E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/ACE/12/10 REV.
ORIGINAL: ENGLISH
DATE: JULY 21, 2017

Advisory Committee on Enforcement

Twelfth Session
Geneva, September 4 to 6, 2017

INSTITUTIONAL ARRANGEMENTS CONCERNING INTELLECTUAL PROPERTY ENFORCEMENT POLICIES AND REGIMES TO ADDRESS ONLINE INFRINGEMENTS

Contributions prepared by Italy, Republic of Korea, Thailand, the United Kingdom, Europol and the Motion Picture Association of America, Inc.

1. At the eleventh session of the Advisory Committee on Enforcement (ACE), the Committee agreed to continue to consider among other topics the "exchange of information on national experiences relating to institutional arrangements concerning intellectual property (IP) enforcement policies and regimes, including mechanism to resolve IP disputes in a balanced, holistic and effective manner".

2. This document contains the contributions prepared by four Member States (Italy, Republic of Korea, Thailand and the United Kingdom), one Non-State Member and one Observer organization on enforcement mechanisms aimed at curbing the growth in the online trade of IP infringing goods and addressing the anonymity, velocity and transnationality of these infringements. Mechanisms discussed include the establishment of specialized police units, intelligence-based investigations, computerized platforms that facilitate online monitoring and data collection, the "follow the money" approach tracing cash flows, website blocking, targeting IP infringing domain names, voluntary measures, and closer cross-border cooperation among enforcement agencies, with right holders and with online intermediaries.

3. The contributions from the police (national and regional), the intellectual property office, the prosecutor's office, the judiciary, and the right holders, demonstrate the challenges of online IP enforcement, the multiplicity of actors engaging in online IP enforcement and the corresponding need for close collaboration in addressing infringements that are frequently of transnational character. The contributions underscore the importance of taking a holistic and comprehensive approach and promoting respect for IP.

4. The contributions are in the following order:

[Contributions follow]

THE ITALIAN EXPERIENCES IN THE FIGHT AGAINST INTELLECTUAL PROPERTY INFRINGEMENTS ON THE INTERNET

Contributions prepared by Col. Vincenzo Tuzi, Head, Intellectual Property Protection Special Unit, Guardia di Finanza, and Dr. Stefano Vaccari, Head, Central Inspectorate for Quality Protection and Fraud Repression in Agri-food Products Department (ICQRF), Ministry of Agricultural, Food and Forestry Policies, Rome, Italy[*]

ABSTRACT

Guardia di Finanza is a law enforcement agency in Italy, operating under a military organization with specific competence in economic and financial matters on the basis of special powers granted by law. The agency has committed to close cooperation with a view to substantially reducing levels of counterfeit goods within Italy and in the European Union. In 2014, it established the Anticounterfeiting Information System (SIAC). The system comprises of an integrated technology platform with a database containing historical and statistical information alongside pictures, documents, information and utility referrals on marks and products, assembled for effective operational uses. A dedicated application, Contraffazione Online Brand Library (COLIBRI), is in the final stages of completion and will facilitate targeted counter-action against intellectual property (IP) infringement on the internet, which now represents the new frontier of counterfeiting.

Counterfeiting on the web and on social networks is one of the most important threats to the future sustainability of intellectual property rights (IPRs). Cooperation with IP right holders is the most effective response to this challenge. Greater collaboration is also required with those working in the area of electronic payments so as to explore the potential of the "follow the money" approach to enforcement. In addition, the increase of undercover operations, such as simulated purchase, would be desirable.

The Central Inspectorate for Quality Protection and Fraud Repression in Agri-food Products Department (ICQRF) is the Competent Authority of the Ministry of Agricultural, Food and Forestry Policies, responsible for preventing and repressing fraud related to agri-food products. In 2016, the ICQRF carried over 48,000 inspections and analytical checks, examining 53,427 products and verifying 25,190 producers.

Effective answers to issues related to the proliferation of online intellectual property infringements have been provided by the ICQRF, which works to make European Union (EU) regulatory instruments more effective and creates new modes of action by implementing cooperation and Memoranda of Understanding (MoU) for the protection of protected designations of origin (PDOs) and protected geographical indications (PGIs) with the major e-commerce platforms such as eBay, Alibaba and Amazon.

[*] The views expressed in this document are those of the authors and not necessarily those of the Secretariat or of the Member States of WIPO.

I. THE EXPERIENCE OF GUARDIA DI FINANZA

A. FACTS AND FIGURES

1. According to official data from survey agencies, the turnover of the so-called "counterfeit industry" in Italy amounts to almost seven billion euros. A survey completed by the CENSIS, on behalf of the Italian Patent and Trademark Office, Directorate General of Combating Counterfeiting, Ministry of Economic Development, estimated that, in terms of revenue loss, counterfeiting accounts for almost 6.9 billion euros, equal to almost two per cent of the total state revenue[1].

2. The results achieved by the enforcement action led by the Guardia di Finanza[2] and the other Police Forces allowed the identification of two peculiar elements underlining the evolutionary trend of the counterfeiting industry.

3. The first is that in recent years the counterfeit market has grown exponentially in volume, with seizures of counterfeit or dangerous products conducted by the Guardia di Finanza rising from 90 million in 2006 to over 393 million in 2015.

4. The second peculiarity is the broad extension of the variety of products being counterfeited, which now include not only luxury goods or expensive commodities, typically in the clothing sector, but also more widely used consumable goods. The most alarming aspect is the rise in the number of seizures of products that are dangerous to the purchasers' health and to public safety: this issue is particularly prevalent in toys, infant products and medicines.

5. The global framework and high scope for profitability in the counterfeit industry indicate the considerable interest and growing involvement of organized crime, both nationally and overseas.

6. In 2015 alone, the individuals reported to the Judicial Authorities numbered 9,416. Half of the subjects reported for counterfeiting are Italian (precisely 52.34 per cent). In addition, over 11,000 enforcement operations allowed for the seizure of more than 393 million products.

7. Numerous surveys also confirm that the internet should rightly be considered as the "new frontier" of counterfeiting and piracy, due primarily to its enormous ease of access, the speed of online transactions and its guarantee of substantial anonymity for suppliers and customers. In the last three years, Guardia di Finanza carried out more than 5,000 web domain seizures.

8. The extent of the counterfeiting problem and the alarming evolutionary trends of the phenomenon, call for countermeasures which are rooted in international cooperation and inter-institutional collaboration. With this in mind, an important multi-agency platform was introduced in 2004 at the Ministry of Internal Affairs, Central Criminal Police Directorate, leading to a systematic exchange between experts of the Guardia di Finanza, Carabinieri and State Police forces, all being part of a working group that also includes the Association of Italian Municipalities and the Italian Authors and Publishers Association (SIAE). Existing cooperation

---

[1] Extent, Characteristics and More Information about Counterfeiting - 2012 Final CENSIS Report - http://www.uibm.gov.it/attachments/Dimensioni%2c%20caratteristiche%20e%20approfondimenti%20sulla%20contraffazione%20-%20Rapporto%20finale%20%282012%29.pdf.

[2] It is worth to highlight the specific characteristics of Guardia di Finanza modus operandi, which is characterized by the use of so-called "cross-operating modules", where multiple powers are jointly exercised: (1) Criminal Police, where the activity is initiated by way of delegation from the Judiciary or otherwise, even if it has been started on its own, then it has led to the identification of a case concerning criminal law; (2) Tax Police, in relation to the investigation of violations of the tax laws; (3) Administrative Police, for the verification of administrative violations.

frameworks with the Italian Patent and Trademark Office, Directorate General of Combating Counterfeiting Ministry of Economic Development (UIBM) and with the National Anti-Counterfeiting Council (CNAC) have also been consolidated.

9. The Ministry for Economic Development has also initiated the Intellectual Property – Elaborated Report of the Investigation on Counterfeiting (Project IPERICO)[3], an integrated database chronicling the activities conducted against counterfeiting.

10. Guardia di Finanza performs anti-counterfeiting along three distinct lines.

11. The first line of defense is the posting of Guardia di Finanza officers in the Customs areas, with the aim of catching illicit traffics of counterfeit and dangerous goods from non-EU countries, before they are introduced into the domestic markets. This measure is incapable of independently countering the counterfeit industry as only 10 per cent of imported goods is inspected by Customs officials due to the enormous volume of trade.

12. The second line of anti-counterfeiting is the systematic economic control of the territory, carried out by our street patrols, who coordinate and cooperate with other police forces and local police agencies, to ensure a timely and diffused reaction to minor illicit traffic and retail sales.

13. The third line of anti-counterfeiting is comprised of the actual investigative activity conducted by the Tax Police units which is oriented not towards seizure at the point of sale to the public, but mainly towards identifying, through incisive and consolidated intelligence activity, the full extent of the fake distribution chain in order to identify the importation channels, illegal production sites, storage areas and major distribution networks of the counterfeit goods. This represents the most significant aspect of the Guardia di Finanza's enforcement action, which allows for the dismantling of the cover behind which criminal organizations hide culpable individuals, proceeds of infringing activities and resulting re-investments. The investigative activity also assists in identifying the locations at which counterfeit merchandise is assembled.

14. The economic and financial police powers allow for a much needed interdisciplinary approach to tackling these forms of illegal activities. The transversal dimension is always present in matters of counterfeit goods, and only a global view, guaranteed by a synergic combination of risk analysis, territory control and investigation, can allow for the achievement of improved, far reaching and lasting results.

B. COUNTERFEITING ON THE WEB

15. Counterfeiting on the internet and through social networks has become insidious and dangerous due to several aspects. The individuals participating in counterfeiting through social networks range from housewives, to university students and the unemployed. They belong to all social classes and occupations, though they are predominantly young. Many hold a certain bidirectional attitude towards the purchase of illicit goods. In many cases a buyer could be a seller at the same time and vice versa.

16. Regarding the supply chains of particular illicit goods, two main systems for stocking illicit goods were identified. The first is representative of street vendors, featuring poor quality items and few items available in the stock of the counterfeiter. This corresponds to very low income.

---

[3] IPERICO (Intellectual Property – Elaborated Report of the Investigation on Counterfeiting) http://www.uibm.gov.it/iperico/home/.

The second is characteristic of internet sellers and features higher quality and more income potential due to increased storage capacity.

17. In cases of counterfeiting through social networks, Guardia di Finanza is used to approaching purchases with intelligence or through direct information provided by the IP right holder. We strongly believe in the usefulness of cooperation with IP right holders in matters of enforcement. For this reason, in 2014, a special online framework – the Anti-counterfeiting Information System (SIAC) – was created through which all registered companies can share information about their IPRs.

18. This online information can be used by all territorial units of Guardia di Finanza to enhance the results of anti-counterfeit and anti-piracy enforcement activities. There are two different procedures that can be used alternatively or jointly. The first is commenced through the Italian Competition Authority (Antitrust), and the other through the Judicial Authority. In both cases, investigations lead to website suppression, identification of all involved individuals, cash flow tracing ("follow the money"), "follow the hosting" and capital measures for criminal laws or tax purposes.

