Winter 2019

Contents

Commercial – good faith

Implied duty of good faith clarified (High Court)

New Balance Athletics, Inc v Liverpool Football Club and Athletic Grounds Ltd [2019] EWHC 2837 (Comm)

The question

What is the scope of implied good faith?

The key takeaway

Acting in a dishonest way would be a breach of a duty to act in good faith. However, there is no breach if a party had an honest belief, even if the basis for such a belief was unreasonable.

The background

In 2011, Liverpool Football Club (**Liverpool**) agreed a sponsorship deal with New Balance Athletics, Inc (**New Balance**). The contract included a "matching right":

- that the parties must negotiate the renewal of the agreement with good faith during the "first dealing period";
- if no agreement was reached, then the club could negotiate with a third party; and
- New Balance would have the ability to match the third party's offer.

After failed discussions regarding renewal of the sponsorship agreement, Nike made an offer to Liverpool that included marketing such as using "*non-football global superstar athletes and influencers of the calibre of LeBron James, Serena Williams, Drake*" and distribution of at least 6,000 stores worldwide to sell Liverpool merchandise. In response, New Balance made a "matching offer", which Liverpool claimed neither matched Nike's offer nor had it been made in good faith. New Balance argued that it would only have breached the duty to act in good faith if they had not intended or knew that they could not uphold the terms of their offer.

The decision

In considering whether New Balance had acted in good faith, Mr Justice Teare looked at (1) the nature of the bargain, (2) the terms of the contract and (3) the context in which the matter arose. He ruled that ultimately, the question for the Court to consider was whether "*reasonable and honest people would regard the challenged conduct as commercially unacceptable*". (*Alan Bates v Post Office* [2019] EWHC 606).

Liverpool argued that New Balance were not able to provide distribution in 6,000 stores, relying on five particular errors which would make the number of available stores lower. One of the errors concerned the stores in Japan; Liverpool noted that 250 of the 400 stores that New Balance claimed could sell merchandise only sold footwear. To this, Teare J stated that, as the Licensed Products in the Nike agreement were defined as including running shoes, there was no error and they had not acted in bad faith by including those stores.

As for the other errors, Teare J stated that if New Balance had honestly thought that they could match Nike's distribution offering (even if they had believed this unreasonably) then they would not have breached the implied duty of good faith as reasonable and honest people would not regard such conduct as commercially unacceptable.

However, as New Balance had not matched Nike's marketing services, particularly providing the non-football global stars of the calibre noted by Nike, the Court held that Liverpool was not required to continue with New Balance.

Why is this important?

The case provides useful guidance on the scope of the duty of good faith. Whilst Liverpool may have believed that New Balance match Nike's distribution services, as long as New Balance could show that they honestly believed that they could, then they would not be in breach of the implied duty.

Any practical tips

Always make sure that you honestly believe the negotiating positions being advanced! Bear in mind that commercially unacceptable behaviour may breach obligations of good faith.

Winter 2019

Commercial

Implied duty of good faith in relational agreements

UTB v Sheffield United

The question

When should a duty to act with good faith be implied into an agreement?

The key takeaway

The duty of good faith is not limited to when the agreement is "relational". The question is whether an obligation of good faith was obviously meant or is necessary for the proper working of the agreement.

The background

The relationship between Kevin McCabe of Sheffield United Limited (**SUL**) and Prince Abdullah bin Musa'ad of UTB LLC (**UTB**) began in 2013 when the parties entered into an Investment and Shareholders' Agreement (**ISA**). The ISA stated that UTB would provide £10m over a period of around two years in return for 50% of the shares in the Blades, who wholly owned Sheffield United Football Club (**SUFC**).

Numerous disagreements subsequently arose throughout 2013 to 2018, leading to the two parties considering how to end their joint ownership of SUFC. SUL acted first and offered to buy UTB's shares for £5m by serving a Call Option Notice under the ISA. However, SUL (purportedly) did not realise that the call option also permitted UTB to serve a counter notice on SUL, enabling UTB to purchase SUL's shares for the same price that SUL had previously offered.

UTB subsequently sought to enforce the purchase of SUL's shares and SUL sought to have the contract declared void or set aside and that UTB sell its shares to SUL at the current value (which has hugely increased since SUFC's promotion to the Premier League in the 2019/2020 season).

The decision

Whilst the Judgment considered a number of legal issues, such as the validity of the contract, specific performance and unfair prejudice (s994 of the Companies Act), this summary focuses on the Court's interpretation of whether good faith could be implied into the ISA.

What is the duty of good faith?

Recent case law has held that an express term requiring the parties to act with the "utmost good faith" towards one another imposed an obligation *"… to observe reasonable commercial standards of fair dealing in accordance with their actions which related to the Agreement and also requiring faithfulness to the agreed common purpose and consistency with the justified expectations of the [other party]*" and that *"… the obligation of utmost good faith in the* [contract] *was to adhere to the spirit of the contract* […] *and to observe reasonable commercial standards of fair dealing, and to be faithful to the agreed common purpose, and to act consistently with the justified expectations of the parties*."

Can good faith be implied into a contract?

The most significant development in relation to whether good faith can be implied into a contract was in *Yam Seng Pte Ltd v International Trade Corporation Ltd* where Leggatt J held that that a duty of good faith could be implied into a "relational" commercial contract.

Relational contracts normally involve a long-term relationship with a substantial amount of communication, co-operation and predictable performance. *Bates v Post Office* (No. 3)[3] sets out a number of criteria that may determine if a contract is relational, such as (i) an intention to perform the parties' respective roles with integrity and fidelity to the bargain, (ii) a commitment to collaboration in the contract's performance and (iii) a high degree of communication, cooperation and predictable performance based on mutual trust and confidence, and expectations of loyalty.

However; whilst the Judge in this case acknowledged the previous decisions in *Yam Seng* and *Bates*, rather than question whether the contract was relational, he considered the test should be whether a "*reasonable reader of the contract would consider that an obligation of good faith was obviously meant or whether the obligation is necessary to the proper working of the contract*".

As a result: (i) given that there were areas in the ISA where good faith was expressly required (therefore indicating that the parties had considered where and where not to act with good faith); and (ii) the contrasting interests of the parties were both reflected in the ISA and at different points in the relationship, the Court found that the terms of the ISA were not subject to an implied term that each of the shareholders were to deal with the other in good faith.

Therefore, the Court held that SUL must sell its shares to UTB, making UTB the majority owner of SUFC.

Why is it important?

This case shows that the Court will not always look to see whether there is a relational contract as a basis to imply a duty of good faith between parties. The Court will look at whether the "*reasonable reader of the contract would consider that an obligation of good faith was obviously meant or whether the obligation is necessary to the proper working of the contract*" (ie applying the test for an "implied term").

Any practical tips

Contracting parties should decide at the outset whether or not it is in its best interests for the contract to be subject to a duty of good faith. Parties should expressly set out this duty (or exclude the duty) in the contract (bearing in mind that if they set good faith obligations for specific terms of the contract, the Courts may interpret this as meaning that good faith will not apply to the other terms of the contract). Bear in mind that certain contracts (eg relational contracts) may be more likely to have implied duties of good faith.

Winter 2019

Commercial – subject to contract

No "curate's egg" approach to terms in a subject to contract document (Court of Appeal)

Farrar v Rylatt [2019] EWCA Civ 1864

The question

Can the "subject to contract" principle apply to certain terms within a document only (rather than the whole document)?

The key takeaway

Documents which are marked "subject to contract" are usually not legally binding. The Court of Appeal has ruled that this principle applies to a document in its entirety and it cannot be claimed that it applies to some parts of a document, but not others (unless the document itself says so).

The background

The appellants were a builder and his construction company. The appellants sought declarations that there were two legally binding profit sharing agreements relating to two of the appellants' property developments. In relation to one of the developments (named **The Barns**), the appellants alleged that the valid profit sharing agreement arose from a heads of terms document, which had been annexed to a building contract.

However, the heads of terms document had not been signed and was marked "subject to contract and without prejudice". The document further provided that the first appellant "will enter" into a joint venture partnership with the respondents in relation to the property development. The net proceeds were to be divided 50:50 between the first appellant and the respondents.

The heads of terms document covered other high-level issues (rather than detached matters) such as:

- timetable for exchanging contracts for the sale of land;
- the appellant's obligations as the seller; and
- a proposal for a joint venture and principles for profit sharing.

The parties also entered into subsequent contracts for the sale of the land and for building works. However, none of the subsequent contracts was entered into for the joint venture or profit sharing purposes.

At the trial, the Judge decided that no legally binding profit sharing agreement arose from the heads of terms. This was not only because of the "subject to contract" label at the top of the document, but also because the heads of terms document was not signed among other things.

The decision

The Court of Appeal criticised the trial judgment, stating that it "*is not as clear as it might be on important issues of fact and law*". However, despite this, it upheld the Judge's finding that the heads of terms document was not legally binding.

In reaching a decision that the heads of terms document was accurately labelled "subject to contract", the Court of Appeal drew particular attention to the following factors:

- the wording of the heads of terms showed that the parties were not yet ready to agree the terms of a contract;
- information was still outstanding and that it was the intention that a further future contract would be entered into;
- the two respondents who were named as a party to the heads of terms were in another country on the date of the document;
- the two respondents named in the heads of terms document did not eventually buy the land, as intended in the document (the third respondent, a corporate entity, did).

The Court of Appeal further stated that the "subject to contract" principle could not apply partially, rather than entirely, to documents. For example, clauses in a document marked "subject to contract" are not legally binding unless the document specifically states that certain clauses are exempt from the label "subject to contract".

Why is this important?

The fact that the "subject to contract" principle cannot be applied partially within documents (unless the document itself states otherwise) is not surprising. However, this Court of Appeal decision provides an authoritative statement of the law, which businesses will find helpful.

Any practical tips?

You should always ensure that your intentions are clearly and accurately reflected in documents. If you intend for certain clauses in a "subject to contract" document to be binding (eg confidentiality, costs or governing law/jurisdiction), ensure that this is expressly stated in the document.

Winter 2019

Commercial – cryptoassets/smart contracts/electronic signatures

Cryptoassets and smart contracts: UK Jurisdiction Taskforce publishes legal statement

The question

What legal status do cryptoassets have under English law? Are smart contracts legally valid and enforceable under English law?

The key takeaway

The legal statement is likely to be legally persuasive, but its principles have not yet been tested in the English courts. The statement provides some key findings:

- Cryptoassets are to be considered property and to be treated as property in law. However, cryptoassets cannot be "possessed" because they are not physical assets. This means that certain legal principles cannot be applied to them.
- Smart contracts are valid and enforceable contracts and electronic signatures are recognised as valid.

The background

The UK Jurisdiction Taskforce (**UKJT**) is one of six taskforces of the Law Society's "LawTech Delivery Panel", which includes industry experts and members from the government and judiciary. The UKJT launched a public consultation on the legal uncertainty regarding the status of cryptoassets and smart contracts under English law in May 2019.

