Summer 2019

Contents

12. Gambling

Commercial

Consultation on Distributed Ledger Technologies, Cryptoassets, and Smart Contracts

The question

What is the legal status of cryptoassets and smart contracts?

Key takeaway

New government consultation asks whether and which type of "*property*" cryptoassets would be categorized as, and whether a smart contract can give rise to legally binding obligations.

The background

The UK Jurisdiction Taskforce (**UKJT**) on 9 May 2019 launched a consultation paper regarding Distributed Ledger Technologies, cryptoassets, and smart contracts. The paper primarily discusses the current legal and investor uncertainty surrounding the use of cryptoassets and smart contracts. This uncertainty is argued to be hindering the development of the technologies and it is hoped that a legal statement made by the UKJT can increase investor and user confidence in the products and promote English law for these technologies.

The development

The legal status of cryptoassets

The crucial issue surrounding the cryptoasset is whether it will be deemed as "*property*" under English law. As the consultation paper states "*if a cryptoasset is not property, it cannot be owned. If it cannot be owned, it cannot be purchased, sold, otherwise transferred in law or rights to it asserted if it is stolen*". As a result the legal classification and concept of a cryptoasset is very important to its future use and investment prospects.

Currently, English law recognises choses in possession, which are physical things, and choses in action, which are legal rights as property. The following question that the consultation asks is if a cryptoasset is acknowledged as a property, will it be a chose in possession or action or another type of property? In order to regulate the law concerning transfers of cryptoassets, cryptoassets must be distinguished and classified under English law.

The legal certainty of smart contracts

The current concerns in relation to smart contracts are whether, like a traditional written contract, they are capable of giving rise to binding legal obligations. The UKJT state that, "*mainstream investors still need to be convinced that their legal rights can be protected when they … enter into smart contracts*".

The UKJT is conscious though that there are some parties who enter into smart contracts specifically because of the lack of legal framework which enforces rights. Therefore, if smart contracts are deemed to give rise to binding legal obligations, it will be crucial for the parties to the smart contract to be conscious of the situations which could lead to these obligations. This raises the following secondary questions:

- How would an English court apply general principles of contractual interpretation to a smart contract written wholly or in part in computer code?
- Would an English court look beyond the mere outcome of the running of any computer code that is part of a smart contract in determining the agreement between the parties?
- Would a smart contract between anonymous parties give rise to binding legal obligations?
- Would there be a statutory requirement for a signature?
- Would a smart contract fulfil an "*in writing*" requirement?

Why is this important?

The consultation addresses key issues concerning the use of smart contracts and cryptoassets and will assist the UKJT to release an authoritative legal statement which "*will either demonstrate that English private law already provides sufficiently certain foundations in relation to the relevant issues, or will highlight particular areas of uncertainty that may be ripe for further clarificatory steps to be taken*".

Any practical tips?

Keep watching! Future announcements and publications issued by the Government on these topics should clarify the legal status of cryptoassets and smart contracts. To the extent existing principles of English law do not address all of the necessary matters, specific legislation to embrace its new technologies will be needed.

Summer 2019

Commercial – fraudulent misrepresentation and non-party losses

BV Nederlandse Industrie Van Eiprodukten v Rembrandt Enterprises, Inc [2019] EWCA Civ 596

The question

What are the requirements for fraudulent misrepresentation? Can a non-party supplier claim loss of profit under a terminated contract?

Key takeaway

The case provides guidance on factual statements made to induce the other party to enter into an agreement and the limited circumstances in which a third party's loss can be recovered.

The facts

Rembrandt Enterprises, Inc (**Rembrandt**) was a supplier of egg products. It contracted with a supplier in the Netherlands, BV Nederlandse Industrie van Eiprodukten (**NIVE**), to supply dried egg powder. The contract was conditional on US regulatory approvals; when these were obtained a price increase was negotiated to cover the regulatory costs.

Subsequently, NIVE informed Rembrandt that its sister company, Henningsen van den Burg (**Henningsen**) would be providing about 50% of the dry egg powder.

Rembrandt alleged NIVE was failing to comply with US inspection requirements and suspended Rembrandt's performance of the contract. NIVE then began proceedings for loss of profits on the sales that would have occurred but for suspension of performance. The claim for loss of profit was on the total amount to be supplied, including the product to be supplied by Henningsen.

Rembrandt argued NIVE had breached a contractual warranty as the product did not comply with US regulations, and that the price renegotiation had been procured by NIVE's fraudulent misrepresentation as the increased price included both the additional costs of complying with US regulations and an additional element of profit.

The decision

The High Court

The judge held that:

- the product supplied by NIVE did comply with US regulation, so there was no breach of warranty
- however, the increased sale price included an element of profit and therefore NIVE's representations in emails to Rembrandt were false representations deliberately made
- it was for NIVE to prove the increased price would have been agreed without the fraudulent misrepresentation, and it could not do so
- Rembrandt was entitled to rescind the second contract, however, that then revived the original contract (without the price increase)
- even under the original contract, the judge held that NIVE could not claim for the loss on the product supplied by Henningsen.

The Court of Appeal

The appeal was dismissed. The key points from the judgment are as follows:

- it was for the representee (Rembrandt) to prove it had been materially "*influenced*" by the fraudulent misrepresentations; it did not need to prove that it would not have entered into the contract but for the misrepresentation
- there was a presumption that a statement which is likely to induce a representee to enter a contract did so induce it – it was for NIVE to rebut that presumption
- NIVE contended it had always intended to use Henningsen to meet its contractual commitments, but it had not communicated this to Rembrandt. Rembrandt had agreed to accept some supplies from Henningsen, but Henningsen had no contractual rights against Rembrandt
- as Rembrandt was not even aware of Henningsen at the time of contracting, the claim for transferred loss failed.

Why is this important?

The decision confirms the presumption of inducement is only factual, but it is "*very difficult to rebut*". The other party must also only show it had been materially influenced by the representation.

The decision confirms that a party to a contract can claim for a third party's losses resulting from a breach, as an exception to the usual rule, only if at the time the underlying contract was made there was a common intention to benefit the third party (or a class of persons to which the third party belonged).

Any practical tips?

Parties should be careful making factual statements that are to be relied upon to enter into agreements – the price negotiation was a new agreement.

If a group company (or third party) is to have a right of recovery (directly or indirectly), include specific drafting to cover such situations (eg through indemnities, amended third party rights provisions, etc).

Summer 2019

Commercial – good faith

Alan Bates & Ors v Post Office Ltd (No 3) [2019] EWHC 606 (QB)

The question

Which characteristics will the court consider when deciding whether a contract is "*relational*" and therefore subject to an implied duty of good faith?

Key takeaways

As the English courts' approach to contractual good faith continues to evolve, the court's (non-exhaustive) list of relational contract characteristics should be borne in mind whilst drafting in order to ensure that implied good faith obligations are appropriately included in or excluded from the contract.

The background

Over several years, approximately 550 sub-postmasters (the **Sub-Postmasters**), who were responsible for running Post Office Branches, entered into either the Sub Postmasters Contract (**SPMC**) (pre-2011) or the Network Transformation Contract (**NTC**) (post-2011) with the Post Office. The SPMC stated that the sub-postmaster was responsible for all losses caused through his own (or his assistants') negligence, carelessness or error. The NTC stated that the sub-postmaster should be fully liable for any loss however such loss occurred and whether it occurred as a result of any negligence by the sub-postmaster, his personnel or otherwise. Both the SPMC and the NTC required the sub-postmaster to pay any shortfall in full.

In 2000, the Post Office introduced, and required the Sub-Masters to use, an electronic accounting system (Horizon) in all branches. Over time, Horizon identified various unexplained shortfalls and accounting errors.

The Post Office maintained that, subject to the SPMC and NTC, individual sub-postmasters were liable and had to prove that shortfalls were not their individual responsibility. The Sub-Postmasters maintained that software defects in Horizon and unsatisfactory training caused the shortfalls and discrepancies. Nevertheless, some Sub-Postmasters paid the (disputed) shortfalls, some Sub-Postmasters' contracts were terminated and other Sub-Postmasters even received criminal convictions.

The Sub-Postmasters brought claims as a group action for financial loss, personal injury, deceit, duress, unconscionable dealing, harassment and unjust enrichment. The Post Office

denied allegations that the Horizon software was defective and raised various contractual defences.

The decision

Although various contractual construction issues were considered, one particular question of wider interest was whether the SPMC and NTC were "*relational*" contracts. The court confirmed that it is the commercial context that decides whether a contract is "*relational*" and provided a (non-exhaustive) list of characteristics that should be taken into account when deciding whether a contract is relational. These characteristics include:

- that there are no express terms preventing a duty of good faith being implied (this being the only determinative characteristic)
- there is a mutual intention that the contract and relationship are long-term
- the parties intend their roles to be performed with integrity and fidelity to their bargain
- the parties are committed to collaboration
- the spirits and objectives of the venture is incapable of exhaustive expression in a written contract
- the parties place trust and confidence in one another (but a different kind to that involved in fiduciary relationships)
- the contract relies on a high degree of communication, co-operation and predictability based on mutual trust, confidence, and loyalty
- one or both parties have invested to a significant degree
- the relationship is exclusive.

To the contrary, the court confirmed that other factors, such as an imbalance of bargaining power, bad behaviour or unfairness of certain terms, were not relevant in determining whether a contract is relational.

The court concluded that, where it is in accordance with the presumed intentions of the parties, a general duty of good faith is implied in "*relational*" contracts. The court clarified that the obligations implied are good faith, fair dealing, transparency, co-operation, trust and confidence. This involves more than a requirement to act honestly; it is an obligation to refrain from conduct which would be regarded, by reasonable and honest people, as commercially unacceptable when taking into account the circumstances of the relationship as defined by the terms of the agreement in its commercial context. However, the court did accept that the implied duty of good faith could be expressly excluded, even where the contract had all the other characteristics and signs of a "*relational*" contract.

In this case, taking into account factors such as the significant personal financial commitment of the Sub-Postmasters, similarities of the SPMC and NTC with employment contracts, and the inherent relationship of trust between the Post Office, the Sub-Postmasters and the public,

the court was satisfied that the contracts were relational. On this basis the Court ordered that 17 of the 21 possible implied terms were to be implied into the SPMC and NTC.

Why is this important?

Although the courts have previously been reluctant to imply a general obligation of good faith in the absence of express wording, this decision (along with the decisions in *Yam Seng Pte Ltd v International Trade Corp Ltd* and *Bristol Groundschool Ltd v Intelligent Data Capture Ltd*) suggests that (some) courts will accept the concept of the relational contract as a basis to imply a duty of good faith (although the determination will turn on the facts in each case). This is likely to be considered by the Court of Appeal (and, perhaps the Supreme Court in due course).

Any practical tips

A contracting party should decide whether or not it is in its best interests for the contract to be subject to a duty of good faith. Generally, the position should be expressly set out in the contract to avoid later uncertainty as to whether the contract was intended to be relational and therefore subject to implied good faith obligations. If it is intended for the contract to be subject to good faith obligations, it is preferable to have express terms stating the specific steps/conduct that each party is required to take. This avoids future uncertainty as to the scope of each party's obligations.

Summer 2019

Commercial – third party rights

Chudley & Ors v Clydesdale Bank Plc (t/a Yorkshire Bank) [2019] EWCA Civ 344

The questions

Can third parties that are not easily identifiable benefit from the Contracts (Rights of Third Parties) Act 1998?

Key takeaway

Courts are adopting a more flexible approach when determining the scope of third parties that are able to benefit from contract pursuant to the Contracts (Rights of Third Parties) Act 1999 (the **Act**). Careful consideration should be given to the third party classes that could potentially be caught by the wording of the contract.

The background

Four investors (the **Investors**) paid money to Arck LLP (**Arck**) to invest in Paradise Beach, a property investment scheme in Cape Verde.

Arck, by way of a letter of instruction (**LOI**), instructed Yorkshire Bank (the **Bank**) to open a segregated client account for the scheme and to use the monies only on certain terms; which included not using the monies without a solicitors' undertaking that the monies would be repaid. However, a segregated account was never opened; instead the money was paid into another account held by Arck and, without any undertaking being given, the money was paid out to Paradise Beach. Ultimately, Paradise Beach failed to repay the agreed return on the investments by the redemption date.

When the Investors later became aware of the existence of the LOI and the fact that their monies had been paid out without an undertaking, they sought to recoup their losses from the Bank by way of damages. This was on the basis that the LOI contained a contract between Arck and the Bank and therefore the Investors were third parties entitled to claim the benefit under the Act.

In particular, the Investors relied upon s1(1)(b) and s1(3) of the Act; that a third party can enforce a contractual term that purports to confer a benefit on them if they are identified in the contract by name or as a member of a class or description. Here the investors argued that reference to "*a client account*" in the LOI was sufficient to identify a class.

The Investors' claim was unsuccessful in the High Court as the first instance judge determined that i) there had been no binding and unconditional contract (a condition precedent had not been satisfied); and ii) although the Bank would have been in breach of contract, there was insufficient evidence that the breach caused the Investors to lose their monies.

Nevertheless, the High Court did accept that **if** there had been a binding contract, then the Investors would have been entitled to the benefit of that contract on the basis of the LOI wording and (it was irrelevant that the Investors were not aware of the LOI at the time that it came into existence).

The decision

The Court of Appeal considered three questions.

