Spring 2019

Contents

Contract – contractual certainty/implied terms

Wells (Respondent) v Devani (Appellant) [2019] UKSC 4

The question

Was a binding agreement reached between a vendor and an estate agent, despite the parties not having specified the circumstances in which the agreed rate of commission would fall due?

The background

Mr Wells developed a block of flats in Hackney. By the beginning of 2008 six of the flats had been sold, one was under offer and seven were still on the market.

Mr Devani was an estate agent who contacted Mr Wells by telephone on 29 January 2008 in relation to the seven unsold flats. The trial judge found that during this telephone call Mr Wells asked Mr Devani about his fees. Mr Devani replied that his standard terms were 2% plus VAT. There was no discussion of the circumstances in which that commission would fall due.

Mr Devani introduced a buyer who completed the purchase of the unsold flats, and he claimed his commission, relying on an oral contract made during the telephone conversation. Mr Wells refused to pay. Mr Devani issued proceedings.

The High Court held that there was a binding contract between Mr Wells and Mr Devani, implying a term that the commission would be due to Mr Devani on the introduction of a buyer who actually completed the purchase.

The Court of Appeal overturned the High Court's decision, holding that the trigger event giving rise to an estate agent's entitlement to commission is of critical importance to a contract between a seller and estate agent. The Court of Appeal held that agreement over this term was essential for the formation of legally binding relations. As there was no contract, the courts could not make an agreement between the parties by implying terms.

The decision

The key question in dispute was whether, objectively assessed, the parties by their words and their conduct intended to create a legally binding relationship.

The words and conduct relied on in a particular case may be so vague that the court is unable to identify the terms on which the parties have reached agreement or to attribute to the parties any contractual intention. However, the courts are reluctant to find an agreement is too vague or uncertain to be enforced where it is found that the parties had the intention to be contractually bound and have acted on their agreement.

In the present case there was no need to imply a term into the agreement reached between Mr Wells and Mr Devani. Whilst there was no discussion of the precise event which would give rise to the payment of commission, it would naturally be understood that payment would become due on completion and made from the proceeds of sale. This was the only sensible interpretation of their telephone call and the circumstances in which it took place.

If it had been necessary to imply a term into the agreement, the Supreme Court would have done so. The Supreme Court disagreed with the Court of Appeal's suggestion that there is a general rule preventing the court implying a term where that will render an agreement sufficiently certain or complete to constitute a binding contract.

Why is this important?

The decision emphasises the court's reluctance to find that an agreement is too vague or uncertain to be enforced where the parties intended to be bound and have acted on their agreement. The decision demonstrates a pragmatic, business-oriented approach to contractual construction, with the court treating the parties' intentions and the way they have acted as key considerations in determining whether an agreement has been reached.

Any practical tips?

Although this pragmatic approach is to be welcomed, to avoid the risk that the courts will find a bargain unenforceable – or imply a term that is contrary to what they in fact intended – parties should take care to ensure all essential terms are expressly agreed.

Spring 2019

Contract – service of notices

UKI (Kingsway) Limited (Respondent v Westminster City Council (Appellant) [2018] UKSC 67

The question

What are the requirements for valid "service" of a completion notice?

The background

In January 2009, UKI began the redevelopment of a building at 1 Kingsway. In February 2012, Westminster City Council informed UKI's agents that it intended to serve a completion notice specifying a completion date of 1 June 2012. The Council asked the agents to confirm the identity of the owner of the building, but the agents declined to do so without obtaining instructions from UKI. At the time, the building was managed by Eco FM under a contract with UKI, but Eco had no authority to accept service of documents on its behalf.

On 5 March 2012, the Council delivered a completion notice by hand to the building, addressed to the "Owner, 1 Kingsway, London WC2B 6AN". It was given to an Eco receptionist, who scanned and emailed a copy of the notice to UKI. UKI received the notice no later than 12 March 2012.

UKI's agents appealed against the completion notice on 29 March 2012, on the grounds that the service of the notice was invalid. Shortly after, the premises were brought into the list with a rateable value of £2.75m. Appeals were made against both the completion notice and inclusion of the premises in the list and were initially heard by the Valuation Tribunal. That decision was later reversed by the Upper Tribunal but re-instated by the Court of Appeal.

Following a further appeal, the Supreme Court needed to determine whether the completion notice was validly served on the date it was received by UKI, despite:

- not being delivered directly to UKI by the Council, but passing through Eco's unauthorised receptionist
- being received by UKI in electronic form.

The decision

It was widely agreed by the Supreme Court that the method of attempted service adopted by Council was "far from ideal".

However, whilst paragraph 8 of Schedule 4A to the Local Government Finance Act 1988 outlines three specific methods of service, these do not exclude the availability of others. The purpose of these reliable methods is simply to minimise the risk of non-delivery. On the facts of this case, as the name and address of the owner could have been discovered by reasonable enquiry, it is clear this was not done.

However, the Supreme Court went on to consider the two legal issues highlighted below.

Indirect Service

Of relevance in this case is whether it matters that the notice reaches the intended recipient indirectly and through the actions of an unauthorised third party.

Consideration was given to the role of the Eco receptionist as an interposing third party. Whilst concepts of agency or statutory delegation remain irrelevant, it was held that the Eco receptionist did what could reasonably be expected of a responsible employee in that position.

Discussions regarding uncertainty were held to be unpersuasive, as the legislation does not make exhaustive provisions for the methods or dates of service. If the date of service is critical to the situation, the relevant authority may wish to minimise the risk of invalidity or failure by specifying the date of service. However, in this situation, the risk of prejudice to the building owner is limited as non-statutory methods depend on actual receipt by the intended recipient.

Electronic Communication

Consideration was also given to the electronic nature of the notice received by UKI.

Prior to the Electronic Communications Act 2000, service by fax was considered valid. Whilst service by fax is not entirely analogous with service by email, there is no good reason to distinguish these transmissions. Therefore, the Supreme Court held that Parliament must be taken to have legislated against that background.

The Respondent was unable to indicate any provision of the 2000 Act which expressly or impliedly restricted the previous law. The purpose of the Electronic Communications Act in 2000 was to provide clear guidance on the use of electronic methods of service by the authorities. The Supreme Court did not believe that this Act would be undermined by a ruling that, on the facts of this case, notice was successfully served by email.

Consequently, it was concluded by the Supreme Court that notice was successfully served and the property was brought into the rating list with effect from 1 June 2012. The Supreme Court reversed the decision made by the Court of Appeal, allowing the appeal and restoring the order of the Upper Tribunal.

Why is this important?

The UK Supreme Court has ruled that a document served indirectly or electronically can still be deemed properly served. This reaffirms the position that if a notice reaches the intended recipient, it is often enough for service purposes provided there is nothing to the contrary specifying service to be effected in a particular way. Furthermore, despite traditional reservations about service by electronic means, these can still be effective if not expressly ruled out.

Any practical tips?

Ensure that notice permissions in agreements are clear and practical. When serving a notice, ensure that contractual and/or statutory methods are followed precisely.

Spring 2019

Contract – frustration

Canary Wharf (BP4 T1) Limited v European Medicines Agency [2019] EWHC 335

The question

Can Brexit frustrate a contract?

The background

In 2011, the European Medicines Agency (the EU body tasked with the evaluation and supervision of medicines for human and veterinary use within the EU) entered into a 25 year lease at Churchill Place, Canary Wharf, which began in October 2014.

Following the UK's vote to leave the EU, in August 2017 the EMA informed their landlord (Canary Wharf) that they would treat the lease as having been frustrated if and when Brexit occurred.

The law of frustration operates to end a contract due to the effect of a supervening event which is: (a) not contemplated by the contract; and (b) is not due to the default of either party. The event has to change the nature of the rights and obligations under the contract such that it is unjust to hold the parties to the contract in the new circumstances.

EMA argued that Brexit would frustrate their lease due to:

- "supervening illegality" as the EMA would no longer have the legal capacity or power to perform its obligations under the lease
- Canary Wharf and the EMA had a "common purpose" entering into the lease for the building to be the EMA's headquarters, and Brexit would thwart that common purpose.

The development

The court rejected EMA's claim. While the judge noted that Brexit was not reasonably foreseeable at the point the lease was agreed in 2011, and that it would mean the EMA could not remain headquartered in London without losing certain protections of being in an EU Member State, this was not sufficient to frustrate the lease.

Whilst the court acknowledged that there were many reasons why the EU would prefer agencies such as the EMA to be headquartered in an EU Member State, these also could not frustrate the lease. In particular:

- on the proper construction of the relevant laws, the EMA's capacity or power to perform its obligations under the lease were not constrained
- even if the EMA was so constrained, and that was sufficient to frustrate the lease, these constraints had been self-imposed by the EU in response to Brexit.

Further, the lease had fully addressed the interests of both parties, and gave the EMA the possibility to leave the premises, with assignment and sub-letting permitted in certain situations. As such, there was no "common purpose" over and above the terms of the lease so as to frustrate the lease when it could not be achieved.

Why is this important?

This ruling provides a reminder of the high bar for parties pursuing frustration of contracts and indicates that, in the majority of cases, parties will not be able to rely on frustration as a convenient exit mechanism to escape unfavourable contracts following Brexit. The judge's reasoning suggests that for any frustration claim based on Brexit to succeed, Brexit itself will have to be a supervening event, rather than any decisions taken in response to Brexit.

Any practical tips?

Consider introducing express contractual permissions to deal with foreseen circumstances and/or, if possible, the consequences of unforeseen consequences, eg through force majeure provisions, termination rights, price adjustment mechanisms, etc. Brexit specific permissions (including customs issues, currency fluctuations, etc) should also be considered.

Spring 2019

Contract terms

The Business Contract Terms (Assignment of Receivables) Regulations 2018 (SI 2018/1254)

The question

How does the Business Contract Terms (Assignment of Receivables) Regulation prohibit restrictions on the assignment of receivables under commercial agreements?

The background

Following a number of drafts (which we considered in a Winter 2018 Snapshot), the Business Contract Terms (Assignment of Receivables) Regulations 2018 (the **Regulations**), came into force at the end of 2018.

The Regulations aim to ensure that SMEs' access to receivables financing (eg invoice-based financing) is not restricted, offering another option to improve liquidity.

The Regulations apply to relevant contracts entered into on or after 31 December 2018. They render ineffective contract terms which prohibit, impose a condition or otherwise restrict a party's right to assign receivables (a right to be paid any amount under a contract for the supply of goods, services or intangible assets) arising under the contract. The contract must be governed by English or Northern Irish law (although opting for foreign law purely to avoid the Regulations will not work). At least one of the parties to the contract must have entered into it in the course of carrying on business in the UK.

The development

The Regulations are designed to benefit SMEs only, as they are primarily affected by restrictions on access to receivables financing. The Regulations therefore do not apply to assignments where the supplier/assignor is a "large enterprise" (defined by reference to the company's latest filed accounts and applicable rules under the Companies Act 2006) or "special purpose vehicle" (a firm of which the primary purpose is to hold assets other than trading stock, or to finance commercial transactions, which involve it incurring a liability under an agreement of at least £10m).

The analysis of whether or not a company is an SME, and can benefit from the Regulations, takes place at the time of the (purported) assignment, rather than at the time the company entered into the contract giving rise to the receivable.

Is there anything to watch out for?

The law in this area is still developing, and uncertainties remain. Despite the Regulations' different drafts and re-drafts, some of the enduring issues include: (i) the somewhat complicated assessment of whether or not a company is an SME; (ii) the potential uncertainty at the time of entering into the contract as to whether the Regulations will apply at the time of assignment; and (iii) the fact that "assignment" is not actually defined in the Regulations – does it cover, for example, assignment by way of sale as well as by way of security? These could all lead to trouble and even litigation down the line.

Even if the supplier is an SME, beware also that the Regulations do not apply to certain types of contract, such as those which concern the sale of a business; the provision of financial services; or any interest in land.

Any practical tips?

Beware of the potential unpredictability of whether the Regulations apply to your business at the time of assignment. At the time of contracting, consider the importance of contract terms which may be said to restrict assignment of receivables, and the impact of those terms being unenforceable. Note in particular that the Regulations may render invalid confidentiality clauses seeking to prevent assignees from obtaining possible sensitive details, such as the nature and price of the goods or services in respect of which the receivables arose.