Following the consultation, the UKJT published a legal statement with the intention of relieving legal uncertainty in this area. The statement is likely to be legally persuasive but its principles have not yet been tested in the English courts.

The guidance

Cryptoassets

According to the statement, cryptoassets are to be considered property and to be treated as property in law. Therefore, cryptoassets are to be subject to laws concerning the passing of property on death, bankruptcy and insolvency, among other things.

However, because cryptoassets are not physical, the UKJT suggests that they cannot be "possessed" in law. In particular, this would mean that cryptoassets cannot constitute "goods" under the Sale of Goods Act 1979 and they cannot be the object of a bailment. The types of security which can be granted over cryptoassets would be limited and cryptoassets cannot be the object of a pledge or lien.

Smart contracts

The UKJT considers that smart contracts are capable of satisfying the requirements for the formation of a valid contract under English law. The UKJT also gives its opinion that smart contracts can be interpreted and enforced using ordinary English legal principles and that they can be enforced in Court.

According to the legal statement, it is very likely that statutory signature requirements will be met by the use of private key encryption.

Why is this important?

The UKJT's statement provides a level of certainty for market players as to how cryptoassets and smart contracts may be treated under English law and by the English Courts. The statement was intended to bolster market confidence.

Any practical tips?

When making legal and commercial decisions in relation to cryptoassets or smart contracts, it is helpful to review the UKJT's position as described in the statement.

Winter 2019

Commercial

Electronic signatures

Neocloeous v Rees [2019] EWHC 2462 (Ch)

The question

Does an automatic email footer render a document "signed"?

The key takeaway

The case affirms the Law Commission's Report on Electronic Execution of Documents, specifically that an electronic signature (including a name typed at the bottom of an email) is capable of executing documents as long as the sender intends to authenticate the document.

The facts

The parties were in dispute over a right of way over the claimant's property on the eastern side of Lake Windermere. The defendant's solicitor, David Tear emailed the claimant's solicitor to confirm the terms of settlement. The email was signed "*David Tear, solicitor and director, for and on behalf of AWB Charlesworth Solicitors"* and followed by Mr Tear's contact details. Emailing in response, the claimant's solicitor, Daniel Wise confirmed his agreement. Similarly, his email was signed "*Daniel Wise – Associate, dispute resolution for and on behalf of Slater Heelis LLP*" and followed by Mr Wise's contact details.

The Tribunal hearing was vacated following settlement negotiations, however the defendant's solicitors requested the hearing be re-listed and the claimant issued proceedings seeking specific performance of the alleged contract of compromise. The claimant argued that the emails referred to above amounted to a single document signed by or on behalf of each party and thus the signature formalities under s2 of the Law of Property (Miscellaneous Provisions) Act 1989 had been met. They reasoned that the name of the sender at the foot of the emails (regardless of whether it had been typed or generated by email managing software) rendered the document signed so long as the inclusion of the name was for the purpose of giving authenticity to the document.

The decision

It was held that Mr Tear had in fact signed the email on behalf of the defendant and therefore the claimant was entitled to the order for specific performance of the compromise agreement as contained in the email exchange mentioned above.

The Judge echoed the *J Pereira Fernandes SA v Mehta* [2016] 1 WLR 1543 test for whether something is a signature – whether the name was applied with authenticating intent – and accepted that, despite not manually typing his name in the email footer, Mr Tear did intend to authenticate and thus sign the email. This was because at some stage Mr Tear had consciously entered the footer information into his email settings, so he knew that his name would be applied as a footer and a means of identifying himself to recipients of his emails. Therefore, the "automatic" nature of the footer was irrelevant for these purposes.

Why is this important?

In an age where electronic communication is the preferred option, this case is significant as it simplifies the document execution process, removing the need for handwritten signatures.

Any practical tips?

Although this case concerned the signature requirement under the Law of Property (Miscellaneous Provisions) Act 1989, it is likely that the Court will take the same view for similar signature requirements under other legislation, unless there are specific requirements for a handwritten signature.

Consequently, when negotiating agreements via email, you should be aware that automated signatures can demonstrate the same authenticating intent as a signature, or manually typing your name at the bottom of the email. If you do not want emails to have such a binding effect, disclaimers or "subject to contract" wording should be used.

Winter 2019

IP

Liverpool FC fail to register "LIVERPOOL" trade mark alone

The question

What should businesses consider when attempting to register a place name as a trade mark?

The key takeaway

Characteristics of the trade mark, such as being distinct and stylised, as well as the categories the trade mark will cover, may contribute to a successful application to register a trade mark that has geographical significance.

The background

Liverpool Football Club (**LFC**) filed an application to register the trade mark "LIVERPOOL" at the Intellectual Property Office of the United Kingdom (**UKIPO**) on 20 June 2019. The application was made in relation to a wide number of goods and services including toys, photographs, clothing and broadcasting services. LFC stated that the application was strictly to protect the club and supporters from buying counterfeit Liverpool FC products; a registered trade mark would make it easier to curb counterfeit merchandise products and protect their brand internationally.

Shortly after LFC filed its original application, it was split into two separate applications. The first application (covering scientific apparatus, clothing, footwear, games and toys) is still under consideration. The second application, (covering office materials, business management services, telecommunication, education and services for providing food and drink) was refused by the UKIPO in a high profile decision.

The decision

Although LFC stressed that it wanted to register the name as a trade mark "*only in the context of football products and services*", its application was unsuccessful. The UKIPO found that LFC could not monopolise the name "Liverpool" due to its "*geographical significance*" as a city. If the UKIPO had granted LFC the rights for the geographical location, it would have granted LFC sole use over the association with Liverpool (the city), and the capability to prevent anyone else's use in this regard.

Interestingly, this application and subsequent resistance mirrors a similar dispute from over 10 years ago, when LFC overcame criticism from local politicians concerning their application

to register a component of its crest; a depiction of the liver bird. Alfie Hincks, local businessman and supporter of rivals Everton Football Club, strongly opposed the application and, on the grounds that the liver bird was well recognized as an emblem of the city of Liverpool, filed an opposition to LFC's trade mark registration. However, the arrangement of the trade mark, featuring both the liver bird as well as the name of the club and the iron gates of Anfield, meant that the trade mark was considered a distinct and stylised mark and therefore it was registered.

What has gone unnoticed by many is that the first application was approved for publication by the UKIPO, published on 8 August 2019 and remains pending. The application is still open for opposition and to date there have been over 100 notices of intended opposition filed. As mentioned above, the goods in this surviving application all fall into the "merchandising" category, which perhaps gives LFC a better chance at a successful registration, given that it would be more realistic to associate merchandising goods exclusively with LFC. For example, Southampton FC's "SOUTHAMPTON" EU trade mark covers three almost identical classes so perhaps this is more of a promising position for LFC.

Why is this important?

The move is not unprecedented and other Premier League clubs such as Tottenham Hotspur Football Club and Chelsea Football Club have successfully managed to trade mark place names in relation to their commercial businesses. Essentially, clubs want to register marks across a wide variety of classes, with as wide-ranging specifications as possible in order to limit the number of counterfeit products and to cover different types of merchandising or sponsorship agreements.

Any practical tips?

As LFC have done, businesses should consider making separate applications covering different categories of items. This way, it is possible that at least the narrower application might be approved. LFC's contrasting fortunes in attempting to register "LIVERPOOL" and their successful attempt to register the liver bird highlight the importance of making the trade mark distinct and stylised (indeed Liverpool have successfully registered as a mark "Liverpool FC" and "Liverpool Football Club").

Winter 2019

Data protection

Lawfulness of automated facial recognition

R (Edward Bridges) v the Chief Constable of South Wales [2019] EWHC 2341 (Admin)

The question

Is the use of automated facial recognition (**AFR**) technology by law enforcement lawful under the Data Protection Act 1998 (**DPA 1998**), the Data Protection Act 2018 (**DPA 2018**), the Equality Act 2010 and Article 8 of the European Convention on Human Rights (**ECHR**)?

The key takeaway

Rights under Article 8 of the ECHR are engaged by the use of AFR, but (in this case) its use by law enforcement struck a fair balance between the rights of the individual and those of the community.

The facts

AFR can help to assess whether two facial images depict the same person. A digital photograph of a person's face is taken and processed to extract measurements of facial features. That data is then compared with similar data from images contained in a database.

This case resulted from the use of security cameras by South Wales Police (**SWP**) to take digital images of the public and match them against images of individuals on SWP's watch lists as part of a pilot project named "AFR Locate". If no match was found, the relevant individuals' biometric data was not stored (although the underlying CCTV footage was kept for a period of time). If a match was made, the police decided how to respond. The technology was used on around fifty occasions at a variety of large public events (for example, the 2017 UEFA Champions League Final).

Mr Bridges, the Claimant, is a former Liberal Democrat local politician. He said that the SWP captured and processed his image on two occasions in the course of AFR Locate. As Mr Bridges was not on a watch list, his image was deleted shortly after it was taken. Supported by Liberty, a human rights organisation, Mr Bridges brought an application for judicial review, alleging that the SWP's conduct was unlawful.

He contended that the use of AFR was unlawful for the following three reasons:

- the use of AFR was an interference with his rights under Article 8(1) of the ECHR which provides that everyone "*has the right to respect for his private and family life, his home and his correspondence*". The use of AFR was neither "in accordance with the law" or "necessary" or "proportionate" as required by Article 8(2);
- the use of AFR was contrary to s4(4) DPA 1998 (that personal data may only be processed fairly and lawfully) and s35 DPA 2018 (the processing of personal data for any law enforcement purposes must be lawful and fair). Additionally, that the use of AFR falls within s64(1) DPA 2018 (as this type of processing is likely to result in a high risk to the rights and freedoms of individuals) and therefore a data protection impact assessment must be carried out;
- under s149(1) Equality Act 2010 (where public authorities must, in the exercise of their functions, have due regard to, *inter alia*, the need to eliminate discrimination and the need to foster good relations between different people) the SWP failed to take into account the fact that the use of AFR would result in a disproportionately higher rate of false-positive matches for women and minority ethnic groups. Therefore, the use of the program would indirectly discriminate. Accordingly, the SWP failed to take into account the relevant considerations from s149(1)(a)-(c) of the Act.

SWP argued that the facial recognition cameras helped safeguard the public and prevent crime, but did not infringe the privacy of members of the public whose images were scanned.

The decision

The Court held that Mr. Bridges' Article 8 rights were engaged, even though the surveillance took place in public spaces and Mr. Bridges' image was automatically deleted immediately following the matching exercise. However, the High Court decided that SWP's use of AFR technology, as part of AFR Locate, was lawful because its common law powers to keep the peace and prevent crime gave it the power to deploy AFR, and because there is legislation (such as the GDPR), practice codes (such as the Surveillance Camera Code of Practice), and policy documents which provide standards against which the lawfulness of SWP's use of AFR can be assessed.

Additionally, the high Court held that no less intrusive measure than AFR was reasonably available to the SWP and that the SWP's use of AFR struck a fair balance between the rights of the individual and those of the community.

