



OFFICE FOR HARMONIZATION  
IN THE INTERNAL MARKET  
(TRADE MARKS AND DESIGNS)



EUROPOL

# Infringements of Intellectual Property Rights on the Internet

5th, 6th and 7th November 2014

A conference co-chaired and hosted by the  
Office for Harmonization in the Internal Market (OHIM), Europol and Eurojust



# Infringements of Intellectual Property Rights on the Internet

5th, 6th and 7th November 2014

A conference co-chaired and hosted by the  
Office for Harmonization in the Internal Market (OHIM), Europol and Eurojust

## Table of contents

Overview	4
Day One – Welcome and Introductory Speeches	6
Right Holder’s Efforts	8
The Internet and Payment Industry Support	10
Google	10
eBay	10
VISA Europe	11
Effective Investigative Techniques in Europe and Abroad – Case Examples from the Public Sector	12
The United Kingdom Intellectual Property Office (UK IPO)	12
Guardia di Finanza’s Operational Experience	13
Hong Kong Customs’ Operational Experience	14
Operation Vigorali	14
Day Two	14
EU agencies and International Organisations – tools and assistance	15
Presentation on Observatory’s Anti-Counterfeiting Intelligence Support Tool (ACIST) and Enforcement Database (EDB)	15
Presentation on Europol’s Operations and Platform for Experts (EPE)	16
Presentation on Eurojust’s Support to Member States’ Operations	17
WIPO’s Role in Addressing IP Infringements on the Internet	18
Day Three – The Hong Kong Approach Against Online IPR Infringements and their Public – Private Partnerships	19
The Work of the International AntiCounterfeiting Coalition (IACC)	21
Current Trends, Potential Threats and Opportunities	22
Small Parcel Consignments (DHL)	22
Business Software Alliance – Potential Links to Cybercrimes	23
Infringing Content and Hosting Services – NetNames	24
Conclusion	26
Annex	27
Digital Piracy Workshop Co-Chaired by The Romanian Police and OHIM	27
Digital Piracy Workshop Co-Chaired by The City of London Police and the Bulgarian Prosecution Service	27
Counterfeiting Workshop Co-Chaired by the Hungarian Prosecution Service and Europol	28
Counterfeiting Workshop Co-Chaired by ICE-IPR Center and the International Public Prosecution Office, Stockholm	30

# OVERVIEW

---

A jointly held conference on Infringements of Intellectual Property Rights on the Internet took place on 5th, 6th and 7th November 2014 at the Office for Harmonization in the Internal Market (OHIM) in Alicante. The knowledge building event was organised and hosted in cooperation between the OHIM, Europol and Eurojust, and underlined their working commitment with each other.

The conference brought together stakeholders from well-known brands and representatives from the private sector including The Audiovisual Anti-Piracy Alliance (AAPA), European Alliance for Access to Safe Medicines (EAASM) and the British Phonographic Industry (BPI); Customs and Police officers from across the Member States, Norway, US and China; European Prosecutors, the European Commission, INTERPOL and the World Intellectual Property Organisation (WIPO).

The majority of online Intellectual Property (IP) infringements are global, cross-border crimes, composed of actors, servers, proxy servers, cyberlockers, targeted markets, producers and sellers working together but existing in many different jurisdictions. Infringers use and abuse the services of the Internet, search engines, online sales platforms, payment service platforms, payment service providers, advertisers, express shipments services and postal services in order to market, sell and distribute their products. There is increasing dialogue about the role of these intermediaries, and how they can support Enforcement through due diligence in the counterfeit supply chain.

Presentations and speakers underlined the transnational bases of Internet crimes and supported the strategic "follow the money approach" proposed by the European Commission in its ten point Action Plan 2015<sup>1</sup>. Speakers highlighted that the increasingly sophisticated and global nature of Cybercrime requires an equally global answer on the behalf of the Judiciary and Enforcement to tackle circumvention techniques and sale methods; the flow of illicit money constantly moves across and into many countries, their jurisdictions and their applicable laws.

Alarmingly, IP infringements on the Internet are not a stand alone crime. Increasingly, the proceeds from IP infringements are reinvested into other illegal activities, including human and drug trafficking activities. The merger of and cooperation between traditional and non-traditional criminal networks, allows them to harness established illicit transport routes, knowledge and manpower across Europe, Third Countries, the US and China.

The aim of the three day event was to raise levels of awareness about the problem and scale of issues surrounding Internet piracy and counterfeiting; to exchange information about best practices and difficulties faced by Enforcement officers owing to the transnational nature of Cybercrime and its constant evolution; to discuss the new tools and databases made available by the EU Observatory, and to extend and develop the network.

.....  
<sup>1</sup>- Communication from the Commission to the European Parliament, the Council and the European Social and Economic Committee: Towards a renewed consensus on the enforcement of Intellectual Property Rights: An EU Action Plan.

Participants discussed infringements and threats relating to pirated software, malware and counterfeit goods (including fake and substandard medicines) sold via the Internet, and the fact that the problem is increasing, owing to adaptable methods used by the infringers involved.

Eurojust and Guardia di Finanza underlined the fact that Intellectual Property Crime is a predicate offence, with direct links to money laundering and serious and organised criminal networks. Piracy and counterfeiting offer large financial rewards for the criminals involved, anonymity via online marketing and sales, and distance from Enforcement, prosecution, and the victims involved. The Federal Bureau of Investigations (FBI) explained the emerging trend of pirated software and malware used in order to infiltrate consumers' bank details and to facilitate identity theft on a global basis - both activities offer very lucrative revenue streams.

Presentations from Enforcement underlined the level of technological and Intellectual Property knowledge held by emerging criminal networks. Such mergers are formed under a fluid structure and render identification and detection very difficult for Enforcement. For example, historical producers of counterfeit medicine and pharma goods are moving away from street trade to online trade, facilitated by the technical know-how offered by cybercriminals - who conversely, benefit from the traditional knowledge of money laundering techniques.

The clothing and sporting goods brand Lacoste underlined the problems in pursuing an investigation into online counterfeit goods across Member States and Third Countries - despite the efforts of brand protection teams working in close cooperation with Enforcement, cross-border cases rarely result in successful actions or damages, and criminal sanctions remain inconsistent in applicability and severity. Participants called for further harmonisation of Internet legislation in general and a review of the E-Commerce Directive<sup>2</sup>.

The commitment on the behalf of brands to protect their products and their clients, and to support Enforcement was highlighted throughout the conference - including the collation of data, solid evidence and presentation of files, Customs' and intermediaries' training regarding seizures and trends, and lobbying. During the workshops, private sector participants called for the establishment of a global soft law, forged through the working cooperation of private and public organisations.

Europol and Eurojust explained the tangible and mobile support they can offer before, during and in the concluding phases of transnational cases - including facilitating Joint Investigation Teams (JIT), rapid mobile response units, secure communication lines and translation services. The Observatory's role as a central European network of IP experts, Enforcement, Judiciary and public and private stakeholders was emphasised, and a presentation given on the secure and free online enforcement tools they have designed to fight IP crime.

The National IPR Coordination Center managed by ICE (U.S. Immigration and Customs Enforcement) explained their focus on outreach training and the need to educate younger children about the dangers caused by piracy and infringements on one hand, and the value of IP and respecting IP on the other. This sentiment was repeated by Hong Kong Customs who explained their work with the Youth Ambassadors Against Internet Piracy Scheme, and Business Software Alliance (BSA) who presented on the ongoing work carried out by Romanian Police with school age children in order to educate an emerging generation of digital and online consumers.

.....

2- EU Electronic Commerce Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000.

The organisers' aim was to enhance contacts and support cooperation within Enforcement, the Judiciary and private sector, in order to combat the phenomenon in a collective and organised manner. The UK Intellectual Property Office - who reported on the rewards of successful collaboration and sustained dialogue between specialised officers in the City of London Police IP Crime Unit (PIPCU), right holders and intermediaries - underlined that there is no one solution. Instead, an armoury of strong and harmonised legislation, technological tools, a clear understanding of available civil and criminal legislation, and enhanced training of Customs, Police, the Judiciary and the private sector should be founded. The UK IPO emphasised the need to develop and present a strong argument about the real dangers of IP Internet crime to policy makers, based on firm evidence and empirical data.

Participants articulated the need for increasing private sector communication alongside conscious and daily cooperation within global enforcement units, in order to combat what are already sophisticated, agile and highly active criminal networks within the European Union, US and Third Countries.

# Day One

## Welcome and Introductory Speeches

---

The Director of the European Observatory on Infringements of Intellectual Property Rights opened the conference and warmly welcomed all participants to the fifth knowledge building event held by the Observatory, for Enforcement. There were 105 participants at the event, including 22 Public Prosecutors.

He underlined the main aims of the Observatory, which is a network of experts, stakeholders and Enforcement, set up to support the protection of Intellectual Property Rights (IPR) by the European Commission, and transferred to the OHIM in 2012. The Observatory focuses on the production of studies and online tools in order to support enforcement activities, topic-specific training events, identification of best practices, and facilitating network growth to include working cooperation with Eurojust, Europol, WCO, CEPOL and EPO, and to create synergies within global enforcement organisations.

