RPC

Commercial law snapshots

Winter 2018

ADVISORY | DISPUTES | TRANSACTIONS

Contents

Page

1. Commercial
Fawaz Al-Hasawi v Nottingham Forest Football Club Ltd [2018] EWHC 2884 4

2. Commercial – liquidated damages/ indemnities
GPP Big Field LLP v Solar EPC Solutions SL (Formerly Prosolia Siglio XXI) [2018] EWHC 2866 (Comm) 6

3. Commercial – contractual discretion
UBS v Rose Capital Ventures Limited and others 9

4. Commercial – letters of intent
Arcadis Consulting (UK) Limited v AMEC (BCS) Limited [2018] EWCA Civ 2222 11

5. Contract
Government announces plans to prohibit certain contractual termination clauses 14

6. Copyright
Reformation Publishing Co Ltd v Cruiseco Ltd (Spandau Ballet) 16

7. Trade marks
Argos Limited v Argos Systems Inc [2018] EWCA Civ 2211 19

8. Data protection
Facebook ordered to reveal who requested deletion of deceased's profile – Sabados v Facebook Ireland 21

ICO Calls for views on GDPR update to Direct Marketing Guide 23

"Google You Owe Us" class action blocked – Richard Lloyd v Google LLC 25

Various Claimants v WM Morrisons Supermarket PLC [2018] EWCA Civ 2339 27

Six month imprisonment in first ICO computer misuse act prosecution 29

Bupa fined for systemic data protection failures 31

Ireland's Data Protection Commission launches investigation into Facebook's data breach 33

Equifax fined £500,000 for data breach of 15m UK customers 35

What if there's no Brexit deal? 37

9. Consumer

Amended UK consumer regulations in advance of Brexit 39

Viagogo ordered to provide better information on ticket purchasing 42

Misrepresentations during the selling process - Burki v Seventy Thirty Ltd [2018] EWHC 2151 (QB) 44

10. Online platforms

Unjustified Geo-blocking Regulation 2018/302(EC) 46

The EU fights "fake news" 48

11. Influencer marketing

#Ad-vice for influencers and brands: how to comply with CAP's new Influencer's Guide 50

Under an obligation to repost an article you've written? You may need #ad – ASA rules against Platinum Gaming Ltd t/a Unibet 55

12. ASA – Data

New CAP Code rules on the use of data for marketing 57

13. ASA – Puffery

"By your side" claim not misleading – Lloyds Bank 60

14. ASA – Pricing

CAP issues new guidance on RRP comparisons 62

Savings claims not substantiated and significant limitations omitted – Laura Ashley Ltd 64

15. ASA – HFSS

Coco's revenge – ASA reverses Kellogg's HFSS decision 67

Placing HFSS ads too close to schools 70

ASA issues guidance on HFSS media placement 72

16. ASA – Prize draws

CAP tips on social media prize promotions 75

ASA announcement on prize winners rule under the GDPR 77

17. ASA – Promotions

Failing to honour a gift promotion – ASA ruling against Superdrug 79

18. Gambling

Gambling ads of "particular appeal" to children: 32Red 82

Consultation on age and identity verification 85

Commercial

Fawaz Al-Hasawi v Nottingham Forest Football Club Ltd [2018] EWHC 2884

The question

Will an entire agreement clause exclude claims for misrepresentation?

The background

In April 2017 Mr Fawaz Al-Hasawi sold the heavily indebted Nottingham Forest FC via a share purchase agreement. The shares in the business were sold for nominal consideration and Mr Al-Hasawi agreed to indemnify the buyer to the extent that the existing liabilities exceeded £6.6m.

During pre-contractual negotiations, Mr Al-Hasawi sent the buyer a spreadsheet showing that the liabilities of the Club totalled £6.56m. The buyer alleged that the Club owed in excess of £10m. The buyer sought to claim for the debts in excess of £6.6m under the contractual indemnity, or alternatively, to claim under Section 2 of the Misrepresentation Act 1967.

The entire agreement clause provided: "*This agreement (together with the documents referred to in it) constitutes the entire agreement between the parties and supersedes and extinguishes all previous discussions, correspondence, negotiations, drafts, agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter*".

At first instance, the Master struck out the misrepresentation element of the claim. He found that the various contractual indemnities showed that the parties intended liability to be dealt with under the contract. He also found that use of the word "*representations*" in the entire agreement clause was effective (distinguishing it from the clause in *AXA Sun Life v. Campbell Martin* [2011] EWCA 133). The buyer appealed the decision to the High Court.

The decision

The High Court reversed the decision of the Master. The judge ruled that:

- the inclusion of contractual remedies did **not** imply that all other types of claim should be excluded
- the entire agreement clause did not say anything about excluding claims (except for collateral warranties). It could therefore not be inferred that claims for misrepresentation were excluded, and

- it was not correct to distinguish the use of the word "*representations*" from its use in the *AXA* case.

Why is this important?

The "entire agreement" clause is one of the most common boilerplate clauses. The court's decision essentially affirms the current position under existing case law – contracting parties need to be explicit if they want an entire agreement clause to exclude misrepresentation.

Any practical tips?

Ensure that your boilerplate contains not only an entire agreement provisions, but also an exclusion of/non-reliance on pre-contractual representations, etc. Parties should also be careful as to what information is being provided pre-contract and is being relied upon – exclusions/limitations do not provide a complete answer!

Winter 2018

Commercial – liquidated damages/ indemnities

GPP Big Field LLP v Solar EPC Solutions SL (Formerly Prosolia Siglio XXI) [2018] EWHC 2866 (Comm)

The questions

Do liquidated damages clauses amount to unenforceable penalties? What is the difference between a guarantee and indemnity?

The background

GPP entered into five substantially similar contracts with Prosolia for the construction of solar power generation plants across the UK. Solar is Prosolia's parent company, who had guaranteed Prosolia's obligations in four of the five contracts (the **Contracts**).

Prosolia became insolvent. The Contracts contained liquidated damages clauses (the **LD Clauses**) covering delays in commissioning. GPP claimed liquidated damages for Prosolia's failure to commission each plant by the date specified in the relevant contract, against Solar as Prosolia's guarantor.

The main issues for the Court to decide were: (i) did the LD Clauses in the Contracts amount to unenforceable penalties; and (ii) was Solar liable for GPP's losses under the Contracts pursuant to a guarantee or an indemnity?

The decision

Liquidated damages or penalties?

Solar argued the LD Clauses should be construed as unenforceable penalties, because the daily rate of liquidated damages accruing under each of the Contracts was the same, despite applying to different plants with differing energy outputs. Further, the LD Clauses had not been subject to detailed negotiation between the parties, and were each referred to as a "*penalty*".

The Court rejected Solar's arguments, and found the LD Clauses to be neither penalties, nor unenforceable. The Court applied the Supreme Court decision in *Cavendish Square Holdings BV v Makdessi and ParkingEye Ltd v Beavis* [2015] (**Makdessi**). Under *Makdessi*, the Court needed to decide if the LD Clauses were "*out of all proportion to any legitimate interest of*

innocent party in the enforcement of the primary obligations" and/or whether the sums stated were "*extravagant, exorbitant or unconscionable*".

The Court decided that, while the sums agreed under the LD Clauses were not a precise calculation of the financial losses conceivable, they did not exceed a genuine attempt to estimate in advance the loss GPP might suffer.

The Court also dismissed the argument that the LD Clauses had not been the subject of detailed negotiation; the parties were sophisticated and experienced commercial entities, with equal bargaining power. Further, use of the word 'penalty' in the wording of the LD Clauses was immaterial; the substance of the LD Clauses was clear.

Indemnity or guarantee

Solar also argued that its obligations under the Contracts applied to it as a guarantor, not as an indemnifier. Solar argued that Prosolia had: (i) failed to disclose "*unusual features*" regarding the project before Solar had entered into the guarantee; and (ii) failed to consult Solar on a significant change to the logistics of the project, which varied Solar's contractual obligations under the Contracts. Accordingly, Solar, as guarantor, could be discharged from any liability under the doctrine of guarantee law.

The Court dismissed this argument, concluding that the guarantee clause included a 'separate and independent obligation and liability' as an indemnity. This guarantee was expressed as a promise to indemnify, and was 'written in language characteristic of indemnities'. Solar was therefore liable for GPP's losses pursuant to an indemnity.

Why is this important?

This case is a good example of the modern approach to liquidated damages/penalties – it is no longer merely a question of whether it is a genuine pre-estimate of losses.

This case also confirms that, in the case of a negotiated contract between equal and sophisticated commercial parties, the Court will consider the parties themselves to be the best judges as to appropriate level of liquidated damages.

The decision is also a useful reminder of the advantages of an indemnity (a primary obligation) over a guarantee (a secondary obligation).

Any practical tips?

Parties should be careful to ensure liquidated damages clauses are proportionate to the likely losses, and not extravagant or unconceivable. Expressing payments as primary obligations as opposed to damages can also assist recovery.

Parties seeking to have the benefit of a third party guarantee should ensure all of the usual guarantee protections are in place (eg no release by reason of variation, delay, forbearance, etc) and ideally have a supporting indemnity (as a primary rather than a secondary, obligation).

Winter 2018

Commercial – contractual discretion

UBS v Rose Capital Ventures Limited and others

The question

Is there a duty to act rationally and in good faith when exercising a contractual right without cause (the *Braganza* duty)?

The facts

UBS granted a mortgage for £20.4m to Rose Capital on a term of five years. The mortgage contained a number of special conditions which included that UBS could demand early repayment of the loan with three months' notice. This demand could be effected without the need for a triggering event (the **Special Condition**).

Four years after the drawdown of the loan, UBS requested early termination and served a notice demanding repayment.

Rose Capital contended that the Special Condition was ineffective because it gave UBS a discretion to call the loan in early and that discretion was subject to a duty of good faith, following *Braganza v BP Shipping Ltd & Anr* [2015] UKSC 17.

UBS argued that the duty of good faith as between a mortgagor and a mortgagee does not arise by contractual implication but by virtue of the creation of a mortgage. Since the ability to enforce the Special Condition was one of absolute discretion, there could be no allegation of bad faith in UBS's decision to do so.

The decision

Chief Master Marsh held that the circumstances in Braganza did not apply. If one party is charged with making decisions which affect the rights of both parties to the contract, then there is a clear conflict of interest and the duty to act rationally would apply. Since UBS' right to terminate the contract without cause was unilateral, there was no conflict of interest.

The Chief Master noted that the contract in Braganza was an employment contract, which by its nature, was created by an inequality of bargaining power. Baroness Hale held that alongside the nature of the contractual relationship, this was an important factor to be taken into account. Such inequality did not exist in the relationship between UBS and Rose Capital.

The Chief Master concluded that as long as the mortgagee exercises the power for proper purposes and not for the sole purpose of vexing the mortgagor, it will neither be in breach of

its duty of good faith nor a Braganza term, if one is capable of being implied on the basis of business necessity.

Why is this important?

This case confirms its limits of the *Braganza* duty, and highlights the importance of not only considering the contractual rights of each party within an agreement, but also the duties the parties may have to each other when exercising those rights.

For example, in contracts where the parties are on unequal footing, the dominant party may have to use its discretion as to whether a contractual right may trigger a Braganza situation where the party cannot make decisions based on the substance of the contract alone.

Practical tips

Parties should be mindful that a stronger duty of good faith may apply where the contracting parties are subject to an inequality of bargaining power. This duty could prevent a party from exercising rights which they would otherwise be entitled to enforce without consideration for the affected party.

Where the implied duties on contractual discretion (a *Braganza* duty) do apply, decisions must be made in good faith and not irrationally, perversely or capriciously, and the decision maker must take the relevant factors (and not take irrelevant matters) into account.

Winter 2018

Commercial – letters of intent

Arcadis Consulting (UK) Limited v AMEC (BCS) Limited [2018] EWCA Civ 2222

The question

What approach does the Court take in relation to the "letters of intent" pending final agreements being concluded?

The facts

AMEC acted as a specialist concrete sub-contractor on two large projects (i) the Wellcome Building (**Wellcome**), and (ii) Castlepoint Car Park (**Castlepoint**). AMEC engaged with Arcadis Consulting (**Arcadis**), to carry structural design works for the projects.

The parties planned on entering into a Protocol Agreement which would govern Arcadis' work on both Wellcome and Castlepoint; whilst negotiations were occurring Arcadis started work on Castlepoint through a letter of instruction from AMEC. The Protocol Agreement was never concluded.

AMEC alleged that the construction of Castlepoint was defective and sought damages of £40,000,000 from Arcadis. Arcadis denied liability and submitted that in the alternative, its liability would be capped to the amount of £610,515 on the basis of a contract.

Arcadis relied on a letter of intent (the **LOI**) sent from AMEC to Arcadis which contained the Protocol Agreement, together with its Schedules and Terms and Conditions. The Terms and Conditions contained a limitation of liability clause (Clause 2A) which stated:

"*The Consultant's liability for defective work shall be limited to whichever is the lesser of:*

(a) The reasonable direct costs of repair, renewal or reinstatement of any part or parts of the sub-contract works to the extent that the Client incurs such costs and/or is or becomes liable either directly or by indirect way of financial contribution to such costs

(b) The sum stated in Schedule 1".

Schedule 1 had been left blank at the time, but a separate letter contained a complete version of Schedule 1, which specified the limit of the consultant's liability was 10% of sub-contract package for insured losses or £610,515.

The decision

The High Court

Coulson J held that a contract existed as evidenced by the LOI, the acceptance of instructions, the commencement of works pursuant to those instructions and the payment for those works.

The Court disagreed that a liability cap had been incorporated into the contract. The Terms and Conditions sent had been superseded by further negotiations and these were never accepted; there was therefore no liability cap as Schedule 1 was ancillary to the Terms and Conditions.

Arcadis appealed the decision to the Court of Appeal with the core question being whether the Terms and Conditions sent were incorporated by reference into the contract.

Court of Appeal

The Court of Appeal allowed the Arcadis appeal and reversed the decision of the High Court; holding that a liability cap had been incorporated into the contract.

The Court distinguished the LOI, or interim contract, under which the parties were working and the final contract, the terms of which would supersede the interim contract once agreed in its completed form. The relevant contract for the purposes of this dispute was the interim contract.

In a letter from AMEC to Arcadis, it stressed that "*work done under this instruction is to be on the basis of … the conditions and terms detailed in the Protocol Agreement, Design Consultancy Terms and Conditions in your possession at present*".

Arcadis accepted the LOI by carrying out the works it had been instructed to do and for which it was paid. In doing so, it accepted the Terms and Conditions and therefore incorporated the liability cap into the interim contract. The fact that the Terms and Conditions did not make it into the final contract did not preclude their use under the interim contract.

