

WIPO MAGAZINE

OCTOBER 2018

SPECIAL
ISSUE



IP value capture: fostering trade by capturing the value of creative industries in developing countries

p. 4



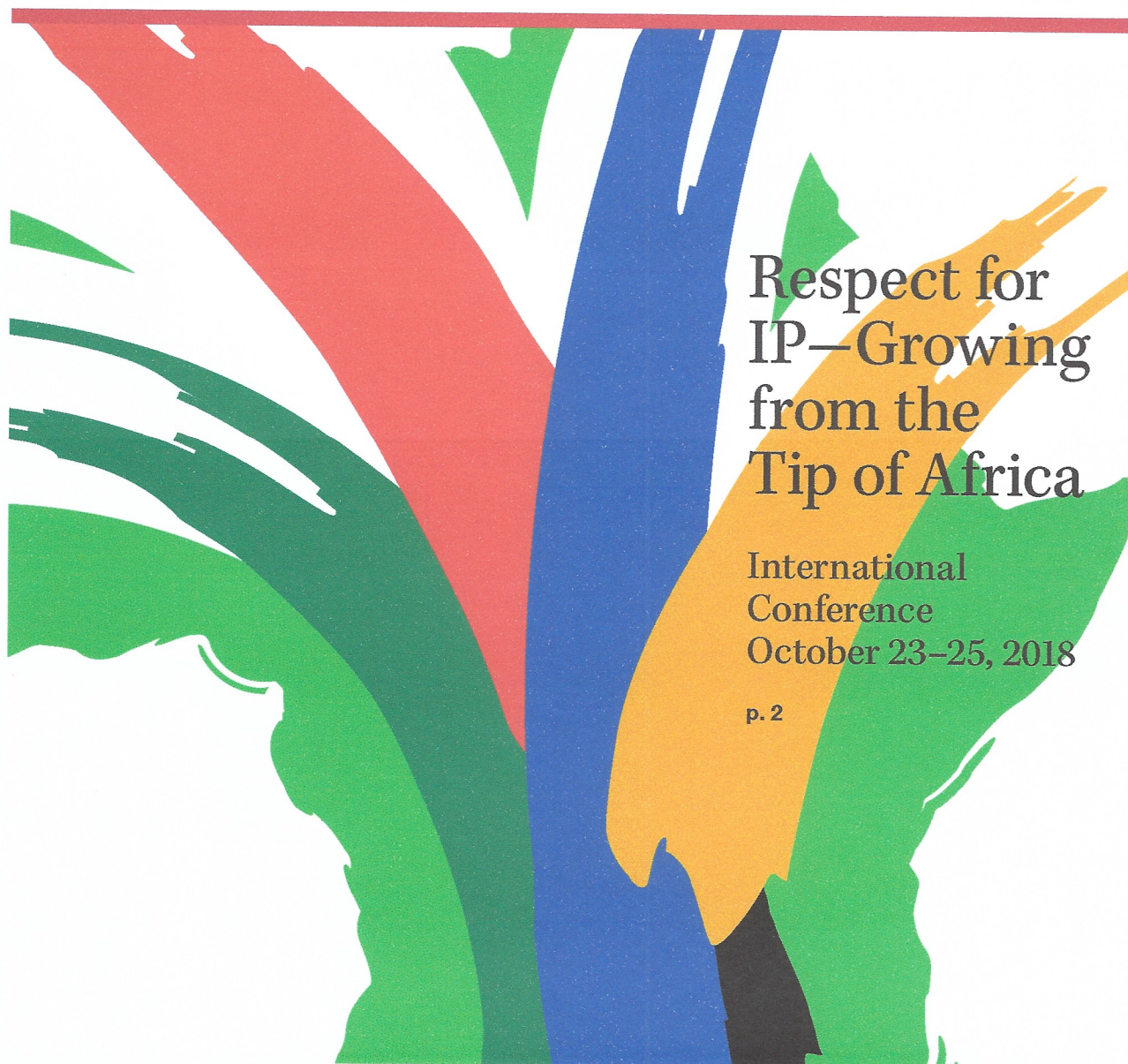
The global digital enforcement of intellectual property

