



Rights holders and intermediaries: all in this together

BASCAP
Jeff Hardy

Anti-counterfeiting 2015 A Global Guide

**World
Trademark
Review**[™]

INTELLECTUAL PROPERTY RIGHTS PROTECTION – NOW MORE THAN EVER

CRITICAL DRIVER OF INNOVATION, GROWTH AND JOBS

Government efforts to stimulate economic growth and employment must include the critical role that IP plays in driving innovation, development and jobs. Now is the time to increase the resources committed to stopping the illegal trade in counterfeits and piracy. Learn more about joining BASCAP and making the fight against counterfeiting and piracy the #1 priority.



Apple
Baker & McKenzie
British American Tobacco
Caterpillar
Chanel
Croplife International
Diageo
Hewlett Packard
Japan Tobacco International
Lacoste
McGraw Hill Financial
Microsoft
NBC Universal
Nestlé
Nike
Pfizer
Phillip Morris International
Procter & Gamble
Shell International
Unilever
Universal Music/Vivendi

Business Action to Stop Counterfeiting and Piracy (BASCAP) connects and mobilizes businesses across industries, sectors and national borders in the fight against counterfeiting and piracy. Members include some of the largest and most recognized companies in the world—all with a common goal of stopping the trade in counterfeited and pirated goods and the associated economic and social harms associated with it.

Learn more at www.iccwbo.org/bascap

Rights holders and intermediaries: all in this together

Author
Jeff Hardy

Brand owners and rights holders rely on intermediaries at virtually every step in the process of producing, distributing, marketing and selling their products and works. Intermediaries play a critical role in providing services within the supply chain, connecting producers and consumers and opening new market opportunities. Most intermediaries are reliable and responsible business partners which do not want to do business with criminals or facilitate the illegal practices of counterfeiting and piracy.

Global markets and extended supply chains make it much harder to know, manage and control every intermediary and see their every transaction. This is complicated by the explosion in internet use, which now connects more than 3 billion people and their devices through a myriad of connected services and platforms. A number of supply chain vulnerabilities have become more evident under these pressures and criminal agents have seized opportunities to exploit them. Identifying and pursuing counterfeit and pirate producers and suppliers is now a multi-jurisdictional and diffuse task, with supply chains that can more easily re-establish themselves after action is taken.

The International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy has released a major new paper, *Roles and Responsibilities of Intermediaries – Fighting Counterfeiting and Piracy in the*

Global Supply Chain looking at a range of important intermediaries to show how criminal networks and other infringers routinely use and abuse intermediary services to facilitate the global trade in illicit merchandise and digital products, documents the steps being taken to prevent this infiltration and suggests further steps to curb these abuses. (<http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/International-engagement-and-Advocacy/Roles-and-Responsibilities-of-Intermediaries/>)

The paper looks at intermediaries operating both in the physical world and online that are particularly susceptible to counterfeiting and piracy:

- 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 cars, aircraft, appliances and computers.
- Transport operators provide critical services that are misused 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. The shipping process requires documentation that yields a paper trail which can help to identify the originators and owners of the counterfeit goods.

- 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 notice from rights holders or raids from law enforcement.
- The category of online sites, platforms and portals includes a wide group of services that connect users to make offers and sales or share content or links. It comprises marketplaces, such as eBay and the Apple App Store; user-generated content sites such as YouTube; social networks such as Facebook; and cyberlockers such as Hotfile. The group also includes websites such as The Pirate Bay, which connect users of peer-to-peer networks. Many of these are used legitimately millions of times daily. They have all been vulnerable to significant abuse through counterfeiting and piracy and must continually improve their systems to tackle such abuse. Others are simply dedicated to piracy and

counterfeiting and encourage users to fill the sites with infringing content.

- Infrastructure providers form the technical backbone of the Internet, on which all web services are built and delivered. Three main services are covered in this category: hosting providers such as Rackspace, which offer the server space to store either a whole website or specific content displayed on other sites; domain registries such as Nominet and their registrars, which provide names for websites and connect them to the IP address of the hosted site; and internet access providers such as British Telecom, which connect users to the Internet – these are the final link as all data must pass through their systems to reach end users and consumers.
- The economic viability of online services depends on search providers, online advertisers and payment processors to find an audience and generate revenue. Search is the critical function that enables discovery within the network across all of these sites; advertising provides both a means of discovery and a source of revenue; while direct payment takes place using credit cards and other payment services such as PayPal.

With knowledge comes understanding

Documenting the ways in which intermediary services are abused is an important first step. Awareness is critical to help responsible intermediaries to deal more effectively with vulnerabilities in their operations, and to curb the activities of intermediaries that knowingly propagate



Documenting the ways in which intermediary services are abused is an important first step. Awareness is critical to help responsible intermediaries to deal more effectively with vulnerabilities in their operations

and/or permit IP infringement through their services.