Why is this important?

This decision acknowledges that commercial parties do not always have the time to wait for their lawyers to negotiate clear signed-off terms and conditions prior to works commencing; the reality is that sometimes interim agreements will have to be interpreted from a series of communications and the conduct of the parties.

Any practical tips?

Parties should be particularly careful when drafting, responding to or operating under letters of intent. Uncertainty as to whether the terms are legally binding, the nature and extent of the terms and the impact of the parties' dealings and other agreements can lead to disputes.

Even if parties in negotiations expect a detailed agreement to be reached in the near future, they should be careful to ensure that the terms of any letter of intent reflect the agreed commercial terms and provide sufficient protection, particularly in terms of payment and liability.

Winter 2018

Contract

Government announces plans to prohibit certain contractual termination clauses

The questions

Which termination clauses will likely be prohibited by any new legislation? Should termination clauses which do not adhere to the new regime be included in contracts? What will be the legal status of termination clauses which are non-compliant with any new legal regime? Will they be void or unenforceable?

The background

In August the Government's response to the insolvency and corporate governance consultation (the **response**) was published. In addition to other suggested reforms, the Government proposed a prohibition on suppliers enforcing termination clauses on the grounds that a party has entered into a formal insolvency procedure, or one of the two proposed restructuring arrangements: the new moratorium or the new restructuring plan. The prohibition may also apply to 'ipso facto' termination clauses, which relate to the debtor company's financial position.

Currently, the provision of 'essential supplies' to companies which are in administration, or have entered into CVAs, is regulated. Rather than adapting the existing regime and amending the definition or designation of what an 'essential supply' is, the Government has opted for a new blanket regime, whereby certain termination clauses are banned. Such a move encroaches upon the freedom of contract but is more in-line with other jurisdictions, such as the USA.

The guidance

The aim of the reforms is to increase protections for creditors and to provide a fair balance between the rights of the company seeking to be rescued and the rights of the creditors seeking payment of the company's debts.

There are exemptions to the proposed blanket regime. For example, some financial services are not covered by the prohibition, which reduces the risk that providers may remove debt facilities in order to avoid the effects of the new regime.

Suppliers will still be able to terminate on other grounds, including for non-payment of debt. The efficacy of the ground of non-payment depends upon how long the supplier's payment term is and how much was left unpaid. If a supplier invoices a company infrequently for large

amounts of money, it will be less happy to wait to invoke the non-payment ground for termination in light of the large amount of money which will likely be unpaid.

Why is this important?

If the proposals are enacted into law, contracts for the supply of goods and services will be subject to prohibitions which restrict the abilities of suppliers to terminate contracts. However, the remit of such restrictions is yet to be determined. For example, it is unclear whether ipso facto clauses which are within the scope of the legislation will be void or unenforceable.

Other uncertainties arise in relation to the question of whether ipso facto termination clauses should continue to be included in contracts. It may be desirable to include ipso facto clauses for the following reasons:

- ipso facto clauses might permissibly be invoked before a trigger event such as insolvency. Although, it waits to be seen whether this will be the case
- a supplier which is significantly adversely affected by not being able to invoke a termination clause may apply to the court for permission to rely on the clause if it were more likely than not that the supplier would enter into an insolvency procedure if it continued to supply
- prohibited grounds for termination may need to be included in the contract for liabilities accruing to the supplier to be given priority as expenses of a moratorium, liquidation or administration. Again, this depends on the shape of any future regime.

Any practical tips?

Keep watching! Future announcements and publications issued by the Government on this topic which outline the scope of any prohibition should clarify the uncertainties mentioned above.

Winter 2018

Copyright

Reformation Publishing Co Ltd v Cruiseco Ltd (Spandau Ballet)

The question

How does the court calculate a reasonable licence fee, and what conduct is sufficient for the court to award additional damages under Section 97(2) of the Copyright, Designs and Patents Act 1998?

The background

Reformation owns the copyright in two well-known Spandau Ballet songs, "Gold" and "True" (the **Songs**). Cruiseco Discovery Travel, are part of the same group of companies and operate cruise holidays.

In June 2017, Cruiseco posted on their websites and a file sharing platform (a link to which was shared with 257 travel agents) a short publicity clip to promote their "Back to the 80's" themed cruise which featured extracts of the Songs without a licence from Reformation (the **Publicity Clip**).

Cruiseco accepted that their Publicity Clip infringed Reformation's copyright in the Songs and, as such, they promptly removed it from their websites and told the travel agents not to use it. However, they failed to remove the Publicity Clip from the file sharing platform.

The question was what damages should be paid for Cruiseco's infringement, to be assessed on the basis of a "reasonable licence fee". Reformation also sought additional damages under Section 97(2) of the Copyright, Designs and Patents Act 1998 owing to the "flagrancy" of Cruiseco's infringement.

The decision

Duration of copyright infringement

Cruiseco's infringement was assumed to be over a period of five days in June 2017, ie from when the Publicity Clip was posted on Cruiseco's websites and the file sharing platform link sent to the travel agents, to when instructions were given by Cruiseco to take it down once they were aware of their infringement. However, Reformation discovered that the Publicity Clip was still available via the file sharing platform, which remained live until two days before trial.

The court found that (i) the travel agents were not an indeterminate number of potential recipients and this was not sufficient enough to constitute the public, and (ii) it was only speculative that the Publicity Clip would be send on to members of the public by the travel agents and this was not strong enough evidence.

The court therefore held that Cruiseco had not continued to make the Publicity Clip available to the public and, as such, the infringement lasted for five days only.

Damages for copyright infringement on the basis of a "reasonable licence fee"
The court took the view that a reasonable licence fee should be calculated by reference to the period of copyright infringement rather than the duration of a licence that would have been negotiated should Cruiseco have sought a licence from Reformation for the Songs.

As for the terms of a hypothetical licence under which a reasonable fee would be charged, it was decided that it would have been for both Songs, it would have covered internet usage, it would have covered point of use sale, and it would not have extended to television usage.

The court lacked comparator licences as evidence, but established that there was substantial value in the Songs even for a short five day period owing to their iconic status. It therefore awarded Reformation £38,750 in ordinary damages.

Additional damages under Section 97(2) of the Copyright, Designs and Patents Act 1998
By Section 97(2) of the Copyright, Designs and Patents Act 1998, the court had the ability to award Reformation additional damages owing to the apparent "flagrancy" of Cruiseco's conduct, being its careless, recklessness and/or deliberate actions leading to infringement.

The Publicity Clip was produced for Cruiseco by Artists Network Australia (**ANA**). Given ANA's experience in the music industry the court found that it should likely have known of the consequences of using the Songs without licence and had "decided to chance it", amounting to (at the least) a reckless attitude. This reckless attitude was assigned to Cruiseco as principal and therefore an award of £25,000 in additional damages was given to Reformation.

Why is this important?
This decision is a useful guide of how copyright damages will be assessed and of the principles that will be applied to a reasonable licence fee and the hypothetical licence. It also provides guidance on the "flagrant" behaviors, and the identities and relative characteristics of the parties, which the court will consider when looking to award additional damages.

Practical tips

Always go through paper clearance procedures (copyright, trade marks, etc) before releasing content or advertising/marketing campaigns. If using third party agencies, ensure they have proper procedures in place and that you have proper recourse against them under your agreement. Act quickly and look to resolve issues (including withdrawing content) if third party rights have been used without permission.

Winter 2018

Trade marks

Argos Limited v Argos Systems Inc [2018] EWCA Civ 2211

The question

How will the Court interpret the three limb test of Article 9(1)(c) of the EU Trade Mark Regulation?

The facts

Argos UK (**Argos**), the well-known UK based retailer, owns two EU trade marks for "ARGOS" which is registered under, among others, for advertising and retailed related services. Argos UK has a large number of brick and mortar stores as well as an online website: www.argos.co.uk. Argos is a member of AdSense and AdWords programmes, not as a partner but as an advertiser.

Argos Systems Inc (**ASI**), a US based company, trades in computer aided design (**CAD**) software which was used to design and construct commercial and residential buildings in America. In 1992, ASI registered the domain www.argos.com. ASI is a partner in Google's AdSense programme and so allowed third party adverts to appear on its website.

Due to a high number of internet users clicking on ASI's website, often erroneously mistaking it for Argos' website, ASI began to earn money as a result of the interplay between AdSense and AdWords. In January 2012, it reconfigured its website using geo-targeting, thereby presenting two versions of the website – one for US visitors and one for UK visitors. The US visitors did not see Google AdSense ads, but they were still visible to visitors including those from the UK and Ireland.

Argos brought a claim under Article 9(1)(c) of the Trade Mark Regulation on the basis that this took unfair advantage of, and thereby infringed, its EU trade mark.

The decision

The High Court

Deputy Judge Spearman held that:

- ASI did not target UK customers and its use of the sign was not in the UK
- the average consumer did not make the link between the sign and Argos' mark, and
- ASI did not take unfair advantage of Argos' mark.

The Court of Appeal
The appeal was not upheld but differed from the High Court judgment.

The key points from the judgment are as follows:

- ASI was targeting UK consumers and found that ASI was effectively providing a billboard service plainly aimed or directed at UK visitors
- the Court of Appeal disagreed that no link existed between the use of the word "Argos" and the British retailer
- UK visitors would immediately realise they were in the wrong place and then either leave the site altogether or click on an advertisement to do so; ASI still obtained an impression fee for doing so. Advantage was therefore taken by this opportunity and the strength of Argos' reputation
- however, despite the tests for "targeting" and the "link" being met, the Court of Appeal concluded that no unfair advantage had been taken of the distinctive character of the ARGOS trade mark
- the Court of Appeal concluded that ASI's use of ARGOS did not cause any customers to click on advertisements for competitors or divert business away.

Why is this important?
This decision provides a useful and noteworthy display of how the Court of Appeal interprets the first and second limb of Article 9(1)(c) of the EU Trade Mark Regulation. Additionally, it demonstrates the bar needed to surpass the third limb of the test.

For Google, it helps clarify and legitimise the Google AdSense programme.

It also confirms how use of a trade mark on a website which hosts ads of appeal to UK consumers may constitute use of that mark in the UK (even though the website does not offer goods or services to those UK consumers).

Any practical tips?
Remember the importance of getting in first with a domain name registration. All Argos' troubles in this case stemmed from ASI getting to the argos.com domain first.

For businesses who are members of the AdSense programme, they should make good use of the "blocking feature" which enables members to exclude or block domains that they do not wish to appear on their website.

Winter 2018

Data protection

Facebook ordered to reveal who requested deletion of deceased's profile – Sabados v Facebook Ireland

The question

Where a social media company has completed a request from an unknown person to delete a deceased's profile and refused to tell the deceased's partner, can a Norwich Pharmacal order be used to disclose the identity?

The facts

In *Sabados v Facebook Ireland* [2018] EWHC 2369 the claimant was a British citizen originally from Bosnia. The claimant had had a serious relationship with a childhood friend for six years before his sudden death. The relationship had been predominantly long distance as the deceased lived in Sarajevo. They communicated every day, often using Facebook Messenger.

Six months after his death, Facebook received an unknown request to delete his profile. The material was irreversibly erased. Facebook refused to reveal who had made the request, but did confirm their process had been followed. Facebook responded to a Section 7 Data Protection Act 1998 (**DPA**) request, by stating that the data from the profile was no longer available. In response the claimant served a claim on Facebook at their Republic of Ireland address. A law firm responded informing the claimant that they acted for Facebook, but that it was not authorised to accept service or enter into correspondence. No acknowledgement of service was filed.

The claimant submitted the following points:

- there was clear evidence that a person unknown posed as a family member in order to get Facebook to delete the profile;
- this act resulted in the permanent deletion of posts and messages stored on it;
- some of this data was the claimant's own personal data under the meaning of the DPA, giving rise to a breach;
- the deletion of the claimant's partner's Facebook profile interfered with her mourning process, which was an intrusion into her private life and a misuse of her private information;
- the course of conduct completed by the person unknown amounted to harassment;
- if the person unknown had gained access to the messages between her and her partner, then this would amount to a breach of confidence;

- without the court making the Norwich Pharmacal order the claimant would not have sufficient information to be able to identify the defendant; and
- the English court had jurisdiction under the Brussels Recast Regulation to make the order.

The decision

The application was granted on the basis that there was a good arguable case a person unknown posed as a family member to get the Facebook account deleted. These actions could have given rise to misuse of private information and breach of confidence. Without the Norwich Pharmacal order the claimant would have had insufficient information to identify the person unknown in order to bring a claim. Facebook had both hosted and deleted the information at the request of the person unknown. The court decided that Facebook was more than a mere witness, as it was mixed up in the alleged wrongdoing.

The court agreed it did have jurisdiction under the Brussels Recast Regulation. The alleged torts were committed or the damage incurred in England. The court cited *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 in support of this conclusion.

Why is this important?

Although the case was heard under the DPA, it serves as an important reminder that extreme care must be taken when handling requests for deletion of personal data to ensure the requestor has appropriate authority. In the era of GDPR when fines are greatly increased, corporations must be even more alert to the consequences of unauthorised erasure of data.

Any practical tips?

It is important to ensure that rigorous processes are in place for deletion requests of a deceased's data, and that they meet GDPR requirements.

Winter 2018

Data protection

ICO Calls for views on GDPR update to Direct Marketing Guide

The question

What should we expect from the ICO's updated Direct Marketing Guide?

The background

According to Section 122(1) of the Data Protection Act 2018 (DPA), the Information Commissioner's Office (**ICO**) must prepare a direct marketing code of practice, taking recent data protection legislation into account.

The data protection changes that are particularly relevant to direct marketing, and are therefore likely to be covered by the guidance, are the requirements around transparency, lawful bases for processing and consent.

The development

The ICO hs announced that it will be updating its existing direct marketing guidance. It opened a call for views on 12 November. This will shut on 24 December 2018. The questions in the survey include:

- what data protection changes should the ICO focus on in their direct marketing code?
- are there any direct marketing changes that should be included?
- is the content in the guide relevant to your organisation?
- do you agree that an updated version should be published before the ePrivacy Regulation is finalised?
- are there any case studies that you would like to see included?

The call for views is the first step of the ICO's process. It is likely to be several months before we see a new version of the code published.

Why is this important?

Interested parties have the opportunity to give their views on what would be most helpful in a new code. The more submissions that the ICO have from affected organisations, the more useful the guidance is likely to be.

The guidance provided by the ICO will be a useful resource for direct marketers. The new code should provide clarity on areas of the DPA which are relatively vague, and which lack practical examples.

The bigger question is how any guidance will sit with the ePrivacy Regulation (still in draft form, but likely to land in 2019/2020). The latter really is a game-changer on the use of data for direct marketing, and not in a good way!