Spring 2019

IP

Supermac's (Holdings) Limited v McDonald's International Property Company Limited, CANCELLATION No 14 788 C (REVOCATION)

The question

What are the requirements for demonstrating genuine use of a trademark?

The background

Supermac's (Holdings) Ltd (**Supermac's**) applied to revoke McDonald's International Property Company Ltd's (**McDonald's**) EU trade mark registration for "BIG MAC" covering classes 29 and 30 (sandwiches etc) and class 42 (services associated with operating and franchising restaurants etc) (**EUTM**) on the basis that the EUTM was not put to genuine use during a continuous period of five years following the date of registration in relation to any of the registered goods and services.

McDonald's filed evidence of use demonstrating that the mark has been used in advertising and on the packaging of the goods that have been marketed. It is also claimed that "*as commonly known and attested to in the affidavits*" millions of products were sold under the EUTM. McDonald's concluded that if the Cancellation Division considered the evidence to be insufficient to show genuine use for all of the contested goods and services, then the application for revocation has to be rejected at least in so far as it is directed against some of the goods and services (eg sandwiches). Supermac's argued that the evidence of use submitted by McDonald's was insufficient to prove that the EUTM was put to genuine use for anything other than sandwiches.

The decision

McDonald's had sought to rely on three affidavits, signed by representatives of McDonald's companies in Germany, France and the United Kingdom. They claimed significant sales figures in relation to "Big Mac" sandwiches for the period between 2011 and 2016 and attached examples of the packaging of the sandwich (boxes), promotional brochures and what appeared to be menus. McDonald's also submitted printouts from its websites and from the "Big Mac" Wikipedia page.

The Cancellation Division held that the evidence filed by McDonald's was insufficient to establish genuine use of the EUTM. In particular, it was held that:

- **Affidavits**: statements drawn up by the interested parties themselves or their employees are generally given less weight than independent evidence. This is because the perceptions of a party involved in a dispute may be more or less affected by its personal interests in the matter; the probative value of such statements depends on whether or not they are supported by other types of evidence (labels, packaging, etc.) or evidence originating from independent sources.
- **Extent of use**: although some of the evidence referred to the relevant time period (eg some of the brochures and printouts from websites) and to some of the Member States of the EU, and the EUTM is referred to in relation to at least some of the relevant goods (eg sandwiches), McDonald's failed to prove the extent of use of its mark.
- **Websites**: the presence of the trade mark on websites can show, inter alia, the nature of its use or the fact that products or services bearing the mark have been offered to the public. However, the mere presence of a trade mark on a website is, of itself, insufficient to prove genuine use unless the website also shows the place, time and extent of use or unless this information is otherwise provided.
- **Brochures**: although the submitted packaging materials and brochures depict the EUTM, there was no information provided about how these brochures were circulated, who they were offered to, and whether they have led to any potential or actual purchases. There was also no independent evidence submitted that could show how many of the products for which the packaging was used (if that is the case) were actually offered for sale or sold.

The Cancellation Division concluded that the evidence did not provide sufficient details concerning the extent of use; other than exhibiting the sign in relation to goods which could be considered to be part of the relevant goods, these materials do not give any data for the real commercial presence of the EUTM for any of the relevant goods or services, including sandwiches. It followed that the submitted brochures, packaging and printouts did not give sufficient information to support the sales and turnover figures claimed in the affidavits.

Why is this important?

This decision applies well-established principles – the evidence filed by McDonald's did not satisfy the stringent criteria for demonstrating genuine use – but viewed against the background that "Big Mac" is one of the most recognised brands in the world and the apparent acceptance by Supermac's that "Big Mac" had been used in respect of sandwiches, it is very surprising that McDonald's were not able to demonstrate genuine use, at least in respect of the sandwiches/burgers for which it is so well known.

Any practical tips?

This decision demonstrates that even the owners of the most well-known brands cannot simply rely on reputation alone; all brand owners must satisfy the criteria set out by the EU IPO in order to demonstrate genuine use. If brand owners are relying on information in an affidavit, they must also provide sufficient evidence in support of any statements made within that affidavit.

Spring 2019

IP

PulseOn OY v Garmin (Europe) Limited [2019] EWCA Civ 138

The question

In the fight between two wearable sports-tech giants, *PulseOn v Garmin*, did the High Court correctly apply the test for infringement of Registered Community Designs?

The background

PulseOn (a developer of heart rate monitor wrist watches) alleged infringement of its Registered Community Design (RCD) for those watches by one of Garmin's sports watches, the "Forerunner 235". PulseOn's RCD sought to protect specific design features of the watch – in particular the shape and arrangement of three oblong LED sensors around a rectangular photo sensor.

Under EU design law, PulseOn's RCD allows it to prevent third parties (including Garmin) from using any design which does not create a "different overall impression" on the informed user. When considering the overall impression of the designs, the informed user will consider the degree of design freedom involved in the design and will place less weight on aspects where there is little or no design freedom (eg due to technical constraints).

In conducting that overall assessment, the High Court concluded that, whilst there was limited design freedom in relation to the placement of the LEDs and sensor (which needed to be placed in such a way so as to detect a person's heart rate), on the balance of the similarities and differences between the respective designs, Garmin's Forerunner design did not infringe PulseOn's RCD.

The decision

PulseOn appealed the High Court's decision on four grounds. The first ground was that the design freedom in the watches was actually wider than the judge stated. As result, PulseOn alleged that its RCDs should have been afforded a wider scope of protection. However, the Court of Appeal found that, whilst the judge may have stated the design freedom more narrowly than he should have (in relation to one particular feature) this did not result in a significantly wider scope of protection for PulseOn's RCD. The judge's conclusion that there was limited design freedom was materially correct.

PulseOn's second ground of appeal was that the judge should not have compared PulseOn's RCDs to enlarged 3D models of Garmin's Forerunner 235 watch (but should have used the actual Garmin product). The enlarged models exaggerated the differences between the designs. On this ground, the Court of Appeal found that usually a RCD should be compared to the allegedly infringing product itself. However, in this case the design in the product was so small that it made the comparison difficult. The judge was therefore justified in using the enlarged 3D models instead.

PulseOn's appeal was based on the third ground that the judge attached undue weight to features which were determined by technical considerations (ie the spacing between the different LEDs and the sensor). The Court of Appeal stated that the judge must have been aware of the reason for the differential spacing and the weight to be given to this in his overall evaluation was a matter for him. It had to be balanced against the fact that the spacing was not amongst the features found, either commonly or at all, in the design corpus, and was therefore entitled to more weight in the assessment.

The fourth ground of PulseOn's appeal was that the judge applied the wrong test for infringement of a RCD by asking himself whether the designs produced an "identical impression". The Court of Appeal found that the correct test for infringement is whether the designs create a "different overall impression". By saying that the designs did not create an identical impression, the judge was deciding that they were different. Whilst he may have used incorrect language, it was clear that he applied the correct test throughout his assessment.

Why is this important?

The decision confirms a number of key principles of European registered design law – both the correct test for infringement of RCDs and also the impact that the degree of design freedom can have on the overall impression of the designs.

Any practical tips?

In highly technical products (where design freedom is limited) smaller design differences are likely to be required for a design to create a "different overall impression" on the informed user. This is because the informed user will be taken to know, and will attach less weight to, the features of a design for which the designer has a limited degree of design freedom. As a result, technical designs and products will need to be more similar to each other for there to be an infringement than purely aesthetic designs where there is more potential for creative endeavour.

Spring 2019

IP

Bayerische Motoren Werke AG v BMW Telecommunications Limited and another [2019] EWHC 411

The question

Can brand owners rely on both registered trade mark infringement and passing off in order to prevent third parties from registering companies which incorporate their brand?

The background

On 12 May 2011, Mr Whitehouse incorporated a UK company under the name BMW Associates Limited (**BAL**). BMW wrote to Mr Whitehouse alleging trade mark infringement and passing off.

Mr Whitehouse claimed that "BMW" stood for his name, "Benjamin Michael Whitehouse". He said he was a one-man telecom railway company, carrying out telecommunications and signalling works. He also stated that he did not advertise his company, but used it for invoice purposes only.

BMW took the view that litigation would be disproportionate, and BAL and BMW (but not Mr Whitehouse himself) entered into a co-existence agreement in March 2012. Under the terms of that agreement, BMW undertook not to pursue its complaint and in return BAL made several undertakings. These included undertakings not to use the word "BMW" in relation to any goods or services except as part of its company name, and/or as part of its trading name BMW Associates, to be used solely in relation to its railway transport services and/or telecommunication routing and junction services.

In December 2017 Mr Whitehouse incorporated another UK company, giving it the name BMW Telecommunications Limited (**BTL**). This was not a breach of the co-existence agreement since Mr Whitehouse was not a party to it.

In July 2018 BMW issued proceedings for trade mark infringement and passing off on the basis that by incorporating BTL, Mr Whitehouse had equipped himself with an instrument of fraud. In the Court of Appeal case of *British Telecommunications Plc v One in a Million* [1999], One in Million Limited had applied for various domain names incorporating well-known brands, including Marks & Spencer. In reaching the decision that the mere registration of a domain name was an act of passing off, it was observed that those who consult the domain register would conclude that One In A Million Limited must be connected or associated with Marks & Spencer Plc. The One in a Million decision has since been applied in the case of *Halifax Plc v Halifax Repossessions* concerning the defendant's registration of a company which included the name Halifax.

The decision

BMW secured summary judgment in respect of its claim for trade mark infringement and passing off arising out of the registration of this UK company under the BMW name.

In respect of the claim for passing off, the Judge held that the case was fully analogous with One in a Million and that there was no real prospect of the defendants (BTL and Mr Whitehouse) establishing that not even a significant proportion of those consulting the UK Companies Register would believe that there is an association between the first defendant and BMW. The Judge therefore granted summary judgment in relation to BMW's passing off claim.

The Judge came to the same view in respect of trade mark infringement, but he did say he would need to be satisfied that the incorporation of the company itself either led to a sufficient likelihood of confusion, or a sufficient likelihood that the requirements of Article 9(2)(b) of the Trade Mark Regulations are met. Ultimately, the Judge was satisfied that the Court of Appeal's observation in One in a Million in relation to the likelihood of confusion amongst those who consult the UK Companies Register in the context of passing off would apply equally to the likelihood of confusion within the meaning of Article 9(2)(b) of the Trade Mark Regulations.

Why is this important?

This decision reinforces the position that brand owners can rely on both registered trade mark infringement and passing off in order to prevent third parties from registering companies which incorporate their brand, even though that company does not trade at all or trades under a different name.

It would also appear that the litigation in 2017 could have been avoided had Mr Whitehouse been a party to the original co-existence agreement.

Practical Tips

To avoid litigation, ensure that directors of companies are signed up to co-existence agreements where they are essentially the controlling mind of the company, and make sure that all the relevant parties have signed up to a co-existence agreement generally.

Spring 2019

IP

European Parliament introduces Directive on Copyright in the Digital Single Market

The question

How will the new Directive on Copyright change the legal and commercial landscape for both rights holders and content platforms?

The background

In September 2016 the European Commission proposed changes to copyright law including introducing a Directive on Copyright in the Digital Single Market with the intention "*to create a comprehensive framework where copyrighted material, copyright holders, publishers, providers and users can all benefit from clearer rules, adapted to the digital era*".

To this end, on 13 February 2019, the European Parliament, the Council of the EU and the European Commission reached an agreement on this Directive. The Directive was subsequently passed by the European Parliament on 26 March 2019 and will come into force from 2021. The Directive includes new rights for press publishers as well as regulating the position between content platforms such as YouTube and the respective rights holders.

The development

Right for publishers of press publications (Article 11)

In the Directive, the new press publishers right will be relevant to online press articles by information society services providers, like Google News, giving journalists a share of the revenue generated. Provisionally, the use of individual words or short phrases of publications will still be allowed without authorisation from press publishers. The new right does not relate to individual users but is targeted at online platforms like news aggregators.

Hosting user guaranteed content (Article 13)

The Directive seeks to regulate the payment received by writers and performers and the revenues enjoyed by the online platforms when they share their output. Article 13 considers that an "online content sharing provider" is communicating with the public when it allows them access to works that are protected by copyright. Sites like YouTube which host user generated works will need to apply for a licence in order to present copyright protected content uploaded by users unless it complies with conditions set out in the Directive. Where no licensing agreements exist with rights holders, the platforms will have to:

- make all efforts to obtain agreement
- ensure the unavailability of unauthorised content where rights holders have provided the appropriate information and
- act quickly to remove any unauthorised content once notified and stop future activity.