Europol thanked the OHIM for their role and cooperation in organising the conference, and explained that, in the twelve months since the Memorandum of Understanding (MoU) was signed between the Observatory and Europol, their joint efforts have intensified to form the basis of a new agreement which will focus specifically on Intellectual Property Crime on the Internet.

Europol explained the need to find a balance between societal freedom and legal economic growth via the Internet. Business and business models across the globe have changed due to visibility on the Internet via E-Commerce. The majority of society uses the Internet to communicate and consume, there are over 750,000 new Facebook users every day, and consumers of all ages learn via online tutorials and online libraries. Criminals exploit the opportunity to engage with consumers via the Internet extremely well, and there is a growing trend of high level criminal gangs contracting IP experts in order to support their activities. To successfully tackle this increasing problem, there is a need for a professional response and a collaboration of efforts across all sectors: IP crime does

not recognise territorial borders. Europol welcomed the involvement of the Judiciary and the private sector, the latter of which are often the first to receive real time intelligence on infringements. The work of the European Cybercrime Centre (EC3) and Focal Point Copy, both housed within Europol was highlighted, which aid other enforcement agencies via legal, operational and physical support.

Eurojust highlighted the transborder and predicate nature of IP crime on the Internet and the ability of those involved to adapt quickly, once discovered. They also explained the difficulty in detecting the actors involved, their links to money laundering, the technicalities of emerging trends, and the lack of dual criminality if more than one Member State is involved in the crime - which is often the case. Eurojust offers a platform, a source of expertise and judicial cooperation, and a translation of issues including the admissibility of evidence to all competent national authorities. The organisation expressed their wish for the knowledge building event to be harnessed fully by all participants and agencies, in order to work together to tackle the transnational nature of Cybercrime.

Google explained their methods to tackle piracy and their efforts to remove infringing pages from the Internet. The company accepts notices regarding removals through the Digital Millennium Copyright Act (DMCA) web form and offers a bulk submission tool for trusted submitters. Over 22 million web pages were removed by Google in 2013 following requests, with an average turnaround of less than six hours. They explained that sites with high numbers of removals are demoted in search results, and the subsequent demotion downranks torrent sites effectively and reduces their visibility.

Google underlined their wish not to be associated with pirates and their aim to enforce copyright, by maintaining strong anti-infringement policies and by shutting down accounts which violate them. The Motion Picture Association of America (MPAA) discussed their focus on addressing three main areas in order to fight infringements of Intellectual Property Rights (IPR) online; they address the infringing sites; they work alongside intermediaries including payment processors and ISP providers, and they carry out activities with children from two years old onwards, in order to educate the future generation to understand why it is so important to respect copyright.

They underlined the importance of public and private sector cooperation in "follow the money" approach, and explained that there is no value in legislating a model that cannot be put into practice. They explained that it is more effective to work directly with intermediaries on a voluntary basis, to find a model that could work. However, the need for supporting legislation was called for, to block major pirate sites and to improve the protection of copyright content.

The successful example of US Enforcement working with the four largest ISP providers was relayed, and the hope that online consumer behaviour can be altered, and the perception of the importance of IPR can be supported, following awareness campaigns and alerts. In the UK, the government has pledged £3.5 million to support a public awareness programme.

The role of search engines, search tools and listings were highlighted, particularly employed by first time users. The Observatory explained to participants the format of the three day event, which included presentations, the exchange of best practices, feedback from the floor, networking and designated workshops focused on digital piracy and counterfeiting. The presentations began.

## Right Holder's Efforts

---

MPAA, the trade association for six major US studios, presented on their centralised enforcement efforts, stemming from a unit base in Brussels, and with support from enforcement hubs in the US, Canada, Brazil, Belgium Hong Kong. The organisation uses a combination of civil and criminal actions including take down notices, site blocking and action against intermediaries, but they stressed the need for support from law enforcement authorities, and strong European jurisprudence.

They explained that traditional source piracy, in which camcorders are used to record copyright content in cinemas, is now complicated by the existence of content in cyber lockers<sup>3</sup>, on linking sites, peer-to-peer sites, and apps. The use of apps to house illegal content is a growing market because app content remains, as do the revenue streams for the apps, after sites are shut down. The user of cyberlockers, using centralised servers, is based on a business model of content theft. The content remains, even if the link to the cyberlocker is broken. Premium consumer subscriptions result in high revenues for illegal downloads, and no tax is paid on this revenue. Confusingly for consumers, website layout often appears identical or very similar to legal sites. BitTorrent sites offer indexing and use adverts throughout a site in order to create revenue. The organisation works proactively in terms of assessing new threats including set-top boxes, app stores and infringing sites such as [www.facebook.com/thetime4popcorn](http://www.facebook.com/thetime4popcorn) and [Joker.org](http://Joker.org).

**Adobe** explained that following the shift to licensed software which manages content via Cloud technology (Adobe Creative Cloud and Adobe Marketing Cloud), piracy was not eliminated, and counterfeit initially increased. The company changed their business model in order to capture the consumer base who search for illegal offers online. *Adobe's* research showed that there are five times more users of pirated *Adobe* products (who pay pirates for their goods), than users of genuine products. The company decided to view these users as potential customers, not thieves, because some of the users of pirated content are well-intentioned victims and not piracy-inclined. Furthermore, they decided to place their main focus on mature markets, made up of a higher proportion of legally inclined users, with an aim of capturing all the demand that the brand creates for genuine *Adobe* products, and helping consumers access legitimate software.

A complete pirated box product, with modified software, is offered for sale three months after the launch of a genuine product. *Adobe* underlined the 33% risk of malware infection when users access illegal software based on the figures in the IDC study<sup>4</sup>. In the face of such statistics, the company emphasised the importance of educational awareness campaigns which convey to the public the benefits of using legal software, and

.....

3- A cyberlocker is an Internet hosting site that allows users to upload files to the Internet for sharing and storing, and generally houses content which violates copyrights.

4- The study, called "The Link between Pirated Software and Cybersecurity Breaches", was carried out by the International Data Corporation (IDC) and National University of Singapore (NUS).

the risks involved in using pirated products. The floor noted the business model of segmenting customers and viewing consumers of pirated goods as potential users of genuine products, and suggested this model could be used by other sectors.

**Lacoste** presented on the Intellectual Property history of their brand, which was the first to use exterior trade marks on clothing, in 1923. They continue to use only selective distribution and named shops alongside an online presence. However, there is widespread counterfeit of the brand, and a prolificacy of sites offering illegal goods, with non-contactable registrants, foreign servers and hosts, and sites who do not reply to cease and desist letters.

*Lacoste's* presentation underlined the problems associated with detecting and pursuing cybercriminals across the globe, including a lack of national case-law and the use of proxy servers. After investigation, the company found many infringing ISPs sit in the Netherlands, Sweden, Malaysia and Belize, and one infringing site often has widespread links to many other infringing domain names. In many cases, the owners do not respond to letters threatening civil action, and ISPs can be switched within seconds. Sites with national addresses but which have no link to that State, cannot be pursued by the national authorities.

*Lacoste* conveyed issues with *ICANN*<sup>5</sup>, the organisation which runs the assignment of domains on the Internet, because it is possible to hide information held on *WHOIS* and mask the identity and address of the traders. Furthermore, the brand called for the end to anonymity for professional traders. They also explained the financial implications of taking available infringing sites off the market – sites that the right holder does not want to use, but must pay for.

Possible legal grounds for pursuing a case include the language used within the infringing content and payment links to a Member State; in the *REACT v Altushost* decision<sup>6</sup>, the Court of The Hague laid down the seizure of assets and liability of the intermediary, based on the E-Commerce Directive.

*Lacoste* called for a harmonisation of enforcement actions across the Member States via a centralised agency, a further harmonisation of Internet Law in general, and a review of the E-Commerce Directive<sup>7</sup>.

**Vitra** presented on problems of enforcing Intellectual Property Rights owing to the differences in European legislation and the difficulties in tracking down the culprits, if they trade exclusively online. *Vitra* is a Swiss furniture design brand who promotes innovation, uses external designers and rely on copyright in order to protect its products. Most counterfeits of its furniture are made in China and shipped to Europe – the rogue companies are generally registered in the UK as legitimate traders because the UK does not protect applied art as copyright yet, but only offers 25 years of protection. Rogue online traders take advantage of the loophole due to the lack of harmonisation of EU law – and some offer fake goods but do not deliver, once payment has been made.

The company underlined the difficulty of enforcing civil judgements against letterbox companies, because the actors do not exist at their official address. They stated that the “follow the money” approach has offered some success, by working alongside intermediaries including payment service providers. To date, public prosecution has not offered a result owing to the differences in cross-border criminal prosecution practice – but payment service providers are able to seize payments made to the counterfeiter’s website, which effectively blocks the revenue on which criminals depend.

.....  
5- The Internet Corporation for Assigned Names and Numbers.

