RPC

Commercial law snapshots

Summer 2020

ADVISORY | DISPUTES | REGULATORY | TRANSACTIONS

Google Snapshots Summer 2020

Contents

Page

1. Commercial cases

Contractual interpretation; rectification 4

Contractual interpretation; limitation period for notifying claims 6

Contractual estoppel; contractual representations 8

Contractual discretion; implication of Braganza duty 10

Force majeure and circumstances beyond reasonable control 12

2. Intellectual property

Luxury and online marketplaces – the next chapter 14

3. Data protection

Cookie walls and scrolling – updated EDPB guidance 16

Continuing the free flow of personal data between the EU and the UK post-Brexit: DCMS Explanatory Framework for adequacy discussions 18

GDPR Codes of Conduct and Certification schemes – the ICO is "open for business" 21

Ashley Judith Dawson-Damer v Taylor Wessing LLP – Court of Appeal rules on legal professional privilege and "relevant filing system" in subject access dispute 23

WM Morrison Supermarkets plc v Various Claimants – Supreme Court rules on vicarious liability for unlawful disclosure of personal data by rogue employee 26

Government publishes approach to post-Brexit trade deal with the EU 29

ICO issues guidance on artificial intelligence: explaining the "black box" 31

ICO outlines priorities and regulatory approach during the coronavirus public health emergency 33

COVID-19 testing and monitoring in the workplace 35

European Commission and EDPB lay out framework for privacy compliant contact tracing apps 37

Data regulation and oral communications 39

4. Digital

Fake reviews probed by CMA 41

5. Consumer

Consumer rights enhanced by the Omnibus Directive (part of the "New Deal for Consumers") 43

Rogue online sellers up against new UK consumer-protection weapon 45

6. ASA: Annual Report

A summary of the ASA Annual Report 2019 47

7. ASA: Surveys

CAP's new "Quick Guide to Advertising Consumer Surveys" 50

8. ASA: Pricing

Make sure the price is right: using reference pricing in ads – Committee of Advertising Practice releases update on pricing practices 52

9. ASA: Superiority claims

ASA ruling on EE – misleading and ambiguous mobile network claims 55

ASA ruling on ASTOK Ltd t/a TVBet – unsubstantiated superiority claims 59

10. ASA: Promotions
ASA ruling on Boohoo.com – "Up to x% off everything" and countdown clocks 61

11. ASA: Influencer marketing
ASA ruling on ASOS – use of "affiliate" for a marketing communication 64

12. ASA: Gender
ASA ruling on Missguided Ltd – the fine line between the mildly sexual and the objectification of women 67

13. ASA: Gaming
CAP warns against promotion of "bad betting behaviours" 69

CAP issues advice notice on the marketing of gambling on eSports on social media 71

ASA ruling against Coral – "Have another go" and socially irresponsible gambling 74

14. ASA: Covid-19
Complying with ASA rules during a pandemic 76

ASA ruling against Revival Shots 79

Commercial cases

Contractual interpretation; rectification

Gwyn y Mor Ofto plc v Gwynt y Mor Offshore Wind Farm Ltd [2020] EWHC 850 (Comm)

The question

How will the Court apply contractual interpretation in the context of the whole of the contract, and an alternative case of rectification of the contract?

The key takeaway

The Court's approach to contractual interpretation is set out in the leading Supreme Court decisions of *Wood v Capita*, *Arnold v Britton* and *Rainy Sky*. In this case, it was the consideration of the relevant provision in the context of the contract as a whole, rather than factual matrix, which was crucial.

The Court also considered an alternative rectification case, for which pre-contractual negotiations and the parties' actual intentions is relevant; although such matters are inadmissible for contractual interpretation.

The background

Ofgem organised the sale of the transmission system of a wind farm comprising 160 wind turbines, located off the Welsh coast. A consortium of Balfour Beatty and Equitix were the preferred bidder (**Buyer**). Various RWE companies were selling the business of owning and operating the electrical transmission link (**Sellers**). The deal was by way of an asset sale for a purchase price of £352m. The SPA was signed on 11 February 2015 and completed on 17 February 2015.

The wind farm used four subsea export cables, which were included within the definition of **Assets** in the SPA. Less than two weeks after completion, one of the cables failed as a result of seawater penetrating a damaged sheath on the cable. A second cable failed in September 2015. The corrosion dated back months or years, prior to the signing or completion of the SPA.

The Buyer claimed for £15m of repair costs under an indemnity in the SPA, which provided that *"[I]f any of the Assets **are** destroyed or damaged prior to Completion … the [Sellers] shall indemnify the [Buyer]*".

The decision

The Court applied the accepted approach to contractual interpretation (referring to *Wood v Capita*, *Arnold v Britton* and *Rainy Sky*). The Buyer stressed the detailed and complex nature of the contract, negotiated over several years with professional assistance, and urged a principally textual analysis, with limited/no regard to the factual matrix. The Sellers sought to advance factual matrix material and suggest provisions that impose wide liabilities should be construed

narrowly. The Court preferred the Buyer's approach, but noted the provision must be considered in the context of the agreement as a whole.

The Court gave judgment in favour of the Sellers, noting that the wording of the indemnity, when considered in the broader context of the SPA, supported the view that it only covered the period between signing and completion – a period of six days.

The choice of the words "*are damaged*" as opposed to "*have been damaged*" (which would have covered historical damage) meant that the parties had intended to exclude pre-signing damage from the scope of the indemnity.

If the parties had intended to give the Buyer the benefit of a widely-drafted indemnity, that indemnity would have also applied to damage that the Sellers had disclosed. Further, the Sellers had provided warranties as to the absence of damage to Assets that did apply to the pre-signing period (but this was qualified to apply only in specific circumstances). The Court noted that these warranties would not give any additional protection if the same issues were also covered by an open-ended indemnity.

The Sellers also advanced a rectification case based on the pre-contractual negotiations. The Court noted that such material was not relevant to the contractual interpretation exercise. However, if the Court had preferred the Buyer's interpretation, the Court indicated that it would have rectified the contract to reflect the Sellers' interpretation, on the basis that the parties shared a common continuing intention, that the parties had communicated.

Why is this important?

This is a useful example of the Court's applying the established approach to contractual interpretation by reference to the whole of the contract, with limited reliance on the factual matrix. It also considers an alternative case for rectification (based on the actual (subjective) intentions of the parties), where pre-contractual negotiations are admissible.

Any practical tips?

Always ensure that the drafting of key provisions is clear. Check for consistency of provisions throughout the agreement, particularly those that deal with the same or similar subject matter. Consider including relevant factual background/context within the agreement (eg recitals).

Maintain copies of communications, notes, transaction files, etc, in case the drafting of the contract has gone wrong and you need to fall back on a rectification argument (and note that the lawyers involved may be required to give evidence!).

Summer 2020

Commercial cases

Contractual interpretation; limitation period for notifying claims

Towergate Financial (Group) Ltd & Ors v Hopkinson & Ors [2020] EWHC 984 (Comm)

The question

How will the court interpret a contractual time limit on notifying claims, in particular to notify "*as soon as possible*"?

The key takeaway

Very careful consideration should be given to notice clauses – all requirements must be met to ensure that a notice is valid and a party should not just consider any longstop date.

The background

The case involved the purchase of the company M2 Holdings Limited and its subsidiaries (the **Company**) which took place in August 2008. In the share purchase agreement (**SPA**) for this deal, the sellers agreed to indemnify the buyers against any losses suffered as a result of or in connection with professional negligence claims, including claims regarding mis-selling which had occurred before the completion of the SPA.

The indemnity was limited by clauses 6.7 and 6.7.3 which stated that the sellers would not have any liability in relation to the indemnity unless the buyers notified the sellers "*as soon as possible*" and in any event prior to and on or before the seventh anniversary of the date of the agreement.

In addition, clause 5.12 regulated the conduct of claims related to the indemnity. The seller required the buyer to attempt to mitigate/avoid proceedings and to enable this, the buyer would disclose all relevant information and documents of the claim to the seller.

In July 2014, the FCA reviewed financial advice given by the Company and determined that there had been mis-selling which resulted in substantial liabilities being incurred. In July 2015 (and still within the seven-year anniversary of the date of the agreement), the buyer notified the seller of their obligations to indemnify them for these liabilities.

The seller refused to indemnify the buyer on the basis that they had not informed them "*as soon as possible*". The buyer disputed this, arguing that the limitation only required them to notify the sellers on or before the seventh anniversary of the date of the agreement. They contended that the wording "*as soon as possible*" should not be considered, given:

- the tautologous and ambiguous nature of the clause, which required notice "prior to", and "on or before the seventh anniversary"
- the undefined meaning of "*as soon as possible*"
- the lack of commercial justification for "*as soon as possible*" acting as a condition precedent.

The decision

The court held that the buyer failed in its claim for indemnification against the seller:

- the clause in dispute was not problematic and the obligation was not satisfied by providing notice within the seven years. The reasonable reader would understand that the clause created dual condition precedents: (1) to provide notice as soon as possible and, (2) in any case, provide notice within seven years from the date of the agreement.
- the commercial circumstances did not impact such an unambiguous term. The court dismissed the buyer's suggestion that the existence of clause 5.12 negated the commercial justification for including the "*as soon as possible*" obligation.
- the lack of specific wording in the SPA regarding what constitutes "*as soon as possible*" did not make the limitation redundant. In this case, after the buyer was informed of the FCA review, they had given notice to their insurer of such claims, but did not inform the seller until a year later. Therefore, on the facts, the buyer had not given notice "*as soon as possible*" and were not entitled to indemnification.

Why is this important?

This is a reminder that the court will give clauses their "natural and ordinary" meaning, even if the commercial consequences for one party are significant. It is also helpful guidance on the approach to contractual limitation clauses.

Any practical tips?

When drafting notice provisions, consider each of the requirements of the notice (eg timing, content and service) and whether each is intended to be a condition precedent (ie if it is not satisfied, the notice is ineffective). This is particularly important where there are significant commercial consequences of the notice (eg indemnities, contractual limitations, renewals/break clauses, etc).

Commercial cases

Contractual estoppel; contractual representations

Wallis Trading Inc v Air Tanzania Co Ltd [2020] EWHC 339 (Comm)

The question

When are parties contractually estopped from adopting a different position?

The key takeaway

If parties conclude an agreement that includes particular contractual representations, they are bound by those representations and cannot later assert an inconsistent position to avoid their obligations (even if it transpires the original representation was not true).

The background

Wallis leased an aircraft to Air Tanzania. In the aircraft lease agreement, Air Tanzania made certain representations, including:

- that the lease was legal and valid
- that it had obtained all required authorisations and consents to enable it to enter into and perform the lease.

Air Tanzania later argued that the lease was invalid because it had failed to comply with Tanzanian public procurement laws.

The decision

The Court held that Air Tanzania was contractually estopped from arguing that the lease was invalid based on failure to comply Tanzanian public procurement laws, because Air Tanzania had already made representations that the lease was legal and valid, and that the entry into and performance of the lease did not conflict with any laws binding on it. These representations had given rise to an estoppel upon entry into the lease. The effect was that both parties had contractually accepted that a certain state of affairs was true, even if it was not or the parties had knowledge of the true position.

Why is this important?

This is a useful example of how contractual estoppel works in practice and demonstrates the worth of standard boilerplate representations and warranties regarding validity and authority to prevent a warranting party from asserting that the true facts were different in order to avoid its obligations.

Any practical tips

Always consider whether standard representations and warranties as to a party's capacity, authority and legality to enter an agreement are included/required. These can be particularly useful for international agreements/jurisdictions where it may be difficult to investigate the position. If there are important assurances provided in the pre-contract negotiations, also consider whether these should be included as representations, warranties and undertakings within the agreement.

Summer 2020

Commercial cases

Contractual discretion; implication of Braganza duty

UK Acorn Finance Ltd v Markel (UK) Ltd [2020] EWHC 922 (Comm)

The question

When will an implied obligation to act rationally when exercising a contractual discretion (a *Braganza duty*) be implied into a contract, and what impact will a *Braganza duty* have on a party's discretion to make a decision?

The key takeaways

Even if a contractual discretion is expressed to be "sole" or "absolute", it is subject to certain restrictions implied by law (a *Braganza duty*). Where a *Braganza duty* applies, the decision maker needs to act rationally, in good faith and take relevant factors into account when reaching its decision.

The factual background

UK Acorn Finance Ltd (**Acorn**) was a bridging finance lender which had obtained default judgments against an insolvent surveyor (the **Insured**). Markel (UK) Ltd (**Markel**) were the professional indemnity insurers of the Insured. Acorn sought to claim against Markel under the Insured's professional indemnity policy.

There was an innocent non-disclosure clause (**IND Clause**) in the insurance policy which provided:

> "*In the event of non-disclosure or misrepresentation of information to Us, We will waive Our rights to avoid this Insuring Clause provided that*
>
> *(i) You are able to establish to Our satisfaction that such non-disclosure or misrepresentation was innocent and free from any fraudulent conduct or intent to deceive*."

As part of the policy renewal process in 2013 and 2014, the Insured confirmed that that it hadn't undertaken work for sub-prime lenders. This was inaccurate because Acorn fell within the definition of a sub-prime lender. The Insured had wrongly believed that the definition applied to residential, rather commercial lenders.

Markel came to the conclusion that there had been a deliberate misrepresentation and non-disclosure by the Insured and sought to avoid the policy on the basis of the IND Clause.

The decision

A so called "Braganza duty" (named after the leading Supreme Court decision in *Braganza v BP Shipping Ltd* [2015]) is an implied obligation to act rationally when exercising contractual discretion. It is implied where:

- the contract gives discretion to one party to make a decision
- the manner in which the discretion is exercised will impact rights held by both parties under the contract
- there is a conflict of interest for the decision maker.

A *Braganza duty* is more likely to be implied in cases where there is unequal bargaining power between the parties.

The Court found that the Insured was required to demonstrate that any misrepresentation had been innocent. The effect of the IND Clause was to give Markel the decision-making power. As such, the Court considered it necessary to imply a *Braganza duty* so that Markel would not be able to exercise its decision-making powers under the IND Clause arbitrarily, capriciously or irrationally.

The Court found that Markel failed to comply with that duty as they had not approached the decision with an open mind or taken into account the Insured's misunderstanding of the term "sub-prime". Further, assumptions had been made about the reliability of the Insured and these had wrongfully been taken into account.

The Court concluded that it was not possible for the same decision to have been reached under the IND Clause if the decision had been approached properly.

Why is this important?

This decision provides further guidance on when a *Braganza duty* can arise and the approach the Court takes when considering the issue. The question of what factors should and should not be taken into account is key.

Any practical tips?

Identify any clauses within contracts that may give rise to a *Braganza duty*. Consider whether these can be restated as contractual rights, without any discretionary element. For discretionary matters, consider whether particular factors should be identified within the contracts; whilst this may limit discretion, it may provide greater certainty.

When decisions are being made, ensure that the decision makers go through a proper decision-making process, identifying the factors that were taken into account and the decision(s) reached. It is good practice for these to be recorded (perhaps with internal/external legal support), so they can be evidenced/justified if challenged.

Summer 2020

Commercial cases

Force majeure and circumstances beyond reasonable control

2 Entertain Video Ltd v Sony DADC Europe Ltd [2020] EWHC 972 (TCC)

The question

What is the meaning of "*circumstances beyond the reasonable control of a party*" in a force majeure clause?

