RPC

Commercial law snapshots

Autumn 2021

ADVISORY | DISPUTES | REGULATORY | TRANSACTIONS

Contents

Commercial

Supreme Court reaffirms established approach to liquidated damages and the interpretation of "negligence" in liability cap

Triple Point Technology Inc v PTT Public Company Ltd [2021] UKSC

The questions

How should a liquidated damages provision for delayed completion operate where termination occurred prior to work being completed or accepted?

How should a carve-out for "negligence" be interpreted when applying a cap on liability?

The key takeaways

The Supreme Court reaffirmed that, if the relevant terms are express and clear, a liquidated damages clause will apply up to the date of termination of a contract and general damages are recoverable from termination onwards.

"Negligence" has an accepted meaning in English law covering both a tortious duty to use due care as well as contractual provisions to use care and skill. The meaning of "negligence" in the relevant clause did not exclude the breach of contractual duties of care.

The background

The Defendant, PTT Public Company Ltd (**PTT**), entered into a contract with the Claimant, Triple Point Technology Inc (**Triple Point**), for the development, implementation and maintenance of commodity trading software. The work was to be completed in various phases linked to corresponding delivery and payment milestones.

Article 5.3 of the contract was a liquidated damages provision stating that "*if [Triple Point] fails to deliver work within the time specified and the delay has not been introduced by PTT, [Triple Point] shall be liable to pay the penalty at the rate of 0.1% of undelivered work per day of delay from the due date for delivery up to the date PTT accepts such work ...*".

Article 12.3 provided that Triple Point's liability under the contract would be capped at the contract price received by Triple Point but that the limitation of liability would not apply to Triple Point's "*liability resulting from fraud, negligence, gross negligence or wilful misconduct*".

Work was slow and Triple Point completed the first phase of work 149 days late. As a result, PTT paid Triple Point for Phase 1 but withheld further payments on the basis that they were tied to milestones for completion. Triple Point did not dispute that it had not met the Phase 2 milestones but suspended work, leading PTT to terminate the contract for breach. Triple Point issued proceedings for unpaid invoices and PTT counterclaimed for damages.

The High Court found Triple Point in breach of contract and awarded PTT unlimited liquidated damages, amounting to £3.51m. On appeal from Triple Point, the Court of Appeal held that PTT was only entitled to limited liquidated damages arising out of completed works.

PTT appealed, asking the Supreme Court to consider three issues: (i) whether PTT was entitled to liquidated damages for the delay in completing work before termination; (ii) whether clause 12.3's negligence carve-out meant that losses arising from Triple Point's negligent breach of contract were uncapped; and (iii) whether liquidated damages fell within the liability cap.

The decision

The Supreme Court found that the Court of Appeal had wrongly interpreted the liquidated damages clause. PTT did not need to "accept" the work for the clause to operate and they were entitled to liquidated damages up until termination of the contract, despite Triple Point's failure to deliver. However, those losses fell within the damages cap.

The Court also construed the carve-out for "negligence" in the limitation clause broadly - losses resulting from Triple Point's negligent breach of contract were uncapped and PTT was entitled to claim them.

Why is this important?

For parties who seek to include and rely on liquidated damages clauses (such as in IT agreements), the decision re-affirms the general approach that liquidated damages accrue until the contract is terminated.

It also confirmed that the Court will choose to interpret "*negligence*" broadly, applying its natural and ordinary meaning under English law, in the absence of wording to the contrary.

Any practical tips?

When drafting liquidated damages clauses, consider the impact of non-delivery and termination and expressly state the consequences.

For liability caps and limitation carve outs, ensure that the wording of the clauses is clear and unambiguous –if the parties intend that certain damages fall within caps or that certain liabilities should be excluded, say so.

Autumn 2021

Commercial

Supreme Court confirms (and confines the scope of) the doctrine of economic duress

Pakistan International Airline Corporation (Respondent) v Times Travel (UK) Ltd (Appellant) [2021] UKSC 40

The question

Does the doctrine of economic (or "lawful act") duress exist and, if so, when does it apply?

The key takeaway

The doctrine of economic duress exists under English law in limited circumstances. To establish liability for the tort of lawful act economic duress, the Supreme Court adopted a conservative approach – whilst bad faith may be relevant in the context, a commercial party can use its bargaining power to negotiate contractual rights or impose onerous terms.

The background

The Claimant/Appellant, Times Travel UK Ltd (**TT**) was a travel agent selling flights to Pakistan on planes owned by Pakistan International Airline Corporation (**PIAC**). Following a dispute over unpaid commissions, PIAC sent a notice of termination to TT, ending their appointment and reducing their ticket allocation. At virtually the same time, PIAC offered TT re-appointment under a new contract, the terms of which required TT to waive all claims for commission it may have had against PIAC under the previous agreement. Considering that it had no viable alternative, TT entered the new contract to avoid collapse. TT then sought to rescind the contract for economic duress and to recover commissions due under the previous contract.

The High Court found that TT was entitled to do so but its decision was overturned by the Court of Appeal, which held that economic duress could not be established, as it considered that PIAC had used lawful pressure to achieve an outcome which it believed, in good faith, that it was entitled to, since PIAC genuinely considered that it had a defence to TT's claims for commission.

The decision

The Supreme Court unanimously dismissed the appeal. It confirmed the three elements to be established for lawful act economic duress: (i) the defendant's illegitimate threat or pressure, (ii) which caused the claimant to enter the contract, (iii) in circumstances in which the claimant had no reasonable alternative to giving in to the threat or pressure.

Due to the lawful nature of the threat, the Supreme Court agreed that the threat's illegitimacy was determined by focusing on the justification of the demand. Where a demand motivated by commercial self-interest would ordinarily be justified, there were "rare" occasions where a demand would be unjustified and enter lawful act economic duress territory. However, the Justices disagreed on what would be recognised as an illegitimate threat or pressure at law.

Lord Burrows considered that the threat or pressure would be illegitimate if: (i) the defendant had deliberately created or increased the claimant's vulnerability to the demand; and (ii) the demand was made in bad faith. Lord Hodge (for the majority) accepted that bad faith may be relevant to the content and context of a demand but disagreed with the emphasis on bad faith. Instead, "*morally reprehensible behaviour which in equity was judged to render the enforcement of a contract unconscionable*" should be treated as illegitimate. This was because a commercial party can use its bargaining power to negotiate contractual rights or impose onerous terms, as there is no doctrine of inequality of bargaining power or general principle of good faith in English contract law.

Despite conflicting opinions on bad faith, the Supreme Court affirmed the Court of Appeal's decision, concluding that PIAC had not used reprehensible means to apply pressure. PIAC's conduct was certainly "*hard-nosed commercial negotiation*", but it had believed in good faith that it was not liable for breach of contract as a result of its failure to pay past commissions. As such, TT fell at the first hurdle for establishing lawful act economic duress.

Why is this important?

This is the first time that the Supreme Court has considered the doctrine of economic duress and its key elements. The decision may be considered conservative - and unhelpful to those on the wrong side of an inequality of bargaining power - emphasising the narrow circumstances where the conditions will be met and suggesting it will be rare in commercial contract negotiations.

Using illegitimate means to manoeuvre a party into a position of weakness to force it to waive its rights could be relevant but, without the "bad faith requirement", there could be uncertainty as to what "morally reprehensible behaviour" is required to establish lawful act economic duress.

Any practical tips?

While the judgment confirms that the boundaries of economic duress are not fixed, succeeding with lawful act duress claims will be very difficult. Claimants may find comparable causes of action, such as undue influence and unconscionable bargains, could be more appropriate.

Autumn 2021

Commercial

Court of Appeal finds no claim for unjust enrichment where it contradicts parties' allocation of risk under contract terms

Dargamo Holdings Ltd and another v Avonwick Holdings Ltd and others [2021] EWCA Civ 1149

The question

What is the interplay between unjust enrichment and contract, and when can an unjust enrichment claim succeed?

The key takeaway

Unjust enrichment has a limited role to play where there is a valid, performed contract. Parties will rarely be able to circumvent clear contractual terms by claiming they have not received all of the consideration expected.

The background

Avonwick agreed to sell to Dargamo and another purchaser (the **Third Party**) its 34% interest in a Ukrainian company, by transferring its shares in an English holding company (**Holdco**) to them. Dargamo and the Third Party sought to acquire additional assets (the **Other Assets**) from Avonwick, including its interest in two additional companies (the **Other Shares**).

The share purchase agreement (**SPA**) provided that Dargamo and the Third Party would each receive 50% of the shares in Holdco for $950m. The SPA expressly provided for the consideration of the shares but did not mention any other assets. By the time the SPA was signed, the parties had also exchanged drafts of a Memorandum of Understanding and a side letter providing for the sale of the Other Assets (including the Other Shares) by Avonwick to Dargamo and the Third Party, but neither document was executed. However, the parties accepted that $200m of the $950m purchase price under the SPA was attributable to the Other Assets, with $165m of that sum relating to the Other Shares.

The Third Party later acquired 50% of the Other Shares, after paying a further $13m to Avonwick as "technical consideration" (said to be required under Ukrainian law). Dargamo refused to pay additional "technical consideration" without assurances that Avonwick would reimburse the payment, and also made no attempt (so Avonwick claimed) to sign a separate SPA for the sale of some of the Other Assets. As a result, Dargamo did not receive its portion of the Other Shares.

Amongst various other claims between the parties, Dargamo brought a claim in unjust enrichment for restitution of the portion of the purchase price that it claimed was attributable to the Other Shares ($82.5m), on the basis that there had been a total failure of consideration. The claims, including the unjust enrichment claim were dismissed at first instance. However, Dargamo was given permission to appeal the unjust enrichment claim.

The development

Following a review of the law of unjust enrichment, the Court of Appeal dismissed the appeal and found that there was no failure of basis amounting to an unjust factor. The parties were merely being held to express terms of a contract that they chose to enter into and comply with.