6- On 29th June 2012, REACT summoned Altushost to appear before the Court, requesting the Court to order a block to access, and keep access blocked from the Benelux to the websites at issue and to cease its hosting services for these websites permanently, based on Article 2.22, section 6 of the Benelux Treaty regarding Intellectual Property (BTIP). The treaty entitles a Judge to issue a cease and desist order for services of intermediaries which are used by third parties to infringe trade mark rights.

7- EU Electronic Commerce Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000.

## The Internet and Payment Industry Support

---

### Google

*Google* underlined the value of the Internet and the opportunities offered to creative industries by online presence.

They posed the question – should the fight be positioned against the effect or the cause? The company receives up to 1.2 million requests about infringing and unsuitable webpages on a daily basis. The content generally reappears if taken down, and they questioned the efficacy of taking down infringing content. The other option is to take down entire sites in Europe: the Copyright Directive<sup>8</sup> provides the legal means to pursue website providers.

*Google* supported the idea of following the flow of money, which is made directly through sales and facilitated by payment service providers, and indirectly, via advertising intermediaries. However, it was noted during feedback from the floor that by targeting payment providers, the effect is targeted, not the cause. The European Commission noted that the Copyright Directive discussed the intermediary “best placed to bring such infringing activities to an end”, and that there should be other tools used including best practices and MoUs.

The floor asked *Google* why they continue to index advertisers in the search engine, after taking down the original content. They replied that it is difficult to ascertain what content is legal at a given time and within a given jurisdiction.

The British Phonographic Industry (BPI) asked if *Google* proactively takes away the option to advertise from known infringers, and explained that in the UK, this method is used alongside blacklisting of repeated infringers.

### eBay

*eBay* (which owns *PayPal*) presented on their activities to promote IP protection. In May 2011, they signed an MoU based on the European Commission initiative with stakeholders, platforms and brands in order to promote a collective effort against counterfeiting online at a European level. Founded in 1995, with 128 million users worldwide, the site houses 550 million live listings. *eBay* has a global presence in over 39 countries but consumer and traders of the site will rarely meet face to face – the concept *eBay* is founded on trust, whilst the sale of counterfeits harm the business.

The *eBay* Global Asset Protection (GAP) team specialise in proactive and reactive investigations. The team has 55 investigators working worldwide alongside global law enforcement and is dedicated to reducing any criminal activity. Via VERO (Verified Right Owners’ Programme), 90% of reported offending listings are removed within an average of 12 hours. *eBay*’s brand risk management policy and detections team promotes responses to infringement reports and offers training and dialogue with global brands.

.....  
8- Directive 2001/29/EC of the European Parliament and of the Council of 22nd May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

## EBAY IS COMMITTED TO IP PROTECTION

**Best Global Brands 2013**

**The New Top 100**

**The Leadership Issue**

**Sector Overviews**

**Articles & Interviews**

**Charts**

**Methodology & Applications**

**Contact info & Downloads**

**ebay**

**“Our success is strongly tied to enabling others to win, whether an entrepreneur or a global brand.”**  
— John Donahoe, President and CEO, eBay

**eBay vs Retail Sector**

Year	eBay Revenue (USD)	Retail Sector Revenue (USD)
2000	~10	~10
2001	~15	~15
2002	~20	~20
2003	~25	~25
2004	~30	~30
2005	~35	~35
2006	~40	~40
2007	~45	~45
2008	~50	~50
2009	~55	~55
2010	~60	~60
2011	~65	~65
2012	~70	~70
2013	~75	~75

ebay and IP protection

The UK Intellectual Property Office (UK IPO) asked what steps were in place to stop the abusers from continuing to abuse via eBay? The company replied that the individual must take an IP tutorial before reengaging in trade via the platform, and if they continue to offend, their account will be suspended.

### VISA Europe

VISA Europe presented on their commitment to safe online business. VISA is owned and operated by over 3700 member banks but does not sign up merchants themselves. In order to protect against card abuse, VISA Europe states that all transactions must be viewed as legal in all applicable jurisdictions. The payment facility enables payments between consumers, retailers, businesses and governments and fosters competition between VISA member banks. However, the growth of online payments via mobile phones and other technology has also increased avenues for exploitation.

The organisation underlined the statistic that fraud has declined to EUR 0.05 in every EUR 100 and suggested there is work to be done with mobile distributors due to the increasing amount of risk when using mobile apps regarding illegal content. They also noted the increase in the use of cyberlockers by online retailers.

VISA’s Electronic Commerce Merchant Monitoring Programme enables merchant termination for infringing merchants within a three day threshold (the programme also deals with sites showing offensive visual material). Rising penalties are applied for non-compliance, and the programme has shown a large rise in reported copyright infringement. Additionally, best practice models guides are given to their acquirers/merchant banks, alongside working groups, forums and monitoring groups for acquirers in order to discuss a common strategy to reduce the sign up of infringing merchants.

The floor asked which trusted source normally communicates information of the infringement, to which *VISA Europe* replied, there must be clear evidence, so the intelligence normally comes from a right holder.

It was explained, that, since the introduction of chip and pin, there is a very low percentage of fraud via their payment method, because it is extremely secure. However, in the US, *VISA* cards are cloned because payment protocol by the customer requires only processing of the magnetic stripe. This is one of the reasons that has caused the transfer from face to face fraud to e-commerce fraud.

The Federation of the Swiss Watch Industry replied their findings show that the weak link in payments is between the card acquirer and merchant.

## Effective Investigative Techniques in Europe and Abroad – Case Examples from the Public Sector

---

### The United Kingdom Intellectual Property Office (UK IPO)

The United Kingdom Intellectual Property Office (UK IPO) reported on counterfeiting's financial effects on government and private sector revenues, and highlighted digital piracy's links to already existing serious and organised criminal networks. Cybercrime is a borderless crime, but national jurisdiction and their sanctions are applied. In the UK, Prosecutors use a range of legislation including the Fraud Act, conspiracy to defraud, product safety legislation, money laundering sanctions and criminal "lifestyle offences"<sup>9</sup>, which allow seizure of assets. Owing to landmark cases, including *Newzbin2*<sup>10</sup> and *OiNK*<sup>11</sup>, guidelines regarding procedure and proportionality have been drawn up. Following the *L'Oréal v eBay* case<sup>12</sup>, the City of London Police's Economic Crime Department has established a proof of process from an economic crime perspective, and an IP Crime Strategy.

The UK IPO presentation underlined the need to use a combination of civil and criminal methods and to work in cross-sector cooperation to successfully tackle digital piracy and online counterfeit behaviour. The National Fraud Intelligence Unit within the City of London Police works alongside rights holders and the Internet advertising industry, in order to produce an Infringing Website List. The Metropolitan Police has developed relationships with domain registrars in order to remove offending domains. Right holders and their brand protection teams increasingly supply complete evidence to support a criminal prosecution, which allows the Police to harness money laundering regulations. However, there are problems regarding the volume of cases, and cases which have insufficient evidence in order to permit criminal prosecution or Police intervention.

In spring 2015, a major multi-media educational awareness campaign will be launched, led by content creators and partly funded by the UK Government. The floor asked what more could be done by *ICANN* regarding due diligence of intermediaries. The UK IPO responded that in order to influence policy, a strong argument based on facts and evidence must be developed.

.....

9- The Proceeds of Crime Act 2002 (POCA) refers to criminal provisions of the Copyright Designs and Patents Act 1988 and of the Trade Mark Act 1994. The effect of Schedule 2 renders counterfeiting a so-called "lifestyle offence", and consequently, counterfeiter's assets can be confiscated under POCA.

10- In a landmark test case in July 2011, the High Court in the UK ordered BT, as an intermediary, to block access to the pirate site *Newzbin2*.

11- *OiNK*'s defence – that it did not physically host any of the music content (as per *The Pirate Bay* defence) was not upheld in court and the owner was found criminally liable.

12- C-324/09 *L'Oréal SA and Others V eBay International AG and Others*, 12th July 2011.


## Guardia di Finanza's Operational Experience

The Guardia di Finanza's presentation set the scene regarding the global use of the Internet and the changing nature of counterfeit sale methods in Italy. With an annual sales volume of EUR 6.5 billion, a loss of tax revenue of EUR 5.2 billion, and 105, 000 lost jobs, counterfeiting has had a huge and negative effect on the Italian national economy.


**ORGANIZATION AND OPERATIONAL LINES OF ACTION OF  
THE GUARDIA DI FINANZA**

**HOW GUARDIA DI FINANZA FIGHTS  
PIRACY AND COUNTERFEITING**

- ✓ **protection of customs areas;**
- ✓ **economic control of the territory;**
- ✓ **business Intelligence;**
- ✓ **web monitoring;**
- ✓ **interception of financial channels used to move the  
proceeds of criminal activity;**
- ✓ **aggression of criminal assets that have the profit of  
counterfeiting and piracy;**
- ✓ **verification of profiles fiscally linked, fair competition  
and consumer protection.**



**EU OBSERVATORY**  
EUROPEAN OBSERVATORY ON INFRINGEMENTS  
OF INTELLECTUAL PROPERTY RIGHTS



Since 2003, Italy has made a concerted effort to increase national IP protection, including the development of an efficient judicial system, the establishment of a specialised civil IP division, reforms to the Industrial Property Code, and most recently the implementation of a law addressing digital copyright piracy. The organisation operates via their Special Department and Territorial Units, whose task is to protect the financial interest of the country and EU economy via Customs actions, business intelligence, web monitoring, the interception of financial channels used to move the proceeds of criminal activity, and consumer protection. Officers work in cooperation with INTERPOL, Europol, OLAF and WCO, and they have a close working relationship with the national Ministry of Economic Development and collaboration through the Market Protection Special Unit and the Special Unit for Broadcasting and Publishing. Their Cyberfraud Intelligence Department uses SIAC<sup>13</sup> and houses anti-counterfeiting intelligence search engines which are based on semantic searches. The department also uses computer forensics and web monitoring risk indicators in order to extract data matched against third party databases. In order to "follow the money", the department uses intelligence to identify the channels of money and look for additional activities, including phishing<sup>14</sup>.

