RPC

Commercial snapshots

Summer 2018

ADVISORY | DISPUTES | TRANSACTIONS

Summer 2018

Commercial cases

Contractual Interpretation - no oral modification clauses

Rock Advertising Limited v MWB Business Exchange Centres limited [2018] UKSC24

The question

Is a no oral modification clause legally effective?

The background

MWB (an operator of serviced offices) provided office space to Rock under a written licence. The licence contained a no oral modification (NOM) clause that stated *"all variations to this Licence must be agreed, set out in writing and signed on behalf of both parties before they take effect"*. Rock (the Licensee) accumulated arrears of licence fees and proposed a revised schedule of payments.

Rock asserted that MWB had orally agreed to vary the licence terms, but MWB considered the revised schedule simply a proposal. MWB then excluded Rock from the premises for failure to pay the arrears and terminated the licence.

MWB issued proceedings for payment of the arrears while Rock counterclaimed for damages and wrongful exclusion. The County Court held that as the variation had not taken place in accordance with the terms of the licence, it was ineffective. Rock appealed successfully to the Court of Appeal which held that the oral agreement to vary the payments was valid and amounted to an agreement to dispense with the NOM clause. MWB then appealed to the Supreme Court.

The decision

The Supreme Court upheld the decision of the trial judge and, although the overall outcome was agreed, Lord Briggs gave a dissenting judgment.

The Supreme Court concluded that the law gave effect to contractual provisions which obliged the parties to follow certain formalities for a variation to the contract to be effective. To have found otherwise would override the intentions of the parties at the time the contract was formed. Lord Sumption (who gave the leading judgment) summarised that NOM clauses:

- prevented attempts to undermine written agreements by more informal means;

- avoided disputes about whether a variation had been intended and about its exact terms; and
- provided a more formal process for recording variations, making it easier to police internal rules restricting the authority to agree to any variations.

Lord Sumption added that estoppel would act as a safeguard against potential injustice. However, he noted that estoppel could not be so broad as to destroy the advantage of certainty provided by contractual terms (including a NOM clause). There would need to be some words or conduct which unequivocally represented that the variation was valid notwithstanding its informality.

Lord Briggs, in his dissenting opinion, envisaged that parties could expressly (or by necessary implication) agree to disapply the NOM clause . However, that line of reasoning no longer appears available (except perhaps as the basis for an estoppel) given the 4-1 majority decision of the Supreme Court.

Why is this important?

If a contract contains an NOM clause, then any oral variation will likely be invalid. In a practical sense this means that the parties must strictly follow the contract formalities in order to be sure that any variation is effective. Typically this will mean a written document signed by both parties, although parties may agree to other terms that set out how the contract may be varied. For example, in larger outsourcing contracts a rigid change control procedure could be agreed that clearly sets out the process and steps that need to be taken in order for the parties to vary the terms of the contract.

Any practical tips?

Make sure any clause that states how a contract can be varied is clear and workable. It is also important to keep in mind the risk profile of the agreement. If relatively small, consider a simpler method for varying the contract. However, larger risk agreements could benefit from a well thought out procedure for varying the contract in order to maintain party certainty. The business should also be made aware of the limits of their power to vary an agreement orally (or not in accordance with agreed procedures).

Commercial cases

Contractual interpretation – express "good faith" clauses

Health & Case Management Limited v Physiotherapy Network Limited [2018] EWHC 869 (QB)

The question

What approach will the courts take in relation to an express "good faith" clause?

The facts

The claimant, Health & Case Management Limited (**HCML**), is a company who referred patients requiring physiotherapy for treatment. The defendant in this matter was Physiotherapy Network Limited (**PNL**), a company which had a UK-wide network of clinics specialising in physiotherapy.

The parties entered into an agreement whereby HCML would refer patients to PNL in exchange for a fee (the **Referral Agreement**). Clause 3.1 of the Referral Agreement stated that HCML would act in good faith to PNL and clause 14.1 included an obligation for both parties to keep all information received from the other confidential.

During 2011, HCML commenced a project to build its own network of physiotherapy clinics under the brand name Innotrex, which became a competitor to PNL. In February 2012, HCML sought an updated list of clinics from PNL, which was to include addresses and contact details (the **Database**). PNL provided the information believing that HCML was developing a geographical pricing model.

Between 2012 and 2014, HCML decreased the number of referrals it made to PNL and eventually stopped referring patients entirely. PNL accused HCML of using the Database to set up Innotrex.

HCML issued proceedings seeking a declaration that it had not acted in breach of contract or confidence; PNL counterclaimed alleging breaches of the same.

The decision

The court concluded that HCML's conduct was in contravention of the express good faith clause and also infringed PNL's database rights. The judge noted:

(a) HCML did not act in breach of confidence as the terms of the confidentiality clause in the Referral Agreement did not restrict HCML from using the information in the Database themselves. The restrictions only prevented HCML from transmitting the information to a third party;
(b) HCML had not acted in breach of contract by failing to make *"circa 700"* referrals per month;
(c) HCML had breached the express good faith clause by incorporating Innotrex, competing with PNL, and obtaining the Database on false pretences with the intention to divert referrals from PNL to Innotrex; and
(d) the good faith clause had been breached by HCML by denying that PNL's database had been used when confronted by PNL. HCML were found to have failed to adhere to the spirit of the Referral Agreement.

The court added that HCML continued to benefit from the commercial relationship which, had PNL been aware of the circumstances, would have been terminated.

Why is this important?

This case illustrates how an express good faith clause can rescue the poor drafting of another clause (i.e. the confidentiality clause). Had the good faith clause not been present, PNL would have been unable to enforce their database rights. This judgment adds to the growing area of database rights, with the court rejecting the defence of consent because the consent was given for an untrue reason.

This case also demonstrates the types of behaviour the courts deem to be good or bad faith and what behaviours will breach an express obligation to act in good faith.

Any practical tips?

Contracting parties should carefully consider the insertion and interpretation of good faith clauses. A well drafted good faith clause could help to bolster any weaker clauses but could also provide another contracting party with a useful backstop where disputes emerge.

Contracting parties should also be careful that their confidentiality provisions are robust and work in their favour to avoid the need to rely on good faith clauses.

Commercial cases

Contractual interpretation – recitals

Blackpool Football Club (Properties) Ltd (Formerly Segesta Ltd) v JSC Baltic International Bank [2018] EWCA Civ 732

The question

What factors will a court consider when interpreting contractual clauses?

The background

Blackpool Football Club (Properties) Ltd (Formerly Segesta Ltd) (**Segesta**) entered into an investment agreement with VB Football Assets (**VBFA**) in 2008 (the **Agreement**). VBFA's rights under the agreement were assigned to JSC Baltic International Bank (**JSC**), who was substituted as the claimant.

Under the Agreement, the parties funded the development of Blackpool Football Club's ground (owned by Segesta). The development's net income would then be divided annually and equally between Segesta and VBFA. To enable phases 1 and 2 of the development, VBFA agreed to loan Segesta £4.75 million and Segesta committed £1 million. In 2010, the club was unexpectedly promoted to the Premier League and Segesta consequently borrowed monies from the club for the third phase of the development. This third phase was to build a hotel, which was operated by a third party, Blackpool Football Club Hotel Ltd (BFC).

In 2011, Segesta paid £181,832 to JSC as its share of 'income'. JSC issued proceedings claiming that (other than for payments for financial years 2009/2010 and 2010/2011) it received no income under the agreement and would have done so had Segesta not incorrectly deducted monies from the income.

The judge held at first instance that the Agreement did not permit: (i) any deduction from income in relation to sums lent to Segesta by BFC; (ii) deduction of losses arising in connection with constructing the hotel; or (iii) sums for notional rent (as the hotel occupied some land owned solely by Segesta) which was outside the scope of the agreement. The decision was then appealed to the Court of Appeal.

The decision

The Court of Appeal agreed with the judge and the appeal was dismissed. Specifically, the Court of Appeal had regard to the relevant recitals and the factual matrix.

Clause 6(A) of the Agreement permitted deductions from the income in certain situations, including *'(i) all items of revenue expenditure (and any expenditure of a capital nature in excess of the amounts provided by the parties pursuant to this agreement) [in relation to the development]'*. The judge concluded:

- in respect of the deductions from income of sums lent to Segesta by BFC, the ordinary meaning of clause 6(A)(i) and the Agreement as a whole did not permit deduction from income of sums lent to Segesta by BFC. Also, clause 19 of the Agreement set out a mechanism for when further funds were required, including a requirement for consent from VBFA. Further, recital (C)(iv) made it clear that the intention of the parties was that the costs of the third phase would "be borrowed from a third party on terms acceptable to the Parties". This was consistent with the finding that the parties did not consider Segesta would contribute over £1million or that BFC would be able to advance funds for that purpose under clause 6(A)(i);
- as the hotel was operated by a separate legal entity, the income and losses of the hotel were those of that entity and were not revenue expenditure in relation to the development. As such, those losses were not entitled to be deducted under clause 6(A)(i); and
- clause 6(A)(i) was only concerned with the actual state of affairs and so despite some of the hotel being built on land outside the scope of the clause, there was no room in the interpretation of the clause for the deduction of notional rent.

Why is this important?

The Court of Appeal reached this decision by interpreting the clause not only using the natural and ordinary meaning of the words of specific clauses in the agreement (more specifically clause 6(A)(i)), but also by considering the clause and agreement as a whole (including the recitals, and specifically recital (C)).

The Court will use all the evidence they have available to reach a decision, and will seek to identify the factual matrix objectively known by the parties on the date that the agreement was executed.

Any practical tips?

Recitals to a contract should be carefully drafted to reflect the purpose and intentions of the parties.

Commercial cases

Damages – "negotiating damages" for breach of contract

Morris-Garner and another v One Step (Support) Ltd [2018] UKSC 20

The question

In what circumstances are "negotiating" (ie *Wrotham Park*) damages available?

The background

The first defendant sold to Mr and Mrs Costelloe 50% of her business which provided support for young people leaving care. One Step was the vehicle company for the transaction. The first defendant had (without the Costelloe's knowledge) incorporated a new company which began competing with One Step.

As part of the transaction, the defendants agreed to be bound for three years by confidentiality, non-compete and non-solicitation covenants in favour of the claimant. Consequently, the claimant brought proceedings against the defendants for alleged breaches of the restrictive covenants. The claimant sought either an account of profits or *Wrotham Park* damages.

The defendants appealed to the Supreme Court. The issues for determination were:

- Where a party is in breach of contract, in what (if any) circumstances is the other party to the contract entitled to seek *Wrotham Park* damages (ie the amount that the parties may have agreed to be paid for the relevant restriction/obligation to be released)?

- Whether the Court of Appeal had been correct to uphold the trial judge's finding that such damages were available in this case.

The decision

The Supreme Court overturned the decision of the Court of Appeal and held that "negotiating damages" (the term the majority preferred to use for *Wrotham Park* damages) were not available to the claimant. The case was remitted back to the High Court for the assessment of the claimant's actual financial loss.