p. 28



Innovating for the whole world: IP's role in development

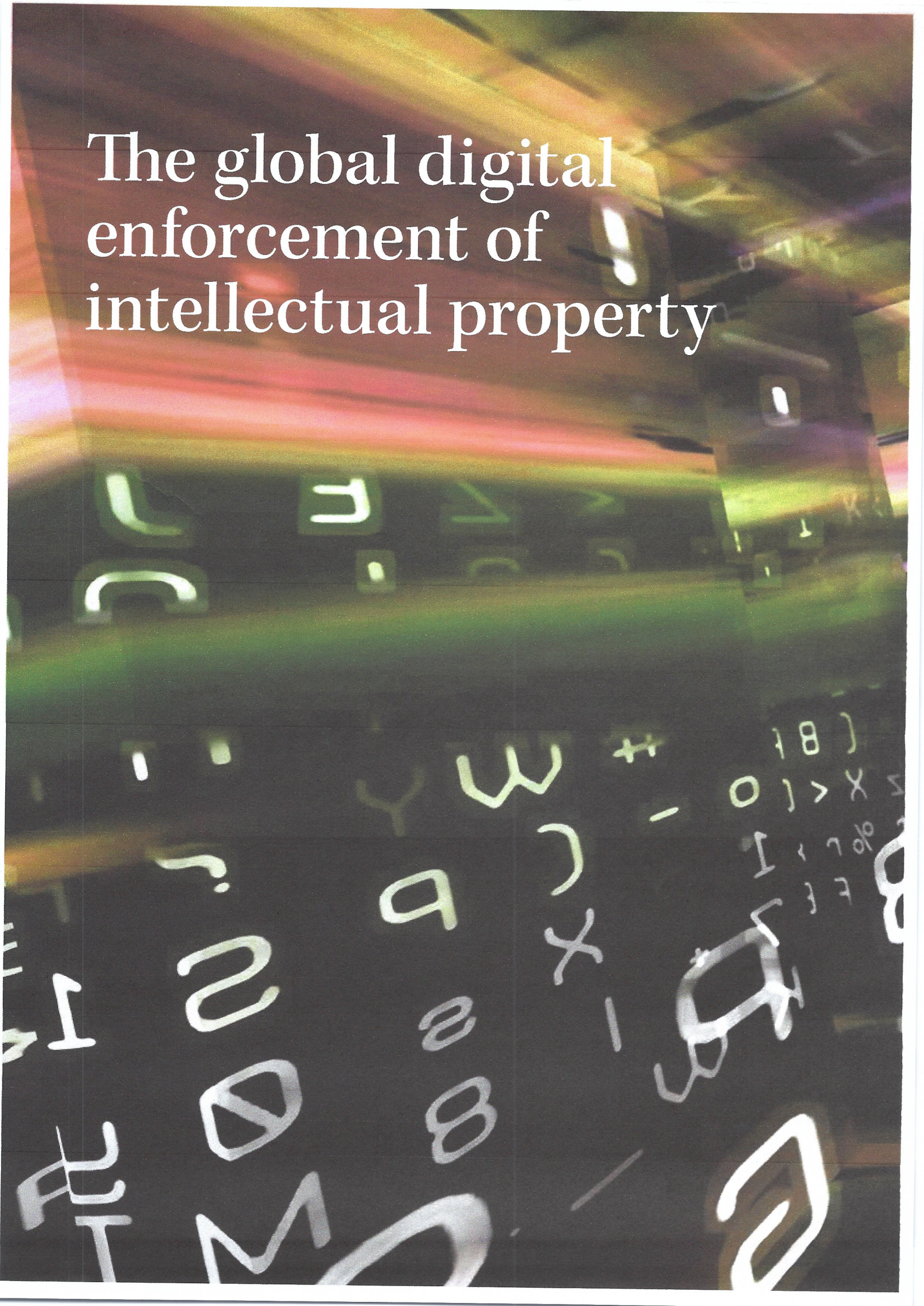
p. 20



Respect for
IP—Growing
from the
Tip of Africa

International
Conference
October 23–25, 2018

p. 2



The global digital enforcement of intellectual property



Photo: Raymond Peltzer - Alamy Stock Photo

Digital technology has transformed our lives, but increasingly, the interconnected technologies we embrace are being turned against us. For example, Bad Actors are using technology to flood the online market with pirated and counterfeit goods.

