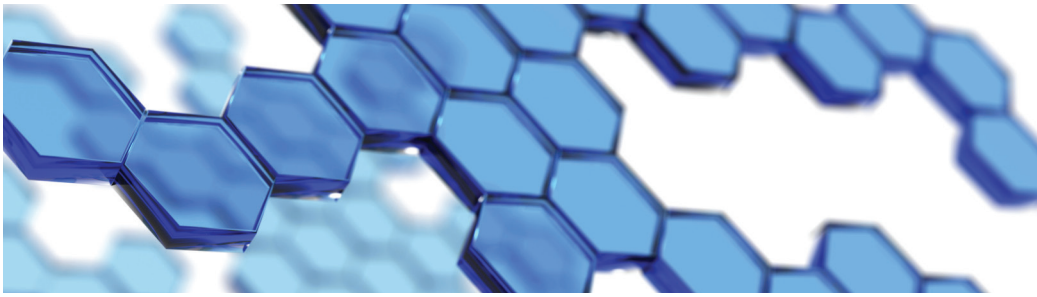
ROLES AND RESPONSIBILITIES OF INTERMEDIARIES:

FIGHTING COUNTERFEITING AND PIRACY IN THE SUPPLY CHAIN



ICC ADVOCACY

BASCAP

Business Action to Stop Counterfeiting and Piracy

EXECUTIVE SUMMARY

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

Table of Contents

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).

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 to help responsible intermediaries more effectively deal with vulnerabilities in their operations and encourage intermediaries who knowingly facilitate IP infringement to stop. The result is a product that challenges the status quo and offers a roadmap for discussion, collaboration and resolution.

Executive Summary

Fakes in the supply chain

Increasingly complex and far-reaching supply chains create new risks and vulnerabilities that enable the infiltration of counterfeit goods and copyright piracy into legitimate trade channels. Counterfeiters exploit the supply chain and feed counterfeit electronic components into mobile phones, computers, printers, automobiles, defense systems and airplanes. Fake raw materials and ingredients can make their way into final products like pharmaceuticals, pesticides and tobacco products—unbeknownst to the manufacturer that sells the final product or the consumer that buys it. This situation can compromise the integrity of final products, generate losses to legitimate businesses and expose consumers to fake, faulty or harmful products.

And while the Internet offers an amazing, virtually unlimited conduit between suppliers and consumers, one in five consumers is unknowingly shopping on websites that offer fake products. Consumers find it difficult to distinguish between a legitimate e-commerce site and one set up to sell fakes—and it's almost impossible to guard against a counterfeit product that has made its way on to a legitimate e-commerce site. At the extreme, some Internet platforms are completely dedicated to piracy and counterfeiting—making so-called "free" movies, music and e-books, and bargain-priced consumer goods widely available, or encouraging users to upload and trade in infringing content on a staggering worldwide basis.

Counterfeiters and pirates are also exploiting other essential intermediary services. Property owners may unknowingly rent space to criminals who use the premises to manufacture or sell fakes. Massive trans-oceanic ships are duped with fake documents to carry millions of containers filled with counterfeit products or fake raw materials. Pirates abuse the Internet's new highways to host fake storefronts and manipulate search results to lure and exploit trusting customers. Payment processors and credit card companies are used to cover online transactions for counterfeits as if they were legitimate purchases. Advertising networks have been hijacked so that for-profit criminal sites are making money from ads representing legitimate companies. And the world's social media websites are being exploited to circulate illegal versions of songs, movies, software and books.

Counterfeiting is big business

The problem of counterfeiting and piracy problem has grown hand-in-hand with the globalizing economy and it is evident that counterfeits account for a growing proportion of international trade. The OECD estimated in 2008 that there are more than $250 billion in physical counterfeit goods moving across borders each year, not to mention in-country activities, Internet infringement, and indirect losses to governments and consumers. Together, it is estimated that the global impact of these activities could add up to a staggering $1.7 trillion annually.

The role and responsibility of Intermediaries

Intermediaries play an essential role in bringing a product from its conception to design, assembly, manufacture, marketing and distribution to the final consumer. They are the backbone of commerce and include suppliers of raw materials and components, transport, shipping and distribution companies, landlords and shop owners, online marketplaces, internet service providers, search engines and advertising networks, websites, credit card companies and even the popular social media sites.

The globalization of trade has dramatically multiplied the number of intermediaries and increased the complexity of global supply chains. The greater the number of intermediaries and the more elaborate the supply chain, the more vulnerable the system is to infiltration and exploitation by counterfeiters.

The fight against the global epidemic of counterfeiting and piracy requires responsible action by multiple parties: governments to enact legislation; police to enforce laws; customs agents to protect borders; rights holders to build protections into their product development, manufacturing, marketing and distribution systems; and consumers to "say no" to counterfeits.

Intermediaries also have a responsibility to restrict use and abuse of their infrastructures to prevent counterfeiting and piracy. 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. Experience shows that most intermediaries, when better informed about potential exploitation and the damage done by counterfeiting and piracy, demonstrate a willingness to secure their portion of the supply chain from abuse.

Study objectives

This body of work examines many, but not all, of the critical types of intermediaries that are vulnerable to IP infringement. It analyses steps taken to reduce vulnerabilities and suggests best practices to curb IP infringements in the supply chain.

The objectives of this study are to:

1. Raise 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 on the part of intermediaries, enlisting them to engage both independently and with rights holders and authorities to discourage counterfeiting and piracy.
3. Identify alternative approaches 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. Present suggested 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

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. 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 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 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 conclusions

While many of the suggested best practices are specific to one intermediary group or another, the comprehensive approach taken in this study reveals a number of valuable cross-intermediary lessons, not the least of which is that lawlessness or facilitating lawlessness is not an acceptable business practice, neither in physical services nor in online services. Moreover, the simple adage that a chain is only as strong as its weakest link applies to defending the supply chain from IP infringements. Standard practices applied elsewhere—such as 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 many of the suggested best practices—are all tried-and-true business practices that also apply to protecting the supply chain from infiltration of counterfeit goods and copyright piracy.

