



myerson

Tech Lite

In this issue:

The IP Of The Tiger

Facebook Data Breaches

IP: Protection and Exploitation

Censoring unwelcome contributors

The Healthcare Sector meets the Tech Sector

www.myerson.co.uk

0161 941 4000

Welcome to Myerson Tech Lite...

At Myerson Solicitors we have the experience and expertise to provide advice to those working within the IT, IP and Data Protection industries and in this issue our experts look at:

The IP Of The Tiger - September's High Court ruling that saw the granting of an injunction prevent servers streaming boxing matches.	03
--	----

Facebook Data Breaches - Explore how Facebook has become the subject of yet more controversy over its poor handling of personal data.	04
---	----

Intellectual Property exploitation and protection	05
---	----

Website Content and how to censor unwelcome content	07
---	----

The new Health Sector Code of Conduct	09
---------------------------------------	----



The IP Of The Tiger.

Intellectual Property Rights In Boxing - Injunction Granted after a large amount of illegal streams took place during September's World Heavyweight Title bout between Anthony Joshua and Alexander Povetkin at Wembley.

On 20 September 2018, the High Court gave a judgement and granted an injunction to block servers that were being used to stream broadcasts of boxing matches, in infringement of copyright.

The Claimant, Matchroom Boxing Limited and others, applied to the High Court for injunctive relief to prevent live streams of its professional boxing matches.

One of the most recent examples of streaming, which Matchroom presented in evidence, were the large number of infringing streams that took place on Anthony Joshua's most recent fight this year. Matchroom and Sky had exclusive licences to broadcast this footage but were deprived of substantial revenue due to the streaming.

During the judgement, Mr Justice Arnold referred to other injunctions he had previously granted on other sporting events, including Football Association Premier League Ltd v British Telecommunications plc [2017].

While the circumstances in the cases referred to were very similar to Matchroom's case, Arnold J said that the order sought by Matchroom differed in the following 2 ways:

The screened events were irregular in their timing, so that it was not possible for the relevant servers to be identified in the same way. Although the criteria set out in the order were

very similar, they would be applied by a particular form of monitoring conducted in the seven days leading up to each event. Although this could in theory lead to over-blocking, the claimant's evidence was that in practice there should be no real difference in effect.

It was not possible to list all the events in a particular season, as there was no boxing season as such, and events were not fixed far enough in advance. The order therefore provided for the defendants to be given at least four weeks' notice of each event.

Regardless of these differences, Arnold J granted the order as it was deemed proportionate in all the circumstances, as it did not impair the rights of the defendants ISPs to carry on business. As the legitimate aim was to prevent the infringement of Matchroom and Sky's rights on a large scale, it was deemed proportionate to limit the extent that internet users can impart and receive information.

If you would like to speak to a member of our IP team, within Dispute Resolution, please call 0161 941 4000.

**For more information
visit: www.myerson.co.uk
call: 0161 941 4000**

Facebook Data Breaches.

What lessons can tech companies learn?

Facebook has recently been the subject of yet more controversy over its handling of personal data following widespread news reports of a serious data breach, which has resulted in 50 million user accounts being compromised. This will be distressing news to shareholders in Facebook whose shareholdings took a hit and were only just recovering from the Cambridge Analytica scandal which plagued the company earlier this year.

Back in July, we reported that the Information Commissioner's Office (ICO) had indicated its intention to impose a fine on Facebook of £500,000, (the maximum fine allowed under the old data protection regime) in respect of the Cambridge Analytica scandal.

The suggestion of a £500,000 fine appeared to be a trivial sum for Facebook, a global company which generates a similar amount of revenue roughly every 7 minutes. The real damage was, of course, to Facebook's reputation and the changing perception of the social media giant in the eyes of its users.

Had the Cambridge Analytica events taken place after 25 May 2018 (the implementation date for the GDPR), then Facebook could have faced a far greater fine of up to 4% of its turnover – in real terms, this means a fine of up to £1.6bn.

It therefore remains to be seen whether the ICO will take more serious action in relation to the latest data breach and use this as an opportunity to flex its muscles with its new powers to impose more substantial fines.