19. Through the "follow the money" approach, we are able to identify and block financial support for online piracy and counterfeiting by reconstructing cash flows. Moreover, we have developed a new investigative strategy called "follow the hosting". Using this method of investigation, once an illegally operating site is identified, officials are able to request that providers verify the presence of one or more of the dedicated Web Hosting, VPS hosting, Cloud Hosting and Server services. In this way, anonymity in services can be overcome and the responsible actor of a domain performing illegal transactions can be identified.

20. We manage all information (e.g., phone numbers, websites, email addresses, persons and companies identified, financial information) relating to counterfeiting via social networks. Following extensive investigations, search warrants may be obtained from the Judicial Authority that allow us to perform a deeper investigation on specific cases, including conducting a search on private premises, economic and financial investigations, analysis of computer forensics, and bank and postal account investigations. This way a complete report capable of finalizing a case is compiled. The "follow the money" approach is particularly useful to the gathering of such information. Prior to or alongside this process, there exists the option to perform undercover operations – particularly through simulated purchase – in cooperation with IP right holders. The advantage of this approach includes the potential to find out useful information such as the origin of the illicit goods, the identity of the sender, and how the system of payment operates. Case studies appear to suggest that counterfeiters utilize a "zero stock attitude", making it harder to find large volumes of infringing stocks through a search warrant.

21. Case studies indicate that infringers use precautions, such as changing phone numbers every two to three months and using social networks for initial contact with consumers only, before moving toward more encrypted means that are very difficult to access by law enforcement. When sending illicit goods, the common postal system is frequently used while payments are normally made using electronic currency. We have evidence to suggest the increase of smarter strategies, such as the use of cash upon delivery systems of payment, which increase the difficulty of tracing payments.

22. An illustrative case study on the problem of counterfeiting via social networks is that of a recent case in Sicily involving a husband and wife in their late twenties selling counterfeit luxury watch products through a social network web profile. In three years the couple gained over 750,000 euros through the sale of counterfeit watches. With this money, they were found to have purchased a luxury car and arranged for a shadow company with the aim of performing self-money laundering of the proceeds of illicit trafficking.

C. THE HOLISTIC APPROACH: THE SIAC

23. SIAC is a project co-funded by the European Commission and entrusted by the Ministry of Internal Affairs to Guardia di Finanza, confirming the key role played by the Guardia di Finanza in this operational area.

24. Guardia di Finanza is aware of the need to create a comprehensive system, incorporating the coordination of all the institutional components and the actors involved in the fight against the counterfeit and piracy industry. The initiative came about through the recognition that in order to face a multi-dimensional and transversal illegal phenomenon such as counterfeiting, all institutional bodies and players involved in combating the industry should join forces.

25. On this basis, the project has been conceptualized as a multifunctional computerized platform made up of different applications aiming to perform the following tasks:

- provide anti-counterfeiting and anti-piracy information for consumers;
- facilitate cooperation between institutional bodies, in particular between Police Forces, including the Municipal Police; and
- facilitate cooperation between institutional bodies and private companies.

26. The SIAC is first of all based on a website that provides an updated portrait of the actions led by the various institutional players that tackle the counterfeit and piracy market, providing users with suggestions and practical advice to avoid buying counterfeit or dangerous products. The system also allows the IP owners to actively cooperate in prevention and suppression actions by sending information about their affected products – through the provision of images, information sheets, expert reports, technical advice, and other formats – for ready reference by the territorial units on the ground.

27. A computerized platform reserved for the Guardia di Finanza and the other Police Forces (including the Municipal Police) is planned for inclusion within the project. This platform will provide innovative ways to collect data, combining all the operational results so as to ensure a more effective and timely analysis of information of particular investigative relevance.

28. Finally, a dedicated application, the Contraffazione Online Brand Library (COLIBRI), is being completed that will allow a more targeted counter-action against counterfeiting and piracy on the internet, which now represents, in every respect, the new frontier of counterfeiting.

II. THE EXPERIENCE OF THE CENTRAL INSPECTORATE FOR QUALITY PROTECTION AND FRAUD REPRESSION IN AGRI-FOOD PRODUCTS DEPARTMENT (ICQRF)

29. E-commerce platforms (such as eBay, Alibaba and Amazon), Social Networks (Facebook, Instagram, WeChat, etc.), and regular websites have enormously expanded the marketing opportunities for millions of producers and billions of consumers. In the agri-food sector, the worldwide growth of e-commerce has revolutionized the market by allowing small Italian producers to reach distant markets. The strong appeal that the “made in Italy” brand has throughout the world has clearly stimulated producers from other countries to propose evocative or usurpatory goods carrying protected names or names clearly evocative of a fake Italian origin.

30. Recent studies show that nearly three billion people in the world use the Internet, and about one billion and two hundred million of them buy online. In 2015, online sales of products and services amounted to 1.671 trillion US dollars and about 7.4 per cent of global retail sales -- an increase of 350 billion US dollars over the previous year. It is estimated that by 2019, these values will more than double, reaching the figure of 3.578 trillion US dollars, or 12.8 per cent of retail sales globally.

31. The Central Inspectorate for Quality Protection and Fraud Repression in Agri-food Products Department (ICQRF) has about 800 units, 29 offices in Italy and six analysis laboratories, all with European Union (EU) accreditation. The ICQRF is also a sanctioning authority for administrative violations in the agri-food sector and plays a major role in countering agri-food criminality and conducts numerous criminal investigations by delegation of the Italian judiciary.

32. In the framework of control activities, ICQRF has a specific action program on the "control on Regulated Food Products e-commerce", whose objective is to protect consumers and traders from unfair competition through a check of the websites and information contained therein about the marketing of foodstuffs. Controls concern internet sales and all forms of communication aimed at promoting, directly or indirectly, agri-food products on the web.

33. A great deal of attention is devoted to protecting quality products with protected designations of origin (PDOs) and protected geographical indications (PGIs) on the web. Article 13 of the EU Regulation No. 1151/2012[4] lays down a number of provisions for the protection of PDO and PGI products, stating that the registered names are protected against any direct or indirect commercial use on generic products, and against any misuse, imitation, evocation or any other practice that may mislead the consumer about the true origin of the product.

34. Overall, in about three years of activity, ICQRF has operated on more than 1,800 worldwide and web-based operations for the protection of Italian products, with interesting results, described below.

35. From 2014 to 2017, the ICQRF, taking advantage of the *ex officio* international protection of PDO and PGI products, resolved 248 cases of usurpation, evocation, direct or indirect commercial misuse, misleading advertising on quality, origin, etc. Infringements took place mostly on the web. In the process of resolving the cases, the ICQRF contacted 15 EU Member States authorities (Austria, Belgium, Cyprus, France, Denmark, Finland, Germany, Greece, Latvia, Netherlands, Poland, Portugal, Spain, Sweden and United Kingdom (UK)) and Switzerland.

36. As in the case of *ex officio* protection, a mechanism for cooperation between Member States in the EU has been established for the protection of PDO and PGI wine products (and generic vineyards) through Regulation (EC) 555/2008[5]. Article 82 (2) of this Regulation provides that each Member State designate a single contact body responsible for contacts with other Member States and with the Commission. The contact bodies shall transmit and receive requests of cooperation on wine controls and shall represent their State in relation to other Member States. The ICQRF has commenced 768 infringement procedures with important results.

[4] Regulation (EU) No 1151/2012 of the European Parliament and of the Council of 21 November 2012 on quality schemes for agricultural products and foodstuffs.

[5] Regulation (EC) No 555/2008 of 27 June 2008 laying down detailed rules for implementing Council Regulation (EC) No 479/2008 on the common organisation of the market in wine as regards support programmes, trade with third countries, production potential and on controls in the wine sector.

COOPERATION WITH WEB PLATFORMS -- EBAY, ALIBABA, AMAZON

37. One of the most innovative activities carried out by the ICQRF on the protection of Italian agro-food is its cooperation with e-commerce marketplaces. If, on the one hand, online commerce offers multiple benefits to consumers and businesses by greatly widening the chances of choice and new investments, on the other hand it represents a new frontier for fraud that is not easy to combat due to the development of telematic transactions and the possible spread of illegal conduct beyond national borders.

38. In response, the ICQRF has activated all available enforcement tools: from detecting violations, to commitments with other Member States, to moral suasion.

39. Under Article 14 of Directive 2000/31/EC,[6] Internet Hosting Providers (IHPs) have no general obligation to monitor sales activities in the network as they have no general obligation to search for illegal activity that could violate third party rights. If, however, IHPs become aware of unlawful activities on their platform, they are required to remove the unlawful content and disable their access to users.

40. In addition, corporate policies of large marketplaces include provisions for the suspension of an account if the same advertiser has instigated multiple illegal activities. Therefore, in order to avoid any kind of liability, IHPs have set up systems for the protection of IP rights (IPRs) that allow right holders to report any infringement: this kind of complaint procedure is known as “Notice and Take-down”.

41. EBay has created the Verified Rights Owner (VeRo) program that allows owners of IPRs (such as copyright, trademarks, patents and PGIs) to report any violations of their legitimate rights. The ICQRF participates in this program, as a representative of the Ministry of Agricultural, Food and Forestry Policies, a holder of IPRs for Italian PDOs and PGIs, and is able to identify potentially non-compliant advertisements and request their removal. In addition, the ICQRF has created its own web page on the eBay platform in order to communicate directly with users and inform them about European and national legislation on compulsory information for agri-food products and product protection issues relating to PDO and PGI. In practical terms, cooperation between ICQRF and eBay has resulted in a simplified procedure following the agreement to a MoU: eBay provides the ICQRF with a Violation Notice format which can be filled in, specifying, in particular, its references and, above all, the “Object Number”, identifying the unlawful item detected on the platform. The second step involves submitting a full violation notification to the VeRO e-mail address, which, if the request proves to be legitimate, deletes the unlawful listing. This simple, and effective system allows this Administration to remove irregular entries from the eBay platform in a very short time.

42. From 2014 to 2017, ICQRF reported to eBay almost 523 irregular advertisements.

43. Furthermore, ICQRF’s cooperation with the Alibaba Group demonstrates that with the right tools and with specific agreements between parties, performing effective controls on the web is possible. Last August, an important MoU was signed, which recognized the ICQRF as a “right holder” of Italian geographical indications, enabling it to join the Intellectual Property Protection program, which allows right holders to submit online complaints about infringements to the platform. Results were achieved quickly. From 2015 to 2017, 103 irregular listings have been removed, in a broad range of cases.

[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

44. Last but not least, without having signed any MoU, in the first half of 2016 the ICQRF implemented a satisfactory collaboration with Amazon. The collaboration is conducted through the exchange of reports sent to the Amazon Europe Legal Department, concerning violations found on its platforms on European domains. In this case too, the results have been remarkable. To date, 168 irregular listings evoking/misusing Italian PDO and PGI wines have been reported.