The interplay between contract law and unjust enrichment was problematic but the two played distinct but complementary roles. Unjust enrichment (and an unjust factor) could not be relied upon to override valid and subsisting legal obligations for one party to confer a benefit on the other, particularly where to do so would contradict express terms of a contract (the so-called "Obligation Rule"). Only in rare cases will an unjust enrichment claim succeed and a failure of consideration be made out, despite the performance of a valid contract.

Why is this important?

This case is likely to be a leading authority for this complex area of law, given its detailed consideration of unjust enrichment principles, its interplay with contract and the concept of "failure of basis". It is also a reminder that an unjust enrichment claim does not provide a means of subverting an agreement. Commercial contracts should expressly set out all agreed terms, including any common expectations or understandings about what the contract provides for, in an executed written document.

Any practical tips?

Make sure the written contract covers all the key issues! In particular:

- cover all assets - If any assets are left unaccounted for, it may be difficult to recover monies paid. Where there is good reason not to include all assets within a specific contract, those assets should be dealt with in another agreement and the reasons for doing so expressly explained in the contract.
- include clear price apportionment where multiple assets are involved – especially where the sale of a business is structured as the transfer of assets and goodwill, rather than shares in a company.
- Clarify what happens if the purchase price is paid but assets are not transferred – for example, an express contractual right to be repaid part of the purchase price (or better still for payment to be linked to transfer).

Autumn 2021

Commercial

Non-contractual intentions are relevant to the reasonableness and enforceability of non-compete clauses

Harcus Sinclair LLP and another v Your Lawyers Ltd [2021] UKSC 32

The questions

Are non-contractual intentions of contracting parties relevant when determining whether a non-compete clause is enforceable?

The key takeaway

The parties' objective intentions and contemplations at the time the contract was entered into are relevant when assessing the reasonableness of non-compete clauses, even if such intentions were not included expressly in the contract itself.

The background

The claimants, Your Lawyers Ltd (**YL**), were instructed by a large group of individuals in respect of claims against Volkswagen Group United Kingdom Ltd in the wake of the vehicle emissions scandal. They intended to apply for a group litigation order and approached Harcus Sinclair LLP (**HS**) to collaborate.

As part of a non-disclosure agreement (**NDA**), HS undertook not to accept instructions from other claimants to the group action, without express permission from YL, for 6 years. However, HS subsequently accepted an instruction from another group of claimants and commenced proceedings on their behalf. They also signed an agreement to collaborate with another law firm, Slater and Gordon. YL applied to the court for enforcement of the non-compete clause.

The High Court agreed that the non-compete clause was enforceable and HS was in breach of contract, as: (i) the non-compete clause protected YL's legitimate interest in pursuing the group action; (ii) it was not more than reasonably necessary to protect YL's legitimate interests, as at the date of the NDA; and (iii) enforcement of the clause was not contrary to public policy. An injunction was granted preventing HS from acting in the group litigation.

The Court of Appeal overturned the first instance decision stating that the NDA only purported to protect confidential information. Whilst the parties had discussed collaboration, the issues had to be considered on the basis of the express provisions contained in the NDA. The Court of

Appeal agreed with the High Court that the non-compete clause was a solicitor's undertaking, but held that the Court had no jurisdiction in respect of it.

The development

The Supreme Court agreed with the High Court that the non-compete clause was reasonable and enforceable. Describing the issue as a "critical question of law", the Court held that YL's legitimate interests when assessing reasonableness comprised both the NDA and the parties' non-contractual intentions at the date of the NDA.

The Supreme Court also clarified the test for enforceability of the non-compete undertaking, identifying two key principles:

1. the non-compete will be reasonable if it protected the promisee's legitimate interests and went no further than was reasonably necessary to protect those legitimate interests, and
2. if the promisee can successfully establish the non-compete is reasonable, then it is for the promisor to show that it is unreasonable as being contrary to public policy.

In this case, it was a common intention that the parties would work together on the group action and this was therefore a protectable legitimate interest.

The court also concluded that the NDA did not constitute a solicitor's undertaking but was purely contractual and concerned a business opportunity. As such, it did not have jurisdiction as it was not binding as a matter of professional conduct.

Why is this important?

This decision shows that the Court will look at the wider context to assess the reasonableness of a non-compete provision, including issues not expressly provided for in the contract. It also highlights the need to adequately identify the legitimate interests that underpin a restraint of trade clause in order to demonstrate its "reasonableness".

Any practical tips?

Before drafting or agreeing a non-compete provision consider the legitimate interests that are being protected. Consider stating these interests within the agreement, either as recitals or within the relevant clause as an acknowledgement from both parties. Also consider how other obligations, such as to protect confidential information, interact with and may support the non-compete provisions.

Autumn 2021

Commercial

High Court strikes out claims for compensation for distress for misuse of private information, breach of confidence and negligence

Warren v DSG Retail Ltd [2021] EWHC 2168 (QB)

The question

Can misuse of private information, breach of confidence and the tort of negligence be asserted as causes of action in a claim for a data breach arising from a cyber-attack?

The key takeaway

A claim against a business concerning data breaches arising from a third-party cyber-attack should be considered under the relevant data protection legislation, not as a claim for misuse of private information, breach of confidence and the tort of negligence.

The background

The case concerns an individual claim (for approximately £5,000) brought against Dixons Carphone (**DSG**). In 2018, DSG was the victim of a cyber-attack under which the attackers accessed the personal data of many of DSG's customers.

The ICO investigated the incident and found that DSG had breached Data Protection Principle 7 under the Data Protection Act 1998, which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of data (the **ICO Decision**). A £500,000 Monetary Penalty Notice (**MPN**) was also issued against DSG. Both the ICO Decision and the MPN were appealed by DSG.

The claimant, who had purchased goods from Currys PC World, subsequently brought a civil claim against DSG claiming that his personal information, including his address, phone number and date of birth, had been compromised in the attack and that he had suffered distress as a result. The claimant alleged breach of confidence, misuse of private information, breaches of the Data Protection Act 1998 and negligence, and sought damages from DSG of up to £5,000 for distress suffered. Except for the claim for alleged breach of statutory duty, the DSG applied to the court for summary judgment and/or an order striking out the claims.

The decision

The High Court struck out the claims, save for the claim for breach of statutory duty.

Breach of confidence and misuse of private information

A successful claim for breach of confidence and misuse of private information would require a form of positive wrongful action on the part of DSG, for example, disclosing the private information in question to a third-party without permission. Whilst highlighting that DSG were the victims of a cyber-attack, the judge remarked that "*both [claims] are concerned with prohibiting actions by the holder of information which are consistent with the obligation of confidence/privacy*". However, neither cause of action imposed a duty of data security on DSG.

Negligence

Under English law, there was no need to impose such a duty of care where the statutory duties applied (in this case, those under the Data Protection Act 1998). Imposing a duty owed generally to those affected by a data breach would potentially give rise to an indeterminate liability to an undetermined class, which would serve no purpose given the obligations imposed under the Act. Even if a duty of care had been established, the claimant had failed to outline the loss suffered properly and the suffering of "distress" did not constitute damage sufficient to successfully plead a tortious cause of action. This claim was also struck out.

Why is this important?

The High Court's decision sets clear boundaries for the claims that can be brought in relation to a third-party cyber-attack. It has established that claims attempting to "dress up" such data breaches as breach of confidence / misuse of information torts, or alleging negligence where no separate duty of care is established, will not be accepted.

Claimants in these types of disputes often obtain "After the Event" (**ATE**) insurance to provide costs protection. ATE premiums are not generally recoverable for the defendant; although there is an exception for "publication and privacy proceedings" (which include claims for "misuse of private information" and "breach of confidence involving publication to the public"; but not data protection claims). This judgment should therefore prevent Claimants seeking to recover ATE premiums for claims which are properly data protection claims.

Autumn 2021

Data

DCMS consults on plans to reform UK data protection regime

The question

What does the Government have in mind for the future of the UK's data compliance landscape?

The key takeaway

The Department for Culture, Media and Sport (**DCMS**) has issued a set of proposals for the reform of the UK data regime which are aimed at reducing the friction in data protection compliance and increasing innovation. Personal data-rich organisations should respond to the consultation by 19 November 2021.

The background

When the UK exited from the EU, it retained the EU GDPR in the form of the UK GDPR which contained substantively the same obligations albeit with some minor amendments. It was this similarity between regimes that no doubt helped the UK secure an adequacy decision by the European Commission earlier this year.

However, the UK has been eyeing up the possibility of diverging from the standards imposed by the EU and this set of proposals arguably represents the first major step in the UK's departure from the EU regime.

The development

The DCMS has issued a set of proposals for reform of the UK data regime aimed at reducing the perceived burden of data protection compliance on business and barriers to international data flows.

Proposals set out various measures including:

- removing or amending specific provisions in the UK GDPR to reduce disproportionate burdens on companies of different complexities ie the end of a "one size fits all" model
- abolishing Data Protection Impact Assessments (**DPIAs**) to be replaced with a more flexible approach to identify and minimise data protection risks that better reflect organisations' specific circumstances
- amending data processing recording obligations in Article 30 but instead requiring that certain records be kept but allowing organisations more flexibility about how to do this in a way that reflects the volume and sensitivity of the personal information they handle

- adjusting the threshold for reporting data breaches to counter the trend of over-reporting with the ICO
- removing the consent requirements for analytics cookies in order to allow for easier consumer profiling and reducing the number of cookie pop ups, and
- implementing a system of adequacy decisions for other countries to which data transfers from the UK may be made, with a focus on risk-based decision-making and outcomes.

Why is this important?

With the potential overhaul of the UK data regime, there may be significant changes to data protection obligations. Whilst, in principle, these proposals appear to be aimed at reducing friction in maintaining adequate data protection standards, it remains to be seen how these will play out in practice and be enforced by the ICO – and, critically, what view the EU forms of these with regard to its UK adequacy decision.