This judgment rejects the proposition that *Wrotham Park* damages are generally available as a type of fall-back claim simply because it provides a fairer outcome and also considers the types of case in which "*negotiating damages*" damages have been awarded.

The judgment identified that negotiating damages could be awarded in the following types of case:

- invasion of rights to tangible movable or immovable property;
- infringement of intellectual property rights;
- damages in substitution for an injunction based on the economic value of the right which the court has refused to enforce; and
- contract cases, but only where the loss suffered is represented by the value of an asset of which the claimant has been deprived, such as the right to control the use of land or intellectual property, or a confidentiality agreement. Lord Reed rejected the proposition that all contractual rights should be regarded as assets. He said instead that this would only be the case where:

  "the contractual right is of such a kind that its breach can result in an identifiable loss equivalent to the economic value of the right, considered as an asset"

Why is this important?

By overturning the decision of the Court of Appeal, this decision limits the scope of *Wrotham Park* or negotiating damages in the context of a breach of contract claim, particularly in respect of non-compete or non-solicitation covenants.

Any practical tips?

Although the availability of "negotiating damages" in the context of breach of contract cases is now limited, such damages are available in intellectual property claims, confidential information cases and other disputes involving property. It is important they are considered when assessing potential damages in these scenarios.

Trade marks

Blocking orders in relation to counterfeit goods

Cartier International AG and others v British Telecommunications plc and another [2018] UKSC 28

The question

Who is liable to pay the costs of implementing a blocking order?

The background

The claimants (entities within the Richemont group, which owns brands such as Cartier and Montblanc) brought a claim against the five major ISPs in the UK after certain websites were selling counterfeit goods infringing the claimants' registered trade marks.

In 2016, the Court of Appeal (confirming the earlier decision of the High Court) held that the defendant ISPs, whilst not guilty of wrongdoing, were inevitably instruments and actors in the infringing activities of websites selling the counterfeit goods. As a result, it was decided that the High Court was entitled to order the ISPs to bear the costs of the implementation of the blocking order.

In reaching this decision, the Court of Appeal relied on European legislation (in particular, the 'InfoSoc Directive' and the 'Enforcement Directive'). The Court of Appeal found that both directives were implicit in deeming it appropriate for intermediaries to bear the costs of implementing the blocking order. One Court of Appeal judge disagreed on this point (Briggs LJ, before joining the Supreme Court). Briggs LJ considered the issue of costs to be a domestic one.

Two of the ISPs appealed to the Supreme Court on the question of who should bear the costs of implementing the website blocking orders. They argued that neither the InfoSoc Directive, nor the Enforcement Directive provided a precedent or binding authority on the issue. The ISPs also argued that there were no CJEU judgments which provided such authority.

The decision

The Supreme Court agreed with the appellant ISPs, concluding that the matter was an issue for domestic English law, provided it was applied within the broad parameters set by the EU (i.e. provided that any remedy is fair, proportionate and not unnecessarily costly).

The Supreme Court held that as a matter of English law, the general rule was that an innocent respondent intermediary ought to be indemnified by the applicant for the costs incurred in implementing the blocking order (unless there was a good reason to order differently).

It was decided that the position was no different from other forms of injunctive relief which required an innocent party to assist a claimant in asserting its rights – such as *Norwich Pharmacal* orders.

The starting point, said the Supreme Court, was the innocence of the ISP. Once it had been established that an ISP was merely a conduit for the infringement, it would not be liable for IP infringement, and there should be no reason for it to bear the costs of remedies which are designed to protect the applicant's rights.

Why is this important?

Whilst giving welcome clarity to ISPs facing blocking orders for websites advertising or selling counterfeit goods, it is notable that this decision diverges from the approach of the courts for website blocking orders regarding copyright infringement (such as illicit streaming).

In copyright claims, it is usual for the ISPs to bear the costs of implementation of the order, whilst the applicant bears the costs of the application.

Any practical tips?

Rights holders should consider whether the overall cost of acquiring the order and paying for its implementation would exceed the benefit the blocking order may bring. ISPs and intermediaries should measure the cost of implementing blocking orders so these costs can be recovered.

Trade marks

Injunctions in the age of digital media

Frank Industries v Nike Retail [2018] EWCA Civ 497

The question

What should be the right scope of an interim injunction where a trade mark is infringed on social media? And how careful do you need to be of using third party trade marks in ad campaigns?

The background

Frank Industries is a ladies' sportswear brand based in Australia. It holds UK and EU trade marks consisting of upper-case letters 'LNDR'. In January 2018, Nike launched its "Nothing beats a Londoner" campaign, in which it used the 'LDNR' sign alongside its famous Nike Swoosh. Frank Industries issued a claim for trade mark infringement under the Trade Marks Act 1994 and the EU Trade Mark Regulation (2017/1001), as well as a claim for passing off. It also applied for an interim injunction to restrain the alleged infringing acts.

At first instance, the Intellectual Property Enterprise Court granted a prohibitory injunction, as well as a mandatory injunction requiring Nike to, within 14 days, "take all reasonable steps to delete the signs LDNR…from social media accounts within its reasonable control" – including Twitter, Instagram and YouTube. The Court directed an expedited trial, and on this basis the duration of the interim injunction was limited to four months. Nike appealed the injunction.

The decision

The Court of Appeal's decision was two-fold.

The prohibitory element of the injunction was upheld. The Court agreed with the analysis that there would be a serious danger of the public associating Frank Industries' goods with Nike's business – potentially causing Frank Industries irreparable harm and loss of goodwill. Conversely, the removal of the 'LDNR' mark would not unreasonably hinder the running of Nike's campaign. The mandatory element of the injunction, on the other hand, was reversed. The Court considered the order to be burdensome, in particular when considering the intricacies and mechanisms of each social media platform:

- YouTube – re-editing the video to remove the marks would entail reposting with a different URL and the loss of millions of comments, links and shares. Nike should instead use

YouTube's facility which allows the infringing sign to be blurred and the rest of the video to remain intact;

- Instagram – deleting posts would result in the disappearance of the whole online conversation and comments. Instead, Nike was ordered to archive existing posts (meaning they would remain in existence, invisible to the public but ready to be resurrected in case of a pro-Nike outcome at trial) and refrain from further posting; and
- Twitter – removal of a post would lead to the loss of the post itself, all likes and re-Tweets and would "deprive Nike of the benefit of the continuing conversations between young Londoners". To delete existing Tweets would have irreversible and far-reaching consequences for Nike. Accordingly, Nike was ordered not to use the mark in future Tweets – but historic Tweets featuring the sign could remain on Nike's Twitter feed.

Why is this important?

In this case, the Court of Appeal had to navigate uncharted legal territory – striking the balance between providing the trade mark owner with adequate injunctive protection until the date of trial, but equally avoiding a detrimental effect to the alleged infringer's social media presence. Most brands today would agree that social media is an extremely powerful weapon in the marketers' arsenal – more than simply a tool for communication, and rather a platform for public discussion and interaction between business and consumer. The Court of Appeal seems to have understood the value of social media and deemed it worthy of protection. In particular, it provided practical and savvy alternatives to the High Court's suggested outright deletion of posts.

Any practical tips?

Though there is now a greater appreciation of the power of social media in the courts, it is still a new and evolving technology. Businesses who engage in social media marketing should be warned that the solutions reached in this fact pattern may not be applied consistently, and a fair balance between the interests of the rights owner and of the alleged infringer may be difficult to achieve in the context of the digital sphere.

This decision also serves as a reminder that the Intellectual Property Enterprise Court, despite being seen as a simpler and more accessible forum, can (and will) impose injunctions – with potentially serious consequences.

Finally, remember the dangers of including third party trade marks in your advertising – whether deliberately or not (noting that Nike used a variation of Frank's 'LNDR', with 'LDNR' instead). Perhaps above all, the case reminds advertisers of the dangers of civil action on digital campaigns – namely the potential of disruption of social media activity, including the possible deletion of long-running feeds and conversations on Twitter, Instagram etc.

Data protection

UK's data retention powers incompatible with EU Law

The question

Are the UK security services' data retention powers compatible with the new privacy regime under EU Law?

The background

The Investigatory Powers Act 2016 (**IPA**) introduced sweeping surveillance powers for UK intelligence agencies and police services, legalising a range of snooping and hacking tools. Two years on, the General Data Protection Regulation (**GDPR**) has brought in an equally sweeping array of privacy rights and sanctions for entities that breach its rules. The GDPR has direct effect as an EU Regulation, and has also been implemented in UK law by the Data Protection Act 2018, putting it into direct conflict with the privacy-limiting provisions of the IPA.

The development

Following a legal challenge by human rights group Liberty (whose campaign has been bankrolled by crowd-funding, raising over £50,000), the High Court has ruled that the IPA is incompatible with European data protection law, and has given the government a 1 November 2018 deadline to re-write its provisions.

The government had previously accepted that some provisions of the IPA were inconsistent with EU law, and had announced that it planned to revise the law by April 2019. However, this ruling has significantly reduced this timeframe and the government will now seek to push through its legislative amendments as soon as possible.

Following the success of their initial campaign, Liberty has announced that it intends to launch further challenges to the provisions of the IPA, including challenging the rules on bulk interception of digital communications. Liberty argues that the ability to intercept communications in bulk and create 'personal datasets' about individuals undermines free speech, privacy and patient confidentiality, legal privilege and journalist's sources.

Why is this important?

This High Court ruling helps to clarify the position regarding personal data and the UK security services in light of the introduction of the GDPR. The court has taken a strong stance in demanding that the government amends the legislation in a shorter timeframe, and highlights that our courts will enforce EU law that contravenes UK domestic law.

The government must now come up with new legislation which seeks to protect the powers of the UK security and police services, whilst complying with wider EU data protection law. While these two aims seem incompatible, it seems unlikely that the government will drop all of the powers brought in under the IPA. Instead, it may be that the government will seek to scale back the IPA by the minimum amount possible in order to satisfy the courts that it is compliant with EU law.

Any practical tips?

Keep watching! The government is now under pressure to come up with a new surveillance law that will comply with EU law. Whilst this will represent a step down from the wide powers currently in force under the IPA, it seems unlikely that it will encompass a complete surrender of its surveillance tools.

This all feeds into the wider Brexit picture of course and whether the UK can benefit from an 'adequacy decision' by the European Commission. Critically, the government's proposal for a special agreement with the EU on data protection has only recently been rejected out of hand by Michel Barnier, the EU's chief Brexit negotiator. If the UK cannot secure an adequacy designation, then we will be a 'third country' from the perspective of data transfers – meaning that there can be no automatic transfer of personal data from the EU to the UK after 30 March 2019. In turn, this could mean inserting model contract clauses into any EU-related contracts which touch on data transfer. Hardly an exciting prospect for the start to 2019…

Data protection

Fine for theft of employer's personal data

The question

Can departing employees be fined for stealing their employer's personal data? Even if the theft is relatively "minor"?