Winter 2018

Data protection

"Google You Owe Us" class action blocked – Richard Lloyd v Google LLC

The question

Do you need to show relevant damage for a claim under the Data Protection Act 1998 (**DPA**)? Can a class action succeed if the members of the class cannot be readily ascertained or be said to share the same interest? Put another way, what are the restrictions on bringing an action for damages under the DPA?

The background

Richard Lloyd (former Which? Director) sued Google on his own behalf and on behalf of others as leader of the Google You Owe Us group. He alleged that Google had secretly tracked and collated browser-generated information from iPhone users, using the Safari workaround, between June 2011 and February 2012, and then sold that information to advertisers. This allegedly included the user's geographical location, IP address, browsing history, race, ethnicity, social class, political and religious views, gender, health and financial position.

Lloyd claimed that this secret tracking breached Section 4(4) DPA. He claimed damages under Section 13 DPA, but no particulars of individual damages were pleaded. Indeed, no financial loss or distress was even alleged.

The Safari workaround was the basis of the Vidal-Hall claims, which had been settled by Google. Lloyd was seeking permission to serve the proceedings on Google LLC out of the jurisdiction.

The decision

To establish permission to serve out of the jurisdiction, Lloyd had to establish that:

- the claim had a reasonable prospect of success;
- there was a good arguable case that each claim fell within one of the jurisdictional gateways, and
- England was clearly or distinctly the appropriate forum to try the claim.

There was no dispute that England was the appropriate forum in which to bring the claim, as the class was confined to residents in England during the period. However, the court concluded that the claim did not disclose the basis for seeking compensation under the DPA.

The statutory right to compensation arose if (a) there was a contravention of a requirement of the DPA and (b) as a result, the claimant suffered damages.

But Lloyd did not identify the damage resulting from the contravention. Equally, the court cannot make a "vindicatory" award of damages.

As to whether the claim had a reasonable prospect of success, the court concluded that the essential requirements for a representation action were absent. The lead claimant and the class did not have the "same interest" under CPR 19.6(1). The alleged breach was not uniform across the entire class, as some affected individuals were heavy internet users, while others engaged only lightly. There were also serious practical difficulties in ascertaining whether any individual was a member of the class in question.

Consequently, the application to serve outside the jurisdiction was refused.

Why is this important?

Although the DPA has been replaced by the GDPR, the principles underpinning the right to compensation remains largely unchanged under Article 82 GDPR and Section 168 of the Data Protection Act 2018. Therefore this case serves as an important examination of how a claim would be considered by the courts.

The court made it clear that individuals need to have suffered actual damage as a result of any breach of data protection law. The decision confirms that the English courts will not entertain frivolous actions from individuals who find that their data protection rights have allegedly been infringed but have not been negatively impacted. It remains to be seen whether this judgment curbs the number of data breach claims moving forward.

Any practical tips?

Beware the class action for data breach! It may seem odd to say this in light of Lloyd's failed case (albeit he is looking to appeal). However, what if Lloyd had chosen a case where he could easily prove actual damage or distress? For example, a case involving a breach of sensitive personal data? At a modest £750 per claimant (a figure suggested as a guide in this case), the maths is pretty horrifying: £750 x 1,000 = £750,000. £750 x 100,000 = £75,000,000!

Winter 2018

Data protection

Various Claimants v WM Morrisons Supermarket PLC [2018] EWCA Civ 2339

The question

Can a business be held vicariously liable for the actions of an employee who deliberately breaches its data protection policies and data protection law?

The background

In 2013 Andrew Skelton leaked the payroll data of almost 100,000 Morrisons employees. Mr Skelton retained a copy of the payroll master file without his employer's knowledge and posted the information to a file-sharing website.

5,518 affected employees brought claims for compensation. They alleged that Morrisons had breached their duties under the Data Protection Act 1998 (DPA) and were liable for the common law torts of misuse of private information and breach of confidence.

The court at first instance found that Morrisons had taken appropriate technical and organisational measures to safeguard personal data. It held that the business had not breached its duties under the DPA, but that it was vicariously liable for misuse of private information and breach of confidence by Mr Skelton.

Morrisons appealed the second issue to the Court of Appeal.

The decision

The Court of Appeal rejected Morrisons' arguments. Their reasoning affirmed the conclusions reached by Langstaff J in the High Court. The key points in the judgment were as follows:

- the DPA does not exclude vicarious liability for misuse of information or breach of confidence. Whilst the provisions of the DPA only require that reasonable measures are taken to protect personal data, strict liability is still possible under the common law. Parliament would have made it clear in the statute if they intended to exclude this type of liability
- Morrisons was vicariously liable for Mr Skelton's actions. His malicious intentions when leaking the information did not prevent this from being made out. The court agreed with Langstaff J's opinion that the incident occurred through an unbroken chain of events.

The Court of Appeal refused Morrisons permission to appeal. However, Morrisons have indicated that they will attempt to take their case to the Supreme Court.

Why is this important?

Even if businesses commit considerable resources to ensuring data compliance, they can still be held liable for the actions of a rogue or careless employee. The costs involved in defending group litigation can be enormous. Businesses should actively consider taking steps to minimise the risk of such incidents and limit their exposure.

Any practical tips?

The Court of Appeal referred to the role of cyber insurance in their judgment. Those concerned about the potential impact of a data breach should review their insurance policies. Businesses should check that they have suitable coverage in terms of the heads of losses and the liability for individual and aggregate claims. Having said this, it must be questioned as to how far insurance cover could extend to the potentially enormous (terminal?) liability created by class actions for data breach.

Another step that concerned parties can take is to ensure that they have access to a consolidated breach response service (like RPC's ReSecure). Following a breach, response services can provide relevant professional support from forensic IT experts and specialist lawyers, and limit the consequences of a breach. These services are offered as a benefit of some cyber insurance policies.

In terms of prevention strategies, IT policies can be designed to restrict the use of USBs and personal email addresses (which are often culprits in data breaches). IT teams can also monitor for breaches of IT policy and look into potentially suspicious activity. There is software available on the market which allows IT teams to identify spikes in data retrieval.

In short, no stone should be left unturned in the quest to limit the risks of a severe data breach. The consequences of a class action include the possibility of astronomical aggregate damages claims (not even counting GDPR-level fines). These could be enough to sink almost any business, however strong their balance sheet.

Winter 2018

Data protection

Six month imprisonment in first ICO computer misuse act prosecution

The question

Is the Information Commissioner's Office (**ICO**) extending the scope and severity of its enforcement powers?

The background

After moving to another company, an ex-employee of Nationwide Accident Repair Service (**NARS**) continued to access personal customer data from a software system also used by his new employer. Mr Mustafa Kasim gained access to the software system, which estimates the cost of vehicles repairs, by using his ex-colleagues' login details without permission and then proceeded to misuse the data. Following an increase in customer complaints about nuisance calls, NARS alerted the ICO of its suspicions that customer data was being misused and assisted the ICO with its investigation.

The ICO's decision to prosecute

The ICO usually prosecutes these types of cases under the Data Protection Act 1998 (**DPA 1998**) or Data Protection Act 2018 (**DPA 2018**) – however, the maximum penalty available for civil or criminal breaches under these Acts is a fine.

In this case, the ICO considered that the nature and extent of Mr Kasim's offences warranted harsher penalties than just a fine, so the ICO took the unusual step of pursuing dual charges against Mr Kasim, under both Section 55 of DPA 1998 (DPA 2018 did not apply retrospectively to the offending period of January to October 2016) and also the Computer Misuse Act 1990 (**CMA**) (which allows for custodial sentences ranging up to 14 years). In particular, the ICO prosecuted Mr Kasim under Section 1 of the CMA, which makes it an offence to cause a computer to perform a function with intent to secure access to any programme or data without permission and carries a custodial sentence of up to two years.

Mr Kasim pleaded guilty to the offence of securing unauthorised access to personal data and was sentenced to six months' imprisonment. Given this guilty plea, the ICO decided not to pursue the charges under Section 55 DPA 1998 to full trial. However, there are ongoing criminal proceedings to recover the benefits of Mr Kasim's deliberate misuse of the data.

With regards to NARS, the ICO recognised that NARS had worked with the ICO during the investigation and put appropriate technical and organisational measures in place to ensure that such a breach did not occur again.

Why is this important?

Although this case concerned the prosecution of an individual, this case is another warning to businesses that the ICO's enforcement practices are increasing in scope and severity.

Despite its previous position that prosecutions under the CMA are outside its remit, it is clear that the ICO is increasingly willing to flex its regulatory muscles and use all of the tools in its arsenal to ensure that the appropriate penalties are handed out for data offences. The head of criminal investigations at the ICO made it clear that the ICO will continue to "push the boundaries" to protect the personal data rights of individuals, even if the circumstances of the case do not fit squarely into either of the Data Protection Acts (1998 or 2018).

Any practical tips?

If businesses wish to avoid liability and stricter penalties from the ICO for deliberate data breaches, it is essential that they remain diligent with regard to their data protection practices and continue to monitor the processing of personal data by employees and ex-employees. Businesses should use strict password systems, keep access records and enforce strict internal sanctions for data misuse by employees. If suspicions of data misuse are raised, businesses should inform the ICO, assist with the ICO's investigation and immediately take steps to mitigate the breach and ensure that similar breaches do not reoccur. It's worth remembering the Morrisons class action case too. The facts were not too dissimilar to this case, in which Morrisons were held to be vicariously liable for the actions of its rogue employee. And so it's not just the regulatory fines which come into view, but also (potentially very) expensive class actions.

Winter 2018

Data protection

Bupa fined for systemic data protection failures

The question

What if an employee goes rogue with your personal data? Will you be able to show effective oversight measures including monitoring of employee access to databases?

The background

Between January and March 2017 an employee of Bupa's Brighton office copied the personal information of 547,000 Bupa customers. The stolen personal information included names, dates of birth, email addresses and nationalities. The employee was able to access the personal information via Bupa's customer relationship management system, from which he sent bulk data reports to his personal email account and subsequently uploaded the data to the dark web.

Bupa was alerted to the breach by an external partner who spotted the data for sale; the employee was dismissed and a warrant for his arrest was issued. Bupa and the ICO received 198 complaints about the data breach.

The decision

The ICO fined Bupa £175,000 for failing to have effective security measures to protect its customers' information.

After investigating the incident, the ICO discovered that Bupa did not routinely monitor the activity log of its customer relationship management system. A defect in the system also meant that Bupa was unable to detect unusual activity taking place within the system, such as the bulk extractions of data carried out by the rogue employee. The ICO's investigation also discovered other systemic failures in Bupa's technical and organisational measures which left 1.5m records at risk. An ICO spokesman noted that Bupa provided 'no satisfactory explanation' for these systemic breaches.

As the relevant data breaches occurred before the introduction of the GDPR, the ICO dealt with the incident under the provisions and penalties of the Data Protection Act 1998.

Why is this important?

Whilst being determined under the provisions of the now-defunct Data Protection Act 1998, this decision highlights the ICO's current proactivity in issuing fines for data breaches and

suggests that the ICO will not hesitate to use its new, stronger powers under the GDPR and Data Protection Act 2018.

The fine also reinforces the need for companies to employ sufficient security measures and strictly control, and monitor, access to of any personal data they hold. The ICO took particular issue with the fact that Bupa was unaware of the risk posed to its customers' personal data, and that it offered no satisfactory explanation for the systemic inadequacies in its system.

Any practical tips?

Ensure that any system which holds, manages or processes personal information is regularly monitored and has mechanisms to detect any unusual activity concerning the data. Restrict access to personal information to only those individuals who strictly need to process the data, and consider restricting the system's ability to copy or extract any information. This will help to both prevent future breaches and to demonstrate to the ICO that the company had in place effective security measures to protect personal information. It may well prevent a GDPR-level fine, and also lessen the risk of (an ever scarier) class action for distress caused by a data breach.

Winter 2018

Data protection

Ireland's Data Protection Commission launches investigation into Facebook's data breach

The background

On 28 September, Facebook disclosed that hackers had stolen keys that allowed them to access up to 50m user accounts with the potential for a further 40m which may have been compromised. The hack allowed the hackers to use the accounts as their own, reading and writing private messages and posts.

Facebook said that the vulnerability had been present on the platform since July 2017 and that they are unaware of how long the hackers have been able to exploit the vulnerability, though say that the flaw was discovered and rectified within two days. The breach was then reported to the Irish Data Protection Commission (**DPC**) the next day.

This is Facebook's largest ever data breach and its first since the GDPR came into force in May 2018 and will therefore be Ireland's first real test of its enforcement capabilities under the GDPR. Facebook find themselves exposed to fines of up to $1.6bn.

The decision

A statement confirming the Irish DPC's formal investigation came on 3 October and stated that "the investigation will examine Facebook's compliance with its obligation under the General Data Protection Regulation (**GDPR**) to implement appropriate technical and organisational measures to ensure the security and safeguarding of the personal data it processes". This is known as the 'security principle' which provides an obligation for organisations to ensure that personal data is kept safe.

The outcome of the investigation is not yet known but a point of interest will be that Facebook is alleged to have had vulnerabilities in its system since July 2017 and, again allegedly, steps were not taken to rectify this until over a year later. Whether Facebook took reasonable steps to discover this vulnerability including whether the flaw would have been discovered through regular system testing will inevitably determine whether they had complied with the security principle forming the centre of the DPC's investigation.

Why is this important?

Ensuring personal data is kept safe is of paramount importance under the GDPR. It is important to take into account the security principle when controlling and processing personal data to prevent being exposed to fines of up to €20m or 4% of an organisation's global

turnover. Whilst the financial implications are vast, the reputational damage that can be done from reporting a breach of any magnitude can be irreparable.

Considerations should be made with regard to the security principle and a party's obligation to take appropriate technical and organisational measures at all times.

Any practical tips?

To comply with the security principle, parties should consider using encryption or psuedonymisation to protect personal data in the event of a breach. Other measures include implementing an information security policy and providing training to those processing personal data, conducting regular risk analysis of storage and processing methods and undertaking system improvements where necessary.

Winter 2018

Data protection

Equifax fined £500,000 for data breach of 15m UK customers

The question

Had Equifax taken adequate and effective measures to protect customer data?

The background

Equifax, one of the world's biggest credit agencies, offered a product called Equifax Identity Verifier (**EIV**) which enables clients to verify the identity of their customers in various electronic methods by entering the customer's details into the Equifax system. The EIV data was originally processed by Equifax's US parent company, Equifax Inc in 2016. The data held for the EIV programme was transferred from the US to the UK. Following transfer of the data, the US company did not then delete the customer data from their systems, despite having no lawful reason to continue storing it.