The key takeaways

Parties should ensure that they have taken appropriate measures to deal with/mitigate potential risks that would impact the performance of their contractual obligations. If they fail to do so, there is a risk that a force majeure clause may not protect them from liability, particularly if it requires there to be "*circumstances beyond the reasonable control of the affected party*".

The background

Sony DADC Europe Ltd (**Sony**) provided storage and distribution of CDs and DVDs for 2 Entertain Video Ltd (**2E**) in accordance with a logistics contract between the parties.

During the 2011 London Riots, a group of rioters broke into the warehouse, looted some of the contents and threw petrol bombs at the stock. The CDs and DVDs stored on behalf of 2E were destroyed in the resulting fire.

Sony's insurers paid a settlement of £8.27m to cover the loss of the stock. 2E subsequently brought a claim against Sony for losses arising from business interruption caused by the destruction of the warehouse (such as loss of sales).

As part of their defence, Sony sought to rely on the following clauses in the logistics contract:

- Clause 14.1: "*Neither party shall be liable for its failure or delay in performing any of its obligations hereunder if such failure or delay is caused* ***by circumstances beyond the reasonable control of the party affected*** *including but not limited to… fire ... riot ...*"
- Clause 10.3, which excluded liability for indirect or consequential loss in connection with the supply of logistics services
- Clause 10.4, which imposed a £5m cap on Sony's aggregate liability for all breaches of the logistics contract.

The decision

The Court found that Sony had failed to take reasonable measures to secure the warehouse against break-ins and arson which could have prevented the incident. Sony was therefore liable for damages for negligence unless the force majeure or limitation clauses applied.

The Court held that, whilst the riots were unforeseen, the risks of a break-in, arson and a fire were not. Sony's inability to perform the logistics contract resulted from circumstances which were within its control because it could have taken measures to deal with those potential risks. As such, the breaches of contract were not "*beyond the reasonable control*" of Sony and the force majeure clause did not apply.

Further, the business interruption losses were not indirect or consequential and therefore were not excluded pursuant to clause 10.3. Finally, the Court found that the £5m cap applied in relation to this claim for business interruption and was not exhausted by insurers' settlement to the wording of the Discharge and Release Agreement.

Why is this important?

The COVID-19 pandemic has highlighted the importance of force majeure clauses, with many businesses struggling to fulfil their contractual obligations in the unprecedented circumstances.

However, this case makes it clear that force majeure clauses are not "get out of jail free" cards, even if one of the listed events occurs. The effect of such a clause will be considered on a case by case basis, depending on the wording of the clause and the relevant facts.

Any practical tips?

Revisit and consider the scope of your force majeure provisions – should this be limited to *"circumstances/events beyond a party's control"* (with specific, non-exclusive examples)? Or should this be a "sweeper" provision, in addition to listed examples of matters that amount to force majeure?

Don't assume that you can rely on a force majeure clause simply because of the COVID-19 pandemic (or any other event listed in a force majeure clause)! In particular, if your force majeure requires "*circumstances beyond your control*", ensure that you have taken the measures to comply with your contractual duties/address potential risks.

Should a potential force majeure event occur, keep records of how and why contractual performance was delayed and any measures that were taken to address/mitigate the impact on contractual performance.

Summer 2020

Intellectual property

Luxury and online marketplaces – the next chapter

Coty v Amazon (C-567/18)

The question

Is an innocent third party liable for simply storing third-party goods that it did not know infringed trade mark rights?

Key takeaway

An innocent third party will not be infringing trade mark rights by simply storing goods on behalf of a third-party seller, provided that the storing party does not intend to offer the infringing goods for sale or put them on the market.

The background

Global beauty company, Coty, holds an EU trade mark (**EUTM**) licence for DAVIDOFF, and distributed the "Davidoff" brand perfume through its German distribution company, Coty Germany GmbH.

Coty claimed that two Amazon companies had infringed its rights in the EUTM by storing and dispatching bottles of "Davidoff Hot Water", that were offered for sale by third-party sellers via Amazon-Marketplace, as Coty had not consented to the bottles being put on the EU market.

Coty wrote to the third-party seller in question and obtained a cease-and-desist declaration. It then wrote to Amazon, to request the return of all bottles offered by the seller. Amazon sent a package containing 30 bottles to Coty. When Coty learned that some bottles were offered for sale by a different third-party seller, it asked Amazon to disclose their contact details. Amazon declined.

Although contracts for the sale of goods via Amazon-Marketplace are concluded between third-party sellers and end-purchasers, Coty believed that Amazon's actions infringed the EUTM and that Amazon should be ordered to cease and desist from storing and dispatching bottles via its "Fulfilled by Amazon" (**FBA**) service.

The decision

Coty's claim failed at the German national courts and was appealed to Germany's Federal Court on a point of law. The Federal Court stated that it agreed with the previous decision that Amazon had not infringed but sought input from the CJEU on the interpretation of EU trade mark law.

An act of infringement under EUTM regulations requires the "use" of a mark in the course of trade. As such, the CJEU was asked to consider whether storing infringing goods for a third party to sell, without knowing about the infringement and without offering to sell the goods or intending to offer to sell the goods amounted to "use" and thus trade mark infringement.

The CJEU held that the answer was no: the provision of storage alone was not enough. For infringement to arise, the storage company must also pursue the aim of offering the goods for sale or putting them on the market. Amazon's lack of intent to offer the goods for sale meant that it had not used (and had therefore not infringed) the EUTM.

Why is this important?

Even though this decision is the latest in a long line of disputes that have seen brand owners (unsuccessfully) attempt to challenge Amazon's business practices, it seems likely that we will see further litigation involving online marketplaces for two reasons:

1. Brand owners argue that Amazon plays more than a passive role by providing the platform on which goods are offered and ultimately sold via its Marketplace and that Amazon effectively steps into the shoes of the third-party seller. Brand owners also note that, in the case of FBA, Amazon itself claims to "*take care of storage, delivery to customers, customer service and returns handling*".

2. the CJEU referred to other provisions of EU law, which allow proceedings to be brought against intermediaries who have enabled economic operators to use trade marks unlawfully. For example, it accepted that if someone is unable to identify the third party on whose behalf goods are stored, the storing party itself would be offering the goods for sale (and therefore infringing). The mixing of products belonging to different third-party sellers could therefore prove problematic for marketplaces like Amazon.

Any practical tips?

Some brands see real benefit in selling via marketplaces such as Amazon due to its popularity amongst consumers, or the ability to more effectively remove counterfeit goods; but joining forces with Amazon will not be for everyone. The COVID-19 outbreak has also accelerated recent trends, including in the luxury retail sector: consumer habits have shifted (even more) online.

Spending habits indicate that for those wishing to retain a physical store presence (andconsumer experience), a clicks and mortar business model will likely be more futureproof. This presents an opportunity for greater collaboration between luxury brands and online marketplaces (whether through the release of more extensive collections or new partnerships) and undoubtedly acts as an incentive for brands to develop and extend their digital presence.

Summer 2020

Data protection

Cookie walls and scrolling – updated EDPB guidance

The question

Are cookie walls permissible? Can scrolling through a website constitute "consent"?

The key takeaway

The European Data Protection Board (EDPB) has updated its "Guidelines on GDPR consent" to clarify that: (a) making access to a website conditional on accepting cookies – known as "cookie walls" – does not constitute valid consent; and that (b) scrolling or swiping through a webpage cannot constitute consent either, under any circumstances.

The background

Consent is one of the six lawful bases for processing personal information under the GDPR. For many internet users, cookie consents are an irritating and inescapable experience when browsing the web. These notices ask users to agree to being tracked when visiting a site for the first time but, are often misleadingly phrased or impossible to refuse. In an effort to make cookie consent more consensual, the EU has published these updated guidelines which make it clear that cookie walls and scrolling are not legitimate means of obtaining consent.

The guidance

"Guidelines on consent under Regulation 2016/679" were first published in November 2017 by the EDPB's predecessor, the Article 29 Working Party. They were formally adopted in April 2018. The EDPB has now produced a slightly updated version of those Guidelines. Two important clarifications appear in the sections of the Guidelines on "Conditionality" and "Unambiguous indication of wishes". These apply to the validity of consent provided by individuals when interacting with "cookie walls" and the question of scrolling or swiping to indicate consent.

Cookie walls

"Cookie walls" make viewing content contingent on consenting to be tracked. This conflicts with the concept of giving people a free choice over whether their data is collected for potentially intrusive usage like targeted advertising. However, as the EDPB notes, if a website "puts into place a script that will block content from being visible except for a request to accept cookies" this "does not constitute valid consent" as the user is "not presented with a genuine choice." So what this means in essence is no more cookie walls.

Scrolling or swiping through a webpage

The other key clarification in the Guidelines is to confirm that the most basic interactions with a website cannot constitute consent. Some website providers, for example, interpret simply scrolling or swiping on the page as agreeing to their tracking policies. The EDPB notes that "such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will not always be possible". Also, if scrolling can constitute consent, it should also be capable of being used to withdraw consent. In the EDPB's words, "in such a case it will be difficult to provide a way to withdraw consent in a manner that is as easy as granting it".

Why is this important?

The Guidelines put beyond doubt what we have known for a long time, namely that cookie walls and scrolling or swiping are not compliant means for obtaining consent.

Any practical tips?

It's clear that market practice has some way to go to catch up with the EDPB, with many sites still presenting all-or-nothing cookie walls that force consumers to consent or go away. Moreover, consent management platforms (CMPs) may have some way to go to reach the level of clarity being recommended by the EDPB, noting that a whole range of "dark patterns" are in play (confusingly designed user interface choices), which can mislead and coerce users, making it difficult and/or time-consuming for users to provide clear consent. A recent study found that only 11% of cookie consent mechanisms were compliant with the GDPR.

Remember that consent is not considered to be freely given if consumers are not provided the ability to give separate consent for different kinds of data processing where appropriate, including for non-essential, marketing-related data processing. Providing the user with full control over their cookie usage really is the only way ahead.

Summer 2020

Data protection

Continuing the free flow of personal data between the EU and the UK post-Brexit: DCMS Explanatory Framework for adequacy discussions

The question

How might the Explanatory Framework recently published by the Department for Digital, Culture, Media & Sport (**DCMS**) assist with enabling the continued free flow of data between the EU and the UK post-Brexit and how might the UK Government's approach to the COVID-19 pandemic affect this?

Key takeaway

The Explanatory Framework published by the DCMS in March 2020 outlines the UK's intention to seek an adequacy decision from the European Commission (the **Commission**) to enable the continued free flow of personal data between the EU and the UK following the Brexit deadline. The unexpected introduction of a global pandemic to this scenario may have some unexpected consequences, not only impacting the ability of many businesses to comply with data protection measures at this time, but also swallowing the focus of policy makers whole. Given the significant value of personal data-enabled services to the UK economy and their reliance on the free flow of data, this process is clearly one to follow.

The background

Adequacy decisions are one of the tools provided under the GDPR to permit for the transfer of personal data from within the EU to countries outside of the EU (**Third Countries**). Under Article 45 of the GDPR, where a Third Country can evidence an equivalent level of data protection to that of an EU state through its domestic law or its international commitments, the European Commission may make a positive adequacy decision. Such a decision allows for personal data to flow unimpeded between the EU and the Third County without additional safeguards and as if it were an intra-EU data transmission.

Note that there is no requirement for the Third Country's data protection system to be identical to those found in the EU. The standard is instead one of "essential equivalence", and a Third Country's data protection system is assessed by an investigation of its protection guarantees and of the relevant oversight and redress mechanisms available.

The development

In advance of the fast approaching January 2021 deadline, the UK requires adequacy decisions from the Commission to enable to continual flow of personal data post-Brexit. The Commission has described such a decision as being a necessary affirmation of the UK's commitment to the protection of personal data and respect for the Union's personal data protection rules.

On 3 March, the DCMS published an Explanatory Framework for adequacy discussions, designed to assist the Commission's assessment by providing an overview of the legal framework that underpins the UK's data protection standards. The Explanatory Framework highlights:

- how existing UK legislation, including the UK GDPR and the Data Protection Act (**DPA**) 2018, offers robust personal protection, equivalent to that provided under EU law
- the UK's historic commitment to the enforcement of the principles underpinning lawful data processing through the means of judicial redress
- the "strong track record" of the UK Information Commissioner's Office (**ICO**) for working closely and effectively with other DPAs as "*one of the three most active data protection authorities in recent years … [and] is influential in driving global privacy standards*."

While the Explanatory Framework pays specific attention to provisions of the DPA 2018 and the Investigatory Powers Act (IPA) 2016, citing the strengths of both pieces of legislation, it will be interesting to see what the Commission will make of the UK's recent legislative proposal – the Coronavirus Act 2020 – and how this will impact the adequacy assessment. The Coronavirus Act proposes increased surveillance powers and the extension of time limits for retaining DNA profiles in the interests of national security amongst other data collection. A recent legal opinion published in respect of the virus tracking apps being proposed for UK use, was critical of the lack of alignment with existing data protection legislation, both national and EU.

Why is this important?

For those unfamiliar with the industry, personal data-enabled services may seem obscure. However, the flow of these services between the EU and the UK is pervasive across all industries and was collectively worth in excess of £100bn in 2018. Failure to achieve adequacy could be expected to result in significant disruptions to trade across the UK. While contractual protections could serve to mitigate this risk, if the UK's status as a global leader in the field of data protection is to be maintained, the importance of obtaining a positive adequacy decision from the Commission cannot be stressed enough. In our current climate it is in no way guaranteed.

Practical Tips

Those involved directly and indirectly in personal-data enabled services should keep a careful eye on internal legislative developments that might signal deviation from the EU's data protection policies. As stated above, the risk to trade can be mitigated through introducing contractual protections in advance of any potential difficulties arising. This makes it all the more important to ensure that you keep Brexit in mind when drafting any Data Protection Agreements which incorporate the EU's Standard Contractual Clauses.

Summer 2020

Data protection

GDPR Codes of Conduct and Certification schemes – the ICO is "open for business"

The question

What is the ICO doing to make it easier for industry specific sectors to comply with GDPR? What is the benefit to businesses in adopting accredited codes of conduct?

The key takeaways

The ICO has formally invited organisations to submit their sector-specific codes of conduct relating to data-protection for its approval. In addition, UK organisations can now apply to the UK's national accreditation body, UKAS, to be accredited to deliver GDPR Certification schemes.

The background

The ICO has recognised that the implementation of the GDPR looks different for each sector, due to the variety of businesses data protection law covers. As such, in a move to provide certainty to organisations across multiple sectors that their procedures and policies foster GDPR compliant data handling, the ICO has offered to approve codes of conduct submitted to it. To cater for data controllers and processors across jurisdictions not covered by the GDPR, the GDPR Certification scheme will allow them to certify their safeguards in place to protect international transfers of personal data.

The guidance

The codes of conduct submitted by trade association and other representative bodies may identify and address data protection issues that are particularly relevant to their members. To encourage the formation of codes of conduct, the ICO is offering advice on meeting the necessary criteria for approval. These criteria include, among other things, the code owner's ability to represent the data controllers and processors it concerns, the data protection issues it intends to address and the method of monitoring member compliance. Furthermore, the code must specify if it is a national code or covers activities in more than one EU Member State.

If the code of conduct is intended to cover non-public entities, it will have to identify an independent monitoring body to fulfil monitoring requirements. This body must be accredited by the ICO against criteria formally approved by the EDPB.