Recent polls carried out by the Open Data Institute demonstrate how people are becoming increasingly mindful about sharing their personal data. Trust is a key issue and, where a company cannot demonstrate that it is trustworthy,

this can have devastating effects on its perception and success.

The conduct of Facebook can teach tech companies some very valuable lessons about their own data processing activities:

- **Due diligence:** It is essential to carry out due diligence on suppliers, contractors and collaborators, particularly where those parties will have access to personal data which you hold.
- **Contractual protections.** Where there is a data processing relationship, the GDPR requires that specific terms are used in the contract to cover the permitted scope of the processing and to allow the data controller to have a right to enforce where the data may be misused.
- **Data security:** With the ever increasing cyber security threats, it is essential that tech businesses have state of the art security measures in place. It is also important to adopt policies and procedures to ensure that your business is able to respond quickly and take appropriate action in the event of a security breach.
- **Compliance:** Whilst there is a perception that the initial hysteria around the implementation of the GDPR has passed, it is still crucial to ensure that your business has the relevant policies and notices in place to demonstrate compliance with the GDPR. Effective compliance will help to mitigate any risks of action from the ICO, and will also re-assure customers that they can trust your business with their personal data.

If you wish to discuss any GDPR or data protection related issues, please contact our specialist GDPR team.

Intellectual Property: Protection and Exploitation.

With the speed at which technologies are advancing, the need for technology companies to innovate and drive competitive advantage is greater than ever. It is vital that tech businesses constantly innovate to drive investment, but also dedicate the time and resource to prevent its ideas from being copied by competitors

Protecting Your Business's IP

Intellectual Property (IP) rights broadly fall within two categories: registered and unregistered rights. Examples of well-known rights include:

Patents: a patent is a registered right granted by the Intellectual Property Office (IPO) and gives the owner a monopoly right to use and exploit an invention. Patents are not easy to obtain and the application process can be expensive and time-consuming, however, if successful, patent protection is an extremely valuable asset to a business.

Trade Marks: trademarks are symbols which may appear or be attached to a business' products or services and represent the goodwill of such products or services. Trade marks may be unregistered and established simply by "use" or registered with the IPO if a UK trade mark.

Copyright: copyright aims to prevent one person copying or using another person's original work without permission. Copyright is unregistered and arises automatically provided certain conditions are satisfied. It protects the first owner i.e. the author or creator. However, there are certain exceptions to this; for example, typically, an employer will normally own the rights to IP developed by an employee at work.

IP rights are important in showing investors that a business has IP capital which it can draw on, and investors are more likely to want to invest in a company that can show it can protect its revenue streams through IP enforcement.

Exploiting Your Business's IP

Once a business has taken steps to protect its IP, there are various ways in which a business can exploit it, whether through direct use, merchandising, or perhaps the most common, selling, licensing and franchising.

Selling: a business can sell its IP by way of an assignment. This simply means that a business transfers its rights in the IP to someone else. A business will most likely be able to negotiate a sum of money for the assignment however, all future earning potential will transfer to the buyer.

Licensing: licences are very flexible and can be a profitable way for businesses to exploit their IP. A business can set out the scope of the licensee's rights, the territory, duration and any restrictions on use. Licensing may allow a business brand to reach markets it may not otherwise have reached, and there may be lucrative on-going fees payable.

Franchising: franchising is a model through which the owner of a business can grow the business by granting others the right to set up a franchise, usually limited to a certain territory, with the benefit of the business brand and experience. This can be a lucrative way to geographically expand a business without capital cost, however the franchise agreement will need to include certain protections and restrictions to protect the business and brand.

Remember, the fastest way to lose a competitive advantage is by allowing others to capitalise on your ideas. Take the time to develop an IP strategy to protect and exploit your IP to ensure you are not wasting crucial resources and getting the most out of your IP.

Impact of Brexit

Brexit is likely to have an impact on IP, particularly those elements of IP that come from EU law (such as European Union trademarks and Community registered and unregistered design rights). The effect of Brexit on IP will depend primarily on whether or not a deal is agreed in relation to the UK's exit from the EU.

