CHALLENGES IN THE CONSUMER SECTOR
TRANSFORMATIVE TECHNOLOGY

In the first of a three-part series, Susan Black, Joel Smith, Hayley Brady, Victoria Horsey and James Balfour of Herbert Smith Freehills LLP examine issues facing the consumer and retail sectors from new and disruptive technologies.

Businesses that provide goods or services to consumers are currently facing some of the toughest challenges to be experienced by any sector. Disruptive technology, as it is often termed, is changing the way that people shop and access consumer services, creating unfamiliar competition and forcing new business models onto what had become settled and historically successful businesses. This article, the first part of a three-part series on issues facing the consumer and retail sectors, explores some of complexities introduced by new technologies, including:

- Whether current laws relating to intellectual property (IP), privacy, data protection and tort are fit for purpose in the context of artificial intelligence (AI), virtual reality (VR) and augmented reality (AR).
- The legal considerations around data use and commercialisation, in particular, privacy and data protection issues.
- The legal issues in relation to contextual commerce and targeted advertising.

EMERGING TECHNOLOGIES

The retail scene is undergoing fundamental disruption and emerging technologies such as AI, AR and VR are taking centre stage in this process. Today's consumers have an overwhelmingly large range of products and services to choose from, and are inundated with a constant flow of advertisements wherever they go. A more personalised experience for their customers is currently something of a holy grail among retailers. Equally, with easy access to goods and services online, retailers and service providers need to ensure an attractive experience in their physical locations in order to encourage shoppers to visit and make additional purchases while in store.

Artificial intelligence

Any consumer that has recently bought something, either online or from a shop, will very likely have interacted with a form of AI or machine learning (*see box "What is artificial intelligence?"*). In the consumer sector, the challenging economic environment and increasing competition to retain customers have pushed retailers to innovate to enhance the customer experience and ultimately generate more sales. AI has the potential to help them to achieve this.

Retail benefits. One of the greatest benefits of using AI in retail is the enhanced customer experience that it can provide. For example,

in the home, AI-powered virtual assistants can use data gathered from their interaction with a consumer and other sources, such as consumer buying trends, to enable retailers to make more accurate product suggestions and even make recommendations based on a person's wardrobe and body shape. The use of chatbots; that is, messenger-based systems fuelled by AI, is also on the rise (*see below*).

AI is also allowing retailers to refine production selection based on customer responses to a series of questions. Cognitive computing platforms enable shoppers to have a more personalised shopping experience when visiting a website. Retailers can also benefit from the use of AI as an internal tool to better understand trends and forecast sales, thereby reducing wasted stock.

Chatbots. AI-powered natural language chatbots are also expected to be a vital enabler for online services and sales, by providing a virtual intermediary to facilitate not only the transaction but also pre-sales and after-sales customer care. Typically, chatbots answer questions from customers based on key words and can detect customer moods. In the retail sector, chatbots provide 24-hour access to customer services, personalising the customer experience and removing waiting times to speak to an adviser.

An early example of this type of functionality was launched in 2017 by Mastercard in the form of a chatbot providing secure checkout functionality through Facebook Messenger. The degree of sophistication of most existing chatbot solutions suggests that there is still some way to go before these technologies can deliver a fluent end-to-end shopping experience from product discovery right through to purchase and after-sales care.

IP issues. In common with other emerging technologies, AI will bring a number of challenges to the existing IP regime, which is struggling to keep up with the fast pace of innovation and will need to evolve and adapt to cover the resulting legal issues properly (*see feature article "Artificial intelligence: navigating the IP challenges", www.practicallaw.com/w-015-2044*).

For example, AI has the capability to generate content or data but it remains to be seen who will be considered the owner of the IP rights (IPR) that arise and who will be entitled to obtain licensing fees and enforce the IPR. This is especially the case given the potentially large number of parties that could be involved in the design, training and use of the AI system. As AI becomes increasingly autonomous, this raises the possibility that the AI software or technology might be the author, and arguably the owner, of any resulting IP. Until the law catches up with the technology, the solution might be to simply agree these issues in commercial agreements at the start of a project and provide for the position to be revised periodically as the project progresses.

Ownership of the IPR in the AI system is also likely to be controversial, particularly since the systems consist of automatically generated code resulting from the system's training. By comparison, currently, in a regular software development scenario, each line of code can be attributed to a human author. Therefore, this may also need to be addressed by way of contract from the start. The possibilities for mass commercialisation of AI systems and the opportunity to license-in or license-out AI technology means that any related agreements should make clear which party owns the background IPR and the resulting, foreground IPR, and any improvements or developments of that IPR.

