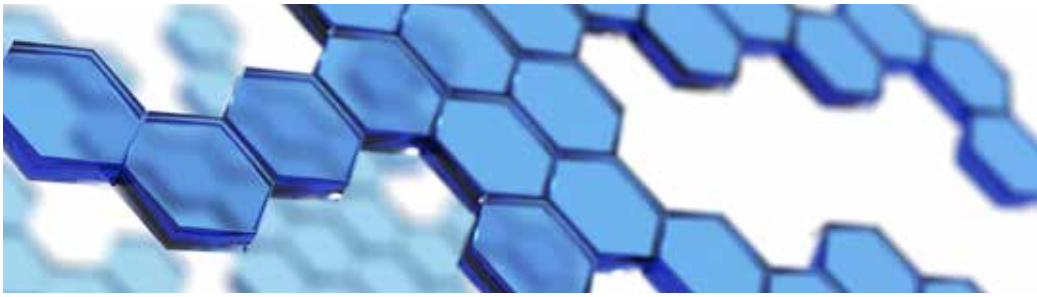
ROLES AND RESPONSIBILITIES OF INTERMEDIARIES:

FIGHTING COUNTERFEITING AND PIRACY IN THE SUPPLY CHAIN



ICC ADVOCACY

BASCAP

Business Action to Stop Counterfeiting and Piracy

MARCH 2015

ICC INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

BASCAP
Business Action to Stop Counterfeiting and Piracy

About the International Chamber of Commerce (ICC)

ICC is the world business organization, whose fundamental mission is to promote open trade and investment and help business meet the challenges and opportunities of an increasingly integrated world economy. With interests spanning every sector of private enterprise, ICC's global network comprises over 6 million companies, chambers of commerce and business associations in more than 130 countries. ICC members work through national committees in their countries to address business concerns and convey ICC views to their respective governments. ICC conveys international business views and priorities through active engagement with the United Nations, the World Trade Organization, the G20 and other intergovernmental forums.

To learn more about ICC visit: www.iccwbo.org

About BASCAP

Counterfeiting and piracy have become a global epidemic, leading to a significant drain on businesses and the global economy, jeopardizing investments in creativity and innovation, undermining recognized brands and creating consumer health and safety risks. In response, the ICC launched BASCAP to connect and mobilize businesses across industries, sectors and national borders in the fight against counterfeiting and piracy; to amplify the voice and views of business to governments, public and media; and to increase both awareness and understanding of counterfeiting and piracy activities and the associated economic and social harm.

Visit BASCAP on the web at: www.iccwbo.org/bascap

Acknowledgements

This discussion paper was developed with considerable input from several IP and subject matter experts who spent hundreds of hours researching, drafting and reviewing each section. In particular, BASCAP would like to thank Chris Oldknow of Elipe Global (www.elipe-global.com), Laura Sallstrom and Christopher Martin of Access Partnership (www.accesspartnership.com), Allen N. Dixon of IIPTC (International Intellectual Property and Technology Consulting), and Paul Rawlinson and his team at Baker & McKenzie (www.bakermckenzie.com).

Table of Contents

Preface

This body of work is a product of the ICC Initiative: Business Action to Stop Counterfeiting and Piracy (BASCAP). While it is written from the perspective of trademark and copyright owners—rather than that of intermediaries and the broader ICC membership—intermediaries of ICC's relevant policy commissions have contributed views and suggestions. The final product is based on the premise that IP should be protected in international commerce and throughout the supply chain. The singular objective is to eliminate vulnerabilities in the supply chain that enable the infiltration of counterfeit goods and copyright piracy.

Millions of intermediaries are operating throughout the global supply chain and the vast majority of these players are conscientious, trustworthy and reliable partners. ICC's own membership includes millions of companies: many are brand and copyright owners; many are intermediaries; and others have no direct interest or link to the topics covered in this paper. So while this paper does not and cannot reflect the views of all ICC members, nor is it a consensus of the global business community, it has undertaken to ensure accuracy, balance and consistency with ICC's long-standing opposition to counterfeiting and piracy, intellectual property rights infringement, unfair trade, illegal commerce and corruption.

For the most part, this body of work substantiates actions intermediaries are already taking independently or in collaboration with rights holders and government authorities to deal with supply chain vulnerabilities. Where these current efforts have been inadequate in protecting against IP infringements, suggestions for better or best practices are put forward. The result is a product that challenges the status quo and offers a roadmap for discussion, collaboration and resolution.

We offer the findings and suggested best practices as a springboard for an ongoing dialog among trademark and copyright owners, intermediaries and governments to find solutions to the infiltration of counterfeiting and piracy into the legitimate supply chain. Our hope is that the suggested best practices will help responsible intermediaries more effectively deal with vulnerabilities in their operations and encourage intermediaries who knowingly facilitate IP infringement to stop.

We welcome feedback and comments on this and other BASCAP activities. Please visit us at: www.iccwbo.org/bascap

Introduction

Trends toward IP infringement in the supply chain

Counterfeiting and piracy impact virtually every product and service category. The days are long past when counterfeiters sold only fake luxury goods or unauthorized CDs and DVDs. Today, counterfeiters are producing fake foods and beverages, pharmaceuticals, electronics, auto parts and everyday household products. At the same time, copyright pirates have created multi-million dollar networks to produce, transport and distribute unauthorized copies of music, video and software.

This problem has grown hand-in-hand with globalization of the economy, and counterfeits account for a growing proportion of international trade. The Organization for Economic Cooperation and Development (OECD) estimated in 2008 that more than $250 billion in physical counterfeit goods move across borders each year, not including in-country activities, Internet infringement, and indirect economic activity and costs. Together, the estimated global impact of these activities could add up to a staggering $1.7 trillion annually by 2015.[1]

Along with trade liberalization, the growth of sophisticated logistics networks and information sharing through data networks and the Internet has dramatically increased the volume of products and information moving around the world.[2] The number of supply chain intermediaries has multiplied accordingly.[3] Consequently, intermediary businesses are playing an increasingly critical role in providing services within the supply chain, ultimately connecting producers and consumers.

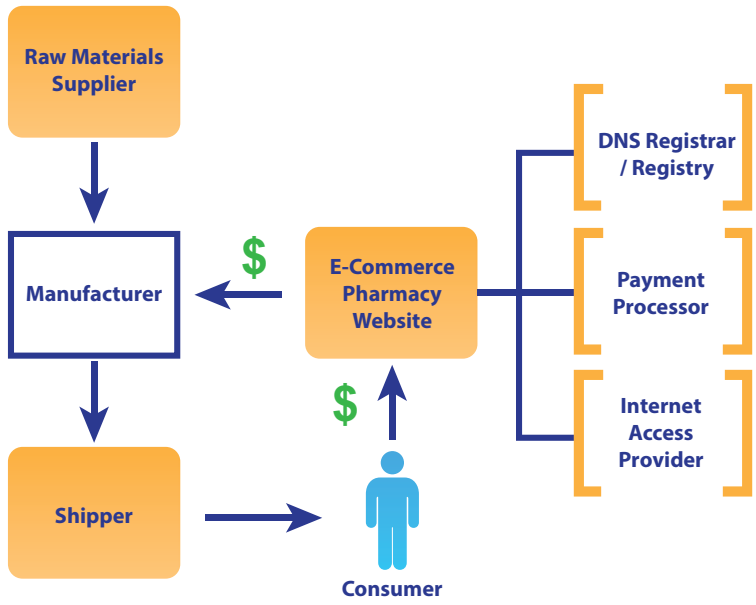
These trends have also created significant challenges for rights holders in detecting, investigating and stopping the flow of counterfeited and pirated materials. In particular, it is much more difficult for rights holders to know, manage, and control every intermediary involved in their supply chains and to see their every transaction. Intermediaries face similar challenges with their sub-intermediaries, suppliers and customers. This situation has exposed a number of supply chain vulnerabilities, and criminal agents have seized the opportunity to exploit them. Individual criminals—and increasingly, organized crime networks—are introducing counterfeit elements through "intermediaries" who are involved in producing, distributing and selling a product, from raw materials through end-of-life disposal.

The Internet has provided a platform for new business models and new revenue sources for genuine goods and services. The Internet has been particularly vulnerable, however, to counterfeiters and other criminals capitalizing on the success (and intellectual property) of legitimate businesses while remaining anonymous and avoiding detection. The growth of Internet banking and online payment services has also become vulnerable to misuse by counterfeiters.

The purchase cycle and delivery of a *counterfeit* pharmaceutical succinctly illustrates ways in which multiple intermediaries can be involved in the purchase, manufacture, and distribution of counterfeit product.

- A consumer purchases a medicine on a website. A payment provider usually facilitates this transaction via credit card, working with one or more merchant banks to deliver payment to the website operator. The website owner may or may not know whether s/he is trading in counterfeit products. Similarly, if the site hosts advertising, the advertiser, ad agency or ad placement service may or may not know that they are financially supporting the distribution of counterfeits.
- The consumer makes the Internet purchase through an access provider on a website hosted by a hosting provider using a domain name provided and supported by an online registrar and/or registry.
- The purchase order goes to the manufacturer, who may be the prime counterfeiter or a legitimate drug manufacturer who has inadvertently procured the counterfeit from a raw material supplier and used it in the drug.
- The manufacturer produces the counterfeit drug and then sends it through one or more shippers who transport it directly to the consumer.

Intermediaries involved in purchase, manufacture, and delivery of a counterfeit



- The consumer takes the drug and realizes reduced or no benefit, while risking potential harm from ingesting the fake ingredients.

In this example, six or more intermediaries could potentially be involved in introducing counterfeiting or piracy into the supply chain. The inherent vulnerabilities of intermediary channels to counterfeits and piracy require action on the part of all parties involved. Intermediaries can be involved—knowingly and unknowingly—to varying degrees and at differing points in the supply chain of every product sector, from electronic components to e-commerce.

Efforts by governments, enforcement agents and intellectual property (IP) rights holders to stop counterfeiting and piracy have traditionally focused on the following interventions:

- stopping fakes at the source of production;
- intercepting them where they cross borders; or
- seizing them at point of sale.

Given counterfeiters' increasing sophistication, however, in penetrating and exploiting every step of the supply chain, governments and IP rights holders must focus on ways to limit (if not stop) infringements at multiple intermediary stages of the supply chain.

Potential partners at these intermediary stages include landlords, ISPs and operators of Internet trade platforms, shippers, financiers and suppliers of raw materials, and many others. Most act responsibly and do not want to be involved in violating their business partners' rights, but the need is increasing to ensure they recognize the consequences of this illegal trade. All businesses, including intermediaries have a corporate and social responsibility to fight counterfeiting and piracy.

Purpose

This body of work is intended to accomplish the following:

- To identify some of the intermediaries involved in a typical supply chain;
- To show how criminals can infiltrate the supply chain and infringe on IP rights through these intermediary channels;
- To document the steps being taken to prevent this infiltration; and
- To suggest further steps to curb the abuse of intermediaries by criminal agents to facilitate the sale of fake goods.

The first step is to explore supply chain vulnerabilities. This discussion paper will also show how criminal networks and other infringers routinely use and abuse intermediary services to facilitate global trade in illicit/illegitimate merchandise and digital products. This awareness is critical for 1) helping responsible intermediaries deal more effectively with operational vulnerabilities; and 2) curbing the activities of intermediaries who knowingly propagate and/or permit IP infringement through their services.

Experience shows that most intermediaries demonstrate a willingness to secure their portion of the supply chain when they are better informed about potential abuses and their negative impact on society. For example:

- Most landlords do not knowingly allow illegal drugs to be sold from their premises.
- Internet service providers (ISPs) have taken positive steps to block and take down child pornography sites.
- Shippers do not knowingly do business with criminals involved in human trafficking.
- Credit card companies have taken action to block payments for illicit commerce (e.g. narcotics, gambling).

Likewise, most intermediaries are willing to cooperate with rights holders and law enforcement, both independently and with industry associations. This paper examines many, but not all, of the critical types of intermediaries that are vulnerable to IP infringement. It analyzes steps taken to reduce this vulnerability and recommends best practices to curb IP infringements in the supply chain. In summary, this paper aims to:

1. **Raises awareness of intermediaries' vulnerabilities** to criminal networks and other infringers who exploit them to facilitate the global trade in counterfeit merchandise.
2. **Identify current approaches** to the problem through voluntary efforts by intermediaries, enlisting them to engage both independently and with rights holders and authorities to discourage counterfeiting and piracy.
3. **Identify alternative solutions** for intermediaries to consider.
4. **Assess whether these programs are working** to deter the infiltration of counterfeit and pirated goods within these intermediary networks.
5. **Suggest best practices and measures** for intermediaries working with rights holders and governments to more effectively address the global counterfeiting and piracy problem. The recommendations are intended to drive discussion, collaboration and resolution. They represent a springboard for taking a broader range of measures, as needed, to mitigate the infiltration of counterfeiting and piracy into the legitimate services of intermediaries in the supply chain.

Organization

Intermediaries in the physical world

Intermediaries are vital to commercial activity, including supplying ingredients and raw materials, distributing products, and providing retail space to conduct sales. Part One looks at three categories of intermediaries operating in the physical world that are particularly susceptible to counterfeiting and piracy:

1. **Raw materials and component suppliers** are a complex network of first-stage intermediaries. These intermediaries provide multiple opportunities for counterfeit ingredients, parts and components to enter the supply chain of otherwise legitimate products. Examples include tainted or poor-quality chemicals used in manufacturing pharmaceuticals, agrochemicals and consumer goods. Poor-quality counterfeit electrical components, software and metals can find their way into autos, airplanes, appliances and computers.

2. **Transport operators** are a critical part of the counterfeiting supply chain. Counterfeit goods depend on land, air and sea shipping and transportation services to cross borders and reach foreign markets. These intermediaries are critical players in stopping the flow of fake goods. Given that the shipping process requires documentation, the paper trail can help identify the originators and owners of the counterfeit goods.

3. **Landlords** play a role in counterfeiting and piracy when they provide a place to manufacture, store and sell illicit products. Landlords may knowingly or unknowingly rent the space needed for one or more of these activities. As landlords are typically not involved in inspecting goods on their premises, they allow this activity to continue unchecked until they receive notice from rights holders or raids from law enforcement.

Intermediaries in the online world

A complex, inter-connected intermediary network is involved in delivering to consumers a seamless range of online services. There are many examples of positive steps and initiatives taken by legitimate providers in these digital supply chains. The scale and nature of the challenges, however, suggest that these providers have to continually improve their defenses to prevent their operations from being hijacked to support illegal activity.

Part Two groups online intermediary activity into three categories. In some cases, however, a single commercial entity may be providing more than one of these services.

1. **Sites, platforms and portals.** This category includes a wide group of services that act as platforms for users to make offers and sales or share content or links. It includes e-marketplaces, mobile app stores, user-generated content sites, social networks and cyberlockers. This group also includes websites that connect peer-to-peer (P2P) network users. Some of these are the biggest names and most popular services on the web, used legitimately many millions of times daily. These services are also vulnerable to massive abuse through counterfeiting and piracy and have to continually improve their systems to stop such abuse. Other services are simply dedicated to piracy and counterfeiting and encourage users to fill their sites with infringing content.

2. **Infrastructure providers.** These services are the technical backbone of the Internet upon which all web services are built and delivered. Three main services are covered in this category. Hosting providers offer the server space to store either a whole website or simply some specific content, which is then displayed on other sites. Domain registries provide names for websites and connect them to the IP address of the hosted site. Internet access providers that connect users to the Internet are the final crucial link, as all data must pass through their systems to reach end users and consumers.

3. **Search, online advertisers and payment processors.** The economic viability of the broad range of services running on the internet depends on these support services to find an audience and generate revenue. This section focuses on search as the critical function that enables discovery within the network across all of these sites; advertising both as a means of discovery and as a source of payment; and direct payment, using credit cards and other payment services.

Key principles found in intermediary-related laws

Guiding principles

Across the sectors considered in this paper, intermediaries are getting involved and taking voluntary steps, to different degrees, to prevent entities engaged in piracy and counterfeiting from using their services. Clearly, a great deal more can and must be done to rally these efforts into a comprehensive, collective response. As in all areas of governance, if businesses' fail to correct market breakdowns or to guard against illicit commerce, governments are obligated to clarify their expectations and when necessary, introduce legislation to help deliver tangible results that voluntary arrangements may not be delivering.

Three key principles govern the balance between voluntary actions and regulated solutions:

1. **Responsibility and accountability.** Addressing the problems of counterfeiting and piracy in the supply chain requires a clear definition of each party's responsibilities. A responsibility to take action does not always rely on liability for infringement. Injunctions may still require a party to take action to end the infringing activity of another.

2. **Complicit behavior.** Responsibility and accountability are usually associated with the level of complicity—the degree of knowledge and involvement—in whatever illicit action takes place. Generally, the law condemns parties who have actual or constructive knowledge of infringement and have some sort of causal or participatory role.

3. **Conditions for "safe harbor" immunity.** "Safe harbor" from liability for infringements varies among jurisdictions. It typically requires intermediaries to meet certain technical requirements concerning their involvement in the infringement; to have and implement clear user policies that prohibit illegal activity; and to act upon notices of illegal activity. The issues of knowledge and control may also be relevant in some jurisdictions. Intermediaries that fail to meet these conditions can fall outside the "safe harbor."

Responsibility and accountability

A key point in addressing counterfeiting and piracy surrounds the question of what degree of responsibility lies with each party.

Legal framework and case law help define responsibility and accountability by delineating parties' expectations for taking action against infringement. Delineating expectations, however, does not always equate to direct or indirect liability, where an intermediary is in a position to end another's infringing activity.

For example, the legal basis for liability could depend upon whether an intermediary service is designed or operated with the clear intention of inducing or promoting IP infringement; or liability could depend upon whether the intermediary service unknowingly facilitates or enables infringement and/or, once aware, whether it takes reasonable steps to prevent it.

Most countries around the world provide a legal basis for liability in these situations, though the approach varies from one country to another.

In US law, for example, an Internet site or service can be liable on the basis of contributory or vicarious liability; or following the US Supreme Court in a 9-0 unanimous decision in *Grokster*[4], the site/service could be liable on the basis that it has been designed or operated with the clear intention of inducing or promoting infringement. There are limits to each of these concepts, of course. For example in *Perfect 10 v. Amazon*[5], the court found that the "inducement" test from Grokster was not met where a search engine was not promoted for its infringing uses. The recent American Bar Association (ABA) report explores the variety of US cases in more detail.[6]

In the UK, Australia and Singapore, liability can be found based on the concept of authorization, which is included within the copyright law. For example, the P2P service Kazaa was held liable in Australia on the basis of authorization liability (see further discussion of this example below). A UK court found that The Pirate Bay was authorizing copyright infringements in the UK (*Dramatico Entertainment Ltd v. British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch), High Court of Justice, 20 February 2012). Subsequent cases in the UK have also found that sites and their users were directly liable for unauthorized communication to the public, given the way they operated.

Canada has recently enacted a provision that finds liability for a service that enables infringements; in some countries in Europe (for example France, Germany and the Netherlands), liability is based on general principles of civil law. Liability under tort law principles also exists, for example in Brazil and Taiwan. In Brazil, the operators of a file-sharing service called K-Lite Nitro were ordered to implement a filtering mechanism to prevent the download of music files and/or phonograms.

Complicit behavior

No uniform solution or approach exists to finding liability; however, as briefly outlined above, the courts in different jurisdictions (both in civil law and in common law countries) have found intermediaries secondarily liable under a variety of theories. Although different jurisdictions have developed their own concepts of secondary liability, the case law shares certain common features. Generally, the law condemns parties who have actual or constructive knowledge of infringement and play some sort of causal or participatory role. Key factors that the courts consider, in addition to knowledge, are: 1) failure to exercise control or take steps to prevent continuing infringement; 2) the receipt of revenues derived specifically from the infringing activity; and 3) specific steps taken to promote or encourage infringement.

In other words, the level of responsibility and accountability is usually associated with the degree of complicity in whatever illicit action takes place. The level of complicity also is generally associated with the intermediary's degree of knowledge and involvement in the activity. The exact contours of this knowledge—whether general or specific—are the subject of many cases in several jurisdictions.

The foundation for much of the cooperative activity between rights holders and intermediaries can be found in the national laws which provide ways of determining whether an intermediary or third party has sufficient knowledge and involvement in a criminal offence or civil wrongdoing to be held liable. For example, a taxi driver who transports a bank robber and his loot, but has no knowledge of what his passenger has done or what is in the bag he carries, is unlikely to be found "aiding and abetting" such a crime. A getaway car driver, however, who has been involved in planning a robbery and keeps his motor running outside the bank when the robbery is taking place, can be held just as liable as those gathering the money at gunpoint inside the bank.[7]

Intermediaries who supply, carry or distribute material for those engaged in counterfeiting and piracy are similarly scrutinized. They may be found liable for their complicity in the illegal activity, whether through knowledge and approval, soliciting, encouraging, controlling, directly benefitting from, or otherwise participating in such activities. In some well-known cases in a number of countries, courts have determined that intermediaries have "crossed the line" in helping counterfeiters and pirates in ways that made the intermediaries themselves also liable. On the other hand, in many other well-known cases, courts have found that intermediaries have not crossed this line. Many of these cases relate to the conditions described in the section below on safe harbors from liability, although these two areas are not always aligned.

In the Australian Kazaa case, a P2P file-sharing service was found liable under the Common law test for imputing civil copyright liability. The service was noted for "authorizing" its users' infringements as it furnished the facilities, had knowledge of and encouraged infringements, had a system the predominant use of which was for infringement, and had

a financial interest to maximize infringement.[8] Similar cases have found that intermediaries can be held liable for trademark infringement to the extent they have knowledge of, control over, and other involvement in activities concerning counterfeits.

On the other hand, in the iiNet case in Australia, the High Court was not willing to impute responsibility to an ISP for the infringing actions of its customers. This court ruled that the ISP was not liable for authorizing the copyright infringement of its users "merely because" it provided the facilities for making such infringement possible. The court found that the ISP lacked the direct technical power to prevent its customers from committing such infringing activities. In its decision, the Court signaled the need for legislative change, stating that the concept of authorization is not well suited to enforcing the rights of copyright owners with respect to widespread infringements via P2P. In the EU, ISPs like iiNet are nevertheless subject to injunctions to bring an infringing activity to an end, for example, by means of site blocking in *UPC Telekabel Wien v. Constantin and Wega.*[9]

US courts have recognized that payment processors may occasionally cross the line from being unwitting providers of services to being complicit in counterfeiters' activities. In *Perfect 10 v. Visa Int'l Serv. Assoc.*[10], the court recognized that in the ordinary course of events, "infringement occurs without any involvement of Defendants and their payment systems" absent extenuating circumstances, and ruled in favor of Visa. In *Gucci America, Inc. v. Frontline Processing Corp.*[11], the court found, however, that intermediaries could be liable for (contributory) trademark infringement under a number of circumstances:

- if a payment processor or other intermediary knows that a customer trades in counterfeit products or is willfully blind to that fact;
- had specific, advance knowledge that they would be providing their services to support the sale of exclusively counterfeit products;
- provided material assistance in making "high-risk" clients effective at selling unlawful goods;
- had viewed the goods sold by the merchants and had seen that the merchants had openly disclosed that they sold products that were "not genuine" and "not authentic."

Similarly, in *Tiffany (NJ) Inc. v. eBay Inc.*[12], the court found that generalized knowledge that trademark infringement was occurring was not sufficient for action, but willfull blindness could be a cause for action. In *Chloe SAS v. Sawabeth Info Svcs. Co.*[13], the court found that the web platform TradeKey fell on the wrong side of the line in its complicity with the transactions occurring on its site.

The notification by rights holders to intermediaries can also play an important role in determining the extent of knowledge and liability. In *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*[14], trademark and copyright infringement was occurring on websites hosted by the ISP. The Louis Vuitton company had sent the ISP some 18 notices documenting these infringements and requested that the ISP either remove the infringing content from their servers or require their customers to remove it. Louis Vuitton received no response from the Defendants. The court found that the service provider's control and knowledge of the infringing websites—evidenced by its failure to respond to the infringement notices—could implicate the service provider itself for "contributory" copyright and trademark infringement. At trial, the jury found the hosting ISP liable and awarded Louis Vuitton $10.8 million in damages.

In the Philippines, recent amendments to the Intellectual Property Code make it possible to hold an intermediary itself liable for copyright infringement on the basis that it benefitted from another party's infringement. The law provides that a person is liable for copyright infringement when one "benefits from the infringing activity of another person who commits an infringement if the person benefiting has been given notice of the infringing activity and has the right and ability to control the activities of the other person"[15] or "with knowledge of infringing activity, induces, causes or materially contributes to the infringing conduct of another."[16]

Conditions for "safe harbor" immunity

Over the last several years, rules have evolved especially for Internet-related intermediaries. Various types of Internet service providers have been granted "safe harbor" protection from liability for monetary damages only for infringements in which their customers may be engaged. In most cases, "safe harbor" is granted under carefully defined conditions that typically require the intermediary to meet certain technical requirements:

- to establish and implement clear user policies that prohibit illegal activity;
- to act upon notices of illegal activity; and
- to be subject to injunctions even where damages awards are not appropriate.

In such cases where Internet service providers fail to act, they can fall outside "safe harbor" conditions. Additionally, "safe harbor" may be jeopardized if providers fail to act when they become aware of infringement in a manner other than receiving a notice, or they become aware of facts and circumstances indicating infringement. The EU E-commerce Directive requires that the service provider has to act "expeditiously" upon obtaining knowledge of infringement to make sure that the infringing content is removed or access to it is disabled. Possible actions for injunctive relief still remain available in the EU, and in the US, Singapore, Australia New Zealand and Taiwan. The above rules reflect the importance of balancing the free flow of legitimate electronic commerce with the need for intermediaries to take reasonable action against illegal activities when they arise.

Internet access and transmission services benefit from "safe harbors" that preclude liability for monetary damage awards, so long as their activities stay within the basic "mere conduit" functions and meet certain pre-conditions, such as having and implementing responsible terms of use with their customers. Again, these intermediaries must recognize the role they can play in avoiding illegal activity. Irrespective of a liability finding, these intermediaries remain subject to court subpoenas, law enforcement requests, injunctions and other court orders. Such legal actions can require them to disclose account details and other information, block access, or otherwise cooperate in the investigation of and remedies against parties engaged in illegal activity.

Legal precedents and regulation

In the absence of effective voluntary programs by intermediaries and rights holders to deter counterfeiting and piracy, national courts have established legal precedents and judgments that clarify and uphold the principles of responsibility. These precedents define the rules of engagement should voluntary efforts prove ineffective. For example:

- *Europe* - In a ruling in interim proceedings against China Shipping, the Summary Judge of the Rotterdam District confirmed that article 6 and 11 of regulation 1383/2003 does not give the carrier the right to claim payment by the rights holder of the demurrage costs.[17] The judge ruled that the principal of China Shipping would ultimately have to pay the demurrage costs. This case supports the argument that the carrier—and not the rights holder—should seek recompense from the consignee and/or the assignor for the demurrage costs.
- *Brazil* - In April 2011, the Brazilian Superior Court of Justice found the 25 de Março Shopping Mall in Sao Paulo liable for reselling counterfeit products. It imposed a daily penalty of R$50,000 (about US$30,000) if the Mall did not stop marketing and selling counterfeit items from Nike, Louis Vuitton, and Oakley, who had sued for damages. The Court ordered the payment of moral damages to these companies.
- *China* - In July 2011, the Beijing Higher People's Court issued decisions that clarified the duty of care for the Silk Street Market and other landlords. It affirmed the 2010 rulings of the lower courts, which had specified the landlord's duty to take reasonable measures in dealing with infringers. It also found that failure to do so could make the landlord jointly liable. The rulings appear to have raised the duty of care for Chinese landlords and required the landlords to take "positive measures" against specific vendors to stop the infringement(s). The rulings also required landlords to avoid repeat infringement(s), provided that the brand owners have duly notified the landlord that the same vendors are selling the counterfeit products.

  Building on the Chinese examples of the Silk Street Market case and the online Taobao marketplace, a recent legal analysis by Wang Zhuo, a judge with the IP Division of the Beijing No. 1 Intermediate People's Court, observed that "in considering the legal liabilities of those providing space for sales to customers, such as the Silkstreet, which leases counters to merchants for selling goods, and Taobao.com, which provides information storage space for merchants for selling goods, the court usually adopts the same standard. When judging whether or not those providing space for sellers meet their performance of duty of care, courts inquire into whether they know of the infringements in market, regardless of virtual or real market, and still take no active measures to stop such infringements."[18]
- *United States* - In *Gucci America, Inc. v. MyReplicaHandbag.com*,[19] following a default judgment in favor of Gucci, Chloé and Alfred Dunhill against defendants claimed to be distributing counterfeit handbags and wallets. The court ordered third-party financial institutions to liquidate all of the assets they held for the defendants, and to give those assets to the claimants. Over $500,000 was recovered.
- In *Gucci America, Inc., et al. v. Curveal Fashion*,[20] the magistrate ordered the New York office of the United Overseas Bank to produce relevant account documents after obtaining information showing [the defendant's] transfer of $900,000 into accounts at UOB Malaysia. UOB refused to comply with the subpoena, and the district court held UOB in contempt of court, awarded Plaintiffs attorneys' fees, and imposed a fine of $10,000 per day for each future day of noncompliance. The two parties settled the case with a $250,000 payment from UOB.[21]

- Also in the US, in *Coach Inc. et al v. Celco Customs Services Co. and Shen Huei Feng Wang*, a jury found a customs broker liable for $8 million for contributory trademark infringement as a result of failing to complete due diligence checks on their customer, despite discrepancies in paperwork resulting from identity theft.[22]

Sector-specific laws and regulations also spell out obligations of intermediaries as responsible actors in fighting IP infringement, counterfeiting and piracy. The U.S. Defense sector is a prominent example of how new regulations can impact intermediaries, primarily in this case with raw material suppliers. In the US, the 2012 National Defense Authorization Act (NDAA) created regulations for counterfeit part detection and avoidance, including the following provisions:

- Contractors are now responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit parts;
- Contractors are also responsible for any rework or corrective action that may be required to remedy the use or inclusion of such parts;
- Contractors must establish qualification procedures and processes to use trusted suppliers and procure electronics from authorized suppliers.[23]

Furthermore, general US Code has several specific criminal proscriptions:

- 18 U.S.C. § 2320 provides for up to 20 years in prison for anyone who intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark.
- 18 U.S.C. § 2318 provides additional penalties for anyone who "knowingly traffics in a counterfeit label affixed…or designed to be affixed to a list of product types that are commonly sold as counterfeits."
- 19 U.S.C. § 1526 authorizes fines against anyone responsible for importing merchandise that is seized under the Tariff Act.

These and other international laws and court rulings serve important roles in ensuring that all parties involved clearly understand their rights and responsibilities.

Part I: Physical Intermediaries

Intermediaries are vital to commercial activity, including supplying materials for input, distributing products, and providing retail space to conduct sales. Unfortunately, these service providers also can be vulnerable to abuse and infiltration by criminal agents. They may unknowingly (and, in some cases, knowingly) aid the illicit practices of counterfeiting and piracy. Counterfeiters are increasingly exploiting many of the same intermediaries that are used for legitimate trade, such as transport operators, shipping companies, raw material suppliers and distributors. Such exploitations are resulting in the placement of fake and illicit products alongside authentic products in stores, markets and on the Internet. This section looks at three categories of intermediaries operating in the physical world that are particularly susceptible to counterfeiting and piracy:

1. **Raw materials and component suppliers** are a complex network of first-stage intermediaries that provide multiple opportunities for counterfeit ingredients, parts and components to enter the supply chain of otherwise legitimate products. Examples include tainted or poor-quality chemicals used in manufacturing pharmaceuticals, agrochemicals and consumer goods. Poor-quality counterfeit electrical components, software and metals can find their way into autos, airplanes, appliances and computers.

2. **Transport operators** provide critical services that are subject to abuse as part of the counterfeiting supply chain. Counterfeit goods depend on land, air and sea shipping and transportation services to cross borders and reach foreign markets. These intermediaries are critical players, together with customs authorities and rights holders, in stopping the flow of fake goods. Given that the shipping process requires documentation, a paper trail can help identify the originators and owners of the counterfeit goods.

3. **Landlords** play a role in counterfeiting and piracy when they provide a place to manufacture, store and sell illicit products. Landlords may knowingly or unknowingly rent the space needed for one or more of these activities. As landlords are typically not involved in inspecting goods on their premises, much of this activity goes unchecked until they receive notice from rights holders or raids from law enforcement.

The following chapters address each of the intermediaries listed above. Each chapter describes the intermediary, explores vulnerabilities to IP infringing activities, assesses current solutions and presents suggested best practices in light of exemplary voluntary programs already in place.

1. Raw materials and component suppliers

In most product supply chains, raw materials, ingredients, and components suppliers are typically the "first intermediaries." Multiple intermediaries may contribute inputs or services toward a final product's manufacture.

Such a complex network of suppliers creates multiple opportunities for counterfeiters to integrate fake inputs into the supply chain or mask the true origin of a production input. For example, products shipped in bulk may not carry overt branding or trademark identification. Without these minimum safeguards, counterfeit materials can more easily evade standard enforcement measures. For instance, at retail points or seizure at the border, enforcement mechanisms rely on trademarks or more obvious packaging discrepancies.

While all counterfeits have destructive effects, the infiltration of fake input materials can present especially severe consequences, with little risk of detection. In pharmaceuticals, for example, fake or sub-standard ingredients in what were thought to be authentic medicines have led to illness and death. In the aviation industry, fake components have been linked to airline disasters. Such consequences, coupled with the challenges of detection, create extra pressure to secure one of the most important parts of the supply chain from counterfeits.

This chapter describes the vulnerabilities to infiltration of counterfeits from raw material, component, and ingredient suppliers in the aviation, pharmaceutical, electronics and tobacco products sectors. The discussion investigates current approaches to the problem, evaluates their effectiveness, and presents suggested best practices for further action.

1.1 Vulnerabilities to counterfeits from raw material, component, and ingredient suppliers

Vulnerabilities in commercial aviation

In 1989, counterfeit airplane parts were responsible for the fatal crash of Partnair Flight 394 over Denmark. The crash resulted in the death of all 50 passengers and five crew members. An investigation found that three of the four bolt-pins holding the airplane's tail to the fuselage were counterfeits—of insufficient strength to withstand the vibrations that tore the plane's tail from its hull in mid-flight.

The Partnair tragedy spurred worldwide awareness of the problem of counterfeit airline parts. A United States audit at that time found that 39% of spare parts in the US Federal Aviation Administration's (FAA) inventories were suspected of being counterfeit. Further FAA investigations found a thriving black market for reselling old and inferior parts as new, with an associated market for falsified FAA inspector signatures. Parts were sold through supplier intermediaries, with channels running from distributors to manufacturers and to airline and third-party repair stations.

While the Partnair tragedy served as an inflection point in addressing the issue, the illicit network for fake aviation parts continues. In 2007, Russian police intercepted and arrested a criminal group for illegally stealing and then reproducing commercial aircraft parts and accompanying documentation for sale in Russia and other countries.[24] Counterfeit airplane parts have become a problem with military aeronautics as well. This issue was recently highlighted in a decision by the Canadian Air Force in February 2013 to continue flying its CC-130J Hercules, despite allegations of counterfeit parts.[25]

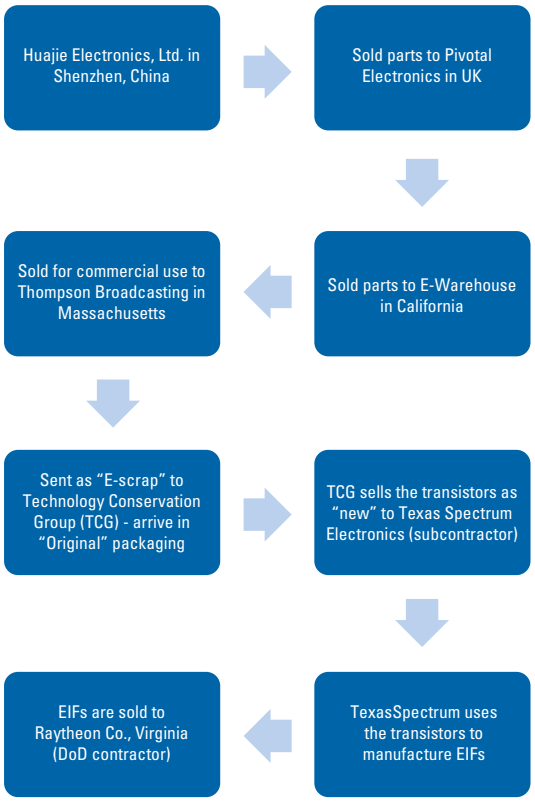
Vulnerabilities in electronics

Given the multiple and widely outsourced secondary components in consumer and industrial electronics, considerable vulnerability exists to counterfeit component infiltration. Counterfeit electronic components can make their way into all manner of products, including computers, mobile phones, printers, automobiles, defence systems, airplanes, and robotics. Counterfeit electronic components ended up in a record $169 billion worth of semiconductors in 2011, and incidents of counterfeit parts have tripled during the past two years.[26]

A 2012 US Senate inquiry detailed the first portion of the counterfeiting process, stating:

"Much of the raw material counterfeit electronic parts is salvaged electronic waste (e-waste) shipped from the US and the rest of the world to Hong Kong. From Hong Kong, waste is trucked to cities in mainland China, such as the counterfeiting district of Shantou in Guangdong Province, where electronic parts may be burned off of old circuit boards, washed in the river, and dried on city sidewalks. Once washed and sorted, parts may be sanded down to remove the existing part number, date code and other identifying marks. In a process known as "black topping," the tops of the parts may be recoated to hide those sanding marks. State of the art printing equipment may then be used to put false markings on the parts. When the process is complete the parts can look brand new."[27]

Figure 1: The route of a counterfeit electronic component. Source: US Senate Report.