Between 13 May and 30 July 2017, Equifax was subject to cyber-attacks on its global business where hackers stole 146m customers' personal information created between 2011 and 2016, including passwords and financial details.

Although Equifax Inc became aware of the cyber-attack at the end of July 2017 and a further smaller breach at the end of August, they did not warn Equifax Ltd until 7 September 2017, after which Equifax Ltd promptly notified the Information Commissioner's Office (**ICO**) on 8 September.

In a probe by the ICO and Financial Conduct Authority after the breach, it was found that Equifax Inc was warned by the US Department of Homeland Security as recently as March 2017 about "critical vulnerabilities" in its cyber-security systems.

The decision

Although the information systems in the US were compromised (owned and operated by Equifax Inc), the ICO found that the UK arm of the company (Equifax Ltd) failed to take appropriate steps to ensure its parent company was protecting the information.

It was found that the company had breached five out of eight data protection principles in the Data Protection Act 1998, including a failure to secure personal data and having a lack of legal basis for international transfers of UK citizens' data.

Equifax was sanctioned with the maximum fine of £500,000 under the 1998 Act and investigations into potential fines for Equifax Inc are still ongoing.

Why is this important?

Multi-national data companies must do all they can to ensure data protection compliance, not only within the UK but also in other jurisdictions where the data of UK citizens is being transferred between jurisdictions.

In addition to the reputational damage of a data breach and a failure to comply with basic data protection principles, the fines are now significantly higher under the General Data Protection Regulation and can be the greater of up to €20m or 4% of global turnover. But this could be potentially small change compared to the potential liability of a class action claim with this number of people affected.

Any practical tips?

In the event of a data breach, you must have regard to Article 33 GDPR which requires data controllers to notify the ICO within 72 hours of becoming aware of the breach. A delay by the parent company in telling its subsidiary would constitute a breach of the GDPR and could expose the subsidiary to massive fines.

Where data is being transferred between jurisdictions, you must consider whether the transferring jurisdiction continues to have lawful reason to store the data. If they do not, there must be an adequate process for the transferee jurisdiction to check and ensure that the data is deleted.

In any event, you must be clear that there is lawful justification for the transfer of data between jurisdictions and that stringent data processing agreements are in place to facilitate this.

Winter 2018

Data protection

What if there's no Brexit deal?

The question

Where does a no deal scenario leave our obligations under EU data protection principles?

The facts

The Government has published a short guidance note on what businesses might need to do in the event that we exit the European Union without agreement. It states that whilst a no deal scenario is unlikely given the mutual interests of the UK and the EU in securing a negotiated outcome, they have a duty to prepare UK organisations for all eventualities.

In the UK, the GDPR and the Data Protection Act 2018 together provide a comprehensive data protection framework. Of course, the DPA 2018 will apply regardless of whether we leave the EU with or without a deal so the UK's data protection standards remain unaffected.

However, the GDPR will only be incorporated into UK law through the enactment of the European Union (Withdrawal) Act 2018 if there is a deal in place. This means that transfers of personal data from organisations established in the EU to those in the UK will change.

In the event of a no deal, the European Commission can issue an "*adequacy decision*" which would allow for personal data to continue to be transferred between the UK and the EU. However, an adequacy decision cannot be made until the UK leaves the EU and becomes a "*third country*". There is currently no timetable in place for finalising an adequacy decision so the UK will be in a lacuna until an adequacy decision is made.

The Government states that you should "*proactively consider what action you need to take to ensure the continued free flow of data with Europe's partners*". In the majority of cases, this will mean relying on an alternative legal basis for transfer, namely the standard contractual clauses adopted by the Commission.

Why is this important?

As the Government says, if the unthinkable happens, we need to be ready. Does that mean we need to start thinking about putting in place the standard contractual clauses with our European counterparts? Sadly, in the Government's own words, "*yes*".

Any practical tips?

A no deal scenario is far from an impossibility. The good news (we hope) is that most businesses are by now GDPR compliant, in that they already have processing and/or controller terms in place with their vendors and customers etc. This should mean a more formulaic approach to setting up the model contract clauses - in other words, the task should not require negotiation of full processing or controller terms, but instead 'simply' signing up the relevant parties to the standard clauses. Then again, this is hardly an exciting prospect for GDPR-weary businesses and their lawyers. Let's hope, if only from a data compliance perspective, that the unthinkable really doesn't happen …

Winter 2018

Consumer

Amended UK consumer regulations in advance of Brexit

The question

What consumer protection provisions are being put in place to prepare for Brexit?

The background

Consumer protection law in the UK is currently governed partly by EU derived law and partly by UK national law. At present, the existing cross-border consumer protection frameworks across EU member states are largely similar and allow consumers to safely make purchases from other member states. In addition, the judicial co-operation framework allows civil claims for breaches of consumer rights to be dealt with in the appropriate member state and the harmonised dispute resolution mechanisms allow complaints to be dealt with properly. However, this position will undoubtedly change as a result of Brexit.

The Government has been making preparations to ensure the seamless continuation of UK consumer protection laws following the UK's exit from the EU, and on 10 December 2018 the government set forward The Consumer Protection (Amendment etc) (EU Exit) Regulations 2018 (**Amendment Regulations**), which will be given effect immediately before exit day in the event that a Brexit deal is agreed. Note that the Government had previously issued a notice, in October 2018, on what would happen in a no-deal Brexit scenario, the upshot being that it is unlikely there will be significant differences in consumer protection laws between a deal or no deal scenario.

The developments

The Amendment Regulations mostly remove references to EU legislation and institutions in UK consumer protection legislation and seek to ensure that EEU to UK consumer import contracts are treated in the same way as those dealing with imports from non-EEA countries. The Regulations also affect the enforcement and complaints rights available to UK consumers.

Amendments to the Consumer Rights Act 2015

At present, the Consumer Rights Act 2015 (**CRA**) covers contractual consumer rights in respect of the sale of goods, services and digital content and contains express provisions in respect of consumer relationships with non-EEA member states. The CRA provides that, where a sales or consumer contract has a close connection to the UK, certain mandatory UK protections will be afforded to the UK consumer, even in circumstances where the parties have agreed that the contract will be governed by the law of a non-EEA state. The CRA will

not however, imply mandatory protections from seemingly unfair contractual terms, where such terms reflect international conventions to which the UK or EU is a party.

The Amendment Regulations will remove the preferential treatment for EU Member States over non-EEA countries. Instead, consumer contracts which are governed by the law of an EEA state will now be treated in the same way as third country contracts and international conventions to which the UK is not a signatory will no longer be excluded from mandatory protection against unfair term provisions even if the EU is a signatory.

Amendments to the Consumer Protection from Unfair Trading Regulations 2008
The Consumer Protection from Unfair Trading Regulations 2008 (**CPRs**) protect UK consumers from traders importing into the EU who engage in prohibited unfair commercial practices (ie by being misleading or aggressive). The Amendment Regulations now mean that consumers will no longer have a direct right of redress against importers into the EU, and instead rights of redress against prohibited practices will only be available against importers into the UK.

Amendments to the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013
The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (**CCR**) currently harmonise the contractual rules across the EEA, so that traders and consumers face only one set of requirements across the EU in respect of pre-contractual information for in-store, distance, and off-premises contracts for goods and services. The Amendment Regulations will amend CCR to make reference only to UK legislation and authorities and to operate in pounds rather than Euros.

Enforcement and complaints
The Amendment Regulations will remove reference to EU member states, legislation and authorities from UK legislation. As such UK consumers will no longer be able seek redress from EU-based traders in the UK courts, and it will become more difficult to enforce UK judgments in EU member states, as there will no longer be an obligation on them to investigate breaches of UK consumer law or progress enforcement actions.

ADR organisations based in the UK will no longer be required to act in cross-border consumer disputes and consumers will no longer have access to the EC Online Dispute Resolution (**ODR**) platform to make complaints, which means that seller businesses may have to remove any (previously mandatory) links to the ODR from their terms and conditions.

Why is this important?
Although currently similar, UK and EU consumer laws are likely to diverge post Brexit.

It is clear that consumers purchasing goods from EU member states will lose certain protections, particularly in relation to the rights of redress under UK complaint and legal systems; however, they will continue to benefit from the mandatory protections under the CRA. Conversely, for EU-based sellers, the scope of the CRA has widened, (ie the CRA will apply in the event that the UK is not a signatory to the same convention as the EU) causing certain contracts to fall under the scope of the mandatory CRA provisions, where previously they would not have.

It remains to be seen whether consumer confidence in cross border purchases will suffer post-Brexit and whether there will be a dip in trade on the basis that consumers are deterred from making cross-border purchases with limited protections. In reality, it is unlikely that lack of access to the ODR system will have a significant impact on trade as there has not been a high volume of consumer claims using the system and instead this change will benefit sellers by removing the burden to have to link to the ODR system on their platforms. The government has, however, accepted that the most costly amendment for businesses under the Amendment Regulations will be re-training staff on new legal and ADR complaints procedures.

Any practical tips?

It is clear that, following exit day, UK consumer rights law and practices will change as a result of the Amendment Regulations (or in a no-deal scenario). When preparing UK consumer contracts that will be governed by the laws of a country other than the UK, EU sellers should carefully consider whether mandatory consumer protection provisions under the CRA will be triggered. Conversely, consumers should check the protections available under the governing law of the chosen EU country prior to purchase, to ensure that they are adequately protected. Cross-border seller businesses should review their ADR and complaints procedures to ensure that proper rights of redress are available to consumers (and look to remove any references to the ODR from their T&Cs) to ensure that consumers remain confident in making purchases from them as businesses.

Winter 2018

Consumer

Viagogo ordered to provide better information on ticket purchasing

The question

What steps will Viagogo be required to take in order to better protect consumers and what does this mean for the company and its consumers?

The background

Secondary ticketing operators have attracted substantial criticism in recent years for preventing music and sports fans from buying seats at popular events by allowing touts to purchase tickets in bulk and charge vast mark-ups via their reselling sites.

In 2017 the Competition and Markets Authority (**CMA**) launched enforcement proceedings against four secondary ticketing websites over concerns that they were breaching consumer protection laws. This resulted in three of the four websites committing to increase transparency. Viagogo, however, did not offer the same assurances and the CMA subsequently launched legal proceedings in August 2018.

The court order

The evening before the CMA's application was due to be heard, a settlement was reached whereby Viagogo agreed to make what the CMA called a "comprehensive overhaul" of its UK website. The parties agreed a court order requiring Viagogo to:

- tell ticket purchasers if there is a risk they will be turned away at the door
- inform customers which seat in the venue they will get
- provide information about who is selling the ticket, and expressly state where the seller is a tout (defined as someone who sells more than 100 tickets per year)
- not give misleading information about the availability and popularity of tickets, which had led to customers being rushed into making a decision or the wrong order
- improve their complaints handling procedure and make it easier for people to get their money back under Viagogo's guarantee when things go wrong, and
- prevent a sale where the seller does not own and may not be able to supply the tickets.

If Viagogo does not comply with the order by January 2019, it could be fined and individuals at the company could face imprisonment.

Why is this important?

The settlement represents another victory for the CMA in its crackdown on secondary ticketing websites. If Viagogo deliver on their commitments, consumers will have advanced rights and we should see a decrease in complaints made to regulators by ticket purchasers who feel they have been misled.

The CMA is not itself entitled to impose fines but has the right to enforce consumer protection law through the courts. It has shown again that it is more than willing to use its powers in the event of a perceived breach – this should be heeded by consumer-facing businesses who choose to dance too closely to the regulatory line.

Any practical tips?

Beware building online processes which sail too close to the wind from a regulatory perspective (whether around pricing techniques or otherwise). Unpicking these can be costly and burdensome, and make it hard to respond to regulators' demands. Above all, don't push the CMA too hard – they'll get you in the end!

Organisations should be aware of the consumer standards they are required to observe and seek legal advice if there is doubt as to compliance. Legal advice is also essential in the event that an organisation is subject to a CMA investigation. Adopting a structured and cooperative approach early on can save considerable time and resources and avoid reputation-damaging litigation.

Winter 2018

Consumer

Misrepresentations during the selling process - *Burki v Seventy Thirty Ltd [2018] EWHC 2151 (QB)*

The question

At what point do misleading statements in a selling process become misrepresentations?

The background

Ms Burki, a divorced mother of three, was seeking a romantic partner. She signed up to the matchmaking service Seventy Thirty Ltd (**70/30**) in late 2014, paying £12,600 for a year's membership.

Before signing up, 70/30's managing director assured her that the database contained a substantial number of wealthy men, a number of whom fitted her criteria. On the basis of those responsibilities, Ms Burki claimed she had been induced to become a member. She ended her membership after five months.

Subsequently, Ms Burki wrote two highly critical online reviews of 70/30, one on Google and one on Yelp. In the former, she claimed the service was a scam. In the latter, she said customers were coerced into accepting unsuitable matches and that the business did not provide the services it promised.

Ms Burki requested a refund, but her request was refused. She ultimately sued 70/30 on the grounds of misrepresentation and deceit. 70/30 counterclaimed for libel and malicious falsehood.

The decision

The judge took a critical view of the 70/30 database. There was a shortage of active paying members as the evidence showed that there were closer to 100 active members and could not "by any stretch of the imagination" be described as a substantial number. The judge found that the status of the men in the database was not clear from 70/30's terms and conditions, albeit Ms Burki acknowledged she had not read them. The representations made to Ms Burki had been untrue and misleading; she would not have joined if she had known the true status of the database. The composition of the database should have been made clear to her. If it had been, Ms Burki would not have had cause for complaint.

It followed that Ms Burki was refunded her membership fee (£12,600) and awarded a small sum of damages for distress (£500). Her claim for deceit did not increase her damages, as

Ms Burki's loss was the sum of her membership fee, which she was already receiving back from 70/30.

The judge found that the first of the reviews left by Ms Burki was defamatory and likely to cause serious harm and financial loss; it was not true that 70/30 was fraudulent or a scam. The damages for this were assessed at £5,000. The second review was also defamatory, but was found to be Ms Burki's true and honest opinion. The claim of malicious falsehood was unfounded, as they were written in the belief, albeit an erroneous one, that her complaints were justifiable.

Why is this important?

This case highlights the importance of being clear with customers about the nature of what they are being sold. It emphasises that attempts to imply to customers that a service will provide more than it is capable of doing can amount to misrepresentation. The courts will not tolerate companies deliberately making a situation unclear.

Any practical tips?

Note that, even if a non-reliance clause had been included in 70/30's terms and conditions, it would not have absolved 70/30 of liability for fraudulent misrepresentation. If the misrepresentation had been negligent, a clause attempting to exclude liability would have had to pass the fairness test under the Consumer Rights Act 2015.