Deal Brexit: if there is a deal then it is likely that a transitional period will apply and existing rights will continue to have effect on much the same basis following Brexit as they currently do. The transitional agreement which will put this into effect has mostly been agreed but there are significant areas of disagreement meaning that it may not be entered into, which would mean that there would be a "no-deal Brexit".

No-deal Brexit: according to the Government's technical notices that it has published to detail the likely impact of a no-deal Brexit, copyright (which is a national right) and patents (both UK and through the European Patent Office, which is independent of the EU) are, in the main, unlikely to be greatly affected by a no-deal Brexit. The Government has stated that rights in existing registered EU trade marks and Community designs will continue to be protected and enforceable in the UK by providing an equivalent UK right. The Government has also stated that all unregistered Community designs in existence at the point of leaving the EU will continue to be protected and enforceable in the UK for the remaining period of the protection of the right.

In a no-deal Brexit, businesses that act as distributors exporting goods bearing third-party trademarks to the EU will need to be careful and may need to seek consent from

the trademark owner. When goods are placed on the market in the EU the trademark owner's rights are "exhausted" and the trademark owner can no longer restrict their onward sale. However, post-Brexit the UK will not form part of the EU, so if goods are purchased in the UK then EU trademark rights will not be exhausted and EU rights could be infringed if the goods are subsequently imported into the EU.

The Government has been preparing for Brexit by introducing draft regulations into Parliament to ensure that the legislative position does not materially change on Brexit occurring. The most recent of these in relation to intellectual property was the Intellectual Property (Copyright and Related Rights) (Amendment) (EU Exit) Regulations 2018, which are designed to remove or correct references to the EU, EEA, or member states in UK copyright legislation to preserve the effect of UK law where possible.

If you would like any assistance in understanding the potential impact that Brexit will have on Intellectual Property, please do not hesitate to contact our expert team on 0161 941 4000 or by email lawyers@myerson.co.uk.

For more information
visit: www.myerson.co.uk
call: 0161 941 4000



“Get off my website!” - censoring unwelcome contributors

The incendiary views of Alex Jones, the “alt-right” voice of InfoWars, were finally banned from Facebook, Apple, YouTube and Spotify earlier this year. This came after a prolonged campaign accusing him of glorifying violence and promoting hate. However, Twitter, the self-proclaimed “free speech wing of the free speech party”, has so far refused to bow to the same pressure and has declined to ban him from the site. While there may be ideological or political reasons behind the differing approaches, this poses the question: when and why should website owners remove content or ban users? Alex Jones is certainly not the only internet contributor to have made inappropriate postings and so in this article we look at the legal reasons for website owners to regulate content published on their website.

Website owners could be forgiven for thinking that these are problems that only apply to tech-giants and social media platforms. However, any owner of a website that allows users to upload content should be aware of the risks and responsibilities posed by user-posted content, whether this is in the form of user reviews, forums or live chat. Leaving aside any reputational or branding concerns that may flow from being associated with the wrong type of content, website owners may be held liable for content posted by their users in certain circumstances.

Potential liabilities

Defamation

One potential source of liability for a website owner is where a user defames somebody via the website. If a user of a website posts a defamatory statement then ordinarily a website

owner would not be liable for the defamation: provided that the owner was not the poster of the statement then a website operator will have a defence to a defamation action. However, the defence can be lost if the website owner acted with malice in relation to the posting of the statement or failed to respond appropriately to a notice of complaint from the person alleging defamation (complainant). If a complainant serves a notice complaining of defamation then the website owner must follow a strict procedure set out in the Electronic Commerce (EC Directive) Regulations 2002 (E-Commerce Regulations). Failure to follow the procedure correctly can lead to the website owner being liable for publication of the defamatory statement. It is therefore important to be aware of and follow the procedure correctly.

As part of the procedure under the E-Commerce Regulations the poster will also be asked whether or not their identity can be provided to the complainant. If they do not provide consent then the website owner may face court proceedings to compel them to reveal the identity of the complainant. While ordinarily the costs of the proceedings will not be met by the website owner it will undoubtedly use up management time and lead to ancillary costs that the website owner will be keen to avoid.