In addition, UK organisations can apply to be accredited to deliver GDPR Certification schemes. Once a scheme is in place, data controllers and processors will be able to apply to it for GDPR certification. Once a business has been successfully assessed by the accredited certification body against ICO-approved certification scheme criteria, it will be issued with a data protection certificate, or seal relevant to that scheme. These will validate appropriate safeguards provided by controllers and processors who are not subject to GDPR for the purposes of international personal data transfers.

However, it's important to note that the adoption of an approved code of conduct or certification of safeguards does not reduce the responsibility on controllers or processors.

Why is this important?

These steps not only make it easier for organisations across multiple sectors to demonstrate compliance with GDPR, but also engender further trust between organisations and individuals sharing their data.

Sector-specific businesses will also have an approved code of conduct to consider, which may entail making changes to existing policies currently in place. Adopting a sector-specific code of conduct will allow businesses to be confident that they comply with GDPR requirements.

The ICO will take into account participation and non-adherence to a code or scheme when enforcing the GDPR against businesses.

Any practical tips?

Businesses should consider contacting their trade associations or industry representatives who may be developing a code of conduct intended for ICO approval, with their views.

It may be more efficient for businesses to adopt the new approved sector-specific code of conduct insofar as it relates to their activities than relying on or upgrading existing policies and procedures.

Summer 2020

Data protection

Ashley Judith Dawson-Damer v Taylor Wessing LLP – Court of Appeal rules on legal professional privilege and "relevant filing system" in subject access dispute

The question

Do paper files constitute a "relevant filing system" for the purposes of subject access requests (**SARs**)? Can legal professional privilege (**LPP**) be used to block a SAR made by a data subject that is owed a duty of "joint privilege" along with the lawyer's primary client?

The key takeaway

The Court of Appeal (**CA**) has clarified the test and associated questions to be considered when determining whether personal data held in a paper file is in a relevant filing system which must be searched on receipt of a SAR. The CA has also reiterated that joint privilege can arise as a matter of procedural law (rather than substantive trust law) and may restrict the availability of the LPP exemption in circumstances where a SAR is received from a jointly privileged data subject.

The background

The claim relates to a discretionary trust settled for the benefit of the late John Dawson Damer, his brother Lord Portarlington and their respective spouses and children (the **Trust**). The Trust was governed by Bahamian Law. In 2006 and 2009, the trustee of the Trust, Grampian Trust Company Limited (the **Trustee)**, appointed a substantial sum (US$402m) from the Trust into four new discretionary funds, in favour of Lord Portarlington and his descendants (the **Appointments**).

In 2014, Ashley Dawson-Damer, the widow of John Dawson-Damer, and her two adopted children (the **Dawson-Damers**), suspicious that the Appointments were influenced by animosity towards them, sought to challenge the validity of the Appointments and served SARs under the Data Protection Act 1998 (**DPA 1998**) on the Trustee's solicitors, Taylor Wessing.

Taylor Wessing refused to provide the data requested in the SARs on the basis that the data was protected by the LPP exemption under the DPA 1998. The Dawson-Damers brought a claim against Taylor Wessing for relief.

The litigation has been long-running and following a previous CA hearing in 2017 (summarised in our 2017 Snapshots) around the scope of LPP and search obligations in response to a SAR, the case was remitted back to the High Court to determine whether (i) certain information, kept by Taylor Wessing in paper files, was exempt from disclosure because the paper files were not a "relevant filing system" for the purposes of DPA 1998 and (ii) Taylor Wessing could rely on LPP in respect of particular documents. Both parties ultimately appealed the High Court judgment.

The "second round" decisions

Relevant filing system

The High Court had found that the personal data, contained in 35 paper files arranged in chronological order and labelled with a description of the Trust could be easily retrieved, was held in a relevant filing system which Taylor Wessing was required to search.

The CA approached its determination by considering the relevant filing system test which is a "*functional one of whether specific criteria enable the data to be easily retrieved*" and setting out four relevant questions for establishing whether the criteria had been met: (1) are the files a structured set of data; (2) are the data accessible according to specific criteria; (3) are those criteria "*related to individuals*"; and (4) do the specific data criteria enabled the data to be easily (or readily) retrieved?

The CA found that the judge had erred in relation to the fourth question; ready access must be enabled by the criteria ie the structure of the files. The files were unstructured and the need to use a trainee and an associate to review the files page by page, with a senior lawyer to review for legal professional privilege, was a clear indication that the data was not easily retrievable. As such, the paper files were not a relevant filing system and Taylor Wessing was not obliged to search them.

Legal professional privilege

The High Court had accepted that "*under English trust law, joint privilege would arise*" as the Trustee had taken advice from Taylor Wessing for the benefit of the Trust, of which the Dawson-Damer's were beneficiaries. However, as the Trust was governed by Bahamian trusts law, which enables a trustee to refuse to disclose information concerning the exercise of its fiduciary discretions, joint privilege was removed. On this basis, Taylor Wessing could claim LPP over particular documents protected by legal advice privilege between Taylor Wessing and the Trustee.

The CA disagreed with the High Court and found that "joint privilege" is not just a matter of trusts law but rather a matter of procedural law built on the principle that "*privilege cannot be claimed in circumstances where the parties to the relationship have a joint interest in the*

subject matter of the communication at the time that it comes into existence". Notably, joint privilege had been recognised in other contexts, such as between shareholder and company.

The question of whether privilege arose was therefore governed by English law (as the law of the country in which the action was brought). As there was no uncertainty under English law that joint privilege applies between the beneficiary and the trustee of a trust, Taylor Wessing could not rely on LPP even in relation to particular documents where joint privilege existed with the data subject.

Why is this important?

Rather than adopting a prescriptive definition, the CA has set out a set of questions to guide businesses in deciding whether the paper files are a relevant filing system. Although this case concerned DPA 1998, GDPR and the Data Protection Act 2018 define a "filing system" as "any *structured set* of personal data …" and it is arguable that the CA's relevant filing system questions will also extend to obligations under the current data protection regime. With many businesses receiving an increasing number of SARs, this decision will be welcomed by those with paper files who will be comforted by the knowledge that they are not obligated to search unstructured files to extract data that is not easily retrievable.

The LLP/joint privilege points determined at this leg of the litigation are particularly technical and most relevant to trust law matters. Nonetheless, the CA clarified that joint privilege is a procedural law matter to be determined under English law and where a data subject is entitled to joint privilege with a lawyer's primary client, even particular documents sought under a SAR cannot be withheld on the grounds of LPP.

Any practical tips?

Upon receipt of a SAR which relates to paper files, consider the CA's four questions to decide whether you can legitimately limit your searches to exclude those particular files.

Where a SAR is received from a data subject with a relationship with the recipient (eg a company shareholder) and you are hoping to rely on LPP to withhold documents, make sure that you consider whether joint privilege will prohibit the availability of LPP protection.

Summer 2020

Data protection

WM Morrison Supermarkets plc v Various Claimants – Supreme Court rules on vicarious liability for unlawful disclosure of personal data by rogue employee

The question

Can an employer be held vicariously liable for the actions of a rogue employee leaking data?

Key takeaway

The law on vicarious liability does apply to data protection, misuse of private information and breach of confidence claims. While data breaches involving employees will turn on the facts of the case, there is some comfort at least for businesses that they will not be held vicariously liable for the actions of a rogue employee.

The facts

Morrisons appealed against a Court of Appeal (**CA**) decision that it was vicariously liable in damages to around 5,000 of its current and former employees (the **Employees**). Personal information about the respondent Employees was published on the Internet by another of Morrisons' employees, Mr Skelton.

Mr Skelton, a senior auditor, held a grudge against Morrisons following previous disciplinary proceedings against him. In November 2018, Mr Skelton was given access to the payroll data of the whole of the Morrisons' workforce in order to collate and transmit it to external auditors. Mr Skelton copied the data from his work laptop onto a personal USB stick and uploaded the data belonging to the majority of employees to a publicly accessible file-sharing website with links to the data posted on other websites (the **Disclosure**). Mr Skelton was convicted of several offences and sentenced to eight years' imprisonment.

The Employees brought claims for compensation against Morrisons on the basis that they were directly or vicariously liable for Mr Skelton's acts and their subsequent distress, whether in breach of statutory duty under s.4(4) of the Data Protection Act 1998 (**DPA**), or for misuse of private information or breach of confidence.

The decision

To recap, the CA held that the common law remedy of vicarious liability was not expressly or impliedly excluded by the DPA. It treated the connection between the employee's conduct and

his employment as critical, and the employee's motive as irrelevant. As such, the CA concluded that the wrongful acts were done during the course of Mr Skelton's employment and therefore Morrisons was vicariously liable.

The Supreme Court had two key issues to consider:

1. whether Morrisons is vicariously liable for Mr Skelton's conduct
2. if the answer to 1 is affirmative, whether the DPA excluded the imposition of vicarious liability for statutory torts committed by an employee data controller under the DPA and/or for the misuse of private information and breach of confidence.

The Supreme Court followed the general principle in *Dubai Aluminium Co Ltd v Salaam* [2002] UKHL 48, namely, that the wrongful conduct must be so closely connected with the acts that the employee was authorised to do by the employer, that the employee might fairly and properly be regarded as having acted in the ordinary course of their employment.

It concluded that there was no such "close connection" in this case as the Disclosure did not form part of Mr Skelton's "field of activities" in that it was not an act that he was authorised to do by Morrisons and because Mr Skelton was not engaged in furthering Morrisons' business when he made the Disclosure – he was pursuing a personal vendetta. Unlike the courts below, the Supreme Court considered it highly material whether Mr Skelton was acting on Morrisons' business or for purely personal reasons.

Although the appeal was determined on the basis above, the Supreme Court also considered the data protection aspect of the case. Lord Reed stated that the "*the imposition of a statutory liability upon a data controller is not inconsistent with the imposition of a common law vicarious liability upon his employer, either for the breaches of duties imposed by the DPA, or for breaches of duties arising under the common law or in equity*". Since the DPA is silent about the position of a data controller's employer, the Supreme Court held that there cannot be any inconsistency between the statutory and common law regimes.

Why is this important?

Employers will welcome the decision and commentary that the mere fact that an employee's job provides them with the opportunity to commit wrongdoing is not sufficient to establish vicarious liability. However, this case is a further example of data breach class actions in circumstances where the claimants suffer no financial loss. Although, at the time, the ICO found no enforcement action was required with respect to Morrisons' compliance with the DPA, the case illustrates that claimants may still seek damages for distress.

Any practical tips?

Employers should continue to monitor and examine their technical and operational measures to prevent personal data breaches in order to reduce the risk of regulatory enforcement and class actions. The case underlines the need for HR teams to signal to the legal and tech teams if they see an employee potentially going "rogue" or suffering in a way which might impact on their ability to safely handle personal data. Reassigning that individual and/or limiting his/her access to personal data may prove extremely prudent in the long term.

Remember also that we have another "live" representative action going to the Supreme Court now, in *Lloyd v Google* (judgment due later this year). This will determine whether, in a representative action, uniform per capita damages can be awarded for data protection breaches without proof of distress or material damage.

One thing is for sure. Representative class actions for data breaches are on the rise and, given the likely sums involved, it's hard to think of anything with more potential to blow a hole in a business's finances. If ever there were a time to check in with your IT director and operational teams that that they are doing everything they possibly can to reduce the risk of a data breach, it's probably now.

Summer 2020

Data protection

Government publishes approach to post-Brexit trade deal with the EU

The question

What is the Government's approach to a post-Brexit trade deal with the EU?

The key takeaways

The UK Government seeks to proceed with EU trade deal negotiations, aiming for a free trade agreement along the lines of the EU-Canada agreement or the EU-Japan agreement.

The background

The UK left the EU on 31 January 2020 and entered an 11-month transition period. During this time, the Government and the EU have been negotiating a trade deal, which if not concluded, will result in the UK trading with the EU under World Trade Organisation rules.

After a third round of talks in May, the Government published a set of 13 documents setting out the UK's approach to the future relationship with the EU. This is set against the backdrop of COVID-19 which has imported a sense of urgency into talks as economic uncertainty affects companies and economies across Europe.

The guidance

The approach taken by the UK is very much along the lines of negotiating a free-trade agreement, similar to those concluded between the EU and Canada, Japan and South Korea. However, it has not proposed to establish new trading relationships in respect of all sectors in one agreement. Rather, it considers that separate agreements may be required for fisheries, law enforcement and more technical areas including aviation, energy and civil nuclear co-operation.

Points of particular importance to organisations with a technological focus include a desire to incorporate provisions relating to electronic authentication similar to those which have evolved in EU agreements with Australia and Mexico in the proposed UK-EU trade deal. The principle of frictionless data-flow in the digital economy was reiterated and should underpin any future trade agreement.

The Government also considers provisions relating to cross border trade in services should ideally be along the lines of those in CETA and the EU-Japan EPA, promoting ongoing liberalisation for trade in services and investment.

The Government holds up CETA and the EU-Japan EPA as a suitable precedent for a substantial number of other areas to be negotiated across multiple sectors.

Why is this important?

For companies engaging in cross border trade, Brexit is likely to be an industry defining event, the consequences of which will be determined by the trade deal struck between the EU and the UK. Adapting to the new status quo may involve relatively minor adjustments in business practices for some, and significant upheaval for other businesses depending partly on the degree to which their activity is underpinned by EU regulation.

Any practical tips?

Whilst there is still a great deal of uncertainty surrounding trade talks, it is still important to keep up with developments to best manoeuvre one's business in relation to the evolving situation.

Summer 2020

Data protection

ICO issues guidance on artificial intelligence: explaining the "black box"

The question

What steps do businesses need to take to comply with the ICO's new guidance on artificial intelligence?

The key takeaways

Organisations using AI to assist in decision making processes should be able to explain how AI has produced its output. This concept of "explainability" is important, as the GDPR may imply a right for data subjects, in Article 15 and 22, to an explanation of an automated decision after it has been made (by virtue of Recital 71). To this end, companies employing AI should produce documentation explaining the mechanics of the AI used, and issue policy guidance to staff covering how they should ensure the decisions made can be explained.

The background

The ICO and The Alan Turing Institute have collaborated to produce the "Explaining decisions made with AI" guidance, which runs to over 130 pages. It sets out, among other things, key principles to follow and steps to take when explaining AI-assisted decisions, including the procedures and policies organisations should consider putting in place.

This is in response to concerns surrounding "black box" AI systems which have opaque inner workings and are inaccessible to normal human understanding. Decisions made with "black box" systems may be difficult to explain to individuals about whom a decision has been made using their personal data.

The guidance is not a statutory code of practice under the Data Protection Act 2018 but is intended as a best practice guide for explaining decisions to individuals which have been made using AI to process personal information. It builds on the ICO's previous work in this area, including its AI Auditing Framework and Project ExplAIn interim report. Whilst GDPR requirements are touched on in the guidance, it also includes points that are wider in scope, such as the ethical considerations around the use of AI.

This is of particular importance to organisations that develop, test or deploy AI decision making systems such as those employing AI based ad-tech.

The guidance

The thrust of the guidance is that procedures should be adopted to enable a company to explain and evidence to a decision recipient how that decision was made with AI.

It is suggested that policies should cover all the "explainability" considerations and actions that are required from employees involved from the concept formation to the deployment of AI decision-support systems.