Patents. The European Patent Office (EPO) issued guidance in 2018 on the patentability of inventions that incorporate an AI or machine-learning element (*www.epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_3_1.htm*). These will be patentable as long as the invention has a technical character. The AI or machine learning cannot be patented but needs to be integrated into a technical advance. In the same way as the computerisation of business processes, only those inventions that comprise a technical advance will be patentable; those which simply make a process more efficient will not be.

However, the EPO's guidance provides that, where a classification method serves a technical purpose, the steps taken to generate the training set and to train the classifier may also contribute to the technical character of the invention if they support achieving that technical purpose. This appears to be an encouraging sign in relation to the patentability of inventions that incorporate an AI or machine-learning element.

Copyright. In the UK, copyright in computer-generated works (that is, where no human author can be identified) is owned by the person making the arrangements necessary for the creation of the work (*section 9(3), Copyright, Designs and Patents Act 1988*). In *Nova Productions Ltd v Mazooma Games Ltd*, the Court of Appeal held that the person playing a computer game was

What is artificial intelligence?

Broadly speaking, artificial intelligence (AI) refers to the concept of machines being able to interact with the world around them by carrying out tasks and reacting like humans. AI is defined by Stanford University as "the science of getting computers to act without being explicitly programmed"; that is, it involves machines using complex algorithms to analyse a large volume of data, recognise patterns and make predictions without the need for someone to program instructions into the machine's software. The system is also able to learn from its mistakes and improve over time, just like a human.

True AI is where a machine can think like humans and create something without human interference. Many people regard intelligent personal assistants, such as Apple's Siri, as an example of AI but, in fact, this technology is best described as "machine learning", which is a subset of AI, although the two terms are often used interchangeably. One way to look at it is that machine learning is the enabling technology which is helping computers to learn about how humans think.

Another concept that is often confused with AI is deep learning, which is a subset of machine learning. This involves combining vast amounts of data and computing power to simulate the human brain, categorising data and finding patterns which it can then apply to other data sets. The differences between these three seemingly separate concepts are not clear cut and they are highly interlinked. For now, machine learning is the fastest growing component of AI but, before it can make real headway towards true AI, machine learning still requires significant improvement.

not the author of screenshots taken while playing the game and had not undertaken arrangements necessary for the creation of the images; it was the persons making the arrangements necessary for the creation of the screenshots (that is, the game's creators) who were the author (*[2007] EWCA Civ 219, www.practicallaw.com/7-314-1956*).

This principle could be applied to an AI or machine-learning situation in that, for machine learning to occur, the machine needs to be fed with information to train it. This process uses skill, labour and judgment, which is the test for establishing copyright under UK law, but *Nova* may need to be distinguished for this argument to succeed. Equally, reliance on skill, labour and judgment may be problematic where copyright is sought in a computer program as a literary work where the EU test under the Copyright Directive (*2001/29/EC*) (that is, whether the work is the author's own intellectual creation) applies. This may cause problems if systems are being trained but are creating a computer program in which the trainer has not had sufficient involvement.

Privacy and data protection. Unsurprisingly, given the extensive collection of data by AI systems from a variety of sources, along with the analytics applied, the use of AI also has privacy and data protection implications. For instance, some types of big data analytics used by AI systems, such as profiling, can have intrusive effects on individuals (*see feature article "Big data: protecting rights and extracting value", www.practicallaw.com/1-595-7246*). Organisations will also need to consider whether the use of personal data is within people's reasonable expectations.

In addition, the complexity of the methods of big data analysis, such as in the context of machine learning, can make it difficult for organisations to show that they are transparent about the processing of personal data. AI is likely to give rise to unique privacy questions and, again, it remains to be seen if the current framework is sufficient or whether regulators will need to fill any legislative gaps.

Liability in tort. It will be interesting to see what the legal implications will be under tort law with respect to the acts and omissions of AI systems. Several countries are seeking to produce legislation which can provide some guidance in this area. For instance, a report prepared in 2017 by Mady Delvaux, a member of the European Parliament, analyses whether robots should have legal rights as an "electronic person" and also whether a robot should be held liable for accidents (*www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html?redirect*).

Among other things, Ms Delvaux's report sets out certain proposed principles, including the fact that a robot must not injure a human being or, through inaction, allow a human being to come to harm. It further states that any future legislation should not restrict the type or the extent of the damages that may be recovered, or limit the forms of compensation that may be offered to the aggrieved party, solely because that damage is caused by a non-human agent. Clearly, this will be a controversial topic and one on which it is very difficult to legislate.