Intellectual property infringement

Another way in which website owners could find themselves liable for users’ posts is if they infringe a third party’s intellectual property rights. This could occur, for example, if the content posted copies a substantial part of someone else’s work (infringing somebody’s copyright) or using an identical/ similar mark to a registered trade mark in a commercial

context (infringing somebody's trade mark).

Hyperlinking content

Particular care needs to be taken in the case of users posting hyperlinks. Where users post hyperlinks to other websites that infringe intellectual property rights, are defamatory or contain illegal, obscene or confidential content then these links can, in themselves, be infringing, defamatory or illegal. This can be of particular concern where website link to sites in other jurisdictions, as the website owner could also be in breach of the laws of those jurisdictions and potentially subject to both civil and criminal liability.

In addition to liability through the courts, website owners could find that their site gets taken down by the internet service provider (ISP) that hosts it if their website contains content that infringes a third party's intellectual property rights. This would be likely to be highly damaging to the website owner's business. Additionally, most ISPs' hosting agreements will include warranties and indemnities against infringing third party rights, so the website owner may find themselves at the end of a contractual claim by the ISP for any losses suffered by the ISP.

What should website owners do?

Website owners should have in place clear rules and guidelines to regulate what content is permitted on their website and give them appropriate rights to remove infringing content and/or ban users who violate the rules. This would normally take the form of an acceptable use policy and content standards, which can be incorporated within the website terms of use. It is often a requirement of ISPs that sites that allow users to post content must have these rules in place. Having an appropriate acceptable use policy will allow website owners to be proactive in managing their users' postings and to react quickly to remove inappropriate content. Sites can also consider using moderators to try to manage what content makes it onto the site and quickly remove any inappropriate content.

If you would like any assistance in drafting your website terms and conditions or an acceptable use policy or in handling any issues that have arisen as a result of inappropriate content

being posted, please do not hesitate to contact our expert team on 0161 941 4000 or by email lawyers@myerson.co.uk.

**For more information
visit: www.myerson.co.uk
call: 0161 941 4000**





The Healthcare Sector meets the Tech Sector as a New Code of Conduct is released

Technology is all around us and non-more so than in the Healthcare Sector. The Healthcare Sector by its very nature is at the forefront of development, discovery, innovation and new technologies, however progress can be slow and many barriers have to be overcome. On 5th September 2018, the Department for Health and Social Care (DHSC) introduced a code of conduct setting out the government's commitment to support innovators in healthcare technology.

The code introduces a set of "gold-standard" principles with the primary focus on protecting patient data and encouraging the use of technology across the healthcare sector to create a trusted environment for data-driven technologies.

The DHSC hopes that the code will:

- help technology suppliers to better understand what is expected of them;
- improve healthcare services through the use of technology;
- encourage and increase the use of Artificial Intelligence; and
- help healthcare providers to choose safe, effective and secure technology.

- The code sets out 10 principles for technology companies to follow and pledges 5 commitments from the government.

The government has committed to:

- simplify the regulatory and funding landscape;
- create an environment which enables experimentation;
- encourage the NHS to adopt innovation;
- improve interoperability and openness;
- listen to users (including technology suppliers, healthcare professionals and patients).

The code is currently voluntary, but it is hoped that organisations will sign up to it to encourage collaboration between technology innovators and the NHS. The government is seeking feedback on the code, and has published an online questionnaire (<https://r1.surveysandforms.com/4c3zqo08-ef3b6jf1>).


The code will then be republished in December 2018, when it is hoped the code will become a standard for technology partnerships.



Myerson Solicitors LLP

Grosvenor House, 20 Barrington Road, Altrincham WA14 1HB

Tel: 0161 941 4000 | Fax: 0161 941 4411 | DX19865 Altrincham

lawyers@myerson.co.uk | www.myerson.co.uk |  myersonllp

Myerson is the trading style of Myerson Solicitors LLP, a limited liability partnership registered in England & Wales number OC347078, whose registered office is as above. This firm is authorised and regulated by the Solicitors Regulation Authority number 515754. VAT Registration number 380 4208 70. Any reference to a partner means a member of Myerson Solicitors LLP. A list of members is available for inspection at our registered office.



myerson