1. The Court of Appeal found that there was insufficient evidence to suggest that the LOI was subject to a condition precedent and therefore a binding contract **did** exist between the Bank and Arck.
2. Looking at the construction of the LOI as a whole, the Court of Appeal accepted that reference to "*a client account*" was sufficient to identify a class of which the Investors were members and to confer an enforceable benefit on them. The Court went further, adding that there is a presumption of enforceability of third party rights under the Act and the burden is on the contracting parties to show that that they did not intend the third party to have the right to enforce the term; any doubts as to the parties' intentions will be resolved in the third party's favour.
3. The Court of Appeal found that the Investors had suffered a loss, that being payment of their monies without the proper undertaking. The Court clarified that it was not necessary for the Investors to demonstrate what would have been done with their monies if the breach had not occurred. As such, the Investors were entitled to damages.

Why is this important?

This case demonstrates that the broad scope of duties owed to third parties (even to those that are not identified either by name or within the master contractual document). The Court of Appeal adopted a flexible approach when determining classes identified in the contract and discarded the requirement for counterfactual evidence to be put forward to demonstrate the loss of the third parties.

Any practical tips

When drafting contracts it is important that consideration is given to any potential obligations that may arise in respect of third parties. Care should be taken not to include wording that **could** unintentionally be interpreted to reference a particular class or third party description. The inclusion of an express term excluding third party rights should be considered in all relevant documents.

Summer 2019

IP – Part 36 offers

Invista Textiles (UK) Ltd & Anor v Botes & Ors [2019] EWHC 58

The question

When can the court not apply the cost consequences of Part 36 offers

Key takeaway

In a recent High Court decision it has been held that parties must ensure that Part 36 offers are "*genuine offers to settle*" as the court will not order costs in circumstances where it is unjust to do so. Furthermore, the decision reinforces the significant weight that is given to whether or not an offeree accepts a Part 36 offer, regardless of whether relief is obtained by the offeree in the first instance.

The background

The claimants, *Invista Textiles UK Ltd & Anor* (**Invista**), are part of one of the world's largest textile groups – specifically making polymers, chemical intermediates and fibres including nylon. Most notably, Invista is known for the brand LYCRA.

Between March and October 2016, a number of employees within Invista's Sustainability Group (the **Defendants**) gave notice of their resignations and, shortly after, set up a new venture. In February 2017, Invista issued proceedings against the Defendants after discovering various files relating to the new venture on a Defendant's work computer. The proceedings were based on allegations of breach of contract or breach of equitable obligations, predominantly in relation to misuse of confidential information and inducing a third party breach of contact.

Main proceedings

In January 2019, Birss J handed down judgment in favour of the Defendants. In his judgment, Birss J considered various issues related to the employment agreements, including, but not limited to, the following:

- **Misuse of confidential information** – the wording of the confidentiality obligations was too wide to be enforceable against a former employee.
- **Non-compete clauses** – the non-compete clause, which was for three-months, was an unreasonable restraint of trade as it was not linked to any genuine need to preserve confidential information.

- **Non-solicitation** – one of the Defendants had breached their non-solicitation clause by seeking to recruit the other Defendants to their new business during the non-solicitation period.

In summary, Birss J held that the contractual position went far beyond what was necessary to protect Invista's legitimate interests and handed down judgment in favour of the Defendants.

Costs proceedings and Part 36 offer

Invista obtained limited relief at first instance against the Defendants as a result of the breach of the non-solicitation provisions, however Birss J held that the "*real winners*" were the Defendants as the predominant claim for misuse of confidence was "*dismissed altogether*" .

In assessing overall costs, Birss J was obliged to take into account a Part 36 offer made by Invista in June 2018. The Part 36 offer requested that the Defendants "*agree to the delivery up or deletion of documents in a schedule*" and pay Invista's costs on the standard basis. As a brief reminder, Part 36 offers are a tactical procedural step aimed at encouraging parties to settle a dispute pre-trial and are designed to "*put the cost risk on the offeree if they fail to accept the offer*".

Following the first costs judgment, Birss J held that Invista had in fact obtained "*a more advantageous position in terms of the relief actually sought*" despite the value being "*inherently unquantifiable*" .However, Birss J analysed the Part 36 offer by Invista as really being "*an admission of defeat*" as Invista's case was far wider than the forensic deletion of documents as it included serious allegations of breach of confidence and misuse of confidential information.

The decision

Ultimately, the Part 36 offer was an offer which the Defendants could not accept as they "*would have to pay all the costs to the case up to that date*", not just the costs relating to documents. As a result, Birss J concluded that it would be "*unjust*" to enforce the consequences of the Part 36 offer as:

> *"…the Part 36 offer itself was not a genuine offer to settle. In fact, if anything, I think the offer has* ***proved to be a barrier to settlement*** *of this dispute because since the offer was made and not accepted and then the admissions were made, the claimants seem to have been approaching this case as if they were entirely protected as to costs."*

Birss J concluded that Invista should pay 71% of the Defendants' costs assessed on a standard basis. The 29% reduction in the percentage of costs awarded was to take into account that Invista had limited success in relation to documents in the main proceedings.

Why is this important?

This case provides a useful reminder of the importance of Part 36 offers in settlement negotiations and the potential costs consequences associated with these offers. Regardless of whether a party has obtained relief, there continues to be significant weight given to whether or not the offeree accepted the Part 36 offer.

Any practical tips

Parties must ensure that all Part 36 offers are a genuine offer to settle and that the court will not order costs where it considers it unjust to do so, for example where a Part 36 offer is a barrier to settlement.

In addition, this case highlights how it may be difficult for an employer to impose restrictions on former employees post-termination. Companies may therefore wish to review their non-compete clauses in employment contracts and obtain advice as to whether any revisions are necessary.

Summer 2019

Data protection

Pensions company fined for unsolicited emails following inaccurate advice

The question

How far can you avoid culpability for a data marketing data breach on the grounds that you were given faulty legal advice or that a third party conducted the marketing campaign on your behalf?

Key takeaway

Even if you have sought out legal and professional advice in order to comply with regulations (which later proves to be inaccurate), you may still be subject to an adverse decision by the ICO. In a data breach scenario, you will still be liable even if the infringing actions were conducted by third parties on your behalf.

The background

Grove Pension Solutions Ltd, a pensions company in Kent, sent nearly two million direct marketing emails without consent between 31 October 2016 and 31 October 2017. The company had instructed a marketing agent to use third party email providers to carry out hosted marketing campaigns.

The pensions company had sought independent legal advice as well as professional advice from a data protection consultancy about the use of hosted marketing. The company acted on the inaccurate advice it received, leading to the action by the ICO.

The ICO's decision

The fact that the company had sought professional advice, which was inaccurate, did not prevent the ICO from issuing a £40,000 fine. The ICO's Director of Investigations and Intelligence, Andy White, said:

"We acknowledge that Grove Pension Solutions Ltd took steps to check that their marketing activity was within the law, but received misleading advice. However, ultimately, they are responsible for ensuring they comply with the law and they were in breach of it".

Moreover, Mr White added that the ICO is available to provide businesses with guidance about electronic marketing and data protection, free of charge. He stated that the company could have contacted the ICO for guidance to avoid the fine.

Why is this important?

This decision is important for two reasons. First, it shows that obtaining erroneous legal or other professional advice for the purpose of navigating electronic marketing and data protection rules will not render you immune to an adverse finding by the ICO. Secondly, the ICO's decision clarifies that the rule that organisations cannot generally send marketing emails unless recipients have given consent applies equally to those situations where an organisation uses a third party to send direct marketing on its behalf.

Any practical tips?

Ensure that you instruct reputable firms for legal advice in relation to electronic marketing and data protection regulations. And don't think that using a third party provider to conduct a marketing campaign on your behalf will somehow excuse you if that campaign is somehow conducted in breach of data regulation.

Summer 2019

Data protection

PPI claims company fined £120,000 by the ICO for spam texts

The question

Will a data controller be held responsible where a third party acting on its behalf breaches data privacy laws?

Key takeaway

This recent ICO decision underlines what we all know – that data controllers need to ensure that they receive informed consent from consumers before using their personal data for electronic direct marketing purposes and that the buck stops with them when it comes to ensuring compliance. Pointing at failings by third parties won't get you off the hook.

The background

Hall and Hanley Ltd (**H&H**) is a PPI claims management company based in Manchester. Between 1 January 2018 and 26 June 2018, it engaged third parties (the **Third Parties**) to send direct marketing text messages on its behalf. In total, 3,560,211 such messages were sent by the Third Parties over the period.

The ICO received a total of 1,353 complaints about the messages sent on behalf of H&H. The complaints stated that the messages had been sent unsolicited and without the recipients' consent. In many cases the recipients had never had PPI insurance.

The ICO sent an initial investigation letter to H&H on 12 July 2018, questioning whether H&H's practices were compliant with the Data Protection Act (**DPA**) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**).

H&H responded that it used the Third Parties to (a) obtain the data or consent of the individuals to whom it intended to advertise its products and (b) send the direct marketing messages. The ICO reviewed the privacy policies of the four websites which the Third Parties used to obtain the relevant data. Two of the websites made no reference to H&H. The other two did include H&H; however, potential subscribers were not given an option to select which third parties were allowed to contact them or their preferred method of contact.

The decision

The ICO found that H&H had contravened regulation 22 of PECR and imposed a monetary penalty of £120,000. Regulation 22 prevents any person or company from transmitting or

instigating the transmission of unsolicited electronic direct marketing communications without the recipient's prior consent. Although H&H had not sent the messages itself, it was the instigator of the direct marketing. As such, it had a responsibility to ensure that valid (direct or indirect) consent to send those messages had been obtained.

The ICO's guidance states that indirect consent will only be valid if it is sufficiently clear and specific, so that the customer anticipates that the relevant organisation will have access to their details and be able to message them. None of the four websites used by the Third Parties were sufficiently clear and specific that H&H would be able to contact them. This satisfied the ICO that H&H did not have the necessary valid consent for the 3,560,211 direct marketing messages which were sent to customers of the websites used by the Third Parties on its behalf.

Why is this important?

This decision emphasises that the ICO will proactively clamp down on organisations which intrude on consumers' privacy. What is particularly interesting in this example is that two of the four websites used by the Third Parties to obtain data used in the direct marketing messages actually included H&H in their privacy policies. However, the ICO confirmed that consent will not be valid where individuals are not properly informed as to what they are consenting to. The monetary penalty notice explained that consent will not be valid where individuals are asked to agree to marketing using generic terms like "*selected third parties*" or a "*long, seemingly exhaustive list of general categories of organisations*". It will also not be valid where a privacy policy fails to provide any information or choice on the method of contact the different companies they listed might use.

The ICO held that H&H did not deliberately contravene regulation 22 of PECR. Instead, it found that H&H acted negligently and failed to take reasonable steps to prevent the Third Parties from contravening regulation 22. The case highlights why data controllers must properly scrutinise any third parties they engage to act on their behalf.

Any practical tips?

This decision demonstrates the vital importance of obtaining informed consent before using consumers' contact details for electronic direct marketing purposes. Data controllers should also verify the methods used by any third parties they engage on their behalf, as the H&H decision shows that they will ultimately be held responsible for any deficiencies in the third parties' conduct. So, in addition to ensuring that the right data processing agreements are in place, make sure practical steps (such as due diligence into third parties, actively audits etc) etc) are taken. Passing the buck just won't wash!

Summer 2019

Data protection

HMRC issued enforcement notice by ICO for use of biometric data

The question

When is consent sufficient for collecting, processing and using biometric data?

The key takeaway

If you collect, use or process biometric data, you must have the *explicit* consent of those individuals concerned. If you are considering setting up a scheme whereby biometric data is used (eg for customer ID verification), you should conduct a full analysis of the data protection rules applicable to the proposed scheme and plan how your scheme will comply. Such methods of compliance include: letting individuals know that they do not have to sign up to services; explaining how they can decline to take part; clarifying to such customers that they will not suffer any detrimental impact ;and completing a Data Protection Impact Assessment (**DPIA**).

The background

HMRC uses voice authentication, a form of biometric data, for caller verification on some of its helplines. Biometric data is special category data under the GDPR and, therefore, requires a higher level of consent for its collection, use and processing.

However, HMRC failed to obtain adequate consent from individuals as required. This is because individuals were not given the opportunity to give or withhold consent. This also meant that HMRC did not have individuals' explicit consent, which is required as a result of the fact that the information was special category data. Furthermore, HMRC had not provided adequate information to the individuals, meaning that any consent they did give was not sufficient.

The decision

In reaching its decision, the ICO took into account the imbalance of power between HMRC and the individuals affected, especially the individuals who might rely on HMRC in relation to benefit claims. Also relevant to the ICO's finding was the sheer number of people affected by this data issue.

To become compliant with data protection regulation, HMRC was required to delete (and oblige its suppliers to delete) all biometric data held under the Voice ID system for which explicit consent had not been obtained.

Why is this important?

Since the GDPR's introduction, this is the first enforcement action which confirms that biometric data is special category data.

Any practical tips?

Beware all systems offering biometric data processing – or rather tread with care, and carry out a Data Protection Impact Assessment for sure. The latter should flush out potential issues and ways to practically address them.

See also the "*key takeaway*" section in the HMRC decision, as this lists example methods of compliance. The blog by the Deputy Commissioner for Policy at the ICO, "*Using biometric data in a fair, transparent and accountable manner*", is also useful.

Summer 2019

Data protection

ICO: Age Appropriate Design Code for information society services

The question

What steps does the Information Commissioner's Office (**ICO**) require to ensure adequate protection of children online?

Key takeaway

The ICO has released a new draft Code outlining 16 standards that will greatly impact online service providers (ie almost all online businesses) in how they deal with child data. Failing to comply with the Code will make it extremely hard to demonstrate compliance with the GDPR.