Virtual and augmented reality

The concept of VR and AR shopping experiences has existed for some time (*see box "Virtual and augmented reality explained"*). For example, many big retailers such as eBay and Ikea have already rolled out some form of AR or VR-assisted retail solution. However, most would agree that the full potential of AR and VR is yet to be realised and some exciting new developments in this area may be just around the corner.

Recent examples. In 2018, PayPal was granted a patent in respect of a new technology which would auto-suggest items to buy based on whatever the individual is looking at through a pair of AR-enabled glasses. This technology would, for example, allow consumers to buy items instantly as they browse through a shop, thereby avoiding the inconvenience of queuing at the till, or even as they see products advertised on a passing bus.

Walmart has also jumped on the VR bandwagon, buying VR startup Spatialand in February 2018. Spatialand, which develops VR software tools to transform existing content into immersive VR experiences, is expected to create new VR and AR applications for Walmart, both for online and physical retail. These kinds of collaborations may, in the future, lead to entirely VR-based shopping "outlets" which not only improve the retail experience for consumers but solve a whole host of real-world barriers to retailers, such as the cost and physical capacity of real estate.

IP issues. The current array of traditional IPR that are devised to deal with real-world circumstances are often ill-equipped to deal with virtual property. For example, a fashion retailer may upload virtual product equivalents onto its app platform and will want to assert the usual IPR over these virtual products, as it does over its real-world products. However, it is often unclear or untested how IPR are to be applied to virtual products. In some cases, the IP law treatment of the meta-characteristics of these virtual products also remains to be determined.

For example, a virtual product may be linked to, or contain, various hashtags, geotags and other virtual characteristics. Although there have been cases involving the use of metatags, the European Court of Justice (ECJ) has held that the purchase by a competitor of a registered trade mark as a metatag was not infringing unless the customer searching was confused by the advertisement for the competing business which came up along

Virtual and augmented reality explained

There are several key differences between virtual reality (VR) and augmented reality (AR). VR is a computer-generated, software-driven representation of real life which is presented to the user. This is achieved by stimulating of the user's senses such as sight and hearing. The aim of VR is to replace completely the real-life experience of a user with an artificial version of that real-life experience, for example, recreating the shopping experience through a headset.

AR is also computer-generated and software-driven but does not seek to replace completely the real-life experience of the end user; instead it aims to overlay the real-life experience of a user with additional information, for example, on a shop floor. The general industry consensus currently is that both technologies have overcome inflated expectations and are ready to develop into more fully formed technologies in the next few years, with VR technology currently more progressed than AR.

with genuine search results (*Interflora Inc and another v Marks & Spencer plc and another, C-323/09, www.practicallaw.com/5-509-5156*).

However, it is uncertain how trade mark or other IP law might be applied to hashtags, geotags and other virtual characteristics. It is possible that the IP law treatment of virtual products and real-world products could be different, and therefore IPR in virtual products may need to be considered separately to their real-world equivalents.

An additional practical problem is that AR and VR users access these systems from all over the world. As a result, the individuals using them can often be difficult to identify and pursue, and it may not always be clear which jurisdiction's IP laws should apply.

Disputes. So far, the AR and VR community has tended to rely on forms of self-governance and internal dispute resolution in order to address any issues or disagreements arising from the conduct taking place when using AR and VR, but it is unlikely that this conduct can escape the restrictions of any applicable laws and regulations. These technologies will therefore also test the understanding of where acts of infringement take place according to existing notions of jurisdiction.

In the context of AR, in particular, various consents may be required in relation to the real-world features which are the background to the AR experience. For example, if a company creates an AR app which overlays onto real-world buildings or features, various licences and consents may be required to use these buildings or features. The company will need to consider the risk of attracting tortious claims such as nuisance and negligence from the owners and occupiers of these buildings, as well as the health and safety implications of potentially encouraging users to enter a hazardous area.

DATA COMMERCIALISATION

The consumer sector is enabling retailers to collect a large volume of data and gain a deep understanding of customer behaviours and preferences, which can translate into long-term benefits for the consumer of the future as well as the businesses serving them (*see feature article "Data assets: protecting and driving value in a digital age", www.practicallaw.com/w-019-8276*).

Shoppable content

Shoppable content is perhaps one of the more tangible applications of contextual commerce. On one level, this concept is not new as shopping channels have been running successfully since the 1980s. However, the revolutionary aspect lies in the possibility of a consumer watching their favourite TV show and being able to buy their favourite character's outfit or the lamp in the corner of the soap opera set by a couple of clicks on their remote-control device or, more likely, by a voice-activated command to their virtual assistant such as Siri, Alexa or Google Assistant.