The background

Daniel Short, a former recruitment consultant, left his employment at VetPro Recruitment in October 2017 and set up his own rival business called VetSelect. VetPro heard of Mr Short's new company and had concerns regarding the integrity of the database VetPro used to recruit vets and nurses. This database contained the personal data of over 16,000 people. VetPro subsequently contacted Mr Short to enquire if he had taken information from VetPro's database when leaving its employment. Mr Short confirmed he had taken some personal data, claiming it was for his own "record of achievement". The matter was then reported to the ICO. During its investigation, the ICO discovered that Mr Short had stolen the personal data of 272 individuals from VetPro's database and used these details for his own commercial gain.

The development

Mr Short pleaded guilty before Exeter Magistrates' Court to unlawfully obtaining personal data under section 55 of the Data Protection Act 1998. Mr Short was fined £355, ordered to pay costs of £700 and also ordered to pay a victim surcharge of £35.

Why is this important?

While this case is not of significant financial value and was not heard before one of the higher courts of the land, it demonstrates that both the ICO and the UK courts are willing to prosecute breaches of data protection laws, even for smaller offences. Mike Shaw, Criminal Investigations Manager at the ICO confirmed that "*Data Protection laws are there for a reason and the ICO will continue to take action against those who abuse their position*".

Any practical tips?

Ensure that your data protection policies and procedures are up to date and compliant with data protection law. This case confirms that the ICO is willing to investigate and pursue even the smallest breach of data protection law. Above all, reminding employees (especially departing ones) about the implication of the unauthorised copying of personal data (in particular the criminal implications) may be a neat way of stopping a potential data breach before it even happens.

Data protection

The new data protection fee

Background

From 25 May 2018, as part of the revamp by the General Data Protection Regulation (**GDPR**), the Data Protection (Charges and Information) Regulations 2018 (the **2018 Regulations**) came into force. Amongst other things, these regulations change the way the ICO fund their data protection work.

Under the 2018 Regulations, organisations that determine the purpose for which personal data is processed (controllers) must pay the ICO a data protection fee, unless they are exempt. This new fee replaces the requirement to notify, or register, as was required by the Data Protection Act 1998.

How much does it cost?

The cost of the data protection fee depends on the size and turnover of the relevant controller. There are three tiers of fee ranging from £40 to £2,900. Tier 1 (£40) is for micro organisations – meaning those companies with a maximum turnover of £632,000 per financial year or who have no more than 10 members of staff. Tier 2 (£60) is for small and medium organisations – meaning those with a maximum turnover of £36m per financial year or no more than 250 members of staff. Tier 3 (£2,900) is for large organisations who sit outside Tier 1 or Tier 2.

The fee is always VAT: nil. The data protection fee must be paid every 12 months. Some organisations will only pay £40 regardless of their size and turnover. These are:

- charities;
- small occupational pension schemes; and
- organisations that have been in existence for less than one month.

There is a fee-assessment tool to assist users with how much they need to pay, which is available at: https://ico.org.uk/for-organisations/how-much-will-i-need-to-pay/.

The ICO will publish details of all controllers who pay the data protection fee on the data protection register, which is available on the ICO website. Although the 2018 Regulations came into effect on 25 May 2018, controllers who have a current notification or registration under the Data Protection Act 1998 do not have to pay the new fee until that registration has expired.

Who is exempt?

Not all controllers have to pay a fee, as there are exemptions. There is no requirement to pay a fee if you are processing personal data only for one (or more) or the following purposes:

- staff administration;
- advertising, marketing and public relations;
- accounts and records;
- not-for-profit purposes;
- personal, family or household affairs;
- maintaining a public register;
- judicial functions; and
- processing personal information without an automated system such as a computer.

The ICO provides questions and answers as to whether there is a need to pay the data protection fee. Even if a controller is exempt from paying a fee, they still need to comply with the other data protection obligations.

Why is this important?

The ICO has the power to enforce the 2018 Regulations and to serve monetary penalties on those who refuse to pay their data protection fee, or for those who have not paid the correct fee. The maximum penalty is £4,350 (150% of the top tier fee).

Any practical tips?

First, work out whether your business is exempt from the new data protection fee. Then work out which tier you fall into and when you will need to pay. Remember that if you are liable to pay the fee, this only kicks in once any existing registration under the old Data Protection Act 1998 has expired.

Data protection

Administrator of Facebook fan page held to be data controller

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the presence of Facebook Ireland Ltd (Case C-210/16)

The question

Is the administrator of a fan page on Facebook a "controller" for the purposes of the Data Protection Directive (95/46/EC) (**DPD**)?

The background

A German company that offers education and training services established a Facebook fan page that allowed it to view general analytical information via the 'Facebook insights' tool. In essence, Facebook would gather statistical data regarding the visitors to the company's fan page and would share this anonymised information with the company. The company would also have Facebook place targeted ads on the fan page. Under this arrangement, the company did not receive or collect any personal data; only Facebook was collecting personal information.

However, the company did not alert any of the visitors to its fan page that their personal data would be collected in order to produce the analytical information and advertisements, constituting a breach of the Data Protection Directive. Due to this, the German Data Protection Authority (**DPA**) (the Schleswig-Holstein) ordered the company to deactivate its fan page.

The company subsequently challenged this order in the German courts, making the point that Facebook was in fact the controller of the data, not the company. By virtue of this, they argued that the German DPA could not make an order against them; they should in fact make an order against Facebook (or more specifically, Facebook Ireland). The German courts agreed with the view of the company and characterised Facebook Ireland as the Controller.

The Court then referred the matter to the ECJ for an opinion on whether or not a DPA can make an order against a non-controller.

The decision

The ECJ rejected the very basis of the question, finding that the company was in fact a data controller, jointly responsible for the processing of data with Facebook Ireland. By virtue of being an administrator of the fan page, the company was responsible for determining the

'purposes and means' under which Facebook Ireland would process the data. It was held that even though Facebook operated the platform upon which data was collected, the company was benefitting from the page and accordingly was subject to the obligations of the DPD.

Why is this important?

This ruling makes it clear that the administrator of a fan page hosted on a social media platform can be considered a controller (or joint controller), particularly where the administrator is responsible for deciding the purposes for which data will be processed or if the administrator gains some form of benefit from the collection and processing of the data. More importantly, the ruling emphasises the need for suitable privacy/cookie notices to be in place that set out how the processing will take place.

Any practical tips?

From the perspective of a business using a social media fan page for marketing purposes and which involves the collection of data, the key message is that you will need to make sure that you have communicated appropriate privacy notices. After all, this case was brought due to a regulatory finding that the administrator of the fan page failed to have a privacy notice in place.

Data protection

ICO guidance: "consent is not the silver bullet for GDPR compliance"

The background

In the final run-up to the GDPR coming into force, the ICO produced a blog post reiterating the message that consent is not the "silver bullet" for GDPR compliance. This is the latest in a series of "myth busting" guidance notes produced by the ICO, and focuses on an area which has attracted a huge amount of attention in the media and among organisations generally. The ICO, no doubt in response to a flood of last-minute queries on the topic, chose to single this issue out for final clarification ahead of the 25 May deadline.

The guidance

The ICO reiterated that organisations do not necessarily need to obtain fresh consent from all of their customers in order to comply with GDPR. The key point is that consent is one of six possible lawful bases on which organisations are able to process data, and "*no single basis is 'better' or more important than the others – which one is most appropriate will depend on your purpose and relationship with the individual*".

One of many helpful ICO resources on this point is the "lawful basis interactive guidance tool" which aims to point organisations in the direction of the most appropriate lawful basis for their particular processing activities. This may be consent, but the overriding message from the ICO is that alternatives exist and organisations should consider each of these rather than automatically requiring their customers to provide consent.

Of course, in some instances it will be appropriate to rely on consent, and in those cases it is important to ensure that that consent meets the higher standard required by the GDPR (ie freely given, specific, informed, unambiguous and active). Particular care should be taken if organisations wish to use existing databases which were compiled on the basis of pre-GDPR consent. If that consent meets the (newer, higher) GDPR standard, then organisations can continue to rely on it. Issues arise, however, where that consent does not meet the GDPR standard and organisations attempt to "re-consent" their database. These issues can be avoided entirely if organisations heed the ICO's advice and rely on alternative grounds for processing data, rather than focusing exclusively on consent.

Other useful takeaways from the guidance include:

- if consent under the Privacy and Electronic Communications Regulations 2013 (**PECR**) is required to send a marketing message, then in practice consent will also be the appropriate lawful basis under the GDPR. However, if PECR does not require consent for marketing, the data controller may be able to consider legitimate interests instead;
- consent is also unlikely to be the most appropriate lawful basis for processing if a data controller requires the individual to agree to processing as a condition of service. If so, the most appropriate lawful basis is likely to be "*necessary for the performance of a contract*"; and
- obtaining parental consent for any child under the age of 13 means implementing age-verification measures and making "reasonable efforts" to verify parental responsibility.

Why is this important?

Based on the number of slightly panicky emails that were being sent out at the eleventh hour asking customers to "re-consent" ahead of GDPR, this is clearly a topic that has got organisations of all shapes and sizes worried. This is in many ways understandable – getting consent wrong can be costly, as the fines handed out to Honda, Flybe and Morrisons demonstrate (and much has been said about the increased fines under GDPR, which only serves to increase the pressure on organisations). However, the ICO has repeatedly conveyed a message of reassurance that the GDPR is not intended to hunt out offenders and punish them with astronomical fines, and the latest message on consent follows this trend. The ICO said that "*scaremongering about consent still persists but the headlines often lack context or understanding about all the different lawful bases organisations could use for processing personal information under the GDPR*".

Again, however, getting consent wrong (particularly any attempt to rely on consent that has been obtained as a pre-condition to the provision of a service) can be costly; we can see the ICO recognizing that organisations may not have appreciated that more appropriate alternatives exist which, if relied on, would not have the effect of depriving the individual of genuine ongoing choice and control.

Any practical tips?

If to be relied upon, existing consents should be reviewed to ensure that they meet the GDPR standard. For example, have pre-ticked boxes been used? The regulators have made it clear that now, only an active, opt in tick box will do (similarly, explicit consent must be clearly and expressly confirmed in words). Consent should also be granular, with separate consents matched to separate processing purposes. The right to withdraw consent must be clear in any consent request. Demonstrating consent has been obtained is key to its validity and recording

and documenting the process must be equally granular. Above all, remember that you should ask yourself in the first place whether another lawful basis altogether might be more appropriate

The ICO's practical examples

- A credit card company asks for consent for personal data to be sent to credit reference agencies. However, when an individual withdraws their consent, the company still sends the data to the agencies on the basis of "legitimate interests". Here, there was no real choice for the data subject to begin with. As such, "legitimate interests" should have been used from the start.
- A café provides free wifi, but individuals need to provide their name, email address and phone number, and agree to the café's T&Cs, in order to access the network. Within the T&Cs it states the customer consents to receiving marketing communications from the café. This means consent to direct marketing is a condition of accessing the service. However, collecting the personal data for direct marketing purposes is not necessary to provide the wifi and so this is not valid consent.
- An individual places their business card into a prize draw box in a coffee shop. This act clearly indicates the individual agrees to their name and contact number being processed for the prize draw. However, this consent does not extend to using those details for marketing or another purpose; a different lawful basis would be needed in order to do so.