Furthermore, it is essential to not only document the processes behind the design and implementation of the AI system, but also the actual explanation of its outcome. It should be comprehensible to people with varying levels of technical knowledge and may help you provide the evidence to explain how a decision was made.

If the AI system is supplied by a third party, it is the responsibility of the data controller in the organisation procuring the AI system, to ensure that it is capable of producing an explanation for the decision recipient.

Why is this important?

Anyone involved in the decision-making pipeline has a role to play in contributing to an explanation of a decision based on an AI model's result. As AI becomes ever more prevalent in mainstream technology, firms should keep abreast of developing guidance. In addition, there may be an implicit right to an explanation of an automated decision after it has been made in the GDPR, as explained above.

Any practical tips?

In the absence of formal specific regulation on the matter, there are several steps which any organisation using AI should consider taking, including:

- producing or updating company policy covering "explainability" and the steps each staff member should take when involved with the creation and deployment of the AI system
- documenting each stage of the process behind the design and deployment of an AI decision-support system and a full explanation of the outcome
- verifying that any third-party suppliers of AI used in decision making processes can explain how the AI has produced its output.

Summer 2020

Data protection

ICO outlines priorities and regulatory approach during the coronavirus public health emergency

The question

How has the ICO reshaped its priorities for regulating UK data protection during COVID-19?

The key takeaway

On 5 May 2020 the ICO published its adjusted priorities during COVID-19 having concluded that its areas of focus should be limited to those where they can have the greatest impact to support innovation and economic growth, while protecting individuals' interests.

The background

On 15 April 2020 the ICO set out its regulatory approach during the coronavirus public health emergency. The ICO explained that it will concentrate on the most significant challenges and greatest threats to the public and will act decisively against those attempting to exploit this unprecedented public health emergency through nuisance calls or by misusing information.

The ICO explained that the law gives them flexibility around how they carry out their regulatory role, which allows them to take "into account the impact of the potential economic or resource burden their actions could place on organisations".

While data protection rules remain unchanged, allowances will be made for the individual challenges faced by organisations. For example, while the document notes that organisations should continue to report personal data breaches to the ICO and that this should still be within 72 hours of becoming aware of the breach, the ICO acknowledges that the current crises may impact this. It will therefore "assess these reports, taking appropriately empathic and proportionate approach".

The guidance

On 5 May 2020 the ICO set out its adjusted priorities, these are as follows:

- **Protecting vulnerable citizens**: the ICO is taking action against those seeking to use or obtain personal data inappropriately during the coronavirus public health emergency, so that the public feel confident that they have protection at a time when they may be especially vulnerable to financial or other loss.

- **Supporting economic growth and digitalisation, including for small businesses**: the ICO continues to provide access to clear information, support and practical tools for businesses to enable them to grow and offer services safely when sharing personal data.
- **Shaping proportionate surveillance**: the ICO is maintaining a high level of awareness and insight of the medium-term privacy and information rights impact of COVID-19, which include contact tracing testing.
- **Enabling good practice in AI**: the ICO are shaping the ongoing development and use of AI in response to COVID-19, to ensure privacy considerations are engineered into the use of AI across the digital economy.
- **Enabling transparency**: the ICO is supporting organisations to be transparent about decisions that affect citizens, including how personal data is used, in order to improve public confidence.
- **Maintaining business continuity**: the ICO is managing its own response and recovery so that its resources and people are in place to deliver throughout the pandemic period and the future.

Why is this important?

In these unprecedented times, the ICO has shown its willingness to supporting organisations through the coronavirus public health emergency and beyond. The ICO has acknowledged its role in supporting frontline organisations that provide vital services and explained that it will fast track advice, guidance or tools that public authorities and businesses say would help them deal with, or recover from, the crisis.

Any practical tips?

Do not take your eye off the importance of data protection compliance! The ICO has made it clear that you cannot use the public health emergency as any excuse for non-compliance.

The ICO recognises that the reduction in organisations' resources could impact its ability to comply with certain aspects of UK data protection law, but it expects appropriate measures to be taken.

Organisations should ensure that they record all decision-making steps, so that this information is readily available if requested by the ICO.

Summer 2020

Data protection

COVID-19 testing and monitoring in the workplace

The question

Can employers test and monitor employees during the COVID-19 pandemic?

The key takeaway

The ICO coronavirus recovery guidance notes that employers may test employees for COVID-19 and monitor employees in the workplace by relying on Article 6(1)(f) GDPR and Article 9(2)(b) GDPR, along with Schedule 1 Condition 1 of the Data Protection Act 2018. This will only be permissible if the processing is strictly necessary for legitimate purposes that bring justifiable benefits and comply with the principles of proportionality.

ICO guidance on testing and monitoring in the workplace

The ICO guidance includes data collation about COVID-19 test results, and monitoring movement of employees within the workplace.

Testing

When considering workplace testing and health data, employers should consider relying on Article 6(1)(f) GDPR and Article 9(2)(b) GDPR, along with Schedule 1 Condition 1 of the Data Protection Act 2018. Article 6(1)(f) GDPR notes that processing shall be lawful only if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Article 9(2)(b) states that processing of special categories of personal data is permissible if the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data subject in the field of employment.

As such, employers will seek to rely on these Articles due to an employer's health and safety at work obligations, so long as they are not collecting or sharing irrelevant data. The guidance confirms that an employer can retain a list of employees who have the symptoms or have been tested as positive for COVID-19, but only where this processing is necessary and relevant for the employer's stated purpose eg it may be necessary to retain a list to determine whether to grant an employee access into a building. If maintaining an ongoing record is necessary (eg to provide ongoing healthcare support to affected employees), the employers must take care to ensure that the list does not result in any unfair or harmful treatment of the employees.

The guidance also states that naming a specific individual who contracted the symptoms should only be done where necessary. If employers are required to share the data with

authorities for public health purposes or the police, then data protection laws will not prevent the employer from disclosing this information.

Monitoring

The guidance allows employers to monitor staff using thermal imaging and traditional CCTV, though the monitoring of employees must be necessary and proportionate. This includes ensuring that employers do not hold more data than that which is necessary for its purpose. The Surveillance Camera Commissioner (**SCC**) and ICO have updated the SCC Data Protection Impact Assessment template to assist employers when considering the use of thermal cameras or other surveillance during the pandemic.

Why is this important?

In light of the COVID-19 pandemic, various employers are seeking to monitor and test employees, however, the processing of data should be limited to only that which is necessary. If employees believe there has been a breach of processing their personal data in accordance with data protection laws, they can complain to the ICO. The ICO can impose sanctions and fines of up to 4% of global annual turnover or €20m (whichever is the greater). Employees can also have grounds to bring whistleblowing claims, and employee/employer grievances.

Any practical tips?

Carefully follow the ICO guidance to identify the purpose for which you are seeking to monitor or test your employees for COVID-19. The monitoring and testing needs to be necessary and proportionate to the purpose, therefore employers should consider if there is a less intrusive way to protect their business and monitor employees without breaching data protection laws.

By conducting a Data Protection Impact Assessment (**DPIA**), employers can record the risks and mitigation steps they have taken prior to monitoring and testing.

Employers should inform their staff of what monitoring and testing will be carried out, the purposes for the monitoring and testing, and what personal data is required. Also consider relevant training for employees who will be processing personal data, as well as introduce measures to limit the number of people with access to personal data, the amount of data collected and the length of time it is retained.

Summer 2020

Data protection

European Commission and EDPB lay out framework for privacy compliant contact tracing apps

The question

How do we balance the need for contact tracing with data protection regulation?

The key takeaway

The guidelines and toolbox prepared by the European Commission and EDPB set out the relevant parameters for a coordinated development and use of contact-tracing applications and the monitoring of their performance. The guidance aims to explain how the collection of location data to enable contact tracing can be lawful and proportionate.

The background

Against the backdrop of an unprecedented pandemic costing hundreds of thousands of lives and freezing economies worldwide, governments, health authorities and private entities alike have been striving to develop and deploy technology in order to curb the death toll and unearth a new way of living. One of the key technological solutions to be used during the crisis are apps, specifically designed to tackle Covid-19. Apps bring a plethora of benefits, such as: helping monitor the spread of the virus, providing users with available testing measures and information on symptoms, and tracing users' contact with other infected users. The intention is that contact tracing apps will be one of a number of important elements to support the gradual lifting of border controls within the EU and the restoration of freedom of movement. However, much of this functionality signifies a grave threat to users' privacy and could ultimately be at risk of breaching privacy legislation worldwide.

The guidance

On 17 April 2020 the European Commission issued a Communication providing guidance on the compliance with privacy legislation of these apps (2020/C 124 I/01). The EDPB followed this by adopting guidelines on 21 April 2020 on the use of location data and contract tracing tools in the context of the pandemic (**Guidelines 04/2020**). These two sets of advice essentially provide a roadmap for app designers to follow to help ensure that their apps adhere to the GDPR and ePrivacy Directive. The two authorities' guidance is summarised by the checklist below:

- in order to win greater trust among the population and due to the sensitivity of the data involved, the Commission suggests that the relevant national health authority should be designated as data controller

- the guidance only applies to apps which are installed and used by users voluntarily and have one or more of the following functionalities: (i) information function; (ii) symptom checker function; (iii) contact tracing function; and (iv) telemedicine function
- users' rights should be guaranteed
- apps should be automatically deactivated when the pandemic is declared to be "under control", and this should not depend on users uninstalling it
- data minimization should be a key principle in determining which categories of data are to be processed (for instance, it clarifies that apps for contact tracing should use Bluetooth technology rather than geolocation data, as such technology ensures the fulfilment of the purpose without requiring the tracking of users)
- limits on accessing and disclosing data must be ensured
- the precise purpose for processing data should be clarified to users and using a blanket purpose such as "preventing further COVID-19 infections" would not meet the threshold. Instead, a separate purpose for each app function should be identified, to which users should be able to consent or refuse individually
- data retention should be strictly limited and based on "medical relevance" only, otherwise deleted. Security measures should be in place to ensure this
- accuracy of data should be ensured
- Data Protection Authorities are to be involved and consulted on app development. Reference is made to Art. 35 GDPR on the need for data protection impact assessments to be performed in relation to large-scale processing of special categories of data.

Why is this important?

The guidelines acknowledge that increased attention must be paid when using apps with contact tracing to minimise interferences with private life while still allowing data processing, with the goal of preserving public health. As pointed out by the Commission, "*People must have the certainty that compliance with fundamental rights is ensured and that the apps will be used only for the specifically defined purposes, that they will not be used for mass surveillance, and that individuals will remain in control of the data*". As such, the guidelines are intended to limit intrusiveness and ensure a common approach that will be trusted by citizens.

Any practical tips?

The guidance is a useful framework for the developer of an app to follow to help ensure its adherence to the privacy legislation. It should be noted that the guidance is not legally binding and it is therefore up to app developers to decide how best to proceed. It is notable that several different models of app are already taking shape; some do not follow the guidance of the Commission and it remains to be seen how regulators, particularly those in the EU, will approach them. What is certain, however, is that regulators across the EU are likely to look unfavourably on apps which do not follow the guidelines.

Summer 2020

Data protection

Data regulation and oral communications

David Scott v LGBT Foundation Ltd [2020] EWHC 483 (QB) (3 March 2020)

The question

Are oral communications caught by the Data Protection Act 1998 (**DPA**)?

The key takeaway

The UK High Court ruled oral disclosures (in this case provided during a telephone call) do not constitute "data", for the purposes of the DPA 1998, and consequently do not fall within the scope of the General Data Protection Regulation (**GDPR**) that has now superseded it.

The background

The LGBT Foundation (the **Foundation**) is a charity which provides a wide range of services including counselling, as well as advice in relation to health and wellbeing. In 2016, the claimant, Mr Scott, referred himself to the Foundation and disclosed details of his substance use and self-harm. Following an initial assessment meeting with Mr Scott, the Foundation shared that information with Mr Scott's GP practice over the phone, due to concerns for Mr Scott's welfare. While the call was entered into the GP's records, no documents or written records were shared with the GP by the Foundation, and communications with the GP practice were entirely verbal.

The Foundation's confidentiality policy (which was set out in a self-referral form that Mr Scott had filled in before his initial assessment with the charity) provided that if there was a reason to be seriously concerned about welfare, the Foundation may need to break confidentiality without seeking consent.

Mr Scott's claim was that the oral disclosure by the Foundation to his GP practice was: a breach of the DPA 1998; a breach of confidence at common law; and contrary to the Human Rights Act 1998. The Foundation sought summary judgment and/or a striking out of the claims.

The decision

The DPA 1998 was in force at the time of the disclosure. It was repealed with effect from 25 May 2018 and replaced by the GDPR and the Data Protection Act 2018. It was held that an oral disclosure of information did not breach the DPA 1998 and the claim should be struck out. The Court made it clear in its decision that the definition of "data" under the DPA 1998 is limited to information that is recorded electronically or manually, it does not extend to *oral*

information. The Judge agreed with the Foundation that a claim under the DPA 1998 could only arise where there had been processing of "personal data" which, to satisfy the definition in s 1 of the DPA 1998, must be recorded in either electronic or manual form. As such, a verbal disclosure did not constitute the processing of personal data, and thus could not give rise to a claim under the DPA 1998.

The court considered that, even if the disclosure had constituted data processing, the Foundation's disclosure was necessary to protect Mr Scott's vital interests, which meant that the Foundation could have relied on an exception to the general restriction to processing of sensitive personal data in any event.

Mr Scott's other claims were also struck out. Although a duty of confidence was owed to Mr Scott, this confidentiality always had a "carve out" attached to it permitting the very limited disclosure to his GP that Mr Scott was made aware of. The Foundation was also not a public authority for the purposes of the Human Rights Act 1998, and there was no reasonable expectation of privacy in the context to engage Article 8 ECHR either. If there was an interference, it was justified, as it was made with a view to his GP helping to reduce his risk of suicide or other substantial self-harm.

Why is this important?

In reaching the conclusion that oral disclosure does not contravene the DPA 1998, the Court referred to Article 2(1) of Directive 95/46/EC of the Data Protection Directive (implemented by DPA 1998). This Article essentially states that the relevant personal data must be processed by automated means or form part of a filing system or be intended to form part of a filing system. The same provision is quoted almost word for word in the GDPR and as such the position that verbal communication does not constitute data processing would very likely apply under the current data protection regime.

Any practical tips?

This case should serve as a valuable and timely reminder to consumers to read terms and conditions to ensure awareness of what can, and may, be done with personal information/data.

Additionally, businesses should consider looking at their policies and training materials to ensure that the notion of what constitutes "data" for the purposes of processing personal data has been correctly understood.

Summer 2020

Digital

Fake reviews probed by CMA

The question

What is the CMA's investigation into misleading online reviews all about and what are websites doing to combat fake reviews?

The key takeaways

The CMA has launched an investigation into fake and misleading review content online and the steps taken by several major websites to combat this. Several websites have made commitments to combat fake reviews on their platforms. Examples of steps websites can take include: (1) removing fake and misleading review content and profiles that write those reviews; (2) updating community guidelines to make it clear such content is prohibited; and (3) implementing robust systems to flag and remove such content in the future.

The background

The COVID-19 lockdown has caused consumers to rely on online shopping more than ever. The importance of genuine online reviews has increased accordingly. If a consumer decides to purchase a product or service online based on a misleading review, they could end up wasting their money and time on a product or service they did not want.