The background

The ICO drafted the Age Appropriate Design Code (the **Code**) to provide standards and guidance for what is expected of information society services (**ISS**) that process personal data and are also likely to be accessed by children under 18. This is in line with the ICO's obligations under the Data Protection Act 2018 (section 123) which required the preparation of a code of practice addressing these issues. The Code is due to be finalized by the end of this year and needs to be approved by Parliament before final publication.

The scope

The Code will apply to ISS, defined as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".

This definition is wide enough to include apps, programs, search engines, social media platforms, online messaging services, online marketplaces, streaming services, online games, news and educational websites, and any websites offering other goods or services to users over the internet. Note that the ICO has confirmed that "*remuneration*" in the definition includes both services funded by advertising and services provided to end users free of charge.

Most online service providers are captured within the definition and they will need to review how they are processing personal data to check for compliance with the Code even if their services are not aimed at children. Essentially, the Code applies if children under 18 are likely to use the service.

The standards

There are 16 standards outlined in the Code. To be compliant, all of the standards must be implemented. Some brief examples of the standards and practical guidance provided are as follows:

- age-appropriate application: consideration must be given to the age range of the audience as well as the needs of children at different ages and stages of their development. The standards of the Code will apply to all users unless there is a robust age-verification mechanism in place to distinguish children from adults. Self-declaration of age or age range on its own will not amount to a robust age-verification mechanism
- profiling: profiling options must be off by default unless, with consideration to a child's best interests, a compelling reason can demonstrate otherwise. Profiling may be allowed if appropriate measures are in place to protect children from any harmful effects, like having privacy settings with options specific to different types of profiling that are switched on by the child
- nudge techniques: nudge techniques cannot be used to lead or encourage children to provide unnecessary personal data, turn off privacy protections, or extend use. There are many different nudge techniques used by ISS. Under the new standards, the only exceptions to allow any use of nudges is for high privacy options, wellbeing enhancing behaviours, or parental controls and involvement.

Why is this important?

Aside from the clear importance of children's personal data and privacy, the Code will require major changes by ISS to their website design and operations to ensure compliance. The consequences of regulatory action include assessment notices, warnings, and of course GDPR level fines. The ICO is likely to take more severe action in cases of harm or potential harm to children than other types of personal data.

Any practical tips?

The definition of ISS catches a huge swathe of online businesses. They should all start conducting internal reviews to assess the impact of the Code. Any failure to comply with the Code will make it extremely difficult to show compliance with the GDPR and the Privacy and Electronic Communications Regulations. When it comes to breaches concerning children in particular, that could provide extremely costly.

Summer 2019

Data protection

Pre-ticked boxes and cookies consents: Planet49

The questions

Is unticking a box sufficient to meet the consent requirements for the installation of cookies? Separately, can you agree to sharing your data with third parties in order to gain entry to a prize draw?

Key takeaways

Unticking a pre-ticked box is not sufficient to demonstrate consent for the use of cookies. Consent must be given actively and separately to any underlying activity. On data-sharing, the case opens up the possibility of trading data for, say, entry into a prize draw if the processing is necessary for participants.

The background

In 2018 the Bundesverband der Verbraucherzentralen (a German federation of consumer organisations) initiated proceedings against an online lottery provider. They alleged breach of German consumer laws implementing the e-Privacy Directive and the General Data Protection Regulation (**GDPR**).

The defendant, Planet49 GmbH, ran its prize promotion on www.meinmacbook.de. In order to enter, participants were required to provide their postcode, name and address. Above the entry button there were two tick boxes.

The first box was not pre-ticked. It asked participants to consent to sponsors and co-operating partners contacting them via post, email and SMS. Entrants needed to tick this box in order to be able to be registered for the competition.

The second box was pre-ticked. It asked entrants to agree to the installation of cookies, which would monitor users' surfing and use behaviour on the websites of advertising partners.

The case centred on whether the consent provided by the second tick box was sufficient for third party processing and the installation of cookies under the e-Privacy Directive and the GDPR. It reached the Bundesgerichtshof (Germany's highest court) and certain elements were referred to the CJEU for guidance.

The decision

The second tick box (agreement to loading of cookies)

Advocate General Szpunar's opinion considered the concept of consent under Directive 95/46/EC (95 Directive) and the GDPR. Consent has to be given actively. It needs to be demonstrated in a separate action, not merely as part of the activity the user is taking part in. The user also has to be fully informed about what they are consenting to. The concept of consent is the same under the e-Privacy regulation as under the GDPR.

The Advocate General found that there was no valid consent in relation to the second tick box. He reached this conclusion on the following basis:

- if the user clicked the participate button, they would be entered into the competition and agree to the cookies in the same click (given that the box was pre-ticked). This meant that it wasn't a separate action
- if the user left the box ticked, it wasn't clear that they had given their free and informed consent, as they hadn't done so actively
- there was no information indicating that the second tick box was optional for entrance to the prize draw, so a user's consent would not have been fully informed.

The Advocate General stated that it didn't make a difference whether the information was personal data for the purposes of Article 5(3); it was clear that stored data on the user's terminal equipment had a privacy aspect to it.

He explained that the "*clear and comprehensive information*" that must be made available (according to Article 5(3)) should allow a user to understand the implications and effect of giving their consent. The user must be told how the cookies function, their duration and which third parties (if any) have access.

The first tick box (agreement to be contacted by third parties)

The Advocate General also considered the validity of consent under the first tick box. He questioned whether a tick box was sufficiently "*separate*" to demonstrate consent and stated that a button would have been preferable.

He also discussed Article 7(4) of the GDPR in relation to the first tick box. Under this provision, companies should not make the user's entry into the contract conditional on consent to processing if the processing is not necessary. Interestingly, the Advocate General considered that third party processing may be necessary for a free prize draw, as users essentially provide their data for the company to sell, in exchange for entry to the prize draw. The user's acceptance of third-party processing is their main obligation. However, the Advocate General said it was ultimately a decision for the German courts to assess.

Why is this important?

Whilst Article 5(3) of the e-Privacy Directive doesn't necessarily apply to all cookies (eg it may not apply to authentication and session-id cookies), this decision provides clear guidance on practices that internet service providers should avoid.

The analysis of consent under the 95 Directive, GDPR and e-Privacy Directive is helpful. It will be interesting to see whether consent for cookies is treated similarly under the forthcoming e-Privacy Regulation, or whether the concept develops further complexity.

Any practical tips?

Avoid using pre-ticked boxes! Care should also be taken to ensure that the explanations provided with tick boxes are clear and explain the function of any cookies, their duration and any third-party access in a way that can be understood by a user without any technical background.

As to trading data for sharing with third parties in exchange for entry into a prize draw, that positon remains unresolved. The Advocate General indicated that, in his view at least, companies could consider whether they have grounds to argue it is necessary for the relevant activity (ie participation in a prize draw). For now, the answer must be to think very carefully before going down this route. What is clear is that when it comes to valid consent, pre-ticked boxes generally spell trouble.

Summer 2019

Data protection

European Data Protection Board issue guidelines on contractual processing for online services

The question

When is it appropriate for Information Society Services (**ISSs**) to process personal data on the basis that it is "*necessary for the performance of a contract*"?

Key takeaway

ISSs must take into account whether the specific contract cannot be performed without the processing – solely stipulating a provision in a contract will not satisfy Article 6(1)(b).

The background

Article 6(1)(b) of the GDPR states that one of the lawful basis for the processing of personal data is when "*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*".

The European Data Protection Board (**EDPB**) has published draft guidelines (which are subject to consultation) setting out when ISSs can rely on Article 6(1)(b). The guidelines both clarify and (in some areas) replace the previous Article 29 Working Party Guidelines on this subject.

The guidelines refer to ISSs as both services, which are normally remunerated for by the consumer, but also services, which are financed through advertising. The EDPB recognises that its opinion on the "*validity of contracts…is outside [of its] competence*", but otherwise provides advice on the analysis and applicability of the Article.

The development

Analysis of Article 6(1)(b)

- **Article 6(1)(b) with the context of the GDPR**
  Article 5(1)(a) of the GDPR states that "*personal data must be processed lawfully, fairly and transparently in relation to the data subject*". In the context of contracts for online services, complying with Article 5(1)(a) means abiding by the relevant contract law; the guidelines give the example that the "*Unfair Contract Terms Directive*" could be applicable for a consumer contract. In addition, both Articles 5(1)(b) and (c) (purpose limitation and data minimization) apply, as they are pertinent to ISSs who generally have the technological capability to gather and process large amounts of

data. Importantly, the guidelines state that the data minimisation duty "*complements the necessity assessments*", which will be described below.

- **Other lawful bases for processing**
  The EDPB, contradicting the previous guidelines, advises that where processing cannot be deemed to comply with Article 6(1)(b), there may be a more suitable basis for processing such as giving consent under Article 6(1)(a). However, this legal basis must be signposted at the beginning of the processing to the data subjects. The EDPB has also emphasized the importance of the data controller's transparency obligations. The guidelines strongly advise to clearly specify whether the lawful basis is under Article 6(1)(a) or (b), as it is possible that a controller might believe that the signature of a contract signifies the consent of the data subject rather than where the legal basis is where it is necessary for the performance of the contract.

- **Necessity**
  The definition of "*necessity*" not only includes the GDPR principles but also, as it has its own "*independent meaning*" in Community law, must take into account fundamental privacy and protection of personal data rights.

  The guidelines outline that in order to define necessity, you have to ascertain the purpose of processing, which in accordance with the GDPR, must be clear, specified and communicated to the data subject. The test that the guidelines set out is a "*fact-based assessment of the processing and of whether it is less intrusive compared to other options for achieving the same goal*". The guidelines suggest that if there are alternative, less invasive ways of processing, then the processing is not "*necessary*". It also specifies that Article 6(1)(b) will not apply to any processing which is "*useful but not objectively necessary*".

- **Contractual necessity**
  As stated above, Article 6(1)(b) is applicable where processing is necessary for the performance of a contract to which the data subject is party or in order to take pre-contractual steps at the data subject's request. The guidelines make clear that "*merely referencing or mentioning data processing in a contract*" does not render the processing "*necessary*" for the performance of the contract.

  Essentially, the purpose of the service should be taken into account when assessing whether Article 6(1)(b) is applicable. The processing should be objectively necessary for a purpose that is crucial to the performance of that service to the individual. The controller should be able to set out how that specific contract cannot be performed without the processing of personal data. When justifying the necessity of the processing, it is important to note that the necessity should be from both the

controller's and the data subject's perspectives. The EDPB gives the scenario of a retailer processing the data of a buyer's credit card and billing address for payment or delivery purposes as an example of what might constitute "*necessary for the performance*" of a contract.

- **Taking steps prior to entering into a contract**
  Article 6(1)(b) states that the processing of personal data may be necessary prior to entering the contract, in order to enable the actual entering into the contract. The EDPB clarifies in the guidelines that unsolicited marketing and other processing undertaken by the data controller or at a third party's request would not constitute as necessary for the purposes of this section of Article 6(1)(b).

- **Termination**
  Generally, where a contract, which uses Article 6(1)(b) as a legal basis for processing personal data, is terminated, the processing of the data for the purposes of the contract will not be necessary and therefore processing must stop. Changing the legal basis for processing would not be advised, unless you have obtained consent to process post termination.

  In addition, on termination of such a contract, in accordance with Article 17(1)(a), personal data must be deleted as it is no longer necessary for the purposes of performance of the contract. Whilst it is possible to keep processing data for specific purposes set out in Article 17(3), the EDPB states that controllers can only retain data if they ascertain a legal basis at the start of their processing and communicate to the data subjects the length of time that they propose to keep records for these purposes post termination of the contract.

Applicability of Article 6(1)(b)

- **Improving or developing a service**
  The guidelines suggest that the purpose of improving or developing a service would not constitute a legal basis for processing under Article 6(1)(b).

- **Fraud prevention**
  The guidelines also stipulate that processing for fraud prevention purposes would not constitute a legal basis for processing under Article 6(1)(b) but processing for such purposes could still be lawful under other sections such as legal obligations or legitimate interests.

- **Online behavioural advertising**
  The EDPB supports the Article 29 Working Party view that "*contractual necessity is not a suitable legal ground for building a profile of the user's tastes … based on his*

clickstream on a website and the items purchased". As data subjects have the right to object to processing of their data for direct marketing purposes in accordance with Article 21, the guidelines state that, as a general rule, Article 6(1)(b) would not apply for the purposes of behavioural advertising as it does not constitute a necessary component of online services.

Moreover, the guidelines explain that the processing of tracking and profiling users in order to target similar audiences cannot be undertaken on the basis of Article 6(1)(b). Given that the processing relates to directing advertisements at other consumers rather than the individual in the contract, the processing would not be necessary for the performance of the contract between the online service and the individual.

- **Personalisation of content**
  Depending on the nature of the services, the importance of the personalisation in delivering the content and the expectations of the average consumer, personalisation of content could constitute an essential element of the services and therefore be deemed as necessary for the performance of a contract.

  The guidelines warn controllers against solely stipulating in a contract that processing is necessary for the performance of the contract, instead advising that controllers carefully consider from all perspectives whether the specific contract cannot be performed without the processing.

Any practical tips?

Consider whether your processing really is **necessary** for the performance of the contract, as the answer will have different implications for data subjects' rights and expectations. In addition, from the outset consider if there is another legal basis justifying the processing of personal data and setting this out to the consumer. This may prove prudent in the event that termination of the contract results in the deletion of your customers' personal data.