The High Court also held that there was no evidence that AFR did in fact produce results which were discriminatory in the way alluded to by Mr. Bridges and dismissed the Equality Act 2010 claim.

Why is this important?

The case is important as it highlights that the Court acknowledged that SWP's use of live facial recognition technology did involve the processing of sensitive personal data of members of the public. However, the ruling indicates an element of deference to the police and the overarching objective to keep the peace and prevent crime (the purpose of the AFR Locate project).

It's also important to note that a factor weighing in favour of the High Court's conclusion that SWP's use of AFR was lawful was that the software's decisions as to identification were always reviewed by a human police officer ("*In our view, the fact that human eye is used to ensure that an intervention is justified, is an important safeguard*") (Para. 33)).

Any practical tips?

The police and private organisations should consider existing data protection law and guidance when using live facial recognition technology.

This level of technology is new and intrusive and, if used without appropriate privacy safeguards, could potentially undermine instead of enhance public confidence in the police.

Winter 2019

Data protection – data sharing

ICO draft Data Sharing Code of Practice

The question

What changes does the Information Commissioner's Office (**ICO**) plan to make to the Data Sharing Code of Practice?

The key takeaway

The ICO's consultation on updating the Data Sharing Code of Practice finished in September. While acknowledging that updates are needed to reflect the GDPR and the Data Protection Act (DPA) 2018, the ICO also commented that "*the foundations do not need replacing*". This is a useful steer for organisations in predicting how the finalised updated Code will look.

The background

The Data Sharing Code of Practice was first published in 2011. As such, an update is certainly due, especially following the implementation of the GDPR and the DPA 2018. Indeed, the consultation and any subsequent updates to the Code are actually required under s121 of the DPA 2018.

Before the Code was drafted, in August 2018, the Information Commissioner launched a call for views so people and organisations could help shape the new Code. The ICO published a summary of responses to that call for views. Many of the opinions offered coalesced around the same broad themes:

- Scope: respondents agreed that the Code should be brought up to date;
- Balance: respondents commented on the need to recognise the benefits of sharing personal data and protecting personal data;
- Confidence: there were comments on the dangers of a "*culture of risk aversion*";
- Guidance: respondents asked for more guidance on ad hoc/exceptional types of data sharing;
- Relevance: respondents placed emphasis on the significance of technological developments relevant to their operations.

The stated aim of the draft Code is to "*give* [organisations] *the knowledge and the confidence [they] need to continue sharing data under the GDPR and the DPA*".

The draft Code

The ICO clearly took on board the feedback from respondents. The new Code addresses some common misconceptions about data sharing, namely that data protection should not prevent organisations or people from sharing data.

More broadly, it is clearly a Code for 2019 and beyond. A key piece of advice is to work towards "data protection by design and default". The draft recommends that organisations do this by putting measures in place to:

- implement the data protection principles in an effective manner; and
- safeguard individual rights.

While the draft Code runs to over 100 pages, the general advice seems to be to follow the key principles of the GDPR.

Why is this important?

The current Data Sharing Code of Practice has been a useful tool for organisations seeking to abide by their obligations under the law. However, both the nature of data-sharing and the law around it are changing rapidly and the fact that a new Code is forthcoming is good news.

Any practical tips?

It's important to remember that the Draft Data Sharing Code is just that – a draft. It has not been finalised and the consultation was geared towards hearing and collating a broad range of views. Organisations should remain attuned to further developments, and read and act on the final Data Sharing Code of Practice when it is published.

More widely, organisations should of course have the requisite data protection measures in place already. The ICO's Guide to Data Protection is a useful primer, but for more substantial projects (eg those requiring a Data Protection Impact Assessment (DPIA)), legal advice should almost always be sought.

Winter 2019

Data protection - DSARs

ICO revises guidance on timescales for responding to subject access requests

The question

How long does an organisation have to reply to a data subject access request (**DSAR**)?

The key takeaway

The ICO's guidance has been amended to state that the time limit for a response to a DSAR starts from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month.

The background

Under Article 12(3) of the General Data Protection Regulation (**GDPR**) a data controller must respond to a DSAR "*without undue delay and in any event within one month of receipt of the request*".

If an organisation receives a complex request or a significant number of requests by an individual, the response can be extended by a further two months. However the individual must be provided with an explanation of why the extension is necessary within one month of the receipt of the request.

A DSAR allows an individual to: (1) obtain records of their personal information held by an organisation; (2) be told who their information is disclosed to; and (3) receive an explanation as to why the organisation is holding it. A DSAR can be submitted by letter, email or social media.

The ICO's previous guidance on DSARs noted that the one-month time limit should be calculated from the day after the DSAR is received until the corresponding calendar date in the next month. This meant that if the DSAR was received on 19 August 2019, the response deadline would be 20 September 2019.

The guidance

The ICO's revised guidance states that the time limit for a response to a DSAR starts from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. This means that if the DSAR was received on 19 August 2019, the data controller should respond by 19 September 2019 (not 20 September).

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. For example if you receive a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, you will have until 30 April to comply with the request. If 30 April falls on a weekend, or is a public holiday, you have until the end of the next working day to comply.

If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond. So if a DSAR is received on 25 November, you have until 27 December to respond (25 and 26 December being bank holidays).

Why is this important?

Time is of the essence! It is important that employees are aware of what a DSAR is and how they can pass these requests to the Data Protection Officer or the relevant staff member/ team … immediately!

The revised guidance provides much needed clarity on calculating time with clear examples for organisations to use. This clarity should allow organisations to stay on the right side of the ICO and fulfil the requests of an individual in a timely manner.

Any practical tips?

Remember that the exact number of days you have to comply with a DSAR varies depending on the month in which the request was made. It may be helpful to adopt a 28-day period for responding to a DSAR to ensure compliance is always within a calendar month.

Data controllers should review and update their DSAR policies and procedures to ensure continued compliance with their data protection obligations.

Winter 2019

Data protection – class actions

Landmark judgment in representative data protection action

Lloyd v Google

The question

Is it possible to bring a representative action for a breach of data protection? Can damages be awarded without proof of pecuniary loss or distress?

The key takeaway

Compliance with data protection should be a higher priority than ever. Class actions and damages for loss of control have the potential to make data breaches even more expensive, potentially to a crippling degree.

The background

In May 2017, Mr Richard Lloyd, a former executive director of Which, filed a class action against Google for its use of the so called "Safari Workaround" during 2011 and 2012.

The Safari Workaround circumvented the privacy settings in place on the browser and allowed Google to place a third party cookie on the iPhone of any user that visited a website containing "DoubleClickAd" content. Information on the individual's browsing habits (browser generated information (**BGI**)) would be collected via the cookie. BGI was then sold to third parties, enabling them to target their advertising towards consumers with specific interests or attributes.

Google was fined $22.5m by the United States Federal Trade Commission for its use of the Safari Workaround. Mr Lloyd brought the opt-out class action in the English courts on behalf of approximately 4.4m iPhone users. In order to bring the claim against Delaware-based Google, Mr Lloyd had to obtain permission of the court to serve proceedings out of the jurisdiction.

At first instance, Warby J refused the application. The reasoning for the decision was three-fold:

- the claimants in the representative class had not suffered damage within the meaning of s13 of the Data Protection Act 1998 (**DPA**);

- the claimants did not have the "same interest" for the purpose of CPR 19.6(1) because they were likely to have suffered different types of harm (if any at all);
- Warby J exercised his own discretion under CPR 19.6(2) to prevent the claim from proceeding. He considered it "*officious litigation on behalf of others who have little to gain from it, and have not authorised the pursuit of the claim, nor indicated any concern*".

The decision

The Court of Appeal unanimously overturned the decision of the High Court. The leading judgement was given by Sir Geoffrey Vos.

The Court found that it was possible to award damages for "loss of control" of an individual's data, despite claimants not having suffered pecuniary loss or distress. Whilst data was not property, it had economic value as it had been sold to third parties. Following that reasoning, losing control of your data has a value. In reaching its conclusion, the Court looked to previous case law on loss of control of private information.

The Court ruled that the claimants in the representative class had the same interest. Each had suffered the same harm, as they had experienced loss of control of their data. However, the loss suffered by each in the class was the "lowest common denominator".

In relation to the final point, the Court exercised its discretion and allowed the claim to proceed. The fact that the claimants had not been specifically identified or authorised the claim did not mean that the claim should be halted.

Why is this important?

Google has announced its intention to appeal the decision to the Supreme Court. Given the Court of Appeal's reference to the "lowest common denominator", damages may be minimal even if Mr Lloyd is successful. However, issues of quantum and liability remain to be decided. The eventual outcome of this landmark case is likely to dictate whether we see more attempts to bring representative actions for data protection legislation in the near future.

The decision on damages for loss of control has potential implications for claims under the General Data Protection Regulation (**GDPR**) as well as the DPA. The Court of Appeal referred to the fact that the GDPR specifically mentions loss of control. The introduction of such damages means that in certain cases, claimants will not have to prove loss or distress. The Court found that they would only be available beyond a certain "threshold of seriousness". Future case law is likely to dictate where this threshold is set.

Any practical tips?

Don’t just think fines when it comes to breaches of the GDPR. Representative class actions are becoming a real and present danger to organisations in the UK and to a degree that may eclipse the level of a regulatory fine.

Winter 2019

Data protection – right to be forgotten

CJEU rules on the territorial scope of the "right to be forgotten"

*Google LLC v Commission Nationale de l'informatique et des Libertés (**CNIL**)*

The question

Do online search engines have to apply the "right to be forgotten" globally? Or only to their EU platforms?

The key takeaway

The CJEU has ruled that EU data protection laws do not require the "right to be forgotten" to be applied on a global scale. Instead, in relation to requests for de-referencing, the right is limited in scope to EU search engines only. However, where appropriate, the supervisory authority of an EU Member State may order that non-EU search engines be de-referenced too.

The background

In 2014, the CJEU established the "right to be forgotten" for EU data subjects in *Google Spain SL v Agencia Española de Protección de Datos* (C-131/12), ruling that, when compelled, online search engine operators were to de-reference (ie remove) links to web pages containing the data subject's sensitive personal data.

Since this ruling, Google has received over 845,000 de-referencing requests from EU data subjects, and has acted on around half of these requests.

In 2015 a dispute arose between Google and CNIL, the French privacy regulator. On 21 May 2015, CNIL ordered that, when granting a request for de-referencing, Google must remove links from all versions of its search engine, including those outside the EU. Following Google's refusal to comply with this order - it continued to de-reference links from its EU search engines only – CNIL imposed a public fine of €100,000. Google appealed to the Conseil d'Etat (the French Council of State), which stayed proceedings and referred several questions up to the CJEU. In summary, these were:

- Does the "right to de-referencing" require search engine operators to de-reference all versions of their search engines on a global basis?

- If not, must search engine operators remove links from the full suite of EU search engines, or only the version which corresponds to the Member State in which the request is deemed to have been made?
- Are search engine operators required to use "geo-blocking" to prevent EU users from accessing the complained of links through a non-EU version of their search engine?