This next-level product placement technology is already being trialled by a number of players in the content and e-commerce sectors. Fox recently launched shoppable content functionality on its "Fox Now" app to enable users to buy items featured in the hit TV series "New Girl". Similarly, Google has recently released a new feature enabling the integration of shoppable content into YouTube videos and advertisements.

However, consideration must be given to legal issues, including:

- The ownership of data.
- Restrictions on the use and exploitation of data.
- The use of IPR and contractual rights to maximise the use or exploitation of data.
- Ensuring that the use or exploitation of data does not cause further issues for the business, including by good information governance.
- Competition law (*see feature article "Data use: protecting a critical resource", www.practicallaw.com/w-012-5424*).

The restrictions applied by the General Data Protection Regulation (*679/2016/EU*) (GDPR) are, of course, also paramount (*see News brief "EU General Data Protection Regulation: on your marks, get set, go!", www.practicallaw.com/w-014-9290 and feature article "GDPR one year on: taking stock", www.practicallaw.com/w-020-0982*).

The internet of things

A plethora of emerging internet of things (IoT) technologies and connected devices is increasingly generating a data goldmine. Examples of IoT technologies include: fridges that automatically order a consumer's favourite food and drinks when stocks are running low; connected vehicles that notify the driver of relevant loyalty-based discounts as they drive past a gas station; and smart advertising panels which not only tailor advertisements on an individual basis but can instruct a passer-by's smartphone to flash up a "click-to-buy" button as they walk past.

Contextual commerce

There is particular scope for the sophisticated exploitation of contextual commerce opportunities from IoT applications that can identify or track individuals, or both, as they move around their environment, whether that is at home, in the car or walking along a street.

E-commerce has revolutionised the retail experience by enabling individuals to buy goods and services from the comfort of their homes with a simple click. Contextual commerce, the next frontier for retail experience enhancement, takes the convenience and spontaneity of one-click purchasing even further by providing a platform through which consumers can make those purchases the instant they see something they want to buy. For example, this could be a product appearing on their favourite TV show or advertised on a billboard as they are walking around town, or perhaps even a piece of clothing being worn by someone they pass on the street.

Whereas e-commerce requires an individual to visit the website or web application of a retailer in order to make a purchase, contextual commerce seeks to capitalise on the purchasing pull of the moment, when a consumer sees something and wants it immediately, by using technology to integrate purchasing opportunities seamlessly into the consumer's everyday activities and surroundings.

Contextual commerce, as a fully-fledged scalable retail channel, is still in its infancy.

However, there are a variety of technologies at various stages of development that may enable contextual commerce to become the dominant platform for retail in the near future. These technologies take a variety of different forms and include:

- The combination of sophisticated and well-organised consumer databases with AI systems which allow for highly personalised real-time consumer targeting.
- Hardware and software that embed retail interfaces into the natural environment of the consumer; for example, shoppable content and mobile device-based retail interfaces powered by augmented reality software (*see boxes "Shoppable content" and "Social media integration"*).
- Technologies that can transform single-use applications into multiple-use e-commerce platforms.

Data privacy and protection

As is always the case with any data-driven technology, data privacy and protection should be on the top of the list of issues to be addressed (*see feature article "Data protection: privacy by (re)design", www.practicallaw.com/w-018-6087*). Many of the technologies discussed in this article, particularly identification and tracking technologies, rely on a degree of personal data collection, processing and sharing that many consumers would regard as intrusive. Consumer consent, combined with clear notices and policies explaining how consumer data will be used, will therefore likely become a cornerstone of contextual commerce (*see News brief "Internet of things: consultation on security of devices", this issue*).

In addition, given the reliance of targeted advertising and contextual commerce on the sharing of personal data between a number of different entities in the retail value chain, including retailers, advertisers and payment services providers, data controllers will need to ensure the adequacy of not only their own data protection compliance but also that of any third-party data processing partners or joint data controllers (*see "Targeted advertising" below*).

Cyber security

Robust technical and organisational measures to mitigate any cyber security vulnerabilities will be of utmost importance, taking into account the sensitivity of some categories of data, for example, biometric data and payment data, which will likely need to be collected and stored to facilitate contextual commerce applications (*see feature article "Cyber security: top ten tips for businesses", www.practicallaw.com/3-621-9152*).

Deriving value

Once data protection and cyber security issues have been addressed, it is worth considering the opportunities arising from the quantity and quality of data that online sales and, in particular, contextual commerce applications are likely to generate. These data sets will be of value to the retailers collecting and processing them, as well as to third parties. Retailers that have invested time and effort acquiring and exploiting data for their own contextual commerce-related purposes may therefore be able to extract incremental value from these data by licensing them out to third parties for other unrelated purposes.