A full 70% of the traced parts in the Senate report came from China, and 20% were re-sold through the UK or Canada. The market entry point for these counterfeit goods is often through independent distributors or brokers offering replacement parts that are no longer in production nor sold by authorized distributors. As in Figure 1, a sale can go through as many as five or six intermediaries by the time the independent distributor receives it, resulting in distributors who may be genuinely unaware of the part's real origin.[28]

Vulnerabilities in pharmaceuticals

Vulnerabilities in the supply chain exist to equally ill-fated effects in the pharmaceutical industry. In 2008, Baxter International was forced to initiate a worldwide recall of Heparin, a widely used blood-thinning drug when it discovered a counterfeit raw ingredient from China had made its way into the production process. That ingredient led to symptoms linked to 149 deaths in the US, and contamination in at least 10 other countries.[29] The cost of the counterfeit component was a fraction of that of the genuine raw material and sufficiently mimicked biological properties of Heparin, suggesting an intentional rather than accidental lapse in manufacturing and sophistication on the counterfeiter's part.[30] (A subsequent lawsuit implicated both Baxter and its Chinese supplier, Scientific Protein Laboratories.)[31] An MIT-led study on the Heparin recall indicated that the way in which the counterfeit made its way into the drug stemmed from the fact that the traditional chemical screening of Heparin's ingredients could not pick up any signature of the counterfeit material.[32] In this case, raw material counterfeiters seized upon a weakness in the procurement process with deadly consequences.

In Africa, counterfeit drugs are limiting efforts to combat diseases such as malaria. *The Lancet* published a study in June 2012 evaluating 21 countries in sub-Saharan Africa, providing data on 2,634 malaria drug samples. More than one-third failed as substandard on the chemical analysis, and about 20 percent were found to be wholly counterfeit.[33] Many suspect counterfeit drugs originate in India and China, but lax regulatory oversight and porous African borders provide conduits for counterfeits into the supply chain.[34] Figure 2 details a set of other prominent examples of substandard and counterfeit medication, as determined by the World Health Organization in May 2012.[35]

SFFC Medicine	Country/Year	Report
1. Avastin (for cancer treatment)	United States of America, 2012	Affected 19 medical practices in the USA. The drug lacked an active ingredient.
2. Viagra and Cialis (for erectile dysfunction)	United Kingdom, 2012	Smuggled into the UK. Contained undeclared active ingredients with possible serious health risks to the consumer.
3.Truvada and Viread (for HIV/AIDS)	United Kingdom, 2011	Seized before reaching patients. Diverted authentic product in falsified packaging.
4. Zidolam-N (for HIV/AIDS)	Kenya, 2011	Nearly 3,000 patients affected by falsified batch of antiretroviral therapy.
5. Alli (weight-loss medicines)	United States of America, 2010	Smuggled into the USA. Contained undeclared active ingredients with possible serious health risks to the consumer.
6. Anti-diabetic traditional medicine (used to lower blood sugar)	China, 2009	Contained six times the normal dose of glibenclamide. Two people died, nine people were hospitalized.
7. Metakelfin (antimalarial)	United Republic of Tanzania, 2009	Discovered in 40 pharmacies. The drug lacked a sufficient active ingredient.

Figure 2: Examples of spurious/falsely-labeled/falsified/counterfeit (SFFC) medicines[36]

Vulnerabilities in tobacco products

Illicit cigarettes generally are not made in compliance with the internationally monitored standards that legitimate tobacco manufacturers follow. For example, the World Customs Organization (WCO) has reported seizures of counterfeit cigarettes containing mites. It also identified dangerous methods of illicit cigarette concealment, such as in barrels of titanium sponge containing toxic chlorine gas that can further contaminate the cigarettes before they are sold.[37]

Certain raw materials and components are essential for the production of cigarettes (e.g., acetate tow filters). Acetate tow is almost exclusively used to produce cigarette filters. Counterfeit and other forms of illicit cigarettes, known as "illicit whites," may not be possible without the acetate tow to make filters. Six global manufacturers[38] provide this essential component, which they can easily trace and identify if they and their intermediaries (e.g., filter makers and selling agents) employ proper monitoring and compliance procedures. INTERPOL Secretary General Ronald K. Noble delineated some of the challenges in his presentation to the Seventh Global Congress on Combating Counterfeiting and Piracy, Istanbul, Turkey, on April 24, 2013:

> "… [C]riminals have hijacked legitimate components/products from their intended use or destination. Take for example, 'acetate tow'–an essential element in manufacturing cigarette filters. In January, authorities in China raided an underground filter production site and seized bales of acetate tow. Based on leads generated, subsequent raids led to the seizure by law enforcement of 40 tons of acetate tow.

What happens when these materials/products reach the wrong hands? It assists in sustaining the production of counterfeit cigarettes. The finished products are then even more difficult to detect as illicit. INTERPOL thus aims to seek collaboration with the acetate tow industry, to provide assistance in containing this illegal diversion."

1.2 Current approaches to the problem

Companies face difficult challenges in determining whether the raw material or component supplier is providing legitimate ingredients. One strategy for dealing with these challenges is the use of "Know Your Supplier" (KYS) programs. Such programs are well established and represent one of the best practices for assuring quality control and supply chain protection. In a broad sense, the term refers to basic due diligence undertaken at the outset of a new business relationship (such as a bank evaluating a loan applicant, or a manufacturer ensuring that a supplier is solvent) and on-going monitoring of that relationship. The same principles have been applied to reduce the infiltration of counterfeits in supply chains.

Suppliers, distributors, and component manufacturers in the early stages of the supply chain can and have established voluntary quality management and accreditation programs to halt the use of counterfeits. While not formally designated as KYS programs, the following examples include important components of the KYS approach. This section describes several of these initiatives and the intermediary actors who have a stake in the supply of raw and component materials. It also highlights common elements that can be replicated, both across sectors and up the supply chain.

Commercial aviation: distributor accreditation program

In the United States, the Partnair tragedy helped spur the FAA to recognize that some management of counterfeit infiltration was necessary. It also encouraged industry engagement and assistance as part of the solution to the problem. By 1996, cooperation with industry groups resulted in the publication of an FAA Advisory Circular, AC 00-56A, which detailed a "Voluntary Industry Distributor Accreditation Program" (VIDAP). VIDAP is an accreditation system based on voluntary industry oversight and a formally established third-party accreditation of distributors.[39] It includes:

- Standards and guidelines for third parties;
- A 17-point review of the distributor's quality system, including checks on traceability, documentation and parts storage;
- Mandated audits every 36 months to comply with the AC.[40]

As of the last revision, the AC 00-56A lists six independent accreditation programs that meet the requirements of VIDAP: the ISO 9000 Series, GAPSA 100, NADCAP AS 7103 and 7104, ASA-100, and TAC 2000. The original AC was updated in 2002 to account for changing technology, but it remains relatively high-level and allows the independent accreditation programs to build on the requirements listed in the original framework. AC 00-56A also allows for a central, FAA-based database where evaluated distributors can be listed. The approach seems to have beneficially spurred competition between the independent accreditors. In this case, the government took the lead in developing a framework, which then provided the basis for industry actors to step up and implement a set of voluntary accreditation programs.

Electronics: standards for parts and vendor management, procurement, testing, and response strategies

The electronics industry provides a valuable precedent for voluntarily preventing counterfeits from reaching final products. In 2009, the SAE, a well-known technical standards sponsor, published a standard called AS 5553 (Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, revised in 2013). The AS 5553 standard provides electronic component manufacturers guidance in deterring counterfeit component provisioning (see Figure 3 for details).

SAE is also currently developing a similar standard for use by electronic component distributors, called AS 6081 (Counterfeit Electronic Parts Avoidance-Distributors) to address other aspects of counterfeit parts prevention.

Though still under development, AS 6081 will seek to:[41]

- Identify reliable sources to procure parts;
- Assess and mitigate the risk of distributing fraudulent/counterfeit parts;
- Control suspect or confirmed fraudulent/counterfeit parts; and
- Report suspect and confirmed fraudulent/counterfeit parts to other potential users.

Additionally, a second standards-development body, the International Electrotechnical Commission Quality Assessment System for Electronic Components (IECQ), established a Counterfeit Avoidance Working Group that is developing a counterfeit avoidance program with accompanying standards to assess and ensure evidence of compliance. The working group is a mix of industry (e.g., Boeing, Honeywell, Airbus), testing laboratory representatives, and certification specialists who have been meeting regularly to develop the program.

While the SAE standard is promising, other standards have been created since its inception, indicating that the SAE standard may require improvements in order to thoroughly address the electronics industry's issues.

The standard defines a variety of processes and techniques that companies should consider to ensure counterfeit raw electronic materials do not enter their supply chains, including:

- Parts management (such as parts selection in designs)
- Vendor selection and supplier management (such as clearly defining expectations that can be communicated to suppliers for their performance)
- Procurement (including specific contract language on purchase orders)
- Inspection, test/evaluation of parts
- Response strategies when suspect parts are discovered

Figure 3: AS 5553 Standard for Electronics

Pharmaceuticals: verified mark program

The US Pharmacopeia Convention has developed a standard and a verification service for pharmaceutical ingredients to assure manufacturers, regulatory authorities, and consumers that drugs bearing the distinctive *USP Verified* mark are of consistent and high quality.[42] The program works by allowing companies, usually end-product manufacturers, to apply for the *USP Verified* mark program to have their own raw ingredients tested, or to verify the quality of a supplier they are using. Suppliers can also voluntarily submit their ingredients for testing. In either case, the qualification process involves evaluating the drug's substance or its excipient (the inactive substance that carries an active ingredient) using a multi-layer approach:

- Auditing the manufacturing site for compliance with existing Good Manufacturing Practices (such as ICH Q7, USP 1078 and IPEC/PQG), and for compliance with the product's labelling or certificate of analysis claims;
- Review of quality control documents and release data, checking for compliance with internal procedures, as well as public pharmacopeia standards and monographs;
- Laboratory testing of samples to ensure compliance with labelling and program requirements;
- Continuing the audit after verification through surveillance testing and full re-evaluation of the product every third year. Manufacturers are also required to notify USP if manufacturing processes undergo substantial changes.

To date, nine companies are participating in the process, representing 16 verified ingredients. The program encourages supply chain risk management through formal assessments of potential suppliers and visible quality assurance labels for consumers.

Tobacco: the Digital Coding & Tracking Association

The Digital Coding & Tracking Association[43] (DCTA) actively responds to increasing illicit tobacco trade by promoting technical standards and digital solutions designed to secure supply chains for excisable fast-moving consumer goods.

The process includes product tracking and tracing, authentication and digital tax verification technologies such as Codentify®.

Codentify® is based on internationally recognized, open technical standards and offers the following:

- Tracking and tracing: enables electronic monitoring of products as they move forward through the supply chain; it also enables tracing backwards through products' journey to identify potential points of diversion;
- Product authentication: enables anyone, anytime, anywhere to immediately verify a product's authenticity using widely available technologies such as a mobile phone or the Internet;
- Digital tax verification: enables governments to verify and control online the volume of products manufactured, and to calculate the commensurate amount of excise and other taxes due.

The tobacco industry has committed to set effective, relevant policies and programs through Cooperation Agreements[44] or Memorandum of Understandings with Intergovernmental Organizations or local law enforcement to fight illicit trade. This commitment has established a system for exchanging information regarding seizures of counterfeit and genuine cigarettes. It has also enabled the industry and governments to identify regional and international illicit trade trends.

Cross-sector standards: ANSI

A good example of best practices to combat counterfeiting can be found in the American National Standards Institute's (ANSI) "Best Practices in the Fight against Global Counterfeiting." Though not aimed specifically towards intermediaries, some of the practices could be useful for intermediaries to incorporate:

- Develop policies and procedures to identify, avoid, and correctly handle and dispose of counterfeit products;
- Provide a systemic approach to anti-counterfeiting, including the following:
    - Reliance upon standards and best practices;
    - Evaluation of organizational threats and product risk;
    - Use of authentication technologies appropriate to the organization and product; and
    - Collaboration with local and national law enforcement agencies.
- Develop a trusted supplier network and/or look to organizations that have developed such networks;
- Require audits of suppliers as part of contractual obligations to assure adequate security, screening, and testing procedures; and
- Urge government to establish a centralized reporting mechanism and database for collecting information on suspected/counterfeit products and parts discovered in global supply chains.

1.3 Additional approaches to consider

The above programs suggest strong actions that address counterfeit supplies and suppliers. Established practices beyond these actions—especially from more general supply chain best practices—could also yield results for raw material and component intermediaries.

KYS and beyond — Know Your Customer

The accreditation programs and practices above are positive examples with strong KYS elements specifically geared towards counterfeiting, but KYS programs tackle only one aspect of the counterfeit chain. Suppliers of illicit inputs require customers. In some cases, customers are complicit in the counterfeit chain or may be active players who facilitate ordering or movement of the counterfeit inputs. Such bad intent is easily achieved given that raw materials and components can go through several supply intermediaries before assemblage.

In this case, "Know Your Customer" (KYC) programs may assist by incentivizing downstream intermediaries to adhere to stricter standards, resulting in increased brand protection and risk mitigation for the intermediary implementing the program. In an ideal situation, intermediaries would combine KYS and KYC programs to address the possibility of counterfeit activity in both suppliers and customers.

For example, a chemical manufacturer may serve numerous legitimate customers for legal downstream uses. It should refrain from supplying that chemical to an unscrupulous customer who plans to use the chemical in production of counterfeit drugs. Similarly, refurbished bolts or electrical wiring may represent legitimate inputs into secondary markets for used car parts in developing countries. A supplier of such bolts might rightly sell those down the supply chain as used or reconditioned parts but not as "new" or "genuine." Of course, the parts should not be rebranded for resale as "new" to a third party repair station for commercial or military jets.

In these cases, KYS programs coupled with KYC programs at multiple stages would help develop due diligence processes to ensure that vendors at each stage in the chain are engaging in good business practice.

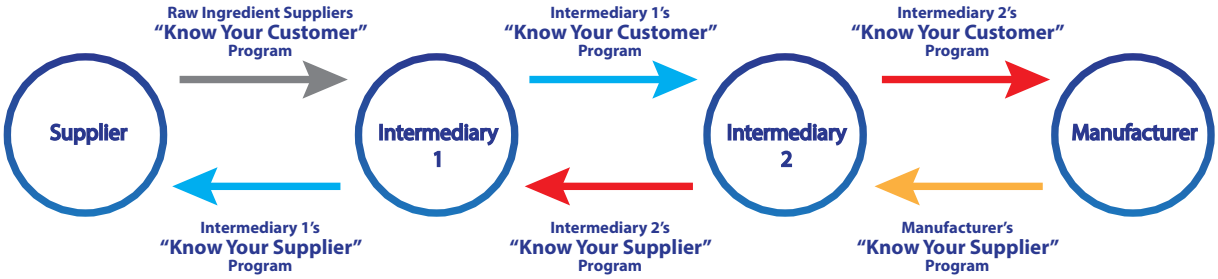


Figure 4: Better due diligence for supply-side intermediaries

Intermediaries can adapt elements from more general KYS and KYC programs to combat illicit trade. For example, tobacco manufacturers have developed robust KYS and KYC compliance programs to fight illicit goods within their supply chains. Intermediaries can apply these same principles to ensure business partners' integrity along any segment of the supply chain (such as by Intermediary 1 or Intermediary 2 in Figure 4).

Philip Morris International's (PMI's) Fiscal Compliance Program (FCP) is designed to ensure that PMI does business only with responsible organizations and individuals who share PMI's commitment to comply with relevant fiscal and trading laws. The FCP establishes requirements for selecting and retaining customers, third party manufacturers, vendors, and other entities that are directly involved in the manufacture, distribution, and sale of PMI products.[45]

Under PMI's KYS policy:

- PMI affiliates must complete due diligence checks, conduct annual reviews, and maintain a semi-annually updated database of approved Logistic Service Providers (LSPs).

The KYS policy is designed to ensure that LSPs that store or ship 25 million or more cigarettes comply with relevant fiscal and trade laws and regulations when dealing with PMI products.[46]

Under PMI's KYC policy:

- PMI will engage only with legitimate businesses.
- All potential new customers, third parties that manufacture PMI brands under license or contract, and entities to which PMI ships at the direction of a customer are subject to due diligence and annual reviews.
- Responsibility is established and designated for monitoring sales and remaining alert to unusual activities and trends.
- Affiliates must certify that order volumes and production volumes are consistent with legitimate demand in the market of destination.
- Letters are sent annually to certain customers indicating that PMI expects them to (i) comply with all applicable fiscal laws and regulations when dealing with PMI products; (ii) resell PMI products only in the approved market of intended destination and nowhere else; and (iii) communicate the messages in (i) and (ii) to their own customers. Customers are reminded that PMI reserves the right to stop supplying its products—or to revoke a license or contract to manufacture such products—to anyone who is involved in activity in connection with PMI products that is either illegal or violates PMI's expectations.

The KYC policy is designed for PMI's customers as well as for these customers' customers. It encourages all customers to apply effective policies within their respective supply chains. Moreover, PMI conducts annual training for employees who are involved in the sale, distribution, shipment and/or storage of PMI products or in establishing policies or business practices relating to those activities.

Another example comes from Japan Tobacco International (JTI).[47]

JTI's KYS compliance program requires the following:

- Analysis of new and existing suppliers and annual certification to ensure they meet JTI business integrity standards, including a requirement for suppliers to cooperate in any illicit trade investigation;
- Regular monitoring of suppliers that includes background credit checks, checks on directors, and the creation of a risk assessment relating to suppliers and distributors;
- Raising awareness among suppliers through proactive engagement to educate them on the need to implement and enforce procedures within their own supply chains.

The objectives of JTI's KYC program are as follows:[48]

- To ensure sales only to customers who they are satisfied will not divert products from the legitimate supply chain;
- To avoid business relationships with potential customers prior to securing all approvals required by local laws and internal corporate policies (inclusive of certification processes for larger customers); and
- To actively encourage larger customers to adopt and enforce their own KYC procedures.

Key elements of PMI's and JTI's KYC programs include the following:

- Termination of contracts with customers found to have engaged in or willingly facilitated illicit trade (as established by documentary or other substantial evidence resulting from an investigative process through a corporate compliance function);
- Annual due diligence and ongoing customer monitoring;
- Clear rules defining all commercial customer dealings, including adequate documentation and secure records administration and storage, sometimes beyond the requirements of local laws;
- In-depth background checks (in addition to those completed during the certification process) mandated for customers operating in countries with significant risk of illicit trade, general lack of regulations or weak enforcement, or where the company has little or no commercial presence, or where the market is considered "high-risk," as assessed by independent organizations (such as Transparency International);
- Records note unexpected significant increases in sales volumes to customers; Records identify substantial changes to a customer's corporate organizational structure or personnel.

Companies have used individual KYC and KYS programs for due diligence and to address issues such as child labor or environmental concerns. Few of these programs, however, are designed specifically to halt counterfeits. Recognizing this challenge, the US Coalition on Counterfeiting and Piracy (CACP) in its "No Trade in Fakes Supply Chain Toolkit" reinforces the suggested downstream-upstream due diligence process. Sections urge both securing legitimate inputs (KYS) and verifying legitimacy of customers and distributors (KYC). Where KYS and KYC programs do address the threat from counterfeit materials, they often do not reach far enough up the supply chain. Additional sectors need to duplicate and adapt these programs in order to assure a significant impact.

Along with deterring infringement, KYS and KYC programs successfully detect and deter counterfeits stemming from unsavory business relationships, saving intermediaries from substantial contract termination costs and potential liability.

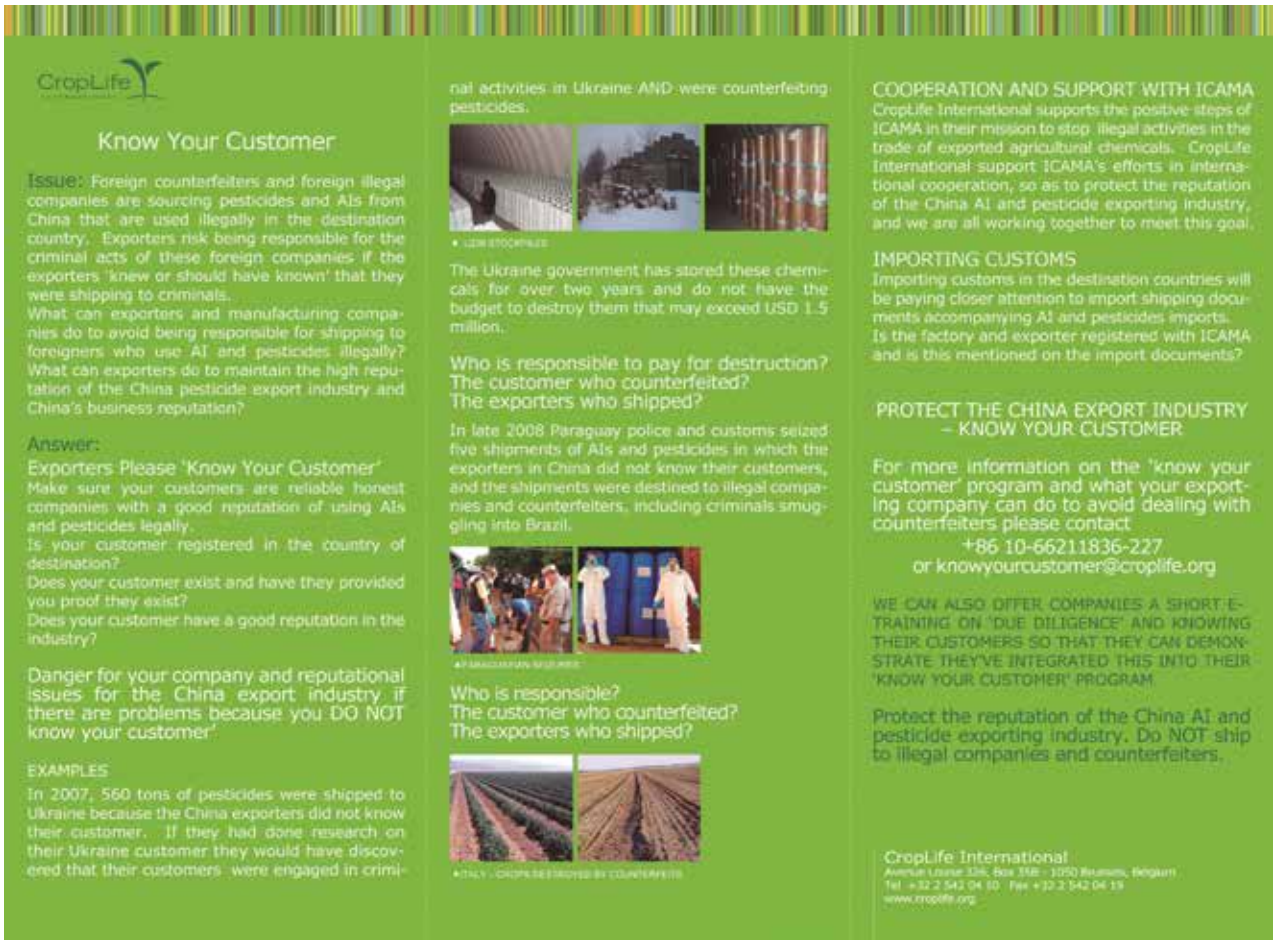
KYC in transport of pesticides

Croplife International has worked with chemical material exporters in China to develop KYC programs that deter such chemicals from finding their way into counterfeit pesticides (see Figure 5 on the following page).

The program, and others like it, specifically asks the following of chemical exporters and shipping intermediaries:

- Do legitimate carriers want to work with counterfeiters and carry counterfeits? If not, what are the carriers doing about it?
- Are carriers (vessel, aircraft) performing any due diligence? At minimum, what are the names and identities of people delivering containers to the vessels, in order to enhance transparency and traceability?
- If carriers are making money transporting counterfeits, and customs identifies them, is it fair to burden the brand owners for storage and destruction costs? Shouldn't the carriers that have been paid by the counterfeiters pay for the resulting "storage and destruction costs" from the unjust enrichment funds they received from the counterfeiters?

Collaboration with shippers on these questions can help foster stronger and more sustainable relationships for both the brand owners and shipping intermediaries.



CropLife

Know Your Customer

Issue: Foreign counterfeiters and foreign illegal companies are sourcing pesticides and AIs from China that are used illegally in the destination country. Exporters risk being responsible for the criminal acts of these foreign companies if the exporters 'knew or should have known' that they were shipping to criminals.
What can exporters and manufacturing companies do to avoid being responsible for shipping to foreigners who use AI and pesticides illegally?
What can exporters do to maintain the high reputation of the China pesticide export industry and China's business reputation?

Answer:
Exporters Please 'Know Your Customer'
Make sure your customers are reliable honest companies with a good reputation of using AIs and pesticides legally.
Is your customer registered in the country of destination?
Does your customer exist and have they provided you proof they exist?
Does your customer have a good reputation in the industry?

Danger for your company and reputational issues for the China export industry if there are problems because you DO NOT know your customer

EXAMPLES
In 2007, 560 tons of pesticides were shipped to Ukraine because the China exporters did not know their customer. If they had done research on their Ukraine customer they would have discovered that their customers were engaged in criminal activities in Ukraine AND were counterfeiting pesticides.

The Ukraine government has stored these chemicals for over two years and do not have the budget to destroy them that may exceed USD 1.5 million.

Who is responsible to pay for destruction?
The customer who counterfeited?
The exporters who shipped?

In late 2008 Paraguay police and customs seized five shipments of AIs and pesticides in which the exporters in China did not know their customers, and the shipments were destined to illegal companies and counterfeiters, including criminals smuggling into Brazil.

Who is responsible?
The customer who counterfeited?
The exporters who shipped?

COOPERATION AND SUPPORT WITH ICAMA
CropLife International supports the positive steps of ICAMA in their mission to stop illegal activities in the trade of exported agricultural chemicals. CropLife International support ICAMA's efforts in international cooperation, so as to protect the reputation of the China AI and pesticide exporting industry, and we are all working together to meet this goal.

IMPORTING CUSTOMS
Importing customs in the destination countries will be paying closer attention to import shipping documents accompanying AI and pesticides imports.
Is the factory and exporter registered with ICAMA and is this mentioned on the import documents?

PROTECT THE CHINA EXPORT INDUSTRY – KNOW YOUR CUSTOMER

For more information on the 'know your customer' program and what your exporting company can do to avoid dealing with counterfeiters please contact
+86 10-66211836-227
or knowyourcustomer@croplife.org

WE CAN ALSO OFFER COMPANIES A SHORT E-TRAINING ON 'DUE DILIGENCE' AND KNOWING THEIR CUSTOMERS SO THAT THEY CAN DEMONSTRATE THEY'VE INTEGRATED THIS INTO THEIR 'KNOW YOUR CUSTOMER' PROGRAM

Protect the reputation of the China AI and pesticide exporting industry. Do NOT ship to illegal companies and counterfeiters.

CropLife International
Avenue Louise 326, Box 308 - 1050 Brussels, Belgium
Tel +32 2 542 04 10 Fax +32 2 542 04 19
www.croplife.org

Figure 5: Croplife flyer distributed at Shanghai pesticide export fair in 2009

1.4 Are these practices working?

These examples demonstrate how voluntary accreditation and quality management systems can be used to deter the infiltration of counterfeit raw material and components into supply chains. Each has clear merits and some limitations.

The longest-running voluntary initiative, VIDAP and its associated third-party accreditation system, has proven broadly successful. The initiative is a positive example of shared responsibility between government and industry. Interviews with leaders in the field of replacement aviation parts suggest that program success in the United States is reflected in the few reported counterfeit problems in commercial aviation in recent years. The rapid and tough prosecution of offenders has also deterred counterfeiters. Unfortunately, the system has not addressed component problems in military aviation, which may be spilling over into commercial lines. Reports in 2012 noted suspected counterfeit ice-detection modules on at least seven commercial aircraft.[49]

Any general assessment of the SAE and USP programs is limited by their relatively short histories. The 2013 revision of AS 5553 that seeks to further globalize the standard suggests that the program is growing and can potentially thrive. Yet the development of alternative standards from the IECQ may indicate that some seek still further improvements. The *USP Verified* mark scheme also continues to grow, yet its effectiveness has yet to be fully evaluated. Criticism of the USP process has been minimal, given that it is the only recognized standard and audit process from an independent third party. The system could further benefit, however, by attracting additional participants and making the voluntary process the norm rather than the exception.

Despite these sophisticated multinational efforts, programs sometimes fail to identify weaknesses. One reason for this shortcoming might be a failure to focus on the individuals behind the counterfeiting action. Criminals can easily start a new company or find new employment and continue their counterfeit activity; for this reason, associated people should be tracked, along with their companies and activities.

Notwithstanding the efforts of organizations such as the ANSI, the CACP, and the Aerospace Industries Association (AIA) which promotes supply chain security, these voluntary practices have not been fully embraced by intermediary companies, especially those distanced from direct interactions with manufacturers. Manufacturers and their partners must continue work to integrate intermediaries into the development and adoption of practices that will halt counterfeits from running through their business lines.

These programs represent only a partial list of all voluntary plans to combat component supply counterfeiting, and more needs to be done, including the application of technology. For example, the US Pharmacopeia Convention runs a Food Fraud Database to track counterfeit ingredients in food products, which reported a 60% increase in food fraud in 2012.[50]

What is clear from the national programs–those in the United States for example–is that combating counterfeiting may begin domestically but can be only fully successful if the efforts become as trans-national as the intermediary suppliers and distributors they aim to stop. It is, therefore, critical to introduce the most successful models throughout the supply chain, especially when that chain crosses international borders. Where these models are not suitable for international application, the standard programs and practices described here can serve as examples to other voluntary programs. Enhanced efforts should be made to gather and share standardized data in order to monitor each program's relative effectiveness.

1.5 Suggested best practices

Raw materials, ingredients, and components suppliers are typically the "first intermediaries" in most product supply chains. Furthermore, multiple intermediaries may contribute inputs or services toward the manufacture of a final product. Such a complex network of suppliers creates multiple opportunities for counterfeiters to integrate fake inputs into the supply chain or mask the true origin of a production input.

1. **Expand Know Your Supplier (KYS) and Know Your Customer (KYC) programs by component and raw material intermediaries to incorporate specific provisions covering the risk of counterfeit infiltration into the supply chain.** The KYS/KYC programs should include ongoing customer/client monitoring, more in-depth background checks for partners operating in problem markets and monitoring for unusual transactions. These should be implemented in clear contractual terms, alongside operational controls such as audits of documents, data and facilities, and regular inspection, testing, and evaluation of sample raw materials, ingredients, and components.
2. **Carefully monitor suspicious customer orders by suppliers of active ingredients and other essential components** that have a limited number of suppliers, as seen in the examples of CropLife engagement in China and acetate tow in the production of tobacco products.

3. **Develop standards and guidelines for third-party accreditation mechanisms**, such as SAE standard on Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition produced for the electronics industry and the US Federal Aviation Administration's Voluntary Industry Distributor Accreditation Program (VIDAP). Trusted supplier networks can then be built using suppliers that adopt these higher standards. Centralized reporting mechanisms, operated by third-party rating agencies or government agencies, should collect information on component supplier counterfeiting, including information on involved individuals as well as companies, with appropriate redress mechanisms to correct mistakes.

4. **Deploy technologies, such as tracking and tracing, where possible, to complement monitoring and compliance efforts**, basing them on open standards to ensure interoperability between systems and to avoid fragmentation across companies, sectors and countries.

2. Transport operators

The process of transporting and distributing product involves a number of key intermediaries, which are grouped here under the overarching category of "transport operators." These intermediaries include vessel, rail and truck carriers, as well as air cargo. With increasing use of the Internet to order and purchase goods, small parcel shippers such as express courier companies and postal services are also important shipping intermediaries. Transport operators represent important intermediaries for this study due to their major role in the supply chain and the transportation of counterfeit goods. Processes and documentation already used by shippers provides an opportunity to help identify and stop counterfeit goods before they enter the supply chain. This documentation is an important information source for enforcement officials and rights holders. The name and address of the shipment originator, payment details, and package origin and final destination—even if only partially accurate—can provide valuable data on the flow of counterfeit and pirated goods.

2.1 Vulnerabilities to counterfeits for transport operators

Counterfeit and pirated goods have been seized in cargo containers shipped by air and sea, in individual packages routed through traditional mail centers, and in packages sent by express mail. Many products move through these channels simultaneously. See Figures 6 & 7 for air and sea routes, respectively, that are most used for counterfeit pharmaceuticals[51] and cigarettes.[52]

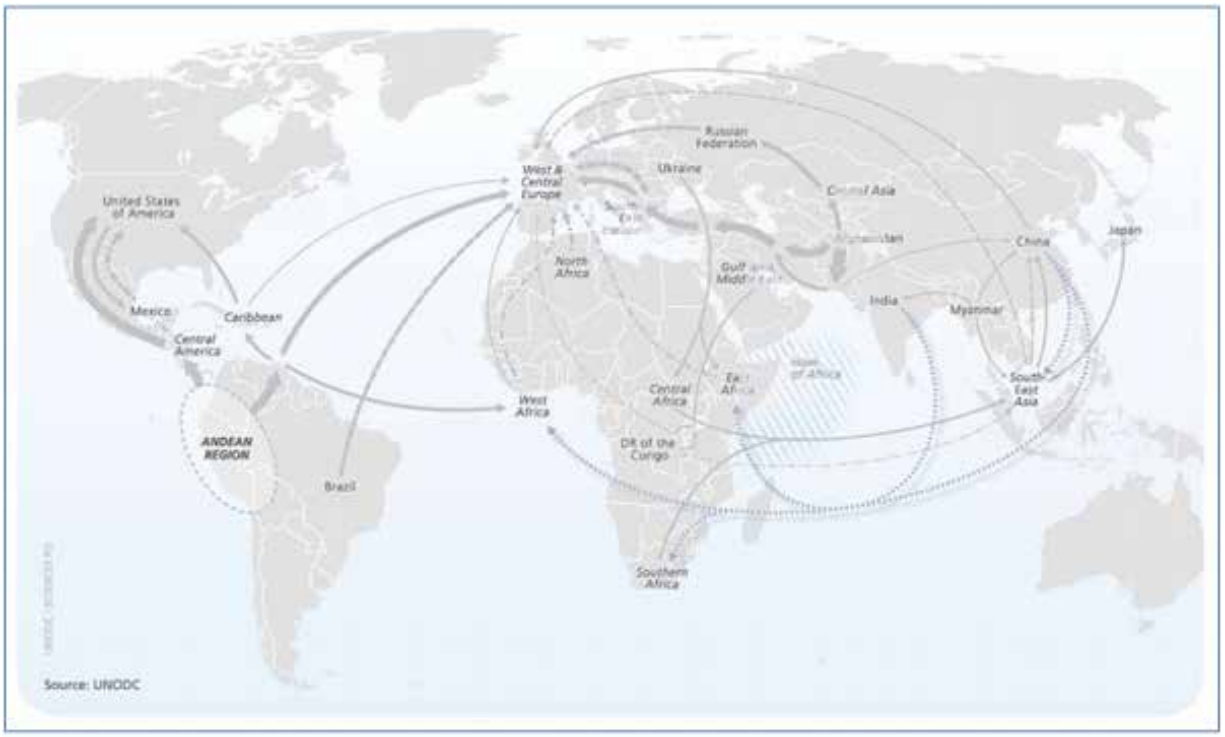


Figure 6: Counterfeit medicines from South and East Asia to South-East Asia and Africa. Source: UNODC.