For less well-established platforms, with turnover of less than €10 million and 5 million monthly users, they will only have to adhere to the conditions that they have made best efforts to receive authorisation and that if notified they act as quickly as possible to remove the content. If the users increase to above 5 million they will in addition have to make certain that notified content does not re-emerge later.

Remuneration for authors/performers

The new Directive gives authors and performers rights to payment on the licensing of their rights and gives them a right to detailed information about exploitation of their work. If a piece of work becomes hugely successful and the fee originally paid was too low, the Directive provides for a contract adjustment correction. It also includes a mechanism for writers/performers to reclaim their rights when their work is not being used.

Exceptions and limitations

The Directive contains a mandatory exception for text and data mining to ease the burden on universities and other research institutions by lawfully permitting them to use new technology to analyse large data sets.

It also includes an online education exception for the use of online teaching, and a conservation and dissemination of cultural heritage exception, giving libraries, museums etc the opportunity to copy the works in their collections and archives with the benefit of new technology.

Why is this important?

The Directive has caused considerable controversy with critics believing that its permissions introduce legal uncertainty and will ultimately harm the creative and digital economies. Some users are also concerned that content will not be as readily accessible. Some concessions have been made, for example, with news aggregators able to include very short pieces of news reports, although exactly what that means still must be agreed upon. The Directive is not enforcing upload filters on user generated content platforms and it appears that memes and gifs will be able to be shared on these platforms. On the other hand, the Directive's supporters believe that it will increase revenues to publishers and creators of content, which will protect and promote the publishing and creative industries.

Any practical tips?

There is considerable uncertainty as to how the Directive will work in practice and what the commercial consequences will be for platforms, publishers/creators and users. Platforms will need to review what content they host/make available, the processes in place to deal with content and seek agreements with rights holders where necessary/desirable. Rights holders will also need to review the exploitation of their content and seek to balance access/availability against (potential) returns.

Spring 2019

Data protection

ICO guidance on contracts and liabilities between controllers and processors

The questions

What are the contractual liabilities and requirements of a data processor and a data controller under the GDPR?

The background

Before the GDPR, a data controller would typically have a contract in place with a data processor which would outline that the processor was secure and would be required to perform the controller's demands. The GDPR, however, has created an obligation for the parties to produce a more substantial contract with a set of further requirements.

The Information Commissioner's Office (**ICO**) has released guidance aimed at assisting data controllers and processors in complying with the GDPR's contract term requirements and by advising them on what their respective liabilities are.

The development

The obligation for a contract

Article 28(3) of the GDPR states that "*Processing by a processor shall be governed by a contract or other legal act …*".

The ICO advises that, in the UK, using a written contract between the controller and processor in relation to its processing activities is the most suitable method of being in compliance with the GDPR. The ICO provides that a direct contract is not necessary as long as the processor is contractually bound to the controller. In addition, any agreement between a processor and a sub-processor must be confirmed in a written contract and must provide an equal level of protection for the data as that in the contract between the controller and processor.

Contract requirements

- The processor processes the personal data only on documented instructions from the controller (Article 28(3)(a)): the ICO informs that, provided that they are written and are in a form that is able to be saved, the documented instructions can be given separately.
- Those processing data must have committed themselves to confidentiality (Article 28(3)(b)): the guidance states that the confidentiality term in the contract should include all employees, including temporary and agency staff who may be able to access the data.

- The processor must take all measures required pursuant to Article 32 (Article 28(3)(c)): the ICO determines these measures to include encryption and pseudonymisation, ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services and providing for regular testing and assessments of the effectiveness of the measures.
- The processor shall not engage another processor without prior specific or general written authorisation from the controller. In addition, if a processor contracts with a sub-processor, it should set out the same Article 28(3) requirements on that sub-processor (Article 28 (3)(d): the guidance clarifies that the actual contract wording need not be exactly the same as the contract between the controller and the processor but the contract should provide the same level of protection for the data.
- The processor, at the end of the agreement, must, on the controller's instruction, either erase or return the processed data and also erase existing copies of the data unless the EU or Member State law provides otherwise (Article 28(3)(g)): the guidance, acknowledging that the deletion of data may not be able to happen immediately, proposes that data does not have to deleted immediately as long as there are the relevant safeguards, the period that it is kept is satisfactory and that the data is deleted in timely fashion.
- The processor must 'make available to the controller all information necessary to demonstrate compliance' with the Article 28(3) obligations and must also 'allow for and contribute to audits, including inspections,' undertaken by the controller or on behalf of the controller: the guidance recognises that there is no obligation imposed on the processor to keep records of the processing that is specifically conducted for the controller. However, there is an obligation for processors to keep a record of their processing activities.

Controller's responsibilities and liabilities

- Art 28(1) states that a controller has the responsibility of ensuring that the processor can provide 'sufficient guarantees' to process and protect personal data in compliance with the GDPR: the guidance states that 'sufficient guarantees' could be determined by the processor's ability to help the controller comply with their obligations, breach notifications and DPIA's as well as being compliant with industry standards and up to date with codes of conduct and certification schemes. The processor should also supply the controller with the other documentation such as record maintenance, security and privacy policies. These examples are not exhaustive.

As an individual can bring a claim against the controller, whom may then be subject to the fines and penalties under the GDPR, the ICO advises that they make sure they and their processors are fully compliant. This is because a controller cannot be fined for a data breach where they can show they had been compliant and were not at all responsible. In addition, if fined, a controller can claim a contribution from the processor if they were at fault.

Processor’s responsibilities and liabilities

As the GDPR does not specify that liabilities and responsibilities should be included in the contract, the ICO advises that controllers and processors should incorporate a term into their contracts stipulating exactly the responsibilities and liabilities for each party.

The processor can be liable if it has not complied with the GDPR, performed data processing without the controller’s instructions or against the instructions or have contracted a sub-processor who is at fault.

Why is this important?

The guidance is helpful in both explaining the specific terms which need to be incorporated into the controller/processor agreement and providing more practical advice.

Any practical tips?

Controllers, processors and sub-processors should review their current contracts to ensure that they comply with the GDPR and that their responsibilities and liabilities are apportioned between the parties.

Controllers should also consider conducting regular audits and keep a record of the processing so that, in the event of a data breach, they can show that they had taken adequate steps to prevent a breach.

Spring 2019

Data protection

European Data Protection Board launches consultation on the territorial scope of the GDPR

The question

When will processing by a data controller or data processor fall within the territorial remit of the GDPR?

The background

The European Data Protection Board (**EDPB**) has opened a consultation on draft guidelines on the territorial scope of the GDPR. The territorial span of the GDPR is defined in Article 3 and is determined by two key criterion contained in Articles 3(1) and (2): the establishment criterion and the targeting criterion. The aim of the proposed guidelines is to assist in determining the application of the territorial scope of the GDPR. It is also intended to inform the process for the designation of representatives of non-EEA controllers and processors that target the EU.

The development

Article 3(1)

Article 3(1) states that the "*Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*".

This sets out a three part test, which the draft guidelines address:

1. An Establishment in the EU

The EDPB states in Recital 22 that "*an establishment implies the effective and real exercise of activities through stable arrangements*". The guidelines note that the "*legal form*" of the arrangement is not the most significant factor and that even the presence of a sole employee or agent might be enough to satisfy this limb of the test. Further, the threshold of "*stable arrangements*", for where the activities of a controller relates to providing online services, is stated as "quite low". Importantly though, the guidelines specify that one cannot determine an "establishment" through solely having a website that is accessible in the EU.

2. "In the context of the activities of" an establishment

The EDPB notes that the relevant processing does not have to be undertaken in the EU establishment for it to be caught by the GDPR. It states that the processing of data in, for example, China would be "*inextricably linked*", to the activities being undertaken in a Berlin establishment, if that establishment was set up to "lead and implement commercial prospection and marketing campaigns towards EU markets", even where there is no data processing in the Berlin establishment. Therefore, the Chinese processing would fall within the scope of the GDPR.

In order to determine the link, the EDPB sets out a two-stage test:

- whether personal data is being processed
- recognising whether there are links between the activity for which the data is being processed and the activities of the establishment in the EU.

3. Regardless of whether the processing takes place in the EU or not
As outlined above, whilst location of the area of the establishment of the data controller or processor **is** important, the place of processing is not a considered factor in assessing if the processing falls within the territorial scope of the GDPR.

Application of the "*establishment criterion*"
The draft guidelines note that the GDPR does not necessarily apply to both a controller and a processor in all situations where there is a relationship between them. A controller, that is based outside of the EU, but has a processor in the EU that processes data of non EU subjects, would not be subject to the GDPR. However, as the processor is situated in the EU, they would be subject to the relevant provisions of Article 3(1) GDPR.

Article 3(2)
Article 3(2) states that the "*Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union".

The EDPB advises a two-part test to assess the applicability:

1. Data subjects who are in the Union
The EDPB states Recital 14, which explains that the targeting criterion applies to more than just citizenship or residence but also to when an individual is in the EU. This must be evaluated at the time when the goods or services are being offered or behaviour is being monitored.

2. Offering goods or services … to such data subjects in the Union
The guidelines note that the offering of information society services falls within the rule and that payment is not the deciding factor. In order to be caught by this limb, the controller or processor must be offering their goods or services to data subjects situated in the EU.

The guidelines state that each case will be considered on its own facts but also gives a number of factors which may indicate that a processor is "offering goods and services" to individuals in the EU such as: the use of a language or currency, mentions of clients who are in the EU, using an EU domain name or providing delivery services to the EU.

OR

2. Monitoring of [data subjects'] behaviour
Similar to the offering of goods and services, monitoring also must take place when the data subjects are in the EU. The EDPB considers the following might be caught by Article 3(2)(b):

- behavioural advertisement
- geo-localisation activities, in particular for marketing purposes
- online tracking through use of cookie or other tracking techniques
- personalised diet and health analytics services online
- CCTV
- market surveys and other behavioural studies based on individual profiles
- monitoring or regular reporting on an individual's health status.

The EDPB did, however, confirm that they would not determine that any data analysis or collection would automatically be considered as monitoring.

Representatives of non-EU Controllers and Processors
Data processors and controllers, who target the EU from outside of the EU, have a duty to designate a representative in the EU unless they are exempt under Article 27(2) GDPR. This could be because they are a "*public authority or body*", if the processing is "occasional" in accordance with Article 9(1) GDPR, or if the processing is "*unlikely to result in a risk to the rights and freedoms of natural persons*".

Designation of a representative
Recital 80 states that "*the representative should be explicitly designated by a written mandate of the controller or of the processor*". This mandate will manage the requirements between the designated representative and the non-EU controller or processor. The representative's duties may be based on a contract with either an individual or a range of commercial bodies such as law firms, consultancies or private companies.

The EDPA clarifies that the function of the representative is not compatible with the position of an external data protection officer (**DPO**), as a DPO must, in accordance with Article 38(3) and Recital 97, have a degree of autonomy and independence.

The EDPA also highlights that the representative should be in the Member State that has the majority of the individuals whose data is being processed but also must remain easily accessible for other data subjects in other Member States whose data is being processed.

Obligations and responsibilities of the representative

Representatives must "*facilitate the communication between data subjects and the controller or processor represented*". In addition, in order to successfully achieve this, the representative must be able to communicate with both the individuals and authorities.

The representatives with the controllers of processors have an obligation to ensure that a record of processing activities is maintained. The EDPB further considers that representatives are liable to enforcement action such as fines and penalties.

Why is this important?

The guidelines will help companies to ascertain whether they have an establishment within the EU under Article 3(1), what types of "offerings of services and goods" and "monitoring" will be caught under Article 3(2) and if applicable, what responsibilities they and their designated representative will have to fulfil. Given the substantial penalties that companies can face for not complying with the GDPR, it is important that data processors and controllers know whether they fall within the territorial scope of the GDPR so that they can make the relevant adjustments to be compliant.

Any practical tips?

The EDPB encourages data controllers and processors to carefully assess their processing activities in order to determine whether they are subject to the GDPR. This is not always easy, and so the guidelines should be welcomed – particularly as they should assist in informing decisions as to when the Model Contract Clauses are required (ie for processing which includes data transfers outside the EEA).