Data protection

ICO draft guidance: legitimate interests as a lawful basis for processing

The background

The GDPR significantly alters the balance of obligations, responsibilities and liabilities for controllers and processors of data. It mandates that a processor must have a lawful basis for the processing of data. This is not a new concept under GDPR. However, there are some impactful changes, particularly when looking to rely on legitimate interests as the lawful basis upon which a processor intends to process data.

The GDPR also brings in new accountability and transparency requirements, meaning that processors must be able to show that they have a lawful basis for each processing operation, and must inform individuals which lawful basis if being relied upon. Furthermore, under GDPR the interpretation of legitimate interests is now broader, encompassing the interests of any third party, including wider societal benefits.

Legitimate interests is the most flexible lawful basis for processing. However, when choosing to rely on this basis it is important to be aware of the extra responsibilities in considering and protecting people's rights and interests. A legitimate interest can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal interests.

The development

The Information Commissioner's Office (**ICO**) has issued draft guidance to assist organisations in identifying if a legitimate interest is the most appropriate basis, and if so how to ensure compliance with the terms of the GDPR. The ICO confirms its interpretation of the GDPR and provides a general recommended approach to ensure compliance.

Legitimate interests is likely to be the most appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Legitimate interests should be avoided in situations where personal data is being used in a way that data subjects would not understand or reasonably expect.

The ICO outlines that, as per the GDPR, when relying on legitimate interests as a lawful basis for processing, a processor must be able to:

- identify a legitimate interest (Purpose);
- show that the processing is necessary in order to achieve it (Necessity); and
- balance it against the individual interests, rights and freedoms of the data subjects (Balance).

The ICO recommends that if you want to rely on legitimate interests in practice, then a three-part test should be undertaken to establish whether or not this is the most practical and applicable basis; the ICO refers to this as a Legitimate Interests Assessment (LIA). This is a light touch risk assessment based on the context and circumstances of the processing of data. In addition to this, recording the LIA will also help to ensure compliance with accountability obligations under Articles 5(2) and 24.

The test outlines firstly that you identify a purpose for the processing (i.e. what is the legitimate interest). Things to consider include the reason for the processing, such as:

- what is trying to be achieved?
- who benefits?
- what would the impact be if the processing did not go ahead?

Secondly, apply the necessity test. Things to consider here include:

- whether or not the processing actually helps to further the interest?
- is it reasonable?
- is there a less intrusive way to achieve the same result?

Thirdly, you must balance the necessity of processing the data against the impact of the processing on the data subjects. The following should be considered:

- the nature of the relationship with the data subject
- is the data particularly sensitive?
- would it be expected for the data to be used in this way?
- what's the possible impact?
- would a data subject object or find the processing too intrusive?

The ICO further outlines that legitimate interests can be relied upon across a variety of situations, including processing employee or client data, intra-group transfers, marketing activities, B2B contacts, processing of children's personal data (although special care should be taken here) and the disclosure of data to third parties.

Why is this important?

Although legitimate interests is not a new concept under the GDPR, the new requirements for processors are key to using this basis as the lawful basis for processing. Accountability and transparency requirements mean that processors need to be more pro-active when it comes to recording the reliance on legitimate interests as a lawful basis for processing.

Any practical tips?

Organisations must understand and be prepared to justify their legitimate interests as a lawful basis for processing personal data. In order to comply with the GDPR's new obligations regarding transparency and accountability, it is good practice to establish a process that, when followed, documents an organisation's assessment of a legitimate interest.

In addition, remember that you must tell data subjects the purpose for processing their personal data and explain to them the basis for relying upon legitimate interests. Hence why building out your privacy policy is key in order to ensure that your legitimate interests justification is clear on existing processing activities and also why you need to revisit your privacy policy as and when new business activities emerge which also seek to rely on this basis for lawful processing.

Data protection

ICO draft guidance: Data Protection Impact Assessments

The question

When and how should a data controller conduct a Data Protection Impact Assessment (**DPIA**) under the GDPR?

The background

DPIAs are a tool for data controllers to build and demonstrate compliance with the GDPR. The process is designed to encourage organisations to describe and audit their processing activity, consider its proportionality, and balance its necessity against the risks to the rights and freedoms of their data subjects.

Under the GDPR, conducting a DPIA is compulsory in certain circumstances (prior to GDPR, privacy impact assessments were best practice). In brief, an organisation should conduct a DPIA before beginning any type of processing that is "likely to result in a high risk".

The development

The Information Commissioner's Office (**ICO**) has released specific guidance for UK organisations on what DPIAs are, when they need to be carried out, how to carry them out and when to consult with the ICO. The guidance is in draft form and was open to consultation (now closed). Once published, the guidance will replace the ICO's previous Code of Practice on conducting privacy impact assessments.

When should a DPIA be conducted?

The guidance sets out and comments on the three instances in Article 35(3) GDPR when organisations must carry out a DPIA:

1. using systematic and extensive profiling with significant effects;
2. processing special category or criminal offence data on a large scale; or,
3. systematically monitoring publicly accessible places on a large scale.

The ICO says that in this context "extensive" implies that the processing covers a large area, involves a wide range of data or affects a large number of individuals. There will be a "significant" effect where the processing has "a noticeable impact on an individual and can affect their circumstances, behaviour or choices in a significant way". Whether processing is large scale will depend on a number of factors, including the number of individuals concerned,

the volume and variety of the data, and the duration and geographical extent of the processing.

The ICO lists the following types of processing as those it considers likely to be high risk, and therefore requiring a DPIA:

- the use of new technologies – this includes the novel application of existing technologies;
- the use of profiling or special category data to decide on access to services;
- profiling individuals on a large scale;
- processing biometric data;
- processing genetic data;
- matching data or combining datasets from different sources;
- collecting personal data from a source other than the individual without providing them with a privacy notice ("invisible processing"); or
- tracking individuals' location or behaviour.

The ICO also refers to the nine criteria identified by the WP29 in its October 2017 guidance, which may act as indicators of likely high risk processing. In brief, an organisation's processing is likely to result in a high risk to data subjects if it involves:

- evaluation or scoring (including profiling and predicting);
- automated decision making with legal or similar significant effect;
- systematic monitoring;
- processing sensitive data or data of a highly personal nature;
- data processed on a large scale;
- matching or combining data sets;
- data concerning vulnerable data subjects;
- innovative use or new technological or organisational solutions; or
- barriers preventing data subjects from exercising a right or using a service or contract.

As a rule of thumb, the WP29 considers that a processing activity meeting two (or more) of the above criteria will require a DPIA.

The guidance says that to assess the risk of processing, organisations should consider the potential impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. As to whether the risk is high, organisations should consider the likelihood and severity of the possible harm. Note that a significant possibility of very serious harm may be enough to qualify as a high risk. Equally, a high probability of widespread, but more minor, harm might still count as high risk.

In the ICO's view, even if there is no specific indication of likely high risk, it is "good practice to do a DPIA for any major new project involving the use of personal data". The ICO's draft guidance also says that organisations should "think carefully" about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

How should a DPIA be conducted?

The guidance explains that a DPIA should begin early in the life of a project, before processing starts, and should run alongside the planning and development process. It should include the following steps:

- identify the need for a DPIA;
- describe the processing;
- consider consultation with the ICO;
- assess necessity and proportionality;
- identify and assess risks;
- identify measures to mitigate risk;
- sign off and record outcomes;
- integrate outcomes into a plan; and,
- keep the DPIA under review.

The guidance states that it is important to embed DPIAs into organisational processes. A DPIA is not a one-off exercise and should be seen as an ongoing process that is reviewed regularly.

Organisations do not need to send every DPIA to the ICO, but the ICO must be consulted if the DPIA identifies a high risk and the organisation cannot take measures to reduce that risk. Processing cannot begin until the ICO has been consulted.

Finally, the ICO notes that a DPIA is not always required, including where the processing is done on the basis of a legal obligation or public task or where a substantially similar DPIA has already been carried. However, "you need to be confident that you can demonstrate that the nature, scope, context and purposes of the processing are all similar".

Why is this important?

Non-compliance with DPIA requirements under the GDPR (ie, failure to carry out a DPIA when mandatory, carrying out a DPIA incorrectly, or failing to consult the relevant supervisory authority) can result in fines of up to €10m or 2% of total worldwide annual turnover, whichever is higher. And remember that a DPIA-level fine would be additional to the higher level fines (€20m or 4% of global turnover) which could follow the identification of other breaches under the GDPR (i.e. for the underlying cause of a breach itself).

A DPIA can also be a vital piece in documenting processing activities, that will allow an organisation to systematically describe and analyse its intended processing, helping to identify and minimise data protection risks at an early stage. This was reiterated in an ICO blog piece dated 26 March by Ian Deasha, Information Rights Regulatory Development Group Manager. He added that an effective DPIA "could have real benefits down the line in ensuring compliance, building external trust and avoiding the possible reputational and financial implications of enforcement action following a breach".

Any practical tips?

The good news is that, according to the ICO, if you have experience of DPIAs, the new GDPR process will be very familiar. Data controllers should take note of the criteria and steps outlined by the ICO, and build them into the design of its DPIA process. In case of any doubt, the favoured option should be to conduct a DPIA – as ever, when dealing with GDPR compliance, it is better to be safe than sorry and no one will blame you for stress-testing a new data activity with the threat of GDPR-level fines looming overhead. The DPIA might also assist in showing compliance if there are any problems going forward as, in theory, it should provide a systematic record of the assessment and minimisation of the risks.

Organisations should seek the advice of their data protection officer (if they have one) and should also consult with individuals and other stakeholders throughout the process. There is an ICO template that organisations can use if they wish, or you can develop your own.

Data protection

WP29 revised guidelines: personal data breach notification

The question

When should a data controller or processor notify a personal data breach?

The background

The GDPR introduces a mandatory obligation on data controllers to report certain types of personal data breaches to the competent national supervisory authority and the individuals whose personal data has been affected. Data processors must also notify any breach to their controller.

The development

The Article 29 Working Party (WP29) has adopted revised guidelines which are designed to assist controllers and processors in assessing whether it is necessary to notify and to react appropriately when a notifiable breach occurs.

What is a personal data breach?

Article 4(12) of the GDPR defines a personal breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

According to the guidelines, breaches can be categorised as:

- confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data;
- availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and
- integrity breach – where there is an unauthorised or accidental alteration of personal data.

When should a data controller notify a personal data breach?

Article 33 of the GDPR requires that a data controller report a personal data breach to the relevant supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The WP29 considers that a controller can be considered to have become "aware" of a breach when it has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. The revised guidelines clarify that a controller only becomes "aware" of a breach at processor level when the processor notifies the breach to it, as opposed to when the processor becomes aware. However, the revised guidelines also now refer specifically to Article 87 of the GDPR and state this places controllers under an obligation to ensure that that they become "aware of any breaches in a timely manner". This reading of Article 87 therefore places a practical burden on controllers to gear up in terms of technology, staff and internal processes to ensure consistent and effective risk assessment so that breaches can be notified promptly.