The decision

Although the CJEU acknowledged that a de-referencing carried out across all of a search engine's domain names clearly met the objectives which underlie EU data protection law, it ruled that these laws did not provide for the territorial scope of such an exercise to extend beyond the EU. However, to provide EU data subjects with a consistently high level of protection, it was necessary for any de-referencing to be carried out across the entire EU. Further, the CJEU ruled that operators are now obliged to attempt to prevent or at least "seriously discourage" internet users from accessing the links through a search engine's non-EU domain names.

That said, the CJEU noted that its determination was not prohibitive. It noted that the supervisory and judicial authorities in each EU Member State had the prerogative to order that de-referencing be undertaken on a global basis following an appropriate balancing exercise of a data subject's right to privacy and the right to freedom of information.

Why is this important?

The clarification of the territorial scope of the "right to be forgotten" is a welcome development for search engine operators. Since the right was enshrined in 2014, privacy regulators have had to grapple with whether or not to extend the right to non-EU search engines and, unsurprisingly, this has led to complications/disputes where regulators have tried to apply the right globally.

However, the CJEU's ruling will have a significant impact upon data subjects seeking to take advantage of their "right to de-referencing". The default position now means that, unless the relevant supervisory or judicial authority orders otherwise, links to pages displaying their personal data will remain accessible outside the EU (and, notably, within the EU if internet users use a virtual private network to circumvent any restrictions imposed).

Any practical tips?

It remains unclear how this ruling will be implemented in each Member State but search engine operators would be advised to listen to the CJEU's emphasis on practical steps to help ensure internet users cannot easily access their non-EU domains as the CJEU said search engine operators should "where necessary" take measures to "effectively present or, at the very least , discourage" users from such access, which must in turn mean considerable focus on geo-blocking.

Winter 2019

Data protection – right to be forgotten

Striking the balance between the RTBF and substantial public interest

*GC, AF, BH, ED v CNIL Case C-136/17 GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (**CNIL**)*

The question

What is the current balancing test for the right to be forgotten as against rights to access information and freedom of expression?

The key takeaway

The Court of Justice of the European Union (**CJEU**) has provided guidance and criteria to be followed by search engine operators when balancing requests by individuals to de-reference search engine results linking to their sensitive personal data with the public's right to access information and publishers' rights to freedom of expression.

The background

Four individuals made requests for the removal of certain links to web pages included in the Google search engine results when searching their names. The links contained sensitive personal information including details of an intimate relationship between a female politician and a mayor, a reference to the PR officer of the church of scientology at a time when a member committed suicide, a judicial investigation into political party funding and a prison sentence for child sexual assaults. When their requests were refused, the individuals complained to the French Data Protection Authority, the Commission Nationale de L'informatique et des Libertés (**CNIL**), but the CNIL refused to grant an order that the links should be de-referenced.

The individuals pursued legal action against the CNIL and the French courts requested clarification from the CJEU on the interpretation of EU data protection directives and the leading case *(case C-131/12)* on the scope of the right to be forgotten.

CJEU decision

The CJEU confirmed that, in circumstances where a supervisory body is asked to verify the operator's response to a de-referencing request, search engine operators are subject to data controller obligations and are therefore required (subject to national rules) to accede to de-referencing requests to remove links to web pages containing sensitive personal data.

However, this obligation is subject to certain exceptions which may justify the refusal to de-reference, for example that the information is of "substantial public interest" or was "manifestly made public by the data subject".

These exceptions are subject to a careful balancing act. Although the CJEU confirmed that the right to privacy will generally override the public's right to information, the following criteria should be considered to determine whether, in those particular circumstances, the substantial public interest in accessing the information should prevail:

- what is the "substantial public interest" in referencing the personal information (e.g. does the individual hold a public role)?
- how sensitive is the information and how will publication interfere with the individual's private life?
- whether it is "strictly necessary" to refer to the individual in order to protect freedom of information of internet users potentially interested in accessing that web page?
- whether the information is accurate, complete and current at the time of the request (in particular, search engines should consider whether the information is outdated by the time of the request and, in any event, should adjust results to prioritise links that refer to the most current state of affairs)?
- in respect of information relating to legal proceedings, matters such as the seriousness of the offence, past conduct and the progress and outcome of the proceedings should be taken into account.

In respect of data manifestly made public by the individual, refusal to de-reference will be justified provided that it is lawful and there are no other compelling grounds to comply with the request.

The CJEU commented that on these facts it would be inclined to grant some of the de-referencing requests on the basis that the information was outdated, some information was particularly sensitive and intimate and the individuals were no longer in public roles.

Why is this important?

This CJEU ruling helps confirm the requirements for de-referencing requests relating to special category personal data on search engines. As such, when considering these requests, search engine operators are required to carry out a balancing exercise between the individual's right to be forgotten against the right of the public to access the information and the publisher's right to freedom of expression.

Although this exercise could be seen to place a more onerous burden on search engine providers, the CJEU's criteria does provide clarity in respect of when the public interest will

outweigh the right to be forgotten and sets parameters around where an individual's right to have links removed can be justifiably denied (e.g. where reference to the individual is strictly necessary for protection of the freedom of information of internet users potentially interested in accessing that web page).

Any practical tips?

Search engine operators should adapt their de-referencing request consideration processes to take into account the CJEU's criteria to ensure that the balancing exercise between the right to be forgotten and the freedoms of information and expression is properly carried out.

Winter 2019

Data protection – cookies

CJEU rules out opt-out consent for cookies

Planet49 GmbH v Bundesverban der Vebraucherzentralen

The question

Can you use pre-ticked boxes for cookie consent?

The key takeaway

The recent judgment in *Planet49 GmbH v Bundesverband der Verbraucherzentralen* has important implications for online businesses. Previously, when website users were asked if they consented to the cookies on a site, if a pre-ticked box was offered and the user did not object, this passed for consent.

However, the recent judgment in the *Planet49* case runs counter to this. As per Article 13 of the GDPR, consent must be "freely given, specific, informed and unambiguous" and according to the CJEU, pre-ticked boxes cannot fall under this definition.

The relevant provisions

The following key sections were referred to and developed in this case:

- Directive 95/46 – which states that 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'
- Directive 2002/58
  - Article 2(f) - "consent" by a user or subscriber corresponds to the data subject's consent in Directive [95/46]
  - Article 5(3) – "*Member States shall ensure that the storing of information, or the gaining of access to information already stored… is only allowed on condition that the subscriber or user concerned has given his or her consent*"
- GDPR (Regulation 2016/679)
  - Article 6(1)(a) – "*processing shall be lawful only if… the data subject has given consent*".

The background

In September 2013, German company "Planet49" ran an online lottery on one of its sites. Users of the site were "confronted" with two tick-boxes relating to the installation of cookies

which had to be filled in to take part in the competition. One of these was “pre-ticked”, meaning that if the user did not object, then they could “consent” by simply clicking through.

The Federation of Consumer Organisations in Germany brought proceedings against Planet49 in an attempt to get an injunction to have the declarations removed. The Federation argued that using such declarations could not constitute true consent.

Following the initial action and an appeal, the Federal Court of Justice in Germany stayed proceedings and referred the below (abridged) questions to the CJEU:

- 1a) Is valid consent (within the meaning of Article 5(3) and Article 2(f) of Directive [2002/58] read in conjunction with Article 2(h) of Directive [95/46]) permitted by way of a pre-checked box which the user must deselect to refuse their consent?
- 1b) For the purposes of Article 5(3) and Article 2(f) of Directive [2002/58], does it make a difference whether the information stored or accessed constitutes personal data?
- 1c) In the circumstances around 1(a), does valid consent within the meaning of Article 6(1)(a) of Regulation [2016/679] exist?
- 2) What information does the service provider have to give within the scope of the provision of clear and comprehensive information?

The decision

The Grand Chamber ruled as follows:

- “*Consent referred to in those provisions is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user’s terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent*”.
- “*The information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies*”.

Why is this important?

The judgment in this case is unsurprising if one reads the GDPR or the ICO’s own guidance on cookies. However, it is an important reminder of the increasingly dim view authorities will take on organisations who do not enable customers to “fully consent” to how their data is being collected or used.

Any practical tips?

The most practical advice would be for online businesses operating in the EU to follow the judgment in the *Planet49* case to get valid “freely-informed consent” from their users.

When it comes to cookies, do not use pre-ticked checkboxes if trying to get consent. Also, be sure to provide your users with the requisite information on the duration, operation and third party access status of the cookies.

Finally, don't forget to keep an eye on the progress of the e-Privacy Regulation. With a ban on “cookie walls” and a heightened focus on cookie consent, this will be a huge shake up for the digital ad space.

Winter 2019

Data protection - cookies

ICO guidance on the use of cookies and similar technologies

The question

Can implied consent be relied on for the use of cookies? Or, in the words of the ICO's blog, "what does 'good' look like?"

The key takeaway

If you use cookies you must (1) tell people if you set cookies, (2) explain what cookies do and (3) obtain the user's consent (which must be actively and clearly given).

The background

The guidance addresses cookies and similar technologies in detail and is intended to provide an in-depth understanding of how the Privacy and Electronic Communications Regulations (**PECR**) applies to the use of cookies. The guidance also provides clarity and certainty around the interplay between the General Data Protection Regulation (**GDPR**) and the PECR cookie requirements.

The guidance

The new guidance highlights the following:

- implied consent is no longer acceptable (eg consent implied from the continued use of the website);
- online advertising cookies require consent (a consent mechanism should allow a user to make a choice, this includes all third-party cookies used in online advertising);
- you should not emphasize the "agree" or "allow" cookie options over the "reject" or "block" cookie options;
- if an organisation uses any third party cookies, it must clearly and specifically name who the third parties are and explain what they will do with the information;
- do not use any pre-ticked boxes (or equivalents such as "on" sliders) for non-essential cookies;
- "cookie walls" which block general access to a website if consent is not provided do not constitute valid consent;
- the ICO's position remains that cookie consent should be separate from other matters, and should not be bundled into terms and conditions or into privacy notices.

Why is this important?

The guidance confirms that the rules on cookies will continue to be enforced by the ICO under the PECR regime (where the maximum fine is £500,000), except where personal data is processed - in which case it would also be open to the ICO to use its enhanced powers under the GDPR (where the maximum is €20m, or 4% of annual global turnover – whichever is greater).

The ICO has indicated that it intends to take a risk-based approach and states in the guidance that it is unlikely to prioritise enforcement action in relation to cookies where there is a low level of intrusiveness and a low risk of harm to individuals. It may consider taking action where an organisation refuses to take steps to comply, or uses privacy-intrusive cookies without taking adequate steps to provide the requisite information and secure valid consent.

Any practical tips?

Think about running a cookie audit! This includes looking at your cookie notices and cookie policy with fresh eyes (or rather through the eyes of the ICO's new guidance).