If done properly, this kind of data commercialisation can represent a significant source of ancillary revenue. However, given the lack of any concrete legal right in data per se, and the difficulty of asserting copyright, database rights or other ancillary IPR in data, successful data commercialisation will likely depend on carefully drafted contractual protections and restrictions relating to third-party use of data.

Social media integration

Facebook's Messenger app provides several in-app features that allow users to transfer money to other users, interact and receive updates from retailers on the platform, and place orders for certain products and services. Given the large number of users and the significant amount of time spent by users on the Messenger platform, these in-app purchasing features make for a convenient contextual commerce experience. While the adoption of these features, both by retailers and consumers, has perhaps not been as rapid or widespread as some might have expected, the development of this technology, through an already popular platform, presents a variety of expansion opportunities.

Perhaps a more obvious route to market for this kind of technology, and one that Facebook has already started to roll out in the US, is the integration of in-app purchasing into Instagram, which is an offering likely to have strong appeal for the millennial audience. Instagram presents a clear opportunity for the integration of contextual commerce as it is the playground of influencers and a platform already used by millions to follow the latest trends in, among other things, fashion, homewares, travel and fitness. Current examples of contextual commerce on Instagram include the integration of a "swipe up to buy" option in Instagram stories and embedded links to items that appear in posts.

WeChat, the Chinese social media application, also provides a number of in-app commerce functionalities that range from making travel arrangements and ordering food, to direct business-to-consumer interaction through micro-stores set up by retailers within the app. These features allow users to make a variety of on-the-go purchases.

TARGETED ADVERTISING

It is estimated that the average consumer is exposed to up to 10,000 advertisements in a single day. Advertising is a big part of the consumer experience and, as technology increasingly plays a protagonist role in daily life, it is no news that online advertisements are steadily replacing the more traditional forms of publicity. Over 40% of the world's population now has access to the internet and users are constantly leaving digital footprints across a range of online channels by willingly sharing large volumes of useful data. This creates a huge market for advertisers, as well as a vast pool of insightful information about consumer behaviours and preferences. Technology giants such as Google and Facebook are also making an impact by creating platforms that enable data not only to be collected more easily but also to be analysed and extracted.

These combined developments have kick-started the reshaping of the advertising industry, particularly in terms of enabling organisations to target advertising at their most receptive audiences. The forms of targeted advertising continuously evolve; they

can be based on a wide range of information, including browsing history, buying habits, sociodemographic traits such as consumers' age, gender, race and economic status, psychographic characteristics, including a consumer's lifestyle, opinions and values, or geographic location, to name a few. Add to the mix the increasingly sophisticated technologies that companies are developing and applying to deepen their understanding of consumer reactions and accurately predict behaviours, and advertising becomes incredibly personalised.

Online behavioural advertising

The most significant type of targeted advertising is known as online behavioural advertising (OBA), which involves the use by companies of information about an individual's online browsing habits to produce advertising that is personalised to that individual's preferences and interests. This can be either site based or network based. The majority of OBA is site based and works through cookie files that are placed on consumers' computers to track the pages that the user visits, either on the tracking organisation's own website only (first-party OBA), or also on third-party partner websites that are members of the same advertising network (third-party OBA). Advertisers that use first-party OBA include, for example, news websites or online retailers such as eBay and Amazon. OBA can also be undertaken at a network level by making use of "deep packet inspection" (DPI) techniques which examine all traffic on a user's computer. This has been trialled in the UK, but is not currently in use.

Social media advertising

Similarly, social media advertising also makes use of its users' browsing activities, for example, by targeting advertisements based on Facebook pages that someone has "liked". Due to the large amount of information that social networks gather, in addition to reactively targeting users based on their behaviour, advertisers on social media can also create profiles and target the consumers before they even undertake any activities online.

For example, Facebook allows advertisers to target an audience in three ways:

- Through precise interests, which enables advertisers to group users according to specific words shared on their timelines, for example, relating specifically to the English cricket team.
- By Facebook categories, which is aimed at those who have shared terms on their timeline that relate to a broader topic or interest, for example, relating to cricket more broadly.
- Partner categories, which are groups created by third-party data providers and are based on the users' browsing activities outside of Facebook.

Location-based advertising

Advertisers can undertake location-based advertising by making use of the location data collected by mobile devices to personalise their messages to consumers based on their current location. Since the data are given in real time, the advertisements are very timely, which is one of the key strengths of this type of targeted advertising.

For example, in 2014, Starbucks tracked users' device identification and location, and provided advertisements based on that information. The metric for assessing success was the number of people that walked into a branch of Starbucks as a result of the advertisement. The conclusion was that the likelihood of a person entering a branch increased by 100% after seeing the location-based advertisement.