The guidelines set out some practical steps that should be taken in all cases:

- information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk;
- risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed;
- notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required; and
- at the same time, the controller should act to contain and recover the breach.

Data controllers should also ensure that they record each breach (as this is an express requirement under Article 35(5) of the GDPR). The WP29 recommends recording the reasoning for decisions taken in response to a breach and clarifies that it will be incumbent on the controller to determine the appropriate period of retention for the breach record(s).

What about data processors?

If a processor becomes aware of a breach, it must notify the controller "without undue delay". The WP29 is clear in its revised guidelines that the processor does not need to assess the likelihood of risk arising from a breach before notifying the controller. It is the controller that must make this assessment on becoming aware of the breach, the controller being deemed to have such awareness as soon as notification is received. Notably, the WP29's original recommendation of immediate notification by the data processor has been reduced in the revised guidelines to prompt notification, reflecting more accurately the GDPR requirement of notification "without undue delay".

What should a notification include?

The guidelines state that the minimum information to be provided in a notification includes:

- the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (DPO) or other contact point where more information can be obtained;
- the likely consequences of the breach; and
- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

When should individuals be notified?

A data controller is required to communicate a personal data breach to the data subject without undue delay when the personal data is likely to result in a high risk to the rights and freedoms of natural persons.

The WP29 says:

- "without undue delay" means “as soon as possible”; and
- a high risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation.

The WP29 identifies the following criteria that should be taken into account when assessing risk:

- the type of breach;
- the nature, sensitivity and volume of personal data;
- ease of identification of individuals;
- severity of consequences for individuals;
- special characteristics of the individual;
- the number of affected individuals; and
- special characteristics of the data controller.

The WP29 says that when notifying individuals, Article 34(2) requires that the controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the DPO or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach.

The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords.

The WP29 recommends that controllers should choose a means that maximises the chance of properly communicating information to all affected individuals. In its view, for example, a notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual.

Why is this important?

If data controllers fail to notify a personal data breach, a fine of up to €10m or up to 2% of global annual turnover can be imposed. In some cases, the failure to notify a breach could reveal either an absence or an inadequacy of security measures and the supervisory authority may also issue a second sanction for the absence of (adequate) security measures (this could be up to €20m or up to 4% of global annual turnover).

Any practical tips?

Where doubt exists as to whether the obligation to notify a breach arises, data controllers should err on the side of caution. Likewise, processors should notify their controllers promptly if a breach is suspected although, as the revised guidelines acknowledge, it is not incumbent upon them to assess the likelihood or degree of risk arising from the breach.

Data controllers and processors should have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. To show compliance with the GDPR it would be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.

Carrying out a Data Protection Impact Assessment should also be considered best practice for ensuring that a personal data breach is unlikely to occur but if it does, that it is understood and acted upon without undue delay, in compliance with the new notification requirements

Online platforms

DCMS report on cyber security for the Internet of Things

The question

What are the risks associated with the Internet of Things and what needs to be done to make the Internet of Things safer for consumers?

The background

While the increasing connectivity via the Internet of Things (**IoT**) is championed by the DCMS as a "fantastic opportunity" for the UK, concerns have been raised over its security. Rapid uptake in devices such as smart thermostats, smart lighting and intelligent speakers paired with the fact that many lack basic cyber security has led to two primary risks being identified:

- consumer security, privacy and safety is being undermined by the vulnerability of individual devices; and
- the wider economy faces an increasing threat of large scale cyber-attacks launched from large volumes of insecure IoT devices.

In the report the DCMS notes that the government must "*ensure that individuals are able to access and benefit from connected technologies safely, confident that adequate security and privacy measures are in place to protect their online activity*". The report advocates a "*secure by design*" approach to consumer IoT security which means that security measures should be embedded in the design process rather than bolted on afterwards. This secure by design approach follows five guiding principles; reducing burden, transparency, measurability, facilitating dialogue and resilience.

The development

This report was commissioned as part of the government's wider National Cyber Security Strategy (outlining the government's cyber security ambition over a five year period). The review upon which this report is based was done in close collaboration with industry and was primarily focused on the development of a "Code of Practice" (**Code**) for those developing, operating and selling IoT services and solutions, including device manufacturers. The Code sets out practical steps to improve the cyber security of consumer IoT products and connected services. It lists 13 points in order of priority for the implementation of the secure by design approach, with the guidance being that the top 3 should be addressed as a matter of priority:

- no default passwords: all IoT device passwords must be unique and not resettable to any universal factory default value;
- implementation of a vulnerability disclosure policy: all companies that provide internet-connect devices and services must provide a public point of contact and ensure that discovered vulnerabilities should be acted on in a timely manner; and
- keeping software updated: all software components should be securely updateable. The need for updates should be made clear to consumers and be easy to implement.

The DCMS notes that the preference of the government would be for the market to solve the issues outlined and for the industry to adopt the "Code of Practice" in order to start making IoT more secure for the consumer. However, if this is not done then the DCMS will look to make the Code compulsory through law.

Why is this important?

The report and subsequent guidelines now expects the producers of IoT devices to build in tougher security measures to negate the risk of cyber security breaches. This will affect device manufacturers, IoT service providers, mobile application developers and retailers. It could signal a significant shift in the way that certain members of the industry develop their IoT products or software. Additionally, while there are currently no published fines or penalties for non-compliance with the Code, it is noted that if the guidance and the Code are not adopted by the industry, the DCMS will push for the Code to be formalised into law, which will result in penalties for non-compliance. The DCMS is also keeping an eye on its international partners in terms of regulations, and will not be worried about bringing the UK into line with those countries that have more stringent regulatory frameworks.

Any practical tips?

Predictably enough, IoT is beginning to attract regulatory attention. The IoT industry as a whole would do well to adopt its own compliance road-map now, rather than wait for the government to start imposing more heavy-handed rules.

Practically speaking, it must make sense for lawyers everywhere to start playing their part in the development of IoT – in particular by sharing these types of developments (eg the DCMS's proposed Code of Practice) with the innovation teams. Understanding where the government's priorities lie (eg via the 13 listed points in the Code) may make a huge difference to the development of IoT devices and wider compliance. This is in addition to ensuring GDPR compliance of course. All in, the lawyer's role in relation to IoT devices is looking increasingly critical…

Online platforms

European Commission Recommendation on illegal content online

The question

What new measures will be required of online hosting service providers in relation to the European Commission Recommendation on measures to effectively tackle illegal content online?

The background

In September 2017, the European Commission adopted a Communication with guidance on the responsibilities of hosting service providers in respect of illegal content online, explaining that the Commission would assess whether additional measures were needed. The Commission has now released a Recommendation 'on measures to effectively tackle illegal content online' following up on their Communication.

The development

The Recommendation published by the European Commission recognises that the presence of illegal content online has 'serious negative consequences for users, for other affected citizens and companies and for society at large'. As such, online 'hosting service providers' (defined in the Recommendation as a provider of information society services consisting of the storage of information provided by the recipient of the services at his or her request) have a responsibility to tackle such illegal content and should be able to take swift action regarding illegal content online.

The Recommendation also states that it relates to all hosting services providers, irrespective of whether they are established in the Union or in a third country, as long as they direct their activities to consumers in the Union. Illegal content is defined as 'any information which is not in compliance with Union law or with the law of Member States'.

Recommended measures to tackle illegal content

The Recommendation states that illegal content online should be tackled with 'effective, appropriate and proportionate measures'. Such measures must also be done in compliance with fundamental rights of all parties concerned, such rights including, amongst others:

- freedom of expression;
- the rights to respect for a person's private life;
- the right to the protection of personal data; and

- the right to effective judicial protection of the users of the relevant services.

As such, decisions by hosting service providers to delete or disable access to online content should take account of the fundamental rights and legitimate interests of their users, alongside the central role that such providers play in 'facilitating public debate and the distribution and reception of facts, opinions and ideas in accordance with the law'. The Recommendation also sets out that it is sufficient to take account of the laws of the Member State in which the service provider is established, or the State in which the services are provided.

Notice-and-action mechanisms

The Recommendation states that provision should be made for mechanisms to submit notices to hosting service providers, which are easy to access and user friendly. Such mechanisms should allow for notices which are sufficiently precise and adequately substantiated to allow the receiving provider to take an informed and diligent decision regarding the notice.

Where content is subsequently removed by a hosting service provider, the provider (where possible) should inform the content provider of that decision and the reasons for taking it (unless it is obvious the content is illegal and relates to serious criminal offences involving a threat to life). The Recommendation also makes provision for a content provider to contest any such decision to remove content by submitting a counter-notice.

Proactive measures

Alongside such notice-and-action mechanisms, hosting service providers should be encouraged to voluntarily take 'appropriate, proportionate and specific proactive measures' regarding illegal content, including using automated means to detect such content. In order to avoid removal of legal content, particularly in the context of automated means, there should be effective and appropriate safeguards to ensure hosting service providers act in a 'diligent and proportionate manner' and that any automated decisions are accurate and well-founded. The Recommendation also encourages cooperation amongst different hosting service providers, and also with 'trusted flaggers' (being entities with particular expertise and responsibilities for tackling illegal content online) to help in the battle against illegal content online.

Terrorism measures

The Recommendation introduces further, specific measures which should be introduced in relation to terrorist-related illegal content online, particularly in relation to dealing with 'referrals' from Member States and competent authorities to take down terrorist related content. Again, the Recommendation encourages hosting service providers to take proportionate and specific proactive measures and to cooperate with other hosting service providers in order to detect, identify and expeditiously remove or disable access to terrorist content.

Reporting

The Recommendation also makes provision that Member States should report to the Commission (preferably every three months) on any referrals submitted by the competent authorities, and the relevant decisions taken by the hosting service providers, alongside information on cooperation with providers regarding tackling terrorist content.

Why is this important?

The Commission's Recommendation sets out a wide suite of proposed measures to tackle illegal content online. These measures place a heavy burden on 'hosting service providers' and will need to be assessed carefully in order to see what actions providers will need to take. The Recommendation does take account of the 'limited resources and expertise' of some hosting service providers, but at the same time still encourages proactive action in tackling illegal content online, and so it is clear that the Commission expects at least some action from all concerned providers.

Any practical tips?

The proposed measures need to be considered carefully in order to assess how they may affect your platform. At the same time, reviewing existing systems and making appropriate changes to proactively tackle illegal content online must be the recommended path, if only to stop harsher regulatory controls coming down the track. Whilst an EU Recommendation is not legally binding, the wide measures and reporting provisions set down in the Recommendation do seem to suggest that a Directive or Regulation regarding the same content matter is likely not far from the Commission's mind. Again, it is better to consider now how these measures may be implemented rather than potentially being pushed even harder to do so later on.

ASA

Advertised delivery restrictions and surcharges: CAP Enforcement Notice

The question

How careful do you need to be about making delivery claims like "Free UK Delivery"? Can you bury additional delivery charges for (say) the Scottish Isles in your T&Cs when making such an absolute claim? (Quick answer = no!)