Summer 2019

Data protection

Notifying data subjects of processing under the GDPR

The question

What are proportional measures to take when meeting the informational obligation imposed on data controllers?

The key takeaway

The consequences for not informing data subjects of processing can be severe, and companies must attempt to inform or take mitigation steps to inform data subjects.

The background

On 26 March 2019, the President of the Polish Data Protection Regulator (UODO) announced its first administrative fine for a company which had failed to meet the information obligations imposed on data controllers under Article 14(1-3).

The company, which processes data to assist their clients' behaviours and decision – making, took the data of sole traders and members of companies' bodies from publically available sources. However, the company did not inform the vast majority of the data subjects of the information required by the GDPR, such as the collected data, the data source, the purposes for which the personal data was intended, the data subject's rights and crucially, the data subject's right to object. The importance of informing the data subjects of the right to object was shown by the fact that of the 90,000 of the 6,000,000 data subjects who were indeed informed, 12,000 of them decided to object to the processing.

As the company did not have email addresses for the remaining data subjects, and only had addresses and telephone numbers for some, they resorted to publishing a notice on their own website. The company claimed under Article 14(5)(b) of the GDPR that to comply with the obligation was impossible or would involve a disproportionate effort as sending out letters to all of the remaining data subjects would financially debilitate them.

The decision

The UODO found that the company's explanation for not notifying the data subjects was unsatisfactory. The UODO explained that the company could have contacted the data subjects either through their telephone numbers or through the method of a standard letter to their address. This option would have reduced the expense which the company argued was disproportionate. In addition, the UODO stated that the company should have taken into

account the cost of notifying the data subjects in their business model, implying that they would not have processed the data from that number of data subjects had they known it was going to be expensive to notify them. Therefore, the UODO found that the company could have complied with their obligations under Article 14 of the GDPR.

Furthermore, in reaching the decision (and the large fine of €219,000), the UODO found that the company's actions were intentional as the company was indeed conscious of the fact that it had to provide the information to the data subjects and had neither attempted to contact the data subjects nor had it announced its intentions to do so.

However, UODO did state that notification was not necessary for the members of the companies' bodies as there was no contact data for these members from the source and therefore the company would have had to find more data regarding the members which would be classified as disproportionate.

Why is this important?

This ruling highlights the importance of notifying data subjects of your processing in accordance with Article 14 of the GDPR and the harshness of the penalties if you do not comply. It also portrays the court's attitude towards the balance of costs and efforts of the data controller informing data subjects and the business' capacity to trade.

Any practical tips?

Remember the obligation to notify under Article 14! If you are processing the data of a large number of data subjects (whose only contact details that you have are their address), it might be possible to notify them through the form of a standard letter which would significantly reduce the cost. In addition, the ruling suggests that processing information does not have to be given to members of companies' bodies if their data was taken from publically available sources.

Summer 2019

Consumer

"New Deal for Consumers" Directive

The question

What is the "*New Deal for Consumers*" Directive? Where has it got to? And how will it impact my business?

The key takeaway

The new Directive has been provisionally agreed but it has not yet been formally approved. The Directive updates four existing consumer law directives, increases consumer rights surrounding digital content and makes provision for Member States to impose heftier fines on non-compliant businesses.

The background

The European Parliament and the Council have provisionally agreed the "*New Deal for Consumers*" Directive (also called the **Omnibus Directive**). The Directive has not yet been formally approved and published in the Official Journal (as at the publication date). However, it is expected that the Directive will be finally adopted this Autumn.

The new Directive

The Directive will update four existing consumer law directives, namely the Unfair Commercial Practices Directive, the Consumer Rights Directive, the Unfair Contract Terms Directive and the Price Indications Directive.

It makes provision for more serious sanctions in the event of a breach of consumer law. For breaches across several EU Member States, the available maximum fine will be up to 4% of a trader's annual turnover in each respective Member State.

Additionally, the Directive will extend consumer rights to digital content and will increase transparency in online market places. One example of the way that rights relating to digital content have increased is the 14-day "*withdrawal right*". Currently, consumers who pay for digital services can cancel their contracts within 14 days after having paid for the service. Under the new Directive, this withdrawal right will also extend to the use of free digital services for which consumers provide their personal data (eg social media, cloud services and email accounts).

The Directive also updates certain other current consumer regulations. For example, consumers will no longer be able to return products that have already been used, rather than

merely trying them out. Also, traders may not need to reimburse consumers before actual receipt of the returned goods.

Finally, the Directive will include new tools for consumers to enforce their rights and get compensation, in particular through representative actions open to consumer organisations monitored by a public authority.

Why is this important?

Sanctions under the new Directive have the potential to be more serious than under the previous consumer law framework. Moreover, the reach of the new Directive will be broader than the directives which are currently applicable (for example, further extending consumer rights to digital content).

Any practical tips?

Breach of consumer rights is soon going to attract (almost) GDPR – level fines. This means not just reviewing the Directive to see how the new rules will impact your business, but also running the rule over your existing processes, agreements etc. The time to sharpen your pencil on your businesses' compliance with consumer rights (across the spectrum) is now!

Summer 2019

Consumer

CMA investigates customers' auto-renewal terms in online gaming terms and conditions

The question

How might the CMA's investigation into auto-renewals and other potentially unfair terms in online gaming contracts affect wider industry?

Key takeaway

Consider reviewing any potentially unfair terms in your customer terms and conditions, for example auto-renewals, cancellation processes and discretion to alter clauses.

The background

The CMA has launched an investigation into the major players of the online gaming industry such as Nintendo Switch, PlayStation and Xbox, in order to determine whether their commercial practices are lawful. It will examine a number of these businesses' contractual provisions such as their auto-renewal (rollover) terms, their refund policies and their terms and conditions.

The development

The CMA has contacted the major gaming companies both to ask for information about their specific gaming contracts and thoughts and experiences to support the investigation.

This action is the second phase of the CMA's response to the Citizens Advice "*super-complaint*" regarding the loyalty penalty, which had identified practices such as expensive exit fees, compulsory auto-renewals, lack of satisfactory warning of the auto renewal and difficult procedures for the cancellation of contracts.

The CMA's new investigation will focus on the issues below:

- **Fairness of contractual terms**
  Do the terms and conditions give the company a wide discretion to alter and amend the worth of the deal? For example, would it be able to increase the price or reduce the number of gaming options available to the consumer?

- **The refund policy**
  Do the companies make the consumers ability to obtain a refund or cancel their contract difficult? If so, what are the factors that deny consumers those rights?

- **The auto-renewal process**
  Is the process of starting a new membership clarified to the consumer? Is the auto-renewal a default option and how regularly is the consumer alerted that their contract will auto-renew before further payments are taken? As Andrea Coscelli, the chief executive of the CMA, stated, "*roll-over contracts are becoming more and more commonplace and its essential that they work well for customers*".

As of yet, the CMA has not come to a conclusion as to whether the companies' contractual provisions are unlawful. However, if they do find the terms unfair then enforcement action will be taken.

Why is this important?

The outcome of this investigation could bring pressure to bear on all companies which seek to impose "*unfair*" terms on their customers, such as auto-renewal terms (without sufficient warning), complex procedures to make cancelling a contract harder or give the company an excessive amount of discretion to alter the terms of the contract.

Any practical tips?

Look at your contracts and determine whether there are any unfair terms. If there is an auto-renewal clause, it may be worth highlighting this term to your customers at the outset of the contract, and giving them plenty of notice before the contract renews and they are charged. In addition, do not obscure the consumer's ability to cancel the contract.

Summer 2019

Consumer

No obligation to provide consumer telephone lines: Amazon

The question

Do e-commerce platforms and retailers have to make a telephone number available to their customers?

Key takeaway

As long as the consumer can contact the trader quickly, the information provided is clear and accessible and communication can happen effectively, then a telephone number is not needed.

The background

The German federation of consumer associations, the **Bundesverband der Verbraucherzentralen**, issued proceedings in Germany seeking a declaration that Amazon infringed German law which implemented the EU Consumer Rights Directive. Article 6(1)(c) the Directive, requires traders to indicate in a clear and comprehensible manner "*the geographical address at which the trader is established and the trader's telephone number, fax number and email address, where available, to enable the consumer to contact the trader quickly and communicate with him effectively*".

Amazon offers an automated call-back facility and an online chat service, but the Bundesverband argued that these were not sufficient to discharge Amazon's legal obligations under the Directive.

The decision

According to Advocate General Pitruzzella's opinion, the aim of the Consumer Rights Directive is to increase the level of protection afforded to consumers, as well as increase businesses' competitiveness in the marketplace. The relevant provisions of the Directive therefore have to be interpreted in such a way as to ensure the highest possible level of consumer protection without impinging on the organisational freedom of businesses, except to the extent strictly necessary for achieving the high level of protection for consumers.

Effective consumer protection is, according to the Advocate General, achieved through ensuring that consumers have the capability to communicate with the business effectively in the environment in which the transaction is carried out, which potentially includes online chat or call-back facilities. The Advocate General added that imposing a specific method of

communication between the parties would be disproportionate to the objectives of consumer protection and liable to impose undue burdens on traders, and be particularly harmful for small undertakings trading on the Internet.

So long as the consumer is able to *"…contact the trader quickly and communicate with him efficiently, and the fact that the information is provided in a clear and comprehensible manner*", their obligations under the Directive are fulfilled. The Advocate General added that the list of communication methods provided by the provision is simply an illustrative one, and the phrase "*where available*" in the provision does not create an obligation on businesses to set up a telephone or fax number if they decide to enter into distance contracts.

Finally, the customer has to clearly understand what communication methods are available to them in the event that they would need to contact the business. The Advocate General also set out that the information has to be "*easily, effectively and relatively quickly accessible by the consumer*" to fall in line with the Directive.

Why is this important?

Platforms and retailers alike are hopeful that the Court of Justice of the European Union will confirm the Advocate General's opinion later this year. This would provide a much more flexible approach to the provision of communication avenues for consumers.

Any practical tips?

Keep your fingers crossed that the European Court of Justice follows the logic of the Advocate General. This approach enables a far more flexible approach to communications with consumers, and one which should enable platforms and retailers to adapt to new communication methods as they evolve.

Summer 2019

Online platforms

New EU Platform for Business Regulation: improving fairness of the trading practices of online platforms

The question

What are the EU's proposals for improving trading practices in the online economy?

Key takeaway

A new set of rules governing business to business online market places are on their way. These will tackle unfair business practices, transparency, alternative dispute resolution and enforcement. The aim is a fairer, more transparent and more predictable online trading environment, in particular for small businesses who don't have the power to take on the online platforms.

The background

On 13 February 2019, the European Parliament, Council of Europe and the European Commission reached agreement on a new set of rules aimed at minimising market disruption in the online marketplace by tackling perceived unfair business practices and a lack of transparency. The rules seek to promote a better relationship between businesses and platforms while minimising sales disruption. Advantages for customers are also expected, both in lowering the prices of goods due to minimising lost sales revenue from disruption, as well as allowing them to seek the best deals in a transparent marketplace. The proposals come under four main categories: unfair business practices; transparency; alternative dispute resolution and enforcement.

The development

Following detailed consultation, the European Parliament, Council of Europe and the European Commission have agreed on a set of rules for online platform traders, the first in this area. The rules are intended to cover all online platform trading including online market places, hotel booking sites and app marketplaces, with some carve outs for micro businesses with less than €10 million turnover and/or 50 staff.

- **Timing**
  The European Parliament needs to approve the draft regulation. Once passed, the new rules will come into force 12 months later, so we are possibly looking at 2020 implementation at the earliest. There will be a review 18 months after the rules have come into force, with an Online Platform Observatory also set up to monitor this quickly evolving area. Keep an eye out for further publications or commentary from

findings of the Online Platform Observatory to track the effectiveness of the new rules, and possible future developments.

- **Focus on certain unfair business practices**
  The rules require that suspensions must be accompanied by clear reasons and an explanation of the method to appeal. Also, in most cases, there must be a notice period for the suspension. Terms and conditions must be in plain language and there must be at least 15 days' notice of any changes, to allow business time to make any required changes.

- **Greater transparency**
  This primarily relates to filtering and search results and also applies to search engines in addition to online marketplaces. Providers must disclose the parameters they use to rank results, to help sellers understand how to optimize their presence but without allowing them to game the ranking system. Additionally, if a provider is a seller in its own right on its own platform (ie in addition to hosting third party sellers) it must disclose any advantages given to its own products. They must also disclose what data they collect and how they use and share it.

- **New ways for resolving disputes**
  These provisions seek to rebalance the negotiating positions of larger platforms and smaller businesses which use them, which do not have the resources to challenge decisions. Providers must have an internal complaints system and there must be alternative provisions, such as mediators. Due to the costs of maintaining an internal complaints system, smaller businesses are exempt from this provision.

- **Enforcement**
  Member states can appoint public authorities with enforcement powers, who businesses can turn to for help. Business associations will also be able to take providers to court for non-compliance with the rules.

Why is this important?

There are concerns that some large, market-defining online market places are not serving the interests of the market as a whole, in terms of the smaller businesses which sell via them and for consumers. There are concerns about inconsistent and unclear suspension at short notice, lack of clarity around how to resolve issues and reluctance of smaller businesses to take on those whose platforms they rely on.

A Eurobarometer survey found that 42% of SMEs use online marketplaces to sell goods and services. The European Commission's impact assessment found that about 50% of business

users had encountered problems, with 38% remaining unresolved and 26% resolved with difficulties. This equated to lost sales of between €1.27 and €2.35 billion.

Any practical tips?