Future developments

In order to maximise the efficiency of targeted advertising, companies are already taking it to the next level by using technology to identify consumer reactions to advertisements. By linking different forms of targeted advertising with emerging technologies, companies can obtain a deeper understanding of the way in which a target audience reacts to and interprets the advertisements that they are exposed to online.

For example, Canon Europe has been working with Clicktale, a digital customer experience company, and using behavioural economics technology to interpret a person's digital body language by analysing user behaviour on the website and classifying them into categories such as "focused" or "disoriented". The technology tracks online behavioural patterns based on millisecond-level actions, including hovers and scrolls. It uses cognitive computing, machine learning and psychological research to enable Canon to enhance the consumer experience and its website design.

The use of sensory research technology can also add real value to brands in the context of targeted advertising. According to Shutterstock, the picture library brand, the choice of images for online advertisements can be a highly influencing factor in catching the attention of consumers. Consequently, the company undertook eye-tracking research which revealed that the images are most effective where they reflect the demographic profile of the target customers. For instance, advertisements that include pictures of children are likely to be viewed longer by parents.

Legal concerns

All forms of targeted advertising can bring huge benefits to the organisations that make use of them, and this is even more the case where companies invest in new technologies that can help them go the extra mile in terms of research and insight.

Targeted advertising can also be advantageous to consumers, who can gain free access to content and no longer have to be exposed to irrelevant advertising. Nonetheless, targeted advertising, and OBA in particular, also gives rise to a variety of concerns and associated legal issues.

Privacy. Privacy is the key concern and consumers have repeatedly expressed worries about the potential misuse of the data collected. Therefore, the issue of obtaining consent from consumers is crucial. In the UK, the processing of personal data as part of OBA must be performed in compliance with the GDPR, which requires that individuals' personal data be processed fairly and lawfully. This means that users must be given notice about the use of their personal data and there must be a legal basis for processing, which is often consent.

However, it remains to be seen exactly how this must apply in practice, depending on the type of OBA that is being used. For example, while it may be sufficient simply to provide the information in a website privacy policy when undertaking first-party OBA, the standard of notice for third-party OBA and when using DPI techniques may have to be higher to satisfy the fairness requirement, given the greater intrusion.

Another related question that has caused a lot of debate is whether OBA must be conducted on the basis of a user's explicit opt-in consent, or whether it is enough for the user to opt out. Best practice would be to obtain opt-in consents but the approach of the advertising

industry is to rely on opt-outs. This is reflected in the UK Committee of Advertising Practice Code and the Internet Advertising Bureau's good practice principles for OBA (*www.asa.org.uk/uploads/assets/uploaded/bd9575a1-cd07-48e7-979b4cbec70dd31f.pdf*; *www.youronlinechoices.com/wp-content/uploads/2010/11/IAB-UK-Good-Practice-Principles-for-Online-Behavioural-Advertising.pdf*). On the other hand, this is further complicated by the fact that the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*) require that prior consent (that is, opt-in consent) be obtained before processing traffic data for the purpose of providing value-added services.

The Information Commissioner's Office considers OBA to fall under this category of services and therefore requires opt-in consent. However, again, it is unclear if this applies to all types of OBA or just where it uses DPI techniques.

Other legal issues. More generally, OBA also has the potential to amount to a criminal offence under the Regulatory Investigatory Powers Act 2000, which prohibits the intentional interception of communications and making the contents available to another person, except in certain circumstances. However, it is unclear if OBA will amount to an interception in all circumstances and it is likely that this will depend on how the technology works, as well as the circumstances of each case.

In addition, the Consumer Protection from Unfair Trading Regulations 2008 (*SI 2008/1277*) (CPRs) prohibit unfair commercial practices that distort consumers' transactional decisions. In the context of OBA, it remains to be seen how successfully it can be argued that a breach of the CPRs arises if consumers take a different transactional decision, for example, by choosing not to view a website, because they were given false or deceptive information about how OBA works.

ONLINE INFRINGEMENT

The rise of online infringement is linked to the ease with which anyone can register a domain name and set up a website, and the popularity of social media and other e-commerce platforms; these have enabled counterfeiters to access cheap routes to market and vastly expand their operations. Counterfeiters can easily raise the profile of replicas by using paid searches on Google or popular hashtags on Instagram. Online piracy is rampant and a significant element of these online threats now comes from accessing unlawfully streamed content, whether music, film or sports coverage.

Injunctions

Given the huge volume of online infringement, IP owners are increasingly targeting intermediaries, such as internet service providers (ISPs), hosting providers and third-party marketplaces as a means of combatting these infringements. The most powerful and effective weapon available to copyright and trade mark owners is a blocking injunction. Counterfeiters rely on intermediaries to provide services and their market access is impeded if these services are blocked.