Experience shows that most intermediaries – when better informed about other, non-IP related uses of their services and resulting negative impacts on society – are willing to secure their portion of the supply chain. 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; and
- credit card companies have taken action to block payments for illicit commerce (eg, narcotics, gambling).

The paper shows that many intermediaries have adopted contractual terms that prohibit the use of their infrastructure or service for counterfeiting and piracy. Services can and should develop these terms and oversee compliance with them. The terms should also apply to any subcontractors so that they flow down the chain, and the tools and processes recommended below and in the paper should be adopted to make compliance with these terms part of day-to-day operations.

Know your supplier

One of the core steps that rights holders and intermediaries can take is to perform due diligence checks on their business partners. Businesses are used to carrying out such checks and risk assessments in relation to data protection, trade compliance or bribery and corruption. Since it is much less common to have procedures and continuous improvement processes in place regarding the handling of intellectual property by supply chain partners, the paper encourages a wider and deeper application of know-your-supplier procedures.

Know your customer

Some sectors go further in performing due diligence on customers as well as

suppliers. This practice is more commonly conducted in order to avoid trading with parties that are subject to government sanctions. Governments have shifted the onus of making such checks onto business in other areas as well, such as requiring banks, lawyers and other professionals to verify identity before providing services and to report unusual transactions in order to combat money laundering.

Compliant customers can be rewarded with enhanced status. In the transport sector, authorised economic operator status in the European Union is based on a shipper's record in addressing security risks. The US Advisory Committee on Commercial Operation (COAC) of Customs and Border Protection formed the IP Rights Enforcement Sub-committee to assist in providing feedback and to work with Customs on IP rights facilitation, enforcement, deterrence, partnership and modernisation programmes.

Improved online identity verification is part of the new agreements that the Internet Corporation for Assigned Names and Numbers (ICANN) requires from domain registries and is a crucial part of proposed updates to the WHOIS database. The BASCAP discussion paper identifies the need for ICANN to ensure that registries are implementing these contractual requirements and to conclude its work on improving WHOIS while developing further protocols regarding proxy services.

The first step in preventing misuse of the services that underpin the modern economy is to ensure accountability for behaviour 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 recognise and address abuses, while respecting obligations such as rights to secrecy of telecommunications.

Development and adoption of voluntary standards

The process of developing a voluntary standard and creating a market in services

supporting it can be seen at different stages among many of the different categories of intermediary identified in the BASCAP paper. The aerospace industry was one of the first to take such an operational approach in this area, and as these standards are developed, they can be incorporated into commercial contracts.

In 1989 the failure of counterfeit bolt-pins holding the tail to the aircraft was 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. A US audit found that 39% of spare parts in the US Federal Aviation Administration (FAA) inventories were suspected of being counterfeit. Parts were sold through supplier intermediaries, with supply channels running from distributors to manufacturers and to airline and third-party repair stations.

By 1996, cooperation with industry groups resulted in the publication of an FAA advisory circular which detailed the Voluntary Industry Distributor Accreditation Programme (VIDAP). VIDAP is an accreditation system based on voluntary industry oversight and formally established third-party accreditation of distributors. The following standards were proposed for independent accreditation programmes:

- standards and guidelines for third parties;
- a 17-point review of the distributor's quality system, including checks on traceability, documentation and parts storage; and
- mandated audits every 36 months.

The risk is still not merely theoretical. For example, in 2007 Russian police intercepted and arrested a criminal group for stealing and then illegally reproducing commercial aircraft parts and accompanying documentation for sale in Russia and other countries.

This process has now spread to other sectors. In online advertising, for example, over the past four years efforts have been made to help brand owners to ensure that they do not market their products on sites supplying pirate or counterfeit materials.

In the United States, the Association for National Advertisers and the American Association of Advertising Agencies, with support from the Interactive Advertising Bureau, released a Statement of Best Practices in May 2012; and in December 2013 UK industry body the Digital Trading Standards Group published the UK Good Practice Principles for the Trading of Digital Display Advertising. These principles include recommendations that contractual terms between buyer and seller identify where content should not appear, and include the use of tools to achieve this.

Just as the FAA plays a role in the



Jeff Hardy

Director

jeffrey.hardy@iccwbo.org

Jeff Hardy has been the director of the International Chamber of Commerce (ICC) initiative Business Action to Stop Counterfeiting and Piracy (BASCAP) since its creation in mid-2005. BASCAP unites the global business community across all product sectors in an effort to stop the counterfeiting of goods and IP piracy. It focuses on setting standards for global performance by governments and companies; framing decisions for policy makers; advocating for the allocation of resources at the highest levels in national governments; and building global awareness.