By **Frederick Mostert**,
 Professor of Practice
 at the School of Law,
 King's College, London
 and Research Fellow at
 the Oxford Intellectual
 Property Research Centre,
 University of Oxford*,
 United Kingdom

Digital technology is arguably humankind's greatest achievement since speech. Thanks to Big Tech and the advent of platforms such as Google, Alibaba, Amazon, Facebook, and Twitter, the way we live, search for things, shop, communicate, and even woo each other have all changed fundamentally.

Digital technology has freed up our time from manual tasks; it enables us to keep in touch globally and to be informed on a scale never experienced in history. But as we open our houses to ever more interconnected technology, as governments ponder the idea of "smart cities," and as the hunger for convenience and speed push caution to one side and increase our attack surface, the same technology we are embracing is being turned against us.

Bad Actors are exploiting technology in multiple ways: by pilfering private data to steal funds from bank accounts; by misusing social media and advertising data; by placing false ads to unsuspecting consumers; by posting child abuse; by texting hate speech, or by spreading fake news. The Bad Actors engage in these activities while hiding behind the hallowed tenets of free speech. They are also weaponizing technology and they are using it smarter and more efficiently than Good Actors.

A case in point is the ruthlessly efficient way in which Bad Actors use technology to flood the online market with pirated and counterfeit goods. Their success in churning out perfect copies at unprecedented volume and speed stands in stark contrast to the slow and faltering way in which Good Actors use technology to authenticate their product through supply and distribution chains.

How then does one reconcile these seemingly irreconcilable fundamental issues in our new world?

THE CHALLENGES OF THE DIGITAL ENVIRONMENT

Existing solutions in the digital environment are often subject to intractable challenges. First, the identity of the counterfeiter is often unknown to the brand or content owner. Second, the anonymity problem exacerbates the "whack a mole" phenomenon – where a webpage is taken down and another online listing pops up under a different URL almost instantly – as the infringers themselves evade identification. Third, the sheer volume and velocity of online counterfeit sales make online listings very time sensitive – they are typically posted for a few hours or days only, making timely online tracking and tracing of counterfeit listings extremely difficult. Fourth, pirates and counterfeiters typically use more than one website in different countries raising questions of international jurisdiction and the enforcement of foreign judgments. And fifth, there is no uniform, international mechanism for delisting and blacklisting online pirated goods and counterfeits.

These challenges raise the thorny issue of whether regulation may be an effective response to the smart use of technology by Bad Actors in the digital world. Regulation intuitively goes against the very grain of the prime directive of the original dreamers of the digital age when they built the Internet. Digital pioneers John Postel, Sir Tim Berners-Lee, and Vincent Cerf postulated a free and unfettered cyberworld – a glorious environment where information flows freely, where the right to know is a given,

*Professor Mostert is also the founder of the Digital Communities Lab (London), United Kingdom.

where scientific collaboration is easy, where you can express your opinions without censure, and where free competition allows you to set up an online business that knows no boundaries or borders. So how then to reconcile that which is potion with that which is poison?

There is, though, an even larger and more pressing issue in the digital era. Courts and legislatures around the world have become woefully inadequate in dealing with, and stopping, the actions of Bad Actors online. As Professor Tim Wu has warned, the volume and frequency of online activities are unprecedented. The law has traditionally lagged behind commercial and technological development. And playing catch-up in the online context has turned into an increasingly desperate struggle by courts trying to keep up with the explosively rapid pace of technological development, as foreseen by Moore's Law (by which the number of transistors per square inch on integrated circuits has doubled every year since they were invented). It makes no sense for a brand or content owner to run to court – at great expense – to stop the single sale of a pirated or counterfeited product on a digital platform because the actual listing typically appears online for only a few hours. Moreover, such action does

nothing to address the multitude of other fake listings posted by other Bad Actors.

SOCIAL MEDIA, PIRATES AND COUNTERFEITERS

A new and particularly insidious threat is the proliferation of counterfeits on social media. A recent UK Intellectual Property Office study warns that “social media is increasingly a key part of a complex eco-system to divert traffic from authentic sites covering myriad rogue online platforms.” The official pages of internationally well-known brands on Facebook, Instagram, and WeChat have all been subjected to counterfeiters using them openly to tout their pirated goods and counterfeits. Jenny Wolfram, CEO of BrandBastion, notes that “during a two weeks’ period earlier this year, one brand pirate posted 114 comments, advertising counterfeit goods on the Instagram accounts of many internationally famous brands.” (See *WIPO Study on Approaches to Online Trademark Infringement*).