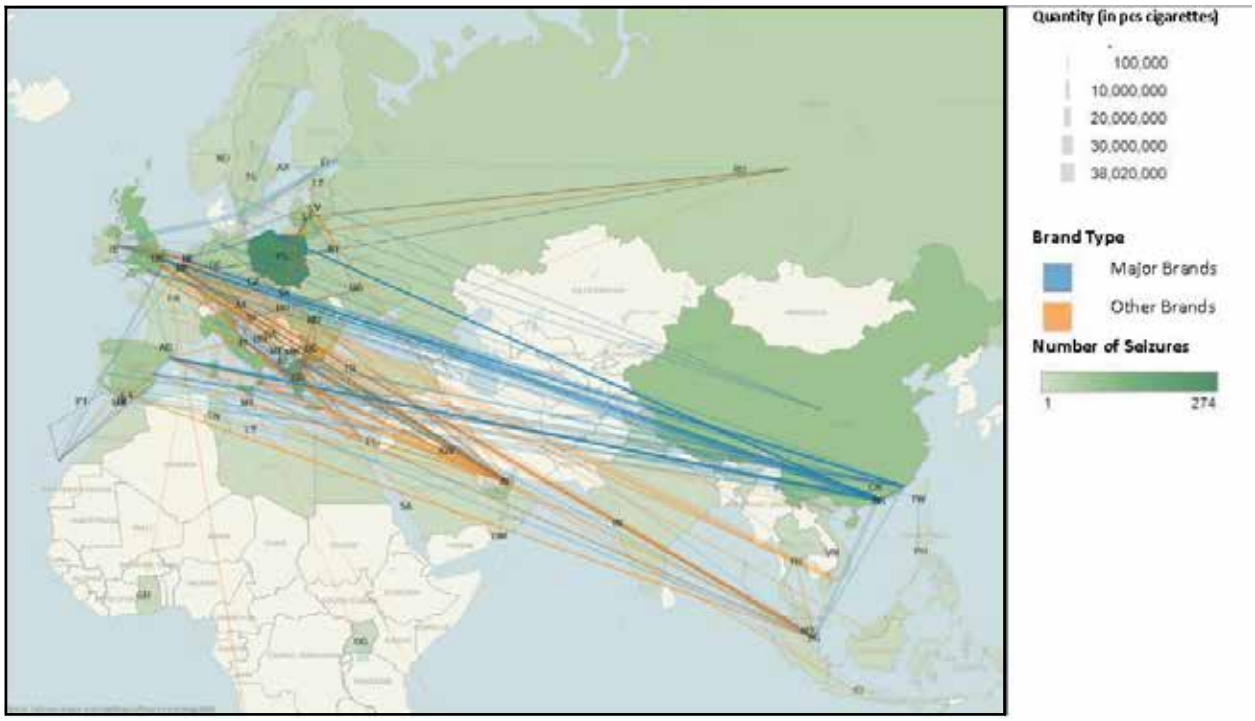


Figure 7: Main countries of provenance for illicit tobacco products in the Eastern hemisphere are, in order of importance China, the United Arab Emirates, Vietnam, Malaysia, the Russian Federation, Singapore, Belarus and Ukraine.

The techniques counterfeiters use to ship goods without detection include:[53]

- Mislabeling shipments and using false documentation; in some cases, counterfeiters use the stolen identities of legitimate transport operators with no history of illegal trafficking to reduce the risk of customs inspecting the infringing goods.
- Shipping goods via a second or third country to disguise the true country of origin, a method referred to as "transshipping." This method is prevalent when shipping counterfeit goods from China. Shipments are often routed through another country's port—perhaps known for stronger IP protection—before they reach the country of destination.
- Hiding counterfeits in shipments of genuine goods to mask their illegal nature and obstruct efforts to identify and seize the infringing products.
- Separating the counterfeit branding materials (such as labels or packaging) from the actual counterfeit product during shipment, and then assembling the product with the fake branding in the country of destination or in a free trade zone.

Quantifying the full scope of counterfeit distribution relative to legitimate shipping is difficult given the array of variables and lack of worldwide reporting. Seizure statistics provide a glimpse into the problem. Figures gathered by Customs indicate that the market retail value of seized products by US authorities in 2012 alone was over $1.25 billion. In 2011, European Union customs detained nearly 115 million counterfeit articles with an estimated value of over $1.2 billion. China was the source of the majority of seized counterfeit exports, while India and states with active port cities like the United Arab Emirates and Greece were also heavily involved.[54]

Vulnerabilities in container shipping — sea and land

Counterfeits that are shipped by large sea container or cargo, and those shipped by overland transport via rail or truck, present challenging vulnerabilities:

- The ease of hiding fake goods inside large shipping containers;

- The enforcement challenges created by the sheer global volume of container cargo; and
- The actions by counterfeiters to mask the true nature of the shipments with false paperwork that is not always easily identified as illegitimate.

As a consequence, the goods transported by these intermediaries are especially difficult to monitor. Sea and land have become the favored means for transporting large volumes of counterfeit and pirated materials, a fact that has been confirmed by existing data. In 2012, less than 7% of the individual seizures by US authorities were cargo shipments, but they carried a value higher than the seizures from all other transport methods combined.

Transport of counterfeit pesticides illustrates the source of the vulnerability. The weight and volume requirements for pesticides often require container shipping. An excerpt from a report on pesticide counterfeiting highlights the sophisticated network for getting goods to market. In this case, shipments of counterfeit chemicals from China were separated from their branding and distribution in Russia:

In June 2008, regional police in Russia uncovered a major pesticide-counterfeiting facility. The police raided premises near the city of Kursk, where around 100 tons of counterfeit and illegal pesticide products were found with an estimated market value of nearly US$1 million. Most of the products were illegal copies of patented and branded products from major legitimate manufacturers pre-packed into containers ready for commercial sale. Adjacent to the warehouse, the police uncovered equipment designed to apply labels and stickers to the bottles, as well as other packaging equipment. Initial examination of the symbols on the seized product containers indicated that the products were manufactured in China. There are also indications that the transport routes to Kursk may be different for differing consignments, with some arriving by sea and others by road and some possibly running through an EU port.[55]

Pesticide counterfeiting is rife worldwide. According to the European Crop Protection Association, EU and non-EU authorities seized more than 2,500 tons of counterfeit pesticides in 2011. Sales of counterfeit pesticides account for 5-10% of total pesticide sales in developed markets such as the EU, and up to half of sales in emerging markets. Counterfeit pesticides account for upwards of $4 billion globally.

An example from Africa illustrates the scale of vulnerability. In 2012, the World Customs Organization (WCO) in partnership with the Institute of Research against Counterfeit Medicines (IRACM) organized a customs enforcement operation called Operation VICE GRIPS 2:

- Operation VICE GRIPS spanned 16 countries: Angola, Benin, Cameroon, Democratic Republic of the Congo, the Republic of Congo, Côte d'Ivoire, Gabon, Ghana, Guinea, Kenya, Liberia, Mozambique, Nigeria, Senegal, Tanzania and Togo;
- Of 110 maritime containers inspected, 84 vessels–or 76%-were found to contain counterfeit or illicit products;
- The effort seized more than 100 million counterfeit products of all categories;
- It also netted 82 million doses of illicit medicines, including anti-malarial and anti-parasitic drugs, antibiotics, cough syrups, and even contraceptive pills and infertility treatments, estimated to be worth over 40 million US dollars;
- Some of the merchandise suggested elaborate or even industrial-scale operations.

> *"We are dealing with structured organizations that specialize in international fraud, which exploit globalization in operations that span continents and countries, using different forms of transport."*
>
> Christophe Zimmermann, in charge of anti-counterfeit operations at the WCO in reference to VICE GRIPS 2 in Africa.

Figure 8: From left to right: Mearsk Charlotte, Hanjin Pennsylvania and Hyundai Fortune

Unfortunately, many counterfeits move through the system without seizure, and others fail because they cause catastrophic accidents during transport. Many criminals mislabel their goods, some of which may be hazardous materials, including items like hazardous chemicals used in counterfeit pesticides. Vessel shippers must load hazardous cargo carefully and appropriately, and when hazardous materials are mislabeled, they can be placed in the wrong location aboard ship. Figure 8 above shows three well-known vessel fires reported to have started due to the mislabeling of hazardous materials. Damage or loss of a vessel can be not only a concern of the intellectual property owner and manufacturer but also a serious financial vulnerability for sea cargo shippers.

Vulnerabilities in air cargo and mail couriers

Air cargo and mail couriers present a similar set of vulnerabilities. These channels are growing rapidly and can be abused by counterfeiters. Trends point to an increase in counterfeiters sending smaller shipments via mail or express consignment/courier operators. Meanwhile, the number of express mail seizures in the US has soared over the past few years to a high of over 10,000 cases in 2011, outstripping other shipping intermediary channels for the first time.[56] This rise may in part be due to increased training and enforcement focus by US authorities. In the EU, the 15% increase in seizures from 2010 to 2011 stemmed entirely from the mail and express courier areas. This surge is due, in part, to the increasing demand for small orders of goods purchased over the Internet.

Counterfeiters also abuse the services by moving smaller goods within the massive volume of packages to decrease the likelihood of detection, just as they hide larger goods within containers.

Rather than ship directly by air to customers, core distributors from such supplying countries will often send shipments to individuals or entities known as “drop shippers” in consumer markets. Frequently utilizing express or expedited mail service (EMS), the distributors engage a system of over 150 cooperating national postal services (separate from private express courier services like FedEx or DHL). The massive volume of air packages moving through EMS makes it an attractive distribution avenue. Once the drop shippers receive delivery, they divide the counterfeits into individual orders and send them on to final customers, either through traditional mail or by express courier (see example in Figure 9).[57] Other sectors afflicted by IPR infringement, such as pirated software, have documented similar distribution and transport networks.[58]

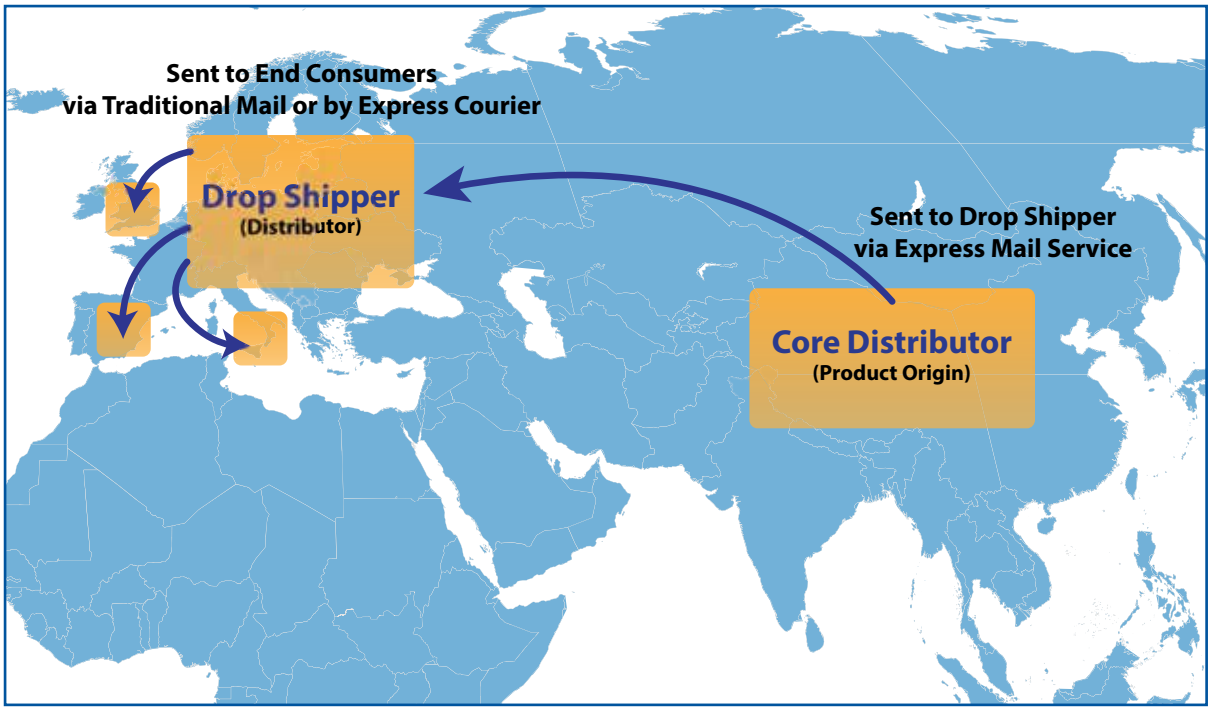


Figure 9: Air transport routes of counterfeit and pirated goods

Such air-based transport does not, however, always travel in expected directions. In 2011, the Dubai customs authorities held an air freight package containing 750 kilograms of illicitly produced and branded cigars after receiving information on the possibility that the package carried counterfeits. The consignment was en route from an Eastern European country of origin to another Middle Eastern destination, an unusual and non-traditional route for counterfeit transport. In this case, the counterfeits were seized and destroyed, and the trader fined over $100,000 by authorities.[59]

Another case informs the global nature and scale of vulnerability. Between November 2011 and February 2012, the U.S. Customs Service, in tandem with the World Customs Organization (WCO), seized more than 30,000 parcels containing more than 150,000 counterfeit items. Officials carried out controls at international mail facilities and express courier depots in a 43-country operation called Hoax II. Items included toys, pharmaceuticals, electronic goods, clothing, DVDs, watches, mobile phones and handbags, as well as other illicit goods such as cannabis seeds, anabolic steroids and amphetamines.[60] The value of items seized in the US airports alone amounted to over $7.3 million. The operation's predecessor, Global Hoax I, focused on pirated goods in 2010 and resulted in the seizure of 142,000 DVDs and 28,000 CDs.

2.2 Current approaches to the problem

Given the scale of the problems and the range of vulnerabilities outlined above, the shipping community must remain engaged and cooperative in efforts to stop shipments of counterfeit goods via all transport avenues. Some shipping intermediaries have made notable efforts to voluntarily assist legitimate manufacturers and customs agencies in stopping the abuse of their services; however, broadening the shipping community's involvement and cooperation is essential to assist in stopping counterfeit transport.

Voluntary monitoring and reporting, partnerships, blacklists, education and data-sharing

Express carriers and postal operators have demonstrated that they are among the more active intermediary partners in the fight against counterfeits. Many express couriers have independently developed voluntary practices and policies both internally and in working with enforcement partners. A good example is DHL's extensive Intellectual Property Rights (IPR) control system that includes the following four elements:

1) *Monitoring and reporting system*
    - Maintenance of a Security Incident Database where all IPR infringing shipments identified by customs are logged in a Global Shipment Incident Database (SID) providing instant visibility to the offending origins;
    - Systematic follow-up on each logged violation with authorities in the location of shipment origin, and action taken on a local level.

2) *Partnership with global authorities*
    - Establishment of direct communication between senior government officials and joint operations to share information targeting IPR smuggling activities;[61]
    - Based on information from national authorities, collaboration with law enforcement to conduct random shipment inspections for IPR items;
    - Monthly reporting and conference calls between regional and headquarter operations to develop additional opportunities that isolate repeat offenders.

3) *Blacklisting repeat offenders*
    - Maintenance of an Offending Shipper List;
    - Joint work with co-loader partners to isolate counterfeit shippers/transport operators.

4) *Education*
    - Structured program of regular visits to educate regional co-loaders on IPR infringement/smuggling trends and tactics along with shipment security requirements;
    - Continued educational cycle with local operatives and x-ray operators to maintain knowledge and expertise in newly detected smuggling activities;
    - Regular workshops and talks provided by customs authorities in anti-smuggling training to frontline operatives.

It is important to note here that express couriers engage in significant data sharing. Some have also implemented programs to attack illicit goods moving through their systems in ways that can target counterfeits. FedEx has granted customs inspectors access to the company's database of international shipments. UPS has also developed software called *Target Search* that enables customs agents to search manifest information for all imported packages passing through its Louisville facility in the United States.[62]

The Global Express Association (GEA), representing the international express delivery companies (DHL, FedEx, TNT, and UPS), has also stated its commitment to comply with all existing applicable laws and regulations. It has further agreed to cooperate as trustworthy partners with Customs in order to address IPR offenses. The GEA believes effective enforcement of IPR infringements requires a risk-based and threat-management approach, as well as cooperation and information sharing between rights holders, customs and express delivery companies. In the GEA's view, practical limitations exist to what its member companies can do. The GEA notes it is not the originator of shipment information, but that it can and will assist Customs as follows:

- *Advance electronic shipment information:*
    - Express delivery companies transmit electronic information in advance of shipment arrival to enable Customs to perform risk assessment and target shipments for further examination.
- *Track and Trace systems:*
    - Allow packages identified by Customs as suspicious to be removed from traffic flows and provided to Customs officers for further examination.
- *Facilities:*
    - Express delivery companies provide Customs officers at express delivery hubs with adequate facilities and equipment to enable them to identify and examine suspect shipments efficiently.
- *Information on shippers and consignees:*
    - Express delivery companies provide Customs administrations with available relevant information that may legally be disclosed on shippers and consignees of shipments identified as containing offending goods.
- *Close accounts of customers publicly identified by customs as repeat offenders.*

As delineated above, express carriers have put good effort into developing systems to aid in the interception of counterfeits and pirated goods. They are doing their part in overseeing their portion of the supply chain, especially in tracking data and sharing information. As with other intermediaries, though, where patterns of customer behavior lead to knowledge of what is being shipped, then they are expected to act to avoid doing business with criminals.

The postal industry has also undertaken initiatives to actively fight against counterfeits in postal flows.

At the international level, the Universal Postal Convention (UPC, signed by 192 countries) was modified in 2008 to include counterfeit and pirated goods in the list of prohibited items (Article 18 of the UPC). This agreement requires that designated postal operators have to inform users about the obligation to respect this prohibition.

In addition, a Protocol had been signed between the Universal Postal Union (UPU) and the World Customs Organization (WCO) to reinforce cooperation between both organizations. Postal operators attend regular joint training sessions on how to discourage the flow of counterfeit and pirated items sent through the mail stream.

Some postal operators have also engaged in government sponsored voluntary efforts. In February 2012, for example Le Groupe La Poste signed a charter on the fight against counterfeit with rights holders *("Charte de lutte contre la contrefaçon – Titulaires de droits, associations représentant des titulaires de droits et opérateurs postaux")* under the patronage of the French Ministry of Economy. To date, 6 professional associations, 21 rights holder companies, 4 ad exchange platforms and 8 postal operators have signed the protocol.

Le Groupe La Poste has reinforced its coordination with the French Customs administration. It now continually facilitates the actions of its international customs officers and postal agents who physically control the suspicious parcels and packages. In July 2011, La Poste and the French Customs organized a joint operation against counterfeits. During five days, customs and postal agents controlled 100% of the parcels entering the international office of exchanges in Paris coming from seven targeted countries: 4% of screened parcels contained counterfeiting goods, 1500 articles had been seized with an average of 22 counterfeiting articles per parcel. The Poste Italiane in Milan also organized a similar initiative.

KYC programs in shipping/transport

The KYC and KYS programs outlined in the previous chapter for upstream raw material and component supply intermediaries have also been promoted to transport operators and shippers to deter counterfeit transportation through the supply chain. KYC programs, in particular, are being considered for vessel companies, especially within the crop protection industry.

In this sense, transport operators and shippers need to know that their upstream customer, for whom they are shipping, is not engaged in counterfeit distribution. For example, vessel companies with effective KYC programs can use their reputation to their own advantage: Their good business practices will attract legitimate brand owners and transport intermediaries who want to monitor all ends of their distribution channels. These reputable vessel companies can help focus customs searches on shippers that employ lower due diligence standards.

KYC and due diligence services

Due diligence on transport operators and other shipping intermediaries—especially on behalf of banks that provide trade credit for international cargo shipments—has long been an accepted practice to avoid financial losses from fraudulent trade. Yet while it has occurred, such due diligence has not been widely applied to the transport operators and shippers themselves. Groups such as the ICC's International Maritime Bureau and others regularly engage in due diligence activities for the shipping industry. Their efforts include specific company reports that can be tailored for shippers to determine the viability of business relationships, for example, investigating a company's shareholders, assets, information on associated companies, and other details.[63] Discussions are under way to consider how due diligence programs can be expanded specifically for identifying and minimizing counterfeiting risk.

Multilateral public-private partnerships

Industry is also collaborating with global intergovernmental efforts to deter counterfeiting and piracy and to provide resources to transport operators and shippers. The United Nation's Container Control Program (CCP), a joint initiative of the UN Office on Drugs and Crime (UNODC) and the WCO, was originally designed to deter drug trafficking by creating sustainable enforcement structures in selected seaports. It has greatly expanded its mandate, however, to counter illicit trade more generally, including counterfeits.

Since the program's launch in 2003, efforts have resulted in the seizure of 483 containers of fraudulent and contraband goods.[64] The program continues to expand, with several added ports in 2012, including the first two in the Caribbean in Suriname and Guyana.[65] In July 2012, CCP accepted its first private sector donation from a major apparel manufacturer. The donation would enhance efforts to tackle the role of shipping routes in counterfeit trade by increasing container inspection and detection of illicit goods.[66]

2.3 Additional approaches to consider

The above programs suggest model actions currently under way to address counterfeits in shipping. As the CCP program indicates, overlap exists between activities to deter other threats—such as drug trafficking, terrorism or general security—and transport of counterfeit and pirated products. Established programs that focus on these other threats can be applied to anti-counterfeiting approaches in shipping channels. They can also serve as institutional bases from which to build programs oriented specifically towards tackling infringement.

The EU Joint Research Council is currently reviewing this area as part of the IP Enforcement Action Plan announced in July 2014.[67] The example of weapons control and export compliance for dual-use technologies provides a clear analogy. King's College in London runs "Project Alpha," a program sponsored by the Ministry of Defence. This program makes many of the same due diligence recommendations in this and the previous chapter.[68]

Partnerships to enhance targeting of counterfeit shipments

Given that the law in most countries requires customs authorities to handle shipment inspections, and given the massive volume of shipments that cross borders daily, much of the difficulty lies in targeting and maximizing inspection resources and efforts. Joint programs with shipping intermediaries and customs offer promising ways to ensure these resources are being utilized efficiently.

Authorized Economic Operator Program (AEO)

The European Union has implemented an Authorized Economic Operator (AEO) program designed to increase transparency and security in the transport of goods to or from the European Union.[69] While not geared specifically towards counterfeiting, this program gives beneficial customs status to voluntary participants that adhere to the program guidelines. These guidelines, mainly focused on security and safety, account for the responsibilities of all stakeholders in the supply chain.

Essentially an accreditation process, the AEO program encourages coordination between customs agents and adherence to responsible security practices by intermediaries. Clear operational parameters make it easier for these entities to do business, and for customs to target their resources towards shipments with higher threat profiles.

The criteria for AEO accreditation include five major sections:

1) *Company information* – volume of business, statistics on customs matters
2) *Compliance record* – compliance history, intelligence information
3) *Applicant accounting and logistical system* – audit trail, accounting system, internal control system, flow of goods, customs routines, back-up procedures, recovery and fall-back, archival options, and information security
4) *Financial solvency* – a record of good financial standing and fulfilment of commitments for the past three years
5) *Safety and security requirements* – security self-assessment, entry and access to premises, physical security, cargo units, logistical processes, non-fiscal requirements, incoming goods, storage of goods, production of goods, loading of goods, security requirements of business partners, personnel security, external services

Many of the AEO program requirements could be applied to accrediting intermediaries with strong IPR protection practices. These criteria could help inform stand-alone programs, and/or the AEO program itself could be augmented to include measures that discourage the shipment of counterfeit goods. Indeed, the AEO program has been extended to specific areas already, for instance, in controlling illegal fishing.[70]

COAC IPR subcommittee

The most developed example of an overarching partnership between customs authorities, rights holders, and intermediaries to specifically fight infringement can be found in the US. The Advisory Committee on Commercial Operation of Customs and Border Protection (COAC) formed an IPR Enforcement Subcommittee to assist it in providing feedback and to work with Customs on IPR facilitation, enforcement, deterrence, partnership, and modernization programs.

As of March 2013, the subcommittee was developing draft recommendations in a number of areas, but nothing has been finalized.[71] Ongoing discussions are centered on ways for the private sector to identify low-risk shipments. These efforts include the possible creation of a Distribution Chain Management (DCM) program aimed at enhancing customs' targeting capabilities. The goal is to improve authentication of suspect goods, similar to the AEO program mentioned above, but specifically targeted towards counterfeits.

Importers who participate in the DCM can expect to see reduced IPR inspections and/or a decrease in the release time for IPR holds. Elements of the DCM under consideration include the following:

- Developing a Unified Trusted Trader program that can certify shipping companies that have proven active in their anti-counterfeiting efforts;
- Developing a pilot *Numeric Identifier* platform based on importer submission to customs of a unique digital identifier, to be provided by the rights holder at shipment origin and logged into a central database; this digital code would identify a shipment as authentic and would be cross-referenced by customs upon inspection;
- Assessing the cost of developing a Business Relationship platform, similar to a social media platform, leveraging its database;
- Promoting the distribution of technologies that assist in the inspection of suspect IPR infringing shipments, such as ultraviolet lights and microscopes;
- Informing rights holders, through outreach to trade associations, that they can assist customs by providing information to determine authenticity through microscopic examination of suspect goods;
- Incorporate Importer of Record Numbers (IOR) for rights holders in Custom's database. Customs is working through legal privacy requirements and determining costs to implement this change, as well as assessing the impact on rights holder resources to enter and manage the IOR numbers.

Transport intermediary action in other areas — sustainability

Transport operators have demonstrated their ability to act together to tackle other crucial industry issues. In a relatively recent initiative beginning in 2011, leading transport operators, shippers, and other key stakeholders from around the world are collaborating to confront environment and sustainability issues through the Sustainable Shipping Initiative (SSI).[72] SSI's 15 members include some of the industry's biggest vessel owners, charterers, and operators, such as Maersk Line, Rio Tinto, Wärtsilä, and BP Shipping. SSI members also include customers like Unilever, classification societies that set technical standards, financial companies and insurers, and issue-area experts like World Wildlife Federation. The initiative has developed a Case for Action, Vision for 2040, Workstreams, and Project Stages.

This type of collaboration suggests that opportunity certainly exists for intermediaries in this industry to band with partners to address common problems. Elements of independent initiatives like SSI could be adapted towards fighting similarly shared threats like counterfeiting and piracy.

2.4 Are these practices working?

While some initiatives have made notable progress, the scope of programs is inadequate at present, given the sector's range of challenges and global nature. The programs detailed above suggest that intermediary engagement must be multifaceted, stretching across numerous types of transport operators. Historically, countries have relied on customs to identify suspicious behavior. In a vastly expanded global marketplace, this method is not proving scalable, and the paradigm needs to shift, as it has in banking and other sectors. Some basic customer due diligence that would pick up the use of stolen identities in paperwork can still be lacking. A US court awarded $8 million to Coach after a finding of contributory trademark infringement by the customs brokerage firm that failed to check the actual identity of its client, despite discrepancies in documentation.[73]

Voluntary programs can be effective, as demonstrated in the express mail arena. In 2011, DHL logged nearly 3,000 IPR records in its SID in the US. It engaged in 50 operations that intercepted a total of 2,600 shipments containing large quantities of counterfeits of various brands. The company has received two letters of commendation from Hong Kong customs regarding its proactive work. Its program to identify counterfeit shippers has resulted in isolating over 400 offending shippers, who have been subsequently blacklisted. These positive outcomes suggest the possibility of continued success in combating counterfeiting. At the same time, the number of counterfeits flowing through express mail continues to rise—and at a faster pace than any other transport intermediary.

In addition, some large cargo transporters have developed internal procedures to hedge against counterfeits. These efforts would be expected of companies that work within KYS/KYC programs or those that have implemented similar due diligence checks of partners. Elements of such programs are also informing related initiatives. For instance, CropLife is educating intermediaries in Africa, and in the Middle East is engaging with stakeholders, supply chain intermediaries, government officials, customs agents, and farmers to deliver training that helps identify and stop the distribution of counterfeit pesticides.[74]

Yet despite multinational efforts to manage transport aspects of supply chains, even sophisticated programs fail to identify weaknesses. More importantly, the simple dearth of established KYC programs designed and implemented by transport intermediaries indicates that much deeper uptake is required. Where recognition of the problem is helpful–as in the warning issued last year by the British International Freight Association to its member forwarding agents to be wary of increasing counterfeit activity—such broad alerts remain insufficient in addressing the problem.[75]

Due diligence practices form the backbone of possible IPR accreditation programs for transport operators. The growing interest in gearing accreditation programs towards counterfeiting offers promising developments, as continuing COAC discussions suggest. Such programs can present business benefits to intermediaries of all types. Optimizing resources for customs authorities also helps target higher-risk shipments for suspected infringements.

The growth of the AEO program indicates that transport operators see value in these efforts. For example, in October 2012, Dutch authorities accredited one of the leading freight forwarders in Europe, CH Robinson, with AEO status. Elements of that and other security programs should be imitated and/or expanded to tackle cross-border transport of counterfeit and pirated goods.

The practices detailed here do not constitute an exhaustive list of current activities but serve to highlight some of the key efforts underway. This chapter underscores the need for transport operators and shipping intermediaries to develop and implement best practices on a broader scale.

2.5 Suggested best practices

Counterfeits that are shipped by large sea container or cargo, and those shipped by overland transport via rail or truck, present challenging vulnerabilities: the ease of hiding fake goods inside large shipping containers; the enforcement challenges created by the sheer global volume of container cargo; and the actions by counterfeiters to mask the true nature of the shipments with false paperwork that is not always easily identified as illegitimate.

As a consequence, the goods transported by these intermediaries are especially hard to monitor. Sea and land have become the favored means for transporting large volumes of counterfeit and pirated materials. At the same time, small parcel shipments delivered through couriers or the postal services have increased dramatically.

Historically, the system has relied greatly on customs to identify suspicious behavior. In a vastly expanded global marketplace, enforcers, intermediaries and rights holders need to develop new solutions as seen in banking and other sectors.

1. **Develop and adopt appropriate voluntary practices to stop counterfeiters' abuse of transport and distribution systems.** This effort can start with adequate due diligence and *Know Your Customer* processes, including quality system reviews for shipping clients and customers. These systems should ensure accurate shipment paperwork, including in-depth background checks for partners operating in problem markets, ongoing customer monitoring, and accurate recording of customer names and identities. Ongoing training of local staff—particularly in high-risk export countries—about current risks from counterfeiting and piracy should become standard due diligence.

2. **Establish contractual terms between transport operators and their clients that specifically call for the (infringing) client to bear the costs incurred from the detention of counterfeit shipments.** Effective due diligence will help identify when counterfeiting is a risk and assure that insurance is in place in the event of a claim.

3. **Put monitoring systems in place to flag shipments of counterfeit and pirated products.** For instance, such systems as DHL's *Intellectual Property Rights (IPR) control system* include notices from rights holders and enforcement authorities (e.g., through track and trace systems). Such systems would also notify rights holders and enforcement agencies at shipment and delivery points when counterfeits are identified.

4. **Establish a provision that requires transport operators to supply electronic shipment information to customs administrations in advance of shipment arrivals.** This provision would enable customs to perform risk assessment and target shipments for further examination. Policies such as those developed by the Global Express Association (GEA) can generate information useful to local and global enforcement authorities for conducting risk-based shipment inspections. Such policies can also track counterfeit transport operators, including both individuals/entities that initiate shipment and actual transport operators, to identify repeat offenders.

5. **Expand the Authorized Economic Operator (AEO) program and other accreditation schemes to include an IPR element.** Adopting higher standards would enable trusted shipper programs and allow rights holders to ship their genuine goods through intermediaries that follow these recommendations.

3. Landlords

Landlords and property owners can become intermediaries in the counterfeiters' supply chain if they rent—knowingly or unknowingly—their property to those involved in counterfeiting activities, whether for production, storage or retail use. If rights holders, trade inspectors and landlords work together to identify and address risks and then implement clear policies, they can effectively deny commercial premises to counterfeiters.

Successful efforts to engage landlords in the fight against counterfeit goods also require ongoing coordination with law enforcement. Some groups have established programs voluntarily and the use of laws and regulations are being applied successfully, but steps to date have been no match for the enormous global use of malls and flea markets for the distribution of counterfeit goods.

3.1 Vulnerabilities to counterfeits for landlords

While instances exist of reputable retail outlets selling trademark-infringing goods, this chapter focuses on counterfeit goods sold at flea markets or in small shops and markets that "specialize" in offering fake goods.[76] The counterfeiters generally do not own the property where these sales take place. The owners of the property—the landlords—are vulnerable because they may not be aware of the illegal activity or they have no idea that they could be liable for these criminal activities.

Landlords are becoming more vulnerable because law enforcement officials, supported by new laws and regulations in some areas, are increasingly targeting them for supporting counterfeiting operations. For example, in 2008, police in New York seized over $1 million in counterfeit merchandise during the city's largest counterfeit bust that shuttered 32 stores, closed three whole buildings on Canal Street, and included the issue of indictments against the landlords.[77] In 2011, a $3 million bust shut down a farmers market in Washington, DC.[78] And in April 2012, US customs authorities broke a record for their largest counterfeit seizure at the Patapsco Flea Market in Baltimore, recovering almost 220,000 counterfeit luxury items worth $47.3 million, including clothing, shoes, jewelry, handbags, DVDs, CDs, perfume, make-up and other personal care items.[79]

The problem is equally severe outside the US. In December 2011, the US and Mexico worked with rights holders to target 66 markets and stores, 55 of which were in Mexico and 10 in South Korea. The raid resulted in the seizure of $86 million in counterfeit products.[80] In January 2012, Singapore police seized $1 million worth of goods that were being sold from makeshift stalls in Choa Chu Kang and Bedok, totalling 176,000 pieces of counterfeit toys and stationery. In February 2013, in Pattaya, Thailand, police conducted a raid to seize $167,000 in counterfeit goods from a market that had just been listed on the Office of the U.S. Trade Representative's "Notorious Markets" list.[81] Although counterfeiting through landlord intermediaries happens primarily through flea markets and malls, a January 2013 raid on an apartment building in Dubai revealed a hidden assembly workshop and 17,000 fake Swiss watches.[82]

While landlords may oversee multiple properties or dozens of tenants and may be more concerned with collecting rent from business owners than monitoring tenant activities, they are nonetheless important intermediaries in the supply of goods. These landlords play an important role in ensuring their premises are not used for illicit activity, including counterfeiting. Some landlords have become more aware of this role and are engaging in practices to deter this activity.

3.2 Current approaches to the problem

Landlord deterrence

In 2002, a number of rights holders joined together with the New York Mayor's Office of Special Enforcement in a public-private partnership to target the City's "vertical flea markets." These large commercial buildings, previously used for storage by the legitimate garment industry, had been illegally subdivided for floor-to-ceiling storage and distribution of counterfeit goods.

A key strategy in this approach was to combine efforts of multiple city agencies, such as the police, fire, sanitation, health and buildings departments with the District Attorney's Office, the Department of Finance and rights holders. The approach relied on combining administrative and criminal code violations with nuisance abatement procedures to deprive counterfeiters and pirates of the premises needed to conduct their illegal businesses. The potential for landlord liability based on tenants' illicit activities served to discourage recidivism and to ensure future compliance and oversight of those properties.

This program, modeled on past successful efforts to address narcotics trafficking, led to agreements with landlords including a variety of terms such as the following:

- unannounced inspections for illegal activity and code enforcement;
- reviews of tenant lists; and
- a requirement that landlords post a bond that could be forfeited in the event of subsequent violations.

Now known as the New York Trademark Task Force, this program has continued operation for more than a decade, and has supplied a model of collaboration that has been adopted in other jurisdictions like Los Angeles. In addition, groups have leveraged efforts to further educate landlords regarding their potential liabilities when tenants engage in the trafficking of counterfeit and pirated goods. They also reinforce steps they can take to prevent such activity on their properties.

Separately, Arent Fox, a law firm representing the luxury brand LVMH, helped create a "landlords program" among property owners in New York City, which later expanded to Miami and Los Angeles. LVMH worked with other brands, legal counsel, and landlords to develop individual best practices for landlords. Arent Fox's landlord program[83] requires "landlords to take specific steps to stop counterfeiting," including:

- hanging signs warning consumers that the tenant is not authorized to sell certain brands;
- specifically prohibiting counterfeiting in the leases;
- hiring a monitor to ensure tenants' compliance; and
- imposing policies to evict any tenant selling counterfeits.

Hanging signs regarding unauthorized sales is only possible in the event that the landlord is already aware that counterfeit goods have been sold. Distributing more general information, however, about counterfeit products to consumers is also a beneficial practice. Monitoring tenants' actions through inspections and in writing specific legal language into leases are also practices that other programs have duplicated with success. The Arent Fox program has resulted only in limited adoption, but landlords could incorporate its practices more generally in other markets to deter counterfeit sales from occurring on their properties.

MoUs and collaboration efforts

Other constructive examples of cooperative actions address the abuse of retail space for counterfeit sales on IPR protection to increase cooperation among all sectors involved. For example, in Thailand, government agencies, representatives of various IP rights holders, and several large shopping centers and malls signed an August 2006 Memorandum of Understanding (MoU) on IPR protection. By targeting strategic areas for action to suppress the sale of counterfeit and pirated goods, the MoU establishes a link between the databases of Thailand's Department of Intellectual Property and its Customs Office.

The MoU fosters a good working relationship and leads to increased efficiency in the fight against counterfeiters.[84] Unfortunately, other reports indicate the initiative has not led to any effective action to combat the sale of counterfeits in the mall; it is indicative that Thailand still has markets on the USTR Notorious Markets list as of December 2012.[85]

Similarly, rights holders and the landlord of China's Silk Street Market established an MoU in 2006 (alongside litigation), but reports indicate that problems worsened in 2007-08, and the market remained on the USTR watch list as of Dec 2012.[86]

Other government-led efforts have been more successful. In December 2012, the Philippines did not appear in USTR's list of "Notorious Markets" for the first time in six years. This success followed a concerted enforcement approach that involved property owners.[87] Over the past years, in the Philippines, lease contracts between major commercial retail establishments and tenants have begun to contain provisions prohibiting the conduct of illicit activities. Additionally, owners of well-known brands have been actively reporting to mall owners and public enforcement agencies on tenants found to be selling counterfeit goods in leased retail spaces, with a request to revoke lease contracts. These efforts have helped increase awareness among owners and managers of commercial establishments. They have helped perpetuate remedies available to landlords against tenants engaged in counterfeiting activities, as well as aiding government enforcement efforts.