On 22 May 2020, the CMA launched an investigation into several major websites, to determine what steps they are taking to protect consumers from fake and misleading reviews. The investigation looked into issues including: (a) suspicious reviews; (b) the presentation of reviews; and (c) how reviews produced by reviewers who have been incentivised by payments or other benefits are handled. The investigation is set against the background of a wider programme tackling fake and misleading online reviews.

Instagram made a commitment to the CMA to combat the buying and selling of fake reviews. By 22 May 2020, it had removed 76 profiles being used to "trade, or facilitate the trade" of fake and misleading reviews after the CMA flagged problems on its site. Last year, Facebook and eBay also gave similar commitments.

The CMA is not the only entity seeking to combat the problem of fake reviews. Consumer group Which also looked into the practice of groups recruiting reviewers to write fake or incentivised reviews. Sellers offered free products in exchange for positive reviews on Amazon.

Steps to consider

In advance of the CMA investigation results being published, a number of points can be distilled from Instagram's commitment to the CMA to combat fake reviews. These may be applicable to other websites which allow users to post reviews.

Instagram has committed to updating and revising its policy guidelines to clarify it prohibits fake and misleading content on its platform, taking down content which Instagram and the CMA has identified as misleading, and putting systems in place to remove offending material from its website in the future.

Why is this important?

The CMA has resolved to take regulatory action against websites which are not doing what is required of them under advertising laws to crack down on fake reviews. Its enforcement will seek to secure the necessary changes to be made by the website, pursuing action through the courts if necessary.

Any practical tips?

Websites should remove fake and misleading review content on their platforms. This includes the removal of profiles used to trade, or facilitate the trade of, fake and misleading online reviews.

Websites should also update their terms and conditions and community guidelines to clarify that they do not tolerate fake and misleading review content.

Given how hard the wind now seems to be blowing against all misleading content, the impetus on platforms to implement robust systems to detect and remove fake reviews (including via staff training) has never been greater.

Summer 2020

Consumer

Consumer rights enhanced by the Omnibus Directive (part of the "New Deal for Consumers")

The question

What exactly is the Omnibus Directive? And how is it strengthening consumer rights?

The key takeaway

Consumer protection is being strengthened, with increased enforcement and transparency measures. This includes extending rights in respect of "free" digital services.

The background

The EU has committed to improving consumer protection in a strategy sometimes labelled the "New Deal for Consumers". As part of that strategy, the Omnibus Directive (**Directive**) came into force on 7 January 2020.

Member States have until 28 November 2021 to adopt the Directive, and until 28 May 2022 to bring it into force. Since it appears that the UK will not be part of the EU by November 2021, it is likely that there will be no obligation to adopt it here. However, a publication from the UK Government would suggest that it also has similar domestic consumer protection legislation in mind.

The legislative amendments

Following a 2017 Commission review of consumer protection regulations and laws (the **REFIT Fitness Check**), the Commission determined that the following Directives needed updating:

- the Unfair Commercial Practices Directive (2005/29/EC)
- the Consumer Rights Directive (2011/83/EU)
- the Unfair Contract Terms Directive (93/13/EEC)
- the Price Indications Directive (98/6/EU).

The update will focus on consumer issues, including penalties for breach, protection in relation to "free" digital services, rights of withdrawal and transparency in online marketplaces.

Key elements

- **Enforcement**: the Directive allows for GDPR-style fines worth a minimum of 4% of a company's annual turnover in the relevant Member State or €2m if a calculation is not possible. Member states can look to introduce higher fines during the implementation period.
- **Consumer claims**: it also grants rights directly to consumers, allowing them to individually pursue claims against any companies in breach.

- **Digital goods and services:** these will now be caught by the definition of goods and services and rights harmonized to match physical goods and services.
- **Transparency**: traders must provide information on their criteria for rankings search results, justify steps taken to ensure reviews on their site are genuine, and inform consumers whenever prices have been personalised. Online marketplaces must inform consumers whenever an item is bought from an individual, and if so that they will not benefit from EU consumer protection law.
- **New obligations on traders and online platforms**: the aim being to better protect consumers.
- **Free digital services**: existing EU consumer protection laws will now extend to services paid for with personal data, due to a change in the definition of "price".

Why is this important?

A key change in this development is the potential size of fines following a breach, following the imposition of a more heavy-handed enforcement regime. Note that if the UK does not implement this Directive but follows through with what has been proposed domestically, fines for consumer protection non-compliance could reach up to 10% of a firm's global revenue. In addition, with class actions generally on the rise (as seen in recent data breach cases), it is not difficult to see this area also attracting similar levels of consumer claims.

Any practical tips?

Begin preparations to ensure your existing transparency mechanisms are up to the additional obligations and improve them if not. Ensure also that any involvement in the provision of "free" digital services meets the same consumer protection standards as anything which is paid for. And look out for UK implementation of this Directive, or whatever domestic alternative is decided on – it could have an even sharper financial bite than that in the Directive.

Summer 2020

Consumer

Rogue online sellers up against new UK consumer-protection weapon

The question

What are the new powers granted to the UK's Competition and Markets Authority (**CMA**) to combat rogue trading in the digital arena?

The key takeaway

The CMA has acquired new EU-derived powers under the new Consumer Protection (Enforcement) (Amendment etc.) Regulations 2020. These allow it to seize control of the accounts of rogue traders on eBay, Amazon and other e-commerce accounts, and even their entire websites, if it thinks "consumer interests" are being harmed.

The background

There has been a long history of campaigns from the CMA for its consumer-law powers to be bolstered through the statute books, which has grown broader and deeper over time. The CMA has routinely warned in recent years that several business sectors are hurting consumers. Its end goal is a sweeping overhaul of its consumer-law powers, as proposed to the Government early last year.

The guidance

The new Consumer Protection (Enforcement) (Amendment etc.) Regulations 2020 came into force on 2 June 2020 and entered UK law as a result of changes made at EU level. Effectively, the new rules will give the CMA a formal means to require the removal of a website or certain pages, apps or social-media posts when the traders implicated are not willing to cooperate.

Anything considered an "online platform" is up for seizing under the Regulations, which comprises "any software, including a website, part of a website or an application, that is operated by or on behalf of a trader, and which serves to give consumers access to the trader's goods and services". This could potentially apply to the biggest to the smallest e-commerce platforms.

Anything deemed to "harm the collective interests of consumers" known as a "community infringement" could elicit the CMA to seek an "online interface order" (**OIO**). Community infringement covers any type of infringement that cuts across consumers' interests, including unfair terms, misleading information or unfairly refused refunds. People and companies targeted by OIO's could be forced to delete their websites or parts of them, disable or restrict

access to them, display a warning to consumers, or even transfer an entire domain name into the CMA's control, should they be deemed used for ill purposes.

However, whilst the UK's regulatory armoury may seem relatively unparalleled, there are judicial constraints that could blunt their edge. In order to safeguard the public from misuse of the new powers, the CMA will have to apply to a court and convince a judge that there is no other way to stop a rogue trader apart from seizure and/or deletion of their website or online sales accounts. While the regulator would only resort to an OIO where it is deemed that there is no other available or proportionate way to deal with an infringement, the two-step process that requires the enforcer to seek approval of an OIO from UK court judges could hinder their use.

Why is this important?

Consumers should be able to trust online markets, and this newfound power will strengthen protection by allowing the CMA to remove online content when it threatens consumers' interests. Given the current debates about the imposition of a vague "duty of care" on platforms, it is reassuring to see an approach centred on judicial oversight, in the form of a court order. This should give confidence to a platform on the receiving end of one of these orders that the action they are being compelled to take has received a reasonable degree of independent scrutiny.

Any practical tips?

Some bigger companies see the new measures as aiming at smaller e-commerce sites that might not have an established cooperative dialogue or mature compliance policies with which to effectively police sellers. Nevertheless, such wide application may make bigger platforms nervous too, as the new rules could make for a resource-sapping new headache for platforms which are already facing increasing scrutiny under the regulatory microscope.

Summer 2020

ASA: Annual Report

A summary of the ASA Annual Report 2019

The question

What are the key points arising from the Advertising Standards Authority (**ASA**) 2019 annual report, published on 3 June 2020?

The annual report

The ASA highlighted three key themes in their 2019 report, as follows:

1. using Technology and working with online platforms
2. prioritisation and partnership working
3. protecting vulnerable people.

Key notes in the report include:

- The ASA launched an Avatar Monitoring which analyses online ads using "avatars" that mimic the browsing of children and young people. This has allowed the ASA to catch careless targeting by gambling operators and brands promoting high fat, salt or sugar foods.
- It focused on prioritisation, partnership working and process improvement, achieving targeted reduction in rulings, in particular by reducing formal investigations into non-sensitive website advertising by small businesses and prioritising an "education first" approach to resolving lower detriment cases.
- It also piloted a systematic approach to tackling pricing issues by a big online retailer, supporting additional verification of reference prices to improve the quality of pricing information displayed to consumers.
- It won two out of two judicial reviews, involving CityFibre and Actegy.
- It is rooting out new ways to tackle scam ads more systematically. Successful delivery of the ASA strategy will involve working more closely with the platforms, combining their substantial investments in ad review systems with ASA independence, regulatory expertise and ability to build positive relationships between stakeholders.
- It notes that it agrees that political advertising should be regulated, though it is not the right body to lead political advertising regulation. It is however ready to explore how it may share its expertise to a more collaborative regulatory arrangement.
- It noted the six strands of their strategy: People, Online, Effectiveness, Buy-In, Enforcement and Independence. It noted it will work with online platforms to protect people from irresponsible ads, as well as deliver regulatory projects on ads that cause the most detriment to people.

- Other key activities demonstrating performance against the ASA's objectives include setting up an ASA/CAP online forum with representatives from online platforms and networks to help improve regulations of online ads.

Using technology in the workplace

- The ASA has been using avatars to monitor age restricted ads. This has helped them monitor, for example, online ads for high fat, sugar or salt (**HFSS**) food and drinks. The ASA identified a number of ads for HFSS products were served in children's online media, in particular YouTube videos aimed at children.
- It enforced a Botox ads ban. A sector wide compliance project in partnership with the Medicines and Healthcare products Regulatory Agency (**MHRA**) occurred. Over 12,000 problem posts were removed from Instagram in the first quarter of monitoring.
- It is using Brandwatch, a social intelligence tool, to strategically monitor ad content online. Using Brandwatch, the ASA can observe trends across a range of online content, such as gender presentation in ads, and also look closely for individual breaches of the advertising rules such as unlabelled ads from individual influencers.
- It is working in partnership with the major ad platforms and networks, and has developed a Scam Ad Alert system to share information about paid-for scam ads. This system allows ad networks to respond quickly to remove them and prevent similar ads appearing.
- It has been working closely with brands and influencers to ensure that they know when to label their ads eg creating a "cheat sheet" for Love Island contestants.

Prioritisation and partnership working

- By implementing an "education first" approach, the ASA resolved a significant number of claims seen on the websites of SMEs without employing a lengthy investigation process, particularly where issues related to harm and offence.
- It has issued advice notes for minor breaches for SME website claims. These give details of why the ad was in breach, and how to amend it.
- It has been working in partnership to tackle misleading pricing references.
- ASA rulings give the HMRC leverage to crack down on misleading tax avoidance schemes also.

Protecting vulnerable people

- This includes working with advertisers to create responsible ads for cosmetic procedures, such as working with MYA to ensure the focus of their ads did not imply that aspirational lifestyles can only be achieved through cosmetic surgery.
- 2019 further saw the first results of a new rule banning harmful gender stereotypes in advertising. There has been CAP guidance published that outlines scenarios that would be considered problematic regarding gender stereotyping.
- The ASA has been working on banning vaping ads on Instagram – in December 2019, the ASA ruled that e-cigarette ads posted from a public Instagram account were not consistent

with the restrictions on E-cigarette advertising on the media, setting a new standard for the industry. E-cigarette brands are required to make their Instagram accounts private so their posts could only be seen by those who actively chose to follow them. Separately, Instagram has decided to remove vaping products from certain aspects of their platform.

- In April 2019, new guidance on gambling and the protection of children and young people came into effect. It adds to the existing guidance of targeting of ads, covering all media including social media and other online platforms. The guidance provides details of unacceptable types of content, including use of popular celebrities and characters for children.
- The ASA has been monitoring the TV ads that children can see, including alcohol, gambling and HFSS food and drinks ads.
- It provided a summary of their complaints and cases; in context. Namely in 2019, the retail sector had the most ads amended or withdrawn.
  - 8,881 ads were amended or withdrawn in 2019, an 18% decrease on 2018 but the second highest total ever.
  - Almost 3x as many online cases were resolved as TV cases in 2019.
  - Trends show that complaints about influencer posts made up more than ¼ of all online complaints.
  - There was a 13% decrease in retail cases, though an 8% increase in leisure complaints.
  - There was a 36% increase in food and drink complaints, though an 18% decrease in business cases.
  - Over ¾ of non-broadcast cases concerned potentially misleading ads, compared with just over 1/3 of broadcast cases.
  - 3% more complaints were resolved than in 2018.
  - Four out of six turnaround KPIs were met.

Why is this important?

The ASA has a six-strand strategy and has been looking at ways of improving efficiency. It has been using AI and innovation to assist in ensuring that ads are compliant, such as the use of avatars and collaborating with platforms to remove ads in breach of the CAP Codes. It has been implementing technology to monitor ads and has enforced bans such as those against Botox ads.

As such, in 2019, the ASA resolved 34,717 complaints relating to 24,886 ads, 70% of which were potentially misleading. In addition, it resolved 4,469 own-initiative compliance cases resulting in 8,881 ads being amended or withdrawn. 99% of formal cases were enforced. 62 sanctions were applied leading to compliance, and only nine advertisers needed to be referred to Trading Standards for further action.

Summer 2020

ASA: Surveys

CAP's new "Quick Guide to Advertising Consumer Surveys"

The question

How does the new "Quick Guide" ensure that marketing claims are made in a manner that complies with the CAP Code?

The key takeaway

Survey headlines should precisely reflect the survey, and the sample size should be appropriate, statistically significant, and representative.

The background

Consumer surveys are a useful tool in promoting a product or service and highlighting the strength of a brand'

s reputation but the most common pitfall that marketers fall into is when their ads misleadingly represent their survey's findings. On 27 February 2020 the Committee of Advertising Practice (**CAP**) published "A Quick Guide to Advertising Consumer Surveys" as a helpful starting point for the use of consumer surveys in advertising.

The guidance

In its guide, CAP stresses the importance for marketers to make clear that their claims are actually based on consumer surveys as opposed to more objective measures.

Marketers also need to ensure that the sample that they use is of sufficient size to justify the claim that they are making – this will be judged on a case-by-case basis. However, the headline claim is likely to be considered misleading if it cannot be substantiated by a suitably large sample size. Where a sample size is not suitably large, marketers are required to amend their headline claim to ensure that it does not misleadingly exaggerate results.

Marketers are also not prohibited from selecting specific individuals or groups to form the basis of their sample, in order to extract a specific or favourable view. However, this does not prohibit selective samples from being used without the marketing communication disclosing that the sample had been specifically selected. In particular, marketers should not make a claim, explicit or implied, regarding the general population, if they are using a sample which is unlikely to represent the views of the general population. This principle can extend beyond sample groups that are customers, to include age ranges that do not represent the population.

Why is this important?