The background

On 11 April 2018, the Committee of Advertising Practice (**CAP**) issued an Enforcement Notice, providing guidance to online and distance sellers regarding advertised delivery restrictions and surcharges. In particular, CAP issued a warning to advertisers regarding incorrect or misleading absolute "UK Delivery" claims. The Enforcement Notice made it clear that where advertising does not comply with the terms of the notice, targeted enforcement action would be taken in order to ensure a level playing field amongst retailers.

The development

In its Enforcement Notice, CAP provides retailers with a helpful breakdown of the most commonly used delivery claims, and the locational requirements of each claim. This guidance is limited to the presentation of delivery charges and restrictions in advertising, including any such claims on websites and social media pages.

(1) "UK Delivery"

Where a claim is made as to UK Delivery, a retailer should have delivery capability across England, Scotland, Wales and Northern Ireland, including mainland and islands (and the Scottish Highlands). However, this need not include any Crown Dependencies (Guernsey, Jersey and the Isle of Man). Where retailers make claims as to "FREE DELIVERY", "FREE UK DELIVERY" OR "£x UK DELIVERY", their delivery capability should be unqualified, and meet the requirements of UK Delivery as set out above. Further, retailers should ensure UK Delivery claims are only made if the price of the product is same across the UK, regardless of location. It was for this reason that a TV advert for a furniture company which featured the voice-over "*Great brands, anywhere you can get online*" was misleading – because there were size and weight restrictions to some parts of the UK, including the Shetland Islands and non-mainland addresses.

(2) "GB Delivery"

A claim as to GB Delivery will include English, Scottish and Welsh mainland and islands (including the Scottish Highlands), but need not include Northern Ireland or any Crown Dependencies. However, any surcharges or restrictions to excluded areas must be clear and upfront. Specifically, CAP warns retailers against including surcharges/restrictions relating to NI under "international deliveries"; this is considered misleading, as NI is a constituent part of the UK. This is why website claims for "*Free delivery when spending over £200*" and "*Free UK delivery on all orders*" was misleading – because the complainant lived in northern Scotland and incurred a delivery charge of £35.

(3) Mainland UK Delivery

CAP considers "Mainland UK" to constitute "Mainland GB"; it includes areas which are part of the GB landmass, or connected to the landmass by road or rail. To this extent, Mainland UK includes England, Wales, Scotland (including the Scottish Highlands), and land connected to the mainland by bridge (such as Skye or Anglesey). However, it does not include islands accessible by boat or water transport. Again, CAP urges retailers to ensure any surcharges or restrictions are clear and upfront.

Why is this important?

That CAP has issued an Enforcement Notice specifically regarding incorrect or misleading absolute "UK Delivery" claims highlights the emphasis that the ASA will place on this issue moving forward. The clear aim here is to create a level playing field amongst retailers, by tightening up on over-sold delivery claims.

Any practical tips?

Beware making headline claims about "Free UK delivery" etc., at least not without first checking if this really is the case. If there are additional delivery charges to, say, the Scottish Isles, then you will need to qualify the headline claim itself to be clearer on which regions actually fall within the free delivery zone (eg amend to "Free GB delivery"). CAP has been explicit in its Enforcement Notice that restrictions on delivery (eg in T&Cs) cannot contradict the headline claim.

Remember also that if there is a single compulsory delivery charge per item for all customers in the UK, then this delivery charge will need to be included in the price.

ASA

CAP Guidance on 'Compulsory costs and charges: Delivery charges'

The question

How should retailers advertise their delivery charges, in order to comply with the Committee of Advertising Practice's (**CAP**) new guidance?

The background

In an increasingly competitive online marketplace, retailers will often engage in creative marketing to drive sales, including offering consumers varied, discounted or even free delivery options. However, in seeking to differentiate themselves from their competitors through exclusion or limitation of delivery charges, retailers risk breaching the CAP Code and attracting consumer complaints to the ASA, or breaching the Consumer Protection from Unfair Trading Regulations 2008. To assist retailers in their pricing and delivery practices online, CAP has issued guidance as to what is acceptable behaviour and what is likely to mislead consumers.

The development

CAP's guidance falls into four categories:

Applicable charges – per order and per product

The CAP Code requires that the quoted price for a product includes any non-optional taxes, duties, fees or charges that apply. As a result, CAP advises that in the context of online shopping, where delivery charges apply per product (giving the consumer no option but to pay the charges to purchase the product), the charges are by definition "non-optional", and should be included in the stated price of the product.

However, CAP advises that where consumers can reasonably obtain a product via other means without incurring a delivery charge (for example, via a click and collect service), retailers need not include the charges as part of the quoted price, but rather should include the charges as a sufficiently prominent qualification to the price. However, where there are only a limited number of collection points, placing delivery charges in a footnote rather than part of the price, will be looked on "unfavourably" by the ASA.

Where charges apply per order, retailers should make clear that delivery charges will apply and place such charges as a prominent qualification to the price. CAP advises that retailers

may state relevant charges on a separate web page to the product, provided the page is clearly linked or signposted to from the stated price of the product; revealing charges during the checkout or payment process will likely be considered to be misleading consumers.

Calculating charges in advance and delivery locations

CAP understands that in many cases, it may not be possible for retailers to calculate delivery charges in advance; charges may depend upon the size and/or weight of the order, the amount ordered, the consumer's location or other factors not known in advance of the consumer putting together their order. In such circumstances, CAP advises that retailers should make clear that delivery charges are indeed applicable, and provide consumers with clear information as to how applicable charges will be calculated.

Retailers should also be upfront with consumers regarding their delivery capabilities; where delivery is not possible to all locations, retailers should use plain and prominent language to address this. Use of language which implies retailers can deliver to locations outside of their capabilities will be considered misleading. In addition, where a retailer can only deliver certain classes of product to a location, any claim of delivery capability to this location should be appropriately qualified.

Free delivery

CAP advises retailers against offering consumers free delivery, unless there are absolutely no restrictions to this claim, including locational factors, or minimum spend requirements. Therefore, it is not acceptable for a retailer to offer "free delivery", where delivery is only offered to consumers in certain locations, or to consumers who break through a specified spending ceiling. Absolute claims like "*FREE DELIVERY ON ALL ORDERS" or "FREE NEXT DAY DELIVERY ON ALL OF YOUR ORDERS THIS MONTH*" are only likely to be acceptable when there are no restrictions.

Free products and inflated delivery charges

CAP advises that retailers may charge for the un-inflated costs of postage of any free products, but this charge should be provided up front to the consumer. However, CAP draws the line at handling, packaging, packing or administration fees; where a product is described as free, these charges may not apply to the consumer or the offer will be considered misleading. Further, any attempt to understate the reality of delivery charges in order to incentivise a consumer to process a purchase, and make a product more attractive, will be considered misleading; delivery charges should be accurate, and reflect the true cost of delivery.

Why is this important?

It goes without saying that the retail environment is becoming increasingly competitive, and accordingly it becomes increasingly tempting for retailers to run attractive messaging on product delivery. However, misleading or confusing delivery offers will almost certainly come unstuck in the event that they come to the attention of the ASA, whether via consumer complaints or competitor challenges. As such, retailers should take note of this guidance to ensure compliance with the CAP Code.

Any practical tips?

Above all, CAP's guidance underlines the need for online retailers to be as clear and transparent on delivery charges as possible. If in doubt, retailers should put themselves in the shoes of a consumer, and consider the likelihood of consumer confusion in relation to their claims.

Remember also not to get in a muddle about where your delivery services extend to and whether additional charges may apply. In other words, if you say "free UK delivery" you should check whether this includes the whole of the UK (including the Scottish Isles!). See separate Snapshot on CAP: new Enforcement Code on Advertised Delivery Restrictions and Surcharges.

ASA

ASA refers Viagogo to Trading Standards for misleading advertising

The question

How likely is the ASA to impose further sanctions when an entity fails to act upon the ASA's instructions?

The background

In March 2018 the ASA ruled that Viagogo was misleading consumers and that it breached the CAP code by failing to be transparent on its booking fees and delivery charges which were added at the end of the booking process. The ASA found that Viagogo were:

- not making clear the total price at the beginning of the customer journey;
- not including the booking fee (inclusive of VAT) upfront; and
- not making clear the applicable delivery fee.

The ASA "*made clear to Viagogo that if changes were not made we would consider imposing further sanctions*". Viagogo guaranteed that they would make all compulsory fees appropriately clear on its website by 26 May 2018. According to the ASA, Viagogo failed to adequately act upon this.

The development

In reaction to Viagogo's apparent disregard for the ASA's ruling, the ASA referred Viagogo to National Trading Standards. Guy Parker, Chief Executive of the ASA, stated "*Where an advertiser or business is unwilling or unable to follow the advertising rules we will act. In light of Viagogo's inability to get its house in order, we're referring it to National Trading Standards to consider appropriate action*". Unlike the ASA, Trading Standards can impose far more stringent penalties, including direct compliance orders, fines or up to two years imprisonment under the Consumer Protection from Unfair Trading Regulations 2008.

Why is this important?

The main takeaway from the referral is that the ASA is taking a far tougher stance on this type of misleading advertising, particularly with regards to misleading pricing information. Guy Parker's comments also highlight a shift in the approach of the ASA when utilising the sanctions that it possesses.

Another weapon in the ASA's armoury is to issue Ad Alerts against non-compliant advertisers. Essentially, an Ad Alert is a request to media channels not to place adverts for the target advertiser. This could be a big deal for Viagogo, which relies on linking strategies in particular to send customers to its site.

Additionally, the amount of attention this referral picked up in the national press cannot be ignored. Consumers are already wary of secondary ticketing sites and big dollops of negative press might lead to a serious drop off in ticket sales.

Any practical tips?

The ASA rarely refers matters to Trading Standards, but this referral clearly shows that the ASA is not going to hang about if it perceives that it is not being listened to. Any advertisers out there with any repeat breaches on their record would do well to sit up and take note. Trading Standards prosecutions can get very ugly for the companies involved, and possibly also for individual directors who may be (criminally) implicated. If you are in this position (ie with concerns about a potential referral coming your way), consider sharing the ASA's Viagogo press announcement and the accompanying news reports with the appropriate management team in your business.

ASA

ASA: misleading "was" price claim: Victoria Plum

The question

When will a "was" price in a savings claim be considered misleading?

The background

An ad seen on 24 November 2017 for a "Mode Ellis freestanding bath" featured text which scored through the price of £1,299 and showed a "now" price of £379. A voiceover on the ad also stated "... *and now at victoriaplum.com you can save up to 70% off, including this contemporary Ellis bath, only £379*". The advert was seen both on TV and Victoria Plum's YouTube page.

Victorian Plumbing challenged whether the savings claim was misleading and could be substantiated as they believed the product was never sold at £1,299.

In response, Victoria Plum provided sales data for a three-month period (including the sales period), which they believed demonstrated the bath was sold at £1,299 and the saving was therefore not misleading. Clearcast (a non-governmental agency which pre-approves most British television advertising) stated Victoria Plum had confirmed to them that the product was sold at £1,299 and that such confirmation demonstrated the discount was genuine and that the product had been sold at that higher price in significant quantities previously.

The development

Victorian Plumbing's challenge was upheld.