Voluntary charter program

One shining example of a voluntary best practice program among landlords is the *Real Deal Campaign*, started by the National Markets Group for IP Protection in 2009 in the United Kingdom.

The program is based on the premise that buying at a market is synonymous with legitimate and enjoyable experiences. Landlords, retailers, law enforcement, and market organizers need to support these shopping benefits while managing out the selling of fakes.

The National Markets Group consulted with its partners (largely IPR organizations and trade associations) to form the program's central feature: a National Markets' Charter, which both physical retail markets and local law enforcement can endorse. As shown in Figure 10, the program involves all stakeholders in the marketplaces, through education and benefits such as best practices, collaboration, and increased legitimacy.[88] A unique feature of the program is the template code of practice given to law enforcement; it is based upon the charter's core principles but can be customized to match local practices or protocol. In 2012, the campaign celebrated its 200th signatory market in the UK.

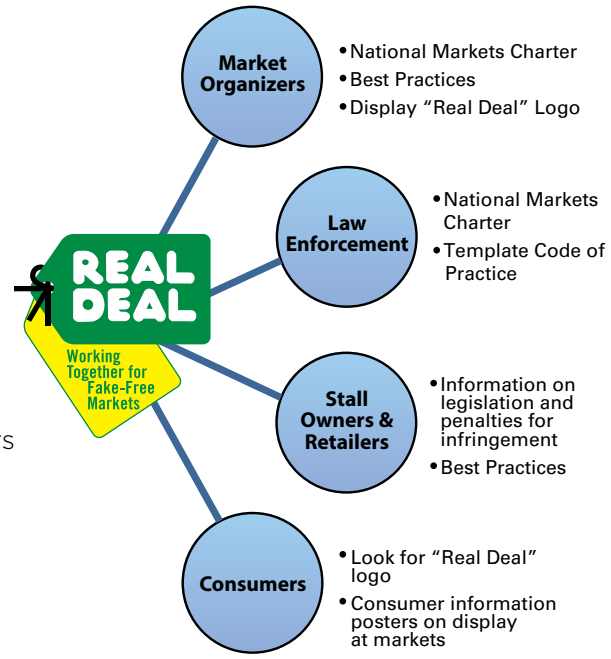


Figure 10: "Real Deal Markets UK" Campaign

3.3 Additional approaches to consider

Anti-drug programs

While some measures address issues related to counterfeit distribution from leased space, lessons can be drawn from established programs that landlords have used to respond to other problems. For example, since the 1980s, pressure has been placed on landlords to assist in the war against illegal drugs. Many of the arguments that have encouraged landlords to proactively report on suspected illicit drug activity can be applied to counterfeiting. One approach has been to list the gains to the property owner in avoiding problems.

Benefits to landlords from better policing of their properties include:

- boosting property values;
- fewer civil penalties;
- less frustration in dealing with dangerous tenants;
- lower risk of related crimes.

In 1992, a law firm for the City of Portland, Oregon, designed one such program relating to drug trafficking, funded by the U.S. Department of Justice. The Hollywood, Florida, police department adopted the program in 1997, presented it to local landlords, and has updated and promoted it ever since.[89] The 42-page guide details the following:

- ways to screen for warning signs in interviews and application materials;
- guidelines for how to coordinate with law enforcement to avoid repeated calls or problems with tenants; and
- a template for an addendum to leases to ensure prompt eviction in the event of drug-related criminal activity.

Small landlord associations promote other best practices or screening efforts, which could apply to a larger-scale program on counterfeit goods. Similarly constructed programs to educate and equip property owners on the indicators of high-risk tenants for counterfeit activity—and on the benefits of eradicating such activity—would strengthen cooperation between landlords and law enforcement.

3.4 Are these practices working?

The programs above indicate that to be successful, efforts to engage landlords in the fight against counterfeit goods also require ongoing coordination with law enforcement, as demonstrated by the New York Trademark Task Force. Some of the voluntary programs and laws and regulations are successful thus far, but they are no match for the enormous global use of malls and flea markets for the distribution of counterfeit goods.

The *Real Deal* markets program in the United Kingdom enjoys a healthy level of participation, with 369 markets enlisted as signatories. The program has several strengths. The Real Deal logo offers a visual badge of legitimacy for participating markets. Additionally, coordinating tools for law enforcement encourage market organizers to collaborate with local governments, improving the effectiveness of both groups. Finally, by educating consumers about their choices, both through display of the Real Deal logo and distribution of pamphlets on counterfeit goods, the program addresses demand as well as supply. This program's model could be expanded to include retail malls and informal markets in other countries.

The Arent Fox landlord program brings awareness of the issue to landlords, but due to its specific application to tenants that have already been found guilty of selling counterfeit goods, some of its best practices may be too specific to be widely applied. This does not mean, however, that the program is ineffective in deterring counterfeit activity. The program has spread within the United States, but its best practices may need to be amended for wider use.

Government-backed MoUs signed in China and Thailand are encouraging, but effective adherence and enforcement have been lacking. Both markets continue to struggle with exceptionally high volumes of counterfeit goods. Landlord efforts in the Philippines have focused on strengthening lease language and increased detection of counterfeit goods being sold by tenants. No widespread program exists, however—such as a set of best practices or training for cooperation with law enforcement—that allows for easy replication of success.

Existing approaches have had enough effect to remove offending markets from the USTR Notorious Markets list; markets could further capitalize on this success, however, by developing and implementing a more formal program like The Real Deal. The passage of the law amending the IP Code of the Philippines is expected to significantly improve anti-counterfeiting and piracy efforts. Although most landlord associations are small, with education, best practices, and other tools, they could assist their members in protecting property values and reputation.

Finally, the focus thus far of efforts to deal with landlords as an intermediary has been on the landlords renting to retail sellers. As these efforts prove successful, more attention needs to be paid to landlords of manufacturing space, storage space, and potentially, office space used by counterfeiters and criminal networks.

3.5 Suggested best practices

Landlords and property owners can become intermediaries in the counterfeiting supply chain if they rent—knowingly or unknowingly—their property to those involved in counterfeiting activities, whether for production, storage, distribution or retail use. If rights holders, trade inspectors and landlords work together to identify and address risks and then implement clear policies, they can effectively deny commercial premises to counterfeiters.

Successful efforts to engage landlords in the fight against counterfeit goods also require ongoing coordination with law enforcement. Some groups have established programs voluntarily and the use of laws and regulations are being applied successfully, but steps to date have been no match for the enormous global use of malls and flea markets for the distribution of counterfeit goods.

1. **Increase landlord education: Explain the risks and benefits of participation in voluntary programs to avoid renting to criminals.** Voluntary efforts are most successful when landlords understand they can avoid prosecution, penalties and loss of property value, or when they see that they can attract customers by marketing their place of business as a "counterfeit-free" marketplace. Given the large-scale operations in giant markets and malls in some countries, more effective coordination between landlords, shopping centers, IP rights holders and law enforcement might be achieved through a voluntary charter. The UK's *Real Deal Campaign* and the MoUs used in counterfeit markets in China and Thailand offer working examples of this initiative.

2. **Landlords should include lease provisions specifically prohibiting activities related to counterfeit goods; they should evict tenants in the event of counterfeit-related criminal activity.** Increasingly, governments require landlords to perform due diligence checks on tenants for immigration violations or money laundering activities. Screening prospective tenants' backgrounds and financial information carefully should be part of standard due diligence regarding counterfeiting and piracy as well. The *Landlord Training Program: Keeping Illegal Activity out of Rental Properties* by the City of Hollywood, Florida, is an example of how landlords can more effectively guard against illegal activity on their premises.

3. **Landlords and market administrators should require periodic inspection of lessees' shops and stalls for obvious counterfeit goods.** Where counterfeiting activity is suspected, these inspections should be combined with reporting mechanisms to inform rights holders and law enforcement. Where counterfeit sales are regular occurrences, operators should post warning notices for consumers regarding the consequences of selling or purchasing counterfeit goods. Guidelines developed by Arent Fox, for example, provide a model approach for providing landlords with specific steps to stop counterfeiting. Conducting regular inspections and writing specific legal language into leases are other practices that have been duplicated with success.

4. **Increase the use of nuisance abatement laws and public-private task forces to target problem landlords.** Cooperative relationships between multiple government agencies and rights holders have proven effective at addressing landlords who continue to facilitate illegal activity on their premises, and nuisance abatement laws are useful tools.

Part II: Online Intermediaries

The explosion in access to and use of the Internet by individuals, as well as a wide range of organizations and businesses, continues to rapidly change daily and commercial life. Consumers can mobilize the Internet's power instantaneously and globally to find, pay for and arrange the delivery of physical items. Consumers can receive and enjoy digital entertainment, education and other information directly from their phone, tablet or computer. This dramatic influx of technology has clearly provided enormous market benefits and opportunities.

Intermediaries also play critical roles in delivering Internet services. A complex, inter-connected intermediary network is involved in delivering a seamless range of online services to consumers, businesses and other entities.

As in the physical world, criminal actors have seized opportunities to gain further profits from counterfeit and pirated goods. Legitimate providers in these digital supply chains have taken positive steps to guard against online counterfeiting and piracy. The scale and nature of infringements, however, have challenged intermediaries to continually improve their defenses to prevent their infrastructures and services from being hijacked to support illegal activity.

Part two of this paper groups the activities of online intermediaries into three categories. Often, however, a single commercial entity may be providing more than one of these services.

1. **Sites, platforms and portals.** This category includes a wide group of services that act as platforms for users to make offers and sales or share content or links. It includes marketplaces, like EBay and Amazon, the Apple App Store and Android Play Store for mobile apps; user-generated content sites like YouTube and Vimeo; social networks like Facebook and vKontakte; and cyberlockers like Hotfile and Uploaded. This group also includes websites, like the Pirate Bay, that connect users of peer-to-peer (P2P) networks. Some of these are the biggest names and most popular services on the web, used legitimately many millions of times daily. But they all are vulnerable to massive abuse through counterfeiting and piracy and have to continually improve their systems to prevent such abuse. Others, such as the Pirate Bay, are simply dedicated to piracy and counterfeiting and encourage users to fill the sites with infringing content.

2. **Infrastructure providers.** These services are the Internet's technical backbone on which all web services are built and delivered. There are three main services covered in this category. Hosting providers, like Rackspace, offer the server space to store either a whole website or simply some specific content, which is then displayed on other sites. Domain registries, like Nominet and their registrars like GoDaddy, provide names for websites and connect them to the IP address of the hosted site. Internet access providers, like British Telecom, that connect users to the Internet are the final crucial link, as all data must pass through their systems to reach end users and consumers.

3. **Search, online advertisers and payment processors.** The economic viability of the services running on the Internet's infrastructure depends on these support services to find an audience and generate revenue. This section focuses on search as the critical function that enables discovery within the network across all of these sites; advertising, both as a means of discovery and as a source of revenue; and direct payment, using credit cards and other payment services like Paypal.

4. Sites, platforms, portals and services

4.1 Online marketplaces

E-commerce marketplace websites provide businesses and consumers with a thriving online marketplace through which to offer, sell and purchase goods and services. These sites use a range of business models for consumer-to-consumer, business-to-consumer, and business-to-business transactions.

The Internet intermediaries discussed in this section are those online marketplaces that do not take title to the goods or apps being sold.[90] Instead, they are primarily wholesale and retail marketplaces, auctions and coupon sites. Well known examples include eBay and Taobao. These companies have a contractual relationship with the traders offering the goods. They are in a position, through both their terms of service and their compliance procedures, to incentivize trustworthy behavior and to remove those that misuse the service to sell counterfeits.

Alongside the billions of legitimate daily online transactions—and despite being some of the best known and used services on the Internet—these services have become vulnerable to misuse, with large volumes of counterfeit products and apps connecting consumers to infringing content on these sites.

4.1.1 Infringement in E-commerce

For physical items, counterfeiters infiltrate both large and small commercial exchanges on e-commerce sites. In blurring the distinction between real and fake products, they succeed in selling staggering quantities of infringing items.

A report examining online offers of five luxury brands found these brands to be offered on 1,100 suspicious e-commerce sites. These sites enjoyed almost 120 million annual visits, representing almost half of the traffic to legitimate sites of the brands in the study.[91] A study of 12 legitimate, global e-commerce sites by Yellow Brand Protection discovered 2.8 million advertisements for counterfeit goods, representing a potential turnover of EUR 1.2 billion per month.[92]

Direct counterfeit sales

When users search for products online, they can experience difficulty distinguishing between legitimate e-commerce sites and those exclusively offering fake goods. A study by the Nielson Company and Mark Monitor found that one in five consumers has unintentionally shopped on a site designed to offer counterfeit products.[93]

Identifying and shutting down websites that sell only knock-off goods is a massive undertaking. Removing their infrastructure and support services will be addressed in later chapters. Policing the larger, legitimate marketplaces such as Taobao, eBay, or Amazon presents a different challenge for identifying and removing infringing content. These marketplaces offer a vast number of legitimate goods and give sellers a great deal of autonomy. For example, the e-commerce website eBay processed $75 billion in sales in 2012 from customers in 190 countries.[94] In addition to the massive number of transactions on eBay, eBay auctions and other auction sites begin the moment they are posted, giving virtually no time to review postings for any problems.

eBay's history with fake goods is mixed. In 2008, an independent review of the site's 2.7 billion auctions identified only 0.15% as potentially counterfeit, but for some brands, this proportion may be much higher. In 2004, Tiffany & Co. claimed that only 5% of its products sold on eBay were genuine. The company consequently engaged in a four-year lawsuit against eBay. Tiffany did not win that lawsuit. eBay was found not to be liable for the counterfeit goods offered among its millions of auctions. eBay was, however, required to remove counterfeit items reported by brand manufacturers. On the other hand, eBay lost a similar case in 2010 in French courts against Louis Vuitton.[95]

Self-reported statistics from online marketplaces are indicative of the scale of the problem. Chinese marketplace Taobao announced that it removed 45.2 million counterfeit products from its service in the first six months of 2012.[96] Between 2010 and 2012, Amazon reported that it blocked 5,900 sellers suspected of infringement, though it is unknown how many may remain operative on the website.[97] Websites and buyers now face so many difficulties discerning between real and fake goods that new websites have emerged that "specialize" in the auction of authentic brands.[98]

Mobile apps

Mobile application (app) marketplaces, valued at $20 billion in 2013, represent another burgeoning e-commerce intermediary that can be used to enable infringement.[99] Some apps facilitate user access to infringing content and are used to gain access to the various services discussed in the next chapter, such as P2P file-sharing sites for uploading and downloading materials, as well as sites for streaming, stream ripping[100] and searching. Hundreds of apps offer infringing downloads, and many of them can be found on the major app stores operated by Google, Apple and Microsoft.

Like many other e-commerce services, some app stores do not pre-approve app content. Unscrupulous vendors, therefore, are free to include or update apps that facilitate copyright infringement, encourage purchases of counterfeit goods, or utilize unlicensed movie content, images, music, and video clips.

Rights-holder groups are in the process of expanding app monitoring in response to recent studies. IP Lasso, for instance, found 90% of 100 widely available apps (through Google Play and Apple's iTunes app stores) mentioning Oscars or the Academy Awards contained content that may not have been authorized.[101]

On a more positive note, some notice and take-down schemes are currently operating on some app stores (including on Google Play and Apple stores). In these cases, the companies notify offending app providers and then remove the sites from the store. Today, the time taken to remove apps from the stores is often unacceptably long.

4.1.2 Current approaches

E-commerce intermediaries and partners are increasingly collaborating with rights holders to test approaches that deter infringement, including government-assisted frameworks, joint initiatives and individual corporate practices. The following section provides an overview of these efforts.

European Commission's Memorandum of Understanding (MoU)

One prominent example of joint efforts between rights holders and e-commerce intermediaries is the publication in May 2011 of an EU Memorandum of Understanding (MoU) on the Sale of Counterfeit Goods via the Internet. The MoU is the result of a joint voluntary effort by leading rights holders and Internet platforms to reduce the sale of counterfeits via e-commerce platforms in EU. The principles currently in place concern the mutual responsibility of rights holders and e-commerce sites to work together to address counterfeit sales and provide guidance on how to address and handle complaints.

The European Commission oversaw the negotiation process as an alternative to potential legislative action, which various parties were contemplating at the time. Its stated purpose is "to establish a code of practice in the fight against the sale of counterfeit goods over the Internet and to enhance collaboration between the signatories including and in addition to Notice and Take-Down procedures."

While non-binding, the MoU outlines a series of principles and commitments applicable for an initial "trial" period. A code of practice would apply for signatories including Nike, Mattel, Unilever, P&G, Microsoft, Amazon, and eBay, among others. In April 2013, the MoU

signatories and the European Commission agreed[102] that they should periodically review whether the MoU is still adequate to combat online offers of counterfeit goods, and that a second review would take place at the end of 2014. Notably, the MoU imposed a moratorium on new litigation between signatories concerning matters covered by the MoU for a minimum of the first year of the MoU's implementation.

MoUs between industry associations and Taobao

Taobao, a Customer-to-Customer marketplace in China, had been a fixture on USTR's "Notorious Markets" list until its removal from the list in December 2012, based on its increasing commitment to anti-counterfeit programs. While Taobao has unilaterally driven most of these programs, in September 2012, Taobao signed an MoU with the Motion Picture Association (MPA) focused on stringent removal of any listings or merchants that infringe upon MPA members' copyrights. While this MoU addresses only certain segments of infringing Taobao listings, the measures could be replicated for other listings on Taobao and elsewhere. The agreement includes the following:

- Removal of infringing products from listings.
- Working with law enforcement to pursue persistent offenders.
- Ensuring all sellers have a valid government-issued "Publication License."[103]

In August 2013, Taobao signed a separate MoU with the International AntiCounterfeiting Coalition. The two organizations are currently working to implement the MoU terms, which focus on improving the impact of Taobao's process for identifying and removing listings for counterfeit and other illicit goods.

Internal corporate policies to deter infringement

Some e-commerce businesses have developed internal best practices and policies with respect to counterfeit and pirated products. eBay's Verified Rights Owner (VERO) program is the best known and most developed example, which according to eBay, "allows intellectual property rights holders to ask eBay to remove certain listings that offer items or contain materials that infringe on their intellectual property rights."[104]

Allegro, a major auction site in Poland, has created and launched a program called Cooperation in IP Rights Protection that allows rights holders to notify Allegro of infringement, whereby the site will take steps to remove offers of counterfeits.[105] Overstock.com also takes steps to stop sales that violate its user agreement. Overstock's policy is "to disable access to infringing materials, and to terminate access of repeat infringers to the site."[106] The hope is that these and other e-commerce sites will implement and further develop corporate policies to combat counterfeiting and piracy.

The Chinese online marketplace Tmall takes this approach one step further. Since its formation in 2003, the website (then owned by Taobao) faced harsh criticism as a hotbed for the sale of infringing goods. After it was listed as a Notorious Market in USTR's Special 301 Report, the website split from parent company Taobao and immediately announced more stringent measures to prohibit fake goods on its site.

Tmall's approach goes beyond most other voluntary e-commerce actions by requiring a cash deposit from each vendor as an authenticity certification. If the merchant is caught selling fake goods, then the merchant loses this deposit.

In addition, Tmall offers consumers a refund of five times the price they paid if they receive counterfeit goods from a merchant–a cost that Tmall then requires to be reimbursed by the merchant.[107]

Finally, if a merchant receives frequent complaints or refund requests but Tmall lacks definitive proof necessary to shut down the store, Tmall employs "secret shoppers" to essentially conduct a "raid" by procuring samples of the good. While the program has not seen overnight success in deterring counterfeits, these enforcement efforts are laudable.

4.1.3 Additional approaches to consider

Online seals, trust marks, and certifications

In many marketplaces, the potential for fraud and abuse has given rise to certification badges and trust marks that are used to assure consumers that they are getting the "real deal" and/or to build their trust in whatever service is provided. Such trust marks are now increasingly issued on the Internet.

Among the most ubiquitous of these marks are security indicators, like the original VeriSign SSL seals now offered through Symantec under its "Norton Secured" brand. The seals convey to users that a website has been verified for security and data encryption and that it is safe to enter payment data. Symantec states that "a trust mark is a form of advertising that communicates to online shoppers that a website meets the requirements of a trusted third-party, which helps them shop with confidence."[108] Other companies offering comparable programs include McAfee, BBB and TRUSTe.

While not entirely focused on counterfeiting, SSL certification is designed to build overall customer trust. Once the website procures the badge or seal, the end user can validate it with a single click-through to the issuer. This concept could be replicated for anti-counterfeiting generally or for specific brands.

An example from the music industry is the *Music Matters* initiative. This initiative—involving artists, retailers, songwriters, labels and managers— highlights the value and significance of music while educating consumers about where to legally find and enjoy digital music. Launched in March 2010 in the UK, the *Music Matters Certification Scheme* helps music fans make ethical and legal choices when looking for digital music online; UK retailers and partners have widely adopted this initiative. The campaign has also been rolled out in Ireland, the US and Australia, and in New Zealand. The sites provide lists and links to a wide variety of websites and platforms offering licensed music.[109] These websites then help fans find the tracks, albums, and formats they want, at the price point they can afford.[110]

Apart from the initiatives described above, customer ratings present other possibilities. For example, Google issues its Trusted Store badge to participating stores that reach a minimum standard of ratings for customer service and shipping reliability. This badge is interactive and is updated as ratings change. It is also verifiable by clicking on the badge to go to a Google verification site. This framework, and customer involvement, makes the badge more dynamic.

A brand reliability or authenticity rating could also be integrated into an anti-counterfeit program. On the conditions that companies provide adequate information to consumers and that appropriate and sector-specific monitoring criteria are in place, this program could reward legitimate e-commerce sellers, gather information about infringement, and educate consumers on the prevalence of counterfeit goods.

Within their own larger e-commerce environments, Amazon and eBay have similar "trusted seller" ratings programs: eBay's "Top Rated Plus" seal indicates a seller's trustworthiness based on shipping time, returns policy, and customer feedback; Amazon's rating system incorporates reviews on all aspects of its products and services.[111] These methods are not fool proof, however, and they face the same problem that authentication marks face in the physical world: the seals of approval themselves can be counterfeited or manipulated using false feedback.

4.1.4 Are these programs working?

An evaluation and review of the EU's Internet MoU was scheduled for mid-2012, but discussions led to an extended evaluation period. The evaluation report has yet to be published.[112] In the immediate term, the MoU has been important in opening avenues for dialog, cooperation and collaboration in dealing with the Internet sales of counterfeit goods. Meeting reports show interest from new entities in participating as signatories—a positive indicator of the program's success and prospects. Contacts between the participating e-commerce platforms and rights holders have improved, although some signatories have asked for more transparency. It should also be noted that the MoU is the EU's first pilot initiative to address Internet sales of counterfeit goods.

Taobao's recent MoUs with rights holder organizations are encouraging, as they represent collaborative action, whereas the company was previously conducting primarily independent, anti-counterfeit efforts. These MoUs have not been in effect for long enough to evaluate their impact, but results so far suggest that rights holders working together with e-commerce actors can achieve increased accountability and information sharing.

Tmall's stringent policies also have not eliminated its problem with merchants' counterfeit sales. For example, just months after implementation of its new program, Tmall merchants with the "Genuine Guarantee" certification (indicating they had been inspected by Tmall) were found to have successfully sold 1,500 fake Casio watches valued at approximately $150,000. Allegations have also identified Tmall's failure to uphold its "five times" refund guarantee, returning only twice the price in some high-volume cases.[113] Time will determine whether Tmall can enforce its strict policies at the level required for merchants to take them seriously. Innovative approaches, however, such as incentivizing customers to report fake goods, are valuable precedents for other e-commerce sites to consider.

App marketplaces are in the early stages of addressing similar issues. The explosive growth of apps means that the sheer volume of issues will overwhelm online web form and email correspondence models of handling infringement. App marketplaces can learn from other more established e-commerce practices and benefit from adopting the recommendations below.

4.1.5 Suggested best practices

This paper summarizes voluntary efforts by online marketplaces to prevent counterfeiting and piracy both on their own and in cooperation with rights holders and governments. The programs also show government's important role in facilitating collaboration. These examples suggest important avenues for developing even more effective programs and involving broader stakeholder constituencies. They also show that measures to counteract transactions of counterfeit goods and pirated material have struggled to keep up with rapidly changing, online e-commerce practices. Clearly, this review supports the premise that vulnerabilities can be addressed through focused, collaborative efforts.

1. **Outline clear *Terms of Service* prohibiting use of a site to sell or otherwise trade in counterfeit or infringing property.** Such terms will enable the prompt removal of infringing products or content. Many e-commerce site policies do disable access to infringing materials on this basis. Terms of Service can also be used to incentivize trustworthy behavior depending on the business model of the service.

2. **Encourage stronger enforcement of the *Terms of Service* between site owners and traders, with increased cooperation between service providers and rights holders.** Terms of Service agreements are only as effective as the efforts made to enforce them. E-commerce site owners must put in place mechanisms to terminate or deter repeat violators of the Terms of Service. Upon receipt of adequate notice from a rights holder, site owners should also implement rapid takedown systems.

3. **Implement due diligence checks by e-commerce site owners to ensure a basic understanding of who is trading on their site.** Checks should include contact information listing true name and street address, as well as banking details or other identity checks and verification practices. These steps could form part of wider verification programs to identify illegal activities, which, in turn, deter counterfeiting and other infringing conduct.

4. **Adopt appropriate, automated risk management tools to identify high-risk behaviors and potential red flags.** Given the magnitude of Internet transactions and the wide variation in online business models, appropriate automated technologies are essential to enable e-commerce site owners and rights holders to identify infringing activities. Such technologies will help them undertake fair and rapid processes for preventing continued infringements.

4.2 Content-sharing services

This chapter looks at content-sharing services like YouTube, Facebook and Dropbox, as well as other platforms that enable the sharing of digital works.

In the digital environment, creative works such as music and films, books, games, images, and magazines can be shared either through sending files to run on a user's device, known as "downloading," or through viewing or listening to the file from its location, which for music and films is known as "streaming." Websites, mobile apps and other software tools can be used as powerful platforms for either of these activities, or to share links to enable these activitites.

Online users rely on these tools every day to create and share a profusion of original, non-commercial content, such as personal blog posts, status updates, personal photos and home videos. Commercial content is also available with the owner's consent in different ways depending on their business model. All of this information contributes greatly to the vibrant online experience we know today. This evolution in technology represents a revolution in citizens' ability to publish to each other at scale, making some of these the most popular platforms on the web.

Photosharing Sites	Podcasting	Social Networking Sites	Video Content or File-Sharing
• Kodak Gallery • Flickr • Instagram • Snapchat	• iTunes • Feedburner • iPodder	• Facebook • Bebo • Twitter • LinkedIn • Google+	• YouTube • DailyMotion • Metacafe • FilesTube
Blogs	**Text-based Collaboration Formats**	**Instant Messaging**	**Group-based Aggregation or Bookmarking**
• Blogspot • BoingBoing • OhmyNews • LiveJournal • Windows Live Spaces	• Wikipedia • Wictionary • PBWiki • Google Docs	• Skype • Google Chat • Trillian • iChat • WhatsApp	• StumbleUpon • Digg • Reddit • del.icio.us • Buzzfeed • Pinterest

Figure 11

While almost everyone—from kids to grandparents—uses these platforms legitimately (see Figure 10), still others abuse them openly, from bullying and hate speech to images of child abuse and invasions of privacy and copyright infringement.

This chapter looks at the efforts of services that are not in the business of offering copyright infringing content, but where it nevertheless may appear alongside larger volumes of entirely legitimate content/offerings. It also addresses those services that have such a large volume of infringing content that they are clearly pursuing a business model based on piracy. In these cases, removing the infrastructure and supporting services that enable them to operate may be the only effective means of preventing abuse.

4.2.1 Infringement and piracy

While the majority of platforms listed above have business models based primarily on legal content, all such services are vulnerable to copyright infringement. The risk varies dramatically from service to service, but in the most extreme cases, some services operate a business model that is clearly based on facilitating or inducing copyright infringement. Depending on the circumstances and the jurisdiction, these sites are considered primary or secondary infringers.

To get a sense of the scale of the problem, a 2011 survey identified an average of 140,000 or more active links daily to infringing movie and television titles across a sample of 500 websites: 75% of the sites offered direct download; 15% offered both download and streaming video; and 12% offered just streaming.[114]

The discussion below addresses copyright infringement issues associated with four different categories of file and video sharing services: user-generated content (UGC) sites, social networks, cloud storage, and BitTorrent sites.

User-generated content sites

User-generated content or "UGC" sites like YouTube, DailyMotion, Vimeo, and Youkou are impressive platforms for users to share video content with the world. A great deal of this content is legitimate, and platform owners either own the content or have licenses with rights holders.

These site designs, however, are also vulnerable to the illegal upload of unauthorized, copyright-restricted content, including short clips and full-length films, TV shows and music videos. When YouTube first became popular in 2006, users uploaded large volumes of copyright infringing videos to the site. The activity led to a number of copyright holders' litigation threats, including a lawsuit filed by Viacom and a class action brought by the English Premier League.

Recognizing the need to promote technological innovation while respecting intellectual property rights on UGC sites, in October 2007, a group of copyright owners and operators of major UGC sites (not including YouTube) announced the formation of a set of best practices known as the "UGC Principles." A key tenet of the UGC Principles is that UGC sites voluntarily agreed to deploy commercially reasonable, highly effective state-of-the-art filtering technology with the goal of eliminating infringing content on UGC sites. Around the same time as the UGC Principles were released, YouTube announced that it would make filtering technology available to copyright owners on its site.

Thus, by late 2007, the use of automatic content-recognition filtering technology to promote innovation and protect copyright had become an industry standard on a number of UGC sites in the US and throughout Europe. Major UGC sites in China, including YouKu and Tudou, later adopted similar technologies.

While filtering technology has prevented illegal content from overrunning UGC sites, shortcomings in the filtering technology, incomplete filtering databases, and uploaders' attempts to circumvent technology still enable large volumes of infringing content to be uploaded every day.

Social networks

Social networks, such as Facebook, Twitter, Bebo, Instagram and Google+, allow users to upload content and share videos, music, photos and other content with network users. These networks can contribute to IP infringement when users share copyrighted material.

While social networks are not presently the most significant contributors to online infringement activity, the U.S. Trade Representatives (USTR) Notorious Markets List currently includes one social network (vKontakte or "vK"), as well as a portal site that includes a social network (Zing.vn in Vietnam). According to the USTR, both of these

sites are forums for commercial-scale piracy of copyrighted works, including, music, film and television shows. The Notorious Markets List identifies a small number of online and physical markets around the world that raise concerns about IP infringement because their scale is large enough to cause economic harm to US and other IPR rights holders.

Significantly, the vK site includes functionality that enables users to upload and share music and videos, and it is a major online source of unlicensed content. The vK website itself allows users only to stream content, not download it; however, vK makes its content database accessible to third parties such as app developers, which enables them to distribute unlicensed content via mobile platforms. vK has not implemented content-filtering technology, and only removes individual links as a result of notices, rather than disabling access to the content itself.

In a series of successful lawsuits, Gala Records, a Russian record label, has obtained judgments totaling more than 1 million rubles against vK due to vK's role in infringing Gala's copyrights.

Cloud storage

Cloud storage services such as Dropbox offer users the ability to upload and store content online. These services are used primarily for legal purposes. Although few controls exist on how widely content can be shared, most users do not allow their stored content to be shared (so called "dumb lockers"), or they only share their materials to a workgroup or colleague. Users may access services like Onedrive, for example, through a website in a browser or through a mobile app. Or these services may appear simply as additional folders alongside those containing files stored on a device. When a user shares a link to a file, Dropbox checks it against a list of files for which the company has received DMCA takedown notices. If Dropbox finds a match, it disables the link.[115]

On the other hand, when content is uploaded and made available to anyone without restriction, the service can quickly become abused for illegal sharing of infringing files. Some services are even designed to incentivize end users to distribute copyright-infringing content to others. This type of service, now commonly known as a cyberlocker, is essentially a distribution hub for copyright infringing content.

The most notorious cyberlocker was Megaupload, which, the US government alleged, created a business model based on copyright infringement. Megaupload offered users financial incentives to upload popular copyright infringing files. At the same time, the site charged subscription fees for "premium" account users that enabled fast and unlimited downloads of files on Megaupload. The site also generated revenue from online advertising. While users could upload non-infringing content to Megaupload, the vast majority of popular files on the site were copyright-infringing.

Megaupload operators were indicted by a US federal grand jury for criminal copyright infringement in early 2012, and the site was seized.[116] In the indictment, the US government alleged that website operators had engaged in a massive criminal conspiracy to infringe copyright and to engage in money laundering. According to the indictment, the defendants' acts caused over $500 million in damages to copyright owners and netted the defendants over $175 million in illegal gains.

At its height, Megaupload was the 13th most heavily used website in the world, accounting for over 4% of all worldwide Internet traffic, and drawing over 1 billion users during its history. Following the indictment and shutdown, many other cyberlockers either went out of business or moderated their policies to decrease their risk of liability. The case itself has still yet to be heard.

In a case involving another cyberlocker, in August 2013, a US district court judge granted partial summary judgment against Hotfile in a copyright infringement suit filed by five major US film studios. The court found Hotfile vicariously liable for millions of copyright infringement acts by its users and ruled that Hotfile was not eligible for safe

harbor protection under the US DMCA.[117] In December 2013, the district court entered final judgment ordering Hotfile to pay plaintiffs the amount of $80 million and to cease operation unless and until Hotfile implemented effective content recognition filtering technology. Hotfile shut down following the entry of judgment.

BitTorrent

BitTorrent is a peer-to-peer (P2P) protocol that became highly popular several years ago, shortly after the demise of the Grokster and FastTrack P2P networks. The developers of those networks were held potentially liable for copyright infringement in the landmark 2005 *Grokster* decision by the US Supreme Court mentioned in the "key principles" section of the introduction to this paper.

In P2P infringements, users are connected to each other by file-sharing P2P protocols like BitTorrent, eDonkey and Gnutella. These protocols typically offer free, downloadable software that facilitates file exchanges among individuals using their own computers. The specialized P2P software program interconnects end-user computer nodes (peers) via the Internet and allows users to search for files existing on other computers connected to the P2P network. These files typically contain copyrighted material such as books, music, movies, and games. BitTorrent sites help users find and connect to files stored across the P2P network.

Today, BitTorrent is the most popular P2P file distribution system worldwide, and the protocol is one of the highest users of Internet bandwidth. In principle, BitTorrent can be used to share any digital content, including public-domain content or content that the author uploads and licenses to other BitTorrent users. In practice, the design of BitTorrent lacks any abuse controls, and the actual use of BitTorrent is overwhelmingly dedicated to copyright infringement.

A 2011 study by Envisional (now known as NetNames) concluded that over 63% of BitTorrent usage was copyright-infringing (and most of the rest was pornography); when pornography was excluded, the figure jumped to more than 99%. The most recent study by Netnames found that in three key regions (North America, Europe and Asia Pacific), the absolute bandwidth consumed by the infringing use of BitTorrent comprised 6.692 petabytes of data in 2012, an increase of 244% from 2010. In the same three regions, infringing use of BitTorrent in January 2013 accounted for 178.7 million unique Internet users and 7.4 billion page views.[118]

Many BitTorrent websites are dedicated to connecting users to pirated content and either encourage or take no effective steps to contain the problem. Courts have found BitTorrent site operators liable for copyright infringement, as outlined in the "key principles" section of the introduction to this paper, including a criminal action in Sweden against operators of the notorious BitTorrent site known as The Pirate Bay. The European Court of Human Rights in Strasbourg ultimately upheld this decision.

As with other forms of widespread infringing activity, these sites can generate substantial income for both themselves and the direct infringers, as well as cause substantial damage to the affected rights holders. In the Pirate Bay case in Sweden, for example, prosecutors estimated that the site generated more than $1.4 million in advertising revenues a year.[119] On the basis of revenues and the value of the infringing activity, Swedish courts imposed a $7 million fine on the defendants found guilty of criminal copyright infringement.[120]

Criminal liability was also found in Finland with the Finreactor service, and civil liability was found in the Netherlands against Mininova. More recently, a US federal court of appeals upheld a ruling that the operator of a BitTorrent site IsoHunt was liable for inducing copyright infringement. In addition, courts in numerous countries have ordered ISPs to block access to BitTorrent sites based on their overwhelmingly infringing nature.

4.2.2 Current approaches to the problem

The complexity of the issues surrounding digital piracy and the diverse nature of the services outlined in this chapter preclude an easy solution to halting infringement on these end-user networks. In the case of sites such as Pirate Bay and certain others referred to above, whether such sites are infringing has long since been settled in numerous jurisdictions. These sites now operate on the fringes of the Internet, underground and anonymously, frequently changing location–so that direct action against them has become very difficult. Yet, clearly, when diligent operators take care to align controls and incentives with lawful behavior, and they use technology to manage risks—both directly and with the help of rights holders—the system can realize substantial improvement. Even where some of these measures are in place, more must be done. Some of the programs detailed below suggest avenues for further collaboration.

Notice and takedown

Acting to stop abuse once it is identified is common sense, and most societies and legal systems expect such a response—in the physical world and online. To address abuses to the services in this chapter, the practice of "notice and takedown" is a fundamental, frequently used tool. As noted in the "key principles" section of this paper, services that are notified about infringement but fail to act generally face some form of liability.