As many marketers tend to contravene the CAP Code in the way they communicate their findings when advertising claims for consumer surveys, this guide will help them stay on the right side of the line so as not to mislead the public when making future claims. Equally, if you feel that a competitor is adding a little too much gloss to their survey claims, the guide should prove a useful resource for planning your best avenues of attack.

Any practical tips?

Some key questions marketers can ask themselves so that they do not fall foul of the CAP Code in the way that they communicate their findings are:

- "Does the headline claim accurately reflect the survey?"
- "Is the sample size statistically significant"
- "Is the sample representative?".

Advertisers are also advised not to ignore earlier CAP guidance – "Substantiation: Consumer surveys and sample claims" – which addresses further key questions that arise in relation to survey data and sample claims. In particular, the earlier guidance warns against making claims based on extrapolated conclusions and stresses the need to ensure that ads do not mislead by exaggerating the results of the survey from which the conclusion is drawn.

Summer 2020

ASA: Pricing

Make sure the price is right: using reference pricing in ads – Committee of Advertising Practice releases update on pricing practices

The question

What are the key points to be considered when using reference pricing in your promotions?

The key takeaway

The ASA's updated guidance is a short but useful reminder of how businesses are expected to responsibly utilise reference pricing promotions, including "was-now" and RRP.

The background

The ASA has revisited its research into consumer understanding of reference pricing, which showed that consumers have a limited understanding of pricing practices, particularly reference pricing, and expect that reference prices are regulated and can therefore be trusted. The research was initially published in 2018 and clearly the ASA still thinks that more needs to be done in this area to ensure that trusting consumers are not taken advantage of. To this end, the ASA has published updated guidance as a reminder of the key points to consider when using referencing pricing in promotions.

What is reference pricing?

Broadly, reference pricing relates to pricing initiatives where a competitive price is made more attractive to consumers through comparison to a less attractive "reference price". Retailers often compare the lower advertised price of a product to the higher reference price, which may be the price at which the product was previously sold (often represented using "strike-through" and "was-now" prices) or a price recommended by a manufacturer or a competitor's price (the recommended retail price (**RRP**)). The ASA regulates and enforces reference pricing through the CAP Code, which reflects the Consumer Protection from Unfair Trading Regulations 2008.

Key reference points

The ASA guidance suggests that responsible businesses should consider these five key points to ensure that reference pricing in ads are not misleading:

1. Use the selling price for that particular sales channel. If the advertised reference price is not the usual selling price through the same sales channel in the ad (eg online or in store) or it was only charged at a limited number of stores, it is likely to mislead consumers.

2. Reference prices should be charged for longer than promotional prices. Generally, the higher reference price should have been charged for a longer period of time than the promotional price. A promotional price that has been charged for longer than the higher reference price may itself become the reference price and is likely to be misleading.
3. Sales matter. The number of sales made at the higher reference price will be taken into account. There should be evidence of "significant sales" at the higher reference price (significance will depend on the product and usual buying behaviours for that type of product) or that the reference price was a realistic selling price. Where only a small number of sales were made at the higher price, the reference price will not be deemed to be the usual selling price.
4. Use the most recent established price at which the product was sold. Beware increasing the price for only a short period of time immediately before the promotion, as this will likely be viewed by the ASA as a misleading exaggeration.
5. Use the usual price. Reference prices should be genuine and not artificially inflated or created. In particular, Rule 3.40 of the CAP Code prohibits the use of RRPs which differ significantly from the price at which a product is generally sold. RRPs should accurately reflect the price consumers will generally pay for the product across the market.

Why is this important?

The ASA's succinct guidance serves as a helpful reminder of what is expected of businesses that use reference pricing in their marketing. It is important to consider the ASA's key points and get this right from the outset; recent ASA decisions, such as the upheld complaint in respect of Zestify Media's "was/now" reference pricing (see our previous Snapshot), demonstrate that businesses may fall foul of the rules, even where they had no intention to mislead consumers, if key pricing elements are not satisfied.

Any practical tips?

Businesses wanting to utilise reference promotions should ensure that they comply with the ASA's five key points to ensure their pricing does not mislead consumers. Practical steps may include:

- thinking about how the chosen sales channels may affect the promotion. For example, be sure to use the usual selling price on the website for website promotions and use a reference price charged across a majority of stores for store promotions. A reference price used online for a product previously only sold in stores is unlikely to be acceptable
- track the length of time that promotional prices are used. Once the promotional price has been changed for longer than the reference price, it is likely to be considered the new reference price for the product
- if there are not already "significant sales" of the product at the reference price, think realistically about the chance of sales at that price before using it
- avoid increasing product prices immediately before the promotion – you could be misleadingly exaggerating the saving

- base RRPs on the usual price at which the product is sold in the market. It will not be enough to say that the RRP was recommended by a manufacturer and RRPs cannot be objectively used where there is only one product on the market.

Summer 2020

ASA: Superiority claims

ASA ruling on EE – misleading and ambiguous mobile network claims

The question

Can mobile network providers claim superiority for a service they provide on their network in their ads?

The key takeaway

Mobile network providers should not mislead consumers by suggesting that the service offered by competitors did not provide the significantly faster speeds that 5G was expected to provide. Furthermore, mobile network providers should be clear in their distinction between a service they provide on their network, and how they brand themselves.

The ad

EE: A national press ad, an outdoor poster, a website, a regional press ad, an Instagram post and a paid-for Instagram post for mobile network provider EE, were seen in May, June, September 2019 and February 2020:

(a) The national press ad, seen on 30 May 2019, featured text which stated "*5G. NOW ON THE UK'S NO.1 NETWORK. Search 5GEE*". Small print was included at the foot of the ad.

(b) The outdoor poster, seen on 2 June 2019, featured text which stated "*5G. IT'S GOT TO BE EE. This is 5G, now on the UK's No. 1 network. Search 5GEE*". Small print was included at the foot of the ad.

(c) The website www.ee.co.uk, seen on 7 June 2019, featured text which stated "*This is 5G, now on the UK's No.1 network*".

(d) The regional press ad, seen in the City AM newspaper on 2 September 2019, featured text which stated "*UNLIMITED DATA UNRIVALLED NETWORK. Get unlimited data on the UK's No.1 network*".

(e) The Instagram post, seen on 2 September 2019, featured text which stated "*UNBEATABLE, UNREPEATABLE, UNTOUCHABLE, UNBELIEVABLE, UNFORGETTABLE, UNFLAPPABLE, UNREPEATABLE, UNLIMITED, UNRIVALLED. Unlimited data on the UK's No.1 Network. Who says you can't?*".

(f) The paid-for Instagram post, seen on 26 February 2020, featured an image of a mobile phone above text which stated "*EXCLUSIVELY ON THE UK'S NO.1 NETWOR*K".

Hutchison 3G UK Ltd t/a Three: A tweet and a wraparound national press ad, seen in August 2019, promoted Three's 5G service:

(g) The tweet stated, "*If it's not Three, it's not real 5G*", and included images of several products including a Superman-like action figure called "Special Man" and "Burt Sampson".

(h) The press ad, a wraparound in the Metro newspaper, stated, "*If it's not Three, it's not real 5G … We're building the UK's fastest 5G network*". The rear of the wraparound stated, "*Spectrum is the wobbly air that network need to transmit data – and we've got more 5G spectrum than anyone else. Plus, not all spectrum is created equal. We're the only UK mobile network to have 100MHZ of 5G spectrum in one big block that's real 5G. We're building the UK's chunkiest spectrum leading, router bursting, lag punishing, speed dominating 5G network. When the future comes, you'll be glad you've got 5G. When the future comes, you'll be glad you're on Three*".

The complaint

The ASA received complaints challenging whether ads (a), (b) and (c) misleadingly implied that EE was the top rated network for 5G capability. Complainants also challenged whether the claims "No.1 network" in ads (a), (b), (c), (d), (e) and (f),"UNRIVALLED" in ads (d) and (e) and "UNBEATABLE" in ad (e) were misleading because a relevant measure was not used and because the small print was either absent or insufficiently prominent.

The ASA also received complaints challenging whether the claim "*If it's not Three, it's not real 5G*" was misleading.

The response

EE responded noting they separated the reference to 5G from the "No. 1 network" claims to ensure that none of the claims stated they were "No. 1 for 5G". EE further stated they drew a distinction between the new availability of 5G and the "No. 1 network" claim through use of the word "now". EE state they made it clear that the new technology had been added to the existing network through the use of the word "on".

EE stated that they had been using the "UK's No.1 network" claim for the previous six years without any challenge from any competitor because they were the largest single network in the UK, and the EE network had outperformed all other mobile networks on objective, relevant and measurable performance metrics for each of the last 6 years, as assessed by RootMetrics.

EE stated that each of the ads stated "on the UK's no.1 network", and that 5G and data-use were both features related to a consumers' experience of using the EE network, enhancing the experience of using their mobile phone. They were not related to ancillary features of the EE business, and the ads did not say that people could get 5G or unlimited data "from" or "with" the UK's no.1 network, rather that they got them on the network.

In relation to the complaints against Three, Three believed the extent of their 5G spectrum and the infrastructure of their network set them apart from their competitors. They believed the

technicalities of 5G were not well understood by consumers, and there was a limit to how much explanation could be included in an ad. Further detailed technical information for consumers was accessible on their website.

Three said the structure of their network (a cloud core and 20 data centres across the UK) delivered the lowest possible latency and better service experience. Three overhauled their network and service delivery systems to increase resilience and capacity and reduce latency, in order to accommodate the expected increase in data usage that would come with 5G.

They further cited the views of the International Telecommunication Union, the European Conference of Postal and Telecommunications Administrators, the GSM Association (a trade body for mobile operators) and Huawei on the importance of a 5G operator having at least 100 MHz of bandwidth if they were to deliver high speed, low latency services. Three believed that as they had access to this bandwidth, it set them apart from other 5G operators, none of which had access to 100 MHz of bandwidth, and that this was what the reference to "real 5G" was intended to relate to.

The decision

In the earlier ruling against Three, the ASA considered consumers were unlikely to be familiar with the technical specifications of 5G and that they would primarily associate it with speeds that were significantly faster than 4G services.

The ASA considered they would interpret the ads to mean that the 5G services offered by other providers would not provide those significantly faster speeds and that there was little value in obtaining 5G from them. The ASA obtained informal advice from Ofcom and understood 5G would provide faster speeds and improved responsiveness; more capacity for the increased number of devices that would be connected and the ability to handle more data, compared with 4G services.

The ASA acknowledged that, all other factors being equal, greater bandwidth would allow a provider to support greater traffic capacity. However, because take up was still so limited, differences in 5G capacity between networks were unlikely to result in material differences in the experiences of end users at the time the ad appeared. The ASA considered Three's 5G service was not, at that time, likely to be so significantly better than other 5G services as to render them not "real" 5G, therefore concluded that the claim "*If it's not Three, it's not real 5G*" was likely to mislead.

In its later ruling against EE, the ASA considered that the words "now on" in each of the three ads, in addition to the full stop after "5G" in ad (a), created a degree of separation between the claim of 5G provision and the claim about EE's network rating, and suggested they had been the "No. 1 network" before the addition of 5G. The ASA considered that consumers would

understand the claims in ads (a), (b) and (c) to mean that 5G capability was now available on EE, and EE had separately been rated the UK's top mobile network operator. The ASA concluded that the ads were unlikely to mislead on that point.

However, the ASA held that the ads were likely to mislead on the points regarding "UNBEATABLE" and "UNRIVALLED". The ASA considered that this would be understood by consumers to relate specifically to the "No. 1 Network" claim in the ad, comparing EE with other mobile network operators. The word "network" could also mean physical infrastructure of a network, as intended by EE. Given the number of potential interpretations of the claim, the ASA considered that it was ambiguous and the basis of the claim was therefore likely to be material to consumers in order for them to make an informed decision.

Why is this important?

The ASA acknowledges the ambiguity of claims such as "No.1" and "Unrivalled" though requires the basis of these claims to be made clear. This is evident in both its rulings against EE and Three. Additionally, advertised claims must be true to the consumer's experience in terms of what the claimed technology actually achieves in the marketplace at the current time. If the substantiation is lacking, then the ad may be deemed misleading.

Any practical tips?

- Avoid using wording which suggests that the service offered by competitors does not provide the level of value the service is expected to provide.
- Be clear on how a service is to be provided in order to avoid misleading consumers eg make it clear that a service is available on your specific network!

Summer 2020

ASA: Superiority claims

ASA ruling on ASTOK Ltd t/a TVBet – unsubstantiated superiority claims

The question

Did TVBet release ads which were misleading and unverifiable by claiming that they were #1 and that they had the biggest sports jackpot?

The key takeaway

Always take great care with ads which claim that a business or service is "number one" or better than the rest of the market.

The ads

In September 2019, two ads appeared for Astok, a provider of live games to the betting industry:

- Ad (a): the first ad, which appeared on a media screen at a "Betting on Sports" trade show, featured the claim "The Biggest Jackpots"
- Ad (b): the second ad was a press ad seen in the iGaming Times and Gambling Insider. It claimed that TVBet was the "#1 World's Live-Games Provider".

The complaint

The ads were challenged by BetGames.tv, who queried whether the claims were misleading and could be substantiated. They also challenged whether they were verifiable

The response

TVBet argued that they had been ranked as number one in a list of live games providers and, as such, the claims were not misleading. They also noted that this information was publicly available at www.logincasino.org and that they would not use these claims in their future advertising.

The decision

The ASA focused on what those using the services would understand from the claims.

Ad (a)

The ASA considered that businesses would understand the claim "The Biggest Jackpots" to mean that TVBet offered a higher jackpot pay-out than all other live games providers, in relation to all their games. TVBet provided evidence from www.logincasino.org that listed TVBet as the provider offering the highest jackpot pay-out, but only out of 5 providers listed. The ASA noted that it was unclear on what that figure was based and that this information did

not satisfactorily substantiate the claim that TVBet offered “The Biggest Jackpots”, as it was likely to be interpreted. The ASA ruled that this claim was misleading and breached the CAP Code.

Ad (b)
The ASA also considered that the claim “#1 World’s Live-Games Provider” would be understood by businesses to mean that TVBet’s live games offering was the bestselling on the market. In order to substantiate this claim, therefore, TVBet had to present evidence that they were the bestselling live games provider across all its games offerings.

TVBet again referred to the ranking from www.logincasino.com. However, this alone was once again insufficient as it only took into account business-to-Business providers of live games. TVBet provider no further evidence to substantiate the claim that they were the best-selling live games provider across all their games offering. Therefore, the ASA concluded that this claim was also misleading and breached the rules 3.1 (Misleading Advertising), 3.7 (Substantiation) and 3.33 (Comparisons with Identifiable Competitors).

In addition, the ASA ruled that these ads were unverifiable. The CAP Code requires that comparisons with identifiable competitors must include (or link to), information that allows businesses to understand and verify the comparisons. The ASA concluded that these comparative claims by TVBet did not contain or direct businesses to information that could allow them to do this, which was a breach of CAP Code Rule 3.35 (comparisons with identifiable competitors).

Why is this important?
The ruling is a reminder that all comparative superiority claims need to be capable of substantiation, including those which refer to the “biggest” or “number one”.

Any practical tips?
Remember that you always need to provide verification when making comparisons with identifiable competitors. This aspect of compliance is often missed in comparative ads.