The ASA considered the claim "*was £1,299, now £379*" would lead consumers to believe they were receiving a genuine saving against the price the product was usually sold. The price history given to the ASA by Victoria Plum showed the price of the bath fluctuated in the period leading up to the sales event. The product was sold:

a) initially at £899 for 35 days;
b) at £949 for a further 10 days;
c) at £999 for 12 days; and
d) at £1,299 on 26 October 2017.

The "was" price of £1,299 in the savings claim had been in place for 27 days before the "now" price of £379. However, the lower prices in (a) to (c) above were in place for a total period of 57 days, representing a significantly longer period.

The ASA considered that as the price had fluctuated between four different prices before the sales event, including for the longest period of 35 days at £899, it had not been demonstrated that the higher price of £1,299 was the usual selling price of the bath. As there was no evidence that the savings claim represented a genuine saving against the usual selling price of the product, the savings claim was found to be misleading.

Why is this important?

The ASA's ruling here highlights its pragmatic approach to considering savings claims. The "was" price was in place from 26 October 2017 to when the advert was seen on 24 November 2017, but previous lower prices had been in place for a longer period. As such, the ASA believed it had not been demonstrated that the £1,299 price was the usual selling price of the product. Therefore, even when it could be demonstrated that a "was" price had been used for a significant period before a sales event, the ASA may find a claim misleading if a lower price had been used for a longer period.

Any practical tips?

Avoid using "was" prices where lower prices have been used for a longer period than the "was" price has been in force. If a lower price has been used for a longer period, the ASA is likely to find that the claimed "now" price does not represent a genuine saving against the usual selling price of the product.

ASA

ASA: "was" prices did not represent genuine savings against usual selling prices - Currys

The question

Can "was" prices be used in ads if the prices claimed were used many months before the promotion?

The background

The ASA received two complaints about two ads for DSG Retail Ltd t/a Currys (Currys). Both complaints related to whether the savings claim in each ad was misleading and could be substantiated.

Ad (a) for a 55" LG OLED TV, seen on 26 November 2017, stated a price of "£1,499.00" in large red text, and "save £1,500.00" in black text beneath this. Smaller grey text in the ad stated "was £2,999 (from 19/04/2017 to 29/06/2017)". Ad (b) for a 65" LG OLED TV, seen on 5 January 2018, stated a price of "£2,499.00" in large red text, and "save £500.00" in black text beneath this. Again, smaller grey text in the ad stated "was £2,999.00 (from 27/09/2017 to 28/09/2017)".

Currys stated that the 55" TV was on sale at the higher "was" price for 72 days, and the 65" TV was on sale at the higher price for 35 days (Currys admitted there was an error in the dates displayed for the 65" TV). Currys also said that the "was" price was representative of the market price at the time they applied and that the "was" price and the dates which applied to that price were clearly presented. Currys also stated that their price promotions contained a specific price advantage which existed and was not misleading. Currys provided price history data for the products.

The development

Both complaints were upheld.

The ASA considered that consumers were likely to understand that the claims "save £1,500" and "save £500" would represent genuine savings against the usual selling price of the products at the time the adverts appeared. The ASA considered that many consumers were unlikely to notice the smaller grey text in the ads indicating when the products had been available at the higher prices. Even if consumers did see this information, it was insufficient to alter the impression that the claims represented genuine savings against the usual selling prices of the products at the time the ads appeared.

The Chartered Trading Standards Institute Guidance for Traders on Pricing Practices 2016 states that a reference price is less likely to comply with the applicable rules if it “refer[red] to previous selling prices that were charged many months ago and therefore no longer represent[ed] a genuine indication of the current value of the item”. The 55" TV had not been sold for £2,999.00 for a period of 150 days, while the 65" TV had not been sold for £2,999.00 for a period of 99 days. The ASA considered that, for both TVs, this meant that £2,999.00 was not the usual selling price of the product at the time the ads were seen.

As the "was" prices referred to prices which were charged several months before the promotional prices were available, the savings claims in the ads did not represent genuine savings against the usual selling prices of the TVs and therefore the pricing claims were misleading.

Why is this important?

This ASA ruling highlights that any "was" prices used in a price promotion must represent the usual selling price of the product at the time when the ad is seen. The fact that a product was previously sold at the "was" price is not necessarily conclusive evidence that it is the usual selling price. This is particularly true if the "was" price has not been used for a period of several months.

Any practical tips?

Be sure to check that any "was" price represents the usual selling price of the product at the time the ad is shown. Even if a price has been previously used, this will not represent the usual price if it was used several months ago. This ruling shows that the ASA is unlikely to give much weight to "was" prices which have not been recently used.

ASA

ASA: "our best prices" claim misleading – Sky UK

The question

What does "our best prices" actually mean? Does it mean our best prices for the relevant products at the time the ad appears? Or does it mean our best "ever" prices or our best prices for a "reasonable" amount of time before the offer?

The background

A national press ad for Sky UK Ltd t/a Sky (Sky), seen in October 2017, included text stating "Get Unlimited Broadband At Our Best Prices". BT, believing that the ad implied Sky was offering their best ever prices, challenged whether the claim "Get Unlimited Broadband At Our Best Prices" was misleading and could be substantiated.

Sky stated that the prices offered were the best prices for the products which were being advertised. They said that new or existing Sky TV customers received better prices for the three products than customers who did not have Sky TV. Further, they stated that the ad made clear the "best prices" offer was based on certain conditions such as the customer taking up Sky TV. Sky said the prices were not offered as Sky's "best ever prices" as Sky did not intend to make a comparison against previous prices offered by Sky. If that was what had been intended, then Sky said that it would have included wording to that effect. Sky contended that the average consumer would understand the difference between "best prices" and "best ever prices" and therefore additional wording was unnecessary.

The development

The complaint was upheld.

The ASA noted that the ad did not clarify the basis of the claim "our best prices" and without this information, consumers would understand the claim "our best prices" to mean that the advertised packages were at a lower price than they had been for a reasonable amount of time prior to the offer being available.

The ASA understood that the basis for the lowest price claim was that the packages were cheaper when purchased with TV than when they were purchased alone. The regulator noted that in the previous month Sky had offered the same broadband products at lower prices.

While the ASA acknowledged that the prices offered were the best prices for the relevant products at the time the ad appeared, because the ad suggested that the packages were at a

lower price than they had been recently, but in the previous month Sky had offered the relevant broadband product alone at lower prices, it concluded that the claim "our best prices" was likely to mislead.

Why is this important?

Without further information being included in an ad, the ASA has stated that a claim relating to "our best prices" will mean that the advertised products were at a lower price than they had been for a reasonable amount of time prior to the offer. Therefore, if lower prices were available within a previous "reasonable amount of time", the claim is likely to be found to be misleading.

Any practical tips?

If a claim relating to "our best prices" is intended to be used in an ad, ensure that either: (a) clarifying information is also included in the advert; or (b) that the product was not available for a lower price within a previous "reasonable amount of time". What constitutes a "reasonable" amount of time may be open for interpretation by the ASA, hence it may be safer to include clarification information within the ad to ensure that consumers understand what "our best prices" refers to.

ASA

ASA: omission of promotional T&Cs: prettylittlething

The question

What information must be included in the main body of an advert?

The background

The following adverts and posts were seen on posters, Instagram, Twitter and prettylittlething.com:

(a) a poster advert, seen in three locations between 25 January and 7 February 2018, stated: "*WANT FREE CLOTHES? FOLLOW US ON INSTAGRAM @PRETTYLITTLETHING prettylittlething.com*";
(b) an Instagram advert, presented as an Instastory, featured on Prettylittlething's Instagram account, seen on 1 February 2018, stated: "*SEEN OUR BILLBOARDS? TO ENTER…STEP 1: FOLLOW @PRETTYLITTLETHING STEP 2: COMMENT 'FREE CLOTHES' ON ANY POST!*";
(c) a Tweet, featured on Prettylittlething's Twitter account, seen on 21 February 2018, stated: "WIN £1,000 PLT vouchers find the PLT unicorn on our Instagram, FOLLOW and comment "PLTUnicorn" on the post Instagram.com/prettylittlething"; and
(d) an Instagram ad, presented as an Instastory, featured on Prettylittlething's Instagram account, seen on 21 February 2018, stated "*SPOT THE UNICORN! TO ENTER: Find the PLT unicorn on @Prettylittlething Instagram feed and comment 'PLTunicorn' MAKE SURE YOU'RE FOLLOWING PLT TOO!*".

The ASA received five complaints challenging whether, by omitting the terms and conditions from the adverts, these adverts were misleading.

Prettylittlething stated that for adverts (a) and (b), this was a limited time promotion from 2 January to 30 February 2018 and the idea was to take consumers on a "journey" from seeing the poster advert to its Instagram account, which would feature the Instagram story with the prize details. The Instagram story was later amended so that the terms and conditions could be found by swiping up from the story. The terms and conditions were also available on prettylittlething's Facebook page. Regarding adverts (c) and (d), prettylittlething informed the ASA that this was a time limited competition from 19 February to 28 February, and the terms and conditions could be found on the relevant Instagram story. Prettylittlething stated that in the future, the Instagram story would include a link to the full terms.

The development

The complaints were upheld.

The CAP code states that all marketing communications or materials referring to promotions need to communicate "*all applicable significant conditions or information*", and the omission of such conditions or information is likely to mislead. While the ASA welcomed prettylittlething's move to link to the terms and conditions in the Instagram stories in the future, and adverts (b) and (d) were later amended, none of the adverts had referenced or provided links to the terms and conditions at the point when they were seen by the complainants. This means that the complainants were unable to retain or easily access the terms prior to entering the promotions. The ASA further considered that more significant conditions such as the closing date and any applicable age restrictions should have been included in the main advert in both online and offline formats, rather than linking to such conditions.

Advert (a) did not include any detailed information about how to enter the prize draw without undertaking several steps. Further, consumers were unlikely to be aware of the applicable age restrictions as the information was not included in the adverts. Additionally, no closing dates were given. These conditions were significant conditions which were likely to influence consumers' understanding of the promotion and their decision whether to enter. Therefore, because the adverts did not include all the significant terms and conditions relating to the promotions, they had breached the CAP code.

Why is this important?

This ruling highlights that even if the terms and conditions are available at some point in an advert (eg by swiping up on the Instagram story), or are later added to an advert, certain significant conditions must still be present in the main body. Any terms and conditions which are likely to influence consumers' understanding of the promotion or their decision as to whether to enter it should be presented in the main body of the advert, otherwise the advert may be likely to be in breach of the CAP code.

Any practical tips?

Assess any prize promotions to consider what terms and conditions are likely to be "significant" in light of the CAP code, and ensure that such information is included in the main body of the advert. Further, include a link or a method of accessing the full set of terms and conditions somewhere in the advert at all times. If your marketing team push back on you, you could do worse than sharing this ASA adjudication with them!

ASA

ASA: blind taste test not misleading - Bulmers

The question

What information do you need to include in a comparative ad to support your claim? Can you round up figures to the nearest percentage if you make this clear in the small text?