Any practical tips?

Organisations which process significant amounts of personal data, or those whose businesses heavily rely on personal data, should make their opinions heard by responding to the consultation by 19 November 2021.

Autumn 2021

Data

DCMS announces post-Brexit global data plan for the UK

The question

How will the UK become a "business friendly" country for international data transfers?

The key takeaway

The UK Government has announced its intention to pursue "data-driven" growth in the economy. Under new post-Brexit data plans, it will prioritise data adequacy partnerships with the USA, Korea, Singapore, Dubai and Colombia, and is creating an international data transfer council of experts to consult on future policies.

The background

The Government had previously suggested in its National Data Strategy (**NDS**) that it would be reforming the UK data protection regime after the UK's exit from the EU. Following a consultation, the Department for Culture, Media and Sport (**DCMS**) published a report earlier this year confirming that its new strategy would continue to maintain high data protection standards while reducing barriers to data transfers in the interests of promoting business. The aim of the reforms is to increase trade and improve public services with data sharing.

As part of its announcement, the DCMS named New Zealand's Privacy Commissioner John Edwards as the UK's next Information Commissioner. In interviews, Mr Edwards said that reform of data protection rules is "*one of the big prizes of leaving" the EU*" and that *"there's an awful lot of needless bureaucracy and box ticking and actually we should be looking at how we can focus on protecting people's privacy but in as light a touch way as possible".*

The development

The package of reforms has now been announced including:

- a new set of data adequacy partnerships
- an international Data Transfers Expert Council, and
- a fresh consultation on how the future data protection regime should function.

As the UK is no longer a member of the EU, the Government can now choose which countries to list as having adequate data protection laws in place. To determine the country's adequacy, the Government will consider the rule of law, the existence of a regulator, and international agreements that that country has entered.

If a country is deemed adequate, organisations can transfer personal data freely between that country and the UK, provided that they comply with relevant adequacy decisions. The Government announced that it will be prioritising adequacy partnerships the USA, Australia, South Korea, Singapore, Dubai and Colombia. In its accompanying Mission Statement, the Government also set out its intention to use these partnerships as a driver for international commerce.

With regards to adequacy assessments the Government has published a UK Manual Template which contains questions that ensures that the relevant information is collected relating to a country's data protection landscape and its adequacy therein.

The Data Transfers Expert Council will consist of 15 individuals from academia, industry and wider society and will work on ways to remove barriers to cross-border data flow. The aim is that the Council will provide diverse expert opinion to inform future Government policy.

Finally, the Government will reform the UK's data protection regime and has announced a consultation on changes that can facilitate transfers of data responsibly and with a less significant burden on smaller companies and start-ups. The ICO announced its plans for this in the form of a consultation at the end of August.

Why is this important?

The UK appears to be pursuing a highly commercial, business friendly, approach to data protection, which may be welcome to many organisations. This represents, and requires, some significant divergence from the EU framework. The current proposals aim to maintain personal data protection and equivalence with the EU while removing certain barriers to transfer. However, the Government press release highlights that maintaining high data protection standards will be a priority.

The EU will be keeping a close eye on these developments for sure, particularly on the UK's data adequacy status if the law in the UK diverges too far from the EU's approach.

Any practical tips?

The UK's data protection landscape is likely to change significantly over the next 18 months, and it is therefore important that all stakeholders within organisations that handle personal data keep up to date with any announcement and contribute to any consultations when offered the chance.

Autumn 2021

Data

ICO consults on new draft international data transfer proposals

The question

What steps are being proposed by the UK's ICO to protect personal data being transferred outside the UK?

The key takeaway

The ICO has published new plans for a framework to replace the EU's SCCs post-Brexit. The proposals include some significant changes to the SCCs, in particular under its new draft international data transfer agreement (**IDTA**). All organisations involved in the transfer of data outside the UK should read them carefully.

The background

The ICO is calling for views on its draft international data transfer agreement (**IDTA**) which will replace the SCCs for personal data transfers outside the UK, and form part of the framework to assist organisations in complying with data protection law.

Following the decision in Schrems II last year, the EU released an updated version of the SCCs in June 2021. However post-Brexit, these updated SCCs will not apply to the UK GDPR. The ICO is therefore seeking to publish its own UK version of the SCCs to make sure they conform with Schrems II, which forms part of retained EU law under the withdrawal agreement.

The development

The consultation was launched in August this year and seeks opinions from stakeholders on the ICOs proposals covering three topics:

- updated guidance on international data transfers
- the draft Transfer Risk Assessment (**TRA**)
- the draft IDTA.

The draft guidance on data transfers primarily concerns the interpretation of Article 3 and Chapter V of the UK GDPR. The ICO is asking interested parties to provide their views on how they interpret these provisions.

The draft TRA sets out measures to evaluate the risks associated with transfers to third countries in order to determine whether the relevant transfer mechanism can be relied on. The ICO's TRA seems to closely align with the guidance put out by the European Data Protection Board following Schrems II.

The most significant part of the consultation is the IDTA. The ICO has adopted a different structure from the new EU SCCs, which are modular. The IDTA has a tabular format, with most clauses applying to all transfers of data irrespective of whether they involve processors or controllers. There are four parts to the IDTA:

- tables which will be filled out for each transfer
- additional protection clauses, to be filled out if the TRA identifies that the transfer mechanism requires additional safeguards
- mandatory clauses to be adopted in their entirety, and
- commercial clauses, which parties can include as an option.

In terms of substance, there are relatively few differences between the IDTA and the SCCs, which is not surprising as the IDTA will also need to incorporate GDPR requirements.

The consultation also proposes an option for the new EU SCCs to be used instead of the IDTA by incorporating a UK addendum. This draft addendum is designed to allow parties transferring EU personal data to insert a section to cover transfers made under the UK GDPR, meaning a smaller administrative burden.

Why is this important?

Although the IDTA and TRA are currently in draft form, the outcome of the consultation will impact anyone who transfers personal data from the UK overseas or provides services or contracts with UK organisations. The inclusion of proposals like the UK addendum suggest that the ICO is alive to the potential challenges of having a different system to the SCCs, especially for businesses that regularly transfer data between the EEA and the UK. However, the fact that the ICO is proposing new acronyms for its transfer documentation shows just how keen the ICO is to create some clear water between UK and the EU's approach to international data compliance.

Any practical tips?

The SCCs have been in place for some time, and organisations are likely to have developed processes based on their use. Any stakeholder that will be affected by a significant departure from the SCCs should consider responding to the consultation with views on how the IDTA will impact their business.

Autumn 2021

Data

ICO approves first certification scheme criteria under the GDPR

The question

How can the Information Commissioner's Office (**ICO**) help businesses and other organisations demonstrate that they comply with data protection standards?

The key takeaway

Three new schemes have been approved by the ICO in order to provide guidance for organisations on compliance with data protection law. They cover: 1) handling personal data correctly when equipment is destroyed; 2) age assurance; and 3) children's privacy online. Organisations will be able to apply for certification under any of the three schemes. Upon being certified, organisations will have evidence of their compliance, enabling them to show that they satisfy certain standards on data protection. It will also protect consumers and give them greater trust in the organisations that achieve certification.

The background

The General Data Protection Regulation came into force in May 2018. After the Brexit transition period, the GDPR was incorporated into British law through the UK GDPR which came into force on 1 January 2021.

The key provision that relates to the certification scheme is Article 42 of the UK GDPR. This effectively states that the ICO will be encouraged to establish these sorts of certification schemes. It also states that the ICO and other relevant certification bodies will be responsible for the assessment of organisations' compliance with the standards and then the approval or withdrawal of certifications. The three newly developed schemes are the first example of the ICO exercising this power under the UK GDPR.

The development

On 19 August, the ICO announced that it had approved the first UK GDPR certification scheme criteria. The three schemes that were approved are as follows:

ADISA ICT Asset Recovery Certification

This certification relates to recovery services which includes processing activities and data sanitisation. It covers applicants who are either data processors or sub-processors. Its aim is to assist controllers in managing compliance within asset recovery. Applicants will be assessed against four criteria:

1. Business credentials: This includes credit scores, insurance details and other business requirements
2. UK GDPR and UK DPA 2018 Compliance: This is an overview of general compliance, which includes incident and data breach management and information governance
3. Risk management: This includes assessment of an organisation's logistics and data sanitisation
4. Non-data service: This includes waste management and reuse.

For applicants to be certified, they will need to pass a full ADISA audit against the criteria.

Age Check Certification Scheme (ACCS)
This scheme is relevant to all Age Check Providers covering a range of age determination, age categorisation and age estimation. This certification will be used to ensure that age check systems are effective. This is vital for organisations that provide anything (goods, services, content) that is age gated.

Whilst there is an extensive list of technical requirements on the processing of personal data for organisations that wish to be certified, the key point is that the standards require applicants to have a publicly stated commitment to reduce the access children have to age-restricted goods.

Age Appropriate Design Certification Scheme (AADCS)
This scheme is relevant to all organisations that process data for services likely to be accessed by children. Apps, websites, social media platforms and online marketplaces are likely to be in scope.

The key requirement is that any organisation certified must identify the needs of children and support those needs when processing personal data. Some of the requirements are outlined below:

- keep children safe from exploitation risks
- protect children's health and wellbeing
- protect and support children's physical, physiological and emotional development.

The full list of actions is contained within the ICO guidance. Organisations will also need to undertake Data Protection Impact Assessments with a particular focus on the rights of and risks to children.

Why is this important?
While these first three sets of criteria have only been released, they are likely to become important stamps of compliance for organisations.

Consumers are also becoming increasingly aware of their own personal data rights. They may start to demand that the organisations they buy from have been certified to comply with the standards set out by the ICO.

Any practical tips?

If seeking certification, organisations should review the relevant ICO guidance in-depth. The ICO has issued comprehensive advice for each of the three schemes, which must be adhered to if you wish to be certified.

