

# Bring out the bots

Ian Block and Andrea Fuelleman examine the need for technological solutions to combat online counterfeiting

The old adage says that imitation is the sincerest form of flattery. Counterfeiting is not a new threat to famous brands – indeed, luxury brands lose about \$30bn worth of income a year to fake goods sold online. With advancing technology, counterfeiting is increasingly manifesting itself in many ways, and most notably, online. The online market is growing at such a rate that it has even caught the attention of the Trump administration, which recently tasked the Departments of Homeland Security and Commerce, among other federal groups, with drafting a plan to combat the sale of online counterfeits.

Counterfeiters are creating fake accounts on social media, using stock imagery and strategic keywords to pass off fake goods as authentic, and using technology to forge importation and warranty documents, all of which can make online counterfeits practically undetectable to the ordinary buyer, especially at the time of purchase.

For many brands, the current landscape places the onus on the rightsholders themselves to regularly (and often manually) scrutinise and monitor the web for infringements, and submit hundreds or even thousands of takedown requests or send individual cease-and-desist letters on a case-by-case basis.

This endeavour can be very difficult and resource intensive given the limited (accurate) contact information available in online listings. While new technology can be used to create and/or mask counterfeits, in many instances, it just as easily can be leveraged to spot them as well. With the significant proliferation of counterfeit goods being offered for sale all over the web, the manual system of monitoring and submitting takedowns is becoming unfeasible and inefficient for many brand owners. As a result, there is an increasing need to develop and adopt technological solutions to help combat the influx of counterfeits online.

Many online retailers are adopting zero tolerance policies and are leveraging technology and marketplace insight to develop tools to help detect and enforce against counterfeits online. While still in its early stages, effective anti-counterfeiting tools often utilise machine learning technology and artificial intelligence, which look for inconsistencies and errors in listings to separate the fakes from legitimate

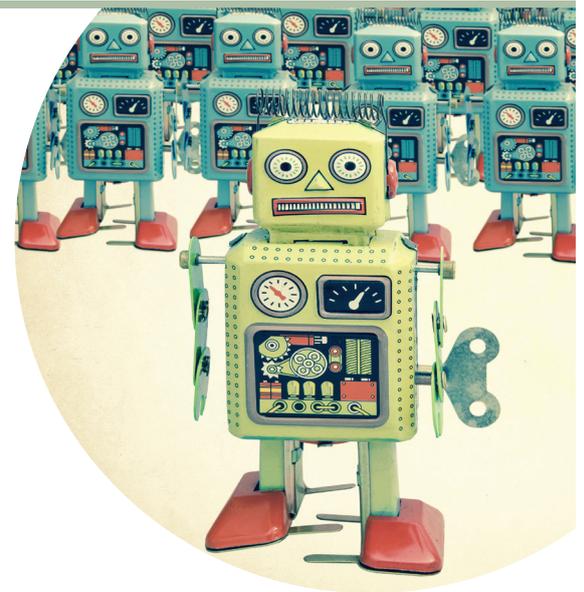
merchandise. Although implementing the new technology is still fairly expensive, demand is gradually increasing.

Highlighting the success of new machine learning and AI-based anti-counterfeiting technology is Entrupy, which is an authentication company that uses a database of microscopic images from luxury goods including bags, shoes, watches, jewellery, and so on., dating back as far as 80 years. Entrupy's algorithms analyse tiny, miniscule details of each product to determine its authenticity. The authentication process utilises a mobile app and specific user generated photos of the goods, which are run through Entrupy's AI algorithms to analyse the images to determine authenticity in real time.

Amazon is also effectively utilising AI and machine learning-based technology. Its zero-tolerance policy, Project Zero, combines industry insight with machine learning technology in a programme that allows brand owners to use self-service, automated tools to remove suspected counterfeits from product listings on Amazon's platforms. With Project Zero (which is still an invitation-only programme), companies provide Amazon with their logos, trademarks, and other information about their brands, which Amazon uses to scan its listings and remove fake products. The data provided by brand owners are also used to strengthen Amazon's automated protections to better catch potential counterfeit listings proactively in the future.

And there are others. Companies like DataWeave, a competitive-intelligence-as-a-service provider for retailers and consumer brands, is launching counterfeit detection solutions that enable consumer brands to identify and curb the presence of counterfeit products on ecommerce websites using AI-powered image and text analytics.

On the payment processor side, Paypal has created an AI algorithm that looks at both the IP and the geolocation of that IP, compares them to the user's account history to see if this matches up with previous actions, and compares it to other users to detect fraud. These are just a few examples of companies that are successfully incorporating machine learning and AI technology into their anti-counterfeiting programmes, and highlights the impact technological solutions may have



on brand owners in the future.

Although machine learning programmes require more input from the brand owners at the outset to define the scope of their rights and become more precise in drawing the line between genuine and fakes, the payoff can be great. For example, in addition to helping curtail the proliferation of counterfeits online, machine learning and AI-based technology to detect and fight online fakes will also help shift the burden away from brand owners being the first line of defense when it comes to monitoring for counterfeits. By shifting to an automated, technological processes for detecting and taking down listings for counterfeit goods, brand owners can utilise their resources more efficiently. Machine learning is an important countermeasure to online counterfeiting; however, it works best when combined with user education and technical countermeasures to combat the threats, all of which should be considered when developing effective online anti-counterfeiting programmes.

## Authors



Ian Block is a partner and litigator in the IP practice group at Neal Gerber & Eisenberg. He focuses his practice on all areas of trademark law and advises clients on building and protecting their brands.

Andrea Fuelleman is an attorney at the same firm. She focuses her practice on brand protection and IP enforcement and prosecution matters.