You need to work out if your business is going to be subject to the new regulation. If so, you will then need to conduct an extensive review of your trading arrangements, from your agreements to your onboarding and other processes. In real terms, you may not have that long to do this – in particular noting the time needed to educate senior management. Getting internal agreement on smoothing off the sharper edges of some of your trading practices can take time. The sooner you get the green light to do so internally, the better.

Summer 2019

Online platforms

Internet of Things – DCMS consultation on security for consumers

The question

What are the Government's proposals for ensuring the security of everyday items which are always connected to the internet (**Internet of Things**)?

Key takeaway

IoT manufacturers need to prioritise "*security by design*" in their products and to start thinking now about how they communicate to consumers on how to (properly) secure their products, including via labelling.

The background

The Department for Digital, Culture, Media and Sport (**DCMS**) launched a consultation on proposed security measures for everyday products with internet connectivity, which closed on 5 June 2019. It sets out proposals for increasing security in products at source as well as providing clear information to consumers to allow them to take their own security steps.

The development

Proposals include a mandatory labelling scheme. This would require devices to be sold with the information required to secure the product. Without a compliant label, they could not be sold.

The consultation also incorporated the key security requirements set out in the current "*Secure by Design*" code of practice for consumer IoT security (as launched last year). This requires that:

- IoT device passwords must be secured with a unique code which is not resettable to a universal factory setting
- manufacturers of IoT products must provide a public point of contact, in order to facilitate disclosure of vulnerabilities
- manufacturers must explicitly state the minimum time for which security upgrades will be provided, with an end of life policy for the product in question.

Following the consultation, the plan is for the labelling scheme to be entered into on a voluntary basis initially, with further regulation to follow once the responses to the consultation

have been considered. An alternative proposal is to prohibit the sale of items which do not comply with the key requirements (as above) of the "*Secure by Design*" code of practice.

Why is this important?

Previous approaches in this area have firmly left the onus on consumers themselves to ensure that the products they use are secure from cyber-attack. Due to a widespread lack of expertise and appreciation of risk in this area, this has led to significant weaknesses. With connected devices becoming increasingly part of the infrastructure in homes and in businesses, it is important that baseline levels of security are included in products, at source by the manufacturers, who are better able to assess the risks and counter the threats.

Any practical tips?

IoT manufacturers who want to get ahead of the curve would do well to start thinking about the voluntary labelling scheme. The more industry can move on a voluntary, rather than regulated, basis the more IoT developers will be able to retain a level of flexibility as the IoT revolution takes hold. Above all, they should adopt a security by design approach. Privacy infringements will not go down well with the regulators who may well be itching to try to keep IoT under control before it really takes off.

Summer 2019

Online platforms

Government response to DCMS report on disinformation and fake news

The question

What does the Government's response to the Digital, Culture, Media and Sport (**DCMS**) select committee report on disinformation mean for businesses with an online presence?

Key takeaway

Independent regulation of businesses with an online presence appears imminent, with any regulator likely to be given meaningful enforcement powers.

The background

On 18 February 2019 the DCMS committee published its final report on disinformation and fake news. The report followed an 18 month inquiry that considered individuals' rights over their privacy, how their political choices might be affected and influenced by online information, and the interference in political elections carried out by malign forces intent on causing disruption and confusion.

The final report called for:

- a compulsory Code of Ethics for tech companies overseen by an independent regulator. The Code would define harmful content and operate on a similar basis to the broadcasting code issued by Ofcom
- the regulator to be given powers to launch legal action against companies breaching the Code
- the formulation of a new category of tech company, not necessarily a publisher or a platform, but which tightens tech companies' liabilities for content
- a legal obligation on tech companies to take down sources of harmful content, including proven sources of disinformation.

The development

On 8 May 2019 the Government published their response to the DCMS report. The Government strongly agreed with the report's findings that the current self-regulatory approach towards tech companies is insufficient and that there is an urgent need to establish independent regulation.

The Government accepted the majority of the committee's recommendations on how to regulate companies with a significant online presence, particularly the need for independent regulation, the need to make companies legally responsible for monitoring and removing harmful and illegal content, and the threat of substantial fines to force companies to act.

The Government declined to follow the committee's recommendation to introduce a new category of tech company. The Government concluded that re-categorising tech companies to simply impose liability for content would not incentivise the systemic improvements in governance and risk management that the Government believes are necessary.

The Government instead endorsed the approach set out in its White Paper on Online Harms, based on a statutory duty of care to protect users and codes of practice to ensure companies meet their legal responsibilities. This framework will apply to all companies that allow users to share or discover content or interact with each other online.

Many of the Government's responses to the Committee's recommendations refer to the plans outlined in the White Paper on Online Harms, and the Government's response to the committee report should be read alongside the White Paper. For further information on the White Paper on Online Harms, please see our snapshot on the Online Harms White Paper.

Why is this important?

The Government's response to the DCMS committee report is a strong indication that meaningful, independent regulation of online businesses is coming. The response prompted the committee chair to say that the "*era of self-regulation is coming to an end*".

The new mechanism that online companies will have to navigate is the statutory duty of care. The statutory duty is likely to apply to global social media platforms, search engines, forums and review sites. All businesses which provide these services or platforms will be expected to comply with the additional obligations outlined in the DCMS endorsed and adopted in the Government's response and the White Paper on Online Harms.

Any practical tips?

Companies facing the proposed regulations (in particular, those with larger online presences) would be well advised to consider, as a first step, their current ability to deal with harmful content.

Summer 2019

Online platforms

Online Harms White Paper proposes regulatory framework to entrench online safety

The question

Can the UK become the safest place in the world to go online?

Key takeaway

To combat the proliferation of illegal and harmful content online, the UK Government has proposed a new statutory duty of care and regulatory framework to make online companies more accountable.

The background

Since it published its Digital Charter in January 2018, the Government has not been shy about its desire to combat, what it perceives as, the unacceptable levels of illegal and harmful content online in the UK. As reported in our Spring 2019 edition of Snapshots, the House of Lords Communications Committee published a high-level report entitled "*Regulating in a digital world*" outlining ten key principles which it proposed should guide the development and implementation of digital regulation in the UK.

On 8 April 2019, the Department for Digital, Culture, Media & Sport (**DCMS**) published the Online Harms White Paper. This White Paper forms part of the Government's drive to make internet companies more accountable for user-created content and contains a number of proposals aimed at introducing a new regulatory framework to ensure the UK is "*the safest place in the world*" to go online.

The development

The White Paper proposes the implementation of a new statutory duty of care to tackle "*online harms*". The scope of "*online harms*" to be covered by the proposed duty is wide, and covers harm caused by child sexual exploitation and terrorist activity, to those caused by cyberbullying, disinformation and the advocacy of self-harm.

A wide variety of companies will be caught by the proposed legislation. Although the White Paper stops short of providing examples, it states that the statutory duty of care will apply to those companies which host, share and/or allow the discovery of user-generated content or facilitates public and private user-interaction online.

These companies will need to take a proactive approach to user safety. They will be expected to take reasonable steps to remove harmful content and activity on their platforms and to introduce effective and easy-to-use user complaints functions. Where a complaint is made, prompt action will be required. Further, companies will need to actively combat sexually exploitative, and terrorism-related, content through targeting monitoring.

Compliance with the statutory duty of care will be overseen and enforced by an independent regulatory body. The regulator will be responsible for developing new codes of practice, and will be provided with a full suite of powers to take effective enforcement action against companies in breach of the new statutory duty. This will include the ability to impose substantial fines, up to 4% of their global turnover.

Why is this important?

In the words of the UK Digital Secretary, Jeremy Wright, the proposed changes mark the end of "*the era of self-regulation*" for online companies. At the more extreme end of the scale, the Government wants to prevent a repeat of the recent tragedy in Christchurch, where a terrorist attack was live-streamed to a global audience through social media platforms. However, it also wants online companies to become more accountable for the online abuse, bullying and fake news which affect internet users on a daily basis. In its current, widely-drafted, form, the statutory duty of care will apply to global social media platforms and search engines, as well as internet forums and even review sites. Such companies will be expected to actively respond to online harms, taking action proportionate to the severity and scale of the harm. To increase transparency, companies will also be expected to provide annual reports to evidence the effectiveness of the measures and safeguards they have in place as well the processes used to identify, block or remove harmful content.

Since being published, the White Paper has come under scrutiny for what some perceive as a clumsy, heavy-handed attempt to police the internet. Some commentators have labelled the proposals a violation of freedom of speech, while others have accused the Government of aggressive censorship. The White Paper pre-empts this criticism, stating that the regulator's powers will not be responsible for policing truth or accuracy online, nor will they encroach on current data protection measures in force under the GDPR. Nevertheless, the scope of the new regulator's responsibilities is yet to be finalised, so it remains to be seen whether such criticism is justified.

Any practical tips?

The current proposals are not yet solidified in statute; instead they form part of a public consultation which is due to end on 1 July 2019. Companies facing the proposed regulations (in particular, those with larger online presences) would be well advised to consider their current ability to deal with online harms effectively and, if necessary, re-vamp their current complaints functions.

Summer 2019

Influencer marketing

Philip Morris burned by its own internal rules on influencer marketing

The question

How careful do you need to be when using youthful-looking influencers to promote e-cigarettes?

Key takeaway

Don't use influencers, models or others in e-cigarette advertising who might look like they are (or indeed are!) under 25. And if a business sets high standards for itself from a PR perspective, don't expect a soft landing if you breach those standards.

The background

Philip Morris International (**PMI**) is an international tobacco company, whose website prominently features its commitment to a "*smoke-free future*". In pursuit of that goal, PMI has developed a number of smoke-free products, including a heated tobacco system – the IQOS.

In recognition of its "*responsibility to market [its] products responsibly*", PMI has set itself four core marketing principles which apply to its worldwide campaigns, including only marketing to adult smokers and ensuring their marketing is honest and accurate. PMI lauds its own marketing standards as being "*in many places, higher than those of some governments*".

One application of its core principles is that PMI "*don't use … youth-oriented celebrities, or models who are or appear to be under the age of 25*".

The issue

In May 2019, following a prompt from Reuters, PMI pulled a global social media marketing campaign, in which a number of influencers under the age of 30 were shown holding and prompting the IQOS. These included what Reuters termed "*rail-thin young women*", some of whom are or appear to be under the age of 25.

This embarrassing mistake resulted in significant negative press coverage for the brand, across marketing websites and mainstream media alike. In a statement to Reuters, PMI said: "*No laws were broken. However, we set high standards for ourselves and these facts do not excuse our failure to meet those standards in this instance*."

Why is this important?

This episode highlights the importance of companies not just complying with the applicable legal requirements in a marketing campaign, but also complying with their own standards, brand message and social values. Brands invest a large amount of time and money in putting together their ads. Picking the right influencers, who have an impact on consumers while also staying true to the brand's message and values, can be decisive in determining whether that investment pays off.

Any practical tips?

In addition to complying with legal requirements, setting additional standards and values for advertising can really enhance a brand's message and add to the effect of marketing campaigns. But companies should always be careful to be true to their own message and any additional standards they set for themselves. Otherwise the potential positives may melt away into an embarrassing negative.

Summer 2019

ASA

CAP: naming prize winners and marketing to children

The questions

When is it necessary to obtain the consent of a parent or guardian to use a child's data for marketing? What process should be adopted in terms and conditions for announcing winners of competitions and prize draws?

Key takeaway

The Committee of Advertising Practice (**CAP**) has changed its rules to reflect the Data Protection Act 2018 (**DPA**). It has (i) clarified 13 as the age at which children are able to consent to their information being used for online services and (ii) changed the requirements on promoters, so that prize winners must be given an opportunity to object to their information being published.

The background

In November 2018 the Committee of Advertising Practice (**CAP**) opened a public consultation on proposed changes to rules 10.16 (Marketing to children) and 8.28.5 (Naming prize winners) of the CAP Code. These changes were aimed at bringing the Code in line with the Data Protection Act 2018 (**DPA**).

Marketing to children: Rule 10.16

Under the original wording of rule 10.16, marketers were banned from collecting the personal data of children under 12 unless they had obtained the verifiable consent of the parent or guardian. Under the DPA, the UK derogated from Article 8 of the General Data Protection Regulations (**GDPR**) and set the relevant age at 13. This resulted in inconsistency between the age at which consent could be given by a child under the DPA and under the CAP Code. CAP sought to address this by amending rule 10.16.

CAP didn't receive any responses to their proposals on marketing to children. In March 2019 they brought the following changes into effect:

- the age at which children can provide consent to the use of their data for online services was increased to 13
- if a child is younger than 13, online service providers have to obtain the verifiable consent of the parent or guardian
- for other marketing purposes (ie not in relation to online services), marketers have to have "*compelling reasons*" to rely on a child's consent (rather than a parent or

guardian) and have to give "*particular regard to the child's privacy rights*". What CAP actually means by "*compelling reasons*" remains to be seen.

Naming prize winners: Rule 8.28.5

The original wording of rule 8.28.5 required that promoters obtained consent from competition entrants so that they could publish the name and county of major prize winners. However, CAP considered this to be incompatible with consent under the GDPR. First, consent is now withdrawable at any time and has to be as easy to withdraw as to give. This presents difficulties when information is published but consent is subsequently withdrawn. Secondly, requiring entrants to give their consent to enter the competition is likely to be viewed as a condition of service and therefore not freely given. CAP proposed changes to Rule 8.28.5 to bring the wording in line with processing for legitimate interests under the GDPR.