For companies offering services likely to be of interest to children, careful consideration of these schemes is highly recommended as is ensuring that no stone is left unturned in ensuring that all relevant safeguards are in place to ensure that children's data is protected.

Organisations are well-advised to keep watching the developments in data compliance like a hawk, and to remain nimble and as responsive as possible to the changing regulatory landscape. It goes without saying that those involved in age-sensitive content or products must remain particularly tuned in, both to the ongoing compliance risks but also the opportunities opening up through developments like these new certification schemes.

Autumn 2021

Data

ICO publishes guidance on three standards of Children's Code

The question

What must organisations do, or avoid doing, to meet the "best interests of the child", "detrimental use of data" and "data minimisation" standards of the Children's Code?

The key takeaway

The ICO's additional guidance should be used to ensure that organisations whose online services are likely to be accessed by children do not breach the Children's Code and subsequently the UK General Data Protection Regulation.

The background

The Children's Code (the **Code**) is a statutory code of practice produced by the ICO. It consists of 15 "standards" which must be met by organisations providing an "information society service" (**ISS**) that children (under 18) in the UK are likely to access. The definition of an ISS is wide and encompasses most for-profit online services, such as apps, search engines, social media sites and content streaming services.

The development

The ICO has provided guidance on how organisations can meet three of the Code's standards, namely "best interests of the child", "detrimental use of data" and "data minimisation".

Best interests of the child

This standard requires organisations to consider children's rights to play, to be safe from commercial exploitation, to be protected from abuse when they interact with others and to have access to a wide range of information and media. The ICO's suggestions for meeting each of these rights are as follows:

1. The right to play:
   - use data analytics to improve gameplay functions, and
   - ensure that children are free to join or leave online groups.

2. The right to be safe from commercial exploitation:
   - avoid default personalised targeting of service features that generate revenue
   - provide transparent information around how children's data may be monetised
   - do not have personalised advertising on-by-default

- abide by the Committee of Advertising Practice standards, and
- avoid marketing age-inappropriate or fraudulent products.

3. The right to protection from abuse when interacting with others:
   - avoid on-by-default data sharing with other service users
   - set privacy settings to "high privacy" by default
   - ensure children understand how their information is shared, and
   - keep children's personal data from falling into the wrong hands.

4. The right to have access to a wide range of information and media:
   - ensure that children can find diverse, age-appropriate information, and
   - avoid serving children with personalised information that is not in their best interests, such as disinformation.

Detrimental use of data

The ICO states that, to comply with this standard, organisations must conform with:

- the UK GDPR;
- industry codes of practice;
- Government advice; and
- any other regulatory provisions.

This is clearly very general advice and so organisations should look to the ICO's more detailed guidance on this standard, located on its website.

Data minimisation

Again, the ICO gives more detailed guidance elsewhere on its website, but its general advice to organisations is that they should:

- be clear about the purposes for which they collect personal data
- consider what personal data is needed to deliver each element of their service, and
- give children as much choice as possible over which elements of their service they wish to use and how much personal data they must provide.

Why is this important?

The Code is not a new law, but rather an add-on to the UK General Data Protection Regulation (**UK GDPR**) that explains how the UK GDPR applies in the context of children using digital services. As such, an organisation found to be in breach of the Code runs the risk of incurring a fine of up to £17.5m (or up to 4% of worldwide turnover), or even facing criminal prosecution. The Code also affirms the ICO's strict approach with regard to protecting the most vulnerable of society from possible exploitation.

Any practical tips?

The Code is strict, but the ICO's guidance is thorough. Organisations that may be providing an ISS to children should go through the guidance carefully and ensure that they comply in full. A Data Protection Impact Assessment template can be found on the ICO's website and may prove useful in ensuring compliance.

Autumn 2021

Data

ICO releases summary of discussions between G7 data protection authorities

The question

How will the G7 data protection authorities cooperate in the future and how will this cooperation potentially shape data protection within those countries?

The key takeaway

The G7 data protection authorities will begin to cooperate more closely in the coming years to harmonise best practices, know-how, legislative developments and enforcement across all the countries in a number of key areas.

The background

Following meetings conducted on 7 and 8 September 2021, the Information Commissioner's Office published a communique which summarised the discussions it had with other data protection authorities in the G7 and their commitments going forward.

As the communique notes, more data is being generated, collected and used than ever before globally, which means that data protection authorities will have to become better at anticipating, interpreting and influencing the advances on how data is used.

The development

The meetings covered seven separate topics under which the authorities agreed on several steps to be taken:

1. Privacy and competition – Cross-regulatory collaboration to support a robust global digital economy
   - Strengthening the collaboration between the G7 data protection authorities and domestic competition authorities on the regulation of digital markets.
   - Sharing know-how with each other with the view to foster consensus, set norms and facilitating practical actions on protecting individuals' rights and maintaining competitive digital markets.
   - Advocating for greater collaboration between the authorities and competition regulators.

2. Shaping the future of online tracking
   - Initiating strategic dialogue between the G7 data protection authorities and technology firms, standards bodies, designers and other parties to examine the role that tech developments play in creating a more privacy-oriented Internet, upholding and preserving the principle of informed and meaningful consent.
   - Continued collaboration between data protection authorities on widening efforts to improve standards of data protection by websites.

3. Designing artificial intelligence in line with data protection
   - Advocating a central role for data protection authorities in the future governance on AI.
   - Creating dialogue on the principles that should govern responsible development of AI.
   - Exchanging intelligence and expertise on novel applications of AI and their privacy implications.

4. Redesigning remedies for the digital age
   - Sharing information and experience on what regulatory remedies work best.
   - Advocating for legislatures to ensure that remedies keep up pace with technological changes and maintain sufficient party across jurisdictions.

5. Pandemic-driven tech innovations
   - Proactively demonstrate a commitment and ability to move quickly when needed, while ensuring high standards in data protection.
   - Advocating for innovation that meets public needs and protections peoples' privacy, which will keep pace with technological change.
   - Ensuring the proliferation of new technologies developed during the pandemic and their use for good and with privacy and data protection in mind.

6. Government access and data flow at international level
   - Engaging G7 Governments to support progressing initiatives at international level on Government access to personal data held by private companies and agreeing principles for the same.
   - Sharing relevant developments in the law and practice and coordinate domestic advocacy and policy efforts.
   - Developing constructive and appropriate relationships with other domestic oversight bodies to ensure consistent approaches to privacy and data protection.

7. Development of a framework for cross-border transfer of personal data and cooperation between G7 data protection authorities
   - Promoting a more open and frequent dialogue between data protection authorities to facilitate discussions.

- Exchanging experiences and practices in the governing of emerging technologies and innovations to foster interoperable regulatory approaches.
- Identifying opportunities for greater enforcement cooperation, including starting by developing a shared understanding of the legal frameworks and enforcement practices across jurisdictions.

Why is this important?

The discussions between the various data protection authorities signal a clear intent for more cooperation and potential harmonisations in terms of both enforcement approaches and legislative developments within the G7.

Businesses, especially tech companies, should keep a keen eye on any developments on the closer cooperation between the authorities, especially in the light of enforcement and data protection standards.

Any practical tips?

While high level, the G7 data protection authority discussions show where the future regulatory lines will be drawn in the data future. This is relevant for all tech companies, but particularly those at the cutting edge of innovation where data tracking and AI play such an important role. Keeping a close watch on how this is playing out on a macro scale may well pay huge dividends in the future.

Autumn 2021

Digital

DCMS publishes policy paper on digital competition regulation

The question

How does the Government plan to drive growth and innovation in digital technologies?

The key takeaway

The Government's principles outlined in its policy paper highlight the light touch approach it wishes to take with regard to the regulation of digital technologies. Intervention is likely to only occur on the most pressing issues of the future.

The background

On 6 July 2021, the Department for Digital, Culture, Media and Sports (**DCMS**) published a policy paper Plan for Digital Regulation, setting out the UK Government's principles for digital regulation in relation to the continued growth of this sector as well as ensuring a continued positive effect on the UK economy. The Government also indicated that it will consult on digital competition regulation regime proposals in summer 2021 in order to facilitate competition in the industry.

The development

The policy paper outlines the Government's overall vision for ensuring effective regulation of the digital technological landscape. The paper sets out new principles which will guide how the Government will design and implement the regulation of digital technologies as well as some practical proposals for how it will ensure a clearer and more streamlined regulatory landscape with the aim of encouraging innovation and competition.

The Government explains that by "digital regulation" it is referring to the range of regulatory tools available that are used to manage the impact of digital technologies on people, businesses and the economy. The plan sets out practical proposals to support a more streamlined regulatory landscape, including options to improve information sharing between regulators to reduce duplicate requests on industry and looking at whether additional duties for digital regulators to consult and cooperate with each other are needed.

The plan sets out three guiding principles policymakers must follow, and states that the Government should only regulate when absolutely necessary and do so in a proportionate way. These principles are:

- actively promote innovation: policymakers must work to back innovation where possible by removing unnecessary regulation and burdens. Where intervention may be necessary, regulators will take a light touch approach utilising non-regulatory measures such as technical standards first
- achieve forward-looking and coherent outcomes: the digital landscape is constantly evolving and can have a profound effect on different elements of the socio-economic landscape. Policymakers therefore must make sure that new regulations complement existing and planned legislation to ensure seamlessness in the introduction of additional regulation with very little impact on businesses, and
- exploit opportunities and address challenges in the international arena: digital technologies have an international reach; therefore, policymakers should take into account international considerations when forming regulations including existing international obligations (including trade deals), expected future agreements, and the impact of regulations developed by other nations.

Furthermore, in order to actively encourage competition, which has been identified as critical to the long term sustainability of the UK digital technologies landscape, the Government has established the Digital Markets Unit (**DMU**), which is to be equipped for proactive oversight and swift action on competition issues before they become significant issues. The Competition and Markets Authority (**CMA**) will also be supporting the DMU. Additionally, the Government consulted on digital competition regulation regime proposals this summer. This consultation closed on 1 October 2021.