Ultimately, the key is that when dealing with customers, you should be careful to confirm that they understand exactly what they are buying. Consider whether any statements being made are an exaggeration. Ensuring that customers are aware of the true situation may avoid allegations of misrepresentation.

Winter 2018

Online platforms

Unjustified Geo-blocking Regulation 2018/302(EC)

The question

Can a business block EU consumers from accessing their website to purchase goods or services?

The background

Geo-blocking is a system which tracks the location of an internet user and blocks access from certain countries. Online sellers geo-block overseas customers for a wide range of reasons. These include difficulties conforming with local laws and accepting foreign payment methods.

On 28 February 2018, as part of its Digital Single Market initiative the European Commission adopted a Regulation on "addressing unjustified geo-blocking and other forms of discrimination". It will apply to businesses from 3 December 2018.

The Regulation aims to reduce fragmentation in the single market, currently estimated to cost around €415bn per year. It seeks to do this by preventing businesses from geo-blocking their websites in other EU Member States. The restrictions should provide sellers with more cross-border sales and give EU consumers greater access to choice.

The Regulation builds on the existing Services Directive (Directive 2006/123/EC). Key provisions of the new Regulation include:

- a ban on blocking or limiting access to websites in other EU Member States (except as required by national or EU law);
- a ban on discriminating against EU citizens or businesses in other ways (for example by charging different prices, or offering more favourable deals in the home territory than in other Member States); and
- a ban on applying different payment requirements where the card used is in the same category, fulfils authentication requirements and is in a currency that the seller accepts.

Scope

The Regulation applies to traders who are selling goods and services in the EU through the use of an online interface. It applies to business to consumer (**B2C**) and business to business (**B2B**) transactions equally, as long as they are on standard terms and are not for resale. The wide definitions of goods and services mean that most online sales will be caught by the provisions.

There are partial exemptions for audiovisual services which supply copyright protected works (eg Netflix) and retail financial services. These services are exempt from the non-discrimination requirements for price and payment. However, they are not permitted to geo-block in other Member States. The Regulation is due to be reviewed in December 2020 and audiovisual services may be added to its scope.

The Regulation does not require businesses to comply with non-contractual Member State laws (such as labelling or sector-specific requirements). Businesses are not required to deliver to new countries or accept new currencies.

What is the impact of Brexit?

As part of their preparations for a no deal Brexit, the UK Government has released a draft Statutory Instrument (**SI**) which deals with geo-blocking. If there were to be a no-deal Brexit, the SI would allow businesses selling online in the UK to apply different conditions to the EU. Sellers would however, still be subject to the Regulation when selling in different EU Member States.

The SI could provide more flexibility for online businesses. However, given the current uncertainty around Brexit, it is far from an outcome which sellers can plan for.

Why is this important?

Many online businesses are still grappling with the implications of the EU's General Data Protection Regulation. The Geo-blocking Regulation adds yet another point on the list of compliance requirements.

The Regulation will require businesses to stop geo-blocking and allow consumers across the EU to have access. They will also need to ensure that their international pricing strategies and payment requirements are not discriminatory.

The good news is that businesses still have some time. Member States are required to appoint an enforcement body and legislate in relation to the level of penalties. There is no enforcement policy in the UK (as of yet) and other Member States are in the early stages of their legislative processes. Germany's fines of up to €300,000 provide an early indication of the level of penalties we are likely to see elsewhere.

Any practical tips?

Businesses can take the Regulation as an opportunity to expand their customer base to a wider pool. The EU is trying to promote a level of uniformity that will encourage customers to consider buying online from businesses based in other EU Member States. Pending Brexit, it is possible that the Regulation will lead to businesses seeing higher volumes of EU sales in the future.

Online platforms

The EU fights "fake news"

The question

What will the EU's code of practice on disinformation mean for tech companies?

The background

On 26 April 2018, the EU Commission released a statement on its intention to combat the spread of online disinformation - also known as "fake news". As part of this, the Commission initiated a consultation, gathering views from stakeholders, and asking tech companies to propose solutions.

On 16 October 2018, the EU's Digital Commissioner announced that a number of high profile industry participants had committed to a voluntary code of practice. These signatories were Facebook, Google, Twitter and Mozilla.

The Commission also published an Annex on best practice, providing information on the steps that the different signatories are taking to comply. The Annex includes details of company policies, initiatives and third party codes that the Commission and the signatories endorse.

The development

The signatories have set a number of objectives, these include:

- removing fake accounts
- providing accessible ways for users to report false information
- improving the systems that monitor how false information is being spread
- improving the transparency of political advertising, and
- minimising the advertising revenue for companies that spread false information.

The signatories will not be subject to any penalties if they fail to meet their targets. However, they have committed to publishing an annual report. Third parties such as the World Federation of Advertisers have agreed to verify their progress.

Whilst there aren't any fines or sanctions, signatories can be asked to withdraw if they are considered to be acting in a way which goes against the code.

Why is this important?

The Commission has stated that it views the code as a positive first step. However, it is willing to regulate the industry if the situation doesn't improve. The Commission's efforts come within the context of the European Parliament elections in May 2019.

Perhaps most importantly for tech companies, the last few years have shown that the reputational damage of fake news and data scandals is considerable. Advertising revenue and share prices can be hit if tech companies are not seen to be taking steps to minimise these issues. Being asked to withdraw from the code or being "named and shamed" by the Commission could have a considerable negative impact.

Any practical tips?

For the signatories, the code represents an opportunity to cultivate a more positive public image around how they are dealing with fake news and data issues. In this sense, it should be beneficial for the platforms both to make the changes and to let customers and advertisers know that they are doing so.

It also provides a potential way for the industry to avoid further regulation. If the Commission is satisfied with the progress that is being made, it is considerably more likely to forego passing regulations in the area – and regulations of any type would inevitably reduce the discretion and flexibility currently available to tech companies.

Winter 2018

Influencer marketing

#Ad-vice for influencers and brands: how to comply with CAP's new Influencer's Guide

With a flurry of adjudications against a number of well-known celebrities, the ASA issuing a call for evidence on the recognition and labelling of ads online in April, and the Competition and Markets Authority (**CMA**) launching a Consumer Enforcement Investigation in August, it seems that influencer marketing remains the hot topic for regulators.

To help influencers and brands comply with the legal requirements around influencer marketing, in particular ensuring that posts are #obviouslyidentifiable, on 28 September 2018 CAP issued a new Influencer's Guide, developed in conjunction with the CMA.

So – what does it say and how can influencers and brands comply?

What is covered by the Guide?

In addition to straight-forward paid advertising space online, the new Guide deals with a number of other types of advertising scenarios that commonly feature influencers:

Advertorial content

Perhaps the most common form of influencer marketing, this is where the influencer and brand work together to create content to be posted on the influencer's social media channels.

In line with previous guidance, CAP has confirmed that there needs to be both "payment" and "editorial control" in order to be considered advertising (and therefore subject to the CAP Code). However, the bar for each of these concepts is relatively low:

Payment – payment does not need to be made for a specific post or series of posts. If an influencer has any kind of commercial relationship with the brand (eg because they are a brand ambassador) and are paid as a result of this relationship, then this is sufficient. Payment also goes beyond monetary payments and includes loans of products/services, incentives, commissions or freebies (eg free products, gifts, trips, services, hotel stays etc).

Editorial control – if the influencer is not completely free to post whatever and whenever they want, then the brand will likely be exercising some editorial control. Specifying what needs to be featured in an image or video, control over timing/number of posts and/or ability of the brand to give final approval or require the influencer to change/remove a post will all likely meet the threshold for editorial control.

Whilst a lack of editorial control will mean that the post is not caught by the CAP Code, the Guide reminds influencers and brands that this type of arrangement is similar to sponsorship and so does still fall under consumer protection law, as policed by the CMA. The CMA requires that the existence of any payment will still need to be disclosed in the applicable posts (see CMA section below).

Affiliate marketing

This involves influencer content that promotes products or services using links or discount codes. The influencer is paid per-click or sale that can be attributed to their content promoting the product.

The Guide confirms that if a post features a mixture of affiliate-linked products and products that have been included by the influencer of their own accord (ie without any incentive), then only the affiliate linked-products need be labelled as advertising content. Whilst this is clearly desirable from a consumer transparency perspective, the Guide does not provide examples of how this can be achieved. For example, if multiple brands are tagged in a post, or if a single post consists of multiple photos, it is unclear how/where influencers would be expected to clearly identify which of the tags are affiliate links. One option could be to include such information within the caption. However, influencers need to ensure that this information is included upfront (ie without the need for consumers to click further) and so character limitations may be problematic in the context of mixed posts that feature multiple brands.

The Guide also states that in the context of affiliate marketing an influencer would effectively be acting as a "secondary advertiser" and so would be equally responsible for ensuring that the content meets all the other relevant advertising rules eg those concerning promotions, pricing etc.

Own advertising by the influencer

CAP has now confirmed that "own advertising" on an influencer's channel is also captured.

So, if an influencer posts about their own products/services – be it their own clothing brand, a restaurant that they own or an event that they are running – these will need to be identifiable as advertising content. It may be obvious from the post's content or the caption (eg if the influencer invites their followers to "come to my event" or makes clear that the products/services they are promoting are their own). However, if this is not immediately clear within the post itself, then best practice would be to include an appropriate advertising disclosure label (see below).

Additionally, any prize draws or giveaways by the influencer in a personal capacity would also be caught by the promotional marketing rules. This means that the influencer would be

responsible for communicating all significant conditions for promotions to consumers and complying with the other provisions of Section 8 of the CAP Code.

Ensuring that ads are #obviouslyidentifiable – what labels should be used?

In order to comply with ad disclosure requirements under the CAP Code the ad "must be obviously identifiable as such". If not already apparent from the context of the ad itself, this essentially means including an appropriately worded and prominently placed label. Responsibility for compliance lies with both the influencer and the brand and both would ordinarily be referenced in any ASA ruling.

CAP has reiterated that labels that make completely clear that the content is advertising are those preferred by the ASA – so, Ad, Advert, Advertising, Advertisement etc are all likely to be acceptable.

Drawing on examples taken from previously upheld ASA adjudications, CAP has confirmed that the following labels are often problematic as they do not present the full picture and therefore risk failing to meet the requirement of making it "obvious":

- sponsorship, sponsored, #spon
- in association with
- thanks to [brand] for making this possible
- just @ mentioning the brand.

Ultimately, the label needs to be upfront, prominent, appropriate for the platform, and suitable for all potential devices in order to be compliant.

Additionally, hiding #ad with several other hashtags or requiring the audience to have to click to "see more" before seeing the label will likely fall foul of the Code. In reality this means including the label in the title, at the beginning of the caption or on the image itself.

Similarly, CAP reiterated that the ASA has recently held that placing advertorial or affiliate content in "stories" will also be caught by the rules.

Beyond the control of the brand: the CMA's expectations

As mentioned above, if a brand has not exercised any editorial control, but the influencer has still been "paid", then consumer protection legislation will still apply – ultimately the "payment" element will need to be disclosed.

One of the most common examples of this would be when influencers are sent an unprompted gift by a brand where there is no formal requirement to post – the brand is gifting the product

in the hope that the influencer will use/wear it and choose to feature the product in a post in the future.

Notwithstanding that there will undoubtedly be many instances where influencers choose not to feature the products they are sent, the CMA still expects that where influencers do feature a free product in a post then this should be disclosed in the interests of transparency. But how to do this?

The Guide suggests that paid-for content (without editorial control) could be labelled as "advertisement feature" or "advertising promotion" in order to ensure compliance from a CMA perspective. However, this raises a complication - there is a risk that this in itself could be misleading to consumers (ie who may assume that a label which references the word "advert" is an advert in the traditional sense, thereby suggesting a formalised relationship between the parties where there is none). In circumstances where free products are gifted by a brand with no strings attached, a more appropriate label could be something along the lines of #gift or "gifted" as this makes clear that the influencer was given the product for free, but the brand did not have any control over the content. However, CAP has stated that the ASA would likely find #gift on adverts to be misleading. It follows that great care should be taken when assessing whether the post will fall under consumer protection regulation or the CAP Code in order to ensure the appropriate label is used. It is also why understanding whether the post is in fact an advert is so crucial - which in turn brings us straight back to the central question of editorial control.

Finally, it is also worth noting that the CMA expects any views expressed by influencers in their posts to be genuine (eg if they talk about any particular results that a product may have, then they should have experienced those results). It is unclear from the Guide whether this would equally be the case where the post is considered an advert within the ASA's remit. If so, this seems to be at odds with traditional ad campaigns which feature high profile celebrities. For example, consumers would not actually expect Kate Moss to actually use Rimmel as her everyday make-up or that Holly Willoughby, Davina McCall and Angela Scanlon regularly use Garnier's home hair colour treatment. Certainly if the post is actually suggesting that the influencer is personally using the products then the views expressed must be genuine. However, the CMA's expectation that views expressed by an influencer must be genuine has the potential to catch scenarios where the brand has provided messaging to be included in posts which are labelled as advertising. This is another example of the tricky overlap between the approach adopted by CAP and the CMA. The backdrop being that one would hope that consumers are savvy enough to recognise that advertising messaging is predominantly provided by the brand (ie and they are therefore not misled).

Is there anything else to remember?

The Guide has re-emphasised that influencers need to be mindful of other areas of the CAP Code, particularly when they are engaged in affiliate marketing or are advertising their own products. Before posting, influencers may want to ask themselves the following questions to help ensure they have addressed other potentially relevant areas under the CAP Code:

- If you are making a claim about a product or service, can you back it up?
- Are you advertising any age-restricted products eg gambling or alcohol? If so, do you know your audience composition?
- Are you promoting heavily regulated products such as food or supplements?
- Are you running your own prize promotion or competition?

If any of the above apply, clearly extra care will need to be taken to ensure that other CAP Code requirements are appropriately covered off.

Comment

Overall, the Guide is a welcome resource, consolidating existing guidance plus the ASA's expectations as discerned from many of the recent rulings into an easily digestible and concise document. The material offers some clear and helpful tips on staying compliant, and deals with a few of the previously considered "grey areas", in particular where influencers are given gifts and where they are posting about their own products and services.

Perhaps the biggest concern is that some areas of the Guide may well be difficult for influencers to apply in practice – for example:

- **multiple brands featured or tagged in a post** – how can influencers easily distinguish the content which is advertising, from the content which is not? As mentioned above, space limitations in captions may make this difficult to achieve in a way which is likely to be considered obvious (ie without the viewer needing to click a "see more" button)
- **unsolicited gifts** – would a label such as #gift or "gifted" be acceptable if there is no editorial control? If an influencer's post features a product from a brand which tthe influencer herself paid for, but the brand has also happened to send her other free unsolicited products (which are not featured), would the fact that she is still receiving free products need to be disclosed?