45. Overall, the ICQRF has acted within the largest e-commerce marketplaces on 794 complaint procedures with a 98 per cent success rate.

46. Such innovative cooperation shows that protection of customers and of the European cultural heritage on the internet is possible. The over 1,800 actions undertaken by the ICQRF in recent years for the protection of Italian food and feed represent an interesting case study in the protection of geographical indications. The high success rates show that there is a strong convergence of interests between marketplaces in offering authentic commercial products on their platforms and the anti-fraud methodology adopted by the ICQRF, which has proven to be very effective in “cleaning up” online marketplaces from irregular products.

47. Equally important is the cooperation with other control authorities: in addition to establishing close ties with European Authorities, the ICQRF has in recent years put in place operational agreements with the United States Food and Drug Administration (FDA) and Alcohol and Tobacco Tax and Trade Bureau (TTB) as well as with China’s General Administration of Quality Supervision, Inspection and Quarantine (AQSIQ) in order to foster knowledge of the issues related to the protection of PDO and PGI products and of the most efficient anti-fraud solutions.

INSTITUTIONAL ARRANGEMENTS PUT IN PLACE IN THE REPUBLIC OF KOREA TO ADDRESS THE PROLIFERATION OF COUNTERFEIT GOODS ONLINE

Contribution prepared by Mr. Lim Junyoung, Assistant Director, Multilateral Affairs Division, Korean Intellectual Property Office (KIPO), Daejeon, Republic of Korea[*]

ABSTRACT

The Korean Intellectual Property Office (KIPO) has a responsibility to respond to harm caused by the widespread dissemination of counterfeit goods. In order to effectively approach this issue, several institutional arrangements have been implemented and utilized.

The Special Investigation Police (SIP) for Trademark was created by KIPO to enhance law enforcement on counterfeits, and an online law enforcement task force was assembled to regulate online transactions of suspected counterfeit goods. KIPO also established the Intellectual Property Online Monitoring System (IPOMS), the Counterfeit Goods Reporting Center, and the Anti-Counterfeiting Council.

However, there are limitations bringing perpetrators to justice. It is necessary to push for the enhancement of international cooperation in order to arrest perpetrators and block sources of distribution of counterfeit goods.

KIPO is continually working to maximize its efforts to create a system that promotes genuine innovation and to curb the marketing, distribution and sale of counterfeit goods, and plans to expand upon these endeavors.

I. BACKGROUND

1. Intellectual Property Rights (IPRs) are a key component of product and service competitiveness, and are perceived as an important resource capable of providing value-added benefits. However, as information and communication technology progresses, the use of IPRs readily spread throughout the world, but also brought attention to the ease in which IPRs infringement could occur. The size of the counterfeit goods market in the Republic of Korea is estimated at around 4.3 billion USD (about 2.0 billion USD worth of goods from abroad and about 2.3 billion USD worth of goods produced domestically).

2. In particular, the online sale of goods via social networking services (SNS) and mobile phones is explosively increasing and the distribution and sale of counterfeit goods have correspondingly soared. It is clear that as the nature of communication between individuals through SNS becomes more diversified, the increasingly private and sophisticated distribution of illegal counterfeit goods resulting from this development is in urgent need of preventive measures.

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

II. MAIN ACTIVITIES

A. SPECIAL INVESTIGATION POLICE (SIP) FOR TRADEMARK AND ONLINE LAW ENFORCEMENT TASK FORCE

3. The Korean Intellectual Property Office (KIPO) has actively pushed for the introduction of a special judicial police authority to eradicate distribution of counterfeit goods and strengthen the foundation of IPR protection. In 2010, KIPO created a Special Investigation Police (SIP) for Trademark as a way of enhancing law enforcement against counterfeits, and established offices in the cities of Seoul, Busan, and Daejeon.

4. In November 2011, KIPO established an online law enforcement task force equipped with digital forensic equipment to firmly regulate online transactions of counterfeits, arrest online sellers of counterfeit goods, and block and/or shut down offending websites.

5. Moreover, SIP has strengthened its strategy for investigations into the manufacturing and online distribution of counterfeit products through the following actions:

- conducting investigation into repeatedly closed or blocked websites on suspicion of selling counterfeit goods;
- building a database and analyzing information from recurrent resale sites which are either from servers abroad or have had many sanctions imposed upon them;
- cooperating with the Korean Customs Service to place adequate border measures;
- encouraging online shopping mall operators to voluntarily delete counterfeit goods distribution sites and to voluntarily monitor counterfeit goods distribution; and
- sharing information and conducting joint crackdowns with other related organizations in order to improve effectiveness.

B. INTELLECTUAL PROPERTY ONLINE MONITORING SYSTEM (IPOMS)

6. In 2010 KIPO established the Intellectual Property Online Monitoring System (IPOMS), an online monitoring system that, in collaboration with the Korean Intellectual Property Protection Agency (KOIPA), a public organization affiliated with KIPO, detects, deletes and/or blocks access to listings of counterfeit goods posted on Korean online marketplaces, auction sites, and individually owned shopping websites.

7. IPOMS uses an automatic monitoring system that aggregates information from sale postings in online open markets and detects counterfeit goods by consulting detection keywords, blacklists, and price information. If the system detects the presence of counterfeit goods, the open markets are then notified so they can voluntarily stop the sale of those goods. After the identification of the counterfeit and the interruption of sale, the system prevents further offenses by blacklisting the seller's ID. The online open markets also prevent registration from blacklisted sellers by monitoring the sellers' personal information.

8. If IPOMS detects a personal online shopping website operating in counterfeit goods, professional monitors gather evidence of additional sales and request a review by the Korea Communications Standards Commission. Access to the site is then blocked or the site is shut down completely. Repeat and large-scale counterfeit sellers may be investigated by the SIP, depending on the circumstances of the case.

9. In addition, KIPO is constantly working to improve IPOMS' functionality. In 2014, a function was added to automatically access a site's bulletin board on an online shopping mall and capture images of information that can be used as evidence of sale of counterfeit goods, and in 2015, a function of collecting URL information of online shopping malls selling counterfeit goods was introduced. The information is extracted from a community or blog site then transferred to a portal site, allowing for the identification and extraction of the URL of the online retailer selling counterfeit goods. In 2016, KIPO expanded the scope of IPOMS' information collection to include mobile functions.

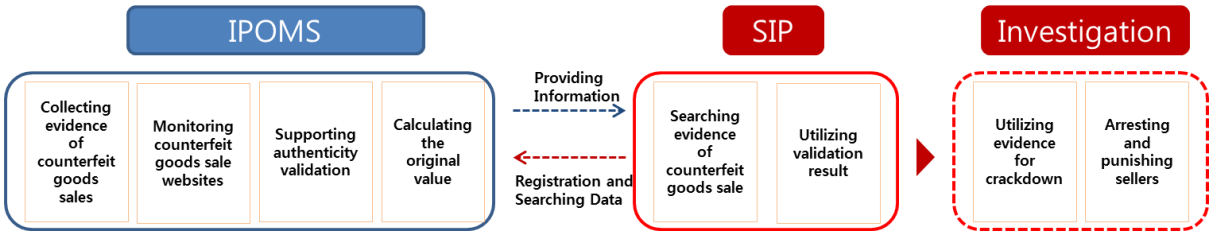
10. In 2016, KIPO prevented 5,888 sales of counterfeit goods in open markets and shut down 368 shopping websites. It also succeeded in confiscating 31,948 counterfeit goods, most of which were in the form of clothing, bags, wallets, and fashion accessories designed by famous Korean and foreign brands.

< Online anti-counterfeiting enforcement activities of KIPO >

	2012	2013	2014	2015	2016	Total
Open Markets (Stopped sales)	4,256	4,422	5,348	5,673	5,888	25,587
Shopping Malls (Shut down)	505	828	454	418	368	2,573
Criminal Charges	109	117	41	170	159	596
Confiscated Goods	25,949	9,099	3,182	38,007	31,948	108,185

11. In order to establish a rapid response system to prevent distribution of counterfeit goods, KIPO has strengthened its capacity to investigate online counterfeit websites through offline investigation links with IPOMS. IPOMS provides addresses and seller information related to fraudulent sites selling counterfeit goods, collects evidence of counterfeit goods sales, monitors websites of counterfeit goods sales, supports authenticity validation and calculates the original value. IPOMS then provides compiled information to SIP to support and facilitate investigations.

< Enforcement support procedure for SIP using IPOMS >



C. COUNTERFEIT GOODS REPORTING CENTER AND COUNTERFEIT GOODS REPORTING REWARD SYSTEM

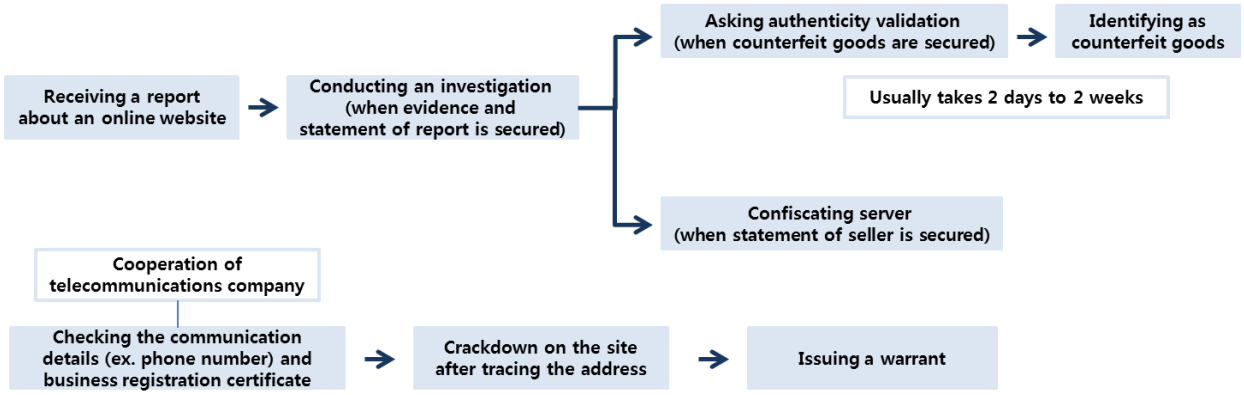
12. KIPO operates the Counterfeit Goods Reporting Center with the goal of eliminating the distribution of counterfeit goods and collecting information relating to the manufacture, distribution and sale of counterfeit goods. KIPO determines whether the content of the reports received at the Counterfeit Goods Reporting Center are an infraction of the Trademark Act or Unfair Competition Prevention and Trade Secret Protection Act of the Republic of Korea.

13. If the degree of offense is minor, the report is dealt with through administrative guidance, including a recommendation of correction. If it is deemed to be a serious offense and subject to criminal charges, the SIP for Trademark will carry out an investigation of the suspect and send the complete case to the prosecutor.