13- The Guardia di Finanza's Anti-Counterfeiting Information System

14- Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

In 2013, Italian enforcement officers intercepted 130 million counterfeit goods. Investigations clearly shows that IP counterfeiting is a predicate offence, sometimes hidden behind seemingly legal businesses, and its proceeds are reinvested in other organised crimes. The Guardia di Finanza underlined the need to harness existing European legislation, specifically Directive 2014/42/EU<sup>15</sup> which provides for sanctions regarding the proceeds of financial crime. Since 2012, the IACC (International Anti Counterfeiting Coalition) has promoted a payment processor initiative called "Rogue Block" and underlines the progressive cooperation right holders and intermediaries.

### Hong Kong Customs' Operational Experience

Hong Kong Customs presented on their Cybercrime cases involving cyberlockers and BitTorrent<sup>16</sup> sites. Investigations into ISP addresses allowed officers to search the residential addresses of the actors involved. Application of the Copyright Ordinance, Chapter 528<sup>17</sup> allowed the criminals to be prosecuted, fined for a maximum of \$50,000 per infringing copy and sentenced to four years imprisonment.

They underlined the fact that digital evidence can be altered very quickly, and cyber units require increasing numbers of specially trained officers to gather forensic evidence. They also pointed that the action of blocking sites does not help Customs to detect the individuals who have produced the counterfeit products.

### Operation Vigorali

Operation Vigorali, a jointly exercised operation in 2013 brought together countries (Austria, France, Spain, UK and other countries), and displayed cross-border and interagency cooperation, with support from Europol and Eurojust. The coordination of efforts in different time zones allowed simultaneous arrests of the criminals involved, in different jurisdictions. The multiagency approach harnessed expertise from the Guardia Civil, Europol, Bundeskriminalamt Wien, the Spanish Judiciary, UK law enforcement, Intelligence from the UK Medicines and Healthcare Products Regulatory Agency (MHRA) revealed the drop shipments of fake pharmaceuticals, produced in India, sent to addresses in the UK, onto Spain and the rest of Europe, with the use of bank accounts in Europe and the US. Europol cross-checked the information on the transnational criminal network, deployed a mobile office at the coordination center of Eurojust and in Austria and mobile equipment to analyse the pharma products.

The officers involved underlined the fact that many of the criminal groups involved in online Pharmacrime rely on existing logistics routes – and they operate with the sole aim to make money, those involved in this case moved from the sale of cigarettes to counterfeit goods, and finally to the distribution of fake *Viagra*. The Austrian Penal Code and the Pharmaceutical Law were applied and the actors involved prosecuted under these regulations.

## Day Two

The second day of the conference commenced with a review of the key messages and feedback gathered during the first day. The Observatory explained the work carried out by the OHIM's established CTM Judges' Network – which

15- Directive 2014/42/EU of the European Parliament and of the Council 3rd April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

16- BitTorrent – a protocol for the practice of peer to peer file sharing, used to distribute large amount of data over the Internet, from one source who holds the complete files.

17- According to which a person commits an offence if he/she distributes infringing copies of copyright works otherwise than for the purpose of, in the course of, any trade or business to such an extent as to affect prejudicially the owner of the copyright, without the licence of the copyright owner. The maximum penalty is a fine of \$50,000 per infringing copy and four years' imprisonment.

brings together criminal, administrative and civil Judges, as well as Prosecutors, from across the Member States for regular training and networking. The Observatory and Eurojust announced their intention to sign an MoU together, in order to further consolidate a strong platform composed of European Judiciary and Enforcement.

Subsequently, four workshops held throughout the morning, for which participants signed up. Two focused on digital piracy and two focused on counterfeiting. In order to discuss more closely the issues and obstacles surrounding enforcement of counterfeit and digital piracy, participants answered the following questions alongside presentations within each workshop;

- What are considered by enforcers as effective measures to counteract both counterfeiting and/ or piracy (practical cases examples of successful operations, particularly cross-border or cross-agency)?
- Is the current legislation up to date and is it really enforced at national level (national experience and constraints to be discussed).
- Is there any example of public-private partnerships that can be considered as effective to counteract both counterfeiting and/ or piracy (existing or new initiatives with a possible comparison between US and EU initiatives)?
- What are the main practical obstacles (funding, exchange of information, lack of harmonised laws) faced by enforcers, and what could be done to face such obstacles?

The key findings and participants' comments are detailed in the Annex as bullet points for ease of reference.

## EU agencies and International Organisations – tools and assistance

---

### Presentation on Observatory's Anti-Counterfeiting Intelligence Support Tool (ACIST) and Enforcement Database (EDB)

Progress on the Enforcement Database (EDB) and Anti-Counterfeiting Intelligence Support Tool (ACIST) was reported. Launched at the end of November 2013, the EDB tool is used by more than 100 companies across 23 sectors who can share information with enforcement agencies about their products. In collaboration with the European Commission, the EDB can now be accessed by Customs authorities across all Member States via their secure network, CCN.

ACIST is a free tool which offers a harmonised data collection of single and multi detentions from Police, Customs and other enforcement authorities, so that they can see how counterfeited goods are moving within the Internal Market. The system enables users to upload relevant data via a user friendly interface, using electronic files (XML, Excel, etc.). Additionally, the system converts the data into a harmonised format so that it can be compared and aggregated, offering users a set of possibilities of data exploitation, including reports and interactive analysis. ACIST generates reports regarding the type of property rights infringed, the timescale, proportion of categories infringed and territory.

The tool launch will be assisted by a road show campaign and training, in order to support Enforcement in the harmonisation of data collection on seizures across the Member States.

### Presentation on Europol's Operations and Platform for Experts (EPE)

Europol's partners sit across all Member States, Third Countries and third parties, with close connections to other law enforcement agencies including Eurojust, INTERPOL, ICE<sup>18</sup>, OLAF<sup>19</sup> and the EMCDDA<sup>20</sup>.

The Operations Department houses EC3, (The European Cybercrime Centre), a Serious and Organised Crime Unit, a Counter Terrorism Unit and the Operational Centre Info-Ex Hub. EC3 is almost two years old; a vision of the European Commission in order to establish a European Cybercrime centre via a mandate. On an operational level, EC3 has three focal points – Cyborg which deals with hacking; Terminal which deals with card skimming, and Twins, which tackles online child abuse.

Focal Point Copy sits within the Economic Crime and European Counterfeiting Group, and was established in 2008. Focal Point Copy has members from over 20 Member States, and focuses on commodity counterfeiting and piracy. Since March 2013 (due to an expansion in the legal framework) it also focuses on health and safety and on hazardous and potentially harmful products - including dangerous pharmaceuticals, foodstuffs and pesticides - in order to address the evolving counterfeit issues in Europe.

In 2010, Europol became an official EU agency. Owing to a European Council decision, the organisation is able to receive intelligence from the private sector, who are often the first to gain information from consumers. Europol acts as a practical contact point regarding serious and organised crime cases involving at least two Member States. In addition to complex and cross-border investigations and seizures on the ground, the organisation offers intelligence, analysis, forensic support, bitmapping and swift mobile office deployment at investigation level. The agency also sends out early warning messages regarding new trends in counterfeit products and runs many liaison and training events, including a recent training event in partnership with OHIM on fake pesticides. The scope of interagency cooperation was highlighted, alongside impressive results in quantities of seized counterfeit goods (via "Operation OPSON" alongside INTERPOL) and seized websites selling counterfeit goods (via "Operation in Our Sites", in cooperation with the US National IPR Center and French Gendarmerie Nationale).



.....  
18- U.S. Immigration and Customs Enforcement  
19- The European Anti-Fraud Office  
20- The European Centre for Drugs and Drug Addiction

## Project “In Our Sites – Transatlantic 3”



- **Europol and ICE teamed with 10 LEA from 8 countries**
- **To seize the domain names that selling counterfeits merchandise on the internet**
- **In 2013, 16 websites hosted in Hong Kong were taken down**

Europol’s online and secure Platform for Experts (EPE) supports invited members (of which there are currently 407) from Enforcement, and people working in IP crime on a daily basis. The platform is organised in different sections dedicated to specific crime areas and open to specific communities of authorised users. It offers an exchange of non-operational information in order to support investigative work – members can upload information, including IP training events and a shared contacts database.