Winter 2019

Data protection – cookies

Major finance, retail and media companies targeted in Irish "cookie" sweep

The question

How does the Irish Data Protection Commission (**DPC**) monitor whether websites are compliant with data protection law?

The key takeaway

If your website contains non-essential cookies, ensure that you obtain valid consent from users.

The background

The DPC is undertaking a review of websites accessed by Irish consumers. Its review focuses primarily on ensuring that the use of "cookies" and other "plug-ins" is compliant with data protection law.

The DPC is assessing the compliance of certain websites with the ePrivacy Regulations and the General Data Protection Regulation (**GDPR**). In particular, the DPC is focusing on whether valid consent for the use of cookies has been obtained from consumers.

The review will initially focus on a limited number of websites (the full details of which have not yet been disclosed), although the DPC has stated that the review may subsequently be extended.

The guidance

A cookie is a small file which holds data about websites visited by users. Cookies have a range of functions: some are essential to access a website, whilst others are non-essential (for example, they might collect data for targeted advertising). In order to use a non-essential cookie it is necessary to obtain the consent of the user.

When cookies collect personal data, the e-Privacy Regulations and GDPR are to be read in conjunction. This means recognising the higher standard of consent. The consent given by the user must be freely given, informed, clear, unambiguous and demonstrated by an affirmative act.

Why is this important?

The DPC has stated that it may conduct formal probes into issues identified during its review. Fines under the GDPR can be up to the greater of 4% of global annual turnover or €20m. Whether you are operating your website in Ireland or elsewhere in the European Union, the requirements in place are the same.

Any practical tips?

If your website uses non-essential cookies, make sure that you obtain valid consent. Whilst it is the Irish regulator that is currently looking into this issue, these standards also apply in the UK and across the EU. Practically, the steps to take include:

- providing a clear explanation of the function of the cookies – language should be non-technical and give details of how any information collected is going to be used;
- avoiding pre-ticked boxes, which aren't sufficient to demonstrate affirmative and unambiguous consent;
- ensuring that users who do not consent to non-essential cookies are still able to access the website;
- setting your webpage up in a way that makes it easy for users to withdraw their consent. This might mean making the original consent form accessible and amendable or providing another simple and obvious route for the user to withdraw his or her consent.

Winter 2019

Consumer

New statutory redemption period for Irish gift vouchers

Irish Consumer Protection (Gift Vouchers) Act 2019

The question

What is the new minimum expiry date for all gift vouchers in Ireland?

The key takeaway

Under the Consumer Protection (Gift Vouchers) Act 2019 (the **Act**), there is now a minimum five year expiry date for all gift vouchers in Ireland. All gift vouchers sold after 2 December 2019 will be caught by the new law (including all current gift vouchers unsold at that date) and therefore subject to the new five year minimum redemption period.

The background

The Act amends the Consumer Protection Act 2007. Before its introduction there was no specific legislation dealing with gift vouchers in Ireland. Retailers were free to determine the expiry dates, some lasting as little as three months on popular gift choices.

The development

According to the Act:

- all gift vouchers must have a minimum five year expiry date and the expiry date must be clearly communicated to the consumer;
- traders are prohibited from requiring that a voucher is spent all in one single transaction (providing there is more than €1 left on the voucher);
- if the voucher contains an expiry date, this date must be specified on the voucher;
- the remaining balance of a gift voucher shall be reimbursed either in cash or another gift voucher;
- if, say, an existing two year voucher is partially redeemed, and the remaining amount is issued on a new gift voucher, then that gift voucher will be subject to the five year expiry period. If the partially redeemed vouchers are not issued as new vouchers, they will not be subject to the five year expiry period;
- a gift voucher contract is not allowed to limit the number of gift vouchers that a person is allowed to redeem in one transaction;

- where a gift voucher contract contains a provision for how a gift voucher can be replaced if it is lost or stolen, then the replacement gift voucher must not expire before the date of the original gift voucher.

Why is this important?

As the Irish Minister for Business, Enterprise and Innovation said "*part of the problem is the great variation on expiry dates which can range from as little as six months to 12 months to 24 months. This often leads to confusion amongst consumers*". The Act changes all this by introducing consistency of redemption periods in Ireland.

Any practical tips?

There is no "reasonable period" afforded to businesses to phase out gift vouchers with durations of less than five years that have not yet been sold. All unsold gift vouchers (ie in print, in stock or instore) as at or after 29 November 2019 will be subject to the new five year minimum redemption period. If you are issuing gift cards in Ireland, you will need to get busy – both in introducing the new redemption period (and all accompanying drafting) and training your staff to be able to deal with customer queries over their redemption rights.

Winter 2019

Confidentiality

ASA seeks injunction for email sent to wrong recipient

ASA v Robert Neil Whyte Mitchell

The question

Is it possible to obtain an injunction to restrain the use or disclosure of confidential information contained in emails accidentally sent to the wrong recipient? Also, is correspondence relating to ASA complaints confidential?

The key takeaway

The case reiterates the questions that the court will ask when deciding whether to grant a prohibitory injunction in breach of confidence situations, namely whether there is a sufficient threat or risk of the respondent carrying out the acts which the injunction would prohibit and whether the applicant was more likely than not to establish at trial that publication should not be allowed. It also helpfully confirms the confidential nature of ASA complaints, and reminds us all of the dangers of email autofill!

The facts

An ASA investigating officer was dealing with a complaint about a billboard advertisement attacking the record of the Royal Bank of Scotland. The ad was apparently funded by the defendant Robert Mitchell. The investigating officer accidentally sent an email and attachments relating to the complaint (including legal advice) to Mr Mitchell. Mr Mitchell was repeatedly asked to delete the emails due to their confidential nature but did not do so.

The ASA issued an application for interim injunction prohibiting Mr Mitchell from using, publishing, communicating or disclosing the email, attachments and information derived from them on the grounds that their contents were confidential and partly legally privileged. Mr Mitchell refused to attend the resulting hearing on the basis that he was not domiciled in England and Wales.

The decision

The judge granted the ASA's application as there was a sufficient threat or risk that Mr Mitchell would, unless restrained, carry out the acts which the injunction would prohibit and that the ASA was "more likely than not" to establish at trial that publication should not be allowed.

In terms of breach of confidence, the judge explained that documents and correspondence relating to ASA complaints were confidential by nature, as complaints required anonymity to avoid “the chilling effect” of publicity. Moreover, disclosure of complaints information would be harmful to the public interest as confidentiality in ASA processes is required to prevent advertisers from gaining an undesirable insight into the private thinking of their regulator.

As for the jurisdiction point, the judge was satisfied that all practical steps had been taken by the ASA to notify Mr Mitchell of the application as required by s12(2) of the Human Rights Act 1998, therefore the court was able to grant relief with Mr Mitchell not being present or represented.

Why is this important?

The case provides a useful justification for why ASA correspondence relating to investigations into complaints is confidential and why it is strongly in the public interest to uphold their confidentiality.

Any practical tips?

Staff should be warned of the potential implications of sending unencrypted confidential information by email and be advised of protocols to ensure the security of correspondence and to minimise the risks.

Above all, be wary of the email address autofill when sending emails! Remember, injunctions don’t come cheap.

Winter 2019

Online platforms

Memorandum of Understanding on online advertising and intellectual property to continue

The question

What steps is the advertising industry taking to minimise the placement of advertising on IPR-infringing websites?

The key takeaway

The signatory businesses and associations to the Memorandum of Understanding (**MoU**) have agreed that the MoU has contributed to the minimisation of placement of advertising on IPR-infringing websites and mobile applications that infringe copyright or disseminate counterfeit goods. It will continue in effect, with new signatories joining the initiative.

The background

The MoU came into effect on 25 July 2018. It included commitments not only to minimise the placement of advertising on infringing sites and apps, but also to remove advertising if the advertiser (or those who place advertising for others) became aware that it is on such a site or app.

A variety of parties signed up to the MoU which included advertisers, advertising agencies, trading desks, advertising platforms, advertising networks, advertising exchanges for publishers, sales houses, publishers and intellectual property owners, as well as representatives and associations of these groups.

The signatories that are directly involved in buying, selling or brokering the sale or purchase of advertising space also agreed to include provisions in their contracts with advertisers and other media buyers to ensure that ads were not placed on inappropriate sites and apps.

Why is this important?

At the end of a 12-month assessment period, the parties evaluated the effectiveness of the MoU under four headings:

- strengthening intellectual property rights protection;
- reducing the harm caused by intellectual property rights infringement;
- upholding fundamental rights; and
- ensuring fair competition.

The MoU was found to have contributed to minimising the placement of advertising on intellectual property-infringing websites and mobile applications. The parties agreed that they will continue to exchange and promote good practice, and develop further new initiatives (eg on technology and tools) and actions to be taken under the “follow the money” approach to intellectual property rights enforcement.

Any practical tips?

Consider bringing your business into line with the MoU by seeking to keep to a minimum any advertising on websites and mobile phone applications that infringe copyright or disseminate counterfeit goods.

The MoU is also now open for new signatories and companies, and trade associations involved in the digital advertising supply chain are strongly encouraged to join the MoU.

Winter 2019

Online platforms

Obligations to remove content

Eva Glawischnig-Piesczek v Facebook Ireland Ltd, Case C-18/18

The question

Can an online platform/host provider be required to remove identical or "equivalent" content that has previously been declared as an illegal post?

The key takeaway

A Member State can require an online platform to remove content that is identical or "equivalent" to content that has already been found to be illegal.

The background

In April 2016, a Facebook user posted on their personal page with an article about Eva Glawischnig-Piesczek, a member and chair of the Austrian green party. The Facebook post also included a thumbnail of the article consisting of a short description of the article and a picture of Ms Glawischnig-Piesczek, and a comment from the user about the article. This comment was found to be defamatory by the Austrian court and as a result Ms Glawischnig-Piesczek asked Facebook that it delete the comment. Facebook refused.

As a result, Ms Glawischnig-Piesczek issued a claim against Facebook and in December 2016, the Viennese Commercial Court awarded an interim injunction in Ms Glawischnig-Piesczek's favour stipulating that Facebook must stop sharing photos of Ms Glawischnig-Piesczek with identical or "equivalent" accompanying text (and that Facebook had to remove the original defamatory post). This was appealed to the Higher Regional Court of Vienna who upheld the judgment, but found that Facebook would only need to prevent the dissemination of "equivalent" content if they had been informed by Ms Glawischnig-Piesczek or another source. This judgment did not satisfy either party who both appealed to the Austrian Supreme Court, who subsequently referred the following questions to the CJEU regarding the E-commerce Directive (the **Directive**):

- Does Article 15(1) of the Directive prevent a Member State from ordering a host provider to take down content that has previously been declared as illegal and other "identically worded items of information"?
- If not, does this also apply in each case for information with an equivalent meaning?
- Is the territorial scope of an order of a Member State limited?

- Does this also apply for information with an equivalent meaning as soon as the operator has become aware of this circumstance?