14. In the case of online offenses, such as a website or blog, KIPO will request the Korea Communications Standards Commission to shut down the website or ask the portal site operators to delete the post after confirming whether or not there was an actual online infringement.

15. To facilitate the reporting of counterfeit goods and to raise public awareness of the illegality of counterfeit goods, KIPO has operated a reward system for counterfeit goods reporting since 2006. A report may concern the manufacture, distribution or sale of counterfeit goods, and can be submitted by anyone.

< Enforcement procedure from a claim on online shopping malls >



16. In 2016, there were 23 reported cases of online sales and rewards amounted to 19.2 thousand USD. Compared to 2015, the 2016 data shows an increase of 228.6 per cent for reported cases and 237 per cent for rewards. This analysis reflects the recent surge in the circulation of counterfeit goods online.

< Counterfeit Goods Reporting Reward in Online Sales >

(unit: cases, thousand USD)

2010		2011		2012		2013		2014		2015		2016	
cases	amount	cases	amount	cases	amount	cases	amount	cases	amount	cases	amount	cases	amount
12	6.9	5	2.2	4	1.7	2	0.9	5	3.3	7	5.7	23	19.2

17. By 2016, KIPO had awarded a total of 1.7 million USD over its 11 years of operating the counterfeit goods reporting reward system. The total value of the original product of counterfeit goods caught by the system amounted to 2.8 billion USD.

D. ANTI-COUNTERFEITING COUNCIL

18. To contribute to sound commercial trade, KIPO launched the Anti-Counterfeiting Council, a public-private cooperation system consisting of 62 organizations and companies including counterfeit goods control agencies, trademark holding companies, online market operators, and related organizations.

19. The Anti-Counterfeiting Council has held seminars attended by all members with a view to:

- sharing online counterfeit product vendor information;
- implementing restrictions on counterfeit product distribution in online counterfeit product sales sites and SNS; and
- facilitating cooperation between trademark right holders and online market operators to restrict counterfeit product sellers and emerging online distribution channels for counterfeit products.

20. Moreover, major member companies participated in a joint enforcement action, quickly distinguishing genuine from counterfeit products at the scene which contributed to the success of the joint enforcement.

E. COOPERATION WITH ONLINE MARKET OVERSEAS

21. Due to the rapid growth of online markets, the damage caused from the distribution of counterfeit goods continues to be reported not only on the domestic but also overseas online markets. Thus, KIPO has begun to pay attention to domestic and overseas distribution of counterfeit goods from overseas online markets.

22. As an example, in April 2014, KOIPA signed a Memorandum of Understanding (MOU) with a global e-commercial enterprise in order to help solve the problem of counterfeit goods circulating through the overseas open markets. The main objective of the MOU is to promote mutual business exchanges between the two organizations in relation to protecting IPR, establishing a cooperative process to promote IPR protection, and endorsing joint public campaigns to protect IPRs. In particular, the MOU provided a procedure for allowing the enterprise to take action in halting the sale of counterfeit products if KOIPA provides information on IPR infringement.

23. As a result, in 2016, KOIPA has helped the enterprise delete 19,621 counterfeit products. The value of the intercepted products amounts to approximately 30.7 million USD and if collateral damages, such as the reduction of sales and decreasing reliability of global companies due to the sale of fake goods, are included, the collateral drop from the effects of the deletion are expected to be much larger.

III. CHALLENGES AND FUTURE PLANS

24. KIPO will expand the role of the SIP and reinforce its online law enforcement task force in order to more efficiently track and investigate avenues of counterfeit goods distribution.

25. In the case of online counterfeit products, most of the habitual distribution websites have servers located overseas. There are many difficulties in effective enforcement because, in many cases, only the nominal head resides locally while the actual administrator stays overseas. Investigations are frequently ceased and considered ineffective. In addition, most suspects continue to sell counterfeit goods even after website access was blocked, by changing their domain address to a similar address.

26. Counterfeit goods distribution is changing, moving away from individuals or small business dealers to corporation dealers with large syndicates at their disposal. There is a need for concentrated control over this emerging profile of distributors. In addition, dealers with a corporate profile, some associated with criminal gangs, produce and distribute counterfeit goods to fund criminal organizations. Therefore, there is a need for more thorough control of counterfeit goods to eradicate them and enhancement of international cooperation is necessary to ultimately block the source of distribution of counterfeit goods.

27. KIPO plans to concentrate on arrests that target recurrent online corporate distribution dealers in cooperation with the prosecutor. In particular, KIPO will work toward strict enforcement against repeat offenders and plans to strengthen cooperation with domestic and overseas organizations to establish a fair trade order. In addition, KIPO will strengthen the information gathering and enforcement against counterfeit goods distribution channels that uses online markets and the newly emerging SNS market.

28. As awareness is critical for eradicating counterfeit goods, KIPO plans to strengthen public-private cooperation. Through the Anti-Counterfeit Council, there are plans to draw up measures to eliminate online distribution of counterfeit products. KIPO will continue to listen to difficulties brought up by online operators and trademark right holders who suffer from counterfeit goods and will expand on cooperation by holding relevant seminars. Moreover, KIPO has plans to actively promote the awareness of the Anti-Counterfeit Council’s key activities to encourage more companies and online providers to participate.

CHALLENGES IN PROSECUTING ONLINE INTELLECTUAL PROPERTY INFRINGEMENT CASES: THE PERSPECTIVE OF THE OFFICE OF THE ATTORNEY GENERAL OF THAILAND

Contribution prepared by Ms. Duangporn Teachakumtorn, Public Prosecutor, Department of Intellectual Property and International Trade Litigation, Office of the Attorney General, Bangkok, Thailand[*]

ABSTRACT

Thailand has, over the years, grappled with intellectual property (IP) infringement. The effective enforcement of IP rights (IPRs) in Thailand is, therefore, seen as a high priority task and one that needs to be resolved promptly. Online infringement does, however, prove very difficult to prosecute due to the transnational nature of the act and the difficulty in securing evidence. Law enforcement in Thailand is reliant on improved co-operation both at national and international level. There is also a clear need for Thailand to allow greater freedom to its public prosecutors so that they can make meaningful decisions and target the larger and more important cases. Ultimately, promoting respect for IPRs is key to resolving the problem. It is important to understand and believe that IP Infringement is a serious matter. Such understanding will greatly assist in eradicating infringing activities in a sustainable manner.

I. OVERVIEW

1. Online IP infringement is one of the major problems Thai public prosecutors have encountered in recent times. The Office of the Attorney General established the Department of Intellectual Property and International Trade Litigation in 1999 to specifically deal with IP infringement. Previous incarnations of IP infringement were of a physical nature, where street vendors or manufacturers of infringing merchandise could be arrested and prosecuted. However, in recent years, there has been a significant rise in counterfeiting and piracy via the use of digital platforms in Thailand, which demonstrates a clear switch from street level trade to online trade. Whilst advances in technology are to be encouraged and embraced, the abuse of such newfound opportunities presents incredibly challenging and complex difficulties to Thai public prosecutors. Investigations into IP infringement occurring within the borders of Thailand are becoming increasingly difficult due to the existence of closely connected foreign elements, taking place outside of the country's borders. For example, domain names of infringing websites may be registered overseas or some offenders may use ISPs located outside Thailand. The difficulties in gathering such evidence and actually proving the infringing activities in court should not be underestimated.

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

II. LEGISLATION

2. Thailand joined WIPO in 1989. The major IP laws currently enforced in Thailand are as follows:

- Trademark Act B.E. 2534 (1991), amended in 2016;
- Trade Secrets Act B.E. 2545 (2002), amended in 2015;
- Copyright Act B.E. 2537 (1994), amended in 2015;
- Protection of Geographical Indications Act B.E. 2546 (2003);
- Protection of Layout-Designs of Integrated Circuits Act B.E. 2543 (2000);
- Plant Varieties Protection Act B.E. 2542 (1999); and
- Patent Act B.E. 2522 (1979), amended in 1999.

3. Thai IP laws conform fully with international standards. Recent amendments to IP legislation include the following:

- Trademark Act: A recent amendment to the Thai Trademark Act includes sound as a new addition to the definition of a mark. Therefore, sound is now a registrable trademark in Thailand. There is also a new and specific provision concerning illegal refilling (the crime of placing a copy of a product within its original packaging) which imposes stronger penalties in comparison to the previous offense stipulated in the Penal Code.

- Copyright Act: The Thai Copyright Act underwent some significant revision. The new provisions include anti-camcording provisions, technological protection measures, right management information, a safe harbor provision for ISPs, a fair use exception, a disabled person exception and a first sale exception.

III. INTELLECTUAL PROPERTY PROSECUTION

4. The Department of Intellectual Property and International Trade Litigation, Office of the Attorney General, is a specialized unit specifically focusing on IP prosecution and international trade litigation. The jurisdiction of the Department covers Bangkok and 5 vicinities, i.e. Samut Prakan, Samut Sakorn, Nakorn Pratom, Nonthaburi and Pathum Thani. IP cases that occur outside the above jurisdiction are handled by prosecutors of the litigation office where the infringement occurs. Upcountry prosecutors tend to handle all type of cases as opposed to just IP.

5. The Department receives in the region of 2,000 IP cases per year. The vast majority of these cases are trademark and copyright infringement cases. There are also patent and trade secret infringement cases but they are still small in number compared to the former two.

A. PROSECUTION PROCESS

6. When an infringement occurs, right holders can initiate legal action against the infringer themselves, which can be criminal, civil or both. Alternatively, they can get law enforcement involved by filing a complaint with an inquiry officer of the Royal Thai Police (RTP) or of the Department of Special Investigation (DSI) of the Ministry of Justice. The officer will conduct a thorough investigation and gather all relevant evidence. Once investigation is completed, the case will be sent to prosecutors to review the facts of the case as well as all available evidence relating to the case. Prosecutors, at this point, may instruct inquiry officers to conduct additional

investigation on any particular points that prosecutors consider need further clarification. Upon completion, prosecutors will decide whether there is sufficient evidence to prove the wrongdoing of the offender in a court of law. If it is deemed that sufficient evidence is available, a prosecution order will be granted and a complaint will be filed with the Central Intellectual Property and International Trade Court (CIPITC)[1] against the accused (now the defendant). Alternatively, if there is insufficient evidence, prosecutors will issue a non-prosecution order and send the case along with his or her opinion and grounds for non-prosecution to the Commissioner General of the RTP or Director General of DSI, as the case may be, to review whether to concur with the prosecutor's order. If the RTP Commissioner General or DSI Director General is in agreement with the prosecutor's opinion, the non-prosecution order will be final. However, if the RTP Commissioner General or DSI Director General considers there is in fact sufficient evidence to prove the wrongdoing, the case will then be submitted to the Attorney-General for a final order.