Why is this important?

The policy paper and the overarching principles demonstrate the Government's commitment to creating a proportionate, innovation-focused regulatory system that will allow for continued, unencumbered growth of the digital technology sector.

Any practical tips?

While the encouragement of competition is positive, larger technology organisations will need to be mindful of their market power and position. Keeping updated on how the regulators will assess competition and when they assess that intervention is necessary will be key. As well as this, being mindful generally of how the Government applies these principles will help companies ensure they are operating within the desired remit.

Autumn 2021

Digital

DCMS and BEIS consult on new pro-competition regime for digital markets

The question

What will a future pro-competition regime look like for digital markets and how will it potentially impact businesses operating in the digital marketplace?

The key takeaway

The consultation presents the digital market with big potential changes to how companies can operate in the space, including a fully enforceable code of conduct. Additionally, companies with significant influence in digital activities will be subject to potential merger controls by the Competition and Markets Authority (**CMA**). It is therefore important for these companies to keep a close eye on the results of the consultation (which closed on 1 October 2021).

The background

Following recommendations made by the Digital Competition Expert Panel (**DCEP**) in early 2019, the Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy (**BEIS**) has released its hotly anticipated consultation on a new regime for the digital market that is aimed at promoting competition in the marketplace. In the consultation the Government is setting out its proposals for reforms to the regulatory regime, which looks to drive greater dynamism in the tech sector, empower consumers and drive growth across the economy.

The development

The consultation notes that there is unprecedented concentration of power amongst a small number of digital firms, which impedes competition within the space. Therefore, it is aiming to undertake an evidence-based assessment to identify those companies with substantial and entrenched market power in at least one digital activity, which will then be designated as having a Strategic Market Status (**SMS**).

Any companies designated as having a SMS are set to be subject to an enforceable code of conduct that will set out how they are expected to behave in the digital market, which attempts to promote fair trading, open choices, trust and transparency, and protect both consumers and smaller companies in the space. The newly established Digital Markets Unit (**DMU**) will monitor the digital market, and it will also have enforcement powers over the new code, allowing the DMU to levy data-related remedies and measures to enhance consumer choice.

The code of conduct will cover several principles for companies with SMS:

- **Fair trading**: trade on fair and reasonable commercial terms; not to apply unduly discriminatory terms, conditions or policies to certain users; and not to unreasonably restrict how users can use a firm's services.
- **Open choices**: not to unduly influence competitive processes or outcomes in a way that self-preferences or entrenches the firm's position; not to bundle or tie services in a way which has an adverse effect on users; to take reasonable steps to support interoperability with third party technologies where not doing so would have an adverse effect on customers; not to impose undue restrictions on competitors or on the ability of users to use competing providers; and not to make changes to non-designated activities that further entrench the firm's designated activity/activities unless the change can be shown to benefit users.
- **Trust and transparency**: provide clear, relevant, accurate and accessible information for users; give fair warning of and explain changes that are likely to have a material impact on users; and ensure that choices and defaults are presented in a way that facilitates informed and effective customer choice and ensures that decisions are taken in users' best interests.

In addition to the code the Government is considering introducing new merger rules for firms with SMS, seeking to prevent harmful mergers where those mergers would further enhance or entrench the powerful positions of firms with SMS. The merger rules are set to be overseen by the CMA.

Why is this important?

The new regime will profoundly reshape how the digital market works, and in particular what bigger companies in the space can or cannot do. The new code of conduct is set to restrict the activities those companies will undertake, and can be enforced by the DMU, as well as by the CMA which will have the ability to block mergers that it deems harmful and anti-competitive. It is imperative that companies that are at risk of being subject to this new code of conduct understand how it will potentially impact their business going forward once it is finalised, and take care in avoiding enforcement actions by either the DMU or the CMA.

Any practical tips?

Review the final code of conduct once it is published and undertake a review of how it potentially impacts your company and its operations in the digital market. It is also important for companies to keep a close eye on the actual outcome of the consultation and resulting legislative actions in the near future.

Autumn 2021

Digital

Government publishes online safety guidance for businesses

The question

What are the key issues highlighted by the House of Lords with the Government's Online Safety Bill?

The key takeaway

The House of Lords welcomes the changes proposed by the Government's draft Online Safety Bill (the **Bill**), but notes that in a number of respects the draft legislation is flawed in that it may result in the over removal of content, thereby curtailing online users' freedom of expression.

The background

The Bill was published in May 2021. It establishes a new regulatory framework to tackle harmful content online, including fines and other sanctions for non-compliance.

The House of Lords Communications and Digital Committee has recently published a report on freedom of information in the digital age (the **Report**), which includes its thoughts and comments on the Bill.

The development

The Report agrees with the Government's approach in a number of respects. It supports the Government's proposals in the Bill which require online platforms to remove illegal content. The Report also supports the Government's intention to protect children and vulnerable adults but notes that the proposals within the Bill in this regard do not go far enough. The Report considers that the police should be provided with additional resources in order to enforce the law on harassment, death threats, incitement, spreading hate amongst other offences. The Report considers that online platforms should contribute to the additional resources provided to the police.

The Report also highlights a number of perceived flaws within the Bill. In its current format, the Bill requires online platforms to state within their terms of use the type of content that is legal, but which they nonetheless consider harmful. This "legal but harmful" content would then be removed at the discretion of the online platform. The Report considers that the Government's approach to "legal but harmful" content is incorrect. The Report calls for existing laws to be properly enforced and for content that is sufficiently harmful to be criminalised, and not left to platform operators to rule on whether certain user generated content should be removed. The

Report cited the recent racial abuse aimed at the England football team as a prime example of behaviour that should be criminalised.

The Report also looks for the Bill to go further and empower platform users in order to promote civility online. Furthermore, there are calls for a duty to be imposed on platform users to ensure that responsible design choices are made, providing users with a neutral means of communicating with one another, and allow users to control what content they are shown through easily accessible settings.

The Report proposes that legal but objectionable content (falling short of legal but harmful) should be dealt with through the platform design (providing a neutral, unadulterated view of content), digital education and competition regulation. This empowerment, the Report notes, would better protect freedom of expression.

Why is this important?

The overarching issue for regulators is how to protect vulnerable online users, whilst allowing those users to freely express themselves. There is clearly a balance to be struck but the Report suggests that the focus should be on protecting those most vulnerable as well as criminalising certain behaviour in order to act as a deterrent.

Any practical tips?

The House of Lords Committee is wary of online content being over removed in a bid to keep vulnerable users safe online and reduce harmful online content. Their approach is based on properly enforcing existing legislation and regulating the design and management of online platforms. In order to better enforce existing laws, the Committee considers that platforms should contribute to the resources of the police.

If the approach recommended by the Committee is taken, online platforms will need to look at the design of their platforms and how information/communications are displayed. Platforms will also need to be prepared for increased enforcement action to be taken by the police in respect of the content displayed.

Autumn 2021

Digital

Law Commission publishes reforms targeting serious harm arising from online abuse.

The question

Will the proposed reforms targeting serious harms arising from online abuse be more effective at criminalising harmful behaviour?

The key takeaway

Current laws governing online abusive behaviour are often ineffective at criminalising generally harmful behaviour and in some instances disproportionately interfere with the right of free speech. The Law Commission (**Commission**) has therefore sought to modernise the law to address online and offline communications in a proportionate and efficient way. This is similar to the recent House of Lords report that suggested the Online Safety Bill does not go far enough to criminalise certain behaviour's online.

The background

The rise of the internet and social media in the 21st century has created extraordinary new opportunities to engage with each other on an unprecedented scale. However, the Commission says that the current laws that govern online abusive behaviour are not as effective as they should be in that they over-criminalise in some areas and under-criminalise in others. The Commission has therefore proposed a number of reforms targeting serious harms arising from online abuse while protecting freedom of expression more effectively. The recommendations would reform the "Communications offences" found in section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003. These offences do not provide consistent protection from harm and in some instances disproportionately interfere with freedom of expression. The Commission focuses on recommending a new offence based on likely psychological harm, and other offences to tackle cyberflashing, the encouragement or assistance of serious self-harm and sending knowingly false communications.

The development

The new harm-based offence

The Commission is recommending a new offence based on likely psychological harm. This will shift the focus away from the content of a communication (and whether it is indecent or grossly offensive) toward its potentially significant harmful effects. As such, the offence would criminalise behaviour if:

- the defendant sends or posts a communication that is likely to cause harm to a likely audience
- in sending or posting the communication, the defendant intends to cause harm to a likely audience, and
- the defendant sends or posts the communication without reasonable excuse.

To complement the harm-based offence, the Commission has made recommendations to ensure the law is clearer and protects against a variety of abusive online behaviour including:

- **False communications**: A new offence of knowingly sending or posting a false communication with the intention of causing non-trivial psychological or physical harm to a likely audience, without reasonable excuse.
- **Cyberflashing**: Amending s55 of the Sexual Offences Act 200 to include the sending of images or video recordings of genitals with the aim of causing alarm, distress or humiliation to the victim.
- **Threatening communications**: A specific offence targeting communications that contain threats of serious harm, designed to deal with the most serious threatening communications. It will be an offence if: (a) the defendant sends or posts a communication that is a threat of serious harm; and (b) in conveying this threat, the defendant intends the victim to fear that that threat would be carried out.
- **Encouragement or glorification of serious self-harm**: A new offence targeting intentional encouragement or assistance of self-harm at a high threshold. The offence will be committed where the defendant encourages or assists self-harm at a high threshold (equivalent to grievous bodily harm).

Why is this important?

The reforms, if enacted, involve a shift away from prohibited categories of communication (eg "grossly offensive") to focus on the harmful consequences of particular communications. The aim is to ensure that the law is clearer and effectively targets serious harm and criminality arising from online abuse, balanced with the need to provide robust protection for freedom of expression. The reforms also seek to "future-proof" the law in this area as much as possible by not confining the offences to any particular mode or type of communication.