However, intermediaries can seek to rely on the hosting defence provided by Article 14 of the E-commerce Directive (*2000/31/EC*). The law on this area has been developing since the ECJ's seminal decision in *L'Oréal v eBay* in 2011 (*C-324/09; see News brief "L'Oréal v eBay: good news for brand owners", www.practicallaw.com/9-507-0026*). This decision affirmed that, under EU law, the defence applies to hosting providers only if they do not play an active role that would allow them to have knowledge of, or control over, the stored data. If the provider is actively involved in the sale of the goods, or on notice and does not act with sufficient speed in applying a take-down procedure, the defence will not apply and the IP owner may have a cause of action against the intermediary.

The UK courts' blocking orders have become more sophisticated, moving away from injunctions directed at the operator of the website or those behind it, to targeting the ISPs hosting the target sites, even though the ISPs are not themselves infringing. The blueprint blocking order was obtained in *Cartier International AG and others v British Sky Broadcasting Limited and others*, where the Court of Appeal granted an order to block access to six websites offering counterfeit versions of the claimants' luxury goods, on the basis of the claimants' trade mark rights (*[2016] EWCA Civ 658; see News brief "Counterfeit websites: ISPs can be forced to block access", www.practicallaw.com/1-631-2486*). The court confirmed that section 37(1) of the Senior Courts Act 1981 and Article 11 of the IPR Enforcement Directive (*2004/48/EC*) can be relied on to grant blocking injunctions against ISPs requiring them to prevent access to the offending websites that were supplying counterfeit goods online.

Cartier has since been relied on by the sports industry, in particular, the Football Association Premier League and the Union of European Football Associations (UEFA), in obtaining live blocking orders to prevent access to certain sites only during live broadcasts of match fixtures (*Football Association Premier League Ltd v British*

The Counterfeit and Piracy Watch List

The European Commission (the Commission) in its paper on the Counterfeit and Piracy Watch List (the watch list) states that the watch list presents examples of reported marketplaces or service providers whose operators or owners are allegedly resident outside the EU and which reportedly engage in, facilitate or benefit from counterfeiting and piracy (*http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf*).

The Commission's stated aim is to encourage the operators and owners, as well as the responsible local enforcement authorities and governments, to take the necessary actions and measures to reduce the availability of goods or services that infringe intellectual property rights (IPR) on these markets. The watch list also intends to raise consumer awareness concerning the environmental, product safety and other risks of buying from potentially problematic marketplaces. The watch list focuses on online marketplaces as piracy and the distribution of counterfeits increasingly take place through the internet.

The Commission states that the watch list is not an exhaustive list of the reported marketplaces and service providers, does not purport to make findings of legal violations, or provide the Commission services' analysis of the state of protection and enforcement of IPR in the countries connected with the listed marketplaces and service providers.

Telecommunications Plc and others [2017] EWHC 480 (Ch), www.practicallaw.com/7-641-0021).

While the first step in tackling online infringement is usually to seek the takedown of websites or infringing content, finding a way through to the root cause or source of the problem is increasingly difficult as sophisticated counterfeiters take measures to conceal their true identities. Locating the actual infringer or operator of a website can be next to impossible, so sending a cease and desist letter can be ineffective. Nevertheless, although the actual infringers are not directly targeted by blocking orders, the orders can be very effective even if they do not offer a complete solution to the problem.

The issue of who pays the costs of implementing these blocking orders can act as a disincentive for IPR owners. In *Cartier International AG and others v British Telecommunications Plc and another* the Supreme Court held that it should be the IPR owners that should pay the costs of implementing these blocking orders (*[2018] UKSC 28; see News brief "Supreme Court judgment in Cartier: costs for website-blocking orders", www.practicallaw.com/w-015-3949*). If the Supreme Court had settled this burden on ISPs, it is likely that a flood of these orders would be sought to prevent not only the streaming of unlawful music, television, film or gaming content, but also the sale of counterfeit and infringing products through online marketplaces.

Other enforcement tools

A practical approach to tackling online infringements is essential. It is important for a business to build up a portfolio of IPR in the territories where it operates. It is a lot easier for a business to use takedown procedures with ISPs and e-commerce platforms successfully if it can point to a registered trade mark or copyright since, in most cases, this allows it to populate a form on the relevant site.

It is worthwhile deploying arguments on copyright for takedowns. By way of example, Twitter shows much higher rates for takedowns based on copyright material: 67% success rate for takedowns following copyright complaints compared to 7% for trade mark complaints. Business owners should scrutinise their terms and conditions on websites and make sure that they adequately protect IPR.