B. CRIMINAL IP INFRINGEMENT

7. There are two types of criminal offense in Thailand, i.e. compoundable and non-compoundable offenses. In the context of IP laws, copyright infringement is a compoundable offense while other IP infringements are non-compoundable. This means that copyright cases can be initiated only with the complaint of the right holders. In addition, under Section 66 of the Thai Copyright Act B.E.2534, right holders can withdraw their complaints at any time, but usually do so after receiving satisfactory compensation. After the complaint is withdrawn, public prosecutors no longer have the power to prosecute such a case. The case will discontinue under Criminal Procedural Code Section 39.

8. Online infringement cases in Thailand often involve copyright and trademark infringement. The infringing activities may take place via online stores. Online stores often stem from physical stores where infringers sell physical pirated DVD movies or songs, or counterfeit goods in their online store or on social media such as Facebook and Instagram. Right holders or investigators will sometimes purchase a small amount of fake goods in order to prove the sale of infringing merchandise. The payment is usually made by bank transfer to the account identified by the seller. After the payment is made, the merchandise will be delivered by mail and will be preserved as the evidence for the case. There can also be digital stores where one can pay to download pirated movies, games or songs in digital format. There is no physical evidence in this scenario.

9. In both types of infringement, bank transfers are most frequently used as primary methods of payment, as opposed to credit cards. There are e-mail addresses which belong to ISPs outside Thailand such as Gmail, Hotmail or Yahoo. Some stores display the seller's phone number while many do not, to avoid detection and possible prosecution. Phone numbers, if indicated, are usually traced to a pre-paid phone which does not require the user to provide ID registration. Obtaining firm evidence in order to secure a conviction proves to be very difficult. The only concrete evidence is bank account transactions as these can allow for the tracing of money from the buyer account to that of the seller. Therefore, the owner of the bank account is often arrested and may face an IP infringement charge as the receipt of these funds to the bank account under their names expose them as the infringer. Unfortunately, there are in fact some instances where individuals are approached and asked to open a receiving account for a small fee. Such activities complicate investigations and prosecutors are presented with very weak and ineffective evidence as a result.

[1] For more detailed information on the Experience of the Thai Central IP and International Trade Court, see WIPO/ACE/11/7, available at http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=342836.

IV. CHALLENGES

A. TRANSNATIONAL CRIME

10. It cannot be denied that advances in technology benefit society in general. However, they also act as an invaluable aid for criminals to facilitate infringing activities on the internet. The form of the offense of IP infringement has changed, for example, from physical stores to online stores, through which the seller can no longer be easily identified and hides behind a cloak of anonymity. The majority of online counterfeiting and piracy cases have some level of foreign involvement. Even though the crime is being detected and committed in Thailand, it is likely that the perpetrator is operating from a different part of the world. Such instances would see the server or domain name exist outside the jurisdiction of Thailand, making it extremely difficult for Thai law enforcement to successfully pursue the case.

B. DIGITAL EVIDENCE AND LACK OF INVESTIGATIVE POWER

11. Preserving and gathering digital evidence before it is deleted or relocated plays an important role in an online piracy investigation. There are occasions upon which investigators fail to gather important information and as a result prosecutors have to instruct further investigation at a later stage – usually up to one year after the infringement occurs – on matters concerning digital evidence. This would allow the criminal adequate time to delete the evidence. Closer initial communication between inquiry officers and prosecutors would enable prosecutors to guide inquiry officers on what evidence is deemed as necessary for trial. The evidence could be targeted and gathered quickly prior to being removed or deleted.

C. BURDEN OF PROOF

12. Just as in other countries, Thai prosecutors have to prove beyond reasonable doubt that the accused actually committed a particular crime. Traditional crimes would see prosecutors bring eyewitnesses to court in an attempt to prove the wrongdoing. However, difficulties arise in the trial of online infringement cases as there are basically no eyewitnesses to identify the infringer. For example, even though prosecutors can prove the infringement takes place from a particular computer, identifying the person operating the computer at the time of the infringement can be extremely difficult.

D. LACK OF RESOURCES

13. With the unique borderless characteristics of the internet, it is difficult for law enforcement to suppress online infringing activities. The ease of registering domain names, removing evidence or relocating the infringing content to other websites within a matter of minutes enables infringers to avoid detection with relative ease. The fluid nature of this avoidance highlights the lack of resources available to tackle these illegal activities.

V. PROPOSED SOLUTION TO IMPROVE PROSECUTION OF ONLINE INFRINGEMENT CASES

A. BETTER COOPERATION

14. Advances in technology have allowed IP infringement to become a global phenomenon. Given the size and complexity of the problem it is clear that it cannot be addressed and resolved by just one country. If infringements are to be tackled in a meaningful manner it will need the commitment and assistance of other countries at both national and international levels.

B. DISCRETION OF PUBLIC PROSECUTORS

15. Unlike some other countries, Thai public prosecutors do not have the discretion to decline a case from investigators provided legal requirements are met. As a result, there are many small cases, and limited resources are allocated to cases involving a single pirated DVD. If Thai public prosecutors were given greater discretional powers they could deploy resources to more significant cases. In turn, investigators would have to present bigger cases in order to be accepted by prosecutors. This system would see the more significant cases of infringement being tackled with the careful allocation of precious resources.

C. INCREASE PUBLIC AWARENESS: BUILDING RESPECT FOR IP

16. This last decade has brought change to the perception towards IP by the Thai people, as more Thai creators and inventors are beginning to be affected negatively by infringements. This has increased the urgency of the need to protect right holders, regardless of nationality, and this is now more widely acknowledged and recognized. Promoting respect for IP will have to be combined with a long term sustainable plan to suppress IP infringement. If one truly feels that counterfeiting and piracy are a crime on par with theft, which should be condemned, the consumer will not knowingly infringe the IP rights of others.

VI. CONCLUSION

17. Due to the complex technical challenges mentioned above, there is no single, simple solution to deter online infringers. Therefore, Thailand should follow the proposed solutions in unison with a vigorous program to promote respect for IPRs. A complete embracement of the principle of respect for the IPRs would be the ultimate and permanent cure against infringement as it would eliminate the root cause of IP infringements.

WEBSITE BLOCKING INJUNCTIONS: THE UK EXPERIENCE

Contribution prepared by Ms. Elizabeth Jones, Copyright and IP Enforcement Directorate, Intellectual Property Office, Newport, United Kingdom [*]

ABSTRACT

In recent years United Kingdom (UK) courts have granted a number of injunctions requiring named internet service providers (ISPs) to block subscriber access to specified infringing websites. *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc [2011] EWHC 1981 (Ch)* was a test case by major film studios who successfully sought an injunction against BT to block access by BT's subscribers to a website known as Newzbin2. Since this first case, ISPs have not opposed the orders sought. Therefore, where the factual circumstances of applications are the same as cases which have been considered by reasoned public judgments, most of the orders have been dealt with by paper. In November 2014, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors [2014] EWHC 3354 (Ch)* required ISPs to block access to websites selling goods infringing Cartier trademarks. This was of particular interest in the UK as there is no UK legislation explicitly providing for such website blocking injunctions where trademarks are being infringed. Such orders are seen as a valuable tool in the available measures for right holders to protect and enforce their intellectual property rights in the UK, but as they take considerable effort and cost to achieve, they are used only for the most seriously infringing websites.

I. INTRODUCTION

1. In recent years United Kingdom (UK) courts have granted a number of injunctions requiring named internet service providers (ISPs) to block subscriber access to specified infringing websites. These are part of a package of measures to tackle intellectual property (IP) infringement including a specialized IP police unit (PIPCU) to tackle IP crime; voluntary measures, including a Code of Practice[1] to stop UK consumers being directed to copyright infringing websites; and educational awareness campaigns including www.getitrightfromagenuinesite.org.

II. THE LEGISLATIVE CONTEXT

2. European Union (EU) legislation provides for right holders to apply for an injunction against an intermediary whose services are being used by a third party to infringe the right holder's IP. Article 8 of Directive 2001/29/EC[2] provides for this where copyright or a related

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

[1] https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement.

[2] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF.

right is being infringed, and Article 11 of Directive 2004/48/EC[3] provides for an injunction to be granted where an IP right is being infringed.

3. Article 8 of Directive 2001/29/EC was transposed into UK law by Section 97A[4] of the Copyright, Designs and Patents Act (CDPA) 1988. When transposing Directive 2004/48/EC into UK law, it was determined that existing UK law already provided for such an injunction, therefore explicit provisions were not introduced.

III. THE FIRST ORDER – NEWZBIN2

4. Section 97A was first used in *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc [2011] EWHC 1981 (Ch)*[5], more commonly known as *Newzbin2*. This was a test case by major film studios who sought an injunction against BT (a UK ISP) to block access by BT's subscribers to a website known as Newzbin2. The application was supported by a number of sectors from the creative industries which were experiencing increasing infringement of their copyright online.

5. *Newzbin2* followed an earlier successful claim for copyright infringement brought by the studios against Newzbin Ltd in 2010. Newzbin was a Usenet indexing website[6], providing its members with a simplified process to search for and access a wide range of digital content posted to Usenet service providers. Film studios were granted an injunction against Newzbin Ltd to restrain further copyright infringement[7], as Newzbin was found to be liable for copyright infringement: authorizing the copying of the claimants' films; procuring and engaging with its premium members in a common design to copy the claimants' films; and communicating the claimants' films to the public.

6. Newzbin ceased operating, but Newzbin2 appeared at the same location, operating in the same manner, and therefore providing continued large-scale infringement of copyright. Its operation had moved outside the UK and was therefore beyond the jurisdiction of the UK courts, although it was still aimed at a UK audience. Initially the studios wrote to BT, asking BT to block access to Newzbin2 or agree to not oppose a court order to that effect. Evidence of the operation of Newzbin2 was provided, along with a summary of the *Newzbin* case. BT noted that it did not support or condone copyright infringement, but would require a court order to block such services, to avoid potential legal liabilities.

7. The studios therefore sought an injunction against BT, as an intermediary using Section 97A CDPA, as the only effective way to prevent, or at least reduce the scale of copyright infringement. This would be achieved by using Cleenfeed, BT's existing technology used to block access to websites featuring images of child abuse.

8. The court set out a number of questions to determine the granting of the injunction:

- Are the defendants service providers?
- Do the operators and/or users of the websites infringe the claimants' copyright?
- Do the users and/or operators use the defendants' services to infringe?
- Do the defendants have actual knowledge?

---

3 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:en:PDF.

4 http://www.legislation.gov.uk/ukpga/1988/48/section/97A.

5 http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html.

6 A bulletin board system predating, but less popular than the world wide web.

7 *Twentieth Century Fox Film Corp v Newzbin Ltd* [2010] EWHC 608 (Ch).

9. The court also considered whether the injunction was a proportionate, effective and dissuasive remedy against infringement.

10. As BT accepted that it was a service provider, the court had two main points to decide – whether BT's services were being used to infringe copyright; and whether BT had actual knowledge of the infringement. It found that BT's customers were using its services to infringe copyright, and that it was sufficient that BT knew of people using its services to infringe copyright – it was not necessary to show knowledge of a specific infringement of a specific copyright work by a specific individual.