Spring 2019

Data protection

ICO guidance on encryption and use of passwords in online services

The question

How can data controllers and processers improve their security measures?

The background

The Information Commissioner's Office (**ICO**) has released guidance on encryption and the use of passwords and online services. The aim is to assist data controllers and processors in processing personal data, in accordance with Article 32 of the GDPR, with the "*appropriate technical and organisational measures*".

The development

Encryption

The ICO has advised that controllers and processors should have policies that adequately regulate the use and implementation of encryption, including educating staff and being up to date with specific guidance and standards. The ICO recommends that the encryption of data in storage protects data against unlawful or unauthorised processing. It also informs that an effective method of safeguarding the data from interception from another party is to encrypt the data whilst it is being transferred.

The ICO has also listed four areas to consider when implementing encryption:

- selecting the right algorithm (and regularly examining its appropriateness)
- selecting the right key size (and ensuring it is large enough to protect from a data attack)
- selecting the right software (and ensuring that it meets current standards FIPS 140-2 and FIPS 197)
- keeping the key secure (and having systems to produce new keys if necessary).

Passwords

Although the GDPR does not expressly refer to passwords, any password system has to be "appropriate", meaning that the password set up should be periodically reviewed and updated.

The ICO questions whether the use of passwords is the safest system to use to protect personal data. The guidance argues that the number of passwords that the common user of an online service has to create results in both short and memorable passwords that are used across a number of webpages. The risk of what is known as "credential stuffing", was illustrated in 2012, when LinkedIn suffered a data breach and lost the passwords of 165m customers, which resulted in a number of other account breaches due to the similarity of their passwords on other sites.

The ICO recommends that a password system should make the accessing of stored passwords (in a readable form) as tricky as possible and also prohibit attackers from attempting to guess the password and username. The ICO also suggests limiting the number of login attempts allowed and basing this number on the perceived behaviour of both attackers and users.

The ICO specifies that hashing algorithms should be used in storing the passwords, rather than being kept in plain text. Regular assessment of the hashing algorithm is also necessary to protect the personal data. The ICO also states that login pages should be protected with HTTPS or a similar provision.

The ICO has listed three areas to consider for any password system:

- password length (which should be no less than 10 characters)
- allowing special characters
- password blacklisting, where passwords are compared to passwords on a “blacklist” which contains popular passwords, passwords that relate to the relevant service and former leaked passwords.

The ICO also notes that ideally a system should provide an easy way for users to construct a secure password and that a website should only have a password renewal system when it is completely essential for the circumstances.

Why is it important?

As “appropriate measures” are not defined in Article 32, the guidance is particularly helpful in ensuring that the right measures are taken with respect to encryption and passwords. All the more important when the ICO also makes it clear that regulatory action may be pursued if non-encrypted data is destroyed or lost.

Any practical tips?

Do not create a burdensome security process for users, whether in setting restrictions on the creation of a password, or requiring regular changes, as research suggests that this behaviour will cause the user to create weaker passwords. Remember also that if you are gathering data from the user to strengthen the password authentication system then this may be considered as processing data and you may be subject to the GDPR.

Above all, consider sharing the guidance with your IT director. All businesses need effective encryption and password systems, and making the guidance required reading within the IT department could prevent a major data breach in the future.

Spring 2019

Data protection

ICO updates its guidance on data protection impact assessments

The question

When should a data controller conduct a Data Protection Impact Assessment (**DPIA**)?

The background

Article 35(1) of the GDPR states that data controllers must undertake a DPIA where a type of processing "*is likely to result in a high risk to the rights and freedoms of natural persons*". If a high risk is identified, and cannot be mitigated, then the Information Commissioner's Office (**ICO**) must be formerly consulted before processing can proceed.

In April 2017, the Article 29 Data Protection Working Party adopted a set of guidelines on DPIAs (the **Guidelines**). These identified a set of criteria to indicate mandatory circumstances when a DPIA would be required. The criteria included the use of sensitive or highly personal data, large scale data processing and the innovative use of new technologies. Where two, or more, criteria are met during data processing, the Guidelines stipulate that a data controller must undertake a DPIA. However, a DPIA may also be required where only one criterion is met.

Under the GDPR, national supervisory authorities such as the ICO are required to publically list the types of processing which they consider fall within the remit of Article 35(1) GDPR. Such publications are subject to the "*consistency mechanism*" provided for in Article 63 GDPR, which kicks in where data subjects across a number of Member States would be substantially affected by data processing. This mechanism allows the European Data Protection Board (**EDPB**) to harmonise guidance provided by supervisory authorities on the types of processing "*likely to result in a high risk*".

Following the ICO issuing draft guidance on DPIAs last spring, the EDPB requested that a number of changes be made in an Opinion (22/2018) published in September 2018.

The development

The ICO has now published its revised guidance, which includes an amended list of examples of data processing "*likely to result in a high risk*". In accordance with the EDPB's comments, the amended list makes it clear where certain types of processing will only be caught when they occur alongside another criterion from the Guidelines.

The processing operations which will only warrant a DPIA when combined with another criterion include:

- those involving the innovative use of technologies, including the processing of new technologies
- instances where biometric data is used to uniquely identify an individual
- where "*invisible processing*" is being undertaken on personal data which has not been obtained directly from an individual
- the tracking of an individual's geolocation or behaviour, both physically and online.

Why is this important?

DPIAs are a fundamental element of the data protection regime established by the GDPR. They have been identified by the ICO as a key part of the new focus on accountability and data protection by both design and default. Their increasing prominence reflects the more risks-based approach which needs to be taken to comply with the GDPR.

Previously, the ICO had always stated that a privacy impact assessment, the DPIAs predecessor, was always necessary where processing operations involved the use of new technologies. By acceding to the EDPB's requests, and making a DPIA conditional on there being multiple criteria in play, the ICO's policy has shifted.

Any practical tips?

Despite this policy shift, the ICO's key message remains the same. It is best practice for DPIAs to be completed whether or not data processing "*is likely to result in a high risk*". Accordingly, data controllers should be slow to discount the need for a DPIA even in circumstances where only one criterion is met.

Spring 2019

Data protection

Video recordings and the journalistic exemption

The question

Does making a video recording on a digital camera constitute the processing of personal data? Can individuals benefit from the “journalistic exemption”?

The background

Mr Buivids made a video recording of police officers going about their duties in a Latvian police station, and then uploaded the footage to Youtube. The Latvian Supreme Court referred the case to the Court of Justice of the European Union (**CJEU**) for a preliminary ruling. The questions for the CJEU were whether the recording and publishing amounted to processing personal data under the Data Protection Directive (95/46/EC). And, if so, does the journalistic exemption apply, even though Mr Buivids was not a professional journalist? Note that, being pre-GDPR, the issues were considered under the Data Protection Directive (95/46/EC).

The decision

The CJEU held that the recording amounted to processing personal data. The recording showed an identified or identifiable individual and so was personal data. The act of storing the video on a continuous recording device (ie on the hard drive) constituted automatic processing of the personal data. Equally, the operation of loading personal data on a web page also constituted processing (of which at least part was automatic).

On the second question, despite Mr Buivids not being a professional journalist, the CJEU held that the journalistic exemption must apply not only to media undertakings but also to every person engaged in journalism. And “journalistic activities” are those which have as their purpose the disclosure of public information, opinions or ideas, irrespective of the means used to transmit them. It is now for the Latvian court to decide whether it appears from the video in question that the “sole purpose” of the recording and its publication was the disclosure to the public of information, opinions or ideas.

Why is it important?

Clarifying the scope of the journalist exemption, this decision shows the developing jurisprudence in support of citizens journalism within the journalistic exemption. Although the applicable Directive here (the Data Protection Directive) predated the implementation of the GDPR, there are similar provisions which still apply so the reasoning is likely to be followed.

Any practical tips?

It's clear that video recording does constitute the processing of personal data. It's also clear that "citizen journalism" may be considered processing for journalistic purposes. Note that, in the Data Protection Act 2018, the UK dropped the condition for the application of the exemption that journalism must be the "sole" purpose of the processing. This all suggests that "citizen journalism" is a concept which will have a strong footing should the debate arise within the English courts.

Spring 2019

Data protection

Does a Facebook Like button on your website make you a data controller?

The question

If the operator of a website embeds a third party plugin (such as the Facebook Like button), does this make it a joint data controller with Facebook?

The background

The Advocate General at the Court of Justice of the European Union (CJEU) has issued an opinion on this question, as raised in the German case of *Fashion ID GmbH & Co Kg v Verbraucherzentrale NRW eV* (Case C-40/17).

Fashion ID is a German online clothing retailer, which embedded the Facebook Like button into its website. This means that each time a user accesses the website, information about that person's IP address and browser string is transferred to Facebook. This happens automatically – it is not necessary for the user to click on the Like button, or for them to have a Facebook account, for the data to transfer.

A German consumer protection association (Verbraucherzentrale NRW) brought legal proceedings against Fashion ID, seeking an injunction on the ground that its use of the Like button constituted a breach of Directive 95/46/EC, which has now been superseded by the General Data Protection Regulation (EU) 2016/679 (**GDPR**). The case was referred to the CJEU for guidance.

The opinion

The Advocate General expressed the view that website operators who embed third party plugins which cause users' personal data to be collected and transmitted, are joint data controllers along with the third party. Consequently, the website operator will be jointly responsible for that stage of the data processing. It followed that the Advocate General considered Fashion ID to be a joint data controller along with Facebook Ireland.

However, the Advocate General also said that the controller's (joint) responsibility should be limited to the operations for which it co-decides on the means and purposes of the processing of the personal data. He referred to the CJEU statement in *Wirtschaftsakademie Schleswig-Holstein* (Case C-219/16), that "*operators may be involved at different stages of that processing of personal data and to different degrees*". Consequently, a joint controller cannot be held liable for the previous and subsequent stages of the overall chain of data processing, as it is not in a position to determine either the purposes or means of that processing.

The Advocate General expressed the view that Fashion ID and Facebook Ireland co-decide the means and purposes of the data processing at the stage of collecting and transmitting the personal data. They both voluntarily cause the data to be processed and transmitted, and there is a unity of purpose between the controllers in the sense that Fashion ID embedded the Facebook Like button on its website to increase visibility of its products via the social network.

The Advocate General concluded that Fashion ID acts a joint controller and has joint liability with Facebook over that stage of the collection and transmission of the data.

The Advocate General also touched on the legitimacy of the processing of personal data in the absence of the website user's consent. He noted that this is lawful under the Directive if three (cumulative) conditions are fulfilled: (i) the pursuit of a legitimate interest of by the data controller or the party/parties to whole the data is disclosed, (ii) the need to process personal data for the purposes of the legitimate interests pursued; and (iii) the fundamental rights and freedoms of the person concerned by the data protection do not take precedence. In this respect, the Advocate General proposed that the legitimate interests of both joint controllers in the Fashion ID case should be taken into account and balanced against the rights of the users of the Fashion ID website.

Finally, the Advocate General said that, where required, the website user's consent must be given to the operator if the website (in this case, Fashion ID) has embedded third party content. Similarly, the operator is under an obligation to provide the website user with the required minimum information.

Why is this important?

We await the decision of the CJEU, which should provide useful clarification on the duties and specific liability of joint controllers. This is important because breach of these duties may lead to strict liability under the GDPR, which states that individuals may exercise their rights against each of the controllers in relation to the processing of personal data over which they have no control.

Any practical tips?

The case is a useful reminder to businesses to know exactly what data processing is occurring via their websites, including as a result of any third party plug ins, such as the Facebook Like button. Properly understanding what's happening from a data perspective is the first step in addressing any potential exposure which may result from being deemed a joint controller of the relevant data.

Spring 2019

Consumer

Secondary ticketing: CMA secures court order against Viagogo to stop engaging in unfair consumer practices

The question

What steps are the CMA taking to crack down on the secondary ticket markets?

The background

For some time now, the CMA has been looking hard at secondary ticket sellers in an effort to ensure that all entities within the market comply with consumer protection laws. Voluntary commitments were given by three of the largest secondary ticketing websites, StubHub, GETMEIN! and Seatwave (owned by Ticketmaster). All three formally committed to new measures in April 2018 in order to make more information available to consumers on their websites.