Given the development of EU case law on this topic, the use of a paywall is a strong indication that a business has not authorised the copying or reproduction of materials from its website. It is important to include express terms on what form of reproduction of materials, if any, is permitted and to consider including a statement on hyperlinking and restrictions on content aggregation or commercial reuse of content or data (*GS Media BV v Sanoma Media Netherlands BV C-160/15; see News brief "Hyperlinking to unauthorised content:*

Related information

This article is at practicallaw.com/w-020-3706

Other links from uk.practicallaw.com/

Topics

Advertising and marketing	topic/0-103-1114
Compliance: data protection	topic/1-616-6178
Consumer	topic/0-103-2038
Copyright	topic/0-103-1270
Data protection: general	topic/1-616-6550
E-commerce	topic/2-103-1274
GDPR and data protection reform	topic/7-616-6199
Information technology	topic/5-103-2074
General IP	topic/0-103-2076
Internet	topic/8-383-8686
Patents	topic/2-103-1306
Social media	topic/0-525-4280
Telecoms	topic/7-205-8953
Technology: data protection	topic/8-616-6207

Practice notes

Consumer law toolkit	7-525-0330
Demystifying artificial intelligence (AI)	w-008-5369
Demystifying IT for lawyers	4-619-6070
Direct marketing: advertising, consumer protection and e-commerce rules	w-011-4000
Legal aspects of managing big data	1-581-1225
Managing cybersecurity risk and compliance	6-615-8326
Overview of copyright	9-107-3741
Overview of cybersecurity	9-617-7682
Overview of GDPR: UK perspective	w-013-3757
Overview of patents	1-107-3660
Protecting brands by enforcement against intermediaries	w-006-8793

Previous articles

Data assets: protecting and driving value in a digital age (2019)	w-019-8276
Data protection: privacy by (re)design (2019)	w-018-6087
GDPR one year on: taking stock (2019)	w-020-0982
Algorithms, apps and AI: the next frontier in discrimination law (2018)	w-013-8054
Artificial intelligence: navigating the IP challenges (2018)	w-015-2044
Data use: protecting a critical resource (2018)	w-012-5424
Blockchain and IP: crystal ball-gazing or real opportunity? (2017)	w-010-1622
Cyber security: top ten tips for businesses (2016)	3-621-9152
General Data Protection Regulation: a game-changer (2016)	2-632-5285
M&A in the consumer sector: key issues on value and structure (2016)	4-633-6315
Big data: protecting rights and extracting value (2015)	1-595-7246

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

ECJ imposes conditions" www.practicallaw.com/2-633-7919). The prominence of terms should be considered and whether there is a click-to-accept function before proceeding to use the website.

Business owners should consider investing in technology or developing apps in-house. Tiffany has developed a mobile app for employees, called FakR, that allows them to report replicas by posting photographs of street sellers hawking fakes or by sending links to questionable online auction listings. Internal reports have surged 60% since it was launched in 2018 and close to 75% of reports are actionable.

Businesses can also use image recognition software to assist in tracking down counterfeits online. There has also been a rise in authentication technologies with many brands developing online authentication platforms or mobile apps, together with a drive to get consumers to register branded goods, as this can help identify counterfeiting hotspots.

There are also a number of third-party websites and resources that may be helpful in tackling online infringement. The EU Enforcement Database is a particularly useful tool to assist in dealing with counterfeit goods which is accessible through the European Union Intellectual Property Office (EUIPO) website (*https://euipo.europa.eu/ohimportal/en/web/observatory/enforcement-database*). IPR holders can upload photographs or other details which may assist enforcement authorities in separating genuine from fake goods. Many customs and police units have added it as a tool into internal secure networks so it is accessible across the EU and endorsed by Europol. It is free and the only requirement for registering an account is having a registered trade mark or design within the EU.

The European Commission (the Commission) has established a counterfeit and piracy watch list (*see box "The Counterfeit and Piracy Watch List"*). This identifies online and physical markets outside the EU that engage in or facilitate substantial IPR infringements, in particular piracy and counterfeiting, in relation to EU consumers. The Commission will monitor the measures and actions taken by the local authorities in relation to the listed markets, as well as those taken by the operators and market owners to curb IPR infringements.

Susan Black is a partner and co-head of Consumer Sector, Joel Smith is a partner and head of IP, UK, Hayley Brady is head of UK Media and Digital, Victoria Horsey is a senior associate and James Balfour is an associate, at Herbert Smith Freehills LLP. *The authors would like to thank Sarah Burke, senior associate, and Rachel Montagnon, Consumer Sector and IP professional support consultant, for their contributions to this article.*