Any practical tips?

Platforms should get ahead of the game and ensure they have the rigorous systems in place to protect people online, before it is soon formally introduced in new legislation. Areas to consider include: age gating; robust monitoring and reporting measures in place in order to seek out and remove harmful content; and user self-verification to make it easier to identify those that seek to cause harm.

Autumn 2021

Digital

NGO submits complaints on allegedly discriminatory algorithms for job ads

The question

How can online platforms ensure their ad targeting algorithms are non-discriminatory?

The key takeaway

An NGO, Global Witness, has submitted complaints about Facebook's ad targeting to the Equality and Human Rights Commission (**EHRC**) and the Information Commissioners Office (**ICO**). Global Witness has stated that the algorithms used by Facebook in their ad targeting are discriminatory. The algorithms in question resulted in certain job adverts being targeted at audiences that were predominantly one gender (eg nursery nurse jobs were targeted at an audience that was 95% female).

The background

Methodologies for ad targeting have become increasingly refined in recent years. Paid search has become more prominent, while organic posts now garner fewer and fewer impressions. The targeting of ads is run by algorithms of increasing sophistication. Platforms are also able to use the data they collect on users to more effectively target their ads. This is all in an attempt to boost CTR (click-through rate) and more importantly, conversions (or sales).

These algorithms are complex and can sometimes lead to results that are biased. In March 2019, Facebook was sued in the USA following allegations that its algorithms were discriminatory. In response, Facebook moved to prevent advertisers from targeting housing, employment and credit adverts to people by age and gender.

Earlier this year, another case against Facebook was brought in the USA. Samantha Liapes alleged that the targeting algorithm had discriminated against her by not showing her ads for insurance. Liapes stated that such adverts are targeted more at male users and younger users.

The development

Global Witness is an NGO based in London. In order to test Facebook's ad targeting, the group ran a series of job ads for particular roles to adults in the UK. Advertisers on Facebook are able to use a range of different targeting methods ie by age group, gender, interests etc. Global Witness instead used "Optimisation for Ad Delivery", which leaves the targeting up to the platform's algorithm. In this case, this was to generate link clicks. This meant that Facebook would show the ads to the audience(s) it determined were most likely to click on them.

Global Witness ran several ads for genuine job openings. Of these ads, 96% of the people shown ads for mechanic jobs were men, 95% for nursery jobs were women, 75% for pilot jobs were men and 77% for psychologist jobs were women. Global Witness has called for the EHRC to investigate these results and whether the algorithm breaches equality and data laws. Global witness has also consulted the ICO under Article 36(1) of the UK GDPR on the basis that the data processing utilised by Facebook's advertising tool presents a high risk of discrimination contrary to the fairness principle contained in Article 5(1)(a) of the UK GDPR.

Global Witness is also calling on the Government make it mandatory for technology companies to make their targeting criteria transparent and to carry out risk assessments on potentially discriminatory algorithms in order to identify potential issues and mitigate these risks.

Why is this important?

All online platforms with a presence in the UK need to be aware of the laws on personal rights, data and much more besides. This issue could be a hint of the future difficulties to be faced in managing automation and algorithms and imbuing them with a human side.

Any practical tips?

Platforms need to be mindful of the possibility of emphasis on optimisation leading to some undesired results. All organisations should seek to strike a balance between leveraging technology so it can be hugely impactful while also remembering to incorporate human checks and balances along the way. Being able to show that an algorithm utilises several metrics in order to target ads effectively will also be helpful to show that the algorithm is not potentially discriminatory.

Autumn 2021

Consumer

CMA threatens Groupon with court action over consumer practices

The question

What are some of the key areas which the CMA focuses on in online marketplaces when assessing compliance with consumer protection regulation?

The key takeaway

Keep an eye on redemption periods for vouchers and the practicalities of meeting the advertised timings. Watch out also for the accuracy of advertised product or service claims. Finally, take great care with your legal commitments around consumer rights and beware the temptation of offering credits instead of refunds.

The background

The CMA launched an enforcement investigation into Groupon UK in April 2021 regarding suspected breaches of consumer Law. Groupon had given undertakings in 2012 to change its practices but the CMA became concerned about whether these undertakings were still being complied with.

In 2012 Groupon UK gave undertakings to the CMA's predecessor, the Office of Fair Trading (**OFT**), to change certain practices that were unfair or misleading to customers. However, the CMA became concerned whether those undertakings were being complied with. Under the April 2021 investigation it is looking into whether Groupon UK is:

- providing refunds to consumers in accordance with consumer protection laws, and
- ensuring that descriptions of items or services on its website are accurate and that products are delivered within the advertised timeframes.

The CMA sought information from Groupon UK to assess whether their business practices breach consumer laws and subsequently assess whether further action is required. In August 2021, the CMA wrote to Groupon outlining its specific concerns resulting from the investigation.

The development

The CMA found evidence that Groupon does not always provide customers with refunds or other forms of redress to which the CMA considers consumers are legally entitled to. In many cases customers were provided with Groupon credits instead of refunds.

The CMA also raised concerns that Groupon fails to ensure that i) consumers can redeem purchased vouchers within the advertised periods; ii) description of goods and service are accurate; iii) products are in stock and delivered within the advertised timeframes; iv) items are of satisfactory quality; and v) customer service is satisfactory when contacting Groupon about problems.

The CMA has given Groupon an opportunity to respond and make further undertakings.

Why is this important?

The CMA actively seeks to ensure compliance with consumer protection regulation and will ensure that breaches are taken seriously. This includes the threat of court action where necessary.

Any practical tips?

Online marketplaces inevitably advertise a whole range of different products and services, which can throw up challenges with consumer protection compliance. Ensuring the teams on the ground know how to describe the offers accurately, and how to deal fairly with disgruntled customers, is a key part of any internal compliance programme.

Autumn 2021

Consumer

CTSI publishes guide on vulnerable consumers

The question

Will the UK Government bring in more robust legislation to protect vulnerable consumers?

The key takeaway

Businesses should constantly assess how well they are dealing with vulnerable consumers and consider whether they have sufficient protection measures in place. The new guidance seeks to help with identifying, and meeting the needs of, these vulnerable consumers in a fair way.

The background

The Chartered Trading Standards Institute (**CTSI**), in conjunction with the Department for Business, Energy and Industrial Strategy (**BEIS**), has produced new guidance - framed as a consultation paper - on how businesses should identify and deal with vulnerable consumers, to ensure that they are treated fairly. The CTSI represents trading standards professionals and seeks to influence Government policy on trading standards. The protection of vulnerable consumers was previously identified in 2018 by the Department for BEIS as an area where the law needed to improve and, in its July 2021 consultation on reforming consumer law, the Government cited improved protection of vulnerable consumers as one of its aims. It appears that this area of law is likely to face change soon.

The development

The guidance adopts a broad definition of vulnerability, describing it in the consultation as depending on the consumer's situation (eg if they are in financial difficulty, suffering a bereavement, or in ill health), or in the market context (eg if they are making a decision based on incomplete information, or they are unfamiliar with the market).

This definition of vulnerability encompasses a lot of people; for example, one-in-six adults in the UK is estimated to have a mental health condition. Furthermore, the impact of the pandemic is likely to mean that the numbers of those in financial difficulty or suffering from a mental health problem (and who therefore may be vulnerable) will have increased, meaning that businesses may have to deal with many more vulnerable consumers.

The guidance proposes methods by which businesses can identify vulnerable consumers and adapt in order to properly support them. The guidance proposes a variety of steps that can be taken in order to deal with vulnerable consumers, including the following:

- considering communication preferences
- not making assumptions about the consumer
- asking how they can better assist the consumer, and
- ensuring that any agreement or decisions are explained in plain English.

Why is this important?

The guidance is in the form of a consultation paper, produced by an organisation that is seeking to influence Government policy. Accordingly, businesses should ensure they have their say on what should be included within the guidance for dealing with vulnerable consumers.

Any practical tips?

The CTSI advises businesses to consider "REAL", namely:

- retain – can the consumer retain what they are being told?
- explain – can the consumer explain what they've been told?
- able – are they able to understand what they're being told? and
- listen – have they listened properly, or are they just repeating what you've told them?

Companies should consider adapting their customer service model to ensure that staff are able to identify and properly assist vulnerable consumers.

The CTSI also recommends that vulnerable consumers' needs are considered at every stage of the development of products and services, and that consumers' different needs regarding communication should be considered (eg someone with anxiety is likely to prefer electronic communication, whereas an older person might prefer a phone call or face-to-face meeting). They also recommend that staff should be trained on the extent to which vulnerability exists in the business' target market. Furthermore, they recommend that businesses have a vulnerable consumers policy which sets out how staff are expected to deal with vulnerable consumers.

Autumn 2021

Consumer

Government consults on reforms to consumer protection law

The question

What are the key proposals set out in the BEIS consultation paper for the reform of UK consumer protection regulation?

The key takeaway

The proposals make it clear that the Government is prepared to strengthen the existing powers of the Competition and Markets Authority (**CMA**) and empowering consumers to enforce their own rights through alternative dispute resolution without resort to the courts. Such substantive changes are facilitated in part by the UK's withdrawal from the European Union, prior to which the consumer law regime was harmonised between EU Member States.

The background

Reform of certain aspects of consumer law, focusing on protecting consumers online and improving enforcement, has been anticipated for several years. Following numerous papers, reports and consultations, on 20 July 2021 the Department of Business, Energy and Industrial Strategy (**BEIS**) published a consultation entitled "Reforming Competition and Consumer Policy" (the **Consultation**).