Typically, rights holders or their designated agents, including trade associations representing rights holders, alert service providers of infringing content on their services. Such notices typically specify the IP rights in question (copyright or trademark), the location and infringing nature of data or material, and a request to promptly remove or block access to such items. The millions of notices registered every year reflect the magnitude and frequency of the infringement problem.

Naturally, rights holders expect that Internet services should promptly take down infringing content or block access to it upon notice. While these companies act upon millions of notices, their response varies significantly. Slow responses result in substantial, continued infringing activity even after a notice is sent, and blocked material is quickly re-posted by the infringer when "stay-down" obligations are not reinforced (see further discussion below). This process is particularly important for pre-release content, where the main market for the work can be quickly destroyed if it emerges or continues to be available online.

To be effective, it is essential that legislators incentivize services to implement an efficient takedown policy. If services promptly take down content upon rights holders' notice or upon becoming aware of facts or circumstances in which the infringing activity is apparent, and certain other criteria are met, they are protected from liability for monetary damages. In many countries, the adoption of this policy is a pre-requisite for certain limitations on liability, so-called "safe harbors":

A notice and takedown regime must include several important procedural/technical points in order to be effective, including:

- no court order or other formality should be required for sending a notice and the service provider should have legally-binding knowledge of the infringement in order to be required to take down the notified content;
- the service provider must cooperate in providing automated methods for rights holders to locate infringements, for example, by making available automated interfaces as well as the expeditious takedown of infringing content;
- upon obtaining awareness/knowledge of infringement—which may or may not result from a rights holder notice—the service provider has to act "expeditiously," "promptly" or "as soon as possible";
- service providers should endeavor to ensure that content that has been taken down as a result of a notice does not resurface on the same platform.

"Safe harbour" protection should not be allowable in cases of non-compliance with the notice and takedown scheme. This stipulation is also the case under the E-Commerce Directive across the EU, under other regimes operating in the US, Singapore, Australia and New Zealand, and also under Free Trade and Trade Promotion Agreements concluded between the United States and various countries. Additionally, an ISP should fall outside the safe harbor not only when it receives a notice but also when it becomes aware of infringement another way, or becomes aware of facts and circumstances indicating infringement and fails to act.

The fact that a service provider has a form of notice and takedown system in place does not absolve it from liability. Courts are increasingly seeing through illusory schemes which are simply an attempt to skirt liability;[121] for example where the site is designed or operated to facilitate infringement, including instances in which rights holders cannot locate and provide specific notification of infringing URLs before they are re-posted.

Automatic Content Recognition (ACR) filtering

The massive scale of online activity has prompted increasing use of technology, such as filtering, to identify and address infringements. By late 2007, most of the major UGC sites at that time had adopted the use of automatic content recognition (ACR) technology or "fingerprinting" for the purpose of reducing copyright infringing uploads to their services.

As described above, major content owners and major UGC sites including DailyMotion, MySpace, and Microsoft's Soapbox publicly released a set of UGC site best practices known as the "UGC Principles." These best practices included technology-driven, automatic filters of copyright infringing uploads before content could become available on their services. Similarly, YouTube made its proprietary ACR technology, known as Content ID, available to copyright holders. The technology could either block infringing uploads of their content or, alternatively, monetize or simply track those uploads. In both the UGC Principles and YouTube's implementation of Content ID, rights holders have access to ACR technology at no cost.

YouTube also maintains a system for users who dispute video filtering. When a user submits a dispute, his or her video immediately becomes available on YouTube, until and unless the copyright holder re-affirms the claim. YouTube maintains additional procedures for users who continue to want to reinstate blocked or removed videos. Since the program's implementation, rights holders have identified more than 200 million videos. More than 4,000 content owners—including every major US network broadcaster, movie studio and record label—have supplied more than 15 million reference files to the system.[122]

Many UGC sites and social networks have effectively implemented ACR-based filtering, and these experiences suggest de facto the establishment of a useful industry norm. It has not been widely adopted by other services, however, such as cyberlockers. The technology has been implemented by some services including Kazaa, iMesh, Mediafire, Hotfile, Hulkshare and Depositfiles, showing that it is feasible and reasonable to implement on a variety of platforms. P2P sites generally do not use ACR-based filtering (or other types of filtering) to prevent the exchange of infringing content.

Direct licensing

Many entertainment companies have entered into commercial agreements with UGC sites (such as Youtube or Dailymotion) or social networking sites (such as Facebook)–both for promotional purposes and to distribute content on those platforms. These agreements may also incorporate anti-piracy measures.

In many cases, these arrangements allow copyright holders to generate revenue from user uploads of copyrighted material to UGC sites. Allowing users to access copyright-protected material easily and to enjoy it legally at a reasonable price aids in the fight against piracy. Such services should consider proactively pursuing collaboration agreements with rights holders that could help mitigate losses from unlicensed content and benefit both parties involved.

Commercial arrangements can also address large-scale users on these platforms. As YouTube "stars" have realized an increase in popularity and viewers on their individual YouTube channels, many have aligned themselves with "multichannel networks" (MCNs) that have created efficiencies similar to those of television or radio networks for programming producers. Examples are Machinima, Maker Studio, FullScreen and BigFrame. Google recently acquired Next New Network, an early MCN behind the "Obama Girl" video.

Some MCNs have then used the YouTube platform without obtaining appropriate licenses for the music used in their extraordinarily popular videos and, therefore, without paying music creators or rights holders for the use of their works. In 2013, Universal Music Publishing announced that it had entered into a licensing agreement with Maker Studio and Fullscreen, two of the big MCNs. This example paves the way for further deals in this maturing business. National Music Publishers Association President David Israelite has cautioned MCNs that merely licensing one music publisher does not absolve them from responsibility (or liability) for any other rights holders whose works are used without permission.[123]

Automated notice and takedown

Although ACR technology is effective when properly deployed, it is reliant on a comprehensive fingerprint database and fast identification algorithms. Some gaps exist in coverage, however, especially concerning pre-release and remixed content. Thus, many UGC sites provide tools, beyond ACR technology, that enable rights holders to automatically and immediately remove copyright infringing content uploaded to UGC services. Such tools, often referred to as "takedown tools," essentially expedite copyright protection for UGC sites and rights holders.

Terminating repeat infringers

Section 512(i) of the US Copyright Act stipulates that service providers must adopt and implement a policy that terminates subscribers/account holders who are repeat infringers. If the service provider fails to abide by these stipulations, it would lose the potential protection of certain important legal safe harbors under the Digital Millennium Copyright Act. The EU's E-Commerce Directive is missing a similar threshold condition. However, the lack of such a policy can, in certain cases (when coupled with other indicators), be considered a criterion for a court in determining whether a site is structurally infringing and outside the scope of the privileges in the Directive.

Not surprisingly, most services at least purport to have a policy, usually set out in their Terms of Use agreements, that terminates users who are repeat infringers. Of course, such a policy alone will not deter or prevent uploading of copyright infringing materials; however, the implementation of such a policy can allow for consumer education about the importance of respecting intellectual property rights. Furthermore, the termination of recidivist infringers creates at least some hurdles for those users who repeatedly upload copyright infringing material. While such users can likely re-subscribe under a new user name (providing new contact information such as a new email address), a repeat infringer policy at least provides some speed bumps for these persistent copyright infringers. The policy also provides a stronger deterrent effect on those who wish to comply with the law and the service provider's policies.

4.2.3 Additional approaches to consider

Education and raising awareness

Educational programs to raise user awareness of the copyright laws plays an important role in decreasing both demand for—and promulgation of—unlicensed content. For example, the RIAA created two programs aimed at providing educators with useful tools to help educate students in grades 3-8 and in college. The initiative showcases the intersection of intellectual property issues with technology and civic responsibility.[124] All the services mentioned in this chapter would benefit from similar educational campaigns.

Predictive tools for risk analysis

Each of the services employs different privacy policies and gathers connection/usage data for its own purposes, whether to target advertising, improve service features or monitor for fraud or other service abuses. Machine learning and pattern recognition using such available data can help identify the likelihood of infringing behaviors. Such risk scoring can be used to focus resources on addressing these abuses through engineering, education or enforcement of terms of service. A recent patent application from Facebook shows how the data in its social network could be put to such use.[125]

4.2.4 Are these practices working?

On UGC sites, such as YouTube and the DailyMotion, the adoption of ACR-based filtering as well as automated takedowns and termination of repeat infringers has largely controlled the problem of mass piracy by end users. While determined users continue to circumvent UGC site filtering, the reality is that UGC sites that follow the UGC Principles or have similar policies (such as YouTube) have effectively and substantially reduced the easy availability of infringing content on their sites. This filtering activity has required substantial investment from rights holders and platforms in both the establishment and the ongoing use of these measures.

These achievements provide a blueprint for other services. Where social networks have employed some of these tools, such as with ACR on Facebook, again the impact is impressive. These companies' efforts pave the way for other services where piracy continues to be a major concern, such as the VK and Zing networks cited by the USTR in its Notorious Markets List.

As for cyberlockers, it remains too early to say whether cyberlocker operators will adopt any meaningful set of best practices intended to substantially reduce copyright infringement on their sites. In the wake of the Megaupload indictment in early 2012, a number of major cyberlockers voluntarily ceased operation entirely or ended their users' file-sharing ability. Many also revised their operating model to avoid rewarding users for uploading large volumes of popular content, which included, almost inevitably, overwhelmingly infringing copies. As a result, copyright holders saw a reduction in traffic and infringement on cyberlockers, and the use of these services fell sharply throughout 2012.[126]

New cyberlockers adopting high-risk practices have emerged in a fairly transparent effort to fill the void left by Megaupload (and to gain the millions of dollars of revenue that Megaupload's operators had once enjoyed). Many more cloud storage providers, however, are building businesses aimed at non-infringing usage. These services now have opportunity to adopt best practices and define industry norms as the UGC principles did in 2007.

BitTorrent site operators have adopted no meaningful infringement deterrents, presumably because the raison d'etre of those sites is to distribute copyright infringing content. While they may have a notice and takedown policy, and individual links may be removed following a request, dozens more links to the same file will remain and new links can be reposted. BitTorrent site operators have made no serious effort to address rampant piracy on the BitTorrent protocol.

Major P2P software application providers have made no effort to build in copyright protection measures in the products they provide to end users. For instance, they could incorporate a form of automated content-recognition technology, or they could show their users how to avoid placing copyrighted content into folders on their computer that the software makes available to share with other users.

More generally, where providers employ notice and takedown, the main drawbacks are the following:

(1) the process can entail serious delays, in particular where the service does not act "promptly";

(2) the sheer volume of links to pirated content on the Internet is so great that it would be nearly impossible for manual "notice and takedown" efforts to ever completely tackle illegal activity; and

(3) unless coupled with measures to ensure that infringing material stays down, all too often infringed content will resurface shortly after the takedown, requiring rights holders to engage in endless series of notices demanding repeated removal of the same material. Automation, however, improves takedown results significantly. It is important that these practices continue and expand.

Once notification occurs or once a service becomes aware of infringement, improved response time would be especially valuable in limiting piracy of all kinds of copyrighted material, particularly time-sensitive items like pre-released software or newly released sound recordings or films. Active measures to prevent reposting material that has been taken down could transform notice and takedown into a truly effective remedy.

4.2.5 Suggested best practices

Many major platforms considered here have established effective measures to reduce their vulnerability to counterfeiting and piracy. Given the massive scale of online activity, the takeaways across these services are that automated tools and technologies—whether for rapid notice and takedown or for filters during upload or sharing for higher-risk services—are vital for effective systems.

The challenge to ensuring legitimate content-sharing is to balance the upload of original content and deter users who flagrantly and repeatedly violate terms of service. While progress has been made, significant illegal content remains undetected on services. Perhaps more troubling, numerous content-sharing services have made no effort to address infringement.

1. **More broadly adopt automated tools for rapid notice and takedown, filtering and redress for any errors.** The massive scale of online activity—whether legitimate or infringing—makes automation vital for effective systems. In many circumstances, the prevention of posting or reposting of infringing content requires efficiencies that only technology can deliver. In particular, where storage services become used for distribution, there are business models that are at a higher risk of abuse, and services using such high risk models should adopt automated content recognition. The effective adoption of this technology by leading UGC and social networking sites provides a compelling example for other services with comparable risks to consider. Where they are adopted, these approaches require constant updating to address file manipulations designed to defeat them. Automation also requires similarly developed redress systems to resolve any mistakes so that platforms can act quickly, responsibly and firmly against repeat infringers and maintain consequences for service misuse.

2. **Encourage cooperation between platforms, technology providers and rights holders to develop technical standards for notices and file fingerprints, enabling interoperability and reducing the impact of fragmentation across platforms.** By adopting the effective measures identified in this chapter, such as those set out in the UGC Principles, legitimate services will not only substantially reduce their vulnerabilities but they will widen the gap between them and other infringing services. Developing common formats for notices and file fingerprints will bring greater efficiencies across this legitimate system.

3. **High-level engagement between service providers, rights holders and government can advance the development and adoption of the practices identified above.** Given Internet traffic growth, rising incidence of infringing activities, and the evolution of technologies, governments can encourage effective response by clarifying expectations of service providers and rights holders to perform sufficient due diligence. It can also prevent misuse by taking strong action against those platforms dedicated to abuse.

5. Infrastructure providers

These services are the technical backbone of the Internet on which all web services are built and delivered. This category covers three main services. Hosting providers, like Rackspace, offer the server space to store either a whole website or simply some specific content, which is then displayed on other sites. Domain registries, like Nominet, and their registrars like GoDaddy, provide website names and connect them to the IP address of the hosted site. Internet access providers, like British Telecom, connect users to the Internet. These providers are the final crucial link, as all data must pass through their systems to reach end users and consumers.

5.1 Internet hosting services

One of the roles that Internet Service Providers (ISP) perform is Internet hosting, a service that "hosts" or stores content for customers. This storage is accomplished either directly on the ISP's network or, more usually, by offering a hosting service for entire third-party websites or platforms. If hosted directly on the ISP's network, the ISP itself has administrator access to the site and can, if necessary, take the content down or block access to it.

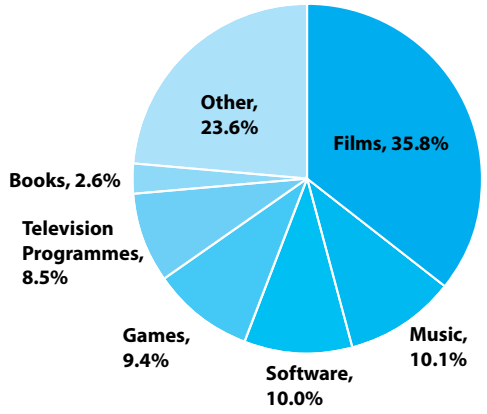
In offering hosting services to others, an ISP may offer its customers storage space and development tools, so users can create their own web space on the ISP servers. The service may allow users to physically locate their own servers in the ISP-hosting facility, or it may simply enable high-bandwidth connectivity for a remotely located server. The references to ISPs in this chapter refer to ISPs that offer hosting services, although many other specialist companies offer just hosting.

Internet hosting services may be technical, automatic and passive if the ISP's activity is limited to storing content at users' direction. If the ISP plays a more active role in the selection, arrangement and presentation of content to users, however, the legal treatment of that ISP's conduct is different. As with Internet transmission services considered in the next chapter, hosting services often represent only one of several functions in which a typical ISP is engaged; many ISPs fall into more than one category. Obviously, a wide range of legitimate uses exists for such services, but criminals and others also use these same services for the illicit sale and distribution of counterfeit and pirated products.

5.1.1 Infringement on Internet hosting services

Infringers use hosting services for counterfeiting and piracy in multiple ways, as described in the two preceding chapters. This chapter focuses on how non-compliant sites use hosting providers' services. It also considers situations when the host can require its customers to take steps against infringement or, indeed, to stop servicing those customers.

Figure 12: Infringing items commonly found on hosted services



The sites considered are those that may store data and then offer unauthorized copies of copyrighted works directly on the service providers' servers. (See Figure 12) Other Internet users can copy them ("download sites") or listen and watch them in real time ("streaming sites"). Some may actively store infringing material on a cyberlocker and then "post" a link to this infringing material on a forum, blog or dedicated site allowing users to download or stream it ("link sites").

Thousands of other websites have been identified selling counterfeits directly to the public. These websites generally look professional and mimic the

genuine brand websites to fool consumers into purchasing goods that are only slightly less expensive than the genuine products. These sites regularly change the host provider and the domain names they use, making it particularly difficult to determine who is running the site.

In some cases, the host provider itself has been found to be targeting cheap services to those who are intentionally making infringing material accessible to the public or for sale. The level of involvement of service providers in such illegal activity has been found in a few cases to be quite substantial. In these cases, the service provider fails to meet the conditions for the limitations on liability reserved for an intermediary that acts only as a hosting-provider. The provider is deemed a principal or accessory actor in the illegal activity and becomes liable for the infringement either directly or under secondary liability concepts.

5.1.2 Current approaches to the problem

Internet hosting services have greater technical control over the servers and services on which third parties' data or files are stored than the ISP access and transmission services considered in the next chapter. This is why many hosting services are engaged in programs to remove or block access to infringing material or offers hosted on their servers. Typically, they take action after receiving a notice or otherwise gaining knowledge that particular infringing activity is taking place on their services.

In many cases, host providers cannot technically "take down" individual items of infringing content, as they do not have the necessary access rights. In such cases, host providers do have the ability to terminate Internet service to the offending customers or servers. This ability is inherent in their businesses, so hosting services need to discharge their responsibilities by enforcing their terms of service so their clients run compliant sites.

Rights holders, therefore, expend a great deal of effort in sending notices to the sites and services hosted by the hosting provider, requesting takedown of the illegal content or link.

Notice and takedown

Most hosting providers' terms of service require their clients to comply with the country's legal framework, including the following conditions: a notice and takedown policy on each client's site; expeditious removal of content following a notice or when clients otherwise become aware of infringing material on their site; and a repeat infringer policy for their website. In many cases, hosting providers simply request that rights holders send individual notices to the contacts on their clients' sites.

Where hosting providers work more closely with rights holders, they can be notified about the nature and operation of their clients' sites or services. Once notified about the infringing nature of the whole site, the hosting provider must enforce its terms of service, requiring that the site remove all infringing content. Failure to respond to the notice would risk the loss of the hoster's safe harbor protection. As sites are generally unwilling to comply, they tend to move to another provider if they hear about these protective actions.[127]

Over time, relationships are developing between hosting sites and rights holders to streamline this process. Infringing sites and services have migrated to far-flung jurisdictions and uncooperative hosting providers. While many hosting providers have provided their clients' contact details, at least following a court order, some hosting services are unwilling to provide accurate customer contact details. This lack of cooperation has been the subject of continued litigation, particularly in the Netherlands.

In extremely urgent cases, such as when sporting events are being streamed live from a customer's server, direct requests drive many hosting services to comply in disabling such streams directly. Increasingly, rights holders and law enforcement are notifying the hosting providers of sites and services each time a notice is sent to the individual site. This increased transparency regarding infringements by their customers enables hosting

providers to see patterns of behavior. They can measure compliance with their terms of service and make more well-informed decisions about the risk of their customers' activities.

While hosting providers are regularly notified when they are hosting infringing sites, the hosting service providers may be uncooperative, especially if they are located in far-flung jurisdictions. It should be clear that such providers lose the benefit of any safe harbor from liability at such points, and government-to-government interaction should follow where safe havens are emerging.

5.1.3 Suggested best practices

In the same way that landlords need to maintain tenant controls to guard against illegal business practices on their premises, so Internet hosting providers should effect appropriate due diligence controls to address and minimize misuse of their services.

1. **Establish due diligence controls by Internet hosting providers to address and minimize misuse of their services.** Controls should include, at minimum, obtaining adequate and accurate identification and contact information including, under appropriate circumstances, true name and street address so that the provider can enforce its terms of service, and rights holders can directly address infringement.
2. **Develop, promote and enforce clear terms of service** and acceptable use policies that prohibit infringing activity and deny hosting services to clients engaging in infringing activity. Terms should also be consistently enforced, and services should cooperate—through information sharing in accordance with applicable law—with law enforcement in investigations and takedown operations of repeatedly infringing websites.
3. **Encourage the development of reliable and transparent risk indexing services.** These services would determine the likelihood of infringing material on a given site, with the goal to incorporate such services into customer due diligence checks. Also institute clear policies for dealing with clients once infringing activities are discovered.

5.2 Domain name services

Users typically identify and access websites (infringing and non-infringing) by reference to their domain names (e.g., nytimes.com). Domain registrars and registries administer the assignment of domain names. A website operator wishing to obtain a domain name will apply to a registrar, who can assign that name to the applicant if it is available. An Internet user who seeks to be directed to an Internet site will either enter the web address– which includes the domain name–in the web browser's address bar, or use a search engine, which will link to that domain.

In either case, the technical means to navigate to the site involves translation of the domain name into a numeric Internet Protocol address (IP address), which is the actual address on the Internet to which the user is taken. A Domain Name System Server (DNS Server) performs the translation, relying on its database, which includes a list of authorized domain names and corresponding IP addresses. Each top-level domain (e.g., .com, .org, .eu) is administered by that domain's registry, which controls the DNS Server for that top-level domain. If the registry removes the domain name from the DNS server (on its own initiative or at the direction of a registrar or of a court or other governmental authority), an Internet user seeking to navigate to the website by using that domain will be unable to access it. A domain name will be removed from the DNS server if, for example, the domain name owner fails to pay the registrar the domain renewal fee.[128]

The domain name system is currently vulnerable to abuse by those who register sites to sell counterfeits or make unlicensed content available, including those who directly seek to confuse and mislead consumers by registering names similar to those of rights holders.

5.2.1 Current approaches to the problem

Domain seizure

Preventing access to illegal sites is a more comprehensive tactic than targeting individual infringing links. One such effort is the US Immigration and Customs Enforcement (ICE) Operation In Our Sites program. Since 2010, in partnership with foreign enforcement agencies, ICE has used existing civil forfeiture remedies against criminal activity to seize 2,252 domain names that were allegedly involved in extensive infringing copyright and trademark activities.[129] When those domain names are seized, the registry and/or registrar are ordered to sever the link between the domain name and the infringing site, thereby cutting off access to that site. Typically, the user is redirected to another site that explains that the domain has been seized due to infringing activity.

Another approach has been for law enforcement to request that registries and registrars enforce their terms of service and stop supporting illegal sites by withdrawing domain names. The Metropolitan Police E-Crime Unit in the UK succeeded in closing thousands of websites involved in selling counterfeit goods online in this way.[130] The new Intellectual Property Crime Unit within the City of London Police is dedicated to tackling intellectual property crime with a special focus on offenses committed online. Rights holders have been working with the Unit to identify and address the domains of copyright infringing websites. In October 2013, the City of London Police requested actions by registries against infringing domains. To date, 33 domains have been taken down as a result. Sites where domains were withdrawn include filemp3tune.com, getmp3muzik.com, mp3bravo.com and SumoTorrent.com.[131]

In March 2011, the acting US Register of Copyrights reported to the US Congress that domain withdrawal is sometimes carried out cooperatively between rights holders and domain-name registrars: "We have also been told that some domain name system registrars voluntarily cooperate with individual rights holder requests to block access to domain names that are associated with rogue websites because these registrars have broad terms of service prohibiting use of domain names for various types of illegal activity, including intellectual property violations. We understand that at least one registrar is actively—and voluntarily—helping rights holders when a domain name is being used in connection with infringing goods and services."[132]

Currently, registrars are not required to pre-check those people registering domain names. As a result, registrants enjoy free access to thousands of domain names that can look very similar to those of brand holders (e.g., louisvuitton1.com).

Information sharing

Registrars and registries provide various levels of customer contact information through the Internet's directory of domain name owners, called WHOIS. All registrars are subject to a certain level of information sharing on WHOIS through their established contracts with the Internet Corporation for Assigned Names and Numbers (ICANN). The information submitted to this database, however, is often false. Checks to ensure the data's legitimacy have traditionally been sporadic and inadequate, allowing rampant database fraud. While domain name registrants (individual buyers) can take advantage of tools to protect their privacy, including "proxy" and "private" registration services, those services have been unregulated.

Two policy processes currently underway within ICANN, however, may offer some relief to the legacy challenges associated with registrant data and the WHOIS database. The first is the recently completed renegotiation of the Registrar Accreditation Agreement (RAA)—ICANN's standard contract with domain name registrars—which sets forth the rules under which registrars may sell Internet addresses. The ICANN Board most recently approved changes to the agreement in June 2013. While the resulting RAA is stronger than the 2009 version, it still bears significant shortcomings, specifically in relation to proxy services. A broader range of proxy services is required to disclose their policies, and registrars could be

liable if the services do not follow those policies. The policies themselves, however, do not have to include verification of contact data of proxy registrants. Efforts are underway within ICANN to develop an accreditation process of proxy services that should be steered toward an enforceable standard. While stricter than its predecessor, the 2013 RAA is only as strong as its enforcement, which must be monitored closely.

The other key policy process currently underway at ICANN is a comprehensive review of ICANN's policies related to WHOIS. While this issue will take longer to resolve than the RAA contract process, it has the potential to dramatically and globally improve the quality and reliability of the WHOIS databases. ICANN has enlisted an expert group to develop recommendations for improving WHOIS, the findings of which are likely to be implemented into policy. The group includes strong representation from the intellectual property community and delivered its final recommendations in June 2014. In summary, they recommended abandoning the current system and adopting a single point of entry into an aggregator of all the WHOIS data from across all domains. Only a minimal amount of data would be available other than to those who had registered for access to this process. There would be greater obligations for data accuracy behind this gated information. This controversial proposal has to work its way through the multi-stakeholder processes of ICANN and it is unclear whether and when this proposal might be adopted. Ongoing active engagement in those deliberations could support the development of stronger global WHOIS policy.

Overall, effective and rigorous ICANN engagement can potentially yield significant global gains in the reduction of piracy and cybercrime.

5.2.2 Are these practices working?

Terminating services to sites engaged in wholesale criminal activities is a natural extension of removing repeat infringers from sites themselves. It requires enforcing terms of service prohibiting intellectual property violations. It also opens an additional avenue of cooperation between rights holders and the hosting community. This action has been relatively rare, however, as registries and registrars prove reluctant to act on notifications of infringement. Instead, they refer rights holders to WHOIS data for direct engagement with the site, or they act only on infringement in a domain address itself, or they provide inaccurate WHOIS data via the compliance procedures.

Domain name service providers should be encouraged and incentivized to participate in efforts to find new ways to proactively or automatically detect unlicensed content. For example, they can adopt risk-based scoring systems, rather than depending on rights holders to identify each instance or link. Then they can notify the associated search engine, ISP, or hosting service. As the EAASM (the European Alliance for Access to Safe Medicines) noted in its "Counterfeiting Superhighway" report, a list of objective criteria can help identify sites that have over 80% probability encouraging distribution and sale of infringing or counterfeit products.[133] Information sharing by registries and registrars of domain name owner contact details through WHOIS and other avenues has also presented difficulties for both rights holders and authorities. Controversy continues over what level of detail is appropriate to balance privacy concerns and regulations with investigations into infringing activity.

The challenge is further compounded by rampant inaccuracy within the WHOIS databases globally, as well as by lax enforcement of data accuracy requirements by registrars, registries and ICANN itself.[134] As suggested in the description of domain seizures, some registrars and registries have been more receptive to ad hoc information sharing. Yet debate continues about appropriate levels and context of information sharing.

As ICANN moves to dramatically expand the Domain Name System through the introduction of new generic top-level domains, the push has been renewed–both within ICANN and from high-level government influencers—to address these issues holistically and protect Internet users from DNS abuse. ICANN's renewed focus on safety, contractual compliance and data accuracy creates opportunities to advocate for aggressive policy reform that could impact the Internet's addressing system globally.

International law enforcement has made a number of recommendations to ICANN that would lead to immediate improvement in the quality and effectiveness of WHOIS data databases as antipiracy tools.[135]

5.2.3 Suggested best practices

Domain names are the language addresses of the Internet. Terminating services by domain name system registrars and their agents to sites that engage in wholesale criminal activities is a natural extension of removing repeat infringers from sites themselves. It allows enforcement of the terms of service prohibiting intellectual property violations, and provides an additional avenue of cooperation between rights holders and the hosting community.

1. **Enact comprehensive ICANN policies to improve Internet safety and deter Domain Name System (DNS) abuse, including a strong Registrar Accreditation Agreement (RAA).** Such policies would place consistent, enforceable requirements on all Internet registrars to maintain data accuracy and filter registrants' illegal activity. Registrars should adopt this new RAA globally, and ICANN should diligently enforce its terms. Registrars must ensure accurate data in the WHOIS database, suspending domains pending data submission following repeated requests, as happens with other services where account holders are delinquent.

2. **Include the use of third-party verification systems by Registrars and ICANN** for any domain name request containing a brand name or phrase registered by the rights holder. This initiative would help stop illicit use in counterfeit websites and cyber-squatting.

3. **Strictly enforce terms of service by Registrars to block or revoke domain names for sites predominantly engaged in infringing activities.** Cooperate with local law enforcement to expand programs that seize sites engaged in illegal trafficking of counterfeit and pirate goods.

5.3 Internet service (access) providers

Underlying all of the services considered in the preceding chapters are Internet Service Providers (ISP) offering basic Internet access and related transmission services. These providers are necessary for transactions of any sort over the Internet, as they enable users to engage with more than 2.4 billion other users, online merchants and services.[136]

These intermediaries are typically major telecommunications companies and third-party access providers, such as universities, although many small providers also deliver access services,[137] including technical, automatic, and passive roles. Everyday Internet users are, therefore, somewhat removed from contact with them, other than paying subscription fees after they have acquired the service. These services do not involve a regular user interface, modification of users' data, or the production, active publishing or hosting of content and are sometimes referred to as "mere conduit" activities.

Since all Internet activities pass through these services, the focus here is on network abuses in the form of infringing peer-to-peer (P2P) file sharing. This activity involves public disclosure of the user's IP address when downloading and uploading (sharing) any given file. ISPs alone associate a particular IP address with a subscriber account. These providers are often the only avenues available to reach an account holder who appears to be engaging in network abuse, whether knowingly or not.

These intermediaries can also play an important part in disrupting piracy and counterfeiting by blocking website access, when the action is appropriate.

5.3.1 Vulnerabilities of Internet access and transmission services to misuse and abuse by IP infringers

IP infringements through P2P transmissions comprise a significant category of Internet copyright infringement. While the exact extent of P2P infringement in relation to other forms of online infringement differs according to industry sector, approximately one-half of Internet users who access music through unauthorized services rely on P2P networks.[138]

P2P file-sharing technology has evolved through several design stages from the early networks like Napster, which popularized the technology, to the later models like the BitTorrent protocol (discussed in detail in above). Globally, the most popular P2P protocol is BitTorrent, with an estimated 200 million users worldwide. In the first half of 2012, BitTorrent was responsible for 21.7% of aggregate Internet traffic in Europe (both downstream and upstream) and 37.5% in Asia-Pacific.[139]

In P2P infringements, users are connected to each other by file-sharing P2P protocols like BitTorrent, eDonkey and Gnutella. These sites typically offer free, downloadable software that facilitates file exchanges by individuals using their own computers. The specialized P2P software program interconnects end-user computer nodes (peers) via the Internet and allows users to search for files existing on other P2P-connected computers. These files typically contain copyrighted material such as books, music, movies, and games.

Among the factors contributing to the widespread adoption and facilitation of P2P file sharing is the increase in Internet bandwidth. Typically, the only role an ISP transmission service plays in P2P infringement is in connecting individual users to the Internet. The ISP is typically not aware of any specific infringing activity by its user-subscribers. As the provider of the infringing user's Internet connection, however–and to the network of other P2P infringers—ISPs may be in a unique position to educate their subscribers and deter them from infringing activity.

5.3.2 Current approaches to the problem

Rights holders, enforcement authorities and other stakeholders have challenged ISPs to implement reasonable and accessible measures that address the abuse of Internet access and transmission services for P2P infringement activities.

With enacted or pending legislation requiring ISPs to take a more active role in preventing P2P infringement, some ISPs have been increasingly responsive. They are now taking steps in many jurisdictions to establish preventive standards and practices (some of them voluntary). These initiatives include: (a) implementing and enforcing terms of service by which the customer agrees not to engage in P2P or other illegal activities; (b) adopting "graduated response programs" by which customers engaging in P2P infringements can be educated and provided with a notice and, in appropriate circumstances, can be sanctioned; (c) participating in public awareness programs; and (d) site blocking based on orders from competent authorities.

Terms of service/acceptable use policies

Virtually every Internet access and transmission service has now implemented customer terms and conditions of service or acceptable use policies to try to limit the abuse of ISP services for illicit activities, including IP infringement. In practice, however, rights holders usually find that ISPs are not enforcing these terms and conditions. These provisions generally stipulate that the account holder and anyone using that account agree not to engage in illegal activities on the service. The terms and conditions of British Telecom's Internet service agreement are fairly typical in this regard:

Residential Standard Terms[140]

> (13) ...You must always follow our acceptable use policies in the way that you use your chosen services, which can be found on www.bt.com/acceptableuse.
>
> (45) For serious misuse described in paragraphs 13 and 14, we may suspend or end the agreement for the service immediately. Otherwise, we will normally give you an opportunity to put matters right within a reasonable time if you break the agreement.

Acceptable Use Policy[141]

> Illegal and inappropriate activities. As an Internet user, while connected to the Internet via BT, you must comply with the relevant laws that apply in the UK.... These are some of the things that you must not do while connected to the Internet:
>
> You must not, by using the service, download, possess or transmit in any way, illegal material...
>
> You must not infringe on the rights of others, including the right of privacy and copyright (an example would be sharing without permission of the copyright owner- protected material such as a music or video file).

Education, notice and graduated response for repeat infringers

Recent initiatives in several countries demonstrate how ISPs are working with rights holders to develop and implement MoU and other programs. These initiatives are educating and providing notice to their subscribers of P2P infringements occurring through their services.

"Graduated response" is a mechanism that a number of countries have adopted. Rights holders search for illegal copies of their protected works being shared on P2P networks; they collect publicly available IP addresses involved in the actual exchanges of files over the Internet; and then store them together with a date/time stamp. This information can then be linked and remitted to a specific ISP.

In the absence of precluding data protection regulations, ISPs with reliable information in hand would have the ability to notify the customer assigned to the IP address provided by the rights holder, without disclosing subscriber data or complying under duress of a court order. Such accessibility is one of the main benefits of a graduated response system. Depending on the country's particular implementation of graduated response, the user's identifying details may not need to be disclosed to rights holders at any stage of the process.

France, New Zealand, Ireland, South Korea and Chile have already implemented graduated response systems. In 2011, the US initiated a voluntary copyright alert system and started sending notices in 2013. In the UK, the 2010 Digital Economy Act provides for a graduated response scheme, but it has not yet been fully implemented. Rights holders, ISPs and the UK Government announced a voluntary scheme in July 2014, which includes investment in a multi-media public awareness campaign alongside notices, modelled on the US approach.[142] These countries have opted for different graduated response procedures. Some involve a governmental/administrative body in sending the notifications (France, South Korea). Other systems are the results of agreements between ISPs and rights holders (US). A system operating in Ireland resulted from a litigation settlement, and still other systems have been implemented by legislation (New Zealand and Chile).

These programs have been the subject of intense debate, especially when first proposed, over their necessity, proportionality, potential effectiveness and the associated costs of implementation. Where plans have been introduced, some evidence exists of a positive impact, although the debate continues about whether it is significant enough to justify the cost and scale of intervention. In France, the government body HADOPI started sending notices to Internet users in October 2010. A subsequent study found evidence that Hadopi

had a positive impact on iTunes sales, which were 23% higher for singles and 25% higher for digital albums than they would have been in the absence of Hadopi.[143] Hadopi has now sent more than 2 million notices, with less than 10% of infringers receiving a second warning.[144] P2P use in New Zealand fell by 16% after the introduction of a similar notice-sending program.[145]

South Korea also shows the positive impact of intermediary efforts. The Korean Copyright Commission and the Ministry of Culture, Sports and Tourism are responsible for sending notices to service providers, primarily cyberlocker operators, when their users infringe on IP rights. The cyberlocker operators then inform their users of their illegal activity. Cyberlocker providers now need to register with the government following the passing of recent legislation. Evidence suggests that these initiatives positively impacted the market; for instance, digital music sales grew by 53% in the first 9 months of 2009, presumably driven by public awareness of the notice-sending legislation, adopted in July 2009.[146]

The US Copyright Alert System

One of the most innovative voluntary programs can be found in the US's Copyright Alert System (CAS). In July 2011, five major ISPs, along with film and music industry rights holders, agreed to implement a cooperative system designed to deter further infringement. The system involves forwarding educational notices, maintaining evidence, and applying "mitigation measures" only to those customer accounts that receive multiple copyright alerts.

These "mitigation measures" are intended not to be punitive but instead to capture the attention of account holders. They range from providing only temporary service, account slowdowns, or other restrictions, to requiring the subscriber to view a copyright course. As a voluntary program, CAS does not require termination of a subscriber's Internet account.[147] The program went live in February 2013.