Given Viagogo's reluctance to voluntarily agree to make such commitments, the CMA pursued High Court proceedings to obtain an order to force Viagogo to comply with its demands. A contested application was due to be heard in the High Court in November 2018, but Viagogo acceded to the CMA's requirements and an order was drawn requiring Viagogo and the other resellers to overhaul their practices by 17 January 2019.

The decision

The order of 27 November 2018 required Viagogo to:

- include information about whether there is a risk that the ticket buyer will be turned away at the door, which seat in the venue they will get and the identity of the seller if it is a business (to allow consumers to benefit from enhanced legal rights when purchasing from a business)
- make changes to its processes to prevent customers from being misled by messages about the availability and popularity of tickets
- make it easier for customers to obtain a refund when things go wrong and to avoid the risk of consumers' claims being rejected unfairly
- ensure certain customers who had previously made claims under Viagogo's guarantee, but didn't get their money back, will receive refunds if they were in fact entitled to them.

In addition to these requirements, the CMA also published an open letter to event organisers, setting out the information required to be disclosed to ticket resellers in order to allow them to meet their obligations under consumer protection laws. It also reminded the event organisers of their own obligations to treat consumers fairly.

On 5 March 2019, the CMA released a further statement to announce that Viagogo had not complied with the order of 27 November, requiring them to make the above changes before 17 January 2019. It said that it is now preparing to take further legal action to ask the court to find Viagogo in contempt. If found in contempt, the company could be subject to fines or have their assets seized by the court. Additionally, its directors could find themselves subject to criminal liability.

Why is this important?

This decision highlights the importance of considering the effect of a lack of information, and misinformation, for consumers. Businesses should be mindful of compliance with consumer law and cooperation with regulatory authorities when investigations are taking place.

Any practical tips?

The other ticket resellers have largely been able to stay out of the press by early commitment to make changes for the benefit of the consumer market. Viagogo, on the other hand, have suffered immeasurable damage from bad publicity, not to mention the mounting legal costs and threat of financial and criminal sanction currently hanging over their heads from their failure to comply with the Order. It goes without saying that, if you find yourself subject to a court Order, you must take all steps to ensure compliance within the deadlines set.

Spring 2019

Online platforms

House of Lords Communications Committee: "Regulating in a digital world"

The background

In January 2018, the Government published its Digital Charter, which identified its key priorities, including protecting people from harmful content and behaviour, the legal liability of online platforms, and data and artificial intelligence. In response to the Internet Safety Strategy Green Paper, it announced that new laws would be created to "*make sure the UK is the safest place in the world to be online*" and committed to the publication of the forthcoming online harms white paper. The latter is expected to address a number of topics covered by the Committee's report, including age verification for social media companies.

On 9 March 2019, the House of Lords' Communications Committee published its report "Regulating in a digital world". The report was far reaching and included some high-level objectives, but with little thought as to how they might be implemented. It is not yet clear which if any of the recommendations will be incorporated into the Government's White Paper.

The development

Regulation

The Lords' Committee posited that existing law and regulation affecting the provision and use of digital services was inadequate and it therefore proposed the creation of an overarching super-regulator, the Orwellian-sounding "Digital Authority", which would not only co-ordinate non-statutory organisations and existing regulators but have over-arching powers in relation to the latter.

A new joint select committee is also proposed, to cover all matters related to the digital world and specifically oversee the Digital Authority, "*to create a strong role for Parliament in the regulation of the digital world*".

This and all other regulators would be governed by a commitment to 10 key principles, many of which appear to be drawn from the obligations imposed under the General Data Protection Regulation and the Data Protection Act 2018:

1. parity
2. accountability
3. transparency
4. openness

5. privacy
6. ethical design
7. recognition of childhood
8. respect for human rights and equality
9. education and awareness raising
10. democratic accountability, proportionality and evidence-based approach.

Parity

The principle of parity was illustrated with the example that social media platforms should face the same obligations in relation to the imposition of age-based access restrictions as providers of online pornography.

Liability of social media platforms

The Lords' Committee considered that the hosting and curation of content which can be uploaded and accessed by the public meant that a notice and takedown model was no longer appropriate. The Committee recommends revising or replacing the protections under the E-Commerce Directive 2000/31/EC, but rejected the imposition of strict liability.

Obligations of social media platforms

Arguing that the moderation processes employed by social media platforms "*are unacceptably opaque and slow*", the Lords' Committee recommends that online services hosting UGC "*should be subject to a statutory duty of care and that Ofcom should have responsibility for enforcing this duty of care, particularly in respect of children and the vulnerable in society*", which should incorporate moderation services and an obligation to achieve safety by design.

The Committee did not accept the evidence calling for external adjudications of complaints or even judicial review of online moderation. Although the Committee does not seek to articulate the scope of the duty, in February the Children's Commissioner published a draft statutory duty of care proposed to be applicable to any online service provider which proposes a duty to "*take all reasonable and proportionate care to protect [anyone under the age of 18] from any reasonably foreseeable Harm*", which is defined as "*a detrimental impact on the physical, mental, psychological, educational or emotional health, development or wellbeing" of children, and from which liability for the acts of third parties can only be avoided if the provider has done "all it reasonably can to prevent Harm*". The factors by which the discharge of the duty should be determined, such as the speed of responding to complaints (legitimate or otherwise), are not proposed to be limited to their application to children, and would therefore have the effect of imposing wider obligations vis-à-vis all users of the service regardless of impact.

Competition

Concerned about the impact of the creation of data monopolies and the consequences for consumer protection, and (perhaps surprisingly) comparing online service providers to utility providers, the Committee recommended that the consumer welfare test needs to be broadened to move away from a focus on consumption and price and that a public interest test should be applied to data-driven mergers.

Algorithms

The design and transparency of algorithms was of particular concern to the Committee.

In an example of a differentiation between acceptable conduct online and offline, the Committee disapproved of the use of technology to take advantage of psychological insights to manipulate user behaviour, for example to encourage time spent using a service. While psychological insights have long been a tool utilised by the retail sector, for example, and even the government itself with David Cameron's "nudge unit", the Committee suggested that ethical design required that "*individuals should not be manipulated but free to use the internet purposefully*". The Committee recommended that the ICO should produce a code of conduct on the design and use of algorithms, potentially working with the Centre for Data Ethics and Innovation to establish a kitemark scheme, but also have powers of audit supported by sanctions.

The Committee also recommended that greater transparency around the use of algorithms and the data generated be achieved by requiring service providers to publish information about the data being generated and its use, as well as by affording users an enhanced right of subject access. The Committee proposed that the former be applicable to both data controllers and data processors.

Terms and conditions

The transparency, fairness and age appropriateness of terms and conditions was also a key focus for the Committee and the Committee suggested that these should be subject to regulatory oversight with any service provider which breached its terms of service being subject to enforcement. This would not appear to encourage service providers to provide gold standard service commitments for fear of being penalised for failing to meet them and could result in a lower common standard.

Why is it important?

While many of the Committee's proposals are likely to be welcomed in some quarters, the practicality of designing and implementing them, and the impact they would have on the majority of users and the provision of services, means that they warrant at least further scrutiny, if not revision or rejection, if the government is to achieve the "right regulation".

The proposals are intended to ensure that unlawful conduct is treated consistently whether online or offline, and there is a stated commitment not to limit free speech or lead to unjustified censorship. However, they extend far beyond the regulation of what is unlawful and trespass on what is deemed to be harmful or anti-social. The proposals would impose more stringent restrictions on the online space than other forums for public discourse, potentially threatening an undue restriction on freedom of expression. They also fail to articulate what constitutes an “online harm”. It is unacceptable to put online service providers in the position of legal adjudicators, with the threat of sanction if they are deemed not to be delivering in the desired manner.

By proposing to regulate the terms and conditions of user services, apparently without seeking to set minimum standards, the Committee risks subjecting the most responsible platforms to the greatest regulation by virtue of seeking to enforce their terms and conditions.

Any practical tips?

Online service providers do not need to make drastic alterations yet but should be aware of what of these changes will mean for their business if they are realised in the White Paper.

Spring 2019

Influencer marketing

CMA tightens noose on ad disclosures

The question

How can brands and influencers ensure they comply with the (tough) approach now being adopted by the CMA?

The background

Following CAP's Influencer Guidance, influencer marketing still remains a hot topic for regulators, with the Competition and Markets Authority (**CMA**) releasing the results of their Customer Enforcement Investigation on 23 January 2019.

16 well known celebrities have given undertakings to the CMA, and further guidance has been issued on how to be transparent with your followers.

The development

The CMA appears to take a much firmer stance to the previously released guidance on some of the more controversial areas of influencer marketing, including when influencers are given freebies, when they are promoting their own product ranges, and where there is a historic relationship between an influencer and a brand.

The CMA have re-stressed that if you have not purchased the product or service yourself, and have received it for free, then this must be made clear. Furthermore, if you do not currently have a relationship with a brand, but have in the last year (or you received free products or services) then this must also be made clear.

The CMA has identified three key areas where influencers can mislead consumers by giving false impressions.

1. You are just a consumer, when in fact you are actually acting for a brand or your own business purposes.

2. You have bought something, when you were actually gifted the product or service.

Both of the above could lead the consumer to think you have purchased the product yourself, as you think it is good value for money or good quality.

3. You have used the product yourself, when you have not, and are making claims about its benefits. This could lead the consumer to reasonably assume that any results being claimed are ones you have experienced first-hand.

How can I avoid misleading consumers?
The CMA has made it clear that the labelling must be easy to understand and transparent, without the need to have to click for more information. This means disclosure should be made upfront, and not buried amongst other hashtags.

Examples of good practice include:
- labelling with “Advertisement feature”
- labelling with “Advertisement promotion”
- using #Ad/ #Advert
- “Paid Partnership” tool in Instagram in addition to the above hashtags.

Examples of bad practice include:
- tagging the brand or business without additional disclosure
- tagging a gift from a brand in the picture or text without additional disclosure
- only using discount codes, competitions or giveaways
- making references to it being your own range
- using ambiguous language such as “thank you”; “made possible by”; “in collaboration with”, etc
- #sp; #spon; #client; #collab
- adding #ad directly after the brand name – [BRANDNAMEad]
- hiding the disclosure among other hashtags or at the end of a post
- product placement where there is an associated payment or other incentive
- only disclosing the commercial affiliation on your front page/profile page/bio.

Additionally, if a post contains multiple brands with which you have relationships, every effort should be made to make them all prominent and clear.

Finally, the CMA was firm in pointing out that there is no perfect solution for labelling your content across all platforms. Influencers and brands need to be conscious of how the different social media platforms present their content, so that they are able to clearly label it.

Why is this important?
The CMA is treating influencer marketing as a regulatory hot topic, and is something all brands and influencers need to take seriously going forwards into 2019.

The CMA undertakings (as signed by the celebrities) include requirements to label posts clearly where you have received gifts from a brand, avoid falsely representing yourself as a consumer, and not claiming benefits for a product when you do not use the product. The celebrities have also agreed to follow the CAP Code and the ASA's associated guidelines. Although the undertakings do not place any further burdens than what has already been stated in both the CMA and in CAP and ASA guidance; the consequences for now breaching the rules could be far more severe.

Any practical tips?

It is important for influencers to remember that posts need to be clearly labelled. It is not enough to assume the consumer will infer that the post is an advertisement/promotion because you have used discount codes, referred to it as your own range, thanked the brand, or disclosed the commercial relationship in your bio.

The guidance has confirmed for the first time that the "Paid Partnership" banner on Instagram is acceptable labelling; however, it still needs to be used in addition with other hashtags to make it clear to consumers.

With the CMA stating that the law is not prescriptive as social media evolves, it still remains far from clear what the best approach is for brands and influencers. Some of the guidance will prove difficult to follow in practice. This is particularly so for influencers who do multiple brand posts on Instagram, and need to declare all the different relationships before the consumer has to click on "see more".

The CMA remains on the look-out for infringers, as indeed does the ASA. For now, the best approach is to play it safe and to be as clear as possible to consumers. If in any doubt, label!

Spring 2019

ASA

The ASA's strategy for the next five years

The question

What is the ASA's core strategy for the next five years? How proactive is it going to be as a regulator in the digital space?

The background

The Advertising Standards Authority (**ASA**) launched its five-year strategy at a conference in Manchester in November 2018. Titled "*More Impact Online*", the ASA's new strategy focuses on making the regulation of online ads stricter and explores the ways in which the ASA can harness new technology and build on relationships with online platforms to achieve this aim. Given that online adverts made up 88% of all adverts where action was taken by the ASA in 2017, it is unsurprising that the regulation of online advertising is central to the ASA's strategy for the next five years.