CAP received three objections to their proposals on prize winner announcements. In March 2019, they brought the following changes into effect:

- promoters are required to publish the surname (rather than full name) and county of major prize winners
- prize winners must be given the opportunity to object before their information is published (instead of being asked for their consent at entry). In such circumstances, they must still provide the information and winning entry to the ASA if challenged
- the privacy of winners cannot be prejudiced by publishing their personal information. So if it is likely that the winner can be identified from their surname and county, then their information should not be published.

Why is this important?

Standardising the age of consent under the CAP Code and the DPA is helpful for online businesses. It provides clarity on the age limits they should use in in their policies. However, the meaning of "*compelling reason for relying on the child's consent*" and "*particular regard to the child's privacy rights*" is not particularly clear. This leaves non-online marketers with uncertainty as to how the new rule should be interpreted.

The change to the rules on prize promotions should leave promoters in a situation where they are more likely to comply with data protection law. This is a welcome step, even if assessing when a surname and county will identify someone may not always be easy.

Any practical tips?

Businesses should tread carefully whenever collecting children's data (whether online or non-online). Their online terms should reflect the increased age threshold of 13 and careful consideration should be given as to how to practically enable a parent or guardian to give verifiable consent for any child under the age of 13. Although the new rules suggest that

parental or guardian consent may not be needed in non-online situations where there are "*compelling reasons*" not to obtain it, judging this will be hard. It follows that the safest course must still be to obtain such consent, at least until such time as CAP clarifies the position.

Make sure you change your precedent competition and prize draw terms to reflect the fact that publication of prize winner information must now be limited to surname and county, and do remember to check with prize winners to give them a chance to object to the publication. And finally, look out for more unique names or winners from smaller counties (or Scottish islands!) where publication of even a surname may reveal their identity. Don't publish if so!

Summer 2019

ASA

Judicial review of ASA decision on "average consumer" test

The question

Had the Advertising Standards Authority (**ASA**) correctly applied the "*average consumer*" test when deciding that the use of the term "*fibre*" in ads for part-fibre broadband was not materially misleading?

Key takeaway

The "*average consumer*" does not need to be reasonably well-informed about particular features of a product being advertised.

The background

In November 2017, following the ASA's review on fibre broadband which examined the use of the term "*fibre*" in ads when describing part-fibre and full-fibre broadband, the ASA announced that the word "*fibre*" was not likely to mislead consumers when referring to part-fibre services in ads. In order to reach this conclusion, the ASA had engaged with both part and full-fibre service providers, consumers, regulators and undertaken customer research. It found that the term "*fibre*" was not one of the significant factors that consumers considered when purchasing a broadband package. Also, consumers would not have chosen differently even with knowledge of the difference between part and full-fibre broadband.

As a result of this conclusion, CityFibre, a full-fibre broadband service provider claimed that the use of the term "*fibre*" in ads for part-fibre broadband, where there was no mention of part-fibre, was materially misleading to consumers. They argued that this had to be the case as full-fibre is "*objectively superior*" to part-fibre. Essentially, part-fibre services use full-fibre from the transmitting station, but the last section to the consumer's home is copper or another material. CityFibre applied for judicial review, arguing that the ASA had made an error in law, as they had incorrectly applied the test for the average consumer under the Consumer Protection from Unfair Trading Regulations 2008 (the **Regulations**).

The decision

The High Court upheld the ASA's decision that the use of the term "*fibre*" in broadband advertisements for part-fibre services was unlikely to mislead the average consumer. The court examined the application of the test under the Regulations, namely "*the average consumer is assumed to be reasonably well-informed, reasonably observant and circumspect*". The Judge, who for the purposes of the decision, deliberated on the basis that full-fibre was

indeed objectively superior to part-fibre, set out guidance on the definition of the "*average consumer*". His conclusions were:

- the "*average consumer*" does not need to be reasonably well-informed about specific characteristics of the product or service, in this case, being aware of the difference between part and full-fibre broadband services. Instead the judge found "*that the average consumer is only to be considered reasonably well-informed about the product or service more generally*"
- it was important to define the concept of the average consumer as a "*particular population of actual persons, namely, consumers at whom the relevant advertising is targeted*". Therefore, in this scenario, the ASA were justified in using the results from the research that they had commissioned to determine their conclusion
- the ASA had not acted irrationally and it was clear from the review and evidence provided that "*the ASA had regard to the recognised benefits of full-fibre"* but the superiority was ultimately *"not relevant to the question it had set itself*".

Why is this important?

This ruling is salient for both products/services and ads that might be deemed to be misleading. Remember that when applying the "*average consumer*" test, the reasonably well-informed consumer only needs to have regard to the product or service more generally and not to its specific features.

Furthermore, the ruling highlights the importance of properly conducted consumer research and that appropriate evidence can be used when coming to a decision about the "*average consumer*".

Any practical tips?

When assessing whether a product or service or its advertising is misleading, identify which characteristics may be misleading and whether the average consumer might be misled by it. Ideally, don't sail too close to the wind. It's best to avoid upheld ASA adjudications on claims which matter to you and judicial reviews are a remedy of last resort, and they're expensive and rarely won!

CityFibre is considering an appeal so look out for further developments on the concept of the "*average consumer*".

Summer 2019

ASA

ASA ruling on Vodafone pricing

The question

Did Vodafone exaggerate the price at which it could offer consumers broadband?

Key takeaway

Where offering a range of packages in respect of your service, ensure pricing claims do not imply minimum pricing options provide maximum service levels.

The ad

Vodafone displayed a page on its website which outlined its broadband service, "*Vodafone Gigafast*". The page displayed headline claims including: "*Blast off at an average of 900Mbps*" and "*Enjoy lightning-fast internet speeds with Vodafone Gigafast Broadband*".

These headlines were followed by smaller text, which stated "*We offer a range of average speeds from 100Mbps to 900Mbps*". Still further down the page were also the following claims: "*Great broadband doesn't have to cost the earth – enjoy Vodafone Gigafast Broadband speeds for as little as £23 a month*"; and *"[d]ownloading a 100GB game usually takes hours… with Vodafone Gigafast Broadband you can become a legend in minutes*".

The complaint

Rival internet service provider Virgin Media Ltd challenged whether Vodafone's claim as to provision of "*Gigafast Broadband*" was misleading, in that it implied that Vodafone's entire service was capable of delivering speeds of 1 Gigabit per second.

The response

Vodafone responded by noting that "*Vodafone Gigafast*" was trademarked, and that the statement itself was disclaimed; a prominent, clear statement stated that the speeds available under the Gigafast line ranged from 100Mbps to 900Mbps, on average.

Further, Vodafone asserted that they were able to deliver speeds to routers at 1Gbps, through use of their "*fibre to the home*" infrastructure.

The decision

The ASA expressed that they felt it was clear from the wording used that Vodafone Gigafast referred to a range of packages available to customers, of which one, was capable of achieving 1Gbps.

The product page featured the claim, "*enjoy lightning-fast internet speeds with Vodafone Gigafast Broadband*", but this claim was qualified appropriately with the following caveat: "*average speeds from 100Mbps to 900Mbps*". The claim as to Gigafast Broadband was therefore, not misleading.

However, the ASA took issue with Vodafone's claims as regards price, namely their claim that "*Great broadband doesn't have to cost the earth – enjoy Vodafone Gigafast Broadband speeds for as little as £23 a month*".

The ASA noted that this pricing claim was not specifically linked to a specific broadband package. As such, the consumer could get the impression that a service costing £23 per month could achieve broadband speeds of 1Gbps. This was not the case - only a service providing an average speed of 100 Mbps could be purchased for £23. A package providing speeds of up to 900Mbps on average would cost the consumer £48 per month.

As such, although the ASA considered that the ad regarding Vodafone Gigafast referred to a range of packages of varying speeds up to 1Gbps, the implication that a consumer could achieve speeds of 1Gbps for £23 a month was misleading. In this regard, Vodafone was in breach of CAP Code rules 3.1 (Misleading advertising), 3.10 and 3.11 (Qualification) and 3.9 (Exaggeration).

Why is this important?

Despite using wording which made it clear that Vodafone Gigafast referred to a range of packages available to customers, only one of which was capable of achieving 1Gbps, Vodafone failed to be transparent in respect of price. As such, it is clear that transparent claims as to service levels will still fall foul of the ASA's rules, if they mislead as to corresponding prices.

Practical Tips

Vodafone has since amended its website to say "*our packages start at £28 per month for new customers purchasing Gigafast Broadband 100*". Clear wording indicating a range of prices corresponding to differing levels of service, will avoid accusations of exaggeration.

Summer 2019

ASA

"Was/now" price claims: Zestify Media

The question

What price can be stated as the "*was*" price to represent a genuine saving when compared with the "*now*" price?

Key takeaway

"*Was/Now*" savings claims must be genuine. Don't advertise such a saving where the lower price is on for materially longer than the higher price and check that sales were actually made at the higher price during the relevant period.

The background

A complaint was made to the ASA about a TV ad for Zestify Media, which showed a crossed-out "*was*" price of £39.99 and a "*now*" price of £19.99, accompanied by a pink circle claiming "*SAVE 50%*". The complainant alleged that the "*was*" price was misleading, believing that the product (an epilator) had in fact not been sold for £39.99.

Zestify Media explained that the product had been priced at £39.99 online for a period of 74 days, between 18 July 2018 and 30 September 2018. This was endorsed by Clearcast, who confirmed that Zestify Media had provided them with an assurance that the product had been priced at £39.99.

The decision

The ASA upheld the complaint: the ad was misleading. Although the epilator had been priced at £39.99, it had not actually been sold at that price. Further, the lower price of £19.99 had been in effect for 96 days, from 1 October 2018 to 5 January 2019 (when the ad was seen by the complainant), a much longer period than the 74 days when the higher price had applied.

The ASA referred to the Chartered Trading Standards Institute's (**CTSI**) Guidance for Traders on Pricing Practices, which includes guidelines on reference pricing (namely, "*price promotions which aim to demonstrate good value by referring to another, typically higher, price*"). The Guidance provides, among other factors, that where "*the price comparison is made for a materially longer period than the higher price was offered*" or a retailer "*repeatedly uses a reference price knowing that it had not previously sold a significant number of units at that price*", then it is less likely to represent a genuine saving, and more likely to be misleading.

Since the epilator had been on sale at the lower price for materially longer than at the higher price, and no sales had been made at the higher price, the ASA agreed that the reference price of £39.99 was misleading and purchasing at the lower price of £19.99 did not represent a genuine 50% saving as the ad claimed.

Why is this important?

Despite the fact that the retailer may have had no intention to mislead consumers and used a reference price which had genuinely been in effect, this ASA decision demonstrates that the test of whether ads' claims are misleading is objective. Retailers must ensure that the information provided to consumers allows them to make an informed transactional decision, including whether to purchase a product. Facts and figures which detract from this, even if "*technically true*", will not satisfy this requirement.

Any practical tips?

Retailers should consider the CTSI Guidance when considering what information is advertised about promotions, including:

- ensure advertised savings are genuine, actually given to the customer when it comes to payment, and have not been exaggerated
- ensure products are actually available for the promotional price at which they are advertised
- avoid comparing prices to misleading, false or outdated reference pricing
- ensure relevant caveats and exclusions which apply to promotional pricing are brought to consumers' attention.

Summer 2019

ASA

Lidl held to mislead consumers with cheesy price comparison

The question

In making price comparisons with a competitor, do you need to take account of their promotional pricing?

Key takeaway

If you know your competitor is offering a price promotion on a product, you can't use the competitor's normal higher price to make your comparison. This applies even if the backdrop to your savings claim is a year-long price comparison.

The background

On 17 January 2019, Lidl featured an ad which consisted of a picture of four different food items and stated "*YOUR MONEY'S WORTH MORE AT LIDL*" and "*PRICES CRUNCHED ALL YEAR ROUND*". In addition, there was text below which stipulated that the total prices of the foods in the image were "*£11.50 at Morrisons*" and "*£9.77 (total) at Lidl*". In addition, smaller text beneath this read: "*Lidl prices correct at time of going to print…Morrisons prices checked at Morrisons.com on 16th January 2019. Excludes promotional pricing*".

Morrisons, who at the time of this ad had a discount on one of the products, a cheddar cheese, argued that the price comparison which Lidl made was not based on the current price available in their stores and so therefore challenged whether the ad was misleading and whether Lidl could substantiate their claim.

The response

In response, Lidl admitted that they did indeed know that Morrisons had a discount at the time that the ad was placed. However, they argued that the content of the ad indicated that the purpose was to illustrate that Lidl was generally cheaper than Morrisons throughout a period of a year. They argued this by pointing to a number of features in the ad, including the two main headlines (above) and the qualifying text that it excluded promotional pricing, which was in the same sized font and alongside the other qualification which stated when the Morrisons' prices were checked.

Further, given their argument that their promotion was in relation to the price of goods throughout the year, Lidl contested that they had purposefully selected Morrisons' higher price for the cheddar rather than the promotional price that had been applied when the ad was seen.

In order to justify the selection of the price, Lidl also stated that the price they had used had been applied to the product for longer and that Morrisons were likelier to charge this price to their customers over the year.

Furthermore, Lidl confirmed that they had already resolved the issue with Morrisons and had agreed not to place the ad again.

The decision

The ASA found the following:

- consumers would understand that the ad was comparing the total price of the four products from Lidl against the same four products from Morrisons
- consumers would expect that the prices would be correct at the time that the ad was placed
- even though there was qualifying information which stated that it "*excluded promotional pricing*", consumers would probably believe that none of the four products in the ad were subject to promotional pricing.

Therefore, the ASA came to the conclusion that consumers, on seeing the ad, would believe that buying the products at Lidl would save them money (£1.73).