11. The court also found that blocking or impeding access to Newzbin2 amounted to specific, rather than general monitoring. The order was considered proportionate, as when the court balanced the rights to protection of property and freedom of expression established in the European Convention on Human Rights[7], the right of studio (and other copyright) owners to protect their IPR outweighed the freedom of expression right of Newzbin2 and BT. The cost of implementation to BT would be proportionate (relying on existing technology, Cleenfeed). The court also agreed with the studios' argument that the order would be justified even if it only prevented access to Newzbin2 by a minority of users. Given the considerable effort and expense involved in bringing the case it was not expected to lead to a flood of requests for similar orders. The injunction was therefore granted, and a subsequent hearing determined the terms of the order[8].

12. Following the success of this case the studios sought (and were granted) similar orders against the remaining major UK ISPs[9].

13. A second application required ISPs to block access to The Pirate Bay (*Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 268 (Ch)*). Brought by music industry representatives, this application was unopposed by the ISPs. Claims for copyright infringement were not brought against the The Pirate Bay operators, but a preliminary issues hearing did determine on the evidence presented that users and operators of The Pirate Bay infringed the claimants' copyright. The court felt this was a sensible way in which to proceed, but did not consider it an essential step for future cases. The application was granted, finding that The Pirate Bay was jointly liable for the infringements committed by users, as it authorized its users' infringing acts of copying and communicating to the public, going far beyond merely enabling or assisting infringement. The court determined that there was no obligation by the claimants to join the operators of The Pirate Bay as defendants to the claim. Neither Article 8(3) of Directive 2001/29/EC nor Section 97A CDPA create any jurisdictional requirement to join or serve the operators or users of The Pirate Bay.

IV. THE EVOLUTION OF ORDERS

14. Since the first case (*Newzbin2*) ISPs have not opposed the orders sought. Therefore, where the factual circumstances of applications are the same as cases which have been considered by reasoned public judgments, most of the orders have been dealt with by paper[10]. A selection of key cases, contributing to the evolution of these orders, are discussed below.

---

[7] Right to protection of property (Article 1 First protocol) and right to freedom of expression (Article 10): http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[8] http://www.bailii.org/ew/cases/EWHC/Ch/2011/2714.html.

[9] Sky, BT, EE, TalkTalk, O2 (Telefonica) and Virgin.

[10] The Civil Procedure Rules provide for the court to deal with an application without a hearing if the parties agree or the court does not consider a hearing would be appropriate.

15. *The Football Association Premier League Ltd v British Sky Broadcasting & Ors [2013] EWHC 2058 (Ch)*[11] concerned a website (FirstRow) facilitating access to television sports broadcast streams, rather than peer-to-peer as in *Newzbin2* and *The Pirate Bay*. Here the court found that although the operators of FirstRow were not committing acts of communication (other host websites were providing the streams) its operators were jointly liable for the communication by the host site operators.

16. *Twentieth Century Fox Film Corporation & Ors v Sky UK Ltd & Ors [2015] EWHC 1082 (Ch)*[12] raised new and different issues, as in addition to requesting ISPs to block access to streaming and BitTorrent websites (host websites), it also included websites providing the Popcorn Time application (an open source application allowing users to obtain film and TV content using the BitTorrent protocol with an integrated media player). The court could not find that the Popcorn Time application website operators were carrying out an act of communication to the public, nor that these sites were authorizing infringing acts. However, it did find that the Popcorn Time suppliers clearly knew and intended Popcorn Time application to be a key means to procure and induce the user to access the host websites, therefore causing the infringing communications to occur, and sharing a joint liability for the copyright infringements. The order was granted.

17. *The Football Association Premier League Ltd v British Telecommunications Plc & Ors [2017] EWHC 480 (Ch)* focused on the illegal streaming of live football matches via set-top boxes, media players and mobile device apps. Traditional blocking orders targeting websites are unable to prevent the majority of infringements as these devices do not rely upon accessing a specific website, but instead connect directly to streaming servers via their IP addresses. The order is 'live', only having effect at the times when live Premier League match footage is being broadcast. The list of target servers for blocking can be 're-set' each week, allowing for new servers to be added, and ensuring that old servers no longer providing infringing content are not blocked. The order was time limited, covering only the Premier League season. Where an IP address is subject to blocking, a notice must be sent to the hosting provider. Permission to apply to set aside or vary the order was given to hosting providers, website or streaming service operators, and ISP subscribers who claimed to be adversely affected by the order. It is expected that further orders will be requested ahead of the new football season.

V. TRADEMARK INFRINGING WEBSITES – CARTIER

18. Initially, all the injunctions sought were concerned with the infringement of copyright. In November 2014, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors [2014] EWHC 3354 (Ch)*[13] required ISPs to block access to websites selling goods infringing Cartier trademarks. This was of particular interest in the UK as there is no UK legislation explicitly providing for such website blocking injunctions where trademarks are being infringed. Having determined that it did have jurisdiction to grant such an order, the court established the threshold conditions to exercise its jurisdiction:

- Are the ISPs intermediaries?
- Are the operators of the Target Websites infringing the trademarks?
- Do the operators of the Target Websites use the ISPs' services to infringe?
- Do the ISPs have actual knowledge of this?

---

11 http://www.bailii.org/ew/cases/EWHC/Ch/2013/2058.html
12 http://www.bailii.org/ew/cases/EWHC/Ch/2015/1082.html
13 http://www.bailii.org/ew/cases/EWHC/Ch/2014/3354.html.

19. The court examined several principles to be applied before granting the order – that the relief must be necessary; effective; dissuasive; not be unnecessarily complicated or costly; avoid barriers to legitimate trade; be fair and equitable and strike a fair balance between the applicable fundamental rights; and be proportionate.

20. The court examined the alternative measures that were available to right holders. These include: action against the operators of the sites; notice and takedown by hosts; payment freezing of the operators' merchant accounts; domain name seizure; de-indexing by search engines; and customs seizure. Whilst some of these were considered to be worth pursuing, the court did not consider these measures to be equally effective but less burdensome than the order requested.

21. As well as blocking of Target Websites, the order extended to their domains, sub-domains and any other IP address or URL notified to the ISPs. It also allowed for affected subscribers to apply to the court to discharge or vary the orders, and included a sunset clause, providing an end point for the order unless either the ISPs consent to, or the court orders that they should be continued.

22. The order was granted but subsequently appealed by the ISPs, who argued the court did not have jurisdiction to grant the injunction; the order was disproportionate; and ISPs should not bear the implementation costs of the order. The Court of Appeal upheld the High Court's decision with one judge dissenting on the issue of who should bear the implementation costs. In February 2017, two ISPs were granted application to appeal to the Supreme Court on the costs issue.

VI. EFFECTIVENESS

23. Such orders are seen as a valuable tool in the available measures for right holders to protect and enforce their IP rights in the UK, but as they take considerable effort and cost to achieve, they are used only for the most seriously infringing websites.

24. In the early days there were a small number of incidents involving over-blocking, where websites not subject to the blocking orders (and not infringing copyright) were inadvertently blocked. This issue was overcome, and does not seem to have happened since.

25. The effectiveness of such orders was considered in *Newzbin2* and *Cartier* as an important factor in assessing their proportionality. Where a site had been subject to a blocking order, a significant decrease in UK traffic to the sites was found. There was no evidence of any major migration of UK users to proxies of the blocked sites, and although there was a steady increase in search terms relating to virtual private networks (VPNs) and Tor (anonymity network), no correlation with the dates of implementation of any of the UK blocking orders was found.

INSTITUTIONAL ARRANGEMENTS TO ADDRESS ONLINE INTELLECTUAL PROPERTY INFRINGEMENTS – EUROPOL'S EXPERIENCE

Contribution prepared by Mr. Chris Vansteenkiste, Team Leader, Intellectual Property Crime Coordinated Coalition (IPC[3]), Europol, The Hague, Netherlands[*]

ABSTRACT

Although not included in the European Union (EU) 2018-2021 priority crime threats, combatting intellectual property (IP) crime remains important for Europol and its partner law enforcement authorities.

In 2016, the Intellectual Property Crime Coordinated Coalition (IPC[3]) was established at Europol with a view to facilitating the full exploitation of Europol's operational and strategic capabilities in the field of IP right (IPR) infringement. The IPC[3] positions Europol as a European central point for specialized knowledge and expertise in investigations of offences against IP while increasing its coordinating capacities and placing Europol in a better position to obtain input from multiple stakeholders, such as the private industry and IPR holder associations.

Recent successful operations related to online IPR infringements supported by IPC[3] underline the vital importance of international law enforcement and judicial cooperation, as well as the need for close collaboration between law enforcement authorities and the multiple public and private stakeholders operating in this field.

I. INTELLECTUAL PROPERTY CRIME: A WIDE-SPREAD PHENOMENON

1. The impact of intellectual property (IP) crime is particularly high in the European Union (EU), with counterfeit and pirated products amounting to up to five per cent of imports, or as much as 85 billion euros[1].

2. IP right (IPR) infringements negatively impact the revenues of the affected businesses and produce adverse social and economic effects that result in thousands of job losses. Moreover, these infringements can also cause very serious harm to the health and safety of consumers, including death, as counterfeit goods are produced without taking into account the health and safety standards and regulations of the EU.

3. Nowadays, most counterfeit products are advertised on the Internet and shipped all over the world. This makes online investigations increasingly important – it is vital that law enforcement agencies have the tools, training and legislation to enable them to conduct such investigations effectively.

---

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

[1] OECD/EUIPO, Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing (2016), Paris.

II. ONLINE TRADE IN ILLICIT GOODS AND SERVICES: THE SOCTA 2017

4. In March 2017, Europol launched its Serious and Organised Crime Threat Assessment (SOCTA) 2017, with the subtitle “Crime in the age of technology”.

5. The SOCTA 2017’s in-depth analysis of the major crime threats facing the EU, serves as the cornerstone of the EU Policy Cycle for Serious and Organised Crime. In the SOCTA 2017, Europol recommended five key priority crime threats (cybercrime, drug production, trafficking and distribution, migrant smuggling, organized property crime, and trafficking in human beings) and three cross-cutting priority crime threats (criminal finances and money laundering, document fraud, and online trade in illicit goods and services).

6. Online trade in illicit goods and services, including counterfeit commodities, has been identified as a cross-cutting crime threat – in other words an engine that enables and facilitates most, if not all, other types of serious and organized crime.

7. Online trade in illicit commodities has been expanding steadily over recent years and it is expected that it will continue to grow rapidly for the foreseeable future. The multiplication of sales platforms, including those hosted on social media, has made online trade easier, more accessible and cheaper. This development has been mirrored in the online trade in illicit goods, as criminals and legitimate traders alike look to online opportunities to grow their businesses. Criminals are able to produce counterfeit goods in large quantities at minimal costs and use online platforms to easily and effectively market their products internationally.