The development

The ASA is particularly keen to tackle the perception that online is a "Wild West". With consumer-targeted scams, fake news and data breaches regularly hitting the headlines, the ASA has acknowledged that there is a general level of consumer mistrust in the online world, and is seeking to ensure that the advertising community does its part to combat this. Accordingly, whilst online-only assets may have historically been seen as lower risk for many businesses (i.e. due to their transient nature and the fact that they may not be as high-profile as TV or OOH ad campaigns), it is clear that they will be more heavily scrutinised going forwards.

So, how does the ASA intend to realise its online ambitions?

- **Collaboration and buy in**. The ASA is pushing for the entire industry to do their part in upholding advertising standards to help ensure that confidence in the self-regulatory system is maintained. The ASA also confirmed that it will look to collaborate further with online platforms to explore ways that these platforms can assist in protecting the public from irresponsible advertising. Monitoring social media for comments on advertising was put forward as a possible avenue to assist the ASA in obtaining consumer insight to help reach decisions on compliance.
- **Improving technology**. The ASA is considering how it can utilise technology such as AI/machine learning/algorithms to proactively combat non-compliant online advertising. This would represent a huge shift in the way that the ASA currently tackles non-

compliance and, if implemented successfully, will help address concerns that the ASA's approach can be akin to a game of "whack-a-mole" with some non-compliant advertisers.

- **Simpler services**. The ASA will explore whether its processes can be simplified and made more user-friendly. For example, the ASA is already considering ways to improve the competitor complaint process and is exploring easier ways for consumers to report non-compliant online adverts to them.
- **Sanctions**. The ASA is seeking to improve its sanctioning of non-compliant advertisers across all areas of online advertising

What is also clear is that some of last year's hot-topics will continue to be a focus for the ASA in the future - with child protection, influencer marketing, gender stereotyping and IoT all receiving a mention at the conference. In particular:

- **Child protection**. The protection of children is high on the ASA's list of objectives for 2019 and beyond. The ASA will continue to focus resource to ensure that child exposure to age-restricted ads in sectors like food, gambling and alcohol is limited. This is hardly surprising at a time where areas like HFSS advertising are receiving increased legislative scrutiny and the ASA is under considerable pressure to demonstrate that the current rules are effective in this area.
- **Native, influencer and affiliate advertising**. Following guidance published at the end of 2018, the ASA will endeavour to raise awareness of regulation in these areas and the consequences of non-compliance, particularly amongst individual influencers who may not have previously been aware of requirements of the Advertising Codes and consumer law when posting content on their channels.
- **Voice, facial recognition, machine-generated personalised content and biometrics**. These areas were also identified by the ASA as presenting labelling, content and targeting issues. In 2018 we saw the first virtual-assistant related complaint to the ASA which concerned a customer's Amazon Echo Dot accidentally interacting with an Amazon TV ad. Although the complaint against Amazon was ultimately not upheld, as our homes become even smarter, it is likely that we will see further adjudications concerning virtual assistants and smart devices.
- **Gender stereotyping**. The ASA re-emphasised its commitment to developing standards on gender-stereotyping in advertising as it is concerned that harmful stereotyping of gender roles or characteristics in ads, eg depicting women as being solely responsible for cleaning the home, restricts the choices, aspirations and opportunities of children, young people and adults. Since launching the More Impact Online strategy, the ASA has issued Guidance on gender-stereotyping (which we have summarised in another snapshot).

Why is it important?

The More Impact Online strategy shows clear intention by the ASA to regulate current and emerging forms of online advertising more strictly, and recognition by the ASA that it will need to adapt to fulfil this ambition. In terms of the ASA's intention to collaborate further with online platforms, this presents an opportunity to develop an online regulatory climate which both protects consumers and allows more freedom to compliant advertisers.

Any practical tips?

Brands will need to be even more diligent when advertising online and will need to continue to pay close attention to ASA announcements and CAP guidance on emerging online advertising spaces.

Also, look out for the ASA taking a more proactive stance towards tackling online infringements. We are already seeing the ASA's deployment of AI and avatars (to mimic children online) in order to pursue brands within certain regulated markets.

Spring 2019

ASA

CAP issues new rule and guidance on gender stereotyping

The question

How can ads avoid falling foul of the new gender stereotyping rule?

The background

There were a number of ads in 2017 that received backlash from the public due to gender stereotyping, such as the GAP ad that dressed a young boy as a "scholar" in contrast to a young girl dressed as a "social butterfly", and the KFC ad which mocked two men's emotional anxiety. Concerns over the portrayal of gender stereotypes led to an ASA review and consultation in 2018. This has resulted in a recently released new rule with accompanying guidance to combat the issue.

The new rule, which will come into force on 14 June 2019, is accompanied by guidance on how to help ads steer clear of negative gender stereotyping. Currently, the CAP Code allows the ASA to intervene if an ad causes "serious or widespread offence". The new rule (4.9 of the CAP Code and 4.14 of the BCAP Code) significantly changes this, stating that "*marketing communications must not include gender stereotypes that are likely to cause harm, or serious or widespread offence*".

The ASA has stated that humour and banter will not be considered as mitigating factors in instances where there is gender stereotyping and added that when contemplating complaints, it will take into account:

- the ads likely impact as a whole and in context
- the view of the group of people that have been stereotyped
- the use of other stereotypes, such as race, age and disability, in the ad.

The guidance

The guidance sets out five scenarios, including descriptive examples, where the ASA may come to the conclusion that harm has been caused.

1. Scenarios featuring gender-stereotypical roles and characteristics

The guidance states that roles include "*occupations or positions usually associated with a specific gender*", whilst characteristics include "*attributes or behaviours usually associated with a specific gender*". It clarifies that it is possible to portray individuals in their gender stereotypical roles. However, ads should avoid positing that the gender's role and characteristics depicted:

- are solely associated with one gender
- limit the choice of behaviour or occupation of that gender
- cannot ever be undertaken by the other gender.

Example ads which may fall foul of the new rule include those which:

- starkly contrast male and female stereotypical roles
- highlight any gender not succeeding in a task solely due to their gender, or
- portray that a woman's application of make up is more important than other parts of their life.

2. Scenarios featuring pressure to conform to an idealised gender-stereotypical body shape or physical features

The guidance states that ads are allowed to contain attractive, successful and healthy people. However, ads should not intimate that a person's mental wellbeing and happiness is dependent on conforming to the idealised gender-stereotypical body shape or physical features.

Further, ads which depict people as unsuccessful or unattractive should not insinuate that the sole reason is because they have not conformed. Importantly for weight loss products and services, the guidance clarifies that 'responsible' ads will still be permitted.

3. Scenarios aimed at or featuring children

The guidance confirms that ads can be clearly directed at children of a specific gender, even when the activity or product is typically associated with that child's gender. But they should be careful to avoid portraying what they seek to promote as unambiguously applicable to only one gender. In addition, ads should not directly contrast a boy's stereotypical characteristics to a girl's characteristics.

4. Scenarios aimed at or featuring potentially vulnerable groups

The guidance advises that ads should show understanding to the mental and physical health of individuals in vulnerable groups who may feel pressure to adapt to certain gender stereotypes.

Ads targeted at new mums implying the importance of attractiveness and being a good housewife over their emotional health and ads directed at teenagers suggesting that a gender-stereotypical body or characteristic is essential to a successful social or love life are both examples of ads that may be deemed likely to harm potentially vulnerable groups.

5. Scenarios featuring people who don't conform to a gender stereotype

The guidance warns that ads, which jeer those who do not fit to gender stereotypes, even when used with humour, will be unacceptable under the new rule. One of the examples given is that of a man mocked for undertaking "female" roles.

Why is this important?

The law currently means that the ASA can only intervene for issues that are likely to cause serious harm or widespread offence, which is a much higher threshold than simply "likely to cause harm". With the clamour of social media and reporting of controversial ads, companies are facing increasing public scrutiny and negative publicity if they breach these rules. It's more important than ever for companies to be extra careful about how they portray gender.

Any practical tips?

Don't make light of gender issues, as humour won't save you! But above all, remember that gender issues are now subject to a lower ASA threshold. Anyone involved in the production of an ad of this type should revisit the guidance as a matter of course. Failing to do so could lead to an embarrassing, and expensive, pulling of a media campaign.

Spring 2019

ASA

BCAP issues guidance on use of superimposed text in TV advertising

The question

What guidelines must superimposed text on TV ads comply with in order not to mislead viewers?

The background

Superimposed text (**supers**) refers to the "small print" found on TV ads, such as wording included for legal/regulatory purposes or in order to qualify, clarify or add significant details about the product or service being advertised or a claim being made.

The Guidance which came into force on 1 March 2019 (the **Guidance**) addressed findings by the ASA and BCAP that supers are often too long, too complex or too hard to read against the background. This can have the effect of misleading viewers, in breach of the BCAP Code and legislation which prohibits misleading claims in ads. The Guidance therefore assists advertisers in complying with the Code and relevant legislation. Note that, just because an ad's supers are not misleading does not mean the other elements of the ad or the ad as a whole are not misleading.

The scope

The Guidance applies only to actual TV ads, not on-demand and other similar services**.** It also applies only to text superimposed onto the ad, usually at the bottom, for the purpose of complying with relevant misleading advertising rules. The Guidance will generally not be relevant to statements included solely for legal/regulatory purposes, to subtitles (eg added for accessibility) and to other text incidentally included within the creative of the ad itself.

The principle

The general principle is that written information which qualifies the ad must be "presented clearly" and reasonably legible, considering the surrounding picture, length of time available to the reader, amount of text to be absorbed and significance of the information being conveyed. Particularly important information, for example, might be emphasised through the voice-over or displayed on screen for an extended time in order to ensure viewers can understand the information and are not misled.

Why is this important?

While the ASA has indicated its intent to allow advertisers an adjustment period until September 2019, so that problematic supers will initially be addressed informally rather than through a formal ASA ruling, the Guidance is part of the ASA's ongoing function to prevent misleading or harmful ads. The ASA has emphasised that the Guidelines represent "big changes" which were needed, and will affect all sectors - some "quite considerably".

Any practical tips?

Advertisers should seek to minimise the use of supers in TV ads where possible. Where supers are necessary, consider the detailed technical guidelines in the Guidance, which set out rules on aspects ranging from size of text, font face and character spacing, to sentence structure, duration of display and position on screen.

Spring 2019

ASA

Carlsberg in the clear on the inappropriate targeting of under-18s

The question

What will satisfy the ASA that an alcohol ad has not been inappropriately targeted at under-18s?

The background

An ad for Carlsberg was seen on 17 May 2018 within the PC game Microsoft Solitaire. The complainant challenged the appropriateness of the ad's targeting since it was seen while playing a game that could be used by children.

The ASA looked at whether the ad breached CAP Code Rule 18.15, which requires that marketing communications are not directed at under-18s through the selection of media or the context in which they appear. It also requires that if any medium has an audience of over 25% of under-18s it cannot be used to advertise alcoholic drinks.

The response

Carlsberg explained that its agencies had placed the ad programmatically with software which uses data to advise on decisions on which ad space to buy. Carlsberg and its agencies had not had any direct contact with Microsoft regarding the placement of the ad. The software compares the online behaviour of the user against that of the selected audience for the ad in deciding its correct placement. Carlsberg was satisfied that the agencies had ensured that the ad was suitably targeted and was not in any way focused on under-18s through the selection of media or its context.

Carlsberg also said that 98.3% of the visitors to the Microsoft website that hosted the games including Solitaire, Sudoku and Mah-jong, were aged over 18 in accordance with the rule that no more than 25% of its audience is under 18. Furthermore, the ad was targeted at users aged between 25 and 34 years of age which gave a seven year buffer over the age restriction. There was nothing in the ad of any specific interest to children.

In order to further limit the risk of under-18s seeing the ad, Carlsberg used behavioural targeting. They used multiple third-party data firms who collected data on age, gender, income and use of other websites, apps and content areas viewed and clicked. Online behavioural data, declared and inferred, was obtained from a variety of sources such as surveys, content downloads, logins, loyalty cards as well as characteristics surmised from a user's online activity.