Initiated in September 2011, the Center for Copyright Information (CCI) is a collaborative effort between the Motion Picture Association, Inc. (MPA), the Recording Industry Association of America (RIAA), the Independent Film and Television Alliance (IFTA) and the American Association of Independent Music (A2IM), as well as five major ISPs—AT&T, Cablevision, Comcast, Time Warner Cable and Verizon. CCI's leadership also includes an Advisory Board comprised of consumer advocates, privacy specialists and technology policy experts. CCI developed and is responsible for operating the CAS.

Under the CAS, content owners notify participating ISPs when they believe an account holder—identified by its Internet Protocol (IP) address—is misusing their copyrights online. The ISP then matches the IP address to the corresponding subscriber account, including a date and time stamp. It sends an alert to the subscriber without sharing any personal information about the copyright holder. The shared assumption is that an overwhelming number of consumers will halt infringing activity once they better understand the risks and legal alternatives.

Should the same subscriber be flagged again for misuse after receiving the first alert, subsequent alerts will follow with varying tiers of information and calls for action. Beyond the notification and education alerts in the beginning stages, an account's additional flags will prompt alerts that require the subscriber's positive acknowledgement. Only after repeated notices to the same account holder will tiered mitigation measures be imposed.

Other key aspects of the CAS worth noting include the following:

- **Significant efforts on the part of rights holders to identify only those files where it is clear that an entire work is obtained, leaving little to no question about its protectable status under copyright law.** Although such measures are expensive to implement and do not capture all possible infringements, they virtually eliminate any false positives, building confidence in the accuracy of the notices.

- **Privacy inherent in the system.** Rights holders will send IP addresses to ISPs, but the ISP is solely responsible for connecting that IP address with its subscribers. Information is not shared in any way with the rights holder; the system is designed not to share that information. It would be shared only via proper legal authority.
- **Flexible ISP notification and responses.** CAS allows the ISP to determine exactly how it tiers the alerts to its customers. ISPs have the latitude to develop a set of responses, from a range of possible measures outlined above, that can work best within their respective networks.
- **Independent Review Program.** Essentially a dispute resolution mechanism, the CAS also establishes a review program that enables subscribers to challenge the alert and designation that their account has been misused. The program maintains subscriber anonymity and privacy in the event of any challenges filed, unless subscribers choose to reveal their identities.
- **Data gathering.** CCI and its partners have stated their intention to gather data on their respective program areas in order to ensure transparency, as well as to discern trends, and at an appropriate point, to implement improvements.

The Graduated Response Programs in France, the UK and Ireland

In France, a graduated response program under the administrative authority HADOPI was launched in October 2010. Under this program, HADOPI can decide, in the case of a third infringement, to refer the case for prosecution, which may result in a fine of up to EUR 1,500.[148]

Depending on the gravity of the infringement (e.g., infringements on a commercial scale), the case can be referred to a criminal court that can hand out a fine of up to EUR 300,000. As of June 2013, the authority issued more than 1.9 million first warnings, about 186,000 second warnings and 663 notification letters at the third step. About 50 files have been submitted to the judiciary who can impose fines of up to EUR 1,500.[149]

In June 2013, a district court imposed a EUR 600 fine and a 15-day account suspension, but the latter was not applied because the relevant provision on account suspensions was repealed. Earlier in September 2012, a tribunal ruled that an account holder had to pay a fine of EUR 150 for negligently allowing his account to be used for infringements.

The impact on legitimate sales is positive: a study found that sales were 23% higher for singles and 25% higher for digital albums than they would have been in the absence of HADOPI.[150]

President Holland appointed an expert, former Head of Canal+ Pierre Lescure, to review the scheme. The report published in May 2013 recommended the transfer of HADOPI functions to the Audiovisual Council (CSA-the public body for the regulation of broadcasters) and to limit potential sanctions to a fine of EUR 60, abolishing the possibility of suspending Internet access.

The report highlighted that the government is responsible for providing copyright protection and that the scheme had a positive impact on P2P piracy and legal offers. It concluded that abolishing the graduated response scheme altogether would not be a good solution, as the alternative would be cumbersome end-user litigation. It recommended simply repealing the provision on account suspensions, which the French government accomplished in July 2013. HADOPI will likely be abolished, and its powers in connection with the graduated response scheme will be transferred to the CSA, although the timeframe for this shift, as well as for further measures, is uncertain.

In the United Kingdom, the Digital Economy Act (DEA) was passed in April 2010. Under the DEA, ISPs would have been obliged to notify subscribers whose accounts had been reported for infringing activities. They would also be required to keep records of reported subscribers on an anonymous basis.

The system was designed as follows: rights holders send a Copyright Infringement Report (CIR) to the ISP within one month following the infringement detection. The ISP has one month to process the CIR and to send out a letter by post to the alleged infringer. After the third notification to the same account holder, and subject to a court order, ISPs are required to disclose the identity to enable rights holders to file a complaint.

The law also permits alleged infringers to appeal the notification at their own expense of £20, which will be paid back if the appeal is granted. ISPs are required to keep anonymous lists of infringers, which rights holders can access on a monthly basis.

After repeated delays regarding the implementation of the DEA, rights holders and ISPs initiated discussions regarding a voluntary solution. In July 2014, the UK government announced its support for an agreed-upon scheme, Creative Content UK.

In Ireland, a 2009 settlement agreement between major telecommunications provider Eircom and the Irish Recorded Music Association (IRMA) implemented a similar P2P notice and repeat-infringer mechanism using a "three-strikes" regime, with temporary suspension of the Internet account as a final consequence. Eircom estimates that only 15-20% of users continue to infringe after the first warning letter and only 10% after the second, with only 0.02% of the overall user total ever requiring further action.

This is an area where careful balancing of users' privacy rights and the proportionality of schemes is important. The French Constitutional Court reviewed HADOPI, and in July 2013, the Irish Supreme Court rejected the Data Protection Commissioner's (DPC) application aimed at ordering Eircom to stop operating the scheme.[151] The outcome of these reviews lends clarity and guidance on the sorts of implementations that have achieved balance in the courts' eyes.

Public education and awareness

Raising public awareness is key for access and transmission services and IP owners to cooperatively address Internet infringement. According to the European Commission in 2011:

> "All stakeholders consider awareness-raising an essential element of a comprehensive strategy to increase the use of online legal content. Consequently, rights holders and telecom operators have in place different specific awareness campaigns which bring positive effects at Member State level, targeting parents and children, teachers and pupils, media and governments. Different strategies are used to convey messages concerning the implications of illegal up- and downloading."[152] For example, one of the key objectives of the aforementioned CCI in the US will be "taking an active role in educating the public about the laws governing the online distribution of works protected by copyright, including educating the public regarding civil and criminal penalties for Online Infringement."[153]

Graduated response systems play an important educative role, as they encourage users to stop infringing, without the need for court intervention, while maintaining user privacy. Universities and colleges can play a special role in this deterrence plan, as the next section shows.

Colleges and universities

Colleges and universities play a special role in the online ecosystem. First, they have the ability to educate their students on matters of appropriate behavior as digital citizens–which includes obtaining music, movies, software, games and books through legal means.

Second, most universities in the United States are usually third-party access ISPs. (As always, depending on the specific services they deliver, they fall into the category of "mere access" provider or host provider–or they fall into both categories). Operating an

on-campus network, these university-based systems often include dormitories and other residential halls. Given their public visibility, universities have a particular interest in ensuring their systems are not misused for illegal purposes.

Since 2008, institutions of higher learning in the United States have been incentivized to develop a plan to "effectively combat" the unauthorized distribution of copyrighted materials by users of their networks, including by "the use of one or more technology-based deterrents." This plan is a condition of eligibility for receipt of federal student aid, under the Higher Education Opportunity Act of 2008 (HEOA). Additionally, as part of the regulation, universities must periodically review the effectiveness of their plans.[154] Most university systems are similar in their approach in that they employ "graduated" steps with specific consequences for the student concerned, emphasizing the educative element and giving the student the opportunity to change his/her behavior.

Site blocking

In order for a robust legal framework to effectively address online piracy, a clear legal basis is essential to require ISPs to block their subscribers' access to infringing websites or services, while striking an appropriate balance between applicable fundamental rights of the IP owner and the user. While this chapter focuses on P2P infringements—and many of the sites blocked by ISPs are sites that index infringing files on P2P networks—blocking addresses other infringing services, such as illegal streaming sites and others that do not take meaningful action to control pirate uses of their services.

One of the main challenges is addressing both counterfeiting and piracy from websites based outside the jurisdiction in which the infringement takes place. Local rights holders cannot be expected to pursue legal actions in all foreign countries where sites fail to take action against piracy. Local ISPs cannot "take down" this material, as they do not host it on their servers.

This limitation has led a number of governments around the world to adopt a legal basis for requiring local ISPs to prevent subscriber access to foreign websites by way of website blocking, predominantly focused on copyright. Singapore adopted such a law in July 2014,[155] and Australia is considering this action as part of its copyright review. Rights holders have brought successful offshore website blocking litigation in many countries, mainly in Europe and Asia, including Austria, Belgium, Denmark, France, Finland, Greece, India, Ireland, Italy, the Netherlands, Spain and the UK.

In this area, courts are balancing the rights of users to receive and impart information with ISPs' freedom to conduct business. Property rights protection ensures that these measures are used only in appropriate cases. Balancing these issues is a matter of significant debate, as players discuss where to use these orders first and where to propose new legislation in order to enable their use. In the US, legislative proposals that were introduced in 2012 as SOPA and PIPA proved controversial and did not progress. A recent study from the American Bar Association's IP Chapter provides a comprehensive analysis of US law and how it might be applied to address foreign websites that offer counterfeit products or pirated content.[156]

In the years following those US proposals, however, courts in several other jurisdictions have ruled that website-blocking measures can be proportionate for ISPs, as they are relatively affordable to implement. The measures are also proportionate to consumers,[157] if threshold requirements are met and due process elements are built into the procedure before issuing a siteblocking order.

In March 2014, the European Court of Justice confirmed this approach.[158] A detailed balancing exercise which looked more deeply at the costs of obtaining and implementing such orders was made by the High Court of Justice of London in *Cartier vs. BskyB* in October 2014.[159] The case also considered the effectiveness of such orders, rejecting the approach of the Dutch appeal court. The court decided to lift injunctions regarding The Pirate Bay on the basis that the orders were not shown to be effective in the evidence

before it. (This case has been appealed.) The Cartier case extended the use of these orders to the blocking of sites selling counterfeit goods[160] based on the inherent jurisdiction of the court and Article 11 of the EU IP Enforcement Directive 2004/48/EC.

These courts have concluded that a number of reasonable, proportionate and technically feasible options are available to ISPs for blocking. The most usual methods for blocking access to infringing sites are implemented at the Domain Name Service (DNS) level (i.e., by blocking the service according to the domain name it uses) or at the Internet Protocol (IP) level (i.e., blocking the service according to its IP address). While DNS-level blocking has some impact, as it prevents casual users from accessing the site, users can easily circumvent such a block by entering the IP address for the site. Where the IP address is shared there is a risk of over-blocking, and in these cases there is still debate about the best approach. However, in many other cases the most effective block is applied at both the DNS and IP levels, and this is emerging as the standard for many countries around the world.

Music sector research has shown that website blocking measures have a marked impact by reducing the usage of the blocked sites. Between January 2012 and July 2013, European countries where blocking orders have been issued saw a decline in BitTorrent use by 11%, while EU countries without such orders saw a BitTorrent use increase of 15%.[161]

Usually a specific legal basis is required in order for rights holders to obtain an injunction against an ISP. Blocking measures around the world have been based on either of the following:

- Specific legislation, such as in European Economic Area countries where Article 8(3) EU Copyright Directive 2001/29/EC provides a legal basis for website blocking injunctions, or
- As applied by government authorities on the basis of general telecommunications powers.

In general, the courts have ordered ISPs to implement the orders in the form of DNS and IP blocking. In all cases, the ISPs have been required to bear their own costs of implementing the blocks. For example, in the UK, in October 2011, a court ordered the ISP British Telecom to block access to the *Newzbin2* website. Similar orders were subsequently obtained against other ISPs. In 2012, the High Court ordered six major ISPs to block the P2P file-sharing website The Pirate Bay in order to prevent UK citizens' access to the website.

The ISPs all either consented to or did not oppose the court orders; nevertheless, the court provided a detailed analysis of the balancing of rights and the proportionality of the orders before making its decision. The UK High Court has since ordered three further BitTorrent websites to be blocked in February 2013 (*Kat.ph, H33T.com and Fenopy.eu*). In July 2013, BitTorrent site EZTV was blocked, and as of September, several proxies—including *eztvproxy.net* and *eztv.dashitz.com*—were added to the block list. The court procedure has been streamlined over the course of these cases and extended to sites that stream sports and films. In October 2013, the British music industry was successful in an application to block 21 websites.

As more sites are blocked, BitTorrent usage significantly declines. For instance, in the UK, BitTorrent traffic declined by 20% in 2013.[162] In a judgment from October 2014, the court referred to Comscore data showing that the number of UK visitors to Bittorrent websites that had been the subject of previous blocking orders had declined by 87%.[163] In December 2012, following contact from the record industry, Pirate Party UK shut down a proxy service that had been enabling some users to circumvent the ISP block.

5.3.3 Are these practices working?

Groups have invested significant effort and resources in the programs described above, following cost benefit analyses to see that these measures are proportionate to the problems and their likely outcomes. Regarding P2P, many of the graduated response programs are still relatively new. While initial indicators are promising, the long-term impact is yet to be seen. The level of online piracy and counterfeiting, however, remains significant. Clearly, further efforts are needed from all sides to help stem the problem. As set out in the chapter on Legal Framework, a comprehensive approach is essential to carefully balance responsibilities and address online infringement in all its forms.

Despite all of these positive indicators, notice and graduated response programs address only part of the problem. First, they address only P2P violations, not unlicensed streaming and streamripping, cyberlockers or other sites that host and make available infringing material. Second, they are not geared towards halting determined infringers. Third, and more importantly, they constitute only one important plank in the fight against online counterfeits and piracy. For online IP infringement other than on P2P networks, other measures are required.

ISPs' terms of service and acceptable use policies that restrict any use of the connection for illegal activity, including specific copyright language, stand as important contractual obligations for Internet users. The terms have not to date, however, provided enough of a deterrent by themselves to halt infringing activity online. Unless ISPs actually enforce these terms of service, they will not have appreciable effect.

5.3.4 Suggested best practices

In their capacity as "mere conduits," ISPs are not usually under a general obligation to actively monitor their services for violations of law. When they become aware of infringement, however, they should take reasonable action. ISPs are often the best—or, indeed, the only—source capable of identifying an account holder behind an IP address from which alleged infringing activity has been detected. They are also in a key position to partner with rights holders.

Significant effort and resources have supported programs such as graduated response. While promising, their impact remains to be seen. The level of online piracy and counterfeiting, however, is still significant, and further efforts are needed from all sides to help stem the problem, while balancing these with protecting customer privacy. In the absence of programs such as these, in some countries, the involvement of a judge or legal authority has been required. In the context of proceedings for example, the competent judicial authorities may order that information relevant within the context of the infringement of an intellectual property right might be provided by the intermediary, whilst also overseeing any actions taken as a result of the information provided. The involvement of a judge can limit the impact of any assignment mistakes, thereby avoiding unjustified enforcement measures.

1. **Improve and broaden strong voluntary and cooperative action to fight counterfeits and piracy by access and transmission providers.** More specifically, programs should be established and promoted to educate users on the harms and consequences of accessing pirated material. New initiatives, such as notice and repeat infringer policies, should be carefully evaluated for effectiveness going forward. ISPs are in a key position to work with rights holders to educate their subscribers that infringement is unlawful.

2. **Develop and implement ISP *Terms of Service* and *Acceptable Use* policies. Language should clearly state that unauthorized downloading or uploading of copyrighted material is a violation of these agreements,** whether through peer-to-peer downloads or uploads, streaming, or any other means. Clarify that ISPs retain the right to suspend or terminate service for repeated or flagrant violation of the *Terms of Service* or *Acceptable Use* Policy.

3. **Implement *Notice* and *Repeat Infringer* policies,** in cooperation with rights holders, based on notice and graduated response principles of the French HADOPI and US CAS programs. These policies should focus on education and awareness and include a reasonable number of notices before employing mitigation measures. In this way, subscribers will have adequate opportunity to change behavior prior to their imposition. An appeal process should be in place at the mitigation stage to provide an opportunity for notified parties to address mistakes.

    a. Share costs equitably. This initiative should include the following: i) recognition of the costs already borne by rights holders to identify and notify the ISPs of instances of infringement; ii) the extraordinary burden placed on independent artists or film makers to police infringing copies of their works; and iii) affordability for small ISPs.

    b. Share aggregated data to assess program effects, such as the total number of monthly notices and a breakdown of first, second, and third (etc.) issues—and use this data to evolve the effectiveness of the system. To address the most serious infringers and following local jurisdictional due process requirements, ISPs should, subject to applicable law, keep and maintain records for a reasonable time to allow rights holders to obtain the actual subscribers' identities associated with a particular IP address.

4. **Block subscriber access to Internet sites or online services** when the courts or competent national authorities find that the sites meet these criteria: (a) they are designed or operated with the clear intention of inducing or promoting infringement; or (b) they knowingly facilitate or enable large-scale infringement and do not take reasonable steps to prevent it. Action should be based on evidence, such as infringement volume, evidence of inducement, notice and take-down operations of the site, any direct or indirect financial benefits, and/or whether courts in other jurisdictions have found the site infringing. This action should not require a finding that the ISP itself has engaged in any unlawful conduct, as the remedy is to prevent harm caused by infringements by third-party sites or services.

6. Search, online advertisers and payment processors

6.1 Internet search engines and portals

Internet users throughout the world rely on Internet search engines and portals to find information on the web. As such, search service providers are important online intermediaries, pointing users to websites and associated content. This chapter considers how search results provided to users of the search services may include links to counterfeiting offers and copyright infringing content, and what can be done to address this.

Search engines and portals automatically cross-reference search terms against sophisticated algorithms that point users to matching websites. Search engines and portals themselves generally operate as websites, with specialized back-end functions that generate and maintain indices of URLs and content (including web pages, images, and digital files) in searchable formats. They often also offer other services, such as email or news, in conjunction with their primary search function. Services such as Google, Yahoo, Bing, Ask, Baidu, and Naver are well-known search intermediaries. These services are often exclusively funded through advertising and are provided free to Internet users.

The ability to point Internet users to specific URLs and websites and web pages–legitimate and illicit–makes search engines critically important in dealing with counterfeit and pirated trade. The dominant search engine Google has committed to improving the visibility of legitimate content and demoting illicit content by improving algorithms and other measures.[164] More work needs to be done in this area to limit the visibility of and access to infringing sites, and to help search engines deliver more accurate and legitimate search results.

6.1.1 Infringement on Internet search engines and portals

Unfortunately, the same or similar search and directional tools that index and return search results for legitimate websites and online services also deliver search results listing sites with infringing materials. These results are often listed alongside legitimate sites or, in some cases, rank higher than legitimate sites. A January 2012 study by Harris Interactive found that 51% of those accessing websites containing unlicensed services in the UK found them through a search engine.[165]

An example from the film industry, noted in a study by Envisional, shows that "querying Google for terms such as 'watch toy story 3 online' reveals a plethora of linking sites and blogs in the top ten results, which offer links to streams of unauthorized pirated versions of the film."[166] Other search engines present similar results. Regarding the music industry, IFPI reports that a search for the name of any artist followed by the term "mp3" still returns a vast number of illegal links on the first page of results.[167]

Search engines are also vulnerable to—and often carry—advertisements for counterfeits and pirated copies. As mentioned above, search engines generate significant revenue through advertising, specifically by selling advertisers the ability to place advertisements alongside, around or above related search results. Most services sell these ads on a pay-per-click basis, with the amount paid based on the advertisement's placement on the page.

Unfortunately, counterfeiters advertising and/or providing links to infringing content often exploit these services. Google itself reported disapproving 224 million "bad" ads in 2012, in an effort to keep pirated goods from being advertised on its Adwords platform—and there is no way to know for sure how many ads their screening efforts failed to detect.[168]

Some search engines also incorporate an "autocomplete" function that helps users find information more quickly by predicting search results based on other searches. This function can, however, suggest searches that promote links to infringing content, as seen in Figure 13.

6.1.2 Current approaches to the problem

In recent years, some search engines and portals have taken steps to develop policies that address links to counterfeit and pirated websites and content.

Figure 13 - Screenshot accessed March 2012

Notice and takedown

The practice of Notice and Takedown (NTD) discussed in previous chapters is also the principal way that rights holders work directly with search engines and portals to remove search results and links to infringing sites. To facilitate the process, large search engines like Google and Bing provide tools for rights holders to request removal of infringing links from search engine web indices and caches.

In October 2013, Google received over 24 million requests by content owners to remove search results pointing to infringing content.[169] These requests covered more than 35,000 specific domains. A recent study found that Google is responsible for over 82% of US-based search inquiries that directed users to infringing online video content–a far higher percentage than the Google share of the US search market.[170]

A number of third parties, such as MarkMonitor, offer services to assist rights holders in identifying infringing content and requesting removal of links. The impetus for developing this removal request system can be found in the notice-and-takedown framework built into the US Digital Millennium Copyright Act (DMCA) of 1998 and legislation similar to the EU's Electronic Commerce Directive in 2000.

Under these schemes, cooperation and compliance with formal notices to remove infringing content can also provide protection against liability in particular circumstances, as set out in the "key principles" section of the introduction to this paper. The DMCA and similar legislation laid the groundwork for an expedited and non-judicial process to combat online infringement. It also instituted safeguards to allow implicated users to request their content be reinstated should it be found to be non-infringing. These laws illustrate ways in which legislation helps trigger intermediaries' cooperation, including incentivizing voluntary action.

Search engine rank demotion

Search-engine market leader Google announced in August 2012 that it would begin accounting for the number of valid copyright removal notices they receive for any given site as another factor in its search rankings.[171] In theory, sites with high numbers of removal notices would (all else being equal) appear lower in the ranking of Google search results, thereby discouraging use of bad actors, and facilitating use of legitimate sources of content.

The changes in the algorithm, to date, apparently have not affected the rankings of such sites. The RIAA published a "report card" on this effort and determined that "Six months later [on February 21, 2013], we have found no evidence that Google's policy has had a demonstrable impact on demoting sites with large amounts of piracy. These sites consistently appear at the top of Google's search results for popular songs or artists."[172]

In September 2013, a report by the UK Parliament House of Commons' Culture, Media & Sport Committee soundly criticized Google for its "derisory" efforts to tackle online piracy and denounced Google's explanation for its inaction as "flimsy." The report cited figures showing that searches for artist, title and "mp3" yield a 61% infringement rate, only 2% lower than the rate before Google implemented said changes.[173] The Committee observed that "Google co-operates with law enforcement agencies to block child pornographic content from search results, and it has provided no coherent, responsible answer as to why it cannot do the same for sites which blatantly, and illegally, offer pirated content."[174]

A more effective rank demotion would help direct visitors to licensed services. According to consumer research by Ipsos MediaCT across nine countries, an average of six in ten Internet users (60%) believe that search engines "should give priority to legal digital music services over pirate services when they show their search results." To the extent that the solution is technically feasible, it appears that this condition would be a popular and responsive measure to mitigate traffic to infringing sites.[175] In October 2014, after Google announced a revised algorithm, an initial report showed data suggesting a significant drop in traffic to demoted sites.[176]

Key-word blocking in autocomplete

Similar problems remain regarding search engines' autocomplete functions. For example, Google announced in December 2010 that it would work to prevent terms from appearing in "autocomplete" that are closely associated with counterfeits and piracy.[177] The details, scale, geographic reach and duration of such autocomplete search-term blocking, however, have not been made public. The measures for responsibly operating search engines regarding their autocomplete and predictive search query functions are discussed below.

Search engines' activities have, on occasion, gone beyond merely indexing the web and selling advertising around it. Instead, prosecutors claim, they actively assisted illegal activity. An example from the pharmaceutical sector shows that Google entered into a non-prosecution agreement with the U.S. Department of Justice in 2011, pursuant to which it paid a $500 million forfeiture "in a settlement to avoid prosecution for aiding illegal online pharmaceutical sales. The settlement 'signals that, where evidence can be developed that a search engine knowingly and actively assisted advertisers to promote improper conduct, the search engine can be held accountable as an accomplice,' according to Peter Neronha, the lead prosecutor."[178]

In that case, evidence suggested that Google's global ad sales team was knowingly telling illegal drug advertisers how to defeat Google's advertising filters to sell banned substances. Notwithstanding the stringent terms of the $500 million forfeiture, a recent Google search for "buy oxycontin online no prescription" returned a variety of Autocomplete terms prompting the user to search Google for counterfeit pharmaceuticals or illegal sources of prescription drugs. A YouTube search, "buy pills online no prescription," returned a video with extensive lists of available prescription drugs. Furthermore, a recent report shows advertising from major brands still being served alongside such videos.[179]

In 2012, the Cour de Cassation, France's Supreme Court for civil and criminal matters, ruled that Google's search engine systematically prompted users searching for music to include piracy search terms through its "auto-complete" function. It then directed users to websites containing infringing music files. In this case, the search engine must be providing the means to infringe on copyright and related rights. The court concluded that rights holders were, therefore, entitled to seek injunctive relief against the search engine's use of the auto-complete function. These measures, however, might not be totally effective in preventing the search engine from directing users to pirate sites.[180] The courts reached a similar conclusion in 2014 in a case against Amazon regarding the use of the Lush trademark that redirected users to competing products through suggested terms.[181]

Advertising policies

When a search engine provider offers search results that feature a specific advertiser, such as the aforementioned sponsored links, the provider should take proactive steps to ensure that the advertiser is not a site or service that (a) facilitates, encourages and/or induces infringement of copyright; or (b) offers, makes available or distributes content that is predominantly infringing—or is in any way in breach of the terms of service agreement.

Both Google and Bing employ corporate policies that prohibit the use of their advertising services to promote infringing content.[182] Specific policies ensure that only legitimate trademark owners or sellers use advertising for trademarked search terms.[183] These search engines also offer remedies for rights holders concerned with possible infringing advertising, or advertised links to counterfeit sites. Little is known, however, regarding the actual enforcement of these policies and the technical tools these companies employ to achieve results.

Bing's Intellectual Property Guidelines on copyright infringement and counterfeiting is indicative of how these policies are framed:

> *Advertising is not allowed that promotes the infringement of copyrighted material or seeks in any way to market products or services that enable the bypassing of copyright protection....*
>
> *Microsoft prohibits the advertising of counterfeit goods on our advertising network. A counterfeit good is one that copies without permission the trademark and/or distinctive features of a product in order to either pass itself off as the genuine product or promote a nearly identical replica or imitation of the original product. Trademark or designer product brand names cannot be modified with "counterfeit," "fake," "replica," "copy of," "inspired by," "bootleg," or any synonym thereof.*

Google has encountered difficulties with advertising that promotes human trafficking and a variety of other illegal activities, including counterfeiting. In 2012, US Representatives Carolyn Maloney and Marsha Blackburn wrote to Google CEO Larry Page requesting assurances that Google would not accept advertising that promoted human trafficking, including prostitution.[184] Notwithstanding assurances, within a few months of the initial letter to Page, Rep. Maloney demanded that Google remove a "sex club" app from the Android Market that was promoted to female students and facilitated prostitution in Maloney's own district of New York.[185]

According to the BBC, Google was also caught brokering advertising that promoted the sale of counterfeit Olympics tickets.[186] A petition calling on Google CEO Larry Page to stop selling advertising that promoted the sale of illegal ivory has received over 75,000 signatures.[187]

The same advertising platforms used for sponsored links on the search page are used to provide advertising across many other websites. Counterfeiters buy and place advertising on these legitimate websites to drive traffic to their own illicit sites, manipulating the e-commerce ecosystem to their gain. These false advertising ploys are exacerbated with the use of an advertising network service such as Google DoubleClick or Yahoo, where counterfeiters can simply provide information on the keywords or traffic toward which they want their advertising targeted.

This submitted advertising "inventory" is then distributed among participating websites that match the target criteria, often with little to no human approval. For instance, if a counterfeit shoe retailer wants to attract more traffic to his or her site, s/he could falsely advertise "Uggs" on legitimate shoe retail sites without any human approval or intervention, diverting traffic away from legitimate goods, in favor of the cheaper but illicit version.

These examples clearly show that search engines need to do much more to prevent advertising from untrustworthy sources to users searching for legitimate and safe content.

Monitoring the activities of commercial partners (advertisers of infringing sites and products) and strict enforcement of their standing policies against advertising counterfeited and pirated products would be responsible and effective measures.

6.1.3 Are these practices working?

Notice and takedown mechanisms have assisted in removing search results and links to copyright-infringing materials online. As with the use of notice and takedown for hosted material, the downside is that this is a time-consuming and costly system, both for rights holders and service providers. Google has acknowledged, however, that of the millions of takedown notices it has received for search, 97% of the claims on infringement are valid.[188]

Notice and takedown systems have proved useful tools to fight copyright infringement online. They also serve as positive examples of how legislation can help build the foundation for non-judicial and proactive cooperation between rights holders and online intermediaries, including search engines. Without sufficient cooperation from search engines—in effecting the necessary technical tools for rights holders to operate such a system—enforcement efforts will remain fragmented.

While search engine services are concentrated in many world markets, some large players in regions like China have been criticized for not upholding generally accepted practices to deter counterfeiting and piracy. In the Google drug case discussed above, Google's employees based in China approved advertising for a site selling Prozac and Valium without a prescription to Americans.[189] Broader global dissemination and incorporation of best practices could be a useful exercise to ensure coordinated efforts to combat counterfeiting and piracy within this channel.

It should be noted that hard goods require a different approach. The measures described above deal primarily with digital piracy issues and not counterfeit hard goods sold from illicit websites. Regarding hard goods, not only does the system described above require many notices to be submitted before a website is demoted from the search results, it may also require a test purchase or even a court order in the case of Google, to prove a trademark infringement.

6.1.4 Additional approaches to consider

In order to help rights holders in their efforts and to prevent consumers from being drawn into illegal behavior online, search engines should consider further measures, such as those outlined below. In addition, reviewing metrics on such measures will prove useful. Search engines still must do more to refine their ability to quickly and efficiently remove infringing links from searches and portals.

Prioritize legitimate sources in search

The majority of search engine users do not look beyond the first page of search results. This behavior is notable because searches for an artist, title and qualifier such as "mp3" often produce a list of search results whose first page is dominated by illegal sources. Therefore, search engines must prioritize legitimate sites in their search rankings. They should include objective and reliable guides that lead users to legitimate sites. A rights holder certification scheme, for instance, would help search engines identify data feeds that can enable and grow systems built on trust scores.

De-index overwhelmingly infringing sites

Search engine providers should altogether remove from their index entire websites, domains and sub-domains that:

- are subject to a court order requiring ISPs to block access to them;
- have been adjudicated by a court to be structurally infringing;
- are known to seriously, egregiously or repeatedly facilitate, encourage and/or induce infringement of copyright;
- are known to seriously, egregiously or repeatedly offer, make available or distribute content that is predominantly infringing; or
- are known to seriously, egregiously or repeatedly offer for sale counterfeit goods.

An appropriate process should be put in place to identify sites that should be removed from the search index and to reinstate only in appropriate circumstances.

De-rank sites that persistently make available unlicensed content

Separate from prioritizing certified sites, search engine providers should use objective criteria to account for infringing content on a website and to rank that site in search results. One possible criterion would be to include the number of delisting notices the search engine has received for the site (excluding those notices that are subject to a valid counter-notice). This is, in fact, the approach that Google announced with its October 2014 algorithm revision.

Auto-complete functions and predictive search query suggestions

As mentioned above, search engine providers should not offer auto-complete functions or predictive search query suggestions that facilitate infringement or direct consumers towards illegal content (for example [artist/track] mp3 free download) or counterfeit goods. Search engines should develop risk scores that correlate with the infringing results retrieved from auto-complete terms, with the intent to cease suggesting them. They should also respond expeditiously to requests from rights holders to remove terms that direct consumers to illegal sites. In the past, Google has made commitments about removing auto-complete terms closely associated with piracy but only with sporadic effect. The company recommitted to addressing these commitments in their October 2014 announcement.

6.1.5 Suggested best practices

Internet users throughout the world rely on Internet search engines and portals to find information on the web. As such, search service providers are important online intermediaries in dealing with the trade in counterfeit and pirated goods. Service providers and rights holders need to continue collaborating to further their voluntary practices, to better identify and remove links to online content, and eliminate websites involved in the distribution of counterfeit and pirated goods. Most copyright owners believe that a broader range of measures should be taken to address the problems described above, but there is no consensus on the measures needed. Based on measure being considered, suggested best practices include:

1. **Enhance notice and takedown systems to offer standardized and efficient notification methods to rights holders** and make information available on their use (such as rankings on the Google Transparency Report). This initiative will involve removing arbitrary limits on the number of search queries that can be processed, the number of search results that can be returned in response to each query, or the number of delisting notices that can be submitted to the search engine provider using their system or API.

2. **Discuss ways to improve keyword-blocking mechanisms and auto-complete functions to better screen links to online infringement** (including offers for illegal pharmaceuticals). Search engines and rights holders should use their expertise and analysis to identify and avoid providing auto-complete suggestions for search terms that have a high likelihood of linking to infringing material.

3. **Take appropriate steps to address advertisements by infringing websites.** Search engines should improve systems to deny search-driven advertising opportunities. Providers should terminate advertising services for any online merchant knowingly engaged in the sales of counterfeit or pirated goods. Providers should also employ adequate training and sanctions to ensure advertising sales staffs comply with such policies.

4. **Improve the discoverability of legitimate services and reduce the prominence of links to infringing content and websites distributing counterfeit goods.** Improvements to notice and takedown, auto-complete and keywords used in search queries provide a strong basis for collaboration between providers and rights holders. This collaboration should test the effectiveness and proportionality of other techniques for addressing infringing sites and links returned in search results, whether initially developed by rights holders, technology suppliers or search engine providers.

   Examples have been proposed or adopted from each of these sources—from search results optimization for non-infringing sites to demoting infringing sites and links based on the provider's own algorithm (as Google has announced), or from a third-party rating service as these mature. Recognizing the divergent views of the efficacy and appropriateness of search engines engaging in the above-described practices, search engines and content companies are urged to engage in dialogue to discuss their information and concerns. Together, they can progress toward resolving these serious issues in a manner satisfactory to all parties.

6.2 Online advertising

While the last section considered advertisements for counterfeits displayed alongside search results and on legitimate websites, this section focuses on the advertising supply chain's vulnerability to display of advertising placed on pirate sites. Such advertising is possible because of the complex supply chain through which each advertising opportunity passes; techniques used by these sites to mask their activities; and the absence of transparency in some parts of the advertising purchasing system.

Advertising is a major source of funding for digital piracy worldwide. The revenue generated can be substantial from advertising on pirate sites containing infringing material. The 2012 indictment of MegaUpload refers to more than US$25 million obtained from advertising. Another recent report by the Digital Citizens Alliance estimated that in 2013, piracy websites generated US$227 million from advertising.[190]

It is important to distinguish responsible advertisers, who work hard to develop their reputation and reinforce consumer trust. These responsible players are keen to ensure that their advertisement placements are not harmful to their brand—as opposed to those advertisers who seek to place their advertisements on illicit sites. Responsible brands, many of which are part of self-regulatory frameworks to tackle piracy, remain an important part of the solution, as the appearance of their advertisements creates the impression that these sites are legitimate.

6.2.1 Vulnerabilities to counterfeiting and piracy for online advertising

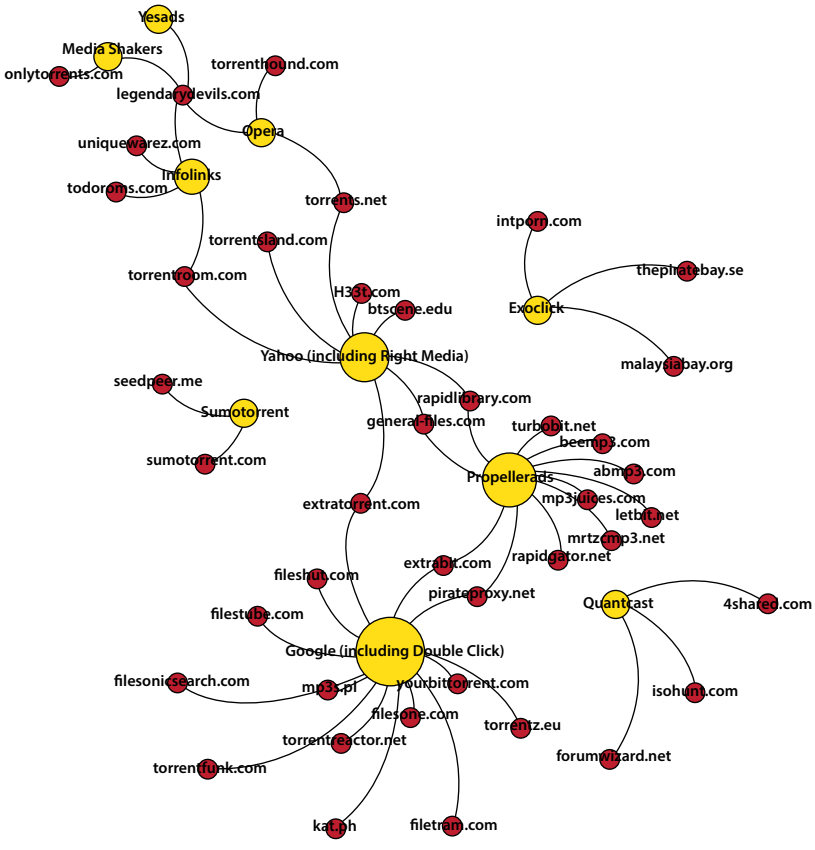
Figure 14: Legitimate advertisement on website selling pirated content

Due to the complexity and sometimes diffuse nature of the online advertising ecosystem, legitimate companies sometimes find that their advertisements have been inadvertently placed on a pirate network or website. For example, an advertiser or advertising agency might inadvertently place an advertisement on a site streaming pirated content, either through an advertising network or ad exchange bidding process in which viewer impressions are automatically selected by cookie data and traffic criteria. The infringing site would then profit from the advertising fee paid by the client. In light of this complex problem, even responsible brands active in avoiding misplacement run the risk of their ads ending up on pirate sites. In the first instance, clients should insist that their advertising partners take precautions to keep their legitimate content from inadvertently being placed on sites that peddle unauthorized goods and services. An outcome of a similar situation can be seen in Figure 14 in which an advertisement by Jeep may have inadvertently supported the operations of an infringing P2P music site.[191]

A January 2013 study by USC Annenberg Innovation Lab,[192] from which Figure 15 is sourced, demonstrates the relationships between the then top 10 advertising networks (yellow) and the infringing file-sharing sites on which their ads most frequently appeared (red). These ads can easily be placed on sites that offer both physical counterfeit goods and pirated content, lowering or completely funding these infringing sites' operational costs.