The development

The Consultation proposes a number of reforms regarding consumer law and policy, including:

Substantive consumer law

- Subscription contracts
  - The Government proposes several reforms in this area. Notably companies will need to be obliged to make consumers aware in plain English of all necessary subscription information at: (i) an early stage in the subscription process; and (ii) immediately before placing their order.
  - The subscription information will need to include: (i) the order or agreement is for a subscription and not a one-off purchase; (ii) information explaining the minimum contract term and price per billing period; and (iii) any auto-renew/auto-extend provisions and the minimum notice period for cancellation.

- Fake reviews
  - Whilst the consultation notes that there is a growing industry of using fake reviews to mislead consumers, it is noted that reviews by experts or online influencers will not be

fake provided they reflect the genuine experience or opinion of the expert or influencer.

- Preventing online exploitation of consumer behaviour (targeted advertising)
  - Although there is evidence of harm from online exploitation of consumer behaviour, including from the Government's Behavioural Insights Team, the consultation proposes that substantive research should be conducted which sets such practices into the wider context of markets, for example exploring the influence of major players and commerce platforms.

- Reducing red tape while maintaining consumer protection
  - The consultation invites views on how it can simplify or clarify consumer law to reduce uncertainty and legal costs for businesses and consumers.

- Strengthening pre-payment protections for consumers
  - The consultation seeks views on amendments in order to protect consumers from the risks of using savings clubs and generally with regard to pre-payment for goods in general.

Enforcement powers

- The consultation seeks to improve the current enforcement powers of the CMA and introduces a proposal for an administrative enforcement regime. The CMA would be able to impose fines on firms of up to 10% of global turnover.
- Supporting consumer's right to enforce their own rights through ADR.
- Collective redress regimes, which would allow the CMA and other enforcement bodies to take action on behalf of consumers.
- Looking at how National Trading Standards can assist Local Trading Standards to enforce consumer law.
- What improvements can be made in terms of guidance to businesses, in order that they can better comply with consumer law.

Why is this important?

While reform to the consumer protection regime has been anticipated for a number of years, the growth in e-commerce has accelerated the need for reform in a number of respects. If put into action, the reforms would alleviate concerns surrounding the CMA's perceived lack of "bite" as highlighted by the Penrose Report and comments of Lord Tyrie (former Chairman of the CMA).

Any practical tips?

Although the reforms are currently housed within a consultation, companies should carefully consider the ramifications of the enhanced enforcement powers of the CMA and begin to think

about adapting policies and internal training in order to prepare for any change to consumer protection law.

Autumn 2021

Consumer

UK Government extends deadline to cease using CE marking until 2023

The question

Why has the UK Government extended the deadline for use of the CE product marking for manufactured goods placed on the market in Great Britain to 1 January 2023?

The key takeaway

On 24 August 2021, the Government announced a one-year extension to the deadline for businesses to transition from using the CE product mark to the new UK Conformity Assessed (**UKCA**) marking. Subject to certain conditions relating to the ongoing use of the CE mark (see below), this mark can continue to be used for products until **1 January 2023**. This doesn't mean that businesses shouldn't start to transition to the new marking as soon as possible to ensure that they are compliant with the new UK regulatory framework.

The background

The UKCA marking will replace EU labelling such as the CE mark, which is currently applied to goods on a self-declaration basis. The CE marking is a manufacturer's claim that its product meets all the specified essential safety requirements set out in certain EU directives. Relevant categories of product must bear the CE marking if they are put on the market in the EU (or EEA).

However, from 1 January 2021, the UKCA marking has been the conformity assessment marking for goods placed on the market in Great Britain. UKCA marking will allow the UK to have a higher level of control over the regulation and product safety of manufactured goods placed on the market in Great Britain.

The development

To give manufacturers time to adjust, the Government initially stated that manufacturers could continue to use the CE marking until 1 January 2022, when placing goods on the market in Great Britain (subject to certain conditions). However, as a result of increasing industry pressure, the Government provided a concession to extend the deadline.

The CE marking may only continue to be used by businesses during this period if any of the following apply:

- the CE marking is currently applied to the goods on a self-declaration basis

- any mandatory third-party conformity assessment was carried out by an EU-recognised notified body (including a body in a country with which the EU has a relevant mutual recognition agreement)
- prior to 1 January 2021, the certificate of conformity previously held by a UK approved body has been transferred to an EU-recognised notified body.

Why is this important?

Businesses will now have more time to apply the new UKCA markings for most products placed on the market in England, Scotland and Wales. From 1 January 2023, the UKCA marking will need to be used when placing goods on the UK market (unless there is a further extension).

However, Northern Ireland will continue to recognise the CE marking for goods placed on the market in Northern Ireland and businesses will need to use the UKNI marking if they use a UKCA body to test their products.

Any practical tips?

Since 1 January 2021, the UKCA mark has been permitted as a valid conformity mark in Great Britain. We recommend that businesses align themselves with the new marking sooner rather than later to ensure product compliance within your organisation and/or supply chain.

Autumn 2021

Advertising

CAP publishes guidance on depicting mental health conditions

The question

What steps must advertisers take in order to ensure that any depiction of mental illness is not socially irresponsible or offensive?

The key takeaway

CAP has published new guidance with a focus on mental health issues, including addiction, triggering/harmful images, medical claims, and suicide.

The background

On 15 July 2021, CAP published a series of new advice notes in order to help advertisers ensure their ads are respectful of peoples mental and emotional wellbeing. The aim of the guidance is to ensure that every UK ad is responsible when it comes to issues regarding mental health.

The development

The advice published focused on the depiction of metal health in the context of a number of specific areas. The advice states that ads that refer to mental illness must not be socially irresponsible or offensive. It is important to note that this is not limited at insensitivity toward mental health, but also glamorising mental health conditions. Specifically, the guidance offers advice on a range of mental health issues, including how advertisers can properly depict or reference the following themes:

- Addiction: The advice notes that there are already specific rules regarding alcohol and gambling. The rules require that such ads must not show irresponsible use of the products or behaviours that may trigger addition.
- Stereotyping of mental health: The ASA notes that many stereotypes of mental health are harmful and offensive. Portraying those with mental health conditions as dangerous, violent or otherwise unpleasant will not be acceptable.
- Triggering/harmful images: The advice notes that there must be a strong justification to include harmful images (such as an awareness campaign). The context of the ad is going to be key here, for example a trailer for a horror film that is not overly threatening is likely to be acceptable. However, unnecessary or out of context usage of threatening imagery or depictions/references to self-harm or suicide will not be permitted.

- Medical claims: There are already strict rules on medical claims and any claim in this space must be able to be substantiated. The advice reminds advertisers that some medical conditions are so serious that they can only be diagnosed, treated or advised on by a qualified medical professional.
- Suicide: The advice notes that extreme care must be taken with ads that contain references to Suicide. Unless there is a strong justification for its inclusion the inclusion of suicidal imagery or the trivialisation/glamorisation of suicide in an ad are very likely to cause serious harm. Sensitive references aimed at promoting awareness of charities may be acceptable.

In addition to the above, the issue of body image and the potential harm that can be caused in relation to body image will potentially have new specific restrictions as CAP and BCAP are also currently considering whether "*specific restrictions should be introduced to mitigate any harms that are not already and adequately addressed by current rules*".

Why is this important?

Mental health is at the forefront of societal importance. Consumers care if advertisements are not responsible and will not hesitate to complain if they take issue with what is being depicted.

Any practical tips?

Extreme care must be taken when depicting any scenes or images which involve scenarios relating to mental health conditions. Not all of these are obvious - for example, gaming ads showing forms of addition may fall into this category (eg which depict certain types of obsessive behaviour). And it is quite easy to see why the presentation of body images and even the use of social media filters may well become the next area of regulatory focus, given the potentially damaging impact this may have on consumers' mental health.

Autumn 2021

Advertising

CAP and BCAP announce progress with gambling ad consultation

The question

What updates have arisen as a result of CAP and BCAP's consultation responding to the findings of the GambleAware Final Synthesis Report?

The key takeaway

CAP and BCAP are working hard to ensure that the most vulnerable members of society are protected from the potential dangers of gambling.

The background

On 6 August 2021, CAP and BCAP published an interim statement that details the progress that has been made on their joint consultation (launched 22 October 2020) that responded to the findings of the GambleAware Final Synthesis Report. The consultation outlined proposals to strengthen rules and guidance around gambling adverts in an effort to further protect vulnerable consumers (under 18's and vulnerable adults). The consultation proposed the following changes/updates:

- the introduction of new rules that would aim to stop the ads being of strong appeal to under 18's. This means that gambling ads cannot feature a person or character likely have a strong appeal to under 18's (this would include sports people, influencers and celebrities). "Strong appeal" would be defined in the same way as it is for the CAP and BCAP rules on advertising alcohol
- updating current guidance in order to prohibit presenting gambling as a way to be part of a community, that it is skill based or implying that certain offers can create security for the consumer
- proposals for potential new restrictions on placement and targeting of gambling ads, and
- technical updates to the advertising codes which would change the introductory/clarifying parts of the sections of the code relating to gambling to ensure that they are up to date with the underlying legal framework.

The development

The interim statement highlights that there was a significant amount of responses to the consultation, particularly in relation to the introduction of a "strong appeal" rule. Specifically, the responses concerned how a "strong" appeal-based rule to restrict the appeal of gambling

advertising to under 18's would actually work in practice. CAP and BCAP are still in the process of considering these responses and have committed to responding fully by the end of 2021.

However, in the interim statement, CAP and BCAP indicated that they are going to move forward with the implementation of revisions to guidance as well as the proposed technical update to the codes based on the responses and outcomes of the consultation. These are:

- CAP's guidance on gambling advertising: responsibility and problem gambling, has been updated in line with the consultation's proposals. The new guidance will be effective from 1 November 2021
- the amendments are designed to protect vulnerable adults, by prohibiting the use of humour or light-heartedness to downplay the risks of gambling or presenting free bets as adding an element of security or reducing risk. Furthermore, the guidance prohibits unrealistic portrayals of winners and the presentation of gambling as a way to be part of a community based or presenting gambling as skill based, and
- the introductory sections to both the BCAP and CAP Codes will be updated in line with the consultation's proposals, to ensure they are more easily understood and reflect the underlying legal framework for gambling. As the changes do not change advertising policy, they will be effective immediately.