The decision

The ASA explained that, since the ad was targeted to a specific set of users on the Microsoft website, the only relevant test was whether it had been targeted at under-18s. The ASA pointed to the results from the third-party data analysis which showed that 98.3% of visitors to the website were aged over 18 and further that Carlsberg had built in a seven year buffer to safeguard the fact that users were aged over 25. Since Carlsberg had used behavioural data including online usage and interest-based targeting, and had also established an age buffer, the ASA believed that these methods adequately reduced the possibility of under 18 year olds seeing the ad.

It was therefore decided that the ad had not been directed at under-18s and was not in breach of CAP Code rule 18.15.

Why is this important?

This decision shows that as long as companies proactively limit, through technological means, the risk of their ads being seen by children, they should be able to maintain that their ads are not directed at children.

Any practical tips?

Marketing firms need to be able to show that they have taken adequate steps to make sure their ads are targeted at 18 year olds and over. The decision is a useful recap of the hurdles that brands need to jump through from a technological perspective to remain in the clear on the advertising of age-restricted goods and services.

Spring 2019

ASA

CAP guidance on misleading "faux fur" claims in clothes and accessories

The question

How careful should retailers be that their "faux fur" products really are "faux"?

The background

CAP has recently issued an "*Enforcement Notice on Misleading 'Faux Fur' claims in clothes and accessories*" following two ASA rulings which found that consumers had been misled by advertisements for faux fur products which had actually contained real fur, in contravention of Section 3 of the CAP Code.

The Enforcement Notice, published on 17 January 2019, encompasses advertising across all media, including websites, social media platforms and online marketplaces and platforms. The Notice requires all retailers to take steps to ensure that they do not advertise products as containing faux fur if in fact they contain real fur.

The decision

The ASA rulings related to a "Faux Fur Pom Pom Jumper" and a "Faux Fur Pom Pom Headband" which were found to contain real animal fur. The ASA found that the retailers who had advertised the products had breached sections 3.1 and 3.7 of the CAP Code. Section 3.1 says that "*marketing communications must not materially mislead or be likely to do so*" and section 3.7 states that "*before distributing or submitting a marketing communication for publication, marketers must hold documentary evidence to prove claims that consumers are likely to regard as objective and that are capable of objective substantiation. The ASA may regard claims as misleading in the absence of adequate substantiation*".

The Enforcement Notice also refers to relevant legislation which retailers must comply with, including the Consumer Protection from Unfair Trading Regulations (**CPRs**) and The Textile Regulation (EU) No 1007/2011 (the **Textile Regulation**). Notably, section 6(1) of the CPRs prohibits a misleading omission of information that causes or is likely to cause the average consumer to take a transactional decision that they would not have taken otherwise. As the RSPCA has conducted a survey to which 95% of participants responded that they would never wear real fur, clearly advertising a product as containing faux fur when it in fact contains real fur would constitute such a misleading omission.

Also relevant is Article 13 of the Textile Regulations, which requires any textile process containing non-textile parts of animal origin to be labelled as "*contains non-textile parts of animal origin*".

Why is this important?

The Enforcement Notice recognises that in most instances retailers are not deliberately trying to mislead consumers about faux fur products, and that the advertisement of faux fur products which in fact contain real fur is usually a result of supply chain issues or a lack of education. However, the Notice also highlights that it is the advertiser's responsibility not to claim that products are made from faux fur if they contain real fur. The Enforcement Notice states that targeted enforcement action will be taken by CAP's compliance team from 11 February 2019 in relation to misleading ads. Retailers selling faux fur products would do well to start taking steps to ensure that they do not contain real fur and that they comply with the CAP Code.

Any practical tips?

The ASA has advised that laboratory analysis is the most accurate method for identifying real and faux fur. However, the Enforcement Notice also provides a three-step test that retailers can use to identify the different between real and faux fur. This includes checking the base of the fur (faux fur will usually have threaded fabric from which the "hairs" emerge), checking the tips of the fur (real fur usually tapers to a point which faux fur does not) and burning a sample of the fur (real fur will singe and burn like human hair whilst faux fur melts and smells like burnt plastic).

In addition to this test, the Enforcement Notice also includes some general do's and don'ts for retailers who sell faux fur products. These include being as transparent as possible about the materials in advertised products, and not assuming that a low cost of a fur product from a supplier means that it is faux fur.

Spring 2019

ASA – pricing

Carwow ruling: RRP claims must reflect the price of products as "generally" sold

The question

What type of evidence is the ASA looking for to substantiate that an RRP is the price at which a product is "generally" sold?

Summary

The ASA has upheld complaints against two ads for a car purchasing platform on the basis that: (i) references to RRP did not reflect the price at which the relevant vehicle was generally sold; and (ii) average savings claims were calculated using RRPs that again the relevant vehicle was not generally sold at.

The ads

The price comparison website www.carwow.co.uk, featured a listing for a Ford Mondeo with an "RRP" of £24,195 (the **Web Ad**). A complainant challenged whether the RRP was misleading, on the basis that Ford's website listed the same car with a lower RRP of £23,590.

Carwow's TV ad, featured the claim that "buyers save an average £3,600", with "savings against RRP" (the **TV Ad**) . A different complainant challenged whether the savings claims made by Carwow could be substantiated, or were in fact, misleading.

The response

In respect of the Web Ad, Carwow argued that its RRPs were gathered from CAP HPI, a third party which gathered and analysed data from numerous industry sources (including vehicle manufacturers and the DVLA). Carwow also confirmed that, following a separate complaint regarding the RRP of the Ford Mondeo, it had received confirmation from Ford that the RRP listed on Ford's own website was out of date and related to a previous model of the Mondeo. Carwow argued that it had based its RRP on CAP HPI's data which was in date, and related to the most recent Mondeo model. Ford had supplied this up to date pricing data to CAP HPI, but had failed to update its own website.

In respect of the TV Ad, Carwow provided evidence that its website explained that savings data was calculated as against "*the Manufacturer's [RRP] for the model*". Clearcast also confirmed that Carwow had provided spreadsheet data to substantiate its savings claim, which showed that across 2017, and the first half of 2018, the average amount consumers saved using Carwow was just under £4,000 across 64,927 sales through the website.

The decisions

Regarding the Web Ad, the ASA acknowledged that the RRP had been provided by CAP HPI, and had been stated in error as a result of an old price being listed on the manufacturer's website. However, the ASA did not consider that the price on the manufacturer's website would necessarily represent the price at which the vehicle was generally sold across the market. As the ASA had not seen sufficient evidence to demonstrate that the RRP stated by Carwow did not differ significantly from the price at which the Mondeo was generally sold, the RRP was considered to be misleading and in breach of Cap Code rules 3.1 (Misleading Advertising), 3.8 (Substantiation) and 3.40 (Price comparisons).

Regarding the TV Ad, the ASA acknowledged that the information provided to Clearcast showed that savings made by consumers against manufacturers' RRPs were above the average used in the ad. However, it noted that it had not seen any evidence to show that the RRPs used in calculating the average represented anything other than the manufacturer's selling prices for the vehicles concerned.

As the ASA had not seen sufficient evidence to demonstrate that the RRPs did not differ significantly from the price at which the vehicles were generally sold, the ASA concluded that the average saving of £3,600 quoted had not been substantiated and was misleading. The TV Ad therefore breached the BCAP Code rules (Misleading Advertising), 3.8 (Substantiation) and 3.40 (Price comparisons).

Why is this important?

It is clear from this ruling that, in order for a RRP to be considered substantiated, and not misleading, the ASA expects demonstration of evidence that an RRP does not significantly differ from the price at which a the relevant product is generally sold across the market by other retailers.

In addition, when setting an RRP (and indeed, substantiating savings claims as against an RRP), advertisers cannot solely rely upon the RRP provided or recommended by the manufacturer of a product.

Any practical tips?

The case is clear that manufacturer price lists, and indeed pricing from a manufacturer's own site, is not sufficient to demonstrate that a price used for an RRP is a price "generally" available in the market. Wider market substantiation is required.

Spring 2019

ASA – HFSS

Mondelez ruling: Peter Rabbit promotion not in breach of HFSS ad restrictions

The question

Should a website built for the purposes of redeeming a prize be deemed an 'advertisement' or simply a functional page? If that website is primarily accessible to those over 18, could it still be considered as being directed at children?

The background

A website for a Cadburys Peter Rabbit promotion was viewed in April 2018. The website showed both an image of the licensed character Peter Rabbit, from the film "Peter Rabbit", and text which read "*Chance to WIN a family holiday – Plus 1000 Peter Rabbit (TM) Prizes*". Further text below the image stated that Cadbury "*were pairing up with a special bunny*", and this was accompanied by more images of characters from the movie "Peter Rabbit".

Sustain, the Children's Food Campaign, challenged whether the ad was:

- for HFSS products that were targeted to appeal to children
- directed, through the website, at children with licensed characters popular to children.

The response

Cadburys argued that the website, where those that had found winning coupons inside the promotional packs could redeem their prizes, was solely a practical and functional web page. It should not be considered as an advertisement and therefore should not be subject to the CAP Code. In the event that the website was to be considered as an ad, Cadburys stated that the website address was only advertised on the coupons inside of the winning products. These products were contained in promotional Easter packs, which Cadburys claimed were mainly bought by adults.

Furthermore, Cadburys stated that the web page and the coupons specified that in order to access the prizes, you needed to be over 18 years old. They also stated that they had safeguarded the website by ensuring that the web page would not work if a participant entered a date of birth which was under 18 years old. Cadburys substantiated these claims by showing statistics of the website traffic sorted by age groups, the youngest of these being 18 to 24 years old.

Through these arguments, Cadburys contended that the website was not an ad and, if it was considered to be so, it was not directed to appeal to children.

The decision

The ASA firstly considered whether the website fell within the remit of the code. As the web page gave details on the promotion and how to redeem prizes, and promotions in non-broadcast media are governed by the CAP Code, the website was deemed an ad and therefore subject to the Code. Since there were photographs of the Cadburys products which were all HFSS, the ad was deemed to be an HFSS product ad.

HFSS ads must not be directed at children and, although the webpage included images of Peter Rabbit characters that would be appealing to children, the language used to describe the competition was not focused on children. It was agreed therefore that the ad was not targeted towards under-16s.

Since no medium is appropriate for HFSS ads if more than 25% of those visiting the site are under 16-year olds, the ASA analysed the probable audience. The only way of knowing about the competition was through the details found on coupons in promotional packs which were of interest to adults and children who found winning vouchers. The ASA concluded that, since it was clearly stated on these tickets that the competition was only valid for over 18s, it was likely that less than 25% of users on the website would be children because adults would enter the competition on their behalf. Therefore, it did not breach the Code.

HFSS product ads must also not include licensed characters popular with children if the ads are aimed at young children. Peter Rabbit clearly falls within that category. However, the ASA concluded that, since the wording of the promotion was directed towards adults with “WIN a family holiday,” and the details and logistics of how to enter were set out on the web page, the content was not aimed at young children and did not breach the Code.

Why is this important?

This decision shows that certain promotional materials, even if they contain appealing characters and prizes to children, may not be in breach of CAP Code restrictions on HFSS products if they are very clearly aimed at adults.

Any practical tips?

HFSS ads continue to attract considerable regulatory heat, especially those which include characters appealing to children. If a website or promotion uses such characters but is intended for adults, then make it expressly clear (in words and promotional terms etc) that it really is meant for adults. Couple this with records to evidence adult-level engagement, and you will increase your chances of slipping below CAP’s restrictions on HFSS advertising.

Spring 2019

ASA – HFSS

Cadbury's Freddo advert banned for encouraging children to eat chocolate

The question

When is an HFSS ad aimed at children? And is age-gating enough? Or is it the ad's content which really counts?

The background

Cadbury ran a series of adverts for its Freddo chocolate bar in July 2018 including:

- a poster advert featuring a cartoon image of Freddo the Frog, located at a bus stop close to a primary school
- Cadbury's webpage "www.cadbury.co.uk/freddo" which featured Cadbury branding and images of Cadbury chocolate products.

Cadbury's website required users to enter their details, including a date of birth, and stated users must be over 16. The home page included information about Freddo related activities, downloads and promotions for children. The page included cartoon icons of Freddo which clicked through to a download of a comic book and audiobook, or through to an activities page.