By the time of the fifth report by USC from May 2013, the top 10 networks most frequently associated with pirate sites had substantially changed, showing that with focused attention, OpenX, Google and Yahoo had removed themselves from the top 10. A recent report from the Digital Citizens' Alliance from February 2014 found premium brand advertising on 30% of pirate sites.[193]

Figure 15: Data visualization of the top 10 advertising networks and larger file-sharing sites



Referenced from USC Annenberg Ad Lab Transparency Report, January 2013. The February report noted that since January, "both Google's various networks and Open X have significantly reduced the number of infringing sites they are placing ads on."

In the successful prosecution of the convicted infringing site Pirate Bay, prosecutors stated that the site generated up to US$1.4 million a year from advertising.

6.2.2 Current approaches to the problem

Statement of best practices — advertising sector

Advertisers and their advertising agencies have begun to help ensure that the media outlets they use to promote legitimate brands and services are not: (1) also being used by counterfeiters and copyright pirates; and (2) do not allow legitimate brands to be advertised or sold on these "rogue" websites.

In an example from the United States, the Association for National Advertisers (ANA) and the American Association of Advertising Agencies (4As), with support from the Interactive Advertising Bureau (IAB), released a *Statement of Best Practices* in May 2012 designed to address online piracy and counterfeiting. The statement calls on marketers to include language in media placement contracts and insertion orders that will prohibit their ads from appearing on so-called "rogue sites" dedicated to infringement of intellectual property rights, including the following three specific references:[194]

(i) All such intermediaries shall use commercially reasonable measures to prevent ads from being placed on such sites;

(ii) All such intermediaries shall have and implement commercially reasonable processes for removing or excluding such sites from their services, and for expeditiously terminating non-compliant ad placements, in response to reasonable and sufficiently detailed complaints or notices from rights holders and advertisers;

(iii) All such intermediaries shall refund or credit the advertiser for the fees, costs and/or value associated with non-compliant ad placements, or provide alternative remediation.

In December 2013, the Digital Trading Standards Group (DTSG), a UK industry body made up of representatives from across the digital display advertising ecosystem, published its UK Good Practice Principles for the trading of Digital Display Advertising.[195] This document is somewhat less prescriptive than an earlier Code of Conduct by sectors of the ad industry proposed through the Internet Advertising Sales House council (IASH). That code specifically prohibited IASH-member advertising networks from placing ads on sites that infringe the rights of any person or entity, including intellectual property rights, but it did not gain traction. The DTSG principles recommend that contractual terms between buyer and seller identify where content should not appear, and they include the use of tools to distinguish legitimate sites.

In July 2013, several advertising networks in the US, including AOL, Google, Microsoft and Yahoo!, with support from the Interactive Advertising Bureau (IAB), announced an initiative aimed at reducing the flow of ad revenue to operators of sites engaged in significant piracy and counterfeiting.[196] Under this initiative, ad networks would commit to a set of best practices requiring them to respond to notices from rights holders concerning the placement of advertising on pirate sites. The US Intellectual Property Enforcement Coordinator (IPEC) praised efforts to create such voluntary solutions.

Law enforcement has also started to focus on advertising as a funding mechanism for online crime. In March 2014, the City of London Police announced that it had launched an Infringing Websites List (IWL), based on its investigations of copyright infringing sites, and made the list available to advertisers through a portal. The introduction of the IWL follows a three-month pilot that took place in 2013 in collaboration with representative bodies of rights holders and the Internet Advertising Bureau UK (IAB UK), the Incorporated Society of British Advertisers (ISBA) and the Institute of Practitioners in Advertising (IPA).

Digital advertising is becoming an increasingly important channel for many copyright- and trademark-reliant companies. As these businesses market their products, e-commerce websites—and the companies that help advertisers identify and buy space on these websites—have a financial incentive to assure rights holders that these sites will not be used to promote illicit goods or create unfair competition to the businesses paying to advertise. The above initiatives mark an important evolution in rights holders' use of their own purchasing power to engage e-commerce participants in deterring advertising on infringing e-commerce websites. These initiatives represent a positive precedent for Internet intermediaries, demonstrating the ability to corral sector support for anti-counterfeiting and piracy programs.

Tools available to advertisers

Businesses that advertise on the Internet, and other participants in the Internet advertising ecosystem, regularly state that they do not want to place ads on Internet sites that traffic infringing content or counterfeit goods. It is often difficult, however, to determine which sites to avoid. In response to that demand, industry has developed tools to assist in identifying such sites and, in some cases, to prevent a business's advertisements from appearing on such sites. Such tools include the following:

- **Content verification (CV) tools.** CV technology provides the ability to block or report, in real time, the serving of an online advertisement onto destinations that have been defined as inappropriate to the advertiser's campaign. Examples of providers of CV tools and their products include Project Sunblock, comScore vCE, AdSafe Media Brand Safety Firewall, DoubleVerify Brandshield and Emediate SiteScreen ASP. ABC (Audit Bureau of Circulations), the UK industry body for media measurement, has a certification program in which it tests and certifies CV tools.[197]
- **Database tools.** WhiteBULLET's IP Infringement Index ("IPI Index") is an example of an online intellectual property risk-rating technology, which assesses and scores websites by reference to their relative degree of IP infringement. Advertising agencies can use this data with clients who do not wish their brand(s) to be associated with sites that infringe copyright and other IP rights. The IPI Index could be used to identify sites that represent a high risk from the client's perspective. The client's orders can mandate checking against the index as part of the conditions for accepting the order. Veri-Site offers a similar site database and risk-rating service. These site data tools need to be combined with an ad-blocking or verification service like those described above in order to provide a true preventive solution.
- **Tracking tools** like HTTP Watch[198] integrate with web browsers to show exactly what HTTP traffic is triggered when a user accesses a web page, allowing examination of the HTTP data. Ultimately, users can see the origin of an online ad.

6.2.3 Are these practices working?

The US advertiser code is too new to evaluate its impact. The "Advertising Transparency Report," issued monthly by the USC-Annenberg Innovation Lab during the first six months of 2013, suggests that major brands are still, perhaps unknowingly, advertising on top infringing sites, as measured by the number of takedown notices received by Google. Study findings to date suggest that companies are not consistently observing the US advertiser code.

The fact that ad networks are engaging with the problem and committing to best practices is positive, but rights holders remain concerned that these initiatives do not go far enough. A disproportionate burden of detection and notice-sending remains the responsibility of rights holders. The US code is limited only to ad networks, and its scope applies to traditional display ads—a maturing market—not to video ads nor to the mobile marketplace, which are growth areas.

Rights owners feel that this initiative also overlooks apparent non-compliance sanction(s); it assumes a very narrow standard for what is a rogue site and does not expressly require any proactive or preventative diligence on the part of ad networks. More efforts need to be undertaken in this area, such as the ICC Commission on Advertising and Marketing's recent policy statement calling on the whole advertising ecosystem to develop self-regulatory programs that ensure online advertising integrity both on sites engaging in or facilitating illegal activity and other sites that brands identify as undesirable.[199]

This initiative's success requires widespread cooperation from major advertisers and more consistent compliance by ad-placement services. Ad verification services must ensure that advertisers' insertion orders are being honored. This area of compliance will also require further development and maturing of businesses, some already in the market, that operate rating services.[200]

The City of London Police pilot from 2013 saw a clear and positive trend, with a 12% reduction in advertising from major household brands on identified illegal websites. The pilot also revealed that almost half (46%) of ads served to the sites clicked through to fraudulent scams.[201]

6.2.4 Suggested best practices

Advertising is a major source of funding for digital piracy worldwide. Consequently, removing advertising support is a powerful tool for deterring infringing sites. All players in the online advertising ecosystem should take affirmative steps toward this outcome. Companies need to work together to more effectively detect advertisements on offending sites and to undertake better compliance analysis.

1. **Develop and promote advertiser codes of conduct to assist in the development of further inter-industry standards and protocols to remove advertising on infringing sites.** Building on the ANA and 4As' statement of best practices, the new standards in the UK developed by the Joint Industry Committee for Web Standards in the UK and Ireland (JICWEBS), and similar codes elsewhere, industry needs to improve detection of advertisements on offending sites and effect better compliance analysis.

2. **Include terms in advertiser contracts instructing online placement services not to place advertising on websites that have a high-risk score for infringing activities.** Advertisers should include contractual commitments from the advertising networks and exchanges to implement a real-time check against an indexing service for any order placed. This should also include the requirement to verify the final placement of orders accepted and executed by the network. It should also require verification of the final ad placement to monitor compliance with the criteria set in the contract.

3. **Advertising agencies and other intermediaries should implement a parallel, commercially reasonable process to exclude infringing sites from their ad placement services.** This process should form a baseline of sites with whom the supply chain will not contract, irrespective of customer concerns, whether based on repeat infringers or evidence-based notifications from rights holders, provided by law enforcement (such as the IWL in the UK) or from their own risk-based criteria.

4. **Communicate more effectively to advertising intermediaries that paying advertising fees to sites that law enforcement is investigating may amount to money laundering.** These actions could be modeled on efforts by the US, UK and EU to ensure that companies address vulnerabilities in the digital supply chain, notably the engagement by advertising intermediaries and their associations in working with the City of London police in the UK.

6.3 Payment processors

Payment processors are critical intermediaries in the supply chain for legitimate products, as well as for counterfeits and other illicit goods sold over the Internet. This group of intermediaries includes credit card companies and networks, acquirer banks within these networks, PayPal and other payment processing and money-transfer services.

Significant sales of any kind via the Internet would be almost impossible without the transmission of payments through these online payment processing services–especially since, in the Internet world, payment by check or money order lacks the immediacy required to match the rest of the automated transaction process. Electronic "cash" options, such as bitcoin, are still relatively new and not widely adopted.

As a result, both the vast number of legitimate traders and sellers of counterfeit goods over the Internet depend heavily on electronic payment services. Evidence of the abuse of payment provider intermediaries for completing transactions for infringing goods is found in the hundreds of billions of dollars of counterfeit goods sold online each year.[202] Following the flow of these funds is one of the best ways to identify the criminals involved in these illicit activities. Another method is to stop the flow of funds to their accounts, including, in some cases, seizing the ill-gotten proceeds of their crimes.

6.3.1 Vulnerabilities to counterfeiting and piracy for payment processors

More than US$200 billion dollars in counterfeit and pirated goods were sold online in 2010 alone, and this number continues to increase.[203] Over US$2 billion in fake goods were sold online in the US alone during November and December 2012.[204] These magnitudes underscore the vital enabling role that payment providers play in illicit Internet commerce.

Site operators, including those whose websites sell counterfeit goods, must gain access to a Merchant ID to do business over the Internet, but information requirements differ based on who issues this ID. As a condition of doing business with banks, credit card companies and online payment system providers, merchants must provide detailed information about themselves to facilitate payments and deposits.

Counterfeiters are no exception, and therefore, payment processors typically know and are able to provide helpful details about the people and companies found to be engaged in counterfeiting and piracy. Consequently, the payment processors can help in the prosecution of counterfeiters found to be operating via the Internet. For example, in taking on new merchants, payment processors can carry out Know Your Customer procedures such as those described in earlier chapters.

The complexity of online payment systems (often involving several different entities) undermines enforcement efforts by complicating tracking of the seller's true identity. Sometimes the merchant relationship is directly with the credit card company (a two-party or "closed loop" system), but with most major credit cards (including Visa, MasterCard, and Discover), the relationship is with a third-party acquiring bank. When a credit card company receives notification of counterfeit or fraudulent activity, it must pass this notice on to the acquiring bank for action. Commonly, this relationship is even more attenuated, as fourth-party payment service processing websites (PSPs) have relationships with the acquiring banks.

See Figure 16 on the following page for two examples of these complex relationships, using MasterCard as an example.[205]

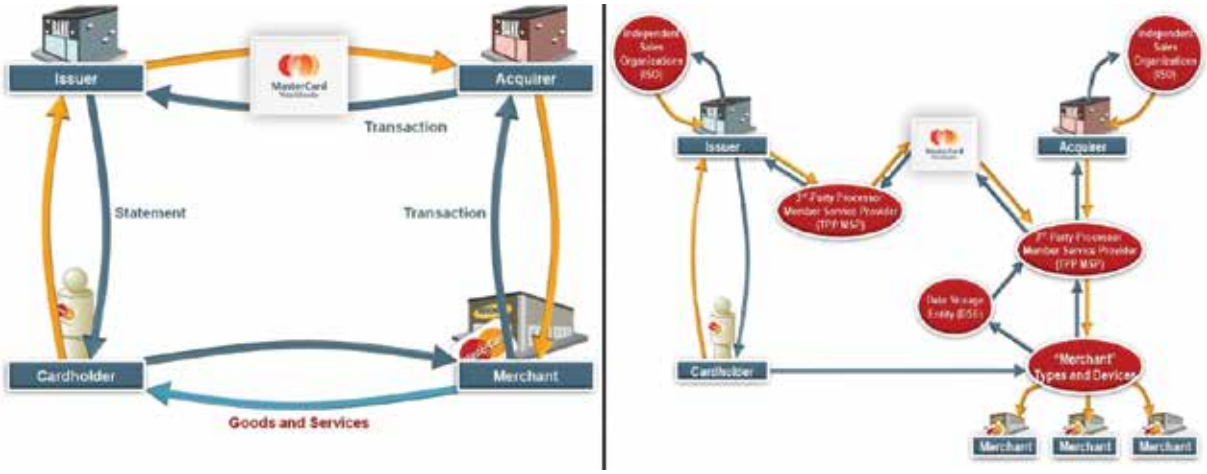


Figure 16: Closed vs. Open Loop Systems. Source: the Copyright Alliance

6.3.2 Current approaches to the problem

Voluntary cooperation with payment processors

One of the first industry-wide programs targeted to deter infringement was proposed in a June 2011 agreement to develop best practices, reached in the US by major credit card companies and payment processors, including American Express, Discover, MasterCard, Visa, and PayPal and MoneyGram.[206] These best practices grew out of meetings convened by the office of the U.S. Intellectual Property Enforcement Coordinator (IPEC) to bring rights holders and payment processors together to explore potential solutions to the increasing Internet sales of counterfeit and pirated goods. Out of these initial discussions, the industry began to develop voluntary practices to withdraw payment services from sites selling counterfeit and pirated goods.[207]

As a consequence, the International Anti-Counterfeiting Coalition (IACC) incorporated the practices into the Payment Processor Portal (now known as the RogueBlock™ program). The IACC designed the program to help rights holders easily notify payment processors of infringing activity, so they can revoke online payments made to "rogue" websites selling counterfeits.[208]

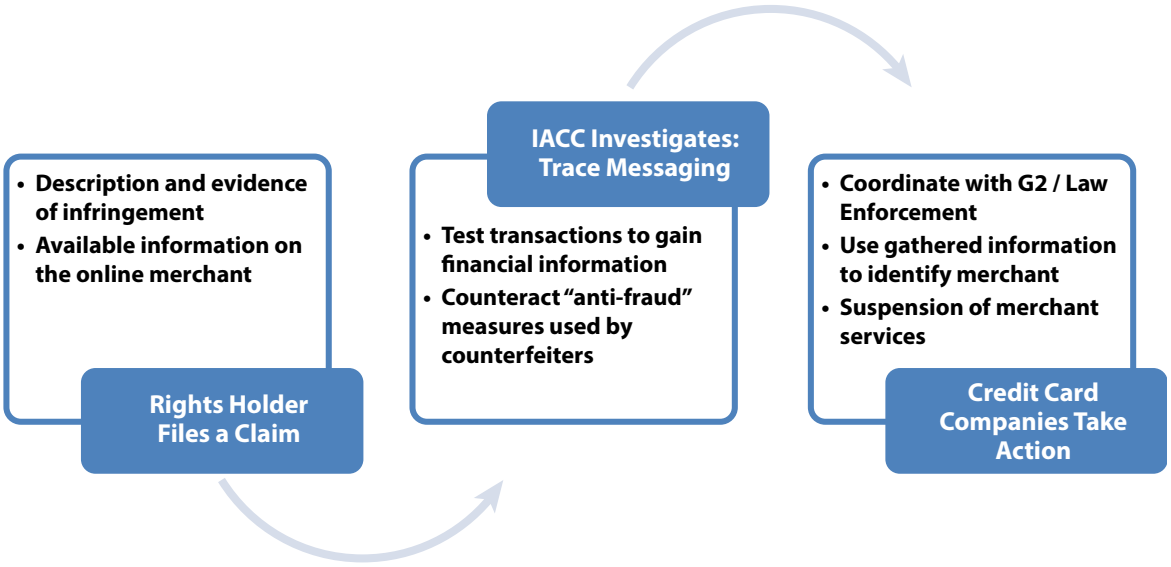
The key steps in the program include:

- a formal claim filed by rights holders;
- an investigation using "trace messaging" by the IACC (a test purchase that traces the merchant information related to the transaction);
- coordination with the National Intellectual Property Rights Coordination Center (IPR Center) in case this claim would interrupt any other ongoing investigations;
- a check to identify any additional related merchant accounts; and
- action on the part of payment processor partners against the merchant based on discoveries from the investigation.

The original program provides a standardized form for reporting rogue websites, including descriptions of the alleged infringement; identities of the site/merchant(s) allegedly engaged in the sale of illegitimate products; and evidence proving the allegation, including proof that the counterfeit could be purchased using a payment processor's services. Such evidence might include a screenshot of the payment processor's logo appearing on the merchant's website and possibly a test purchase transaction.

The program also describes actions for the payment processor to undertake in investigating an infringement claim, including a request for proof of authorization to sell a product, and suspension of payment services if the merchant continues to conduct illicit sales.

Figure 17: Elements of the Payment Processor Portal Program



The program expanded rapidly since its 2012 launch, with over thirty rights holder participants, eight payment processor partners, and multiple law enforcement partners. Despite the program's success, challenges remain. For example, counterfeiters are using more sophisticated measures to detect and evade trace messaging (and subsequent termination of accounts). Examples of these measures include counterfeit merchants making phone calls to confirm orders, or blocking certain IP addresses from accessing their locations. In addition, counterfeit activities increasingly seem to be consolidating with a few particular illegitimate payment service providers that have become increasingly sophisticated in their efforts to evade detection.[209]

The success of the IACC program has extended beyond its original intent. In 2013, the IACC was approached by two major online trading platforms—AliExpress and DHgate—to work with one of its payment processing partners to help clean up infringing listings and sellers on those platforms. The IACC's payment processor partners have also called upon IACC rights holders to assist in training acquiring banks and third-party processors. This sort of collaborative activity is indicative of the opportunities that exist for expanded mutual assistance between rights holders and intermediaries as their engagement and relationships mature.

Rights holder, law enforcement, and payment processor coordination

Rights holders continue to work with payment providers, such as MasterCard, Visa and PayPal, to ensure unlicensed entities are not using their payment services. Representing the recording industry worldwide, IFPI estimates that a program of cooperation involving the City of London Police in the UK has prevented over US$540 million of illegal trade since its launch in 2011, based on the revenues each service generated before payment services were removed.[210]

The program involves IFPI, on behalf of its members, submitting an evidence package to the City of London Police regarding unlicensed sites, which are often based in Russia and Ukraine but offer infringing content to a global audience. The police review this evidence, and if they find a service is operating illegally, they will pass on its details to the payment provider associated with an illegal transaction and other payment intermediaries.

Upon review and confirmation, the payment providers may decide to halt services to a particular merchant bank account for that site. Current payment provider partners in this program include MasterCard, Visa (Inc. and Europe), PayPal, PaySafeCard, Amex, Monitise, PhonePayPlus and Zong. The initiative has now halted payments to more than 50 unlicensed websites, and the program is expanding beyond unlicensed download sites to include infringing cyberlockers.

The Center for Safe Internet Pharmacies (CSIP)

Payment providers have also teamed up with pharmaceutical and pharmacy industry sectors to encourage safe online pharmacies under a 2011 non-profit initiative called the Center for Safe Internet Pharmacies (CSIP).[211] Founding members include payment services and credit card companies such as American Express, Discover, MasterCard Worldwide, Visa, and Paypal, which support the effort through voluntary enforcement.

In the case of payment processors, enforcement consists of removal of payment services from infringing sites once they are identified. Other members—such as Enom, Go Daddy, Google, Microsoft, Neustar, and Yahoo!—participate by de-registering domain names or refusing to advertise fake pharmacies.

The organization's specific goals are as follows:

- Provide a neutral forum for sharing relevant information about illegal Internet pharmacies among members;
- Aid law enforcement efforts where appropriate;
- Establish a publicly available list of all safe online pharmacy websites; and
- Educate consumers about how to find safe medicine online through partnerships with government leaders, regulators, law enforcement, public health and consumer groups, and health care providers.

In addition to its list of safe providers and the ability to "check" a source or purchased drug using its online tools, CISP has a reporting function to allow consumers to blacklist websites that are selling counterfeit drugs. CISP's approach is notable due to its combination of consumer education and enforcement through removal of payment services from sites engaged in counterfeiting and piracy.

6.3.3 Other approaches to consider

Before the launch of these joint industry initiatives, individual credit card companies already had established policies to self-regulate transactions involving illegal drugs and pornography. For example, Visa has provided periodic reminders to its member financial institutions of their responsibilities to ensure that only legal transactions enter the Visa Payment System.

Visa has directed members' attention to controlled substance lists and problematic drugs maintained at the FDA and DEA websites.[212] The company also appears to have self-initiated a regular program of Internet monitoring to ensure that its payment services are not used for the sale of Schedule II controlled substances. This initiative supplements Visa's program to monitor the Internet for credit card sales of child pornography.[213]

While financial service providers, such as credit card companies, generally are not required to question or monitor the legality of the transactions using their facilities or services, exceptions do exist. For example, when the use of a payment processor is so unusual as to suggest illegality in its own right (such as transactions that trigger a Suspicious Activity Report or Currency Transaction Report), or the illegality is both overt and egregious (such as child pornography or Schedule II controlled substances), payment services have voluntarily monitored the use of their systems or services for the illegal transactions.

Some financial service providers have also adopted rigorous internal monitoring programs to detect merchants selling counterfeit goods before rights holders report them. In many cases, when they find a website that they believe may be selling counterfeits, they will reach out to the IACC for confirmation from the rights holder before terminating the account.[214] This kind of proactive approach is effective and beneficial and should be adopted more widely.

6.3.4 Are these practices working?

The IACC program demonstrates robust coordination between rights holders, payment processors, credit card companies, and law enforcement. It employs sophisticated ways of tracking information on counterfeiters, and it has been successful in shutting down some operations.

In its initial two years of operations, the program has identified over 8,900 "rogue" websites and 32,000 payment channels to the payment industry. The result has been the termination of over 3,000 individual counterfeiters' merchant accounts. Over 97% of those payment channels had been terminated or found to be unavailable. The IACC has reported a decreasing number of suspect sites that are able to take payments.[215] A US-based report from October 2012, reviewing both individual payment processor programs and that of the IACC, found "encouraging evidence that such financial takedowns are effective."[216]

Unfortunately, online counterfeiters and infringers often move on to payment service providers that are more difficult to track. Combating these types of PSPs will take increased effort and funding. As payment sector partners analyze intelligence developed through the program, proactive best practices must be put in place before taking on new merchants, including best practices of third-party acquiring banks. These programs need to be developed and improved to prevent rogue merchants from pursuing illegal activities.

The partnership between IFPI and the London City Police is similar in that it involves coordination between rights holders and payment providers. It also directly involves the police who determine whether infringement is extensive enough to move forward. It would be encouraging to see other law enforcement organizations participate in and expand upon this program. As already mentioned above, IFPI estimates that its program has prevented US$540 million in illegal trade since the launch in 2011.[217]

For the pharmaceutical sector, the CISP program's main strength is a resource for consumers investigating the legitimacy of online pharmacies or online product purchases. It also provides an incentive for legitimate online pharmacies to gain a spot on the program's list of safe pharmacies. CISP does allow for reporting: the four participating pharmaceutical companies actively identify and submit "rogue" sites through the portal. The associated public awareness campaigns also have the potential to decrease demand for online counterfeit goods. CISP's main weakness lies in the time-consuming, systematic process required for enforcement or removal of offending online pharmacies.

The independent, voluntary efforts of some credit card companies to monitor and identify more overtly illegal activities, such as child pornography or highly controlled substances, could provide the basis for possible prevention programs in the area of counterfeit goods sold online. They could also be rolled into larger best practices programs—assuming that liability risks, costs and other valid considerations could be managed collaboratively.

6.3.5 Suggested best practices

Electronic payment services are critical to transacting business online. Removing such services has proved highly effective in disrupting sites selling counterfeit products and infringing downloads. There is strong cooperation from the financial industry in this area, both with the City of London police in the UK and the IACC in the US. Such cooperation is based on clear contractual terms between financial intermediaries within the payment networks. Engagement by government and law enforcement to secure commitments by rights holders and intermediaries has helped to operationalize the process.

1. **Improve financial institutions' due diligence processes, including vetting methodologies during account applications that would require merchants to undergo licensing checks and other steps.** Networks can further develop these programs through enhanced on-boarding procedures and collaborative training of banks, PSPs and Merchants by credit card companies and rights holders. As part of this process, they can use the third-party ratings services described in the advertising section of this discussion paper.

2. **Enable streamlined notice and takedown actions by employing easy and standardized notification methods for rights holders. The rights holder should also provide a detailed evidence package to the payment processor.** The IACC program serves as a model for rights holders' provision of standardized notifications to payment processors.

3. **Develop pattern recognition and criteria that could indicate red flags of overtly or egregiously illegal transactions** through cooperative efforts by services, rights holders and enforcement agencies.

4. **Improve dispute resolution mechanisms. This initiative includes a procedure by which payment processors can require merchants to provide documentation to support any claims.** They would also terminate payment processing services for any PSP or online merchant shown to be knowingly engaged in the sales of counterfeit or pirated goods.

Conclusions

This paper is underpinned by the recognition of the vital role intermediaries play in the global supply chain for legitimate commerce. Brand owners and intellectual property rights holders rely on many intermediaries at virtually every step in the process of producing, distributing and selling their products and works. Most intermediaries are reliable and responsible business partners who do not want to do business with criminals or facilitate illegal counterfeiting and piracy practices.

However, this is not the case throughout the supply chain. The purpose of this discussion paper has been to focus attention on the growing misuse and exploitation of intermediary channels to facilitate the production and distribution of counterfeits and pirated goods and services. The paper includes lessons learned by both rights holders and responsible intermediaries and suggests recommended best practices—many based on actions already being taken independently by intermediaries or in collaboration with rights holders and government authorities. The goal is to prevent infiltration of the supply chain by criminal networks and ultimately, stop the flow of counterfeits and other infringing and illegal goods and services.

Across the sectors considered here, intermediaries are becoming involved to different degrees to keep piracy and counterfeiting out of their services. Clearly, a great deal more can and must be done to transform these efforts into a comprehensive, collective response. Where intermediaries are not participating, governments have a strong role to play in clarifying their expectations at a high level. They must drive voluntary arrangements by focusing on outcome delivery and legislating in the absence of progress. All such procedures and legislation must appropriately balance competing fundamental rights.

Voluntary schemes require a sustained commitment by all parties. This investment may come from a few leading companies that want to make a difference and establish new standards. Progress can also come as a result of litigation and promulgation of clear rules that drive intermediaries to adapt. Landlords in the Philippines, for example, began including specific prohibition of counterfeiting in commercial leases after the government made changes to the Intellectual Property Code, which could hold them accountable for infringing activity on their properties.[218]

While establishing collaborative agreements is important, it is only the first step. The test of whether they yield meaningful results lies in their effective adoption in day-to-day operations. A number of the approaches identified in this paper are at that critical stage.

In fact, the theme that emerges most strongly across all chapters is that a gap exists between contractual terms of service and use of infrastructure and the enforcement of these terms. This shortcoming is often exploited to allow the intermediary channel to be exploited for counterfeiting and piracy.

Once this vulnerability is identified and understood, corporate due diligence practices need to be developed and adopted for contractual compliance, just as they have been for regulatory issues such as bribery and corruption, money laundering and ethical sourcing. Where due diligence practices are slow or ineffective, governments must act to preserve the market's integrity. Clearly, in some areas, such as electronic components and illicit tobacco, regulation is already in place. In other areas, such as terms on bills of lading indemnifying shippers for customs costs by their clients, are currently routinely left unenforced in counterfeiting cases.

This paper covers a wide range of intermediaries and addresses the different challenges faced across each of these various players. While many of the suggested best practices are specific to one intermediary group or another, a number of valuable lessons cut across all or several types of intermediaries. For example, the supply chain between producers and consumers is only as strong as its weakest link. It also conveys an understanding that lawlessness or facilitating lawlessness is not an acceptable business practice—neither in physical services nor in online services.

Most importantly, this comprehensive approach provides valuable cross-intermediary lessons; we hope that businesses operating in one sphere can learn from the experiences of those operating in another. For example, establishing and enforcing clear contract terms, knowing customers and suppliers, developing industry standards and codes of practice, identifying and guarding against high-risk behavior patterns, adopting preventive tools, and deploying technologies that improve the effectiveness of the many lessons learned above are all tried-and-true practices that apply here.

Key conclusions

Establish and enforce clear contract terms. This paper has shown that many intermediaries have adopted terms that prohibit the use of their infrastructure or service for counterfeiting and piracy. Services can and should develop terms that specify the corporate due diligence oversight outlined in these suggested best practices. These terms should also apply to any sub-contractors so that they flow down the chain. The tools and processes recommended below and in each chapter should be adopted to make compliance with these terms part of day-to-day operations.

Implement Know Your Customer or Supplier programs. The first step in preventing the misuse of the services that underpin the modern economy is to ensure accountability for behavior through identity verification. In higher risk scenarios, particularly in business-to-business transactions, intermediaries should require authenticated identification that enables them to screen their customers and suppliers and recognize and address abuses, while respecting the obligations of rights to secrecy of telecommunications. Initial customer and supplier screening is critical. The development and use of these practices in areas like online advertising to avoid placing advertisements on high-risk sites is a strong example to be adopted across services, both on and off line.

Develop industry standards and codes of practice. Industry and government standards provide frameworks that drive responsible action. The Authorized Economic Operator program for shipping and the standards developed in electronics and aviation sectors are good examples. The requirements in the US National Defence Authorization Act, like those in the Higher Education Opportunity Act, show how government adoption of standards in public procurement can serve as model practices.

Utilize automated tools to identify transaction patterns. Better technology and collaboration between intermediaries, rights holders and agencies can more effectively identify high-risk behavior patterns and enable resource allocation where it is most needed. Appropriate technology use is increasingly essential in ensuring compliance with contractual language prohibiting the abuse of services for counterfeiting and piracy.

Track and trace, content filtering, content verification and other technical measures to deter the entry of counterfeits and pirated works into the supply chain in real-time are evolving and are being used more broadly as they are improved. Intermediaries' adoption of preventative tools should be in proportion to the risk or reality of high-volume abuse.

Increase automation and transparency of notification, takedown and redress systems, so that these scale to the size of the systems for which they are used.

Intermediaries, government agencies and rights holders must coordinate better, not only to share information and experience among themselves but also to inform, educate and involve consumers, users, customers and business partners about avoiding counterfeit goods and pirated works. The key elements of success include the following: a general openness to cross-stakeholder dialogue; experimentation; flexibility to structure obligations that work within existing systems; definable goals and expectations; and development of policies (both corporate and joint efforts) that solidify commitment and outline the necessary actions for each actor to help stop infringement.

Governments can accelerate the adoption of higher standards and more effective prevention measures by bringing parties together. They must define expectations both in driving voluntary activities and in clarifying the law through enforcement and legislation. Where needed, governments should step forward to propose standards or to clarify obligations.

Rights holders must continue to engage with intermediaries and government—from production through distribution to consumption. Intermediaries' and governments' abilities to connect disparate pieces of intelligence across supply chains, both digital and physical, remains crucial to informing effective action. Encouraging adoption of responsible practices among intermediaries, rights holders, and authorities is needed now. Sharing and dialogue among stakeholders in the fight against counterfeiting and piracy will help ensure that the best practices for deterring illegal activity in one area can be usefully applied in others.

Together, these ongoing efforts will help stem the flow of counterfeits and pirated goods around the world. Building on these lessons to develop new initiatives constitute the next step in delivering a more prosperous future for the businesses that deliver the world's products and services—and the safety and reliability that consumers deserve.

Notes

[1] See full BASCAP Report 'Estimating the global economic and social impacts of counterfeiting and Piracy', February 2011 at http://www.iccwbo.org/Data/Documents/Bascap/Global-Impacts-Study---Full-Report/.

[2] For an overview of the development of global integration see this World Trade Report 2013 from the 'WTO World Trade Report Factors shaping the future of world trade' 2013 at http://www.wto.org/english/res_e/booksp_e/world_trade_report13_e.pdf

[3] International merchandise trade ballooned from $2 trillion in 1980 to over $18 trillion in 2011. Maritime transport alone handles over 80% of the volume of global trade. It accounts for over 70% of its value, with global seaborne trade expanding on average by 3.1% every year since 1970. On the Internet, the number of users has more than quintupled since 2000, with business-to-consumer e-commerce growing by over 21% in 2012 to top $1 trillion for the first time.

[4] Supreme Court of the United States, 27 June 2005, *Metro-Goldwyn-Mayer Studios Inc v. Grokster Ltd and other.*

[5] 508 F.3d 1146 (9th Cir. 2007).

[6] American Bar Association, "A Section White Paper: A Call for Action for Online Piracy and Counterfeiting Legislation" at: http://www.americanbar.org/content/dam/aba/administrative/intellectual_property_law/advocacy/ABASectionWhitePaperACallForActionCompositetosize.authcheckdam.pdf

[7] This discussion is summarized from A. Dixon, Liability of Users and Third Parties for Copyright Infringements on the Internet: Overview of International Developments, in Strowel, Peer-to-Peer File Sharing and Secondary Liability in Copyright Law. Cheltenham: Edward Elgar. 2009.

[8] *Universal Music Australia Pty Ltd v. Sharman License Holdings Ltd.,* [2005] FCA 1242 (5 September 2005), http://www.austlii.edu.au/au/cases/cth/federal_ct/2005/1242.html

[9] Case C-314/12, Judgement of the Court of (4th Chamber) of 27 March 2014

[10] 494 F.3d 788 (9th Cir. 2007), aff'd, 494 F.3d at 808.

[11] 2010 WL 2541367 (June 23, 2010) (Baer, J.).

[12] 600 F. 3d 93, 106 (2d Cir. 2010).

[13] *Chloé SAS v. Sawabeh Info. Servs. Co.*, No. CV 11-04147 GAF (MANx), 2013 U.S. Dist. LEXIS 187398 (C.D. Cal. Oct. 8, 2013).

[14] 591 F. Supp. 2d 1098 (N.D. Cal. 2008).

[15] Section 206 (b) of the Intellectual Property Code of the Philippines (as amended by Republic Act No. 10372) , http://www.gov.ph/2013/02/28/republic-act-no-10372/

[16] Section 206 (c) of the Intellectual Property Code of the Philippines (as amended by Republic Act No. 10372) , http://www.gov.ph/2013/02/28/republic-act-no-10372/

[17] Judgement Summary Judge Rotterdam District Court of 22 august 2006, LJN:AY6661, 264805/KG ZA 06-591).

[18] Wang Zhuo , 'A comparative analysis of legal liability bore by e-commerce platforms for IP infringements' June 2012 at http://ipr.chinadaily.com.cn/2012-06/01/content_15450498.htm

[19] 07 Civ. 2438 (JGK) (S.D.N.Y.). [Along these lines, the US Senate Judiciary Committee has introduced a bill (S 968) that would require online advertising networks, credit card companies and search engines to cut off support for any site found by the courts to be "dedicated" to copyright or trademark infringement. Under S 968, if a website were deemed by a court to be dedicated to infringing activities, federal agents could then tell the US companies that direct traffic, process payments, serve advertisements and locate information online to end their support for the site in question. Copyright and trademark owners would be able to follow up those court orders by seeking injunctions against payment processors and advertising networks.]