Apart from lost sales for the legitimate brand owner, pirated goods and counterfeits listed on social media can pose a significant threat to public health and safety.

Existing solutions in the digital environment are often subject to intractable challenges, which raise the thorny issue of whether regulation may be an effective response to the smart use of technology by Bad Actors in the digital world.

Photo: gorodenkoff / iStock / Getty Images Plus



Photos: MBI / Alamy Stock Photo



A recent UK Intellectual Property Office study warns that “social media is increasingly a key part of a complex eco-system to divert traffic from authentic sites covering myriad rogue online platforms.”



Photos: vichai phubutphapan / Alamy Stock Photo

Digital technology has transformed the way we live, search for things, shop and communicate.

In the United Kingdom, a recent law enforcement operation seized “tens of thousands of counterfeit and unsafe goods, including dangerous cosmetics, perfumes, razor blades, electrical products and chargers, as well as clothing, footwear, leather goods and tobacco products.” (See *WIPO Study on Approaches to online trademark infringement*). The haul ranged from such items as “Android TV boxes with unsafe mains chargers, to several hundreds of counterfeit Cinderella dolls containing high levels of toxic phthalates.” The UK National Trading Standards warns that “fake goods are not subject to the stringent safety checks that genuine goods, made by legitimate businesses, must comply with.”

In addition, listings of counterfeit goods on social media inflict serious reputational harm on brands. Customers of the genuine brand are confused by listings that piggyback onto the genuine social media pages of brands and are tricked into buying fake products. These disgruntled customers, in turn, post their own very damaging remarks about the brand on the same media page for all other customers to see. Counterfeiters have established dedicated storefronts on social media platforms such as Facebook, possibly in an attempt to evade the more stringent anti-counterfeit measures increasingly being adopted by online e-commerce platforms like Alibaba, Amazon and eBay.

The root cause of nefarious activity is anonymity on the Internet. The cloak of anonymity allows Bad Actors to evade detection. Only if the wrongdoing is systematically tracked and traced to the source of the problem – from the digital world to a physical location – can enforcement make any substantive headway.

Although it seems logical to stop the toxic flow of counterfeit and pirated goods at the distribution point of the gatekeepers – the web, and social media platforms – this is as successful as trying to make a river reverse its flow at the estuary.

ALIBABA'S ALTERNATIVE APPROACH

Alibaba has adopted an alternative approach, following up on initiatives developed by the Chinese and UK governments. It is tracking and tracing pirated and counterfeit goods directly from the digital platform listing to the physical source (see *Intellectual Property and e-commerce: Alibaba's perspective*, page 35).

It has spearheaded the use of new technologies such as big-data analytics and machine learning, thereby setting a new benchmark for web and social media platforms in this area. These measures serve to both proactively remove counterfeit listings and track down the source of counterfeits and the factories that produce them.

By working with law enforcement authorities, Alibaba's system is able to intelligently parse information to identify counterfeiters and potentially reveal the manufacturing source by tracing the movement of funds. Alibaba's initiative has already borne fruit. By sharing information gleaned from these tools with law enforcement officials in China, authorities have seized counterfeit goods worth RMB 1.43 billion (approximately USD 209 million) and eliminated 417 production rackets.

DIGITAL TOOLS

Social media and web platforms, intermediaries, and right holders around the world are at the forefront of the battle against digital copying. These groups have responded to the problem by developing and adopting an array of digital tools in surprisingly similar ways. But what are the intended and unintended norm-setting consequences of these digital tools?

The current online environment cries out for a legal analysis of the contemporary technical tools employed to combat digital infringements. They include Blockchain applications; social media tools; blacklisting and whitelisting; follow-the-money tools; domain name tools; search engine de-indexing; hack-back and active defense; and various notice actions.

As much as one would like a court of law to mete out individual justice in every single case, this ideal is unrealistic and makes no sense in the digital environment. As pointed out in the *Financial Times* (8 June 2016), “Pirates are more adept at using new technologies than those trying to shut them down.” Michael Evans, Alibaba's president, has asserted, however, that Alibaba has “the tools to change the way the war is waged ... using data and technology ... to defeat the counterfeiters... If Alibaba delivers, it will be a game changer by stopping counterfeiting at source rather than at platform level.”