Ultimately, while the Guide does not cover all the bases, at the very least influencers are now in a better position to gauge when their content is advertising and how it should be labelled. For scenarios that do not seem to fall squarely within the Guide, or campaigns that involve higher risk areas (eg food, supplements, alcohol or gambling) legal advice should be sought by both the influencers and the brands and agencies that they work with in order to ensure that their campaigns stay on the right side of the regulatory line.

Influencer marketing

Under an obligation to repost an article you've written? You may need #ad – ASA rules against Platinum Gaming Ltd t/a Unibet

The question

When should a twitter post promoting a blog be classed as an ad, meaning that it should be clearly labelled as such?

The background

A tweet posted on 27 October 2018 by racehorse trainer Nicky Henderson stated "w*e're underway with the jumps and my exclusive @unibet blog is now ready to read*". A link to the blog was included.

A complaint was made under 2.1 and 2.4 of the CAP code for failing to make it obviously identifiable that the communication was an ad.

Unibet argued that although Nicky Henderson was under an agreement as a brand ambassador (the Agreement) and had to display Unibet branding, he was under no obligation to tweet on their behalf nor did they have editorial control over his Twitter account.

Unibet explained that the Agreement required Nicky Henderson to have regular interviews with a broadcaster, which would then be transcribed into a blog, and publicised on his social media accounts.

However, the Agreement stated that Nicky Henderson was required to start a Twitter account that would be managed by Unibet on his behalf, although he would have the right to approve all tweets sent on that account. Unibet argued that this did not reflect the reality of the Agreement, as most of the posts on his account were not related to Unibet. Furthermore, Mr Henderson already had a social media account prior to the Agreement, which Unibet did not have any input into. As Unibet were satisfied that Mr Henderson did not require direct assistance to fulfil his obligations, they did not facilitate him in doing so.

The ruling

The ASA upheld the complaint on the following basis.

The key tests as to whether the tweet was an ad were, firstly, whether Unibet had paid Nicky Henderson or entered a reciprocal agreement with him, and secondly, the degree of control that Unibet had over the content of the tweet.

Under the Agreement, Nicky Henderson was required to publish his blogs on social media, therefore the ASA concluded that he had been paid by Unibet to promote their brand on social media.

The ASA acknowledged that Unibet did not directly manage Mr Henderson's social media accounts. However, Nicky Henderson was specifically obliged to update his followers about his blog on social media; consequently, this was sufficient to meet the control test.

Therefore, the post was a marketing communication and should have been obviously identifiable as such. Nicky Henderson's twitter profile did state that he was a brand ambassador for Unibet; however this was not sufficient to differentiate between the tweets that were marketing communications and those that were not. The tweets on Nicky Henderson's blog, therefore, should have been identified as such, which could have been achieved by using #ad.

Why is this important?

The decision further expands the scope of social media posts that should be labelled with #ad. And now means that journalists and bloggers, who are under a contract which requires an obligation to repost their articles, will need to label these posts with #ad to ensure they are obviously identifiable.

Any practical tips?

If you are engaging anyone to promote a product, service or article on social media, care must be taken in checking whether it will be classed as an ad by the ASA. If so, it will need to be clearly labelled as such. Given the energy that the ASA (and indeed the CMA) are currently putting into pursuing influencer advertising, the message is clear - if in doubt, safest to use #ad.

Winter 2018

ASA – Data

New CAP Code rules on the use of data for marketing

The question

How have the Committee of Advertising Practice's (**CAP**) rules on the use of data for marketing changed as a result of the General Data Protection Regulation (GDPR)?

The background

The Advertising Standards Agency (**ASA**) previously regulated data protection issues under Section 10 (Database practice) and Appendix 3 (Online behavioural advertising) of the CAP Code. Section 10 regulated the general use of data for direct marketing, while Appendix 3 ensured that data based on the browsing behaviour of web users was collected and used in a controlled and transparent manner. Following the introduction of GDPR, CAP carried out a public consultation on the use of data for marketing.

The development

As a result of the consultation, the CAP Code rules on the use of data for marketing purposes have been amended and new rules have been introduced.

Narrowing CAP's remit

Section 10 has been updated to clarify that the ASA will now only regulate data protection issues specifically related to marketing (to avoid encroaching on the remit of the Information Commissioner's Office (**ICO**), who is better placed to deal with wider data protection matters). As such, "pure data protection matters" now fall outside of the ASA's remit (these matters are widely interpreted to include any matters that replicate GDPR provisions, for example, data security and transfers of data outside the EEA, or matters where the interpretation of GDPR is unclear).

The ASA maintains to power to refer marketing data matters to the ICO where necessary and the ASA and CAP will also be advised by an independent expert panel (the Direct Marketing Commission - an independent industry watchdog) when "legitimate interests" is being used as the basis for processing data in marketing cases.

Removal of Appendix 3 from the Code

Appendix 3 has been removed from the Code and going forward, online behavioural advertising, will be regulated under Section 10.

Alignment with GDPR

The updated Section 10 rules now reflect key GDPR definitions and requirements in that they:

- include key definitions, such as consent, controllers and personal data
- clarify that others involved in sending marketing communications (ie data processors), such as marketing agencies or service suppliers, are responsible for compliance with data use rules (alongside data controllers)
- prohibit persistent and unwanted marketing communications (Rule 10.1)
- mirror Article 13 and 14 fair processing notice requirements to ensure proper transparency in data collection (Rules 10.2 and 10.3)
- allow personal data to only be further processed for reasons that are compatible with the original purpose for obtaining the data (Rule 10.4)
- mirror GDPR requirements that consent must be given before marketing data is processed (Rules 10.6 to 10.8 and 10.12)
- mirror GDPR requirements that marketers must have a legitimate interest to process customer data where they do not have prior consent (Rule 10.5)
- include specific rules for special categories of data – such as personal data that reveals the racial / ethnic origin, political opinions or religious beliefs of a consumer (Rule 10.9)
- make clear that suppression records should be kept to ensure that marketing communications are not sent to individuals who have asked not to receive them (Rule 10.10)
- require marketers to make reasonable efforts to avoid marketing to consumers that they know to be deceased (Rule 10.11), and
- clarify that consent is not required for corporate subscribers (Rule 10.14).

The new rules, contained in Section 10, are already in force, however, they are subject to a 12-month review, and the ASA accepts that for the first six months it is likely to deal with most matters informally (unless a formal ruling is required in the interests of the public or a particular sector).

It is likely that these new rules are likely to be revised further in the near future, as CAP has launched a separate consultation specifically related to data for marketing in respect of children and prize winners (CAP is yet to publish the outcome of this consultation) and has also confirmed that it will reconsider the new rules once the new Regulation on Privacy and Electronic Communications (the **ePrivacy Regulation**) is implemented.

Why is this important?

Businesses should by now be fairly comfortable with the new data rules for marketing, as the changes broadly reflect the general requirements under GDPR. While the ASA has suggested that it will deal with matters informally for six months, marketers should not think that the ASA is taking its self-regulation duties lightly. Data protection has been marked as being high on

the ASA's agenda and the ASA has purposefully maintained the power to refer matters to the ICO, who may then impose harsh penalties for non-compliance.

Any practical tips?

Marketers should ensure that they are familiar with the new Section 10 rules and other data protection legislation generally. Marketers should ensure that they have appropriate systems and procedures in place to collect data in a transparent manner, to properly obtain consent (potentially by implementing an opt-in rather than an opt-out system) or have a legitimate interesting in using the personal data of the relevant consumers. In so far as possible, marketers should also consider the type of consumer whose data they wish to deal with – ie have people in the distribution list asked not to be included in marketing communications, are they known to be deceased or does their data fall into a special category for the purposes of the relevant communication – if so, marketers should consider the additional Code rules which may restrict the use of personal data in those particular circumstances.

Winter 2018

ASA – Puffery

"By your side" claim not misleading – Lloyds Bank

The question

How do you distinguish between advertising "puffery" and a misleading ad?

The background

A TV ad run by Lloyds Bank (**Lloyds**), seen in February 2018, showed a black horse running through various scenes, with a voiceover stating "*yesterday, today and tomorrow we have been and always will be by your side*". At the end of the ad text stated on the screen "*by your side for over 250 years*".

In January 2017, several former Halifax Bank of Scotland (**HBOS**) employees were convicted for financial fraud. Lloyds later acquired HBOS. Keystone Law, a firm of solicitors representing victims of the financial fraud committed at HBOS (the most famous of these being TV presenter Noel Edmonds), objected to the actions Lloyds Bank had taken to address the fraud and challenged whether the claim "by your side" was misleading. They believed the claim "by your side" was misleading as they believed Lloyds had not supported or been "by the side" of the victims of this fraud.

Lloyds stated that "by your side" summated the "reliability, accessibility and security" it provided to customers, and the only claim which required substantiation was "for over 250 years", for which they could provide sufficient evidence. Lloyds also argued that the ad did not promote a specific product or service and could therefore not be misleading nor have omitted any relevant information. In any event, Lloyds stated that the ad could be substantiated due to the size of its banking network, the variety of its services, its customer base, the average number of customer interactions each month and other initiatives.

Regarding the HBOS fraud, Lloyds stated that the convictions related to criminal conduct prior to its acquisition of HBOS and that it had launched a review to determine any appropriate compensation. Lloyds further explained that there were approximately only 70 companies impacted by the fraud, equivalent to 0.001% of Lloyds' business customer base. Further, Lloyds argued that the complaint was about whether a retail consumer ad was misleading, rather than a business ad.

Clearcast noted that it had asked for substantiation of the 250 year claim and the rationale for the use of "by your side". Clearcast stated it was satisfied that viewers would infer the

message related to reliable, accessible and secure banking and did not agree the fraud case should be conflated with the “by your side” strap line.

The development

The complaint was not upheld by the ASA.

The ASA stated that the ad did not reference the HBOS fraud case or any relevant steps it had taken regarding compensating victims of the fraud. As such, the ASA considered that viewers would understand the ad to be general brand promotion and the claim “by your side” was “advertising puffery”, not requiring objective substantiation. The ASA did not consider “by your side” to be a commentary on the situation of the victims of the HBOS fraud case, and as the ad contained no references to fraud, the ASA did not consider details of the case to be material information which needed to be included in the ad. As such, the ASA concluded the ad was unlikely to mislead.

Why is this important?

Whilst the HBOS fraud case is a serious case of criminal conduct, the ASA did not impose any higher standard upon Lloyds because of it. The ASA considered the ad on its own specific circumstances and considered that it was unlikely to mislead. As such, this ruling should reassure companies running adverts that they are unlikely to be penalised for complaints regarding events unconnected to the ad.

Any practical tips?

Carefully consider what information is provided in any ads, and the extent to which this may negate a puffery claim. Lloyds escaped any ASA penalty as their ad did not mention the HBOS fraud and the strap line “by your side” was clearly a generic claim. However, the ASA’s approach may well be different if the text, voiceover or imagery of the ad makes any specific references which could be the subject of a complaint.

Winter 2018

ASA – Pricing

CAP issues new guidance on RRP comparisons

The background

Advertisements using comparisons against recommended retail prices (**RRP**) have long been the norm, but advertisers should be aware that these price comparisons may mislead customers if the RRP differs significantly from the price at which the product or service is generally sold.

One requirement for using an RRP is that the product must be "*generally sold*" at the RRP price. This will often depend on the product and sector in which the advertisement relates. This term has not been specifically defined. Additionally, what constitutes "*a significantly different price*" can also be difficult to determine. However, where a product is sold in a number of different retailers for similar prices and it can be proved that the advertised price is similar to those already in the market, it is unlikely that the ASA will find that the RRP differs significantly.

The decision

The new guidance provides an insight into the ASA's mind-set on RRPs. It states that:

- RRPs given by the manufacturer should not be the only substantiation for savings claims:

  A complaint against *Marcandi Ltd t/a Madbid* was upheld on 22 February 2017 where the advertiser had used the RRP of a Mini ONE car on an auction site. The ASA held that the RRP was not the price at which the product was generally sold. Where a product is no longer on the market, it would not be possible to demonstrate the price at which it is generally sold and an RRP should not be used.

- RRPs should not be used where the marketer is the only seller of the product:

  Where the price has been set by the marketer, it is unlikely to be accepted as an RRP. If a seller wants to compare against their own selling prices, the "was £xx, now £xx" should be used instead, as stated in the *Money Expert Ltd* ruling on 1 October 2014.

- RRPs should not be used for products that have not yet launched:

  An auction website made multiple savings claims by stating the RRP for an Apple Watch which had not yet launched. The RRP price was taken from a pre-launch news article

which estimated the price range. This was not sufficient to demonstrate that the item was generally sold at that price (*Blionix Ltd t/a liklebid*, 22 February 2017)

- Comparisons against advertised RRPs as opposed to the price at which the product is sold is unacceptable:

- In *Colgate-Palmolive (UK) Ltd* (30 October 2013), where a toothbrush was sold at the RRP of £169.99 for 12 weeks and then sold for a further 32 weeks at £84.99 or less, the ASA concluded that a claim that the product was "*worth £169.99*" was misleading.

Why is this important?

In the era of choice and variety, retailers will always try and differentiate themselves on cost. It is important to bear in mind that RRP remains as a guide and that retailers cannot use it solely for the purpose of demonstrating a saving for customers where that purported saving is misleading.

Any practical tips?

When making comparisons, retailers should consider whether the RRP really is the price at which the product is generally sold. If there is a significant price difference between the RRP and the price at which the product or service is already on the market, using the RRP as a comparator would not be recommended (pun intended).

If retailers are the sole seller of a product or service and want to use a price comparison for marketing, they should consider using a "was £xx/now £xx" style advertisement instead – and (naturally!) ensure that their selling processes/records can comply with the requirements of the was/now rules.

Winter 2018

ASA – Pricing

Savings claims not substantiated and significant limitations omitted – Laura Ashley Ltd

The question

How careful do you need to be in substantiating savings claims? And in what circumstances can you extend a promotional closing date?

