

Collaboration with Legal Operators: Collaborate with legal cable TV and

internet service providers to jointly promote the advantages of legitimate set-top boxes, such as high-definition content, stable services, and legal compliance.

iv. Transparency of Information

Provide the public with easily understandable information explaining the risks and potential consequences of using pirated set-top boxes. This can be done through official websites, educational brochures, and other resources.

v. Discounts for Legal Services

Encourage providers to offer special incentives to users of legitimate set-top boxes, such as price discounts, gifts, loyalty points, special programs, or high-speed internet services, to increase motivation to use legitimate services.

V. Conclusion

This project primarily focuses on OTT TV set-top boxes, exploring regulatory methods and actions from both legal and technical perspectives to provide recommendations for our current system. Law and technology are inseparable; regulations formulated without considering technical feasibility may lead to ineffective enforcement and limited practical benefits. In this regard, our project aims to identify technical approaches that support the implementation of regulations while also analyzing the operational methods of illegal OTT TV set-top boxes to provide feedback for regulatory improvements and suggestions.

The widespread presence of sellers or users purchasing set-top boxes and subsequently installing software via the set-top boxes' internet connection to access unauthorized streaming media websites, thus enabling the viewing of audiovisual content, is a prevalent issue in the market. Through such illicit streaming devices, OTT platform operators, content creators, and rights holders suffer significant economic losses, posing a pressing problem that many countries are eager to address.

Currently, our country adopts a passive detection approach to illegal set-top boxes. To enhance effectiveness further, adopting proactive defense mechanisms could be considered. Since audiovisual applications require proximity to users, video content is typically hosted within domestic internet service providers' data centers. By requesting cooperation from these providers for convenient search and blockage methods to address commissioned demands for audiovisual services, rapid responses to infringement incidents can be facilitated. Even if the infringing content originates from abroad, effective blocking or prohibition measures can be implemented to prevent infringement activities.

Based on the aforementioned research, most countries currently have copyright-related civil and criminal regulations to address acts of copyright infringement through set-top boxes through judicial procedures. While copyright holders have a range of legal enforcement mechanisms to assert their rights, the primary issues lie in the limitations of time, procedural complexity, and enforcement effectiveness. Therefore, the availability of numerous enforcement measures does not necessarily translate into widespread adoption or genuine efficacy in practice.

Looking ahead, illegal set-top box operators may evolve, potentially even adopting practices that do not bind to specific set-top boxes. This means that regulatory focus may shift from "OTT TV set-top boxes" to encompass the broader "OTT TV" domain. To address this, collaboration between government and private entities is essential to swiftly identify infringement activities and strengthen response measures through proactive defense strategies. However, regulatory actions can be contentious, potentially encroaching on freedom of speech. Therefore, further research is warranted to devise more nuanced regulations.