[20] 09 Civ. 8458 (RJS) (S.D.N.Y.).

[21] *Gucci America, Inc. et al v. Curveal Fashion et al at* http://www.rfcexpress.com/lawsuits/trademark-lawsuits/new-york-southern-district-court/50897/gucci-america-inc-et-al-v-curveal-fashion-et-al/summary/

[22] *Coach Inc. et al v. Celco Customs Services Co. and Shen Huei Feng Wang* at http://law.justia.com/cases/federal/district-courts/california/cacdce/2:2011cv10787/520847/177/

[23] IHS, 'Combating Counterfeits in the Supply Chain' at https://technology.ihs.com/389481/

[24] RT, 'Fake aircraft parts dealers arrested in Russia', July 2007 at http://rt.com/news/fake-aircraft-parts-dealers-arrested-in-russia/

[25] UPI, 'No grounding of Canadian CC-130Js', February 2013 at http://www.upi.com/Business_News/Security-Industry/2013/02/08/No-grounding-of-Canadian-CC-130Js/UPI-61601360350030/#ixzz2LSpOspQc

[26] IHS Technology, 'Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market' April 2012 at http://www.isuppli.com/Semiconductor-Value-Chain/News/Pages/Top-5-Most-Counterfeited-Parts-Represent-a-%24169-Billion-Potential-Challenge-for-Global-Semiconductor-Market.aspx

[27] Carl Levin, U.S. Senator Michigan, 'Background Memo: Senate Armed Services Committee Hearing on Counterfeit Electronic Parts in the DOD Supply Chain', November 2011.

[28] *Ibid.*

[29] CNN, 'FDA thinks it has trigger in heparin deaths', April 2008 at http://articles.cnn.com/2008-04-21/health/fda.heparin_1_heparin-deaths-scientific-protein-laboratories-changzhou-spl?_s=PM:HEALTH. See also 'Bad medicine', October 2012 at http://www.economist.com/node/21564546; Baxter also faced lawsuits and lost its first case – Bruce Japsen, 'Baxter loses first Heparin case', June 2011 at http://articles.chicagotribune.com/2011-06-09/business/chi-baxter-loses-first-heparin-case-20110609_1_baxter-heparin-animallike-substance-scientific-protein-laboratories.

[30] Walt Bogdanich, 'Heparin Find May Point to Chinese Counterfeiting', March 2008 at http://www.nytimes.com/2008/03/20/health/20heparin.html?_r=0

[31] Japsen, *supra* note 29.

[32] Massachusetts Institute of Technology, 'Scientists Unravel Heparin Death Mystery', June 2008 at http://www.sciencedaily.com/releases/2008/04/080423171529.htm

[33] Fogarty International Center, 'Fogarty study shows poor quality malaria drugs pose threat', May – June 2012, Volume 11 Issue 3 at http://www.fic.nih.gov/News/GlobalHealthMatters/may-june-2012/Pages/fake-malaria-drugs.aspx

[34] Kathleen E McLaughlin, 'Counterfeit medicine from Asia threatens lives in Africa', December 2012 at http://www.guardian.co.uk/world/2012/dec/23/africa-counterfeit-medicines-trade

[35] World Health Organisation, 'Medicines: spurious/falsely-labelled/falsified/counterfeit (SFFC) medicines', May 2012 at http://www.who.int/mediacentre/factsheets/fs275/en/index.html

[36] *Ibid.*

[37] International Tax and Investment Center, 'The Illicit Trade in Tobacco Products and How to Tackle It', April 2011, pg. 14 at http://www.iticnet.org/images/The%20Illicit%20Trade%20in%20Tobacco%20Products%20and%20How%20to%20Tackle%20It%20-%20Second%20Edition2.pdf

[38] Global Acetate Manufacturers Association, 'Membership of GAMA' at http://www.acetateweb.com/membership.htm

[39] See Aerospace Industries Association of America, 'Counterfeit Parts: Increasing Awareness and Developing Countermeasures', March 2011at http://www.aia-aerospace.org/assets/counterfeit-web11.pdf; Find the actual program detail – U.S Department of Transportation, Federal Aviation Administration, 'Advisory Circular', September 1996 at http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/list/AC%2000-56/$FILE/AC00-56.pdf

[40] *Ibid.*

[41] Kevin Beard, 'Counterfeit Parts Impacting the Global Supply Chain' at http://www.nqa-usa.com/resources/articles_detail?id=72; Aerospace AS553 Resource Centre at http://www.as5553.com/

[42] U.S. Pharmacopeial Convention, ' USP Verified Pharmaceutical Ingredients' at http://www.usp.org/usp-verification-services/usp-verified-pharmaceutical-ingredients

[43] Digital Coding & Tracking Association, 'About us' at http://www.dcta-global.com/about-us.html

[44] EC European Anti-Fraud Office, 'Cigarette Smuggling' at http://ec.europa.eu/anti_fraud/investigations/eu-revenue/cigarette_smuggling_en.htm

[45] Philip Morris International, 'What is Illicit Trade' at http://www.pmi.com/eng/tobacco_regulation/illicit_trade/pages/illicit_trade.aspx

[46] This requirement is mandated by the EC Agreement (see Philip Morris International, 'Illicit Trade – E. C. Agreement' at http://www.pmi.com/eng/tobacco_regulation/illicit_trade/pages/ec_agreement.aspx)

[47] JTI, 'Anti-illicit trade' at http://www.jti.com/how-we-do-business/anti-illicit-trade/our-programs/

[48] *Ibid.*

[49] Eric Savitz, 'The Serious Risks From Counterfeit Electronic Parts', November 2012 at http://www.forbes.com/sites/ciocentral/2012/07/11/the-serious-risks-from-counterfeit-electronic-parts/

[50] Jim Avila & Serena Marshall, 'Group Finds More Fake Ingredients in Popular Foods', January 2013 at http://abcnews.go.com/US/exclusive-group-finds-fake-ingredients-popular-foods/story?id=18281941

[51] United Nations Office on Drugs and Crime, 'Counterfeit Products' at http://www.unodc.org/documents/data-and-analysis/tocta/8.Counterfeit_products.pdf

[52] European Commission, 'Stepping up the fight against cigarette smuggling and other forms of illicit trade in tobacco products - A comprehensive EU Strategy', June 2013 at http://ec.europa.eu/anti_fraud/documents/2013-cigarette-communication/1_en_act_part1_v9_en.pdf

[53] National Intellectual Property Rights Coordination Center, United States, 'Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad', November 2011, p10 and 53 at http://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf

[54] Bridging the Gulf, ' UAE on top five list of counterfeit exporters', August 2012 at http://www.bridgingthegulf.org/en/news/news/UAE_on_top_five_list_of_counterfeit_exporters.html?id=967

[55] Frederick M. Fishel, 'The Global Increase in Counterfeit Pesticides', January 2012 at http://edis.ifas.ufl.edu/pi210

[56] U.S. Customs and Border Protection, Office of International Trade, 'Intellectual Property Rights Fiscal Year 2012 Seizure Statistics', January 2013 at https://www.hsdl.org/?view&did=733538

[57] Felix Gillette, 'Inside Pfizer's Fight Against Counterfeit Drugs', January 2013 at http://www.businessweek.com/articles/2013-01-17/inside-pfizers-fight-against-counterfeit-drugs

[58] The United States Department of Justice, 'Michigan Man Charged with Selling Counterfeit Microsoft Software Worth More Than $1.2 Million', November 2012 at http://www.justice.gov/opa/pr/2012/November/12-crm-1335.html

[59] Munir Suboh, 'Seizure of Counterfeit Branded Cigars Imported in Air Freight', May 2012 at http://www.tamimi.com/en/magazine/law-update/section-6/may-4/seizure-of-counterfeit-branded-cigars-imported-in-air-freight.html

[60] National Intellectual Property Rights Coordination Center, 'Operation Global Hoax II Nets Tens of Thousands of Counterfeit Goods in 43 Country Operation' at http://www.iprcenter.gov/partners/ice/news-releases/operation-global-hoax-ii-nets-tens-of-thousands-of-counterfeit-goods-in-43-country-operation; and see also U.S. Immigration and Customs Enforcement, 'Operation Global Hoax II Nets Tens of Thousands of Counterfeit Goods in 43 Country Operation', February 2012 at http://www.ice.gov/news/releases/1202/120221washingtondc.htm

[61] This has proved an effective approach, and is, for the moment, focused heavily on China.

[62] CSR Press Release, UPS, 'UPS Global Trade Technology Showcased for U.S. Customs Compliance', January 2006 at http://www.csrwire.com/press_releases/24356-UPS-Global-Trade-Technology-Showcased-for-U-S-customs-Compliance.

[63] ICC Commercial Crime Services, 'International Maritime Bureau' at http://www.icc-ccs.org/icc/imb

[64] See UNODC-WCO Container Control Programme (CCP) at https://www.unodc.org/unodc/en/drug-trafficking/horizontal-initiatives.html

[65] United Nations Office on Drugs and Crime, 'UNODC-WCO Container Control Programme welcomes its first Caribbean members', August 2012 at http://www.unodc.org/mexicoandcentralamerica/en/webstories/2012/unodc-wco-container-control.html

[66] Phil Taylor, 'UN office taps private sector aid for anti-counterfeit programme', July 2012 at http://www.securingpharma.com/un-office-seeks-private-sector-aid-for-anti-counterfeit-program/s40/a1275/

[67] See European Commission, Action Plan on the enforcement of Intellectual Property Rights at http://ec.europa.eu/internal_market/iprenforcement/action-plan/index_en.htm

[68] Lucy Jones, 'Partners Against Proliferation: Good Practice Guidance', May 2013 at http://www.acsss.info/alpha/partners-against-proliferation

[69] See European Commission, 'Authorized Economic Operators Guidelines', June 2007 at http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/AEO_guidelines_en.pdf; A similar program exists in the USA that focuses on terrorism, called the customs-Trade Partnership Against Terrorism (C-TPAT) – see U.S. Customs and Border Protection, 'C-TPAT: Customs-Trade Partnership Against Terrorism' at http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/

[70] European Commission, 'The IUU Regulation', October 2009 at http://ec.europa.eu/fisheries/cfp/illegal_fishing/info/handbook_original_en.pdf

[71] See Advisory Committee on Commercial Operations of U.S. Customs and Border Protection (COAC) at http://www.cbp.gov/trade/stakeholder-engagement/coac

[72] Sustainable Shipping Initiative at http://www.ssi2040.org/

[73] *Coach Inc. et al supra* note 22.

[74] CropLife Africa Middle East Newsletter, January 2013 at http://www.croplifeafrica.org/uploads/File/forms/communication/newsletter/2013/newsletter_january_2013.pdf

[75] Victoria Knowles, 'Freight Forwarding Agents Warned of Rise in Carriage of Counterfeit Items', September 2012 at http://www.freight-int.com/news/freight-forwarding-agents-warned-of-rise-in-carriage-of-counterfeit-items.html

[76] Pallavi Gogoi, 'Wal-Mart's luxury problem', June 2006 at http://www.nbcnews.com/id/13300234/; see also Jonathan Stempel, 'Burberry accuses TJX of selling counterfeit goods', March 2010 at http://www.reuters.com/article/2010/03/10/tjx-burberry-idUSN1016984620100310.

[77] Alison Arden Besunder & Steve Kimelman, 'Arent Fox "Landlord Program" Eradicates Illegal Counterfeits of Clients' Products at "Counterfeit Triangle"', June 2008 at http://www.besunderlaw.com/pdf/Landlord-Counterfeiting-Liability-Arent-Fox-6-3-2008.pdf; see also Jefferson Siegel, 'Police bust 'Counterfeit Triangle' on Canal St.' Volume 20, No. 42, March 2008 at http://www.downtownexpress.com/de_252/policebust.html

[78] Rachel Tepper, 'Counterfeit Bust: $3 Million In Goods Seized At D.C. Farmers Market In Coordinated Effort', November 2011at http://www.huffingtonpost.com/2011/10/18/dc-counterfeit-seizure-farmers-market_n_1018283.html

[79] Richard Webster, 'Patapsco Flea Market busted with more than $47 million in counterfeit goods', May 2012 at http://www.examiner.com/article/patapsco-flea-market-busted-with-more-than-47m-counterfeit-merchandise

[80] Jerry Norton, 'U.S., Mexico seize $84 million in counterfeit goods', December 2011 at http://www.reuters.com/article/2011/12/22/us-counterfeit-seizure-idUSTRE7BL17V20111222

[81] Bangkok Post, 'Pattaya cops seize fake products', February 2013 at http://www.bangkokpost.com/breakingnews/338169/pattaya-cops-crackdown-on-fake-products

[82] Shane McGinley, '10,000 fake watches seized in Dubai raid', January 2013 at http://www.arabianbusiness.com/10-000-fake-watches-seized-in-dubai-raid-485208.html

[83] Alison Arden Besunder & Steve Kimelman, *supra* note 77.

[84] Satyapon Sachdecha, Anti-counterfeiting 2009 – A Global Guide, 'Thailand', http://www.worldtrademarkreview.com/issues/article.ashx?g=41168b8c-5ed0-4ca2-b93b-9940fa99db4c

[85] International Intellectual Property Alliance, '2009 Special 301 Report on Copyright Protection and Enforcement – Thailand', 2009 at http://www.iipa.com/rbc/2009/2009SPEC301THAILAND.pdf

[86] Office of the U.S. Trade Representative, 'Out-of-Cycle Review of Notorious Markets', December 2012 at http://www.ustr.gov/sites/default/files/121312%20Notorious%20Markets%20List.pdf

[87] See PMC, "Enforcement Of IP Laws In Philippines – A New Beginning" at http://www.mirandah.com/pressroom/item/301-enforcement-of-ip-laws-in-philippines-a-new-beginning

[88] Real Deal at http://www.realdealmarkets.co.uk/about/index.shtml

[89] Hollywood Police Department, 'Landlord Training Program' at http://www.hollywoodfl.org/DocumentCenter/Home/View/153

[90] Organisation for Economic Cooperation and Development (OECD), 'The Economic and Social Role of Internet Intermediaries', August 2010, p12 at http://www.oecd.org/sti/ieconomy/44949023.pdf

[91] Security Week News, 'Digital Piracy and Counterfeit Goods Sites Generate More than 53 Billion Visits Annually', January 2011 at http://www.securityweek.com/digital-piracy-and-counterfeit-goods-sites-generate-more-53-billion-visits-annually

[92] Yellow Brand Protection at https://www.yellowbp.com/

[93] Allison Enright, 'An anti-counterfeit sting hits 132 e-commerce sites on Cyber Monday', November 2012 https://www.internetretailer.com/2012/11/27/anti-counterfeit-sting-hits-132-sites-cyber-monday

[94] eBay, 'Why eBay is the place to be for Sellers in 2013'at http://pics.ebaystatic.com/aw/pics/sell/sellinfocntr/seller-growth.pdf

[95] Janice Yucel, 'The outlet for counterfeit luxury goods: e-commerce', March 2013 at http://blogs.blouinnews.com/blouinbeattechnology/2013/03/20/the-greatest-platform-for-counterfeit-luxury-goods-e-commerce/

[96] Doug Palmer, "China's Taobao makes big push to shed U.S. "notorious" label" September 2012 at http://uk.reuters.com/article/2012/09/26/uk-usa-china-internet-piracy-idUKBRE88P1OE20120926

[97] Thad Rueter, 'Amazon wins a marketplace ruling', August 2012 at http://www.internetretailer.com/2012/08/24/amazon-wins-marketplace-ruling

[98] Janice Yucel, *supra* note 95.

[99] Sue Zeidler, 'Hllywood targets "rogue" mobile apps in war on pirated content', February 2013 at http://www.reuters.com/article/2013/03/01/net-us-hollywood-apps-idUSBRE92003Y20130301

[100] "Stream ripping" is the process of using browser or application (PC or mobile) based software to convert streamed content – which is intended for transient listening – into permanent copies of recordings available on demand on the listener's equipment. A particular problem for the music industry arises from sites and apps that convert licensed video content to audio.

[101] Sue Zeidler, *supra* note 99.

[102] European Commission, 'the functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet', April 2013, p. 16 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0209:FIN:EN:PDF

[103] Phil Muncaster, 'Taobao shoots pirates on Hollywood's orders', September 2012 at http://www.theregister.co.uk/2012/09/10/baidu_alibaba_taobao_piracy_deal_mpa/

[104] eBay, 'How eBay protects intellectual property' at http://pages.ebay.com/help/policies/programs-vero-ov.html

[105] See Allegro's Cooperation in IP Rights Protection program, http://poznaj.allegro.pl/wop/

[106] Overstock, 'Terms and Conditions' at http://www.overstock.com/7935/static.html

[107] Xinhua, 'Tmall to crack down on fake products', December 2011at http://www.china.org.cn/business/2011-12/18/content_24183301.htm

[108] Symantec, 'White Paper - Internet Trust Marks - Building Confidence and Profit Online', 2012 at http://www.creativsymantec.com/webhosting/downl/internet-trust.pdf

[109] See, for example Pro Music at http://www.pro-music.org/

[110] See Music Matters at http://www.whymusicmatters.org/

[111] eBay, 'Build your Business' at http://pages.ebay.com/sellerinformation/sellingresources/toprated.html

[112] European Commission – Intellectual Property – Fight against counterfeiting and piracy, 'Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet – 3rd Quarterly Meeting – 26 May 2012 – Summary', September 2012 at http://ec.europa.eu/internal_market/iprenforcement/docs/mou_meeting_summary_26052012_en.pdf

[113] Doris Li, 'The IP dilemma of Tmall', May 2012 at http://www.chinaipmagazine.com/en/journal-show.asp?id=813

[114] See Motion Picture Association of America, 'The Cost of Content Theft By the Numbers', 2011at http://msl1.mit.edu/furdlog/docs/2011-08_mpaa_infographic.pdf

[115] Greg Kumparak, 'How Dropbox Knows When You're Sharing Copyrighted Stuff (Without Actually Looking At Your Stuff)', March 2014 at http://techcrunch.com/2014/03/30/how-dropbox-knows-when-youre-sharing-copyrighted-stuff-without-actually-looking-at-your-stuff/

[116] US District Court for the Eastern District of Virginia , Indictment, 5 January 2012 at http://www.washingtonpost.com/wp-srv/business/documents/megaupload_indictment.pdf

[117] *Disney Enterprises, Inc., et al. v. Hotfile Corp.,* et al. USDC S.D. Florida, 8 July 2011.

[118] David Price, NetNames, NetNames Piracy Analysis, 'Sizing the Piracy Universe', September 2013 at http://copyrightalliance.org/sites/default/files/2013-netnames-piracy.pdf

[119] Blog, Sam Sundberg, 'TPB har tjänat tio miljoner om året', Svenska Dagbladet, March 2009 at http://blog.svd.se/thepiratebay/2009/03/02/tpb-har-tjanat-tio-miljoner-om-aret/. Piratebay denied such levels of income and claimed even not to have made a profit.

[120] N. Kobie, 'Pirate Bay trio lose appeal against jail sentences', PC Pro, November 2010 at http://www.pcpro.co.uk/news/363178/pirate-bay-trio-lose-appeal-against-jail-sentences#ixzz1SjywcqBr.

[121] *EMI Records Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2013] EWHC 379 (Ch) at http://www.bailii.org/ew/cases/EWHC/Ch/2013/379.html

[122] Figures taken in October 2013 from YouTube, 'Statistics' at http://www.youtube.com/yt/press/en-GB/statistics.html

[123] NMPA, 'What's new' at https://www.nmpa.org/media/showwhatsnew.asp?id=79

[124] Music Rules! at www.music-rules.com and Campus Downloading at www.campusdownloading.com

[125] Ernesto, 'Facebook uses "social signals" and profile information to stop piracy', December 2013 at http://torrentfreak.com/facebook-uses-social-signals-to-stop-piracy-131203/

[126] See IFPI, 'Digital Music Report', 2013 at http://www.ifpi.org/content/section_resources/dmr2013.html

[127] BREIN, 'Uncooperative hosting provider liable for damages', October 2012 at http://www.anti-piracy.nl/nieuws.php?id=282

[128] Internet registries and registrars do not actually host sites, but deactivating or redirecting a domain name is akin to blocking access to the Internet site that had used that domain name.

[129] See U.S. Immigration and Customs Enforcement, 'ICE, European partners seize 328 Internet domains selling counterfeit goods in coordinated operation', June 2013 at http://www.ice.gov/news/releases/1306/130626washingtondc.htm

[130] BBC News Technology, 'Police Crackdown on fake shopping sites', November 2011 at http://www.bbc.co.uk/news/technology-15820758

[131] See press release announcing the new initiative at BPI, 'Music Industry Welcomes Launch of New Intellectual Property Crime Unit' at http://www.bpi.co.uk/media-centre/music-industry-welcomes-launch-of-new-intellectual-property-crime-unit.aspx

[132] Hearing on: "Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II", at http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg65186/pdf/CHRG-112hhrg65186.pdf

[133] European Alliance for Access to Safe Medicines, 'The Counterfeiting Superhighway', 2008 at http://www.eaasm.eu/cache/downloads/dqqt3sge9hwssgcgcos440g40/455_EAASM_counterfeiting report_020608(1).pdf

[134] In the latest in a long series of studies commissioned by ICANN with regard to Whois, a 62-page draft report issued by the National Physical Laboratory (UK) in September 2013 concludes that bad actors, who use the Domain Name System to facilitate illegal or harmful activities, try to avoid being identified or found, and that use of proxy or privacy registration services is one way they do so.

[135] See the list of 12 recommendations made by ICANN, 'Law Enforcement Recommendations Regarding Amendments to the Registrar Accreditation Agreement' at http://www.icann.org/en/resources/registrars/raa/raa-law-enforcement-recommendations-01mar12-en.pdf

[136] Internet World Stats, 'Internet Users in the World' (accessed March 2013) at http://www.Internetworldstats.com/stats.htm

[137] Many third party providers also offer hosting services (which are dealt with in Chapter 2).

[138] IFPI Digital Music Report 2012 at page 16, available at http://www.ifpi.org/content/library/dmr2012.pdf

[139] See David Price, *supra* note 118, pages 19 and 26 referencing data from Sandvine Inc.

[140] BT, 'Terms and conditions', January 2014 at http://www.productsandservices.bt.com/consumerProducts/dynamicmodules/pagecontentfooter/pageContentFooterPopup.jsp?pagecontentfooter_popupid=13408.

[141] BT, 'Acceptable Use Policy (AUP)' at http://www2.bt.com/static/i/btretail/panretail/acceptableuse/.

[142] See the UK government announcement at https://www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy

[143] Brett Danaher, Michael D. Smith, Rahul Telang, and Siwen Chen, "The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France" (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240

[144] See IFPI, *supra* note 126 at page 30.

[145] See Hadopi, 'Rapport d'activité', 2012-2013 at http://www.hadopi.fr/sites/default/files/page/pdf/HADOPI_RapportAnnuel_2013.pdf

[146] IFPI Digital Music Report 2010, page 26, http://www.ifpi.org/content/library/dmr2010.pdf

[147] Center for Copyright Information, 'Memorandum of Understanding ("US MOU")' 6 July 2011at http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf; Updated amendments to MoU available at Center for Copyright Information, 'Resources & FAQ' at http://www.copyrightinformation.org/resources-faq/; see generally J. Menn, Financial Times, 'ISPs agree on web piracy crackdown' July 2011at http://www.ft.com/intl/cms/s/0/b1becb14-a99c-11e0-a04a-00144feabdc0.html#axzz31mBaGHL6.

[148] The Hadopi laws also provided for a legal basis to apply account suspensions but this provision has been repealed by a Decree in July 2013. This is the result of the Lescure recommendations mentioned further below.

[149] See Hadopi, *supra* note 148.

[150] Danaher et al., *supra* note 143.

[151] *EMI Records (Ireland) Limited & ors v The Data Protection Commissioner* [2013] IESC 34.

[152] See European Commission, 'Synthesis Report on the Stakeholders' Dialogue on Illegal Up- and Downloading', March 2011, p. 5 at http://ec.europa.eu/internal_market/iprenforcement/docs/synthesis_report_2009_2010_en.pdf

[153] *Ibid*, sec. 2(A).

[154] A detailed description of the HEOA and its requirements can be found at Educause, 'Higher Education Opportunity Act' at http://www.educause.edu/library/higher-education-opportunity-act-heoa. A description of the plans and policies of certain universities that characterize themselves as "role models" in this area can be found at Educause, 'HEOA Role Models' at http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/educause-policy/issues-and-positions/intellectual-property/heoa-role-models.

[155] Baker & McKenzie.Wong & Leow, "Amendments made to the Copyright Act sharpens Singapore's anti-online piracy tools", August 2014 at http://bakerxchange.com/rv/ff00194ae1868eb8fefd25a1ef468feb515574c8/p=1

[156] American Bar Association *supra* note 6.

[157] This has been expressly found by courts for instance in Austria: Higher Regional Court of Vienna 14 November 2011 (1 R 153/11v) *Constantin Film Verleih and other v UPC Telekabel Wien*; Denmark: Copenhagen City Court 25 October 2006, *IFPI Danmark v Tele2 A/S*; in the United Kingdom, High Court [2011] EWHC 1981, 28 July 2011, *Twentieth Century Fox Film Corp and others v British Telecommunications PLC* and costs were specifically reviewed in Cartier v BSkyB http://www.bailii.org/ew/cases/EWHC/Ch/2003/3354.html

[158] Infocuria, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, [C-314/12] 27 March 2014 at http://curia.europa.eu/juris/document/document.jsf?doclang=EN&text=&pageIndex=1&part=1&mode=lst&docid=149924&occ=first&dir=&cid=516813

[159] *Cartier International and Others vs BSkyB and others* [2014] EWHC 3354 (Ch). http://www.bailii.org/ew/cases/EWHC/Ch/2003/3354.html

[160] *Ibid* paragraph 167.

[161] See IFPI Digital Music Report 2014, at http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf

[162] IFPI Digital Music Report 2013, page 41, http://www.ifpi.org/downloads/dmr2013-full-report_english.pdf

[163] *1967 Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3444 (Ch) at http://www.bailii.org/ew/cases/EWHC/Ch/2014/3444.html

[164] Google, "How Google Fights Piracy" 2014 report at https://drive.google.com/file/d/0BwxyRPFduTN2NmdYdGdJQnFTeTA/view?pli=1

[165] See IFPI, *supra* note 126 at p 28.

[166] See Envisional, 'Technical report: An Estimate of Infringing Use of the Internet', January 2011 at http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf

[167] See IFPI, *supra* note 126 at p 28.

[168] See Google infographic on 'Winning the War on Bad Ads' at http://services.google.com/fh/files/misc/info-final.pdf

[169] Google, 'Transparency Report', September 2013 at http://www.google.com/transparencyreport/removals/copyright/?hl=en

[170] See Millward Brown Digital, Understanding the Role of Search in Online Piracy (Sept. 2013)

[171] Google, 'Transparency Report' at http://www.google.com/transparencyreport/

[172] RIAA, "Google's Move to Demote Pirate Sites - Is It Really Working?" February 21, 2013 at http://www.riaa.com/news_room.php?content_selector=riaa-news-blog&blog_type=&news_month_filter=2&news_year_filter=2013

[173] See House of Commons, Culture, Media and Sport Committee, 'Supporting the creative economy', HC 674, paras. 31-32, September 2013 at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/674/674.pdf

[174] *Ibid.*

[175] See para 4.1.1 of the report by Mike Weatherley, IP Advser to the UK Prime Minister at http://www.mikeweatherleymp.com/2014/05/29/search-engines-and-piracy-a-discussion-paper-by-mike-weatherley-mp/

[176] Ernesto/TorrentFreak: "Google's New Search Downranking Hits Torrent Sites Hard" at http://torrentfreak.com/googles-new-downranking-hits-pirate-sites-hard-141023/

[177] Kent Walker, General Counsel, Google, 'Making Copyright Work Better Online', December 2010 at http://googlepublicpolicy.blogspot.com/2010/12/making-copyright-work-better-online.html

[178] Thomas Catan,'Con Artist Starred in Sting that Cost Google Millions', January 2012 at http://online.wsj.com/article/SB10001424052970204624204577176964003660658.html

[179] Digital Citizens Alliance, March 2014 at http://media.digitalcitizensactionalliance.org/3DE696054309A422E45E08789A37B98CA008EEE5/62eb9ba4-d80b-48f0-af35-9f1870757265.pdf

[180] See Cour de Cassation Arrêt n° 832 du 12 juillet 2012 (11-20.358) - Première chambre civile [in French] at http://www.courdecassation.fr/jurisprudence_2/premiere_chambre_civile_568/832_12_23884.html

[181] *Cosmetic Warriors v Amazon.co.uk Limited* [2014] EWHC 181 (Ch) at http://www.bailii.org/ew/cases/EWHC/Ch/2014/181.html

[182] For Bing: See Bing ads, 'Intellectual Property Guidelines' at http://advertise.bingads.microsoft.com/en-us/support-center/search-advertising/intellectual-property-guidelines; For Google: See Google, 'Copyright' at http://support.google.com/adwordspolicy/answer/176015?hl=en

[183] Google, 'Adwords Trademark Policy' at http://support.google.com/adwordspolicy/answer/6118?hl=en&ref_topic=1626336

[184] Congress of the United States, Washington DC, Letter addressed to Mr. Larry Page, CEO Google Inc., April 2012 at http://blackburn.house.gov/UploadedFiles/Blackburn_Maloney_Letter_4-3-12.pdf

[185] Jane Hamsher, 'Rep. Maloney Letter Blasting Google's Larry Page Over Android Sex App Marketed to Students', September 2012 at http://bytegeist.firedoglake.com/2012/09/18/bytegeist-exclusive-rep-maloney-letter-blasting-googles-larry-page-over-android-sex-app-marketed-to-students/

[186] Adrian Goldberg, 'Google admits profiting from illegal Olympic ticket ads', January 2012 at http://www.bbc.co.uk/news/business-16468846

[187] Change.org, 'Petitioned Larry Page: Larry Page, CEO of Google: Pull all ads promoting the sale of ivory on Google pages immediately' at https://www.change.org/petitions/larry-page-ceo-of-google-pull-all-ads-promoting-the-sale-of-ivory-on-google-pages-immediately

[188] Tony Romm & Michelle Quinn, 'Google search to be anti-piracy enforcer', October 2011 at http://www.politico.com/news/stories/0812/79573.html

[189] See Thomas Catan, *supra* note 178.

[190] Lucia Moses, 'New report says how much advertising is going to piracy sites', February 2014 at http://www.adweek.com/news/advertising-branding/new-report-says-how-much-advertising-going-piracy-sites-155770

[191] USC Annenberg Lab, 'Ad Transparency Report', January 2013 at http://www.annenberglab.com/sites/default/files/uploads/USCAnnenbergLab_AdReport_Jan2013.pdf

[192] USC Annenberg Lab , 'Online Advertising Transparency Report' at http://www.annenberglab.com/adminfiles/files/USCAnnenbergLab_AdReport_Jan2013.pdf

[193] See Digital Citizens Alliance, "Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business" at http://media.digitalcitizensactionalliance.org/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf

[194] Association for National Advertisers, 'ANA, 4A's Release Statement of Best Practices Addressing Online Piracy and Counterfeiting' at http://www.ana.net/content/show/id/23408

[195] JIC WEBS, 'DTSG UK Good Practice Principles', December 2013 at http://www.jicwebs.org/agreed-principles/digital-trading-standards-group-good-practice-principles/153-dtsg-uk-good-practice-principles

[196] See 4A's, 'Industry Groups Urge Marketers to Take Affirmative Steps to Address Online Piracy and Counterfeiting', March 2012 at http://www.aaaa.org/news/press/Pages/050312_online_piracy.aspx

[197] See Audit Bureau of Circulations, "The value of content verification tools," http://www.abc.org.uk/-News-And-Views-/News/The-value-of-content-verification-tools//

[198] HttpWatch at http://www.httpwatch.com/moreinfo.htm

[199] International Chamber of Commerce, 'ICC Policy Statement : Safeguarding against misplacement of digital advertising', March 2014 at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2014/ICC-Policy-Statement---Safeguarding-against-misplacement-of-digital-advertising/

[200] See for example, Katy Bachman, 'This man protects marketers from bogus websites', March 2013 at http://www.adweek.com/news/technology/man-protects-marketers-bogus-websites-149345 (discussing "Veri-Site," a company offering the service of rating websites for infringement. See section 4.2.5 above for examples of some of these services.

[201] See paragraph 41.4 of the report from the IP adviser to the UK Prime Minister, Mike Weatherley at http://www.olswang.com/media/48204227/follow_the_money_financial_options_to_assist_in_the_battle_against_online_ip_piracy.pdf

[202] See Katie Evans, 'Online counterfeit sales will cost businesses $135 billion this year', January 2011 at http://www.internetretailer.com/2011/01/05/online-counterfeit-sales-will-cost-businesses-135-billion; and Barbara Thau, 'Find a faker: How to spot online counterfeiters', 2012 at http://today.msnbc.msn.com/id/42016042/ns/today-money/t/find-faker-how-spot-online-counterfeiters/

[203] For the 2010 figure, see ibid.

[204] For the 2012 figure, see TechJournal, 'Cybercriminals sold record number of counterfeit and fake goods online', January 2013 at http://www.techjournal.org/2013/01/cybercriminals-sold-record-number-of-counterfeit-and-fake-goods-online/

[205] See PowerPoint from the Copyright Alliance, 'The Value of System Integrity: How the Franchise Protects Cardholders' at http://copyrightalliance.org/files/Mastercard%20DC%20Trip%20on%20Piracy.ppt

[206] U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement, 2011 at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_2011_report.pdf

[207] *Ibid.*

[208] G2 Web Services, 'The International AntiCounterfeiting Coalition Developing New Online Tools to Choke Off Money to Rogue Websites', September 2011at http://www.g2webservices.com/iacc/

[209] See International AntiCounterfeiting Coalition (IACC), 'IACC Payment Processor Portal Program: First Year Statistical Review', October 2012 at http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf

[210] See IFPI, *supra* note 126 at p 28.

[211] The Center for Safe Internet Pharmacies at http://www.safemedsonline.org/

[212] Mark MacCarthy, 'Safety of Imported Pharmaceuticals: Strengthening Efforts to Combat the Sales of Controlled Substances over the Internet' (statement given by the Senior Vice President, Public Policy, Visa USA, Inc. before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, U.S. House of Representatives, December 13, 2005).

[213] *Ibid.*

[214] ACEC recognizes that there may be practical limitations on the relief that credit card companies and other payment services can provide. For example, even if a seller's account is blocked, it may be difficult to stop the seller from opening a new account at one of many other Visa or MasterCard member banks. There may also be issues concerning the credit card companies' right to take action under current law without a court order, which could be addressed in any legislation addressing these matters.

[215] IACC, 'Payment Processor Portal Service Extended to Service Providers', August 2012 http://members.iacc.org/news/104806/Payment-Processor-Portal-Service-Extended-to-Service-Providers-.htm

[216] Full report available at Damon McCoy, Christian Kreibich et al., 'Priceless: The Role of Payments in Abuse-advertised Goods', October 2012 at http://cseweb.ucsd.edu/-savage/papers/CCS12Priceless.pdf

[217] See PMC *supra* note 87.

[218] http://www.mirandah.com/en/categories/item/301-enforcement-of-ip-laws-in-philippines-a-new-beginning.html

The International Chamber of Commerce

ICC is the world business organization, a representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world.

The fundamental mission of ICC is to promote open international trade and investment and help business meet the challenges and opportunities of globalization. Its conviction that trade is a powerful force for peace and prosperity dates from the organization's origins early in the 20th century. The small group of far-sighted business leaders who founded ICC called themselves "the merchants of peace".

ICC has three main activities: rule setting, dispute resolution, and policy advocacy. Because its member companies and associations are themselves engaged in international business, ICC has unrivalled authority in making rules that govern the conduct of business across borders. Although these rules are voluntary, they are observed in countless thousands of transactions every day and have become part of the fabric of international trade.

ICC also provides essential services, foremost among them the ICC International Court of Arbitration, the world's leading arbitral institution. Another service is the World Chambers Federation, ICC's worldwide network of chambers of commerce, fostering interaction and exchange of chamber best practice. ICC also offers specialized training and seminars and is an industry-leading publisher of practical and educational reference tools for international business, banking and arbitration.

Business leaders and experts drawn from the ICC membership establish the business stance on broad issues of trade and investment policy as well as on relevant technical subjects. These include anti-corruption, banking, the digital economy, marketing ethics, environment and energy, competition policy and intellectual property, among others.

ICC works closely with the United Nations, the World Trade Organization and intergovernmental forums including the G20.

ICC was founded in 1919. Today its global network comprises over 6 million companies, chambers of commerce and business associations in more than 130 countries. National committees work with ICC members in their countries to address their concerns and convey to their governments the business views formulated by ICC.

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 F +33 (0)1 49 53 28 59
www.iccwbo.org

The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 F +33 (0)1 49 53 28 59
www.iccwbo.org