The background

Laura Ashley Ltd (**Laura Ashley**) ran adverts in four emails between January and February 2018:

- the first email stated "Extra 10% of ALL home sale", with further text reading "SALE CONTINUES – UP TO 50% OFF* HOME + EXTRA 10% OFF*" and "UP TO 70% OFF* FASHION + FURTHER REDUCTIONS". The asterisks in the text did not link to any further writing;
- the second email stated "Blink and you'll miss it, 40% off everything ends tonight", with further text reading "NEW SEASON LAUNCH EVENT ENDS TONIGHT 40% OFF* EVERYTHING". Again, the asterisk did not lead to any further text;
- the third email stated "Hurry, 40% off EVERYTHING event ends TONIGHT", with further text reading "due to higher than expected order volumes, some of you may have experienced difficulty online over the weekend in placing your orders" and "OFFER HAS BEEN EXTENDED ENDS MIDNIGHT TONIGHT 40% OFF* EVERYTHING". Again, the asterisk did not lead to any text; and
- the fourth email stated "Decorating event with up to 50% off starts today", with further text reading "DECORATING EVENT starts today" and "50% OFF* Wallpaper and fabric, 40% OFF* curtains, 30% OFF* furniture, 30% OFF* paint". These asterisks also did not link to any further text.

The ASA received a complaint challenging whether: (a) the savings claims in the ads were misleading and could be substantiated; (b) ad (2) breached the code as the closing date had been extended; and (c) whether the ads failed to state significant limitations as the asterisks did not link to any text.

Laura Ashley stated that their promotions were planned six months in advance and there was typically a one to two day break between promotions, although this may change due to unforeseen circumstances such as the extension of the offer in advert (3) due to technical

issues. Laura Ashley provided evidence as to their dialogue with their technical team regarding the issues customers had with ordering products.

Laura Ashley also provided pricing information for products from their fabric, wallpaper, paint and ready made curtains stock, along with stating 10% of products in the "UP TO 50% OFF* HOME" and "UP TO 70% OFF* FASHION + FURTHER REDUCTIONS" sales were given the quoted discount. Laura Ashley also stated the asterisks were not linkable to further information, but would amend their ads to ensure a hyperlink was included to direct customers to detailed terms and conditions.

The development

The ASA upheld complaints (a) and (c), but not complaint (b).

In upholding complaint (a), the ASA considered that consumers would conclude a significant proportion of items included in the two sales would be discounted by 50% and 70% respectively, with all products within the "HOME" range included in the up to 50% off sale and all products within the "FASHION" range in the up to 70% off sale. The ASA also considered that consumers would understand from the claims that they would be making a genuine saving against the usual selling price of the product. The pricing evidence provided by Laura Ashley demonstrated that the products were only on sale for the higher "full price" for very limited amounts of time and so these higher prices were not the prices at which the items were usually sold. As such, the savings claims did not represent genuine savings against the usual selling prices. Further, no evidence was provided that a reasonable proportion of items were discounted at 50% and 70% in the two sales. As such, the ASA concluded the claims had not been substantiated and were therefore misleading.

In upholding complaint (c), the ASA noted that the terms and conditions for the sales made it clear the sales only applied to selected items within the relevant ranges, so it was likely some items within the ranges were not included in the sale altogether. However, despite Laura Ashley stating these terms and conditions would be linked to in their future emails, for ads (1) to (4), consumers were likely to understand that the discount would be applied to each product in a given range, when that was not the case. The conditions clarifying that some items were excluded should have been made more prominent in the ad. As the ads failed to state the significant limitations and qualifications of the sales events, the ASA considered them to be misleading.

In rejecting complaint (b), the ASA noted that consumers were likely to understand from the relevant email that the sale would finish at the end of the date of the email, the text "Blink and you'll miss it, 40% off everything ends tonight" reinforced the impression that consumers would have to act quickly to take up the offer. The ASA noted that the sale was extended another day, and considered that the CAP Code states closing dates must not be changed unless

unavoidable circumstances beyond the control of the promoter make it necessary. The ASA considered the evidence provided by Laura Ashley regarding customers' difficulty in making secure payments and determined that such circumstances were unavoidable and beyond the control of Laura Ashley, and had they not changed the closing date, those who sought to participate within the original terms would have been disadvantaged.

Why is this important?

This ruling reinforces the need for promoters to be able to substantiate all savings claims made in ads, and also to state all significant limitations and qualifications of any sales events. The ASA's ruling confirms the need to provide evidence demonstrating that any sales event represents a genuine saving against the usual selling price of the products, not a price at which they are sold for a limited time. The ruling also reinforces the need to include all significant limitations on an event; here, the use of asterisks not linking to any further information made it even clearer that certain information may have been omitted.

In rejecting complaint (b), the ASA highlighted its pragmatic approach to promoters extending deadlines, but also reinforced that it is likely to find a breach of the CAP code where a sales event is extended past the closing date for reasons within the control of the promoter.

Any practical tips?

Ensure that you can substantiate any savings claims made in ads. If you cannot provide sales evidence showing the usual selling price of a product, and that the sale presents a genuine saving, you are likely to feel the wrath of the ASA. Further, ensure that any significant limitations are included in an ad and the full terms and conditions are linked to from the text of the ad. On closing dates, only extend these if the circumstances are truly beyond your control!

Winter 2018

ASA – HFSS

Coco's revenge – ASA reverses Kellogg's HFSS decision

The question

Can a brand-generated character known for advertising HFSS products be used to promote a non-HFSS product to children?

The background

A TV ad for Coco Pops Granola was shown during a children's programme on 3 January 2018. A pack of Coco Pops Granola, a bowl and a jug of milk were shown in the foreground. Small on-screen text shown throughout most of the ad stated "Enjoy as part of a healthy diet and active lifestyle, 45g of Coco Pops Granola = 9% RI for sugar".

The Obesity Health Alliance challenged whether the ad was for HFSS products that were targeted to appeal to audiences below the age of 16.

The ASA Council originally ruled that the focus of the ad was the general Coco Pops branding (by virtue of the audio logo, the dominant Coco Pops brand name, the use of Coco the monkey, the yellow colour etc) and these elements were significantly more prominent than the references to the granola product. Kellogg's challenged the ASA's decision.

The response

Kellogg's confirmed that the product featured was not an HFSS product. The product was consistently referenced throughout the ad, and at no point was there a reference to the Coco Pops brand in isolation or to any other product in their range. Furthermore, they said that the ad was clearly distinguishable from other products in their range, and that as such there would be no confusion that the ad was only promoting the Coco Pops Granola.

Kellogg's highlighted that CAP's HFSS Guidance recognised that ads for non-HFSS products may use a brand-generated character or branding synonymous with a specific HFSS product, and that it also recognised the power of such brands to promote healthy alternatives to HFSS products. Kellogg's argued that if the ASA was to find that the ad had the effect of promoting an HFSS product it would reduce take-up of the granola product, which would be inconsistent with the Government's objectives on tackling unhealthy eating, and would discourage advertisers from developing healthier product alternatives.

Furthermore, Clearcast had approved the ad as the granola product was very prominent and not incidental to the branding. This meant that both parents and children would be able to tell the difference between the advertised granola product and Coco Pops original cereal.

Decision

In a reversal of the ASA Council's earlier decision (8 August 2018), the complaint was not upheld.

The ASA noted that the ad did not feature any HFSS products. However, the ASA had to consider whether the ad had the effect of promoting an HFSS product through the use of branding.

Coco the Monkey is a well-established brand character with the Coco Pops range; as such, the ASA considered it was therefore incumbent on Kellogg's to take careful steps to ensure that, if ads for non-HFSS products in the range were directed at children, they did not have the effect of promoting Coco Pops original cereal or other HFSS products in the range.

The ASA concluded that Coco Pops Granola was the focus of the ad throughout, including through the use of close-up shots of the product and the product pack (both of which were of a different appearance to other products in the range), and two references to "Coco Pops Granola" in the voice-over, including once by Coco. The brand name "Coco Pops" was also not used on its own. Although the ad drew attention to the milk "turning chocolatey", which was a phrase used in ads in relation to Coco Pops original cereal and other HFSS products in the range. However, given that it was self-evident that the Granola product had the same effect on milk, the ASA considered its inclusion did not give greater prominence to the Coco Pops range branding generally than to the Granola product itself.

Therefore, it would be clear to both adult and child viewers that the product being advertised was Coco Pops Granola. Hence why the ASA ultimately determined that the ad was not an HFSS product ad for the purposes of the Code. It was therefore not subject to the restrictions prohibiting HFSS product ads from being shown around children's programming.

Why is this important?

The decision is a welcome reversal of the previous ASA decision. The latter had caused quite a stir in the food and drink market, as it had effectively meant that any brand known as a HFSS product or range could have struggled to be used for a non-HFSS product as well.

Any practical tips

It is important to note that Kellogg had to make it clear in the ad that it was only promoting a non-HFSS product. If the ad had featured the Coco Pops brand in isolation and/or not featured the granola product as prominently, then the ASA's decision might well have stood. It

follows that care still remains the watchword for all non-HFSS advertising which uses elements of HFSS branding.

Winter 2018

ASA – HFSS

Placing HFSS ads too close to schools

The question

How close is too close when advertising an HFSS ad near a school? And what falls under the meaning of school?

Background

Under CAP 15.18 HFSS ads must not be directed at people under 16 through the selection of media or the context in which they appear. No medium should be used to advertise HFSS products if more than 25% of its audience is under 16 years of age.

In a series of recent decisions, the ASA has looked at HFSS ads that have allegedly been placed too close to schools, and have arguably been targeting children.

The decisions

- McDonalds Ruling – this concerned two McDonalds HFSS ads which were placed by the media owner JCDecaux. McDonalds had instructed JCDecaux not to place their ads within 200 meters of schools, in line with their policy. One of the ads was mistakenly placed within 47 metres of a primary school and the other within 95 meters of a nursery. Whilst JCDecaux admitted that the first ad had been mistakenly placed, they also provided evidence which estimated that the actual audience composition around where the ad was placed was around 21.84% under-16s (ie below the 25% benchmark). The ASA rejected this argument, and concluded that McDonalds had violated the 100 metre rule, and as such the placement of the ad breached the CAP Code. Regarding the ad placed near a nursery, the ASA concluded that this was not a breach as nurseries are not considered unsuitable to carry HFSS ads. This follows the standard approach taken by the outdoor ad industry.
- Burger King Ruling – this was a straight-forward application of the 100m rule concerning an ad, again placed by JCDecaux, within 96 metres of a primary school. The complaint was upheld.
- Subway Ruling - this concerned a Subway ad which promoted its “sub of the day” range, of which six out of seven were non-HFSS. Notwithstanding that the range mainly consisted of non-HFSS products, the ASA nevertheless considered that because the poster featured an HFSS product it was considered to be an ad for HFSS products. However, the complaint was ultimately not upheld by the ASA on the basis that sites located near to children’s centres (rather than primary/secondary schools) were not

considered unsuitable to carry HFSS ads under the standard approach taken by the outdoor ad industry.

Why is this important?

The combined effect of these three rulings is that it is now very clear that the ASA will apply a 100m placement rule around schools strictly – even when there is data to suggest that the actual audience may well have been below 25% under-16s. Interestingly, the rule only applies to primary and secondary schools and not to nurseries (see McDonalds ruling) or children's centres (see Subway Ruling). This may prove helpful in the context of other perceived "child friendly" locations (eg theme parks).

Any practical tips?

If an ad runs the risk of being classed as an HFSS ad do not place it within 100m of a school. Caution should be used when promoting HFSS products near other areas popular with children.

Winter 2018

ASA – HFSS

ASA issues guidance on HFSS media placement

The question

How can ads avoid falling foul of the CAP Code's HFSS restrictions?

The background

Under CAP 15.18, HFSS ads must not be directed at under-16s through the selection of media or the context in which they appear and no medium with an audience that consists of more than 25% of under-16s should be used to advertise HFSS products.

On 3 August 2018 the ASA issued "Food: HFSS Media Placement" (the Guidance) as a guide for advertisers on how to stay compliant with CAP 15.18.

Responsible targeting

The Guidance lists two main methods for targeting marketing communication, and explains how both can be used to ensure the ad reaches the correct audience.

The first is based on audience composition in which the ad appears. When placing an ad, marketers will need to ensure that they have a good picture of the composition of the audience. Robust, specific audience measurement is best practice. However if this is not available then general data can be acceptable, although this is a riskier approach.

The second method is using data to include or exclude individuals on the basis of their age, or other relevant criteria. If using data to create a mailing list, marketers must be able to demonstrate they have taken all reasonable steps to exclude under-16s. In some situations age specific data may not be available. In these circumstances age can be inferred from the interests and interactions of the individual.

Website content

Marketers must ensure they have a clear understanding of the audience composition of the website before placing HFSS ads. Best practice would be to hold data demonstrating that no more than 25% of the website visitors are under-16s.

The Guidance also stresses that, even if less than 25% of the audience is under-16s, CAP 15.18 can still be breached if the ad is designed for children. In the recent Cadbury ASA ruling, the material had clearly been produced for children, and given that it was downloadable

content it was likely that it would end up being given to children. Therefore this was considered to be directly targeting children.

Social media

It is expected that marketers will use all tools available to them to prevent under-16s from seeing the ad. This includes the use of internet based targeting tools. If these tools are available then the 25% targeting rule would not apply, as the ad could be sent to a defined set of users and avoid under-16s completely.

In a recent ASA ruling, Walkers avoided falling foul of CAP 15.18 by only targeting social media users who had an independent store loyalty card or visa card, and were therefore independently verified as over-18s.

The Guidance also notes that influencers will be expected to use these tools as well to ensure that any HFSS posts/ads are not targeted at children.

Apps

If an app has considerable appeal to children, then simply relying on age-gating will not be enough, given that these can be easily bypassed. As with other forms of untargeted media, marketers will need to be able to demonstrate that no more that 25% of the app users are under-16s.

In a recent ASA decision, the Squashies World app breached CAP 15.18 as the app had particular appeal to under-16s. The only tool used was age-gating and there was no data available to show the audience composition.

Is the content relevant?

The Guidance notes that the content is a contributing factor when the ASA assesses the likelihood of whether an audience for an ad was appropriate. The more the ad is likely to appeal to children, the more likely that the ASA will expect there to be clear data that the audience composition does not have greater than 25% under-16s.

Why is this important?

HFSS advertising remains a (very) hot topic. This Guidance serves as an important reminder to marketers on best practices when creating HFSS ads. Given the large volume of HFSS rulings in recent months, it is clear that the ASA are taking a strict approach, so the Guidance should be closely followed.

Any practical tips?

When creating an HFSS ad that may appeal to children, advertisers should ensure that robust audience data is available in case of an ASA complaint. They should also ensure that they

are using all available technology to block under-16s from being able to see HFSS ads on social media, websites, etc.

ASA – Prize draws

CAP tips on social media prize promotions

The question

What steps do you need to take to run a compliant prize promotion on social media?

The background

The Committee of Advertising Practices (**CAP**) publishes guidance on how the CAP Code applies to different industries and advertising platforms. Recently it has released a series of notes about how its rules apply online.