### Presentation on Eurojust’s Support to Member States’ Operations

In 1999, the Tampere EU Council decided to establish a permanent body of judicial coordination (Eurojust) to reinforce Member States’ efforts to combat serious and organised cross-border crimes. Eurojust was established in 2002. Eurojust competence indirectly covers IP related crimes including other forms of criminality such as counterfeiting and forgery, money laundering, computer crime, fraud, corruption, financial crime and participation in a criminal organisation.

The European Union consists of 30 jurisdictions that end at their physical national borders. Consequently, there are various legal problems involved in cross-border investigations and prosecution – including the admissibility of evidence, lack of dual criminality, positive or negative conflicts of jurisdiction, and the danger of *ne bis in idem* (double jeopardy) situations. International mutual legal assistance (MLA) treaties and EU mutual recognition (MR) measures including freezing orders (FO) and European arrest warrants (EAW) have not been implemented into national laws in a harmonised way, which often creates barriers against their smooth execution.

Today, Eurojust College consists of 28 National Members seconded by each Member State, made up of Prosecutors, Judges and Police officers who have the authorisation to exercise judicial cooperation and coordination. Individual National Members or their College may request the national authorities of a Member State to investigate or prosecute specific acts; to accept that one Member State is in a better position to undertake an investigation or to prosecute; to coordinate between Member States and to set up joint

.....  
2- EU Electronic Commerce Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000.

investigation teams (JIT). National authorities should report almost all serious cases involving transborder crimes within the EU, in which at least three Member States already cooperate. They are to provide Eurojust with necessary information on JITs; possible and existing conflict of jurisdiction cases; controlled deliveries; recurrent refusals or difficulties regarding MLAs, EAWs, and FOs. Eurojust offers support to identify and resolve the legal and practical gaps.

Eurojust offers a quick information exchange platform between national authorities, including the management of coordination meetings in order to coordinate parallel investigations, to discuss judicial strategies and operational roles. Eurojust also offers coordination centres so that arrests, searches and seizures can be carried out simultaneously and with secure communication lines. Very often, Europol is invited to share their data.

Joint Investigation Team (JIT) management is one of Eurojust's most important tools. According to the 2000 EU MLA Convention, it is a judicial instrument which facilitates extended mutual legal assistance. From a judicial point of view, it restricts judicial barriers, and importantly, the presiding trial Judge may not exclude any evidence collected during the investigation in another Member State (under a different procedural regime). Eurojust expertise is offered to generate the establishment of a JIT, in drafting JIT agreements; and in financing the actions under JIT agreements.

Eurojust's financial support normally covers the costs of travel, accommodation and meals; simultaneous translation during meetings and for records of testimonies and ongoing hearings; and the loan of technical devices including secure mobile phones, laptops and printers.

Additionally, Eurojust hosts EU network headquarters within its administration, namely the Secretariats of the Joint Investigation Teams, the European Judicial Network, and the Genocide Network.

It is foreseen that an European Public Prosecutor's Office (EPPO) will be established by means of a regulation "from Eurojust" (Article 86, Lisbon Treaty) to combat crimes committed against EU financial interests. Currently, there is a lot of legislative effort to draft the future EPPO structure and competence.

### **WIPO's Role in Addressing IP Infringements on the Internet**

WIPO facilitates enhanced cooperation among Member States in the development of balanced international normative frameworks, whilst WIPO Standing Committees serve as forums for treaty negotiation. The organisation helps to develop tailored and balanced IP legislative, regulatory and policy frameworks – and, upon request, the WIPO Secretariat provides legislative assistance to its Member States.

The Advisory Committee on Enforcement (ACE), was established through the General Assembly in 2002 after TRIPS, and addresses global enforcement issues, alternative resolution systems in IP, the role of the Judiciary, Enforcement, education and awareness raising. Work is focused on motivations for infringements and methodologies to measure the social, economic and commercial impact, and preventive actions and successful measures to complement ongoing enforcement methods with the aim of reducing the size of the market for pirated or counterfeited goods.

WIPO treaties under the international normative framework aim at responding to the challenges raised by digital technology and in particular, the Internet<sup>21</sup>, unauthorised transmission over digital networks (Article 8 of WCT/ Article 10 and 15 of WPPT), and storage of works in digital form in an electronic medium. WIPO established the Uniform Domain Name Dispute Resolution Policy (UDRP), which operates outside the courts but preserves court as an option.

Internet infringements trigger Private International Law questions, including competency and recognition. WIPO is currently working on a project to collate case-law on these aspects on cross-border online IP infringements.

## Day Three

# The Hong Kong Approach Against Online IPR Infringements and their Public- Private Partnerships

This year marks the 40<sup>th</sup> anniversary of Hong Kong Customs investigations and the organisation was awarded the Global Anti-Counterfeiting Award by the Global Anti-Counterfeiting Group.

Between 1998 to 2011, there was an increase of 1,330% in seizures of infringing goods by Customs worldwide. Customs is the sole IP enforcement agency in Hong Kong and covers imports and exports, and serious and organised crime. The organisation works with Europol, ICE, INTERPOL, WCO and mainland China.



.....  
21-The Beijing Treaty (2012) foresees protection of audio-visual performances and establishes the IP rights of performers in their audio-visual performances. There have been discussions surrounding another treaty regarding broadcasting rights. The Joint Recommendation Marks on the Internet (2001) offers a soft law instrument, aimed at applying existing trade mark legislation in the context of the Internet in order to avoid infringements and unfair competition.

Their presentation underlined the successful methods used to tackle rapidly changing IPR infringements in Hong Kong, and the regular review of what can be effectively enforced on a practical level – and what cannot. It is acknowledged that, although repeated foot raids to local flea markets selling fakes via catalogues (the criminals aimed to avoid prosecution by not displaying the physical products) caused their activity to drop by 90%, some sellers know how to circumvent detection by enforcement officers.

During the past decade, Customs used the sanctions provided for in Chapter 455 of the Organised and Serious Crime Ordinance (OSCO) to combat the organised nature of IP infringements, Cybercrime and linked money laundering offences. The OSCO foresees up to 74 months imprisonment for sentenced individuals. In 2004, a landmark case involving copyright piracy saw the prosecution of an individual under OSCO, and resulted in the confiscation of the proceeds of the crime. A strong message was relayed to the Public about digital piracy, segments of which view the illegal downloading of material for private purposes as acceptable.

Since 2010, there has been huge rise in piracy via the use of digital platforms in Hong Kong, which marks a switch from street level trade to online trade. The presentation highlighted the fact that once the IP crime has reached a global level – owing to the global marketplace made possible via the Internet – potential income streams are huge, in comparison to a local or national audience.

Hong Kong Customs manages specialised IP crime teams including an expert scene handling team and an expert digital evidence handling team. The Electronic Crime Investigation Centre was set up in order to provide research and development for officers, and to offer training on current trends and technology used in Cybercrime. Hong Kong Customs' Lineament Monitoring System helps to automatically analyse digital files and websites. In order to attain right holders' verification of the nature of seized goods, without the need to travel, an Electronic and Recordation Triage Centre (ERTC) facilitates video communication and file sharing concerning the goods in question – the details of which can be converted using a 3D printer. If the goods are found to be counterfeit, raids can be carried out and goods seized far more quickly. In Hong Kong, Customs are able to disclose information to any relevant party for crime prevention and detection purposes.

Hong Kong Customs works in cooperation with *Yahoo*, *eBay* and *Amazon*, and express couriers including *DHL*. Between 2012 and 2013 there was a 1300% increase in seizures. Due to intelligence from the private sector, Customs have been able to train *DHL* staff in counterfeit goods specifics and to search for and identify risk indicators, so they can act as an expansion to the Customs' team.

In order to address the increasing problem of Pharmacrime, work has been carried out in cooperation with the Consumer Council regarding dispensaries selling counterfeit pharma goods and medicines, including disclosure of actors' details. The Intellectual Property Rights Protection Alliance (IPRPA) brings together right holders and law firms to share intelligence and training.

However, there continues to be a demand for pirated content and for counterfeit goods. The presentation consolidated the message from those earlier in the conference, which underlined the need to engage with younger children of primary school age. Since 2006, Hong Kong Customs have been working alongside the Youth Ambassadors Against Internet Piracy Scheme in order to raise awareness about the dangers posed by fake products, and about the polar benefits of respecting IPR.

Recently, it has been agreed to set up a task force on Cybercrime between Customs, the Hong Kong Department of Justice, Homeland Security, the City of London Police, Europol and INTERPOL.

## The Work of the International AntiCounterfeiting Coalition (IACC)

Founded in 1979, the organisation started out as a collaboration of luxury brands – now, the IACC works on behalf of brand owners from every sector across the world.

The IACC Rogue Block Programme sprang out of the debates following the proposed Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA). The IACC continues to explore voluntary collaboration where legislation is not an answer. The programme works on copyright piracy, the sale of prescription goods without prescriptions and circumvention activities employed.

The organisation has partnered with major credit card and money transfer companies including *Visa Europe* and *Visa International*, *American Express*, *PayPal* and *MoneyGram* and works in dialogue with them.