The decision

The CJEU replied accordingly:

- The Directive does not prevent a Member State from requiring removal of content that has been formerly declared illegal.

The CJEU considered that the speed with which information is shared on the internet means that illegal content could be shared and replicated with ease and so it was reasonable for a Member State to be able to remove access to such identical information. Further, in accordance with the Directive, the CJEU held that (as Article 15(1) stipulates), requiring such removal would not impose on providers a general obligation to monitor.

- "Equivalent" content should be covered by the injunction.

The CJEU recognised that, as statements were held to be defamatory because of their overall meaning rather than the specific words used, an injunction should cover content that conveys the same underlying message (even if the words are not identical). However, so as not to impose too heavy a burden on host providers to search for content, "equivalent" content must contain specific features of the infringing comment such as the named individual, and the post must be such that there is no need to be carry out an independent assessment of the content. Given the technological capabilities of Facebook, it was held that the burden would not be too onerous.

- There is no limitation on territorial scope.

The CJEU found that, subject to international law, Member States can make enforceable worldwide orders.

- Given the answers to questions 1 and 2, the CJEU did not respond to the 4th question as being informed of the "equivalent" content would not impose a general obligation to monitor (under s15(1)).

Why is this important?

From an online platform/host provider's perspective, the CJEU judgment highlights the current drive towards greater regulation of online platforms/content. The ruling attempts to balance the burden placed on host providers to search for replicated illegal content with the need to protect individual's rights. However, requiring host providers to take down "equivalent" content could

be difficult as it may require human judgement, rather than just advanced search tools. With regards to applying worldwide search orders, it will be interesting to see how these global injunctions work in practice and whether countries with broad censoring policies will take advantage of this to try and prevent news spreading abroad.

Any practical tips?

The CJEU ruling does not impose an obligation on host providers to monitor for illegal content, but the providers should be aware of their obligations once illegal content has been flagged to them. Further, the providers should set up processes to identify and remove identical and "equivalent" material to content that they have already removed.

Winter 2019

ASA – influencer marketing

ASA ruling on contractual relations – Brooks Brothers

The question

Can a post by an influencer be deemed to be an ad, even when the post is at the influencer's own initiative and to his own followers, and not at the direct request of the relevant brand?

The key takeaway

Even where a post is organic (ie at the initiative of the influencer), beware of any contractual relationships which may already be in play with the brand. This will likely tip the post into being a marketing communication.

The ad

An Instagram post by fashion influencer Matthew Zorpas, posted in March, featured an image of himself being measured for a suit, accompanied by text which stated "*A man in a well Made to Measure suit will always have a better attitude. Get 25% off your #madetomeasure experience at @brooksbrothers.unitedkingdom in Regent Street until March 31st*", followed by various hashtags.

The complaint

The complainant challenged whether the post was obviously identifiable as a marketing communication.

The response

Brooks Brothers confirmed that although it had a contractual agreement with Matthew, the post in question was in fact an organic post and not sponsored by Brooks Brothers in any way. Brooks Brothers provided copies of various other Instagram posts by Matthew which were paid sponsored posts and compared it with the post in question. Matthew also stated that the Brooks Brothers post in question was an offer that he shared with his followers, rather than paid for by the brand.

The decision

The ASA understood that Matthew was contracted to post a minimum number of stories across his social media networks as part of his financial agreement with Brooks Brothers. The ASA noted from the agreement that specific hashtags were to be used for each month in which the content was posted, coupled with the "Paid Partnership" and "advertised by brooksbrothers.unitedkingdom" labels, which were included in previous posts by Matthew. The

influencer had used the hashtags that were stipulated in the agreement for the month of March to promote the “Made to Measure” campaign and the influencer had tagged the brand in the image and caption.

By virtue of the contractual agreement, the ASA concluded that Brooks Brothers had sufficient control over the content of the post for it to be considered a marketing communication and therefore falling within the remit of the CAP Code. Brooks Brothers were therefore found to be jointly responsible for ensuring that promotional posts by Matthew were compliant with the CAP Code. Even though the post was at the influencer’s own initiative, it reflected commercial arrangements with the brand. As such, the post was always at risk of being considered an ad, regardless of the fact that it was an organic one without boosted distribution. There was nothing in its content, such as “#ad” placed upfront, that made it clear that it was an ad.

Why is this important?

The CAP Code states that marketing communications must be obviously identifiable and must make clear their commercial intent, if it’s not obvious from the context. The ASA is committed to achieving transparency in this area, and will almost always view a contractual arrangement with an influencer (even if not directly connected to the post in question), as evidence of a form of editorial control over the posts of that influencer.

Any practical tips?

Actively monitor your influencers! Even though Matthew Zorpas made the post at his own initiative, this was still deemed to be under Brooks Brothers’ control by virtue of the contractual arrangement they had with him. Active monitoring of his social media activities (eg by someone in the branding team “following” him”) might well have caught this before it became an issue by a simple request to mark all his posts for Brooks Brothers with #ad.

Winter 2019

ASA – influencer marketing

ASA ruling on "#brand ambassador" – Cocoa Brown

The question

Does the use of "#brand ambassador" in an Instagram caption make the post easily identifiable as an ad?

The key takeaway

According to the ASA, the term "#brand ambassador" is not sufficient to identify a post as an ad. In order to comply with the CAP Code rules on recognition of marketing communications, the ASA requires a clear, prominent identifier such as the term "#ad" in content that comes under the marketing communications umbrella.

The ad

An Instagram post on TV personality Olivia Buckland's page, seen on 12 February 2019, featured an image of Olivia holding a pink bottle with the logo "CB" visible on it.

The visible caption on the post stated "*The V-Day prep is well underway and I'm topping up my tan with my fave @cocoabrowntan by @marissacarter 1 HOUR TAN MOUSSE … more*". Once the caption was clicked on, additional text stated "*Original –it gives me such a natural glow with no streaks and is the perfect accessory for date night with bae [heart eye emoji] Get yours now @superdrug #TeamCB #CocoaBrownTan #ValentinesDay #BrandAmbassador*".

The complaint

The complainant challenged whether the post was obviously identifiable as a marketing communication.

The response

Cocoa Brown said they advised Olivia that "#ad" should be used on all future posts on Instagram. Olivia Buckland said that "#brand ambassador" was used on the post, in addition to her Instagram Bio. Olivia provided a dictionary definition of a "brand ambassador" as "*a person who is paid or given free products by a company in exchange for wearing or using its products and trying to encourage others to do so*" and stated that she believed this made clear that some of her posts were marketing communications.

The decision

The ASA understood that as a "brand ambassador" for Cocoa Brown, Olivia Buckland was paid to market their products, and that Cocoa Brown had some control over any content she produced in relation to their products. The ASA therefore concluded the post was a marketing communication which fell within its remit.

The ASA considered whether the post was obviously identifiable as a marketing communication. The ASA held that the inclusion of the term "#brand ambassador" in Ms Buckland's Instagram bio was unlikely to be seen by Instagram users at the point they were viewing individual advertising posts and as such this was insufficiently prominent to ensure that individual posts were each obviously identifiable as ads.

While the term "brand ambassador" was likely to suggest to readers a general relationship with the brand, the ASA considered that it was unlikely to convey that Cocoa Brown had both paid for and had a level of control over the content of the post.

Additionally, the ASA then assessed the post as it would have appeared in-feed and considered that there was nothing in its content, such as "#ad" placed upfront, that made clear to those viewing it that it was an ad.

The ASA upheld the complaint that the post was not obviously identifiable as a marketing communication and breached CAP Code rules 2.1 and 2.4 (recognition of marketing communications).

Why is this important?

The term "#brand ambassador" is not sufficient to differentiate between posts that are marketing communications and those that are not. The recent rulings by the ASA indicate that the term "#ad" (or "advert", "advertising" or "advertisement") is the only sufficiently clear identifier for marketing communications.

Any practical tips?

The term "#brand ambassador" can still be used within a caption of a post or bio. However, if you want an influencer to be a "brand ambassador", any paid-for-posts (or any other content that would be considered a marketing communication) must also include the term "#ad" and this must be placed prominently within the caption (prominently being upfront rather than in a bio or a click away caption).

Winter 2019

ASA – influencer marketing

What is the right # to use when labelling an ad?

The question

What is best, and worst, practice in labelling a post as an ad?

The key takeaway

The ASA and CMA have clarified what they are looking for in ad disclosures. They have also given practical tips to brands to ensure that their influencers obey the rules.

The guidance

In order to comply with ad disclosure requirements under the CAP Code the ad "must be obviously identifiable as such". If not already apparent from the context of the ad itself, this essentially means including an appropriately worded and prominently placed label. In a recent training seminar (October 2019) the ASA and CMA gave the following advice:

The following labels are **always** acceptable:

- Ad, #Ad
- Advert
- Advertising, and
- Advertisement.

The following are **sometimes** acceptable, but only in particular circumstances:

- Paid Promotion
- Brand Ambassador
- Free gift from [brand], or
- On loan from [brand].

The following are **risky**:

- Sponsored
- Gifted, #gifted
- Affiliate.

The following should **not** be used:

- Spon, #Sp
- Brought to you by …
- In collaboration with …
- Thanks to [brand], or
- #client.

Why is this important?

The regulators are firming up on the #tags which they find acceptable. Essentially, though, the mantra stays the same – if in doubt and there's a whiff of editorial control (in any form), use #ad.

Any practical tips?

If you are an organisation working with an influencer it is best practice to:

- keep records of all the influencers you have gifted products to;
- provide clear guidance to influencers on what is expected of them in terms of adequate disclosure;
- ensure that there is a clear obligation on the influencer to properly disclose, as a term in the contract (if there is one); and
- actively monitor the social channels of those influencers to check that they are complying.

Also, watch out for content being created in your brand's name or on your brand's behalf. The CMA seems to be moving to a position where the brand is responsible for compliance. If this bears out, then active monitoring should be a critical component of your compliance processes.

Finally, if you are working with an international influencer on a global campaign that isn't specifically targeted at the UK, but the influencer has UK followers, it is worth noting the following:

- there is no minimum number/percentage of UK followers that the influencer must have before the ASA/CMA would consider it to be within their remit; and
- the key question is whether the marketing communication is directed to a UK audience – linking through to a UK webpage or having pricing in pounds will indicate that it is directed at a UK audience. If these factors are not present, it does not mean that the post has not been directed to a UK audience.

Winter 2019

ASA – social responsibility

ASA ruling on "humorous" tweets – Burger King

The question

How careful do you need to be when using topical events to let loose a branded tweet? Put another way, was the combination of Nigel Farage, "milkshaking" and "#justsaying" a responsible tweet by Burger King?

The key takeaway

Be cautious! Before attempting to go public with a "humorous" tweet or ad on current affairs, assess the social impact that it may have and consider whether it will breach any of the rules in the CAP Code.

The ad

A tweet sent by the official Burger King twitter account on 18 May 2019, included the text, "*Dear people of Scotland. We're selling milkshakes all weekend. Have fun. Love BK. #justsaying*". Before the tweet was deleted it had received over 19,000 retweets and 108,000 likes.