Mr Hardy joined the ICC in 1999 as a policy adviser and previously held various positions with the US government.



The first step in preventing misuse of the services that underpin the modern economy is to ensure accountability for behaviour through identity verification

aerospace example, the City of London Police is making available the Infringing Website List, enabling industry bodies such as the Internet Advertising Bureau UK, the Incorporated Society of British Advertisers and the Institute of Practitioners in Advertising to point members towards this as a resource when implementing the principles.

Using intelligence to be proactive

Regular training is included in the control system of logistics firm DHL and is mirrored in the area of payment processing. Credit card networks and other electronic payment providers have organised regular regional events to disseminate knowledge to acquiring banks and other parts of the payment network to help them to proactively spot potential abuse, as well as preparing them to act on notices of particular transactions. Such training helps to develop the pattern recognition that can lead to proactive identification of risky transactions beyond simply a notice and takedown approach.

Fraud teams at e-commerce platforms including eBay and Alibaba, and advertising platforms such as Google, regularly report removing large volumes of listings based on their own analysis. This is similar to the use of compliance technologies on stock exchanges to look for suspicious transactions resulting from insider trading.

Similarly, Google's recent announcement of a revision to its algorithm to demote sites in search results based on notices of infringement is an example of how analysis of the data regarding abuse of a platform can

inform proactive approaches.

Overall, the practices in the BASCAP paper suggest that better technology and collaboration between intermediaries, rights holders and agencies can more effectively identify high-risk behaviour patterns and facilitate resource allocation where it is most needed. Appropriate technology is increasingly essential in ensuring compliance with contractual language prohibiting the abuse of services for counterfeiting and piracy.

As they improve, track and trace and other technical measures to deter the entry of counterfeits and pirated works into the supply chain are being used more broadly. Intermediaries' adoption of preventive tools should be in proportion to the risk or reality of high-volume abuse.

Governments have clear role

The role of government in facilitating and maintaining focus on improving outcomes from these processes is another common theme. As with the examples above, the Office of the US Intellectual Property Enforcement Coordinator has been instrumental in facilitating several voluntary initiatives, including in the payment processing sector and addressing counterfeit pharmaceuticals sold via the Internet.

The European Union brought together e-commerce platforms with a memorandum of understanding in 2011 and the July 2014 EU IP Enforcement Action Plan focuses on risk management and supply chain due diligence as a key enabler of counterfeit and piracy reduction. The

EU Joint Research Council is incorporating piracy and counterfeiting into its review of the use of track and trace in addressing security threats.

Governments must also secure their own supply chains, and this provides an opportunity to encourage the adoption of standards and reward compliance through their use in public procurement contracting.

Comment

Across the sectors considered in the BASCAP paper, what becomes clear is that intermediaries are getting involved to different degrees to take responsibility for keeping piracy and counterfeiting out of their services; but that a great deal more can and must be done to transform these efforts into a comprehensive, collective response. While the discussion paper suggests best practices that are specific to each of the intermediary sectors reviewed, there are overarching lessons and best practices that, if adopted, can benefit all.

In conclusion, rights holders must continue to engage with intermediaries and government from production through distribution to consumption. The ability to connect disparate pieces of intelligence across supply chains, both digital and physical, remains crucial to informing effective action.

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.

It is vital to encourage the adoption of responsible practices among intermediaries, rights holders and authorities. Sharing and dialogue among stakeholders in the fight against counterfeiting and piracy will ensure that the best practices for deterring illegal activity in one area can be usefully applied in others.

As intermediaries align themselves with voluntary efforts and raise the bar for keeping counterfeiting and piracy out of genuine commerce, those that are complicit or wilfully negligent become more visible and can become the focus of enforcement efforts where needed. The development of new initiatives built on the lessons learned thus far will deliver a more prosperous future for the businesses that deliver the world's products and services – and secure consumers the safety and reliability that they deserve. **WTR**



BASCAP

International Chamber of Commerce
33-44 avenue du Président Wilson
75116 Paris
France

Tel +33 1 49 53 28 27

Fax +33 1 49 53 28 59

Web www.iccwbo.org/bascap

**To learn more about contributing to
Anti-counterfeiting 2016 – A Global Guide, contact:**

John Eborall on
+44 20 7234 0606 or at
jeborall@GlobeBMG.com
(EMEA & Americas)

or

Dan Cole on
+852 5665 5774 or at
dcole@GlobeBMG.com
(Asia-Pacific)