The ASA, taking into account the fact the cheddar cheese was indeed on promotion at Morrisons on the day Lidl had checked the prices and was £1 less than what was featured on the ad, held that the ad was likely to mislead consumers (as the difference would have been £0.73).

The ASA instructed Lidl not to show the ad again and that future price comparisons should be clear and show the actual prices which were available to consumers.

Why is this important?

This ruling illustrates the importance of clarifying to consumers the basis of the price comparison. Despite Lidl's qualifying terms, the ad was not clear enough in portraying the differences between its own prices and Morrisons prices.

Any practical tips?

Be careful when making price comparisons – do not compare competitor products which you know are on promotion and clarify to the consumer which prices are being used when comparing items.

Summer 2019

ASA

CAP issues guide on comparative advertising campaigns

The question

What must marketers consider when running a comparative advertising campaign?

Key takeaway

Consult the new guide early before kicking off the creative process behind a comparative advertising campaign. And remember that you don't need to name competitors for an ad to identify them, and therefore be caught by the (tougher) comparative advertising rules! Making an objective "*best*" or "*leading*" claim could still catch you, for example because it makes a comparison with the whole market. This underlines the need to authenticate any objective claim, and provide sufficient proof to substantiate any claims that are made.

The background

The Committee of Advertising Practice (CAP) issued new guidance on 28 February 2019 identifying the key points for compliance by marketers in relation to comparative advertising.

Issues to be identified

The new CAP guide identifies four main issues:

- **Type of claim**
  Marketers need to think carefully about what claim is being made and how it will be interpreted by consumers. The guide specifically warns against using ambiguous claims as these risk misleading consumers, and reminds marketers to ensure they have evidence to support an objective claim before the ad is run.

- **Is it a comparison with an identifiable competitor?**
  If a comparison is made to an identifiable competitor, specific CAP Code rules apply. The guide highlights that the name of a competitor or a competitor's product does not need to be stated for the ad to include an "*identifiable*" competitor. Being "*identifiable*" will vary widely between markets, ads, claims, audience and the context.

- **Are the right things being compared?**
  The guide sets out that any comparative ads need to compare products which meet the same need or are intended for the same use – there needs to be a "*sufficient degree of interchangeability*" for consumers between the products being compared.

- **Is the comparison verifiable?**
  The guide highlights that comparisons with identifiable competitors need to objectively compare one or more material, relevant, verifiable and representative features of the products. Such features can include price.

Superiority claims

The guide also sets out information relating to claims of superiority or "*top parity*" (being claims that a product of an advertiser is one of the best). Unless claims are obviously "*puffery*", the ASA is likely to regard any claims of superiority as objective. CAP warns against marketers from using the term "*best*", as it could, in context, be considered a subjective claim, but also may well lead a consumer to believe the advertised products or services to have been shown to be better than their competitors.

Leading claims

The guide notes that "*leading*" claims such as "*UK's cheapest*" are likely to be interpreted as a comparison of the advertised product against all its competitors, meaning such competitors are identifiable. The ASA may well consider such a claim to be in comparison to the whole market, and therefore expect to see evidence comparing the advertised product to the whole market, rather than just its leading competitors.

Comparing like for like

The CAP Code states that ads need to compare products or services which meet the same need or which are intended for the same purpose. The new guide states that, in order to comply with this requirement, marketers need to ensure the basis of any claim is clear that the ad is not likely to mislead consumers materially.

Verifiable comparison

Any comparison with identifiable competitors needs to be verifiable. The guide states that, for a comparison to be considered verifiable, enough information must be included in the ad to enable a consumer to fully understand and check the accuracy of the claim. This information can include what the claim is based on and, in some cases, a signpost for consumers to find this information.

Why is this important?

The guide provides helpful information for marketers on comparative advertising campaigns, but also provides warning signs about what to avoid and the possible consequences. It highlights that marketers need to be able to verify any objective claim, and to provide evidence to substantiate any claims made.

Any practical tips?

Watch out for any superlative claims, eg "*best*", "*leading*" "*cheapest*" etc. Depending on context, you may be making an objective claim against the whole market, and these types of claims can be hard to substantiate.

Summer 2019

ASA – HFSS

Government consults on HFSS advertising

The question

What are the Government's new proposals for advertising restrictions for High in Fat, Salt or Sugar (**HFSS**) products?

Key takeaway

The Government wants to reduce the amount of HFSS product ads online and on TV. The pressure is on companies to engage now in order to ensure that too draconian advertising restrictions are not put into effect.

The background

On 18 March 2019, the Government launched a consultation on further advertising restrictions on TV and online for HFSS products. Essentially, the purpose of the consultation is to reduce children's exposure to HFSS ads. It sets out a number of proposals for both broadcast and online advertising.

The current rules which govern children's programming prevents ads which are aimed at promoting HFSS products to children. In addition, existing rules permit HFSS ads to be shown where 25% of the online audience is aged under-16. The Government does not wish to amend these existing regulations and any proposals taken forward from the consultation would be implemented alongside the current rules.

The development

Broadcast consultation options

Option 1: Introduce a watershed on broadcast TV

Under this proposal, HFSS products would not be permitted to be advertised between the watershed hours of 05:30 to 21:00. As this would unfairly impact on channels that have low levels of child viewers, this proposal includes an exception for channels which have only 1% of the total children's audience (around 90,000 children).

Option 2: Advertising restriction ladder

This proposal aims to incentivize companies to reformulate products or have healthier products on the market by having a ladder system to decide which products can and cannot be advertised in the watershed hours. The ladder would have three sections (whose thresholds could be redefined when necessary):

- products in the top group would have complete advertising freedom
- reformulated and healthier products would be given an advertising freedom
- the bottom group would be prevented from advertising in the watershed hours.

Option 3: No watershed
This proposal would provide no further advertising restrictions for HFSS products

Online consultation options
Option 1: Introduce a watershed online
Similar to the broadcast proposal above, this would restrict online ads for HFSS products between the watershed hours of 05:30 to 21:00. This would apply to banner and video ads. However, the Government has called for opinions on how this may apply as they acknowledge that this might be difficult to enforce for some areas (such as ads that become viral and influencer marketing).

Option 2: Strengthen current targeting restrictions
Existing rules allow children to see HFSS product ads where less than 25% of the audience are children under the age of 16. The consultation proposes that the percentage of the audience under-16 should be lowered to 10%. The Government believes that whilst this would not debilitate the ability of advertisers to place ads online, it would reduce the number of children under-16 watching the ads by more than half.

The existing rules also allow advertisers discretion as to what evidence they can provide that children are not being subject to behaviourally-targeted ads. The consultation proposes to strengthen this rule by setting advertiser standards higher for providing evidence. For ads that are directed at audiences with similar demographics and browsing activity, this proposal would set out a specific list of sources of evidence, such as data provided or inferred from users, which advertisers must adduce to show that children are being excluded from behaviourally-targeted advertising. Where advertisers cannot show this evidence or evidence which proves that the audience was less than 10% children under-16, HFSS product ads would not be permitted.

Option 3: Mixed option, so different options for online sectors
For video-ads which are viewed in a similar way to broadcast ads, such as on Video On Demand Services, VSPs, YouTube, Facebook Video etc. there might be a higher risk of HFSS product ads being displaced. As a result, there are stronger calls for watershed prohibition for these types of ads. For other types of advertising, strengthening the current targeting restrictions as set out above would be more appropriate as they are viewed differently to broadcast advertising.

Why is this important?

The Government is attempting to reduce the number of HFSS product ads that children see both online and on TV. Proposals such as the 05:30 to 21:00 watershed could make placing HFSS product ads more expensive and less effective, as there will be less available time slots. The suggestion of the advertising ladder may result in companies having to reformulate their products or release more healthy products onto the market and the proposal to reform current targeting restrictions may mean that advertisers have to take further measures in order to prevent children from being exposed to behaviourally-targeted ads.

Any practical tips?

If you are in any way involved in HFSS products or their advertising, engage in the debate! These are critical times for the food and drink industry and engaging with the Government now may help ensure a more balanced end result. Keep an eye out for any further developments and write a response to the consultation as the Government is keen to work across the industry in order to address the differences between types of ads on different media.

Summer 2019

ASA – HFSS

ASA rules that Chupa Chups ads don't suck

The question

If you're careful about placement and knowing the demographic of your audience, how safe are you showing ads for products high in fat, salt or sugar (**HFSS**)? And what about using characters and celebrities popular with children for sugar-free products, which may be synonymous with the core HFSS range?

Key takeaway

Ads for HFSS products must not target children, either through use of popular children's characters or celebrities, or through the media or context in which the ads appear. The key is to ensure they are not presented in a way which targets children, as successfully achieved for Chupa Chups in this case. Equally, care over the presentation of related ads for non-HFSS products should mean you can steer clear of breaching the rules.

The background

Rule 15 of the CAP Code sets out rules for ads relating to food, food supplements and associated health or nutrition claims. This includes:

- Rule 15.15 "*Licensed characters and celebrities popular with children must be used with a due sense of responsibility. HFSS [food and drink] advertisements that are targeted directly at pre-school or primary school children through their content must not include licensed characters or celebrities popular with children… Licensed characters and celebrities popular with children may present factual and relevant generic statements about nutrition, safety, education or similar*".
- Rule 15.18: "*HFSS product advertisements must not be directed at people under 16 through the selection of media or the context in which they appear. No medium should be used to advertise HFSS products, if more than 25% of its audience is under 16 years of age*".

CAP advertising guidance catchily called "*Identifying brand advertising that has the effect of promoting an HFSS product*" additionally explains that "*HFSS products can be promoted both directly, by including them in an advertisement, and indirectly, through the use of brands or branding that is synonymous with a specific HFSS product.*"

Recently, The Children's Food Campaign (**Sustain**) complained to the ASA about a number of online ads for the lollipop brand Chupa Chups (manufactured by Perfetti Van Malle UK Ltd

(**Perfetti**)). Sustain questioned whether certain of the ads (i) being for a HFSS product were appropriately targeted; and (ii) were HFSS food ads including licensed characters or celebrities popular with children and targeted through their content directly at children.

The ads were featured variously across Chupa Chups' website and Facebook page, and on celebrity Emma Blackery's YouTube channel. These ads included:

(a) the Chupa Chups website itself, which featured appealing product pictures and Chupa Chups-related ads presenting popular vloggers
(b) Facebook posts including (i) a Mr Men-type lollipop character; (ii) an illustration humorously suggesting that "*ancient Chupa Chups history*" should be on the school curriculum; and (iii) a video with a play on a well-known proverb, captioned: "*Give a kid a Chupa Chups and you feed them for a day. Teach a kid how to unwrap a Chupa Chups and they suck for a lifetime*"
(c) a video featuring Emma Blackery and vlogger Noodlerella reading out facts about Chupa Chups whilst doing impressions.

The decision

The complaint was not upheld; the ads were all found to be lawful.

(a) – Chupa Chups' website

The ASA considered that the Chupa Chups website as a whole was a product ad, which included many elements clearly promoting HFSS products. However, even though the website had a "*youthful character*", the ASA's view was that it was not directly targeted at children either through its content or media. Although the website included an "*age gate*" which required young users to confirm they had permission before gaining access to the website content, the ASA expressed doubt as to whether age gates are an effective deterrent. Rather, since (a) the website design and content was not likely to appeal to under-16s more than over-16s, and (b) analytics data suggested that less than 25% of visitors to the Chupa Chups website were likely to be under 16, the conclusion was that the website did not breach the Code.

In reaching that decision, the ASA demonstrated its evidential flexibility: Perfetti's demographics data showed that most visitors to both its influencers' YouTube pages and its own Facebook page were over 18, and the ASA considered this was reflective of the "*overall profile of Chupa Chups' online audience*". On this basis, although no direct demographics data was available about the Chupa Chups website, the ASA were nevertheless prepared to infer from the other available data that it was unlikely that over 25% of Chupa Chups' website visitors were under 16.

(b) and (c) – Facebook posts and video ads

The ASA considered that the Facebook posts and video ads all related to non-HFSS products (Chupa Chups' sugar free lollipop range). This was the case even though these featured or resembled the main Chupa Chups brand, which is associated with HFSS products. Factors which contributed to finding that these ads were nevertheless not for HFSS products included:

- clearly distinguishing the advertised non-HFSS products from the main HFSS product range with prominent words such as "*sugar free*"
- use of logos and images otherwise associated with HFSS products in a context which was specifically for advertising the non-HFSS product range
- regular reference to, and exclusive display of, non-HFSS products, even where the overall HFSS brand was mentioned
- deliberately drawing consumers' attention to the packaging, flavours and benefits of the non-HFSS range, to the exclusion of the HFSS range with which the brand is otherwise associated.

Why is this important?

This ruling provides useful guidance on the ASA's application of these Code rules relating to targeting children to advertise HFSS products. The ruling underlines that it is not illegal to advertise HFSS products, even where ads use characters or celebrities that are popular with children, and even where children are known to be amongst those ads' audience. What is important is that those characters and celebrities are used, and HFSS products are promoted, "*with a due sense of responsibility*", so that children are not directly targeted by the ads' content or medium.

The ruling also suggests that the ASA are unlikely to find an HFSS product range is being advertised, even where the brand is otherwise "*synonymous with a specific HFSS product*", where the ad's clear and specific intention and content is focused on that brand's non-HFSS product range.

Any practical tips?

Companies looking to advertise HFSS products should ensure that an ad's use of characters and celebrities popular with children, as well as the ad's selection of media for the ad and the context in which it appears, do not result in children being "*targeted*" by the ads.