IACC investigations which analyse the various payment channels used, show that many of the infringing sites and pages that feature on the Internet today are run by the same actors. This fact helps when trying to close down payment services for infringing sites, because one network, operating hundreds of sites, typically uses only a few merchant accounts. When the payment providers are contacted, fewer files and less requests for closure are submitted by the IACC.

The organisation estimates, of 3000 acquiring banks worldwide, there are around 200 who are willing to sign up high risk (counterfeit) merchants. The IACC has had success in closing over 4000 merchant accounts.



Today, there exists a complete shadow sector in suppliers for rogue sites – builders, bullet proof hosters, and bullet proof payment processors. However, research shows that there has been a pronounced reduction in the use of traditional credit card payment activities by rogue sites – even if named payment methods are advertised on sites, they are not always available. Consequently, consumers are asked to send money directly to the counterfeiters, which might dissuade them from buying from those sites.

The floor asked if there were plans to share IACC tools with Hong Kong Customs, to which the IACC replied favourably.

## Current Trends, Potential Threats and Opportunities

### Small Parcel Consignments (DHL)

*DHL* explained their active IPR enforcement policy which focuses on smuggling and fraud in the supply chain and their work with Hong Kong Customs – a relationship based on trust.

#### ACTION BY DHL EXPRESS

---

- Targeting and closing accounts identified by regulators as shipping IPR goods.
- Active involvement in closing IPR websites using the DHL brand.
- Targeting suspect shipments globally using Customs intelligence on known IPR shippers.
- Focus on increasing knowledge management.
- Active engagement with rights holders and regulators to find successful solutions.

The presentation underlined how quickly criminals adapt to *DHL* investigative measures. There is currently a large problem with undervaluation of parcels sent from the Asia Pacific trade lane, including sellers sending forged email and *PayPal* receipts to try to circumvent *DHL*'s request for proof of cost, before shipping.

Some States within the EU currently impose a 100% Customs control on any small consignment originating from Asia Pacific, which causes problems for legitimate businesses caught up in these controls and *DHL*, who have consequent problems fulfilling their service to legitimate clients.

The company underlined their progressing relationship with German Customs and with HMRC and the UK Border Force, but added that there is still a long road ahead in engaging with Customs who, at times, take unilateral action against IPR infringements.

*DHL* owns all vehicles and means in their supply chain, a track and trace system and a strong IT system supported by three quality control centres. Over 24,000 items of counterfeit were intercepted by *DHL* in 2012. As a business, they explained their wish to protect their customers by driving out counterfeit goods – but that they cannot identify counterfeit from non-counterfeit for every right holder.

## KEY CHALLENGES

- Adaptation by counterfeiters to action taken by DHL Express
- Increased professionalism in targeting unwitting consumers
- Unclear picture of the true levels and trends in IPR smuggling
- Need for greater focus on collaboration between Customs & Private Sector
- Focus of IPR measurement on the number of seizures rather than on the number of individual items

5 IPR Knowledge and Awareness  
Building Conference – Allocations 6 – 7 November 2014



The company requires information from the private sector and from Customs, in order to target accounts; shipments can be matched to named accounts, and those clients can be asked to remove the infringing products – or the products can be stopped before reaching their destination and put on the market.

### Business Software Alliance – Potential Links to Cybercrimes

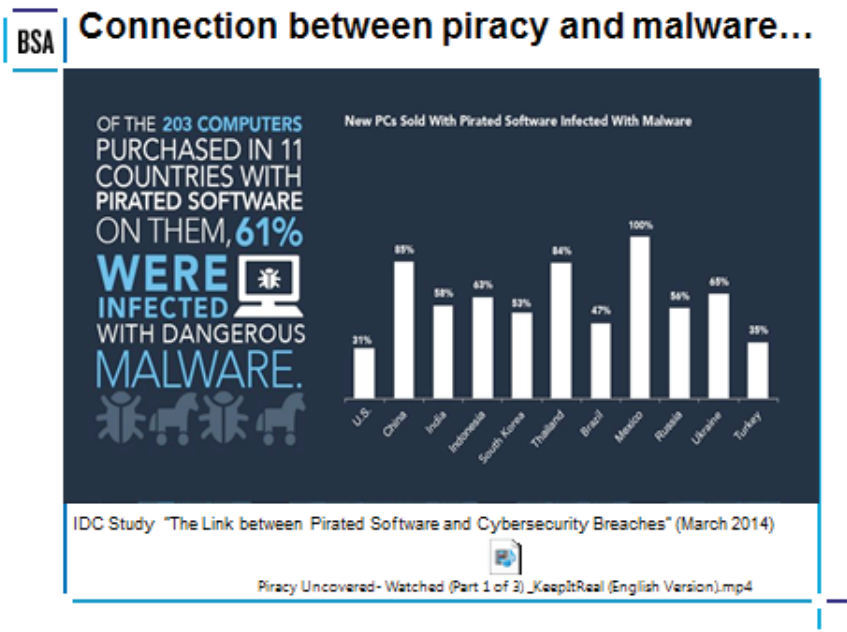
According to the *Norton* Report 2013, twelve people are victims of Cybercrime every second<sup>22</sup> – which adds up to 400 million victims every year, and 50% of adults have been victims during the past year. Cybercrime costs businesses USD 450 billion per year.

Software copyright infringement has strong links to Cybercrime – pirated software originates from unauthorised sources and brings unwelcome guests such as malware. Even those who have chosen to use pirated software, have the possibility to become a victim via Botnets, network intrusion, denial of service

.....  
22- The Norton Report (formerly the Norton Cybercrime Report) is one of the world's largest consumer Cybercrime studies, based on self-reported experiences of more than 13,000 adults across 24 countries, aimed at understanding how Cybercrime affects consumers, and how the adoption and evolution of new technologies impacts consumers' security.

attacks, data theft and online fraud. Botnets are used prolifically as a tool by organised criminal networks. A study called "The Link between Pirated Software and Cybersecurity Breaches" (see page 6) charts the alarming rise in new personal computers (PC) sold with pirated software infected with malware. The study estimates that enterprises will spend USD 127 billion in dealing with security issues as a result of malware associated with pirated software.

The organisation underlined the key to fighting the issue is education of the Public, regarding the real and serious dangers posed by using pirate software, including the risks to children when online. The Romanian Police currently works in Bucharest schools in order to spread interactive awareness campaigns via role play and themed talks.



The BSA has created an anti-piracy guide in cooperation with the Romanian authorities, the General Public Prosecutor's Office and General Directorate of Police so that every national law enforcement officer has sufficient knowledge to approach the matter.

### Infringing Content and Hosting Services – NetNames

NetNames offers services to aid the protection of brands online and domain name management. The company uses a range of technical tools and focuses on the activities of cybersquatters and abuse of brand names. They use their in-house analysts and knowledge of business to flag infringements and web pages offering counterfeits, and assist in their removal. The company sends cease and desist letters, which have a 91% compliance rate, and their main aim is to prevent damage to brands in terms of reputation and visibility – right holders do not necessarily approach the company in order to recoup money.

.....

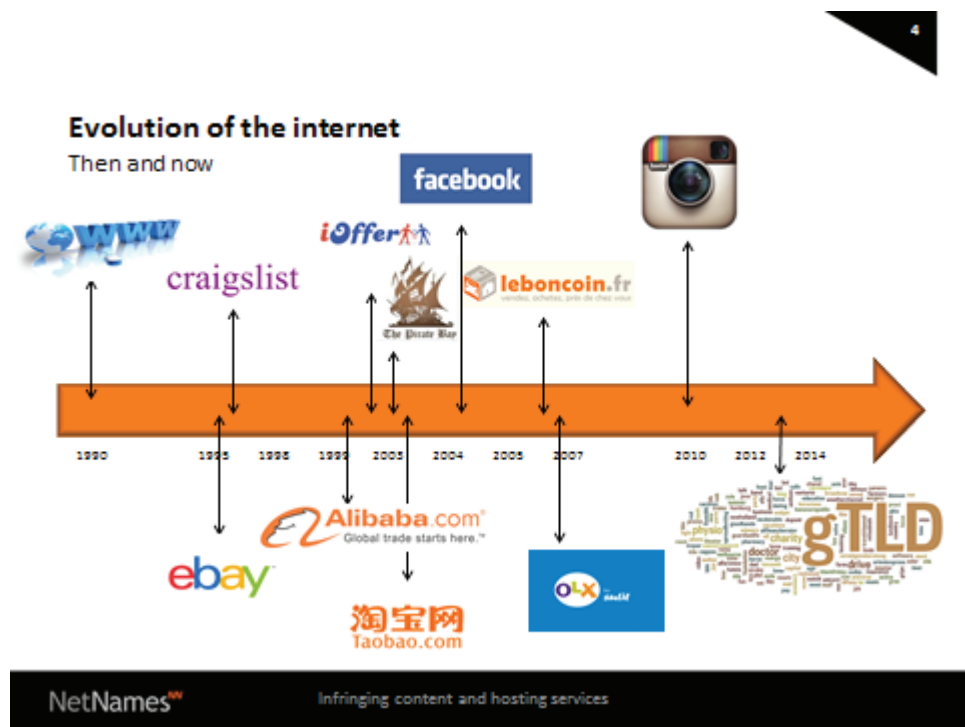
3- A cyberlocker is an Internet hosting site that allows users to upload files to the Internet for sharing and storing, and generally houses content which violates copyrights.