Summer 2020

ASA: Promotions

ASA ruling on Boohoo.com – "Up to x% off everything" and countdown clocks

The question

Can retailers use time limited offers on their website (eg using countdown clocks), and claim they have a sale of "*up to x% off everything?*". Does the line "*applicable to selected lines only*" work as a disclaimer if not "all" your products benefit from the discount?

The key takeaway

Retailers are not allowed to imply that all products are included in an offer if certain products are excluded. Retailers should also not use time limited discount offers if that is not the case.

The ad

Two ads for the online fashion retailer, Boohoo.com UK Ltd t/a Boohoo, were seen in November 2019:

- Ad (a): An email featured a headline which stated, "*UP TO 60% OFF EVERYTHING* + AN EXTRA 10% OFF DRESSES, TOPS AND JUMPSUITS***". Smaller text below stated, "USE CODE: PARTY10 ENDS MIDNIGHT". The corresponding asterisk stated, "**Up to 60% off everything is automatically applied and applicable to selected lines only. Limited time only. ** Use code PARTY10 for an extra 10% off dresses, tops & jumpsuits. Excluding sale and applicable to selected lines only. Ends midnight 04.11.2019*".
- Ad (b): The Boohoo home page displayed a headline which stated "*UP TO 75% OFF ABSOLUTELY EVERYTHING + AN EXTRA 10% OFF! CODE: EXTRA. ENDS 10PM*". There was a banner at the top of the page which stated, "*FREE NEXT DAY DELIVERY ENDS IN: 00:50:45*". At 10pm the Boohoo home page displayed the headline, "*UP TO 75% OFF ABSOLUTELY EVERYTHING + AN EXTRA 10% OFF! CODE: EXTRA. ENDS 11PM*". There was another banner at the top of the page which stated, "*FREE DELIVERY ENDS IN: 00:59:17*".

The complaint

The ASA received complaints that:

- the claim "*up to 60% off everything*" in Ad (a) only applied to selected items, thus complainants challenged whether the claim was misleading

- the offers reset after the countdown clock reached zero, therefore the complainants challenged whether Ad (b) misleadingly implied "*UP TO 75% OFF ABSOLUTELY EVERYTHING + AN EXTRA 10% OFF!*" would revert to the higher price once the countdown was over.

The response

Boohoo stated that the asterisk corresponded with text below which explained that the discount excluded certain lines. Boohoo believed that the qualification made it clear to the consumer that the excluded products were items that were typically excluded from all promotions they offered. Boohoo stated that the product lines that were excluded from the discount comprised less than 4% of their products.

Boohoo acknowledged that the use of a countdown clock was a mistaken use of the format. Following an internal review, they stated they would not use countdown clocks in ads unless the offer varied on their expiry.

The decision

Both complaints were upheld.

The ASA considered consumers would understand the claim "*up to 60% off everything*" to mean that all products on the Boohoo site were included in the promotion, whereby all products would be discounted, with a significant proportion of products being sold with a 60% discount.

The ASA considered that the presence of an asterisk after the claim and the corresponding text below which stated "*Excluding sale and applicable to selected lines only*" was not sufficient to counter the overriding impression of the ad that all products would be discounted. Because consumers were likely to interpret the claim "*up to 60% off everything*" as applying to all Boohoo products when in fact 4% of lines were excluded, the ASA concluded that the ad was misleading.

The ASA understood that once the countdown clock reached zero, it reset to repeat the same free next day delivery offer with a new countdown clock counting down to zero, and this re-occurred at every hour throughout the day. Likewise, the "*up to 75% offer*" also reset at the end of each hour with the same offer alongside a claim that the promotion finishes at the end of the hour. The ASA considered that consumers were likely to regard the offer as a time limited promotion and expect it to expire at the end of the countdown clock. The countdown clock was therefore likely to pressurise consumers into making swift transactional decisions, including purchasing the product, without giving their purchase the due consideration they normally would because of the misleading implication in the ad that the offer would run out at the end of the time period. The ASA concluded that the ad was misleading because consumers would expect the offer of free next day delivery to end and the 75% discount price

to revert to the usual price after the countdown clock ended, when in actual fact it reset at the end of each hour. This meant that the promotions were not actually time limited.

Why is this important?

Retailers should take care not to mislead consumers by implying all products are included in an offer if this is not the case. A "selected lines only" disclaimer won't help you. Retailers should also not use marketing techniques to pressure consumers into making swift transactional decisions, including purchasing a product, as a result of artificial time restraints.

Any practical tips?

A disclaimer can't qualify a headline claim, so beware stating that an offer applies to all products when there are in fact exclusions – and don't think a "selected lines" only disclaimer will help you in these situations.

Time limited offers which pressurise consumers into making hastier choices than normal are almost always going to be open to scrutiny, so only use them if you can be sure that the offer will end when the clock runs out.

Summer 2020

ASA: Influencer marketing

ASA ruling on ASOS – use of "affiliate" for a marketing communication

The question

Is the use of "affiliate" sufficiently clear to identify an affiliate advertorial as a marketing communication?

The key takeaway

Advertisers must ensure that affiliate links are obviously identifiable as marketing communications and must make clear their commercial intent upfront, for example, by including a clear and prominent identifier such as "#ad". The use of the term "affiliate" is unlikely to be sufficiently clear as a standalone label to ensure affiliate ads are obviously identifiable.

The ad

An Instagram story seen on Zoe Sugg's Instagram page on 6 July 2019 featured an image of Zoe wearing a floral maxi dress. Text stated "*Lots of you loving the dress I'm wearing in my newest photos! ... it's from @missselfridge Swipe up to shop … (Also popped it on my @liketoknowit profile if you'd rather shop straight from the app)*".

Additional text at the bottom right-hand side of the image, obscured by the direct message icon, stated "**affiliate*". Swiping up on the story took users to a product page on the ASOS website.

The complaint

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

The response

Asos.com t/a ASOS responded that Zoe Sugg was an ASOS affiliate, which meant that she could earn commission from ASOS sales through a third-party influencer network. ASOS stated that it did not have any advance knowledge of, or direct input or control over, the Instagram story in question but had made it clear to all of their affiliates that disclosure labels needed to be clear and prominent. ASOS accepted that the disclosure in Zoe Sugg's story was not sufficiently prominent, as it was obscured by the platform's on-screen graphics when viewed on a mobile phone. However, they stated that the use of the term "affiliate" should have been considered an adequate signpost of a purely affiliate relationship in place between

a brand and influencer. It added that “affiliate” was a clear and accurate description of the nature of the content.

To further demonstrate this, ASOS referred to the 2019 Ipsos MORI report on “*Labelling of influencer advertising*”, published in September 2019. They specifically referred to an example ad from Twitter (which was tested in the research) where a higher proportion of participants identified the example with “#advert” upfront and “#affiliate” at the end as being “*definitely an ad*” (48%) than the post with only “#affiliate” at the end (44%). The report stated that the difference was directional rather than significant. Based on this, ASOS argued that the lack of significant difference in understanding between the two examples demonstrated that “affiliate” was equally as suitable a label as “advert” or “#ad” to disclose affiliate ads.

Ms Sugg’s company, Zoe Sugg Ltd, said it had explained to users that she received an affiliate commission by using the identifier “affiliate”, and that users would therefore be clear as to the nature of the relationship between her and the third-party influencer network app.

ASOS also stated that the report showed that, in some instances, the term “affiliate” was better recognised than the term “ad” when used at the beginning of the text in an ad. It referred to an example Instagram story ad tested in the research where “#advert” was used at the start of the post and it was recognised as marketing communications by 43% of those surveyed. In another example, where “#ad” was used at the start of the text in an Instagram post, 36% of participants recognised it as an ad. ASOS also referred to another example where 38% of participants had recognised a tweet, which used the term “affiliate” at the end of the text, as an ad. Zoe Sugg Ltd said the findings demonstrated that the term “affiliate”, when used in the same placement as the term “ad”, was as least as likely as that label to result in an ad being identified as such.

The decision

The ASA upheld the complaint. Although it acknowledged that ASOS had no direct input into or control over the ad, the ASA nonetheless considered that, as the direct beneficiaries of the marketing material through an affiliate programme, it was jointly responsible for the ad and its compliance with the CAP Code.

Regarding the ad in question, the text “affiliate” was obscured by the app’s “direct message” icon. Although it acknowledged that the ad included references to the brand of the dress and a call to action to purchase it, the ASA did not consider the affiliate content sufficiently clear to indicate to users that there was a commercial relationship between Zoe Sugg and ASOS and that the story was an ad.

The ASA considered whether the term “affiliate” itself would be sufficient to obviously identify an ad as such. Both ASOS and Zoe Sugg Ltd had pointed to various examples in the research

which they believed supported the argument that “affiliate” was a sufficient label to communicate that content was an affiliate ad. However, only 38% of participants felt they would be able to confidently explain what the word “affiliate” meant when displayed on social media, which put it amongst the terms that participants were least confident explaining.

The ASA said that in no example where “affiliate” was used in isolation did more than 45% of participants recognise it as an ad, and the low levels of recognition of ads in the research overall demonstrated the difficulties of obviously differentiating ads from other content on social media platforms. It considered that the term “affiliate” was therefore unlikely to be sufficiently clear as a standalone label to ensure affiliate ads were obviously identifiable.

The ASA concluded that the ad was not obviously identifiable as such and did not make clear its commercial intent. It therefore breached CAP Code Rules 2.1 and 2.3 (Recognition of marketing communications).

Why is this important?

The ASA upholding the complaint is a clear warning to retailers’ and brands’ marketing departments about their responsibilities when working with online influencers. Even where a brand may be unaware or have no direct input into or control over the ad, as a beneficiary of the marketing material, the company will be jointly responsible for adhering to CAP guidelines. Additionally, advertorials must be marked clearly as marketing communications from the outset. It will not be sufficient to hide clear signposts or use diluted labels.

Any practical tips?

The use of “affiliate” as a standalone term within marketing material is not a strong enough indicator of commercial intent. The ASA requires all parties to ensure that commercial content includes “*a clear and prominent identifier such as “#ad” at a minimum*”.

Summer 2020

ASA: Gender

ASA ruling on Missguided Ltd – the fine line between the mildly sexual and the objectification of women

The question

Were poster ads released by clothing company Missguided on public transport overly sexualised, inappropriate or likely to cause serious offence?

The key takeaway

The ASA is likely to order the removal of any ads which focus on explicit nudity, are overly sexualised or objectify women.

The ads

In November 2019, Missguided released two poster ads:

- Ad (a): the first (on the London underground) featured a model wearing a pink wrap mini-dress, showing the model's legs and cleavage
- Ad (b): the second (at a train station) featured the same model leaning against a side table wearing an unbuttoned jacket with nothing underneath, seer tights and high heels.

The complaint

The ads were challenged by complainants, who believed the images objectified women and were overly sexualised. It was argued that Ads (a) and (b) were offensive and that ad (a) was inappropriate for display where it could be seen by children.

The response

Missguided Ltd strongly contested that the posters did not overly sexualise and objectify women. It stated that the images were in keeping with industry practice and that similar ads were commonplace in the fast-fashion industry. It also said that it had not received any direct complaints and that it had followed a stringent approval process, which included approval from the CAP Copy Advice team and external media agencies.

Missguided also disputed whether the image in the first ad was inappropriate for display where it could be seen by children, because it was evident that the target audience was not children.

The decision

Ad (a)

The ASA considered the ads separately and ruled that, although some might find the ad distasteful, the imagery in ad (a) was no more than mildly sexual and featured no explicit nudity. In addition, the focus on the ad was on the model and the dress, as opposed to a specific part of her body. Accordingly, the ad was also not inappropriate for children and this particular ad did not breach the CAP Code.

Ad (b)

However, the ASA considered that the model in the second ad would be seen as "being in a state of undress" and that the focus was not on the clothing being advertised, but rather on her chest area and lower abdomen. They also considered that the image contained a sexually suggestive pose which objectified women. Consequently, the ASA concluded that the second ad was likely to cause serious offence and breached CAP Code Rule 4.1 (Harm and offence).

Why is this important?

The ruling is yet another example that the ASA will not tolerate the use of overly sexualised models in fashion ads. It is extremely important that retailers ensure that their ads are not considered overtly sexual. Great care should be taken to ensure that the tone of the ad, in terms of pose and nudity, is not inappropriate. It would also be sensible to ensure that the focus of the imagery is not on explicit nudity or on anything that would be seen to be objectifying women.

Practical tips

Getting advice on your ads in advance from the CAP Copy Advice Team doesn't get you off the hook!

You need to stand back and always think about the impact of your ad, in particular in light of the ASA's strong stance against objectifying women.

Summer 2020

ASA: Gaming

CAP warns against promotion of "bad betting behaviours"

The question

What has CAP identified as promoting "bad betting behaviours"?

The key takeaway

Any content promoting a gambling product or service which could lead to financial, social or emotional harm is likely to be considered a breach of the ASA rules.

The background

On 23 April 2020, the Committee of Advertising Practice (**CAP**) issued an advice note stating that gambling ads must be socially responsible and not portray, condone or encourage gambling behaviour which could lead to financial, social or emotional harm. The note also illustrates various examples of the type of betting behaviours which should not be promoted, as this would likely be a breach of advertising rules.

The development/guidance

- **Not an escape**: the guidance starts by stating that ads which suggest that gambling can provide a form of escape from personal and professional problems (such as loneliness or depression), are unlikely to be tolerated. An example was provided of a previous ruling, which suggested that online gambling can be used as a form of "rehab", which the ASA considered breached social responsibility advertising rules.
- **Never a solution**: the ASA continued by urging marketers not to state or imply that gambling can ease financial concerns. The ASA has previously upheld complaints against businesses that suggest that gambling can provide a sustainable income, an alternative to employment or a way to reduce personal debt.
- **Absolutely no pressure**: any ads which put pressure on people to gamble are likely to fall foul of advertising rules. Examples of ads which were deemed socially irresponsible by the ASA include those that have suggested that gambling could lead to personal success and an ad which asked viewers *"are you a spectator or are you a player?*".
- **Best of the rest**: ads should not:
  - suggest that gambling takes priority in life
  - link gambling to sexual success or attractiveness
  - link gambling to resilience
  - exploit susceptibilities or lack of knowledge of the young or vulnerable

- condone gambling in a working environment
- exploit cultural beliefs or traditions about luck.

Why is this important?

CAP's commitment to social responsibility has been affirmed in the CAP Code and in various rulings. However, there are particular concerns in relation to the COVID-19 crisis and the lockdown, as evidence suggests that mental health issues and anxiety are more prevalent during these challenging times.

Any practical tips?

The ASA has become particularly focused on the conduct of the online gambling industry. It is likely to crack down on those who produce content which promotes irresponsible gambling or targets those that are vulnerable, such as those who could use gambling as an escape from personal problems and the lockdown. The ASA is also encouraging people to report gambling ads which are seeking to exploit the Covid-19 crisis or the lockdown, for example those that attempt to propose gambling as a solution to the problems that are associated with the current climate, such as boredom.

Summer 2020

ASA: Gaming

CAP issues advice notice on the marketing of gambling on eSports on social media

The question

How do gambling operators stay on the right side of the advertising rules when creating marketing for gambling on eSports on social media?

The key takeaway

The CAP Code rules that apply to the traditional marketing of gambling also apply to eSports and cover social media in the same way as they do all other non-broadcast media.

The background

In July 2019, GambleAware published interim findings on its project to evaluate the impact of gambling advertising and marketing on children, young people and other vulnerable groups. Part of their work included a dedicated study looking at gambling marketing on social media.