When advertising HFSS products, companies are advised to:

- avoid designs and celebrities which specifically appeal to children
- use truly effective solutions for restricting young children's access to content that promotes HFSS products, not solutions which are easily circumvented

- avoid media and contexts which might effectively target children, bearing in mind the demographics of the ad's viewers
- ensure effective and appropriate demographics analytics are in place, with data which allows monitoring of age ranges to ensure children do not make up over 25% of viewers of HFSS ads.

This case also includes helpful pointers on how to advertise non-HFSS products which feature or resemble the core HFSS brand, such as clearly distinguishing the two and specifically calling out the packaging, flavours and benefits of the non-HFSS range.

Summer 2019

Gambling

ASA uses child avatars to tackle irresponsible gambling ads targeted at children

The question

How has the ASA's introduction of new technology, such as child avatars, impacted on ad monitoring and enforcement?

Key takeaway

The ASA is pro-actively using avatars (which mimic child-like behaviour) to identify when regulated ads (gambling, alcohol, HFSS etc) are being irresponsibly targeted at children.

The background

On 20 May 2019, Guy Parker, the chief executive of the ASA, outlined that the ASA's "*new five year strategy is focused on strengthening further the regulation of online advertising and using new tech to protect the public*". To that end, the ASA has introduced new technology in the form of "*child avatars*" which mimic children's online behaviour, in order to monitor the types of ads that children are prone to see online.

The development

The ASA, with the assistance of a data and analytics company, formulated seven online avatars which simulated the behaviour (on non-logged-in-environments) of children of varying ages, an adult, and a child and an adult using the same device.

As a result of these avatars, the ASA has announced that it had banned ads from five gambling operators whose ads were served to the child avatars. During a two week period where the ads were monitored, the ASA found that out of 24 children's websites monitored, 11 showed gambling ads.

The bookmakers responsible for the ads have accepted that their ads should not have been available to children on those sites, but sought to place responsibility onto third parties who had wrongly placed the ads on behalf of the gambling operators. The ASA has informed these companies that they must review the placement of their ads and take appropriate measures to make sure the mistake is not repeated.

Due to the successful outcome of the monitoring through avatars, the ASA is currently exploring whether these measures can be extended to logged-in environments such as Facebook, Instagram, and Twitter and extended to the monitoring of other age-restricted

advertising, such as for HFSS products and alcohol. In addition, the ASA, in its annual report, confirmed that it has "*established a team of digital specialists*" and is also determining how other new technologies can help the ASA protect the public.

Why is this important?

The use of new technology will enable the ASA to be pro-active in taking action against irresponsible ads as they will be able to ban ads without there having to be a complaint from a member of the public. Further, as shown by the action taken against the gambling operators, the ability to view which ads children can see online will facilitate the ASA to take swift action against the responsible parties.

Any practical tips?

Make sure your business or any company which your business uses to place your ad takes sufficient measures to keep ads from being directed at children.

Even if the ad is not offensive and is therefore unlikely to attract a complaint, particularly if it is only likely to be seen by a child, the introduction of avatars means that no, wrongly placed ad is safe from the watching eyes of the ASA's avatar operators!

Summer 2019

Gambling

Tottenham Hotspur rapped by ASA for use of young player in betting tweet

The question

When is it possible to feature an individual under the age of 25 in a gambling ad?

Key takeaway

If you're a gambling or alcohol brand, make sure your ads don't use images of individuals under 25. Beware team shots! The ruling also reinforces the rule that any marketing communication with an individual under 25 years of age can only be placed in a location where a bet can made through a transactional facility, such as the gambling operator's website. This is important as gambling operators need to be aware, especially in sports scenarios where many of the related individuals are under 25, that their partnerships and social media influence with companies, such as football clubs may be restricted by this rule.

The background

Tottenham Hotspur's heartbreak in Madrid was not the only loss they suffered on their Champions League journey this year. Their tweet announcing their starting line-up, before their knock-out round game against Borussia Dortmund, contained a link to the William Hill website and was deemed to contravene the CAP Code as it was socially irresponsible.

The ad

The tweet, viewed on 5 March 2019, was challenged by the ASA as it consisted of an image of the starting line-up where two of the players, Harry Winks and Davinson Sanchez, were under the age of 25 as well as a link to the William Hill website, an image of the gambling operator's logo and accompanying text which read "*Latest odds from @WilliamHill*".

The response

Tottenham Hotspur and William Hill contested that Harry Winks and Davinson Sanchez were included in the image because they were in the starting line-up. In addition, they argued that whilst both players were under 25 years of age, they were neither the centre of attention of the ad nor shown on an individual basis and were not of more importance to the team than the other players in the image. Finally, they claimed that the underage players were in the image alongside the rest of the starting line-up, all of whom were over the age limit of 25.

The decision

In response to Tottenham and William Hill's arguments, the ASA determined that Tottenham's tweet had dual purposes; the first was to notify Twitter users of the starting line-up, and the second, judged to be equally important, was to offer users the chance to bet on the game.

The ASA considered the situation with regards to Rule 16.3.14 of the CAP Code which states that "*no one who is, or seemed to be, under 25 years old may be featured playing a significant role in marketing communications*". The ASA held that whilst Harry Winks and Davinson Sanchez were of no greater significance than the other players in the line-up, each player had a similar "*significant*" role in the marketing communication.

The ASA also looked at whether the inclusion of Harry Winks and Davinson Sanchez in the tweet fell under the exceptions that this rule contains, namely:

- those under 25 may appear in marketing communications that are located in a place where a bet can actually be made
- the person under 25 may only be used in those communications to highlight specific betting selections where that person is the subject of the bet offered. The image or depiction used must show them in the context of the bet and not in a gambling context.

As the tweet was from Tottenham Hotspur's twitter account and not a transactional facility through which a bet could be placed, such as William Hill's own website, nor had the underage players been used to illustrate specific betting selections where they were the subject of the bet offered, the ASA found that the ad did not fall into the above exceptions and was, therefore, socially irresponsible and in breach of the CAP Code.

Why is this important?

This ruling highlights the strict application of the "*significant role*" in Rule 16.3.14 and 18.16 of the CAP Code which relates to under-25s appearing in alcohol ads. It reinforces how careful gambling operators and alcohol companies need to be. Even when the younger individual is in a group with older individuals, the significance of that role will not become less so because there are other individuals also playing significant roles in the same marketing communication.

Any practical tips?

If you wish to place an individual under the age of 25 in a gambling ad, make sure that the ad is placed in a location where a customer can make a bet and ensure that where the individual is used they are only there to illustrate specific betting selections where they are the subject of the bet offered. The image or other depiction used must show them in the context of the bet and not in the gambling context.

Above all, keep on your toes when it comes to team shots! Younger age players (ie under 25 from a gambling and alcohol perspective) can easily be in a shot which the marketing team wishes to use in an ad. Think about educating the team, including those tending your social media accounts. You don't want your ads receiving the wrong type of (regulatory) attention!

Summer 2019

Gambling

CAP and BCAP issue gambling advertising guidance

The question

What must you do in order to ensure a gambling ad is not aimed towards children?

Key takeaway

Marketers must take heed of the new gambling guidance by taking "*all reasonable steps*" to use data correctly and "*particular care*" when engaging with influencers in order to make sure that ads are not directed at under 18s.

The background

Between 2016 and 2018 the Department of Digital, Culture, Media and Sport (**DCMS**) carried out a review of gambling policy, raising two important issues: (1) what is the impact of gambling advertising on problem gambling; and (2) what is the impact on children and young people?

In response to the DCMS' review, the Committee of Advertising Practice (**CAP**) and the Broadcast Committee of Advertising Practice (**BCAP**) and the ASA issued a joint letter detailing ongoing enforcement and policy work. This letter also committed CAP, BCAP and the ASA to develop new guidance on the interpretation of the relevant rules.

CAP and BCAP have now published updated gambling advertising guidance in an effort to address the potential risks to children and young people posed by irresponsible gambling advertising. The new guidance took effect on 1 April 2019 and underlines the protections provided by the Advertising Codes; specifically, under-18s must not be addressed by gambling advertising or targeted through media placement or ad content, and ads intended for adults must not contain content of particular appeal to under-18s.

The development

CAP and BCAP's new guidance highlights how the relevant rules should be interpreted in respect of gambling advertising and children.

Rule 16.3.13 of the CAP Code prevents marketing communications being directed at those aged below 18 "*through the selection of media or context in which they appear*". The new guidance states that marketers must ensure they take "*all reasonable steps*" to use the data available to include or exclude individuals based on their age or other criteria. Under-18s, or those individuals whose online behaviour suggests they are under 18, should not be targeted

directly with gambling advertising. The guidance also states that where social or online games feature marketing communications for gambling games, these should not be directed at under-18s.

The guidance also highlights that marketers need to take "*particular care*" if engaging influencers to promote gambling products or brands; the influencer's likely appeal and audience data should be assessed to ensure under-18s do not make up over 25% of the audience.

The new guidance also prohibits gambling ads likely being of "*particular appeal*" to under-18s. Such "*particular appeal*" is determined by assessing whether the content appeals more to under-18s than to those over 18. The guidance provides an extensive list of particular examples of characters which may of particular interest in determining "*particular appeal*", including, amongst others, superheroes, exaggerated animated characters, children's cartoons and fairy-tale characters. The guidance highlights that marketers should also exercise caution in relation to the overall theme and imagery of an advert; if such themes and imagery is likely to be of appeal to under-18s, it is more likely that it will ring alarm bells with the ASA. The guidance also explains that prohibitions on ads appealing to children extend to the names of online games; marketers should avoid using names involving specific characters or general tropes which are familiar to children or often directed at children.

The guidance also warns against the use of "*youth culture*" in ads. This can extend to themes or content associated with youths, including music, video games, fashion, language and other cultural references. This is a very wide term, and marketers should be wary of using any imagery or themes which could be considered as part of "*youth culture*".

Why is this important?

From 1 April 2019, the ASA will have regard to the requirements of the new CAP and BCAP guidance in respect of the gambling portions of the UK Advertising Codes. This means that marketers involved in producing gambling ads must take heed of the new requirements, and ensure that ads are not targeted towards under-18s in any way. This involves reviewing available data and investigating target audiences of influencers etc. in order to ensure gambling ads are responsibly targeted.

Any practical tips?

If you are considering launching a marketing ad which could potentially be considered as targeted towards under-18s or using imagery or themes which are of particular appeal to under-18s, consider whether it may breach the new requirements. The ASA will expect to see that you have done the appropriate research into the target audience of the ad, and for you to be able to show that it is not of particular appeal to under-18s. If this cannot be done, the ad will need to be reconsidered.

Remember also that the ASA is now actively deploying avatars to mimic child-like behaviour in order to keep a watch on gambling ads making their way through to children audiences. This underlines the need for gambling brands (and indeed all others speaking in regulated markets, like alcohol) to take extreme care with the flavour of their advertising and its targeting. As the ASA says, it will expect to see "*robust evidence that [marketers] have been diligent in forecasting the likely audience for a marketing campaign*".

Summer 2019

Gambling

Betfred avoids irresponsible gambling ad breach

The question

When does an ad showing characters gambling during everyday activities cross the socially responsible line in the BCAP Code?

Key takeaway

Ads must not portray gambling as an indispensable activity. The key (as here) was not to show gambling as taking priority in life.

The ad

Online betting company Betfred advertised its online bingo games, which are available on mobile devices, by depicting characters playing bingo on their phone while completing everyday tasks. The ad depicted two characters: a woman playing mobile bingo while exercising, and a man playing while preparing a meal. Further, the ad included the following voiceover, which linked the online game back to the activities the characters were carrying out:

"*Love to chill in the bath? Make it a thrill and laugh with Betfred bingo. Forget those two little ducks, soak up the action and win big bucks. You can even join in whilst making the tea with games from as little as just 1p!*"

The complaint

The BCAP Code states that marketing communications for gambling must not portray, condone or encourage gambling behaviour that is socially irresponsible, or could lead to financial, social or emotional harm. Further, it also states that marketing communications for gambling must not portray gambling as indispensable or as taking priority in life, for example over family, friends or professional or educational commitments.

The complainant, having viewed the television ad on 20 January 2019, complained that the ad normalised gambling, by showing the characters gambling while carrying out every day activities. As such, the complainant argued that the ad was socially irresponsible.

The response

Betfred argued that the ad did not encourage excessive gambling, and noted that gambling was not shown as the sole activity undertaken in the home environment. Further, the ad depicted gambling across a range of situations, instead of portraying one character whose life

included gambling during a range of daily activities; viewers would not perceive gambling as having taken priority over the characters' daily lives.

In addition, Betfred argued that the ad did not portray gambling as an indispensable activity, or that enjoyment of life was changed by gambling. There was no insinuation that gambling is favourable over other social activities, nor did the ad promote unrealistic positive or negative emotions. Finally, the ad did not promote high stakes gambling, or depict characters who were isolated from family, friends, work or education.

The decision

The ASA concluded that the ad did not portray, condone or encourage gambling behaviour that was socially irresponsible, or portray gambling as indispensable or as taking priority in life and as such, did not breach the BCAP Code. The ASA decided that the ad did not focus on characters gambling instead of undertaking daily tasks, but rather portrayed characters as using the online betting app in conjunction with daily activities.

Why is this important?

The ASA stressed that the most important factor in their decision making was that Betfred's ad did not portray gambling as taking priority over character's lives. This is clearly the most important consideration when deciding if an ad of this nature is socially irresponsible contrary to the BCAP Code.

Summer 2019