4- The study, called "The Link between Pirated Software and Cybersecurity Breaches", was carried out by the International Data Corporation (IDC) and National University of Singapore (NUS).

The company uses data collated to form links between serial offenders and organised crime by reviewing key words on a monthly basis regarding infringing sellers - to check whether they are still trading in the same products, and have simply changed their marketplace. *NetNames* offers an Anti-Counterfeiting Service, to rapidly detect and enforce against infringements across all online channels. Many online pharmacies use fake certification, logo abuse and non-secure payment services, leaving customers and brands at serious risk of harm.

The presentation underlined that teenagers experience peer pressure to access pirated content such as TV programmes which are not allowed within certain jurisdictions, using *BitTorrent*. Their studies suggest that there are 370 million users who explicitly search for infringing content.

They underlined the increasing occurrence of IP and other commercially sensitive information leaked onto websites, online forums and social networking sites, including *Twitter*, in addition to personal financial information.



Cybercriminals are one step ahead of changing technology. An important step in removing the visibility of online infringing products is to stop their ability to register websites and use web pages in the first instance, and it was concluded that more could and should be done on *ICANN*'s behalf in order to act proactively in relation to the 6000 new generic top level domains (gTLD).

## CONCLUSION

---

Presentations and feedback throughout the conference emphasised the expanding role of intermediaries – even if involuntarily – in the marketing, sale and transport of infringing goods sold via the Internet. These organisations include registries, search engines, advertising companies, payment platforms and payment service providers which facilitate the online presence, visibility, marketing and sale of infringing goods – and once sold, couriers and shippers of physical counterfeit products. The need for due diligence and voluntary collaboration throughout the supply chain proposed by the European Commission in its Action Plan 2015, was strongly supported at the conference. However, the practical and daily obstacles faced by intermediaries were highlighted in presentations by *DHL, eBay and Google*, including the sheer quantity of infringing web pages, evolving techniques used by cybercriminals, and the daily volume of small parcel counterfeit consignments.

The recurring message in presentations from the private sector was their aim to break the supply chain between infringers and the Public at an early stage, by reducing the visibility of counterfeiting on websites and on search engines. They called for cooperation on the behalf of *ICANN*, search engines and registrars in order to prevent the initial registration of such sites and their subsequent rankings.

All participants agreed that there is not only one solution. The Internet is constantly evolving, as are the methods used by infringers. Participants discussed the need to strengthen working cooperation between the private and public sectors across the globe, in order to establish a *soft law*. It was also agreed that intelligence and data about counterfeit goods, their producers and sellers should be shared more readily, in future – an opportunity that has been largely ignored, to date. The will to cooperate and establish strong interagency contacts and regular dialogue was expressed very audibly during the conference and networking sessions. Enforcement officers from ICE, Hong Kong Customs, the City of London Police and Prosecutors from across the Member States underlined their wish to work to a common end.

The demand for counterfeit and digitally pirated products remains. However, it was noted that the Public's knowledge of the dangers of such products is negligible. There is a need to increase awareness about the threat to personal security posed by Cybercrime, including the use of non-secure computers and pirated software. Recent focus has increased on the education of primary school aged children alongside teenager consumers, about the role of Intellectual Property in their lives; every day, young children are exposed to and consume downloaded and online content. It was stressed that educating the next generation on the realities of illegal goods and services, and the consequences of buying from those who produce and sell them, must be approached – and with care.

Today, there exists a complete shadow sector in suppliers for infringing websites – builders, bullet proof hosters, and bullet proof payment processors. The loss of revenue and jobs from the global economy to this shadow economy was highlighted in tangible figures during presentations. Discussions during the workshops concluded that a combined effort of civil and criminal legislative application, in addition to the use of best practice models would benefit Enforcement in the fight against online IP crime. However, it was repeatedly shown in case studies that the differences in legislation across the Member States presents many procedural obstacles when pursuing cross-border cases, and should be addressed by legislators.

The three day knowledge building event on infringements of Intellectual Property Rights on the Internet was a huge success, and this sentiment was expressed by all participants. The conference achieved its aims,

.....

3- A cyberlocker is an Internet hosting site that allows users to upload files to the Internet for sharing and storing, and generally houses content which violates copyrights.

4- The study, called "The Link between Pirated Software and Cybersecurity Breaches", was carried out by the International Data Corporation (IDC) and National University of Singapore (NUS).

perhaps the most urgent of which is to support the formation of new working relationships between the Judiciary, Enforcement and the public and private sectors. It was widely acknowledged that the criminal networks who act purely for financial gain, have established strong cooperation with each other. The remarks at the end of the conference underlined participants' wishes to match the scale of that working cooperation in order to proactively tackle future criminal activity online.

## ANNEX

---

### 1. Digital Piracy Workshop Co-Chaired by The Romanian Police and OHIM

- A presentation from The Audio Visual Anti-Piracy Protection Alliance (APPA) underlined the investigative problems regarding the obtention of convincing live digital evidence, the scale of economic impact, and identification of key suspects. Following hacking in the 1990s and card sharing in the recent past, pirated content is now redistributed through unlicensed means such as signal rebroadcasting. However, the necessary criminal procedural tools are available in the Council of Europe Cybercrime Convention, signed in Budapest in 2001, including production orders, freezing orders and data interception orders. The importance of following data collated through forensic investigation, in addition to "following the money" was stressed.
- INCOPRO presented on their methods to secure near real-time intelligence from domain name registries, app stores, social networks and search engines, as well as collating data about infringing websites, hosts, advertisers and payment providers.
- Site blocking via civil actions has proved to be highly effective in the disruption of access to infringing sites, especially in cases which involve a multitude of jurisdictions.
- 3D printing is set to challenge manufacturers of physical products in ways resonant of the challenge that was posed through the digital revolution of the Film and Music Industries.
- The question was posed - do we need new legislation? It was concluded that legislative amendments are needed in Third Countries including China. Instead, more focus should be placed on the prioritisation of Internet IP cases - providing quicker procedures, securing digital evidence and making sure that investigators, Prosecutors and Judges possess adequate knowledge of the problem, the technical challenges and the legislation available. There is also a need to heighten public awareness.
- More evidence is required regarding the impact of digital piracy on the economy and on lost jobs.

### 2. Digital Piracy Workshop Co-Chaired by The City of London Police and the Bulgarian Prosecution Service

- Enforcement activities to disrupt counterfeiter's possibilities to trade, by interrupting the money flow to websites was highlighted as a main aim. For this, international cooperation is needed. A global problem requires a global solution, and the flow of money moves around the world and across many countries.

- In the UK, best practice has seen the use of Civil and Criminal Law in tandem, by blocking ISPs, blocking access to websites, and by using the Confiscation of Proceeds of Crime Act. The use of civil blocking orders in the UK is becoming standard practice.
- Primary legislation has not developed as quickly as current technology.
- Police and Prosecutors need to exploit the tools available.
- Enforcement officers require specific and ongoing training regarding Internet crime.
- In Italy, counterfeiting laws are stronger than anti-piracy laws.
- In the Czech Republic, Cybercrime laws have been ratified.
- Partnerships between the public and private sector has been put into practice with support from the City of London Police, who collaborate with trade associations and right holders to identify "bad actors" and to gather evidence that can be used in criminal cases, using technology such as *whiteBULLET*.
- A discussion took place about the use of Industry experts seconded into Police forces, and Police analysts working with Copyright holders and other right holders in order to teach them about, for example, levels of evidence etc.
- The main obstacles to effective enforcement were discussed, including displacement – after action has been taken, the criminals may move to another country and use proxy servers etc., and bullet proof hosts and registrars, who act as "domainers"<sup>23</sup>. Additionally, insuring that investigators have correct and sufficient training and skill sets requires a large amount of resources.

### 3. Counterfeiting Workshop Co-Chaired by the Hungarian Prosecution Service and Europol

- The Alliance for Safe Online Pharmacies' (ASOP) presentation revealed the new, emerging threat of fake medicines sold online – globally, 97% of online drug seller sites are operating in violation of applicable laws. The source country is invariably India, and the products are distributed throughout the Eastern European Union. The websites created and used by the infringers are visually sophisticated in order to mislead consumers, offer wide ranges of medicines including fake heart, IVF and cancer drugs, without licences, and of which the contents are unknown.
- Online counterfeit drugs contain incorrect amounts of active ingredients and in some cases, poison.
- Problems lie in the apparent benefits in buying medicines online – no prescription is needed, and the goods can be ordered from home.
- Awareness raising campaigns are needed to educate consumers about the dangers of buying medicines online.
- Criminals do not care about the dangerous, and sometimes fatal consequences to consumers – they operate purely to make financial gain.