A significant proportion of tweets highlighted within the report were eSports-related, with some of those tweets explaining how consumers can gamble on eSports. Having assessed the report and analysed a sample of the data, the Committee of Advertising Practices (**CAP**) created an advice notice on eSport-related gambling marketing on social media.

The advice notice applies to gambling marketing on all social media platforms, including, but not limited to, Facebook, Instagram, Twitter, Snapchat, Twitch and TikTok.

The guidance

Recognition of marketing

If a promotion is being advertised by a third-party social media account then it needs to be clear, this also includes affiliate marketing. CAP recommend using a clear identifier when the content is an ad, ie "#ad" at the beginning of the post.

Targeting

Marketers must target ads responsibly for gambling on eSports on social media. CAP Code Rule 16.1 states that "*marketing communications for gambling must be socially responsible, with particular regard to the need to protect children, young persons and other vulnerable persons from being harmed or exploited*".

The rules require that marketers take all reasonable steps to:

- ensure that advertising is not targeted at under-18s, either through the selection of media or the ad's content
- prevent advertising directed at adult audiences posing a risk to under-18s.

Marketers should take care to ensure they don't inadvertently target under-18s through the content of their ads.

Appeal to under-18s

If the ad holds particular appeal to under-18s due to its content or placement then the ad is likely to be of concern. CAP Code Rule 16.3.12 states that "*marketing communications must not be likely to be of particular appeal to children or young persons, especially by reflecting or being associated with youth culture*". Marketers should note that the ASA has previously ruled that cartoon-like imagery, characters that are recreated as toys and highly animated and stylised exaggerated features are all likely to hold particular appeal to children.

Terms and Conditions

Significant T&Cs which are likely to influence a consumer's understanding of an offer should be made sufficiently clear in gambling ads on social media (including offers of free bets and bonuses).

The CAP Code Rule 8.17 states that "*all marketing communications or other material referring to promotions must communicate all applicable significant conditions or information where the omission of such conditions or information is likely to mislead*". The terms and conditions in promotions must be made suitably clear and those that are significant T&Cs are very likely to be required in a post itself on social media.

Affiliates

Affiliates of gambling operators must also abide by the strict targeting and content rules. Beneficiaries of an affiliate's marketing material will be held equally responsible for the ad.

Influencers

Gambling operators are also held responsible for the content produced for them on social media by influencers. Remember - if an influencer has a strong youth appeal or a significant child audience, they may not be suitable for use in a gambling campaign.

Why is this important?

Given the global suspension of nearly all sporting events, eSports has gained a vast amount of popularity. Given that the demographic of players and fans of eSports are under 18, marketers should ensure they are well versed in the rules and ensure their campaigns adhere to the rules.

Any practical tips?

The ASA has made it clear that they are keeping a close eye on the marketing of gambling ads relating to eSports. Marketers should remember that they have responsibility for ensuring that the advertising of their content must be compliant, irrespective of the use of affiliates or social influencers.

Marketers should always step back and consider the risks and potential for harm of their ads whilst also taking into account the demographic of eSports fans and players.

Summer 2020

ASA: Gaming

ASA ruling against Coral – "Have another go" and socially irresponsible gambling

The question

How careful do you have to be when advertising repeat gambling?

Background

In March 2020, a Tweet on Coral's Twitter page featured the below ad:

- "*We're as passionate about the bet as you are. So, get your stake back as a free bet if your horse fails to finish. #CoralRacing 18+, T&C's Apply*". A link to a video ad was captioned "*Have another go*" and began with horses racing and superimposed text which stated "*STRONG, FAST, RELENTLESS, RIDERLESS*".
- The ad then showed a jockey about to fall off his horse with the text "*GET A FREE BET BACK WITH FAIL TO FINISH*", which was repeated by a voiceover.
- Finally, the ad showed a man looking disappointedly at his phone. However, his mood changed, and he began smiling when he discovered a free bet back. The voiceover then stated, "*For the passion of the bet: Coral Racing*".

The complaint

The complainant challenged whether the ad was irresponsible, on the basis that it encouraged repeated gambling.

The response

Broadly, Coral denied that the ad encouraged repeated or socially irresponsible gambling and stated that they believed the ad adhered to the ASA's Advertising Guidance. In particular, they argued that:

- the free bet promotion was a recognised industry campaign tool that did not encourage repetitive play. It simply provided a form of insurance in the event the horse failed to finish the race
- the promotion was not designed to cause financial or social harm as consumers were not required to use additional funds if they decided to exercise the free bet
- the ad did not encourage gambling beyond what a consumer would ordinarily gamble
- the video did not insinuate that the decision to gamble was taken lightly.

The decision

The starting point is that the CAP Code states that marketing communications for gambling must not "*portray, condone or encourage gambling behaviour that was socially irresponsible or could lead to financial, social or emotional harm*". In addition, marketing communications should not encourage repetitive participation, trivialise gambling or give the impression that the decision to gamble should be taken lightly.

Considering this, the ASA accepted that consumers did not have to use additional funds when taking up this optional offer. However, it considered that the statement "*Have another go*", alongside the video showing a man whose morale was boosted after receiving a free bet, suggested that the decision to gamble had been taken lightly. The ASA concluded that this was likely to encourage gambling behaviour that was potentially harmful as it would encourage some people to take up the offer repetitively.

The ASA held that the ad breached CAP code (Edition 12) rule16.3.1 on gambling.

Why is this important?

With online gambling trends set to continue to rise, gaming firms will increasingly be under the spotlight to ensure that their marketing communications are lawful and not socially irresponsible. It is extremely important that they ensure that their advertising to consumers do not directly or indirectly encourage gambling behaviour that may be interpreted as socially harmful by the ASA.

Practical takeaways

Gaming firms should ensure that any ads do not promote behaviour that could be socially damaging or harmful to the consumer. Advertisers should also ensure that communications do not give the impression that the decision to gamble should be taken lightly and do not trivialise gambling. The ASA specifically mentions "*encouraging repetitive participation*" as an example of harmful behaviour.

Summer 2020

ASA: Covid-19

Complying with ASA rules during a pandemic

The question

In light of the new UK's Advertising Standards Authority (**ASA**) and Competition and Markets Authority (**CMA**) Guidance, what do brands need to be aware of when marketing during the COVID-19 pandemic or similar "exceptional circumstances"?

The key takeaway

Whilst the rules on advertising have not changed as a result of COVID-19, the ASA has announced that there will be "*an uncompromising stance on companies or individuals seeking to use advertising to exploit the circumstances for their own gain*", including where adverts seek to exploit people's health-related anxieties or difficult financial or employment circumstances. The ASA will be looking to actively protect consumers from coronavirus scams and products and brands may need to take a more nuanced approach with marketing material.

The background

Since the start of lockdown, the ASA and the CMA have published a series of guidelines, blogs and rulings that will assist promoters, influencers, agencies and brands as they continue to navigate the various ASA rules during the COVID-19 crisis. The Guidance also highlights the reporting tools that will help consumers make complaints about coronavirus-related ads and unfair commercial practices.

The guidance and advice notes

A. Promotions

The ASA published Guidance on "Dealing with unexpected events when running promotions"on 7 May 2020.Within the Guidance, the ASA draws attention to section 8 of the CAP Code which governs promotions and covers the possibility of events which are unexpected and beyond the promoter's control. In relation to existing promotions, a business can only make changes to the terms and conditions in exceptional circumstances under consumer law and the ASA rules. The COVID-19 outbreak is recognised by the ASA as an "exceptional circumstance" and may require promoters to rethink aspects of a current promotion. However, promoters must be able to show that:

- the changes are necessary because of the crisis
- they have kept participants updated on any amended rules
- consumers would have entered the promotion even if the new rules had originally been in place.

If the COVID-19 outbreak has impacted a closing date of a competition, the promotor must be able to demonstrate:

- why it is necessary to change the date
- that changing date the date would not be unfair/disadvantage those who participated under the original terms.

Additionally, if the current situation has also impacted the ability to award prizes within the usually mandated 30 days, a promotor is not permitted to cancel a promotion without awarding any prize at all. Promotors must actively communicate with consumers that a prize or a suitable equivalent will be awarded as soon as possible.

Where the availability of promotional items has been affected, promoters must be able to show they had made a reasonable estimate of demand. Simply using the disclaimer “subject to availability” will not relieve promoters of their obligation to do everything reasonably possible. If promoters are no longer able to supply and fulfil demand for a promotional offer due to COVID-19, Rule 8.11 requires promoters to ensure timely communication and offer refunds or substitute products, where there is a detriment to applicants and consumers.

B. Free trials and subscriptions

During lockdown, subscription platforms like Netflix have significantly increased. To incentivise consumers, brands will typically offer free trials. In response to this uptake, the ASA has published top tips on advertising free trials responsibly. The Guidance does not include new information but reminds businesses of the information which needs to be clearly provided to consumers, including:

- what a consumer needs to do to trigger the free trial
- whether a subscription payment automatically applies to the consumer unless the trial is manually cancelled
- details as to how the consumer can cancel
- the extent of the financial commitment if the consumer does not cancel
- any other significant conditions, such as the end date for commencing the free trial or whether limitations apply, such as the trial being made available to new customers only.

In addition, the Guidance reminds brands that, in order to use the term “free trial”, the offer must be genuinely free to the consumer. Businesses can charge for delivery provided that it is the genuine, uninflated cost of postage, but cannot charge the consumer for packing, packaging, handling or admin fees.

C. Promoting alcohol

The ASA has also published advice specifically for alcohol marketers to ensure that alcohol-related promotions do not encourage excessive drinking. This is especially relevant during lockdown, as Alcohol Change UK reports that one in five people are drinking more than usual during lockdown. Brands should be mindful that they are prohibited from claiming that alcohol can cure boredom, provide escapism or a solution to other problems.

Why is this important?

The ASA has been very clear that it will take an extremely dim view of anyone seeking to capitalise on the pandemic to sell products or services. The CMA have also launched a taskforce to tackle negative impacts within its remit of the COVID-19 outbreak as well as an online service through which businesses and consumers can report COVID-19 related unfair practices.

Any practical tips?

Be sensitive to the unintended impact marketing material may produce as well as to the key message your brand is trying to convey. Mentioning the pandemic in adverts is allowed provided it is not done in an exploitative or inaccurate way.

However, brands must be mindful of the ASA's tough stance as well as the recent media criticism that some businesses are inappropriately "corona washing" (brands seeking to ally themselves with the national effort or frontline workers without an obvious connection).

Additionally, any businesses advertising their charitable efforts related to COVID-19 should be mindful that they will need to comply with rules on charitable marketing and specific charity law requirements.

Summer 2020

ASA: Covid-19

ASA ruling against Revival Shots

The question

Can companies make health claims in ads for their food products?

The key takeaway

Ads must ensure that they do not state or imply that their food product could prevent, treat or cure human disease, including COVID-19. Any health claims made in advertising must be authorised on the EU Register of nutrition and health claims, they must have met the conditions of use for the authorised claims, and properly communicated the meaning of the authorised claim.

The ad

One Facebook ad and two Instagram ads were posted by Revival Drinks Ltd t/a Revival Shots:

- Ad (a): The Facebook ad, posted on 12 April 2020, stated "*Each stick of Revival contains … 500mg of vitamin C* …" and featured an image with text that stated "*VITAMIN-C HAS BEEN PROVEN TO BOOST IMMUNITY BY MANY GLOBAL STUDIES … IT IS NOW BEING TESTED IN THE USA & CHINA AS A POSSIBLE CURE FOR COVID-19*".
- Ad (b): The first Instagram ad, posted on 12 April 2020, was the same as ad (a).
- Ad (c): The second Instagram ad, posted in April 2020, stated "*Today we have officially past 500 independent verified reviews on Amazon … Here is one of the latest reviews from a customer in UK … #immunity #immunityboost #vitaminc … #staysafe". The image featured a five-star review which stated "Great ! After developing symptoms of a sore throat & headache I got paranoid. I ordered this concentration of Vit C and took one stick. In about half an hour I felt instantly revived and my headache disappeared and sore throat was greatly reduced. Since taking I have had no symptoms. I highly recommend … 30 March 2020*".

The complaint

The complainant challenged whether the ads implied that the product, or the vitamin C the product contained could cure COVID-19, could prevent or cure disease, and could boost immunity. The complainant challenged whether these ads complied with the Code.

The decision

The CAP Code stated that claims which stated or implied a food could prevent, treat or cure human disease were prohibited for foods; this included food supplements and drinks. The ASA

considered the ads therefore implied that consuming Revival Shots could, through their vitamin C content, help to cure COVID-19. Furthermore, given that Ad(c) was posted in mid-April 2020 during the COVID-19 pandemic, referred to symptoms sometimes associated with COVID-19 and the reviewer's "paranoia" about those symptoms, and included the hashtag "#staysafe" which was commonly associated with the pandemic, the ASA considered consumers would understand that the claims in the review were intended to be understood to relate to COVID-19. The ASA considered the ad therefore implied that Revival Shots could help to cure COVID-19. The ASA held that the ads breached CAP Code (Edition 12) rules 15.6 and 15.6.2.

According to Regulation (EC) No. 1924/2006 on nutrition and health claims made on foods (the Regulation), which was reflected in the CAP Code, only health claims listed as authorised on the EU Register of nutrition and health claims (the Register) were permitted in marketing communications. The CAP Code defined health claims as those that stated, suggested or implied a relationship between a food, drink or ingredient and health. Ads (a) and (b) stated that Revival Shots contained vitamin C and that "*VITAMIN-C HAS BEEN PROVEN TO BOOST IMMUNITY*…". Ad (c) included the hashtags "*#immunity #immunityboost #vitaminc #vitamins #vitamind*". Claims that a food or nutrient was relevant to immunity or could "boost" immunity are health claims for the purposes of the Regulation.

The Register included the authorised health claims that vitamins C and D (and other vitamins) "*contribute to the normal function of the immune system*". However, Revival Shots had not provided any evidence to demonstrate that their products contained any vitamin in amounts sufficient that they could use any of those authorised health claims in advertising for their products. Furthermore, the ASA considered that the claim "#immunity" did not properly communicate the meaning of those authorised health claims to consumers, and the claims "BOOST IMMUNITY" and "#immunityboost" exaggerated the meaning of those authorised claims' wording. Because the ads made specific health claims but the ASA had not seen evidence that any of Revival Shots' products met the conditions of use associated with a relevant authorised claim on the Register, and the advertising claims in any case did not properly communicate the meaning of relevant claims authorised on the Register, the ASA concluded the ads breached the Code. The ASA held that the ads breached CAP Code (Edition 12) rules 15.1 and 15.1.1.

Why is this important?

Ads must ensure that they comply with the CAP Codes and do not state or imply that their food product could prevent, treat or cure human disease, including COVID-19. Health claims made in advertising must be authorised on the Register, they must have met the conditions of use for the authorised claims, and properly communicated the meaning of the authorised claim.

Any practical tips?

Advertisers should take extreme care with any claims associated with preventing or treating illnesses. Any indication that an advertiser is taking an opportunistic approach to a health scare is never going to sit well with the ASA.

Summer 2020

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

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

38/F One Taikoo Place
979 King's Road
Quarry Bay, Hong Kong
T +852 2216 7000

12 Marina Boulevard
38/F MBFC Tower 3
Singapore 018982
T +65 6422 3000

RPC