In May 2019 a McDonald's Restaurant in Edinburgh chose not to sell milkshakes amid concerns that people were buying them to throw at Brexit Party leader Nigel Farage, who was holding a rally in the city. McDonald's had made this decision as Farage had been hit by a milkshake during a rally in Newcastle a few days earlier.

The response

The tweet received 24 complaints. The complainants challenged whether the ad was irresponsible, offensive and encouraged violence and anti-social behaviour.

Burger King responded that the tweet was intended to be a tongue-in-cheek reaction to recent events where milkshakes had been thrown at political figures.

Burger King stated that it did not endorse violence and that was made clear with a follow-up tweet that stated, "*We'd never endorse violence – or wasting our delicious milkshakes! So enjoy the weekend and please drink responsibly people*".

A Burger King spokesman said: "*It appears some have misinterpreted this as an endorsement of violence, which we absolutely reject. At Burger King, we totally believe in individuals' right to*

freedom of expression and would never do anything that conflicts with this. We'd never endorse violence or wasting our delicious milkshakes".

The decision

The ASA upheld the complaints and banned the ad.

It considered that the ad was likely to be seen as a reference to the recent incidents of "milkshaking" political figures. Despite the intention being a humorous response to the suspension of milkshake sales by Burger King's competitor (McDonald's), the ASA considered that the tweet could be understood as suggesting that Burger King milkshakes could be used to "milkshake" Nigel Farage.

The "milkshaking" incidents had been widely reported in the media and there was a fear by the ASA that those who saw the tweet were likely to be aware that Nigel Farage was due to make more public appearances in Scotland that weekend.

The ASA believed that the ad condoned the previous anti-social behaviour and encouraged further instances. Therefore it held that the ad was irresponsible, offensive and encouraged violence and anti-social behaviour and breached CAP Code Rules 1.3 and 4.4.

Why is this important?

Engaging with audiences and responding to current affairs is an important part of a modern communications strategy. This decision reminds organisations to take particular care when responding to current affairs and that what is humorous to one person may easily be seen as irresponsible and anti-social by another.

Any practical tips?

In our fast-moving, digital age it is tempting to take a quick, topical and humorous dig at a competitor or use real-time developments in the news to reach a vast social media audience. But tread carefully – you have to sit back and coldly work through all the potential interpretations, especially ones that can portray your brand in an irresponsible or anti-social light. Best to loop in your legal team – not because they won't have a sense of humour (!), but because it's their job to take a more measured view of the potential repercussions.

Winter 2019

ASA – social responsibility

ASA ruling on phrases which may have a sexual connotation – Boohoo.com

The question

How easy is it for a campaign to be deemed "socially irresponsible" where it refers to a phrase which could possibly have a sexual connotation?

The key takeaway

Even if a word could be used in a legitimate (here, fashion) context, brands have to be extremely careful that the message cannot be interpreted in a socially irresponsible way. This is particularly the case where a young audience is involved.

The ad

A marketing email from Boohoo, received on 15 July 2019, featured the subject heading "Send Nudes [eyes emoji]". The body of the email contained a photo of a female model wearing a beige jacket with the words "*Send nudes. Set the tone with new season hues*" written across the image.

The complaint

The complainant challenged whether the reference to "send nudes" was socially irresponsible.

The response

Boohoo.com UK Ltd said that their use of the word "nude" was solely to describe the colour resembling that of the wearer's skin. They said they targeted their customers by sending them the latest fashion trends, including the trend for "nude" colours. They said that the word was widely used by other retailers in relation to apparel. The Boohoo brand targeted customers aged 16 to 24 years old. To sign up to Boohoo's website, the terms of use stipulated that the individual must be at least 18 years of age. The ad was sent to individuals who had agreed to Boohoo's terms of use. It should not have been sent to any individual under 16 years of age.

The decision

The ASA upheld the complaint.

It acknowledged that the term "nude" was commonly described to refer to colours that were similar to some people's skin tones. However, at the same time, the phrase "send nudes" was likely to be understood as referring to requests for sexual photos, which could be a form of

sexual harassment. The ASA also noted that an increased pressure to share such photos has been linked to negative outcomes for young people.

Boohoo's target market was aged 16 to 24. The ad had only been sent to those who self-declared that they were over 18. However, given the general price point of Boohoo's clothing and the age of the target market, there was also likely to be some overlap with even younger teenagers who aspired to looks associated with a slightly older age group. The ASA acknowledged that the ad was playing on a well-known phrase to highlight a fashion trend, but considered the specific reference chosen had the effect of making light of a potentially harmful social trend. Furthermore, the subject heading "send nudes" in the email, without any further context, was likely to be disconcerting for some recipients, particularly those who might have personal experience of being asked to "send nudes".

In the context of an ad aimed at a relatively young audience who were more likely to be harmfully affected by pressure to share sexual images of themselves, the ASA held that the reference to "send nudes" was socially irresponsible and breached the CAP Code (Edition 12) Rules 1.3 (Social responsibility) and 5.1 (Children).

Why is this important?

This decision highlights that brands, especially brands which have a relatively young audience, will be coming under increasing pressure to prepare ads in a responsible way and must take particular care to avoid causing potential harm to children/young people.

Any practical tips?

In order to determine whether an ad or promotion is irresponsible, the ASA will be taking into account the medium and context in which an ad appears, the product being advertised and the audience that's likely to see it as well as continuing to monitor the prevailing standards in society. Retailers and brands should take this and other recent ASA rulings into consideration and adapt accordingly.

Winter 2019

ASA – social responsibility

ASA ruling on Imperial Tobacco

The question

When can e-cigarette advertisers encourage "new" users of their products?

The key takeaway

E-cigarette advertisers should make clear that ads are for the attention of existing smokers or nicotine-users and ensure that this message is also clearly depicted in associated headline claims or dialogue.

The background

Imperial Tobacco Ltd t/a Blu advertised its Blu e-cigarettes using three outdoor posters:

- a drawn female character wearing sunglasses and holding an e-cigarette with the headline "*I blu do you?*" alongside the claim "*NEW MYBLU. HANDY AND EASY VAPING*"
- drawn female and male characters wearing sunglasses, each holding an e-cigarette with the headline "*you blu too? who knew?*" alongside the claim "*NEW MYBLU. HANDY AND EASY VAPING*"
- a drawn female character wearing sunglasses holding an e-cigarette with the headline "I'm new to blu" alongside the claim "*NEW MYBLU. HANDY AND EASY VAPING*"

Each of the posters also included small text which stated "*FOR EXISTING ADULT SMOKERS & VAPERS ONLY*" and "this product contains nicotine 18+ only. Not a smoking cessation product".

Allen Carr Easyway, a stop-smoking initiative, and 12 members of the public challenged the adverts on the basis that they encouraged non-smokers and non-nicotine users to use e-cigarettes. In response, Blu took the position that the claim "*For Existing Adult Smokers & Vapers Only*", which was displayed prominently and in large, dark text (in contrast to the light blue background), clarified that the ads were only targeted at existing smokers and vapers.

The decision

The ASA investigated the complaints under Rule 22.8 of the Cap Code, namely that "*marketing communications must not encourage non-smokers or non-nicotine-users to use e-cigarettes*". The ASA commented that, although the "*For Existing Adult Smokers & Vapers Only*" wording on its own was unlikely to deter a non-smoker or non-nicotine user from being

responsive to the ads, the headline taglines did not encourage non-smokers to use e-cigarettes. The ASA found that the headlines in posters 1 and 2 did not actively suggest that non-smokers should take up e-cigarettes and, in particular, the headline in poster 3 suggested that the character was a new user of that particular Blu product as opposed to being a new user of nicotine products in general. On this basis the complaint was not upheld.

Why is this important?

Although the complaint was not upheld in this case, the ASA's decision serves as a reminder that e-cigarette advertisers must be careful not to suggest that any new customers depicted in their ads could be interpreted as being non-smokers that have taken up smoking or vaping as a result of the advertised product. Indeed, the ASA's rationale in this complaint is reminiscent of the previously upheld 2014 Vape Nation complaint in which the ASA explained that ads which portray a person exchanging normal cigarettes for e-cigarettes might be acceptable, whereas ads which would lead consumers to understand that a non-smoker who had subsequently taken up e-cigarettes would not be acceptable.

Any practical tips?

Where possible, advertisers should both clearly state that e-cigarette ads are for the attention of existing smokers and nicotine-users only and ensure that this message is also clearly depicted in associated headline text or dialogue to avoid any ambiguity as to the target audience.

Winter 2019

ASA – social responsibility

ASA ruling on promoting alcohol – Tequila Rose

The question

What if your influencer looks younger than they are when it comes to posts promoting alcohol?

The key takeaway

Tread carefully when mixing alcohol and influencers. Check audience demographics, as well as other factors such as whether the influencer is, or **seems to be**, under 25

The ad

Fashion blogger Holly Ah-Thion published two posts seen on 4 May 2019 on her Instagram account @thekittyluxe, for the alcoholic liqueur brand, Tequila Rose:

- The first post showed Holly holding a shot glass filled with pink liquid, a bottle of Tequila Rose and another shot glass filled with pink liquid on a table in front of her. The post was captioned:

  "*#AD Dressed for the occasion. One for me, one for you. Date night feat. @lovetequilarose. Tequila, but not as you know it…#TequilaRose Strawberry Cream, is pure creamy, strawberry, yumminess in a glass*".

- The second post featured a bottle of Tequila Rose and two shot glasses filled with pink liquid on a table next to a vase of flowers.

The complaint

One complaint challenged whether the ads inappropriately targeted individuals under 18. The ASA also challenged whether the first post breached the Code because Holly appeared to be under 25 years old.

The response

Halewood International (the makers of Tequila Rose) stated that 98% of Holly's followers were over 18 and that her profile described her as a "millennial" with posts related to fashion, brunch, jewellery and city-living; interests it felt wouldn't appeal to individuals under 18. Halewood said it was unaware that Holly was under 25 when they approached her for the campaign and provided evidence showing that she was 25 when the first ad was published and screenshots of posts made by her in the run-up to her 25th birthday.

Holly provided a copy of her Instagram Analytics breakdown which showed 2% of her followers were aged 13-17 years. She said the post was supposed to depict a "date night" which she believed was an adult theme.

The decision

CAP Code rule 18.15 requires that ads for alcoholic drinks are not directed at people under 18 through the selection of media or the context in which they appeared. It further requires that no medium should be used to advertise alcoholic drinks if more than 25% of its audience is under 18. The ASA did not find the ads in breach of rule 18.15, as Holly's content (which consisted primarily of posts about lifestyle, travel and shopping) did not generally focus on themes likely to be appealing to under 18s and did not feature under 18s. Additionally, as the posts were non-paid for, the ads would only have been seen by her followers and in the feeds of those who "re-grammed" her posts. Audience figures provided showed that less than 25% of Holly's audience were under the age of 18.