On 22 October 2018 it published a guidance note which focuses on the way that prize promotions are run on social media. This new note builds on the information in Rules 8.18-8.28 of the CAP Code and the guidance on prize promotions published in July 2016. It provides detail on steps that businesses should take and on how the ASA has interpreted the rules in past investigations.

The development

In the note, the 'key things to remember' are:

- putting important information in the initial ad – the ad should include the closing date and any conditions of entry. If the participant is required to purchase an item this should be clear from the start
- signposting to the full terms and conditions – participants should be able to access a copy of the terms before they enter the promotion (whether by hyperlink or signpost). This is particularly important where they will immediately be entered if they like or share a post
- dealing with participants fairly and avoiding undue disappointment – promoters need to demonstrate that they have a clear way to gather all entries, that all entries are put into the draw and that participants have a genuine chance of winning
- picking prize draw winners at random – promoters need to show that the winner was selected at random. The selection process can be done by a computer program, by an independent person or under the supervision of an independent person
- awarding the prize – if the prize isn't available, promoters need to ensure that they provide an appropriate alternative. The promoter must take adequate steps to alert winners that they have won.

Why is this important?

The key message is that whenever a prize promotion is being run it is important to comply with the CAP Code. The use of Facebook, Twitter or Instagram doesn't exempt a business from the requirements to conduct prize draws fairly, and display information so that it is clear to consumers.

Any practical tips?

Businesses should ensure that their promotions and social media teams are briefed on the guidance in this note and that it becomes integrated into their processes. Faster and less formal interactions between customers and businesses can make it harder for businesses to ensure that the rules are being followed. This may be stating the obvious, but building in time to check that the rules are indeed being met is always a good idea.

Winter 2018

ASA – Prize draws

ASA announcement on prize winners rule under the GDPR

The question

Are promoters still required to publish the details of prize winners? How does this sit with the GDPR?

The background

According to (existing) Rule 8.28.5 of the CAP Code, promoters are required to:

"*either publish or make available on request the name and county of major prizewinner and, if applicable, their winning entries except in the limited circumstances where promoters are subject to a legal requirement never to publish such information. Promoters must obtain consent to such publicity from all competition entrants at the time of entry. Prizewinners must not be compromised by the publication of excessive personal information*".

During a consultation on Rule 10 of the CAP Code in May to June 2018, CAP became aware that Rule 8.28.5 might not comply with data protection legislation.

Under the changes brought about by the General Data Protection Regulation (**GDPR**) and Data Protection Act 2018 (DPA) the definition of consent has become more stringent. Consent must now be given by clear and affirmative action, and it must be possible to withdraw.

This presents an issue. For example, if the participant's consent is withdrawn, the promoter will not be able to publish their details. In September CAP announced that they were updating their Code and would not enforce Rule 8.28.5 in the interim.

The development

CAP have proposed an amended version of 8.28.5 so that promoters:

"*must either publish or make available on request such information to indicate that a valid award took place – ordinarily the surname and county of major prizewinners and, if applicable, their winning entries. At or before the time of entry, promoters must inform entrants of their intention to publish or make available such information and give them the opportunity to object to the information being published or made available. In such circumstances, the promoters must nevertheless still furnish the details of the prizewinner and winning entry (as set out*

above) to the ASA, if challenged. The privacy of prizewinners must not be prejudiced by the publication of personal information and in limited circumstances (for example, in relation to National Savings) promoters may need to comply with a legal requirement not to publish such information".

CAP had a consultation on this clause open until 7 December 2018.

CAP has expressed the opinion that this Rule strikes the balance between transparency on prizes and the privacy of the prizewinner. Usually a surname and county will not be sufficient to identify a person (and therefore will not be data processing). Where it will be sufficient to identify the individual, the details do not need to be published and can be provided to the ASA if challenged.

Why is this important?

Promoters should not breach data protection laws in an attempt to comply with the CAP Code. They can now remove terms which require entrants to give their consent to the winner announcement in order to participate. Instead, promoters can seek consent to publicity after the prize has been awarded.

Winter 2018

ASA – Promotions

Failing to honour a gift promotion – ASA ruling against Superdrug

The question

What happens if you run out of gift stock so you can't honour a promotion? Put another way, what must you do to ensure promotions are administered fairly?

The background

The ASA investigated two separate complaints in relation to two Superdrug promotional campaigns, those being:

- "**Promotion** 1" – "*Free ORS Magic Hair Towel when you buy 3 Black and Asian hair products*" instore, and
- "**Promotion 2**" – "*Free Primer when you buy 2 St Moriz products*".

In both cases, the complainants argued that the promotions had not been administered fairly, and therefore breached Section 8.2 of the CAP Code, which provides that:

"*Promoters must conduct their promotions equitably, promptly and efficiently and be seen to deal fairly and honourably with participants and potential participants. Promoters must avoid causing unnecessary disappointment*".

In the case of Promotion 1, the complainant argued they had purchased the qualifying items, but that store staff had advised the promotion could not be honoured, as a delivery of the free gift had not been received by the store.

In the case of Promotion 2, the complainant argued that they had purchased the required number of St Moriz products, but had been told following purchase that the free gift was out of stock.

The response

Promotion 1

Superdrug responded with the following:

- an expected delivery of the free gift had not been received by the store, prior to the complainant's visit, due to unforeseen weather

- affected stores had been issued with a communication explaining that affected customers should be offered an alternative free gift
- all promotional material had been tagged as "*subject to availability*"
- IT systems for the relevant store did not show any qualifying purchases had been made in-store on the day in question.

Promotion 2

Superdrug explained that the complainant had not received the free gift as a result of an IT error, which meant the free gift had not been auto-added to the complainant's qualifying order. The issue had come to light on 9 May 2018, and an urgent request had been logged to investigate, and remedy the issue. Superdrug confirmed that the gift had been in stock for the whole of the promotional period (25 April – 22 May 2018), and a workaround had been provided following the error, to send the primer to affected customers.

The decision

Promotion 1

Following investigation, the ASA noted that the relevant store had received delivery of the promotional gift the day before the complainant claimed to have visited the store. As such, the initial delivery issues which Superdrug claimed to have affected availability, had not played a part in the availability of the gift in this instance. Superdrug was, regardless, responsible for ensuring sufficient stock was available at the start of and throughout the promotion.

The ASA also noted that:

- while Superdrug had advised staff to offer affected customers an alternative gift, this had not occurred in the case of the complainant, and
- while Superdrug had not logged any qualifying purchases on the relevant date, the gift's unavailability may have deterred the complainant from making the purchase, hence the lack of evidence of the same on Superdrug's IT system.

Finally, the ASA noted that the use of "*subject to availability*" did not relieve promoters of their obligation to do everything reasonable to avoid disappointing participants.

Therefore, the promotion concluded that the promotion had not been administered fairly and the Code had been breached.

Promotion 2

While the ASA accepted that the product had never been out of stock, the IT issue had existed for at least five days of the promotional period, and therefore had likely caused disappointment to a number of customers, alongside the complainant.

The ASA upheld the complainant's complaint, and concluded that, as the promotion was likely to have caused unnecessary disappointment to participants, it had not been administered fairly, and had breached the Code.

Why is this important?

Retailers should be aware of the high standard of behaviour required under Section 8.2 of the CAP Code. They must take all necessary steps to ensure customers are not disappointed by their inability to fulfil the terms of their own promotion.

Any practical tips?

Plan ahead! The ASA showed little sympathy to Superdrug, even where unforeseen circumstances had arguably caused the disappointment experienced by customers. Make sure your promotion is well planned, in order to ensure as successful execution as possible and to minimise customer disappointment.

Winter 2018

Gambling

Gambling ads of "particular appeal" to children: 32Red

The question

How easy is it for gambling websites to stray into creating content which is of "*particular appeal"* to children and therefore banned under the CAP Code?

The background

The BCAP Code states at Rule 17.4.5 that advertisements for advertising must not "*be likely to be of particular appeal to under-18s, especially by reflecting or being associated with youth culture*". Gambling ads therefore must not appeal more strongly to under-18s than they do to over 18s.

The complaints

Ant and Dec's Saturday Night Takeaway is a popular family variety television show. 32Red Ltd is a gambling website which aired a TV Ad for "*Ant and Dec's Saturday Night Takeaway online slots game*". The ad featured Ant McPartlin's voice stating "*Welcome to Ant and Dec's Saturday Night Takeaway. Featuring Ant versus Dec free spins and the amazing 'Win the ads bonus feature*". This was followed by Declan Donnelly stating "it's time to play win the ads". The voiceover concluded "*play online, on mobile and on tablet. Get £10 free when you join 32Red.com where you're the big deal*". As the voiceover ended the theme music to the show played in the background.

One complainant challenged whether or not the ad was irresponsible, because it linked gambling to Ant and Dec's Saturday Night Takeaway and was therefore likely to be of particular appeal to under 18s in contravention of BCAP Rule 17.4.5.

The response

32Red responded by stating that Saturday Night Takeaway was not targeted at under 18s and that it had a wide audience profile featuring many different age demographics. Under 18s, 32Red stated, were an under-represented portion of the population of the audience of the show. They were able to provide BARB data (audience data) which showed that across 2017 and 2018 the BARB index for the programme was around 90 and that no single episode over this time frame had indexed over 120. A BARB index of over 120 would indicate that a programme did have a particular appeal to under-18s.

Additionally, the appeal of Ant and Dec to under 18s had been previously considered by Clearcast in 2015, at which point an ad linked to the programme 'I'm a celebrity get me out of

here' (which was also presented by Ant and Dec) was reviewed and cleared by Clearcast. It was noted that Ant and Dec were approaching middle age and presented a wide range of programming, and therefore they were not associated with youth culture. Additionally, the careers of Ant and Dec had begun in children's programming in the early 90's when they were young. Clearcast considered that while it was likely that during this time Ant and Dec would have been popular with under 18s, they have been involved in a large variety of programmes since then and have garnered a more general appeal. Their audience from the early 90's would have grown up with them and it was thought that the pair's current establishment as TV comedy presenters does not have a greater appeal to under 18s.

The decision

Throughout their assessment the ASA judged the advert using the test of whether or not the advert is likely to appeal more strongly to under 18s than over 18s due to the specific appeal of Ant and Dec's Saturday Night Takeaway to under 18s.

In their assessment the ASA placed a lot of emphasis on (i) the available BARB data; and (ii) the specific elements taken from the TV show that were featured in the ads (the voiceover from Ant and Dec, the theme tune and the reference to the 'Win the Ads game'.)

The BARB data showed that while many under 18's watched the show, it consistently produced an index score below 120, meaning that the TV show did not have a greater appeal to under 18's than to the general viewing population as a whole. The ASA considered that, notwithstanding any specific content in the ad that might appeal particularly to under 18s, references regarding the programme in the gambling ad were unlikely to breach the BCAP code.

The ASA then considered that the specific elements taken from the TV programme in the two ads – the theme tune, the voice-overs from Ant and Dec, and the reference to the 'Win the Ads game' were generic features of the programme, and therefore unlikely to particularly appeal to Under 18s more so than over 18s.

The complaint was not upheld.

Why is this important?

This ruling reinforces how the ASA will assess the full context of ads that could potentially be of interest to children and the elements it will focus on when making its decisions. Additionally, it highlights how the ASA will look into the wider context of the materials that have the potential to be appeal to an audience under the age of 18.

Additionally, the reliance on BARB data here shows that certainty of audience is important when producing marketing communications that are heavily regulated, such as gambling.

Any practical tips?

Don’t appeal to kids when creating gambling content! Being certain of the audience data of any TV shows or characters that are associated with any gambling advertisements will be helpful in showing that you are advertising responsibly.

Winter 2018

Gambling

Consultation on age and identity verification

The question

What are the new age and identity verification rules that the Gambling Commission proposes to introduce?

The background

In an effort to curb underage gambling and, following recommendations made in the March 2018 *Review of Online Gambling*, the Gambling Commission has published a consultation with regards to enhancing the process of verifying customer's age and identity.

The consultation applies not only to remote gaming and betting licensees but also to identify verification solution providers and some society lotteries and external lottery managers (eg "instant win" games). The Commission is asking all interested parties to be proactive in suggesting ways in which future verification can be undertaken.

The current Licence Conditions and Codes of Practice (**LCCP**), created in 2007, require licensees to complete the age and identification review within 72 hours. Within this allotted time (and before checks have been carried out) the customer can gamble and deposit money, but may not withdraw their earnings. In the event that the customer is underage, the licensee must return their money. Remote lottery licensees have the same standards. Furthermore, the licensee is not obligated to check the age or the address of every customer that pays with a credit card – a randomised check will fulfil the current requirements.

The development

Age verification

The Commission wants to introduce more stringent rules than the current 72 hour time limit and a non-mandatory credit card check. Licensees and remote lottery licensees will have to identify the age of their customers:

- before they are able to deposit money or gamble
- before they are able to access free-to-play versions of gambling games or free-to-play online instant win games that licensees and remote lottery licensees make available on their websites.

The Commission has not set out a process by which the licensees should carry out the verification of age and has not prohibited the use of third party software or credit reference

databases to verify age. The Commission is aware that many licensees already have systems to identify the age of their customers before they are allowed to gamble and that new advances in software could result in faster checks.

Identity verification

The Commission has proposed that licensees should be obtaining and verifying information about their customers at an earlier stage in their relationship with them. Licensees would have to authenticate a number of details about the customer including the name, address, date of birth and email address before they are allowed to gamble. Furthermore, where the customer needs additional checks, the proposed regulation would not allow licensees to permit them to gamble until they had confirmed all the relevant information needed.

The Commission has also proposed to strengthen the current randomised credit card verification provision that licensees should make sure that the customer's name is the same as the name that is connected to the payment process.

The Commission would require that the suggested rules, on the implementation date, apply to both new and current customers, meaning that every registered customer is properly verified.

Why is this important?

With the rise in marketing and advertising of gambling coinciding with the increase in the rates of underage gambling, there is a growing awareness of the need to make changes to prevent underage gamblers.

The current provision of a 72 hour time for a check-up allows underage participants to deposit money and gamble without authorisation for three days. In addition, free versions of games on licensees' websites are seen to contribute to the encouragement of underage gambling. The suggested provision concerning the names of the payment maker and the customer are intended to identify young people who may be using other people's credit cards to gamble.

The abolishment of the 72 hour rule may help protect gamblers in general from being treated unfairly, as currently some gambling businesses use the rule to postpone a customer's collection of earnings.

Any practical tips?

Promotions for new users of a betting company are common-place, often with the aim of enabling them to sign up quickly and make bets on the same day. The new verification processes may mean releasing advertising or marketing for a particular bet earlier than normal.

Winter 2018

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

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

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

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

DM27820421

RPC