In response to an increase in online sales of pirated and counterfeit products, voluntary cooperation between

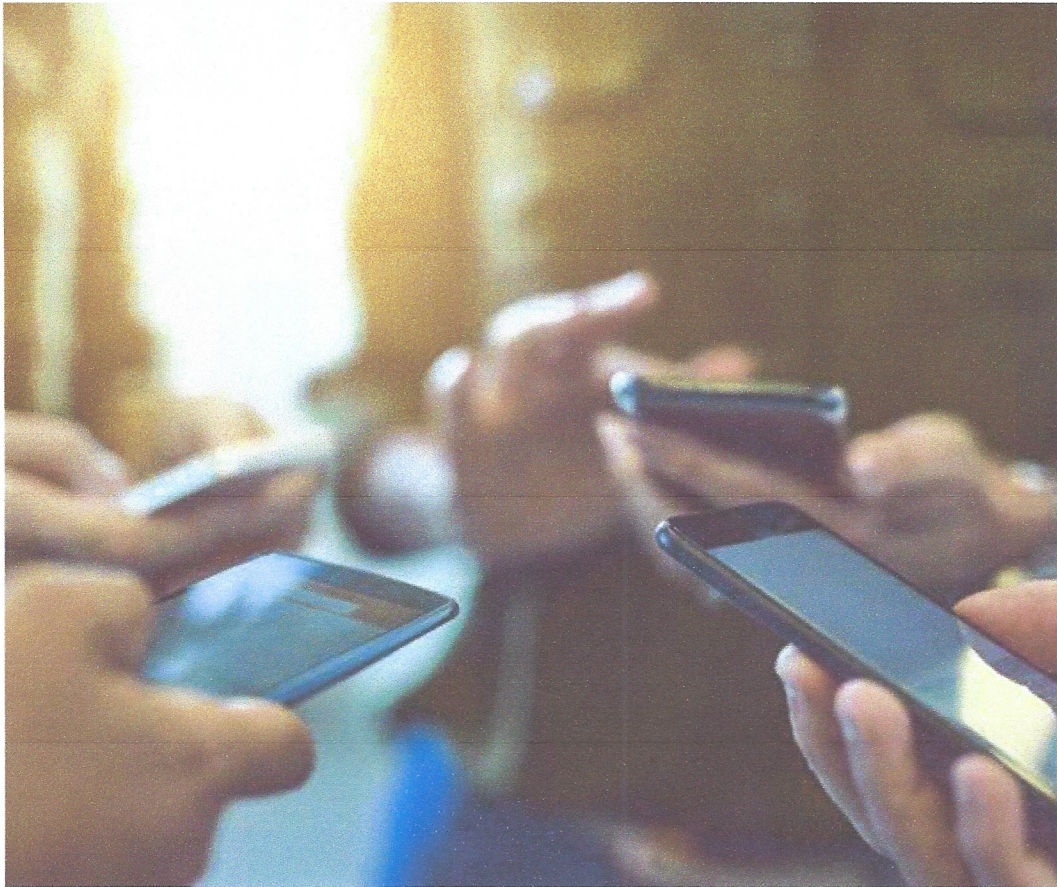


Photo: Peopleimages / E+ / iStock / Getty Images Plus

online platforms and right holders has proven successful, to some extent, but has not been fully effective in stopping online counterfeit sales. These measures are designed by web and social media platforms themselves (the new gatekeepers), drafted in cooperation with right holders, or supported by states and their administrative authorities.

THE NEED FOR GLOBAL GUIDELINES

De facto guidelines have already developed around the world with right holders, online and social media platforms, and government law enforcement authorities voluntarily cooperating across borders. These guidelines are in need of further evolution because the Internet is by its nature global. As anyone in charge of enforcement efforts will attest, the borderless digital environment and associated global jurisdictional issues make matters vastly challenging. They represent some of the great digital challenges which directly affect the law on online private data, social media advertising, hate speech, fake news, counterfeiting, and piracy at this moment. They also bring a certain provocative element and excitement to this body of law.

Effective digital counter-measures are dependent on voluntary, collaborative, technical, and legal standards. In-depth research is urgently needed into the new norm-setting which flows directly from the use of digital tools that are already paving the way for new legal standards throughout the world.

The borderless digital environment and associated global jurisdictional issues represent some of the great digital challenges that directly affect the law on private data, social media advertising, hate speech, fake news, counterfeiting, and piracy today.