However, rule 18.16 of the CAP Code states that people shown drinking alcohol or playing a significant role in a marketing communication must neither be, nor seem to be, under 25. While accepting Holly was 25 at the time of the posts, the ASA considered that Holly may have been deemed to be under 25 by some consumers and as she was the focus of the image, she played a significant role in the ad, causing the ad to be in breach of the Code.

Why is this important?

This ruling highlights that drink brands must not concentrate on audience demographics alone – they need to look at the wider context of the ad and whether other sections of the Code may be in play (eg age restrictions on those featured).

Any practical tips?

When using an influencer to advertise alcohol, think not just about their age, but also how old they look! And don't forget the ever-important audience demographics. Put another way, make sure you tick all the boxes when mixing that dangerous cocktail of alcohol and influencers.

Winter 2019

ASA – gambling

ASA ruling on Casumo

The question

Can a gambling ad be seen to be targeting vulnerable consumers if it appears in a Google search result for those trying to "unsubscribe" from gambling ads?

The key takeaway

For advertisers and gambling operators, you must ensure that the term "unsubscribe" and any other similar terms and combinations in respect of gambling should be on your exclusion list for targeted advertising. This will prevent ads from appearing when certain terms or search combinations are typed into a search bar and will aid in the protection of any vulnerable persons.

The ad

In May 2019, following a search for "how to unsubscribe from all gambling", a Google sponsored search result for Casumo Services Limited (**Casumo**) was shown which read "*Welcome Bonus to New Players Casumo 100% and 20 Free Spins*" and stated "*Create an Account & Play now!*".

The complaint

The complainant challenged whether the ad was irresponsibly targeted.

The response

Casumo stated that its ads were served to people who searched for "gambling" or similar terms. However, Casumo had created a list of excluded terms or combinations to prevent their ads from appearing when certain terms or search combinations were typed in the search bar.

In this case, the particular combination had not been foreseen because Casumo claimed it did not consider the word "unsubscribe" would be used by customers looking to self-exclude. Instead, Casumo said that the word "unsubscribe" would be more likely to relate to a customer looking to stop receiving marketing emails or to cancel a subscription, rather than to self-exclude.

Upon being notified of the complaint, Casumo made the search term inactive and also reviewed their wider list of excluded search terms, to ensure it would exclude ads being served to vulnerable consumers. Casumo also provided a list of those terms to the ASA and

confirmed the block applied to all their campaigns. They stated that their exclusion list was continuously reviewed and changed based on trends and advice from their Compliance team and their Responsible Gambling Strategist.

Based on this, Casumo believed they had ongoing steps and processes in place to protect vulnerable individuals and high risk players, which would ensure their Google ad targeting was socially responsible. However, given their view of the standard meaning of "*unsubscribe*" (namely being removal from a mailing list) they did not consider they had targeted the ad in an irresponsible manner.

The decision

The ASA held that consumers who searched "how to unsubscribe from all gambling" were likely to be seeking further information about the tools needed to opt out from receiving gambling ads, or about the tools needed to self-exclude from and/or block gambling websites, with a view to potentially making use of those tools. Such consumers would be likely to include vulnerable persons looking to restrict their exposure to gambling outlets and ads for gambling.

The ASA noted that rule 16.1 of the CAP Code requires that marketing communications for gambling should have particular regard to the need to protect vulnerable persons from being harmed or exploited. Although Casumo had immediately taken action to address where their ads were served, the ASA considered that there was a strong possibility that vulnerable customers who might have been trying to block their exposure to gambling sites might have been served the ad.

The ASA therefore ruled that the ad breached CAP Code Rule 16.1 and had not been targeted responsibly.

Why is this important?

The ruling is an important reminder for advertisers on how search and excluded terms and combinations must be carefully used in targeted advertising – especially when a regulated product is being promoted (for example, alcohol) and when the targeted audience may be vulnerable (for example, children).

Any practical tips?

For gambling operators, ensure that the term "unsubscribe" and any other similar terms and combinations in respect of gambling is on your exclusion list for targeted advertising. Additionally, for all advertisers, like Casumo, you should continue to monitor and review your terms in line with social trends.

Winter 2019

ASA – gambling

ASA ruling on Merkur Cashino Ltd

The question

Can ads on the back of bus tickets be seen to target protected age categories?

The key takeaway

The ASA found that a gambling advert placed by Cashino Gaming Ltd on a child's bus ticket did not breach CAP Code rule 16.3.13. This was because:

- the ad was deemed to not be directed at under-18s through the selection of media or context in which it appeared; and
- under-18s did not make up more than 25% of the audience.

The ad

In May, an advert for Merkur Cashino was seen on the back of a child's bus ticket on a route that served a number of local schools. The ad read: *"£5 Free Plays on a machine of your choice with this ticket!*".

The complaint

A complaint was made, suggesting that the ad was inappropriately targeted at those below 18 years of age.

The response

The CAP Code stipulates that "*marketing communications for gambling must not be directed at those aged younger than 18 years through the selection of media or context in which they appeared*". The ASA also requires marketers to demonstrate that protected age categories ie under-18s, do not make up more than 25% of the audience.

Cashino Gaming Ltd (trading as Merkur Cashino) argued that the ads were not likely to be of particular appeal to under-18s. The company also stated that its ad agency, TicketMedia, had confirmed that children aged between five and 15 years old made up 23.1% of its passengers.

National Express West Midlands, the bus operator, also stated that only 27% of all journeys in a term-time week were made by passengers who bought a ticket, and the vast majority of those were adults.

The decision

As outlined above, the ASA found that the ad did not contravene the CAP Code. This is because it found that:

- ads on bus tickets were not in media "specifically directed at under 18s";
- the ad's audience was less than 25% under 18s (a high of 15% in term-time).

While the ad appeared on the back of a child's bus ticket, the ASA determined that ads on the back of bus tickets did not appear in media specifically targeted at under 18s. The ASA also identified that the highest percentage of child tickets issued on that bus route was 15% during term time.

The ASA did reflect that such an ad might contravene the CAP code on a route that served a number of schools, as the audience in such a case might be more than 25% under-18s. However, that was not the case on this particular route or with this particular bus ticket.

Why is this important?

The decision comes in a climate where the ASA is more proactively clamping down on gambling adverts that breach the CAP Code. Indeed, in October, online casino Casumo was forced to retract an ad that actively targeted gambling addicts.

Any practical tips?

The case highlights the need to always step back and consider where regulated products (here, gambling but it could equally have been alcohol) are advertised. The key question to ask is "will kids see this?" and, if there's a chance, then stop and think how real the risk is. To show just how carefully you need to think about this, the ASA's ruling shows that if the bus ticket had been used on a route which served a number of schools, then the outcome might have been very different.

Winter 2019

ASA – misleading claims

ASA ruling on Dyson

The question

How careful do you need to be when making factually correct claims in a context which might change their meaning?

The key takeaway

When promoting the specifications of a product, make sure that other elements of an ad don't make the claim misleading.

The ad

A video ad on Dyson's website which aired in July showed the testing of Dyson's Light Ball Multi Floor vacuum cleaner being used around a house. There was a scene that showed the product plugged in at the bottom of some stairs whilst a technician climbed to the top step using the detachable nozzle of the vacuum. As this scene was being shown, a voiceover referred to an "*instant release wand, with a total 13.8 metre reach*".

The complaint

The ad received one complaint that the ad "misleadingly implied" that the length of the hose between the vacuum cleaner and the wand was 13.8 metres, despite its actual reach being "significantly shorter" at just 4.4 metres.

The response

Dyson explained that the voiceover listed various attributes of the product including, "improved engineering to make it quieter", "it is easier to carry" and "included an instant release wand; with a total 13.8 metre reach". According to Dyson, the statements were separate features and should not have been read as meaning that the release wand was 13.8 metres long.

Dyson also stated that that the "total reach" represented the measurement from the plug socket to the end of the longest combination of included accessories.

The decision

The ad was banned for wrongly implying that the length of its vacuum hose stretched more than triple its actual reach. An ASA spokesman added that the 13.8 metre reach should only be used to refer to the distance from the plug socket to the nozzle.

Why is this important?

The ruling reminds us that the ASA looks at ads through the eyes of the average consumer. In this case, the consumer would interpret the claims “instant release wand” and “with a total 13.8 metre reach” together and would therefore take the claim to mean that this was the maximum length of the hose when extended, from the main machine to the model.

Any practical tips?

Make sure your creative team resists the temptation to include something that is factually correct in a context which becomes misleading. Here, the plug socket to nozzle length was indeed 13.8 metres, but it was used alongside a reference to the instant release wand which was never going to reach that far from the main machine. Taking care over the presentation of claims (whether verbally or visually) is the key to prevent your ad being pulled.

Winter 2019

ASA – misleading claims

ASA issues guidance on how to deliver a compliant marketing subscription box

The question

How careful do you need to be when offering a free trial? What does a free trial "subscription trap" look like? And how do you avoid setting one?

The key takeaway

A free trial for a subscription package needs to include all the material information a consumer needs to make an informed decision on whether or not to enter into the subscription commitment.

The background

The ASA has recently published advice on providing compliant "free-style" trial subscription box offers.

The ASA's advice is to include all significant conditions, which will be any information likely to affect a consumer's understanding of the subscription box with respect to their decision on whether or not to buy it. Rule 8.17 of the CAP Code provides details which need to be included:

- how to participate, including costs or other factors likely to influence a consumer's decision;
- any free-entry route explained clearly and prominently;
- the start date, if applicable;
- the closing date;
- any proof of purchase requirements;
- if applicable, the number and nature of any prizes or gifts and, if the numbers are not predetermined then, a reasonable estimate should be provided;
- any restrictions that may apply, such as age or location;
- any limitations on the availability of the promotion;
- the promoter's name and address, if it is not obvious from the context.

Further to Rule 8.17, the following are examples specific to subscription boxes that are likely to affect a consumer's understanding:

- whether a paid subscription starts automatically after the trial unless it is cancelled;
- how to cancel if the method of doing so is not what a consumer may reasonably expect;
- the extent of the financial commitment in the case the subscription is not cancelled during the trial period.

The placement and prominence within the ad of any material information and significant conditions is also key. Essentially, the consumer should see any material information and significant conditions before choosing whether or not to buy a free trial subscription offer. Significant conditions should always be included and any other terms and conditions can be signposted for the consumer if they are easily accessible. As examples:

- stating “T&Cs apply” is unlikely to be sufficient;
- information should not be hidden at the bottom of the page;
- information should be immediately visible, pop-ups are not sufficient.

Consider also the CAP Code for all aspects of the ad and refer to the specific rules that may apply to the products or services included in the subscription box.

Why is this important?

The advice demonstrates the ASA’s expectations on ensuring consumers are fully informed about subscription boxes and its desire to ensure that they will be satisfied with the product or service and wish to continue with it.

Any practical tips?

Ensure commitments for a subscription box are explicitly clear for consumers and that any significant conditions are included in the ad as prominent and distinct from other information.

Winter 2019