8. The SOCTA 2017 suggested the sale of counterfeit goods as a priority within the cross-cutting crime threat of online trade in illicit goods and services. However, following discussions at the Standing Committee on Operational Cooperation on Internal Security (COSI) Support Group meeting on May 12, 2017, the Council of the EU decided not to include it as a priority in the fight against organized and serious international crime between 2018 and 2021.

III. THE INTELLECTUAL PROPERTY CRIME COORDINATED COALITION

9. As a response to emerging trends and in line with the Europol Strategy 2016-2020, Europol established a new organizational entity, the so called Intellectual Property Crime Coordinated Coalition (IPC^3).

10. This new team, launched in July 2016, is part of Europol’s Operations Department, within the European Serious and Organised Crime Centre, and has been built on the work undertaken by the Analytical Project COPY, which remains the operational platform for criminal analysis. The IPC^3 is being financially supported by the European Union Intellectual Property Office (EUIPO) through a yearly grant agreement.

11. Increased capabilities, including a higher number of team members, have certainly strengthened Europol’s efforts to combat counterfeiting and piracy both online and offline.

12. In this specific crime area, law enforcement authorities largely depend on the contribution of multiple public and private stakeholders (e.g., IPR holders, registry offices/observatories, and health and safety authorities). Therefore, IPC^3’s role in coordinating information exchange, acting as a central point for specialized knowledge and providing expertise in investigations is of vital importance.

13. IPC[3]'s main objectives consist of:

- Providing operational and technical support to the competent authorities;
- Facilitating and coordinating cross-border investigations;
- Monitoring and reporting online crime trends and emerging modus operandi;
- Enhancing the harmonization and standardization of legal instruments and operating procedures to counter IP crime globally; and
- Reaching out to the public and law enforcement by raising awareness and providing training in this specific field of expertise.

IV. EUROPOL IPC[3]'S ACTIVITIES AGAINST ONLINE IPR INFRINGEMENTS

14. Online marketplaces are a key distribution channel for counterfeit goods. The sales volume of counterfeit goods online has increased significantly over recent years. Counterfeiters often use social media platforms to advertise their products. Thousands of online shops are used to sell counterfeit goods. The increasing use of parcel and postal services makes it difficult to detect counterfeit commodities in the postal flow.

15. IPC[3]'s strategy foresees a number of activities and tasks related to online infringements of IPRs and online financial payment systems. Consequently, the team's Internet monitoring capabilities have been increased and further growth is expected.

16. Activities undertaken include a wide range of actions, from monitoring the Internet to gathering intelligence. IPC[3] performs regular Open Source checks in order to acquire as much information as possible on IP addresses, websites, email accounts, registrants, physical addresses, telephone numbers, servers and other relevant data. This aims to support investigations by enriching referrals received from members of IPC[3]'s network, as well as enhancing the quality and quantity of existing intelligence.

17. Intelligence gathering activities encompass "scanning" the most popular social media networks, advertisements and virtual currency platforms. The goal behind this process is not only to facilitate Member States and Third Parties to seize infringing websites, but also to support competent authorities in the field of "tracing the money" by gathering significant information and monitoring emerging trends with regard to online financial payment systems.

18. IPC[3] is also committed to raising public and law enforcement awareness by delivering early warning messages, training and strategic reports on online infringement.

V. TARGETING IPR INFRINGING DOMAINS, OPERATION IN OUR SITES (IOS)

19. Since 2012, the periodically recurring international operation In Our Sites (IOS) has tackled the sale of counterfeit goods and online piracy on e-commerce platforms and social networks. The operation is coordinated by Europol IPC[3], working closely with the United States Immigration and Customs Enforcement (US ICE) and Interpol.

20. In 2016, IOS saw the participation of 27 EU Member States and Third Countries and the voluntary support of 24 private partners. By collecting referral lists from IPR holders, national law enforcement authorities have been able, with Europol's support in collecting and crosschecking information, to take down 5,158 websites selling counterfeit merchandise, arrest 10 people and seize goods worth over 1.75 million euros.

21. Web users attempting to access websites which have been taken down are now directed to a web domain containing a banner that informs them that the website has been closed down by law authorities.

22. Cooperation with representatives of IPR holders remains crucial for monitoring and reporting IP infringing websites to national authorities via Europol and is a key element of operation IOS. Partnerships with the private sector include not only IPR holders, but intermediaries and IPR protection companies as well.

23. Since 2012, operation IOS has experienced regular improvements, achieved with the analysis of the previous edition of the operation. However, the continuous evolution of criminal *modus operandi* requires constant development of operational activities.

24. The way forward that is currently foreseen will incorporate further consolidation of IPC^3's solid public-private partnerships and increasing enforcement measures on social media platforms advertising and selling counterfeit goods.

VI. RECENT OPERATIONAL SUCCESSES RELATED TO AUDIO-VISUAL PIRACY

25. IPC^3's efforts in combating online IP infringement do not stop at the seizure of websites selling counterfeit goods but also include the fight against audio-visual piracy, an area in which several successful operations have been undertaken over the last years.

A. OPERATION CASPER (2017)

26. Operation Casper represents a great example of cross-border cooperation against illicit distribution of pay-tv channels.

27. A joint investigation led by the Spanish National Police, with the support of the Bulgarian authorities, IPC^3 and Eurojust, resulted in the dismantling of a criminal network responsible for the illegal distribution of more than 1,000 pay-television channels on a European scale through the use of Internet Protocol Television (IPTV) technology. In a coordinated action, eight suspects were arrested and 12 searches carried out simultaneously in Spain and Bulgaria. Investigators seized the servers used to provide illegal access to the channels, alongside numerous documents.

28. IPC^3 supported the investigations by providing operational coordination and support, forensic expertise and facilitating information exchange between law enforcement agencies and private-sector partners. On the day of action, Europol's experts were deployed to Spain and Bulgaria, equipped with Mobile Offices, to support operational activities on the spot.

B. OPERATION FAKE (2016)

29. Another successful operation in the field of audio-visual piracy is operation FAKE.

30. A joint investigation led by the Spanish National Police and Tax Authorities, with the support of the German local police of Hanau, IPC^3 and Eurojust, has resulted in the dismantling of a criminal network specialized in the illegal distribution of pay-television channels in Spain. The illicit distribution was done through pirated decoders (card-sharing) and the Internet.

31. During a joint action in May 2016, 38 house searches were carried out simultaneously in seven cities in Spain. Europol supported the investigations on the spot by deploying two experts equipped with Mobile Offices. This allowed for real-time intelligence analysis and cross-checks against Europol's databases, as well as extractions of data from phones and data storage devices.

32. In total, 30 suspects have been arrested in Spain, and 48,800 decoders seized, alongside 183,200 euros in cash, 10 luxury vehicles, one counterfeit luxury car, a private plane, several financial documents and IT equipment. It has been revealed that the criminals used bitcoin mining centers to launder illicit profits into virtual currency. In the framework of the investigations, Spanish authorities dismantled six bitcoin mining centers (one of the highest numbers in Europe so far) and seized 78.3 bitcoins.

33. The arrestees imported decoders from China, designed the firmware used to decrypt the television signals and distributed them to final customers via dedicated web pages and Internet forums controlled by them. The criminal group also used IPTV technology to illicitly offer more than 1,600 television channels from different countries. They used servers located in various European countries, including Germany which took down the server upon request of the Spanish authorities.

VII. IPC^3 TRAINING FOR LAW ENFORCEMENT OFFICIALS

34. IPC^3 regularly organizes training related to online IP crime aimed at law enforcement authorities.

35. For example, on May 11 and 12, 2017, at the Europol headquarters in The Hague, an in-depth training on audio-visual piracy was delivered to law enforcement officers, including prosecutors from across Europe, in collaboration with the Audiovisual Anti-Piracy Alliance (AAPA) and the EUIPO.

36. The day and a half training event included sessions on the technologies used to protect content: how pay-television companies work with intermediaries such as hosting providers, payment providers and advertisers to disrupt the supply of pirated content; how to investigate and analyze piracy; and how to collect and retain evidence, including through the use of live forensics. Current cases involving illegal streaming and card-sharing were also thoroughly analyzed during the break-out sessions.

CROSS-INDUSTRY VOLUNTARY MEASURES TO REDUCE ONLINE PIRACY

Contribution prepared by Mr. Dean S. Marks, Executive Vice-President, Deputy General Counsel, Chief, Global Content Protection, Motion Picture Association of America, Inc. (MPAA), Los Angeles, United States of America (USA)[*]

ABSTRACT

Piracy of copyright works has reached huge levels as a result of increasing internet bandwidth and availability, creating challenges for enforcement. In addition to conventional enforcement methods, a combination of increased legitimate online offerings and effective voluntary measures are essential to diminish the overall levels of online infringement. Unlike laws and regulations, voluntary measures can quickly be adapted to address changing forms of online piracy. Such measures benefit not only right holders, but also internet intermediaries, service providers, governments and individual users of the internet. Voluntary measures should therefore be encouraged by governments as an important means of addressing online copyright piracy.

I. ONLINE PIRACY ENFORCEMENT CHALLENGES

1. Before the digital age, authors and their authorized licensees were able to exercise a reasonable amount of control over the country-by-country use of their works. Infringement occurred, but it was generally territorially limited. Where infringing copies were produced in one country for distribution in another, right holders could often rely on customs authorities to stop the import and/or enforce against local distributors of such infringing analog copies.

2. But it is not just the borderless and instantaneous nature of the internet that strains enforcement of copyrights. More often than not today, the key components and operations of a single pirate website are spread among several different countries. It is not uncommon, for example, that the operator of a pirate streaming site is living in one country, but the site is hosted by a service provider located in a second country. The files of the infringing content to which a pirate site connect are frequently hosted on a cloud service provider in a third country. Pirate sites often use Content Delivery Networks (CDNs) and reverse proxy services located in a still different (e.g., fourth) country. And the domain name under which the site operates may be controlled by a domain name registry located in a fifth country. Clearly this new paradigm of infringement strains the foundational notion of territoriality of copyright law and increases the difficulty of effectively enforcing copyrights.

II. VOLUNTARY MEASURES TO REDUCE ONLINE PIRACY

3. Given the challenges described above, encouraging internet intermediaries, service providers and businesses to stop doing business with websites engaged in large scale copyright infringement has become a key strategy in the fight against online piracy. Some have referred to this as the “follow the money” approach. But this strategy involves more than gaining the

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO, and do not necessarily reflect the position of the Motion Picture Association of America (MPAA) or its member companies.

cooperation of payment processors and online advertisers. Hosting providers, domain name registries and registrars, CDNs, cloud storage services and even internet access providers and search engines all can serve a constructive role by adopting measures to prevent their platforms and services from being abused for copyright infringement.