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 misused 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.

The following list summarizes the cross-cutting measures that can be utilized by all intermediary sectors to eliminate vulnerabilities in the supply chain that enable the infiltration of counterfeit goods and copyright piracy:

- **Establish and enforce clear contract terms.** This paper shows 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 Defense 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: 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.** 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.

Suggested best practices

For each of the six categories of intermediaries, the full study presents a set of suggested best practices—mostly voluntary in nature—for intermediaries working together with rights holders and governments to more effectively address the global problem of counterfeiting and piracy.

The suggested best practices are largely derived from the analysis that precedes them in each section of the full report, with the aim to highlight the use of the best possible measures that have been promoted, tested or have already been taken by some intermediaries somewhere to address abuse of their services. The following is a summary list of these for each of the six categories.

Part I: Physical Intermediaries

Chapter 1. Raw materials and component suppliers

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.**
2. **Carefully monitor suspicious customer orders by suppliers of active ingredients and other essential components.**
3. **Develop standards and guidelines for third-party accreditation mechanisms.**
4. **Deploy technologies, such as tracking and tracing, where possible, to complement monitoring and compliance efforts.**

Chapter 2. Transport operators

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.**
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.**
3. **Put monitoring systems in place to flag shipments of counterfeit and pirated products.**
4. **Establish a provision that requires transport operators to supply electronic shipment information to customs administrations in advance of shipment arrivals.**
5. **Expand the Authorized Economic Operator (AEO) program and other accreditation schemes to include an IPR element.**

Chapter 3. Landlords

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.**
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.**
3. **Landlords and market administrators should require periodic inspection of lessees' shops and stalls for obvious counterfeit goods.**
4. **Increase the use of nuisance abatement laws and public-private task forces to target problem landlords.**

Part II: Online Intermediaries

Chapter 4. Sites, platforms, portals and services

4.1 Online marketplaces

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.**
2. **Encourage stronger enforcement of the *Terms of Service* between site owners and traders, with increased cooperation between service providers and rights holders.**
3. **Implement due diligence checks by e-commerce site owners to ensure a basic understanding of who is trading on their site.**
4. **Adopt appropriate, automated risk management tools to identify high-risk behaviors and potential red flags.**

4.2 Content-sharing services

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.**
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.**
3. **High-level engagement between service providers, rights holders and government can advance the development and adoption of the practices identified above.**

Chapter 5. Infrastructure providers

5.1 Internet hosting services

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.**
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.**
3. **Encourage the development of reliable and transparent risk indexing services.**

5.2 Domain registrars

Domain names are the language addresses of the Internet. Terminating services to sites that engage in wholesale criminal activities by domain name system registrars and their agents 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 abuse, including a strong Registrar Accreditation Agreement (RAA).**
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.**
3. **Strictly enforce terms of service by Registrars to block or revoke domain names for sites predominantly engaged in infringing activities.**

5.3 Internet service (access) providers

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, judicial authorities may order that information relevant to the infringement of an IPR might be provided by the intermediary, while also overseeing any actions taken as a result. 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.**

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.**

3. **Implement *Notice* and *Repeat Infringer* policies, in cooperation with rights holders, based on notice and graduated response principles.**

4. **Block subscriber access to internet sites or online services that a competent authority or court has found to be designed or operated with the clear intention of inducing or promoting infringement; or to be knowingly facilitating or enabling large-scale infringement without taking reasonable steps to prevent it.**

Chapter 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 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.

Examples below have been proposed or to some extent adopted—from search results optimization for non-infringing sites to demoting infringing sites and links based on the provider's own algorithm (as Google has recently announced), or from a third-party rating service as these mature. While most copyright owners believe that a broader range of measures can and should be taken to address these problems, search engines and content companies are urged to engage in dialogue to discuss divergent views on the efficacy and appropriateness of search engines engaging in these suggested best practices. Together, they can progress toward resolving these serious issues in a manner satisfactory to all parties.

1. **Enhance notice and takedown systems to offer standardized and efficient notification methods to rights holders and make information available on their use.**

2. **Discuss ways to improve keyword-blocking mechanisms and auto-complete functions to better screen links to online infringement.**

3. **Take appropriate steps to address advertisements by infringing websites.**

4. **Improve the discoverability of legitimate services and reduce the prominence of links to infringing content and websites distributing counterfeit goods.**

6.2 Online advertising

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.**

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.**

3. **Advertising agencies and other intermediaries should implement a parallel, commercially reasonable process to exclude infringing sites from their ad placement services.**

4. **Communicate more effectively to advertising intermediaries that paying advertising fees to sites that law enforcement is investigating may amount to money laundering.**

6.3 Payment processors

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.**

2. **Enable streamlined notice and takedown actions by employing easy and standardized notification methods for rights holders.**

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, including a procedure by which payment processors can require merchants to provide documentation to support any claims.**

Closing Remarks

The singular objective of this study is to eliminate vulnerabilities in the supply chain that enable the infiltration of counterfeit goods and copyright piracy. It is intended that this product challenges the status quo and offers a roadmap for discussion, collaboration and resolution.

Notably, defending the supply chain from IP infringements should employ the same standard practices applied elsewhere, such as 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 many of the suggested best practices. All are tried-and-true business practices that also apply to protecting the supply chain from infiltration of counterfeit goods and copyright piracy.

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

ICC INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

BASCAP
Business Action to Stop Counterfeiting and Piracy

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