The background

A September 2017 magazine ad for Bulmers Cider released by Heineken UK Ltd t/a Bulmers (Heineken) stated "2/3 of drinkers prefer the taste of Bulmers Original to Magners Original". The small text of the advert stated "SOURCE: Cardinal. 65.8% in a head to head blind taste test, surveyed in Nottingham and London June 2017. Excludes those who expressed no preference. Sample size: 146 regular apple cider drinkers".

The ASA received two complaints challenging whether the claim that two thirds of drinkers prefer Bulmers Original to Magners Original was misleading and could not be substantiated. Heineken stated that the claim was based on a study undertaken by Cardinal Research and argued that the sample size was robust and as such supported the extrapolated conclusion that two-thirds of drinkers preferred Bulmers Original to Magners Original.

The development

The complaints were not upheld by the ASA.

The ASA judged that the ad made clear the number of people surveyed and that readers were likely to realise the '2/3' claim was based on the 146 people surveyed, and not all drinkers. The ASA did note that 65.8% was 0.9% less than the equivalent percentage of two-thirds, but the fact that the unrounded figure had been provided in the small text meant that consumers were unlikely to be misled by the gap between the figures.

Heineken provided a copy of the study methodology to the ASA, which indicated the number, gender and age category of the participants in the study. The methodology also explained that the proportion of male and female participants in the two age categories (18-34 and 35+) were weighted in accordance with Kantar Worldpanel Alcovision data in order to ensure that the sample was weighted to give a representative sample of cider drinkers. The ASA took expert advice on the methodology and considered that for such a market research survey, the sample used by Heineken reasonably matched the Kantar data and as such was sufficiently representative of the cider drinking population. The ASA also concluded that the sample

population was large enough for sufficiently sensitive results to show that around two-thirds of people preferred the taste of Bulmers Original to Magners Original.

Considering the above, the ASA considered that the sample size and methodology were adequate to substantiate the claim "2/3 of drinkers prefer the taste of Bulmers Original to Magners Original" and therefore the ad was not misleading.

Why is this important?

For companies considering launching a comparative advertising campaign, this ASA ruling provides useful guidance to help ensure that such an ad does not fall foul of the CAP Code. The ruling helps clarify what information must be included to support a claim, and also what the ASA will consider to be a 'reasonable' study in order to substantiate such a claim.

The discussion of the discrepancy between 65.8% and the percentage representation of two-thirds also indicates that the ASA is willing to take a pragmatic approach to such discrepancies, provided the small text draws attention to the true number.

Any practical tips?

Comparative claims are ripe for attack from consumers, competitors and statisticians (!) alike. Ensuring robust evidence and methodology is behind a comparative study is critical in order to substantiate the data, noting that a copy of the methodology and details of any studies may be needed for passing to the ASA to defend a complaint. The small text of the ad must also include enough information to inform a consumer about the number of study participants, the conditions of any test, and any other material information. Finally, even if there is only a slight difference between any figure claimed in an ad and the true figure, ensure that the small text includes the actual figure.

ASA

ASA: "studio-quality" camera claim not misleading - Apple

The question

What factors will the ASA consider when assessing statements made in ads? And what meaning will be given to industry standard terms when used in a different market context?

The background

For the release of its new flagship mobile device (iPhone X), Apple ran a television advert which stated: "Radically new cameras with Portrait Lighting. Studio-quality portraits. Without the studio. See portraits in a whole new light".

Two complainants challenged the advert on the basis that promising customers a "studio-quality" camera experience was misleading and could not be substantiated.

Apple stated that "studio-quality" lacked a clear industry standard meaning. They submitted that across the photography industry there are wide variances between equipment, techniques, lighting and talent. As such, they argued the term should be subjectively interpreted.

Apple further stated that the iPhone X had multiple camera features (in both the hardware and software) which reflected studio equipment and effects, for example:

- the Portrait Lighting feature enables users to create lighting effects and compose images such as those seen in studio images, such as images with a strong depth of field effect; and
- the 50 mm focal lens in the iPhone X is one of the most popular lens choices for professional studio portrait photographers.

Supporting this position, Clearcast reiterated that "studio-quality" was not an official or measurable term. In their assessment, the images were a fair reflection of the camera's capabilities.

The development

The ASA found in favour of Apple and concluded that the advert was not misleading.

In reaching this decision they considered how a customer would interpret the featured text "studio-quality portraits" when presented alongside the video demonstrations in the advert. In this context, the ASA determined that customers would interpret that the phone's lighting effects would enable customers to imitate a portrait image taken in a studio environment.

The ASA recognised that the camera lens on the iPhone X (50 mm focal lens) was a piece of equipment that commonly features in studio photography. Also, they noted that the images shown in the advert were a true reflection of the phone's capabilities.

Why is this important?

This decision reinforces that statements given in advertisements should not be considered in isolation. Instead, they must be considered in the entire context in which the customer will interpret the statements. Here, this included video demonstrations in the advert which supplemented the meaning of "studio quality".

The decision also indicates that common industry terms may be given different or diluted meanings when placed in a different market context. For instance, "studio quality" in the professional photography industry can be interpreted differently as to when the phrase is used in the context of the mobile telephone market.

Any practical tips?

Advertisers need to carefully consider the context of any featured text or statements. In particular they should consider how an ordinary customer may interpret any claims made and whether these claims can be factually substantiated.

Particular care must be taken when using phrases with industry standard undertones. Any advert falsely claiming industry standard features without the requisite substantiation may well result in a breach of the CAP Code.

ASA

CAP consults on harmful gender stereotypes

The review

The Committee of Advertising Practice (**CAP**) has launched a public consultation on a new rule to tackle harmful gender stereotypes in advertising, as well as guidance to advertisers on how the new rule should be interpreted in practice. The consultation proposes to introduce the following new rule to cover both broadcast and non-broadcast media: "*Advertisements must not include gender stereotypes that are likely to cause harm, or serious or widespread offence*".

Background

The consultation comes after the Advertising Standards Authority (**ASA**) published a report entitled '*Depictions, Perceptions and Harm*' last year that provided an evidence based case for stronger regulation of advertisements that feature certain kinds of gender stereotypical roles and characteristics. The types of advertisements targeted are those that have the potential to cause harm by contributing to the restriction of people's choices, aspirations and opportunities, which may impact the way people interact with each other and the way they view their own potential.

Rules are already in force in relation to offence and social responsibility to ban advertisements that include gender stereotypes on the grounds of objectification, sexualisation and unhealthily thin body images.

Terms of reference

The proposed new rule seeks to identify specific harms that should be prevented, rather than banning gender stereotypes outright. The guidance provided in support of the new rule provides examples of scenarios likely to be problematic in future advertisements. Examples include:

- an advert that depicts a man with his feet up and family members creating a mess around the home while a woman is solely responsible for cleaning up the mess;
- an advertisement that depicts a man or a woman failing to achieve a task specifically because of their gender eg a man's inability to change nappies; a woman's inability to park a car;
- an advertisement that seeks to emphasise the contrast between a boy's stereotypical personality (eg daring) with a girl's stereotypical personality (eg caring) needs to be handled with care; and

- an advertisement that belittles a man for carrying out stereotypically "female" roles or tasks.

The consultation closes on 26 July 2018.

Why is this important?

The project lead at CAP, Ella Smillie explained: "*Our review of the evidence strongly indicates that particular forms of gender stereotypes in advertisements can contribute to harm for adults and children by limiting how people see themselves and how others see them and the life decisions they take. The set of standards we're proposing aims to tackle harmful gender stereotypes in ads while ensuring that creative freedom expressed within the rules continues to be protected*".

Any practical tips?

If you see any type of gender stereotyping in copy or artwork for an advert, put the brakes on – if only to give yourself a chance to reflect on the potential implications of the messaging. Even ahead of the outcome of the consultation, you need to be sure you're not breaching existing restrictions in this area, or worse, alienating your customers.

ASA

CAP announces 12 month review of rules on advertising HFSS products

The review

The Committee of Advertising Practice (**CAP**) has announced the terms of reference for its review of the rules introduced in 2017 on the advertising of food and soft drinks high in fat, salt and sugar (**HFSS**) in non-broadcast media.

Background

CAP's original HFSS rules were announced in December 2016 and came into force in July 2017. The rules ban the inclusion of HFSS product advertising in children's media and other media where children make up 25% or more of the audience. The rules cover non-broadcast media environments, such as social media and TV-like services online and even extend to poster sites located near schools. The rules also ban HFSS product adverts that target younger children by including licensed characters and celebrities that are popular with children.

The rules were introduced following extensive consultation with the public health community, the advertising industry and other key stakeholder groups in response to the concerns around children's diets and the change in media habits brought about by the growth of online environments.

CAP took the decision to bring its non-broadcast media rules into line with the Broadcast Committee of Advertising Practice (**BCAP**) rules for TV advertising, despite the fact that evidence suggests that advertising is likely to have no more than a modest direct effect on children's immediate food preferences.

Terms of reference

The review will begin on 1 July 2018, one year after CAP's original HFSS rules came into force, with the aim of conclusions being published in the autumn.

The review will assess:

- compliance with the new rules by advertisers;
- the success of regulators in amending or removing advertising in breach of the rules; and
- the impact, both economic and otherwise, of the rules on children's media and advertising.

The review will specifically include:

- monitoring and assessment of media environments popular with children;
- enforcement work to address identified problems;
- analysis of Advertising Standards Authority (**ASA**) complaints data, rulings and enforcement actions;
- analysis of ASA and Ofcom enforcement activity in relation to TV advertising for HFSS products, in order to determine the implications for non-broadcast advertising;
- an invitation for and analysis of stakeholder submissions on the effectiveness of the rules; and
- an invitation for and analysis of submissions from media owners and advertisers on the economic impact of the rules with specific reference to the impact assessment published in CAP's public consultation document.

Why is this important?

It's clear that governments are increasingly targeting advertising of HFSS products as part of their wider battle against the impact of obesity on society. For example, recently the Scottish Government has called for a ban of advertising HFSS products on TV before the watershed. Many argue that this is a heavy-handed way of dealing with one aspect of the wider obesity problem, and could drastically impact on the media spend of some of the biggest advertisers in the country. There are also wider repercussions for the media channels themselves (eg digital platforms). Many are set up to put restrictions around, eg alcohol and betting adverts, but spotting HFSS products is much harder. HFSS product advertising is quickly becoming one of the hottest topics in the advertising arena.

Any practical tips?

Identifying brand advertising that has the effect of promoting an HFSS product is not always easy. The ASA has provided a toolkit to assist with identifying whether the content described would likely be regarded as a HFSS product advertisement. The toolkit, which includes various sources, is available at: https://www.asa.org.uk/news/hfss-toolkit.html.

Tower Bridge House
St Katharine's Way
London E1W 1AA
T +44 20 3060 6000

Temple Circus
Temple Way
Bristol BS1 6LW
T +44 20 3060 6000

11/F Three Exchange Square
8 Connaught Place
Central Hong Kong
T +852 2216 7000

12 Marina Boulevard
#38-04 Marina Bay Financial Centre Tower 3
Singapore 018982
T +65 6422 3000

26604850