A. PAYMENT PROCESSORS

4. Substantial progress has been made in the area of voluntary measures with major payment processors. Mastercard and Visa, two of the world's largest processors, have actively engaged with the Motion Picture Association of America (MPAA) to implement effective policies to prevent their services and systems from being used by websites dedicated to copyright infringement. Furthermore, both Visa and Mastercard accept referrals from the MPAA for cyberlockers[1] dedicated to infringement that appear to accept payment from Visa and/or Mastercard. PayPal also accepts such referrals and was one of the first payment processors to terminate services to infringing cyberlockers. Operators of pirate websites frequently resort to a myriad of tactics to circumvent the terminations. Nevertheless, Mastercard, Visa and PayPal proactively monitor the space in addition to their ongoing cooperation with respect to right holders' referrals. As a result of the foregoing voluntary measures, a substantial drop in user traffic to many cyberlockers has occurred.

B. ONLINE ADVERTISERS

5. Online advertising is another area where progress has been made. In 2012, the leading associations of advertisers and advertising agencies in the United States pledged to exclude operators of copyright theft websites from partaking in the revenue streams provided by advertising for legitimate products and services[2]. But given the complexity of the online advertising ecosystem, more needed to be done to stem the substantial flow of advertising revenues to pirate sites. Therefore, a number of major players in that ecosystem - notably the Association of National Advertisers (ANA), the American Association of Advertising Agencies (AAAA), and the Internet Advertising Bureau (IAB) - have joined together with MPAA members, other right holders, and technology platforms to launch the Trustworthy Accountability Group (TAG)[3]. TAG's Brand Integrity Program Against Piracy aims to help advertisers and their technology partners screen out websites that present unacceptably high risks of engaging in copyright or trademark infringement, thus helping to implement a "follow the money" strategy for depriving operators of pirate sites advertising revenue. TAG has great potential to provide a voluntary, industry-led solution to help choke off the huge advertising revenue that makes online copyright theft financially viable today.

---

[1] One of the most succinct definitions of "cyberlocker" is the following: "Unlike legitimate cloud storage services whose clients are people and businesses that need to store, access, and share data, the cyberlocker business model is based on attracting customers who desire anonymously to download and/or stream popular, copyright infringing files that others have posted. The cyberlocker business model is designed around content theft. In fact, cyberlockers generally pay or provide various incentives to those who distribute popular infringing content and discourage the use of their services for reliable data storage." See p. 1 "Behind the Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions" A NetNames Report for Digital Citizens Alliance https://www.netnames.com/assets/shared/whitepaper/pdf/dca-netnames-cyber-profibility-1.compressed.pdf September 2014

[2] See https://www.ana.net/content/show/id/23408 April 2012

[3] See generally "Fight Internet Piracy," Trustworthy Accountability Group (TAG), at https://www.tagtoday.net/piracy/.

6. Other countries have adopted different vehicles for assisting online advertisers to stop doing business with pirate websites. In the United Kingdom (UK), Operation Creative and the Infringing Website List (IWL) have already achieved results. Operation Creative is a partnership among the Police Intellectual Property Crime Unit (PIPCU) of the City of London Police, right holders and the UK advertising industry. It allows right holders to identify and report, with detailed evidence packages, copyright infringing websites to PIPCU. PIPCU then independently evaluates the websites and attempts to contact the website operators to correct behavior. If the website persists in its infringing conduct, then PIPCU adds the website to the IWL. Advertising agencies have access to the IWL via an online portal and use it as a resource to identify websites on which they may choose not to place advertising because of such websites' infringing nature. Operation Creative and the IWL have resulted in a 73 per cent reduction in advertising from the top UK advertising companies appearing on copyright infringing websites[4]. An interesting and valuable feature of Operation Creative and the IWL is the facilitating role of the government and the credibility that PIPCU's involvement brings to the effort. Recently, the MPAA has worked with governments and local advertisers in Hong Kong (SAR), China and Viet Nam to launch IWLs in those countries and regions.

C. DOMAIN NAMES

7. One of the most direct ways to disrupt a pirate website is to suspend its domain name. The MPAA has worked with domain name registries on voluntary measures to suspend the domains of websites engaged in clear and pervasive copyright infringement. In 2016, the MPAA entered into a Trusted Notifier arrangement with Donuts, the registry of the largest number of new top level domains (TLDs). Under this voluntary agreement, MPAA can refer websites engaged in clear copyright infringing activity that are operating under TLDs administered by Donuts after MPAA attempts to contact the hosting provider and registrar of the pirate website to resolve the matter. In addition, under the Trusted Notifier arrangement MPAA submits to Donuts an evidence package and a statement that the referred website has been subject to human review by MPAA[5]. The Trusted Notifier arrangement has worked well and TLDs of pirate websites have been suspended pursuant to it. A similar Trusted Notifier arrangement has been reached with Radix, a Dubai based registry and Asia's largest new generic TLD registry, which operates .online, .tech, .space, .web and several other TLDs[6]. Furthermore, the MPAA has entered into more informal voluntary notification arrangements with other TLD registries. As a result, to date more than 25 TLDs of pirate websites have been suspended pursuant to these voluntary measures. While pirate sites can, and usually do, migrate to new TLDs, the jumping to different domains creates friction.

---

4 See "Operation Creative Sees 73 Percent Drop in Top UK Advertising on Illegal Sites" https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Operation-Creative-sees-73-per-cent-drop-in-top-UK-advertising-on-illegal-sites.aspx, August 2015.

5 See Donuts and the MPAA—Striking the Right Balance, http://www.donuts.domains/donuts-media/blog/donuts-and-the-mpaa-striking-the-right-balance, February 2016.

6 See Radix and the MPAA Establish New Partnership to Reduce Online Piracy,http://www.prnewswire.com/news-releases/radix-and-the-mpaa-establish-new-partnership-to-reduce-online-piracy-579359971.html, May 2016.

D. HOSTING PROVIDERS

8. Hosting providers are another group of internet intermediaries upon which pirate websites rely. For cyberlockers, the loss of hosting can be devastating because these sites depend on substantial amounts of server capacity. For streaming and linking sites, the takedown from a hosting provider is less damaging and these sites often will rapidly reappear on less or non-cooperative hosting providers because these sites are "light" and do not actually store the pirate content files themselves. Nevertheless, the loss of hosting can be disruptive since it is a critical intermediary upon which all pirate websites depend.

9. In MPAA's experience, voluntary cooperation from hosting providers with respect to terminating services to websites engaged in piracy usually follows after a court has ruled that the particular hosting provider must terminate service to one or more identified pirate websites. This is particularly true in Europe given its legal regime of allowing right owners to go to court and seek injunctive relief from intermediaries and service providers with respect to online piracy without the need to prove any liability — either direct or secondary — on the part of such intermediaries. This legal regime has been invaluable in setting a foundation for collaboration between right holders and service providers in Europe. As a result, trusted referral programs are in place between the MPAA and a number of hosting providers across Europe.

III. INCENTIVES TO ENGAGE IN VOLUNTARY MEASURES

10. Reducing the scope of and damage from online piracy constitutes a clear incentive for copyright owners to seek voluntary measures. But what benefit do service providers, internet intermediaries, payment processors, online advertisers and the like see in undertaking such measures?

11. Several factors have persuaded these parties to engage in voluntary measures to collaborate with copyright owners. First, many companies do not wish to be associated with those engaged in illegal activities, including copyright pirates. Moreover, turning a blind eye to doing business with pirate websites can result in damaging repercussions. In the United States of America (USA), for example, intermediaries have been named as unindicted co-conspirators in criminal copyright prosecutions. In addition, service providers and internet intermediaries frequently view voluntary collaboration with right holders as a better alternative to the possibility of government regulation or costly litigation over potential copyright infringement liability (direct or secondary) and/or loss of safe harbor protections. Indeed, voluntary collaboration between right holders and service providers and internet intermediaries yields mutual benefits of creating an internet ecosystem that is more hospitable for legitimate commerce and safer for consumers[7].

[7] Users of pirate websites are 28 times more likely to be exposed to malware. See report by Digital Citizen Alliance, "Digital Bait: How content theft sites and malware are exploited by cybercriminals to hack into internet users' computers and personal data."
https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0f03d298-aedf-49a5-84dc-9bf6a27d91ff.pdf, December 2015.

IV. HOW GOVERNMENTS CAN ENCOURAGE VOLUNTARY MEASURES AND THE BENEFITS OF DOING SO

12. Governments can encourage the pursuit of voluntary measures by copyright owners and internet intermediaries and other service providers to reduce online piracy in several ways. They can hold hearings to explore how pirate websites are supported by local internet intermediaries and service providers (such as payment and advertising services) and encourage collaboration with copyright owners to end such support of pirate websites. Governments can also enact high-level laws or regulations that embrace "responsibility without liability," such as Europe has adopted in Article 8.3 of the EU Copyright Directive[8]. Further, governments can task law enforcement agencies to work with internet intermediaries and service providers to encourage them to adopt voluntary measures to cease doing business with pirate sites. The UK government's work via PIPCU, as described above, serves as an example.

13. When effective voluntary measures are undertaken to reduce online piracy, governments win as do citizens at large. For governments, effective voluntary measures result in fewer demands on law enforcement with respect to illegal piracy and potentially less need for legislation or regulation. In addition, because effective voluntary measures often reduce the need for litigation, they result in a reduction of demands on the judicial system. Finally, as online piracy diminishes legitimate online commerce in copyrighted works grows[9], which yields tax and other business related benefits to governments. For consumers, reducing online piracy reduces the risks from malware and privacy attacks.

V. CONCLUSION

14. No single silver bullet exists to end online piracy. Vigilant law enforcement actions and targeted civil litigations remain critical tools to address the most severe cases and to create the necessary legal precedents. Given the massive scale of online piracy, however, a combination of increasing legitimate online offerings and effective voluntary measures are key to diminish overall levels of online infringement. Voluntary measures are not necessarily restricted to national borders and have the required scalability to offer a viable path to reduce the ease and profitability of online piracy. Unlike laws and regulations, voluntary measures can quickly be adapted to address changing forms of online piracy[10]. Moreover, as this paper has described, voluntary measures create a classic win-win scenario, as they benefit not only right holders, but also internet intermediaries, service providers, governments and individual users of the internet. Voluntary measures should therefore be fostered by governments as an important means of addressing the scourge of illegal online copyright piracy.

[End of document]

---

[8] See Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML

[9] See, for example, the study by Carnegie Mellon University that found that site blocking of 19 pirate sites in the United Kingdom (UK) led to an increase in legitimate online consumption. "Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior" https://techpolicyinstitute.org/wp-content/uploads/2016/04/UK-Blocking-2-0-2016-04-06-mds.pdf, April 2016.

[10] For example, Amazon, eBay and Facebook all recently amended their policies/terms of service to prohibit the sale and advertising of devices loaded with pirate applications that facilitate the streaming of infringing content. See http://variety.com/2017/digital/news/facebook-bans-kodi-piracy-devices-1202445930/, May 2017. These changes emerged in part from ongoing collaborative exchanges between right holders and all three online platforms.