.....  
23- "Domainer" is a term used to describe an individual/ organisation who buys and sells domain names, with the purpose of generating profit either by selling the domain names at a higher price later in time or from advertising activities.

- A study carried out on the behalf of *Sanofi* in France, Germany, Italy, Spain and UK in 2014 found that, while a majority of consumers (66%) have heard of drug counterfeiting, respondents seemed to have little information on the issue of counterfeit medicines and 77% said they had not been adequately informed or are ignorant on the subject.
- In many cases, brand's biggest competitors are counterfeiters.
- From July 2015, each Member State must have a list of online licensed traders in pharmaceutical products .
- Work must be done to build relationships with current "safe haven" registries in order to monitor clearly infringing sites and registrants who abuse .
- Intelligence must be shared. Data is collected at European ports and borders regarding export and import of counterfeit products, but often, the opportunity to share this information amongst Enforcement is not exploited. This opportunity should be facilitated in future.
- Telemedicine, whereby consumers speak to a person who claims to be a doctor and drugs are prescribed via the Internet, poses large potential problems in future.
- It was agreed that intermediaries including advertising companies, postal services, and shipping companies should be engaged in voluntary efforts to stop the flow of money and goods.
- IP address providers including registrars should also be engaged - if sites cannot be registered, they will not appear in search engines results and their link to consumers is thwarted.
- Counterfeit affects cosmetic products on large scale - *L'Oréal* explained that their biggest competitors selling online are counterfeiters, with 80% of fake products originating from China. The company works in close cooperation with the Chinese authorities, in order to detect the source, and disrupt the production and trading chains. They also work to reduce the visibility of infringing sites using their visuals and trade marks illegally, in order to promote seemingly legal offers. *L'Oréal* has used civil actions against online infringers illegally selling under their trade names within Europe, with prolific presence on *eBay* and *Amazon*.
- Following test purchases of fake goods, the company pursues and implement preliminary injunctions, which prove effective in applying pressure on other infringers.
- Participants agreed that once detected, a rapid response is needed - unfortunately, current laws prevent some timely reactions, and the removal of a domain name is often an uphill battle.
- The widespread use of the Internet in trade and communication affords cybercriminals anonymity and flexibility, and adds distance between them and their crime.
- The role of social media in counterfeit activities is huge and increasing.

- The problem is a global one: counterfeit goods are imported and exported all over the world, which complicates and delays the collation of information and the establishment of cross-border cooperation. The perpetrators constantly adapt their *modus operandi* in the face of the efforts of national-based Enforcement.
- Participants called for a harmonisation of regulations in order to support Enforcement.
- In general, national enforcement is reactive, not proactive.
- Effective measures include the pursuit of domain names – visibility is very important for the perpetrators – and taking civil action against Internet service providers if they refuse to cooperate.
- The role of the Judiciary in mutual legal assistance was highlighted: judicial services can offer support in quickening the process by the application of effective tools, especially in the EU.
- The partnership between the private and public sector is of utmost importance – the private sector often detects IP infringement first hand and can provide valuable information to the authorities.

#### 4. Counterfeiting Workshop Co-Chaired by ICE-IPR Center and the International Public Prosecution Office, Stockholm

- Presentations from the private sector again highlighted that they consider strong cooperation by brands and the implementation of good practice models, the best way to tackle IP infringements .
- To set the scene – the production of Swiss watches in 2011 was approximately 30 million items. The estimated production of fake Swiss watches is approximately 40 million items per year.
- The Swiss Watch Federation revealed the huge scale of action carried out by brands themselves. The federation has an Internet group composed of 42 brand members whose main aim is to reduce the visibility of fakes on websites and on search engines. The federation acts as a single point of contact for consumers. They carry out Customs training regarding seizures and trends, use *Google* DMCA in order to remove search results, work alongside registrars and carry out test purchases on suspected counterfeits. Importantly, they aim to cut the link between the buyer and seller and have created a specific tool which collects data via *WHOIS* in order to locate the ISP address, country and other details of the infringing website in question.
- However, the reluctance of brands to feature an online form for consumers who have encountered counterfeiting underlines their wish to place distance between themselves and the fact that their goods are counterfeited.
- The private sector stated that if there are large numbers of counterfeit goods, a criminal case is effective.
- The private sector underlined role played by social media including *Facebook*, *Youtube*, *Instagram*, *Pinterest*, and *Photobucket* in selling counterfeit, using a direct link between seller and purchaser. *Youtube* has a content tool regarding copyright infringement, but it was questioned whether it is used against counterfeiting.

- The Swiss Watch Federation set up a “fake” website. It houses content in order to raise public awareness about fake watches and the risks of buying counterfeit for consumers – such as a lack of quality but also the risk of identity theft, when buying from rogue traders.
- The National IPR Center stated “We are not going to seize or arrest our way out of this problem”. They explained their focus on raising public awareness online, and the effective message of Homeland Security’s seizure banner which features on a banned website.
- They explained their work with Industry in order to feature their online form on partner sites including the National Football League (NFL). They noted original reluctance on behalf of brands to feature the form on their site regarding counterfeit, but this is progressively being overcome.
- It was found to be useful to close down payment facilities including VISA on infringing sites, because consumers are not so eager to use, for example, *Western Union* or hand over personal details.
- The private sector again highlighted the need for intelligence from logistics companies regarding senders’ details.
- All participants agreed that there is not only one solution. The Internet is constantly evolving, as are the methods used by criminals. Participants discussed the need to strengthen cooperation between private and public sector across the globe, in order to establish a *soft law*.
- Seized domain names must be paid for and maintained by the right holders who have pursued their seizure, otherwise they would be taken up and re-established by the counterfeiters. It was suggested that the seized sites are used to raise public awareness by placing an informative banner on them.
- The Belgian Cybersquad, (which sits under Belgian Customs) focuses on Internet fraud and IT forensics. They are a member of the CCWP (Customs Cooperation Working Party) established by the European Commission. They highlighted a large initial challenge of limited funding and resources.
- In Belgium, Customs are able to confiscate all means used for smuggling, including websites and cars: a counterfeit goods case is regarded as a smuggling case under Criminal Law.
- Under an administrative procedure, Belgium Customs work in cooperation with the registries, including *EURid*<sup>24</sup>, who check the registration of sites and have the power to close them down. Belgian Customs worked closely with the US during “Operation In our Sites” and Greece during “Operation ERMIS”, which focused on the detection of counterfeits in parcels.
- There was a call for common European pressure against logistics companies. Successful collaborative work has been carried out by Maltese and Belgian Customs with *DHL*.
- There is a need to increase awareness about the lack of security posed by Cybercrime, including the use of non-secure computers and pirated software.

.....  
24- EURid is the not-for-profit organisation that operates the .eu top-level domain, following a tender process and appointment by the European Commission.

- It was noted that the legal framework is not up to date with Cybercrime, and that legislators should be made aware of this.
- ICANN licences registries to sell levels of domain names. Participants called for regulations to be put in place regarding the dispensation of registries.
- Enforcement operations are generally reactive, not proactive.
- There is a delicate balance between privacy and the need to monitor criminals using technological means, such as wiretapping. It was noted that there is an emerging trend for criminals to talk on Skype, in order to avoid detection.
- International cooperation between Enforcement must improve, because serious and organised criminal networks have already established international cooperation. If the case involves cross-border action, it was suggested to work alongside the liaison team at Europol to contact counterparts in the country in question.
- The example of the Pharmaceutical Industry model was discussed, who provide a huge amount of intelligence to Enforcement in order to progress cases.
- *MarkMonitor* presented on the specific and urgent need to educate the younger generation about what is and is not permissible or legal on the Internet. They echoed the view of ICE, which is that catching counterfeiters will not result in the eradication of counterfeiting. International cooperation between Enforcement must improve, because serious and organised criminal networks have already established international cooperation. If the case involves cross-border action, it was suggested to work alongside the liaison team at Europol to contact counterparts in the country in question.
- They underlined the criminals' need for investment in the early stages, of setting up their sites - they need to pay their hosting providers. Advertising offers the finances which keep streamers and digital pirate solvent. The company advocated the efficacy of the "follow the money approach" in order to break the link at intermediary level via registrars and hosting providers.
- *MarkMonitor* allows a huge collection of data on trends and behaviour via automated data aggregation on a global scale. Their emergency response team is used by Sports Industry brands in order to take down thousands of infringing links to live streaming events within minutes.
- Business incomes are suffering huge damage due to illegal downloads of their software, and online videos showing ways in which to pirate their goods.
- Substantive law is generally harmonised across the Member States owing to the many conventions. However, procedural law is not harmonised, and from a Prosecutor's point of view this poses many issues. It was noted that in the US, it is possible for the Police to provoke a crime and subsequently prosecute (so called "sting" operations). This cannot be done within the EU.









OFFICE FOR HARMONIZATION  
IN THE INTERNAL MARKET  
(TRADE MARKS AND DESIGNS)



EUROPOL

# Infringements of Intellectual Property Rights on the Internet

5th, 6th and 7th November 2014

A conference co-chaired and hosted by the  
Office for Harmonization in the Internal Market (OHIM), Europol and Eurojust