The webpage "www.cadbury.co.uk/freddo" also featured a promotions webpage which could be clicked through to. This page included an over 18 age verification process, and when this was satisfied, linked to a page with images of many Cadbury chocolate products. The page also featured a promotion stating "*WIN BIG ADVENTURES WITH FREDDO & FRIENDS There are 1000s of fun-filled adventures to be won, from Go Ape to Legoland. Have a look at all the amazing prizes here*". To enter, you had to buy any participating chocolate bar and enter the barcode on the back of the package.

Cadbury also ran two YouTube videos on its own channel:

- one titled "*Freddo meet Freddo – UK*" showing a Freddo cartoon interacting with a chocolate biscuit and a caption stating "*NEW Freddo Biscuits are spinning into the biscuit aisle. Crunchy biscuit dipped in delicious milk chocolate… Freddo meet Freddo!*"
- a second video titled "*The Missing Hop*". The video featured Freddo, and a voice-over which stated, "*Deep in the heart of the jungle evil casts a shadow over good, and only one frog can save the day. It's Freddo! He's brave. He's quick. He's a good friend. Freddo*

and the Missing Hop". On-screen text stated "*PARENTS, SEARCH 'MISSING HOP' FOR THE FULL ADVENTURE www.cadbury.co.uk/freddo*".

Two complainants challenged whether the poster, the "www.cadbury.co.uk/freddo" webpage, the promotional webpage, the downloadable comic book and audiobook and the two YouTube videos were ads for products that were high in fat, salt or sugar that were directed at children. They also challenged whether the promotional website linking from "www.cadbury.co.uk/freddo" was an ad for HFSS products which was targeted directly at pre-school and primary-school children, and included a promotional offer.

Cadbury stated the poster was mistakenly placed close to a school due to an error by the owner of the poster site, and this was acknowledged by the owner. Cadbury stated their webpages were corporate websites to provide information about products and promotions, not being aimed at children. Cadbury stated they took steps to ensure children were unable to access the website by requiring age verification.

Cadbury also stated that in the comic book and audio book, no reference to Cadbury branding, Freddo or chocolate products were made. Cadbury said no elements of the YouTube videos were directly targeted at children. For the promotion, Cadbury noted participants had to be 18 or older to be eligible.

The decision

The complaints were upheld in relation to the poster ad, the webpage "www.cadbury.co.uk/freddo", the downloadable comic book and the downloadable audio book only.

The poster ad featured an image of a Freddo chocolate bar, and was located within 100 metres of a school. The ASA therefore concluded that the audience of the ad was significantly skewed towards under-16s. Therefore the ad breached the Code as HFSS product ads are not to be directed at children.

As the Cadbury Freddo website featured a cartoon image of Freddo the Frog, the Cadbury logo and distinct purple background as well as a Freddo-branded activities page, these were likely to be familiar to young children and because branding associated with a mainly HFSS product range, the website was an HFSS product ad. The ASA noted that age gates are not necessarily a deterrent to children and the content was designed to be engaged with by children. The ASA therefore considered it to be directed at children and constituted a breach of the Code.

The promotional webpage was considered an HFSS product ad due to its use of chocolate products. However, the age gate and the tone of the competition instructions, along with the fact that under-18s could not enter, led the ASA to deem that it was aimed at parents and not children.

The audiobook and comic books contained the words ‘Freddo’ and ‘Freddo the Frog’, which were likely to be familiar to children in the context of chocolate. The cartoon image of Freddo was also similar enough to the usual image on the HFSS products so as to be associated with the chocolate bar. Therefore, the books were an HFSS product ad. As children may engage with the books in the presence of, or under the supervision of parents, both were specifically created as content for children under 16 years of age and would be given to children, therefore they breached the Code.

As the YouTube videos used the Cadbury Freddo branding and featured an HFSS product, they were HFSS product ads. The demographic data of Cadbury’s YouTube subscribers was that less than 25% were registered under-18. Whilst users can watch the videos without being logged in or subscribed, the ASA ruled that by taking into account the available data, the ads were not targeted at children.

On the second challenge, whilst some imagery on the promotional page was of HFSS products, the tone used was appealing to adults as well as children and the wording used was directed at adults. It followed that the ad was not deemed to have directly targeted pre-school or primary children.

Why is this important?

This decision provides useful clarity (and lots of examples) of what the ASA will and will not consider to be an HFSS ad targeted at children. For example, the ASA determined that, despite including an age-gate, much of the content on Cadbury’s website was aimed at or designed for children and so still constituted a breach of the Code.

Any practical tips?

Don’t rely on age-gating! Depending on the content, an ad may still be seen to be targeted at children.

From a wider perspective, this decision is a helpful guide for anyone running HFSS ads (marketing teams included), and should help encourage deeper consideration of the light in which they will be seen, who their target audience really is and where they will be run.

Spring 2019

ASA – promotions

Compare the Market: qualifying language in ad too material to be communicated by on-screen text

The question

How prominently do you need to show qualifying language in an ad which is material to the offer in question?

The background

A TV ad was aired in July 2018 which promoted Compare the Market's "2 for 1" meals offer. However, two complaints were received by the ASA that the ad was misleading, as it did not sufficiently communicate the fact that the offer was only redeemable through the Compare the Market app.

The ad itself showed characters sat at a dining table with one of Compare the Market's meerkats stating, "*I'm here to split the bill with you all*". At this time, small text at the bottom of the screen listed information and conditions, including the condition that the offer was app only. Later in the ad, the meerkat stated "*Introducing Meerkat Meals. Get 2 for 1 on food when you buy through Compare the Market*". Concurrently, prominent text at the top of the screen stated "*Meerkat meals. 2 for 1 on starters, mains and desserts*".

The response

Compare the Market gave various reasons as to why the ad sufficiently communicated that the offer was app only. Among these, the company stated that the app only condition was clearly communicated through on-screen superimposed text. For example, the company stated that, with reference to BCAP guidance, the text was held on screen for a suitable amount of time, the text was simple and the font was the correct size.

The decision

The ASA ruled that the ad was likely to mislead, breaching BCAP Code rules 3.1, 3.10 and 3.11. According to the ASA, the fact that the offer was only available through the app was material information which had not been communicated clearly enough. The ASA cited the fact that the material information was not referred to in the voice-over, referenced by any characters or shown in the large on-screen text. Moreover, while "app only" did appear in the small on-screen text while the offer was referred to by the characters at the start of the advert, later in the advert, when the offer was mentioned again, there was no such on-screen text mentioning the limitation.

Why is this important?

The ruling against Compare the Market's ad highlights that it is not always sufficient to mention material information in on-screen text only. In the ruling, the ASA considered that the on-screen message was insufficient compared to the overriding message of the advert, which was created by (among other things) the voice-overs, the characters' speech, the large on-screen writing and the lack of small on-screen writing the second time the offer was mentioned.

Any practical tips?

Keep on your toes! Look out for those conditions which are so material that they need to be included in the main body of the ad, and not just the on-screen text.

Spring 2019

ASA – promotions

Red Bull's wings clipped on health and concentration claim

The question

How did a claim that Red Bull can boost health and concentration fare with the ASA? Does the increased trend towards tighter regulation based on health grounds signal a rough ride ahead for energy drinks companies?

The background

In January this year, following a solitary complaint, a London Underground poster campaign of Red Bull's was banned by the Advertising Standards Authority (**ASA**). In the poster, which allegedly promoted Red Bull's "*National 4pm Finish Day*", the slogan which prompted concern was as follows: "*Because to leap every hurdle a hectic day brings, you just need to know: Red Bull gives you wiiings*". The ASA decided that the ad "*implied that Red Bull could help improve consumers' mental focus, concentration and energy levels, and therefore increase productivity*". Consequently, the poster campaign was banned and Red Bull was told not to imply that its product can boost health and concentration.

The development

The banning of Red Bull's poster campaign follows a trend of increased ad regulation based on health concerns. The most notable of which so far this year has been the ban on junk food advertising across London's public transport network in February, as spearheaded by London Mayor Sadiq Khan.

There are other indications which point towards a crackdown on products such as energy drinks based on health concerns. For example, the sugar tax was introduced in 2018 and the government has also proposed a ban on sales of high-caffeine and high-sugar drinks. In addition to this, many UK supermarkets have banned sales of energy drinks to under-16s. These developments raise the serious question of whether a ban on advertising energy drinks could be on the cards.

Why is this important?

It goes without saying that advertising has a real impact on sales. The energy drinks market is already contracting, with global consumption in 2017 increasing by only 5%, a decrease from previous years. Looking forward, from GlobalData's Soft Market Insights 2018 UK report, it is anticipated that the energy drinks category will suffer a gradual decline in value terms until

2023. With this in mind, curtailing sales or ads for of energy drinks could be a further blow to the bottom line of energy drinks brands.

Any practical tips?

As with any sensitive market, extreme care must be taken with the advertising of any regulated products (from HFSS to gambling to alcohol). The heat attracted by ad complaints can only serve to fuel wider demand for even greater regulation. So all claims, even relatively innocuous claims like Red Bull's "*gives you wiiings*" in the context of overcoming a "*hectic day*", need to be screened extremely carefully.

Spring 2019

Gambling

In-app ads for Tombola Arcade

The question

Were ads in the "I'm A Celebrity, Get Me Out Of Here" app (the **app**) for a tombola arcade inappropriately targeted at under-18s?

The background

The CAP Code states at Rule 16.1 that "*marketing communications for gambling must be socially responsible, with particular regard to the need to protect children, young persons and other vulnerable persons from being harmed or exploited".* Rule 16.3.13 states that marketing communications must not "*be directed at those aged below 18 years … through the selection of media or context in which they appear*". Gambling ads must therefore not deliberately appeal to under-18s more than over-18s.

The complaints

The app displayed ads, including an ad for Tombola (International) plc t/a tombola arcade (**Tombola**). One ad was headed "*PLAY OUR SLOT GAMES*", another said "*Play our scratch card games*" and a third ad alerted users to "*A CHANCE TO WIN A SHARE OF £250,000 FOR FREE CLICK HERE*". The ads included the following: "*tombola arcade proudly sponsors I'm A Celebrity*" and "*begambleaware.org Terms apply. 18+*". By clicking on the ad, the user was taken to the Tombola's website.

The issue was whether the ads were targeted appropriately. Notably, the challenge to the ad came from the ASA themselves (as opposed to a concerned individual or group).

The response

Tombola said that they had reviewed the viewer demographic of the TV show "I'm A Celebrity, Get Me Out Of Here" before they were confirmed as a sponsor. They had found that the 2017 audience comprised over 90% adults who were 18 and over. Tombola pointed out that they had included "*18+*" and "*begambleaware.org*" and used an adult tone in their text; all indicating that Tombola was for adults. The ads also brought the user to a website which again indicated that it was for over-18 users and prevented under-18s from registering to play.

ITV Broadcasting Ltd (**ITV**), publishers of the app, supported this argument, pointing out that the TV show itself was not targeted at under-18s. ITV argued that the purpose of the app was to allow viewers of the programme to interact and engage with the TV show, as the app allowed users to vote, watch trailers and read articles about the show.

The decision

The complaint was upheld.

The ASA made it clear that the CAP Code required marketers to take reasonable steps to minimise exposure of their ads to under-18s. The app itself hosted a range of content relating to the TV show. The ASA considered that the app would only be of interest to those already engaged with the TV show, established to be largely adults. While there was no age profile of the users who downloaded the app, there was no evidence to show that it was predominantly children using it. However, some under-18s would have downloaded the app. Given that fact, the app needed a mechanism to restrict under-18s from viewing the ad, which it did not have. Tombola had therefore not taken sufficient care to select an appropriate media for their ads in order to minimise children's exposure. The ads were therefore in breach of the CAP Code.

Why is this important?

This significant ASA ruling suggests that apps may only host gambling ads if either the app can only be downloaded by over-18s or targeting mechanisms are in place to prevent under-18s from viewing the ad. This ruling was upheld despite the ASA accepting that the app and the associated TV show were not directed at or appealing to children.

Any practical tips?

In Tom Watson's (Labour's deputy leader) words: "*Gambling ads should not be on apps that will clearly be used by kids: It's simple*". His comment reflects the growing concern over the apparent rise in the number of children who are problem gamblers. The message seems clear. If an app is likely to be used by under-18s, unless it's got mechanisms built-in to target ads towards over-18s (or direct them away from under-18s), it is now highly risky to use these types of apps for gambling advertising.

Spring 2019