Why is this important?

These development's highlights CAP's ongoing commitment to social responsibility within the gambling arena.

Any practical tips?

The updates mean that advertisers will need to adjust their methodology when it comes to gambling ads so that they are not caught out by any changes to the advertising codes. Big gaming brands in particular will need to keep a close eye on future developments, such as the potential for restrictions on ads with "strong appeal" to under 18's. The latter could have significant and far reaching consequences for gaming operators and their sponsors.

Autumn 2021

Advertising

CAP publishes guidance on country of origin claims

The question

What do companies need to be mindful of when it comes to country of origin claims?

The key takeaway

It is important to be clear and upfront with consumers regarding the country of origin of products. Misusing British imagery or misleading as to UK company status will get unfavourable attention from the ASA.

The background

Following the UK's withdrawal from the European Union, there has been an uptick in British consumers looking to support the UK economy by purchasing products manufactured in the UK from British based companies. The onus is very much on the brand to ensure that the consumer is properly informed about the country of origin and that advertisements properly comply with the advertising codes.

The development

In September 2021, CAP produced three key pieces of guidance for companies to assist with country of origin claims. The guidance is as follows:

- companies should not hold themselves out as a UK company if this is not the case. While there is nothing wrong with companies using a .co.uk domain name or presenting prices in GBP if they are not based in the UK, they must ensure that material information with regards to the geographical location of the company is made clear. Furthermore, caution should be taken not to present a company as being entirely UK based in situations where a company is UK registered but the processing of orders/shipping of orders occurs from outside the UK. Finally, and quite obviously, care should be taken to ensure that consumers are not misled regarding the origin of a product. Phrases such as made in Britain, grown in Britain, built in Britain should not be used if this is not the case
- careful use of national flags and emblems is encouraged. Marketers may use national flags and emblems in marketing communications, provided that in doing so consumers are not misled about a products country of origin
- ensure you have the requisite permissions before using Royal Arms and Emblems. Rule 3.52 highlights that marketers that want to use Royal Arms or Emblems must not do so without permission from the Lord Chamberlain's Office. Any feature of the Royal Arms or

Emblems is likely to strongly imply an official endorsement and so marketers should ensure that they have the requisite permissions before including such marks.

Why is this important?

This advice clarifies the rules regarding country of origin claims and reinforces what will be seen as non-compliant. With companies looking to capitalise on a wave of support for British products, now is the time to ensure that the marketing teams don't get a little loose in making more of a "British" connection than is actually there.

Any practical tips?

Companies should ensure that they are upfront with consumers about the country of origin of their products and from where products are being shipped. This is not to say that marketers cannot be creative in their use of British themes, however this needs to be done in a way that ensures that consumers are fully aware of where the product originated.

Autumn 2021

Advertising

Prize promotions need prizes!

The question

If you are an influencer running a competition, how careful do you need to be when establishing entry criteria and awarding prizes?

The key takeaway

Ignorance of the rules governing promotions is no excuse. Just because an influencer is an individual doesn't mean that they do not have to be mindful of the relevant rules and regulations. Additionally, careful thought and specificity of entry requirements (eg *must be a follower of the account at the time of the prize draw on X date*) is very important and applicable to all competitions regardless of size.

The ad

An Instagram post from influencer Briley Powell featured the text "£250 PLT VOUCHER! PLUS Filter by Molly-Mae Tanning Kit Beauty Works Professional Styler The White Company Seychelles Set @BRILEYPOWELL". Below that, the post went onto to state "WIN £250 TO SPEND ON PRETTY LITTLE THING + THIS BUNDLE Give away includes £250 PLT Voucher Filter by Molly-Mae FULL tanning kit Beauty Works Professional Styler The White Company Seychelles Set OPEN INTERNATIONALLY TO WIN: Like this post Tag your bestie Share to your story (tag me) Both must be following @brileypowell Unlimited entries! The more you enter = the more chances of winning Winner announced on VALENTINE'S DAY (A MONTH TODAY) I had planned this giveaway to celebrate reaching 25K which seems a lifetime away so thought why not treat a lucky lady (or lad?!) for vday instead! GOOD LUCK ALLLL"

The CAP code provides that "*Promoters must award the prizes as described in their marketing communications or reasonable equivalents, normally within 30 days*" (rule 15.1) and that "*withholding prizes is justified only if participants have no met the qualifying criteria set out clearly in the rules of the promotion*" (rule 8.27).

The complaint

Following the close of the competition, the ASA received a complaint from an entrant of Ms Powell's competition who had been notified that they had won the prize drawn but had not received the prizes. Ms Powell said she was not aware of the requirements associated with running a giveaway and had only done so to thank her followers for their support. She stated that she posted the other prizes (except the voucher) but did not have tracking information. She further argued that the complainant had breached the rules of the giveaway by not being

a follower which was a condition of entry and claimed that the complainant used spam accounts to find and participate in competitions and therefore withheld the voucher.

The development

The CAP code states that promoters are required to award the prizes as described in their marketing communications within 30 days. While the ad did specify how to enter and when the winner would be drawn, it did not state by which date the prizes would be awarded, which means in any case they should have been awarded within 30 days of the closing date of the competition. The ASA noted that while Ms Powell did send 3 of the prizes, it was her responsibility to ensure there was sufficient procedures in place to be able to show that the prizes had been sent. Furthermore, the code sets out that prizes may be withheld if a participant had not met the criteria set out in the rules of the promotion. Ms Powell stated that she withheld the voucher described in the post because the winner had not followed the Instagram page @brileypowell which was a requirement of the prize draw. However, Ms Powell was unable to explain how the complainant had been selected as the winner if they had not complied with the entry criteria.

The ASA understood the prize winner could have been following the Instagram page at the time of the prize draw entry and winner selection but have unfollowed the page by the time Ms Powell reviewed the entry. However, there was no requirement that entrants had to continue following the social media page after the competition closing date. The ASA therefore considered that Ms Powell had not demonstrated that the winner had not complied with the prize draw entry requirements and that there was a justifiable reason for withholding one of the prizes. Consequently, the ASA upheld the complaint and found that there was no evidence the prizes had been awarded nor that there was a justifiable reason to withhold a prize.

Why is this important?

This ruling confirms the ASA's zero tolerance approach to letting influencers off the hook, simply because they are often individuals. It also shows the importance of ensuring clear and specific entry requirements as well as ensuring that prizes are sent out in a secure manner. This case not only shows the importance of adherence of the advertising rule for influencers, but also serves as a reminder of the need to ensure compliance for the brands who work with them.

Any practical tips?

When working with influencers, particularly when arranging a product giveaway or similar promotion, it is important to ensure that the influencer fully understands the rules in place to ensure that any promotion is run in accordance with the CAP Code and that there is an adequate level of supervision. A lack of knowledge or ignorance of the rules is no excuse.

Autumn 2021

Advertising

Consumer surveys and Vodafone's "The UK's best…" claim

The question

Can you use consumer surveys to support marketing phrases such as "*The UK's Best…*", when advertising your product or service?

The key takeaway

It is possible to use consumer surveys as the basis for your claims, but you must be very careful around the presentation of those claims. You must also ensure that the basis of the survey itself can support the claim. Here the ASA determined that the subjective nature of the user survey in question meant that it could not be used as substantiation for a comparative claim which included an objective component.

The ad

In the context of the mobile phone industry, January 2021 saw Vodafone present itself as being "*The UK's best Network*" in a paid-for internet search ad. Prior to this, in March 2020 on their website and in a press ad, Vodafone claimed they were awarded, "*the UK's best mobile data network*" alongside an image of a gold medal with the claim "*No. 1 Mobile Network Performance. Nperf. 2019*". The press ad went further to encourage consumers to "*Switch to 5G. On the "UK's best mobile data network*".

The complaint and the response

Vodafone's competitor EE challenged whether the claims relating being the "UK's best…," were misleading, capable of substantiation and verifiable.

Vodafone said that the claim would usually read "*The UK's Best Network as voted by readers of Trusted Reviews*", but it had appeared as just "*The UK's Best Network*" due to a technical error. They had also removed the claim on learning of the complaint. The Trusted Reviews award was made following a poll-based survey where users were asked which network they deemed to be the best. Vodafone received 59.88% of the votes in relation to this specific category. Vodafone went onto the further state that the Trusted Reviews award was based on readers' subjective overall preference of a network, which they believed was made clear on the "Networks" page of Vodafone's website. They believed the complete wording of the claim also made it clear to consumers that the claim was based on consumers' subjective views.

The adjudication

1. Vodafone's March 2020 claim of being "*UK's best mobile data network*" was based on third-party testing data conducted by nPerf. This concerned the ASA who noted that testing participants *were "self-selected"* from a sample generally and not representative of the UK overall. As consumers were likely to view this reference to nPerf as a technical reference based on robust testing of mobile data networks, this was considered misleading by the ASA. This, coupled with lack of signposted specific information available to consumers regarding the testing methodology, led the ASA concluding the ad unverifiable and therefore in breach of CAP Code 3.35.
2. Vodafone's January 2021 internet ad claim of being "*the UK's best network*" highlighted the perils of trying to rely on subjective user reviews when substantiating comparative claims. Vodafone admitted that they omitted the phrase "*as voted by readers of Trusted Reviews*" in error. The ASA analysed the user review process itself and found it to be overly subjective for the claim Vodafone had made, not least as the comparative nature of the claim required an objective component. It was unclear to the ASA how subjective preference alone would deliver such data.

Ironically, in the lead up to the ASA ban of Vodafone's adverts, Three UK (the complainant) had also faced bans for similarly bold statements after a complaint by Vodafone. Digital data providers will continue to face the hurdle of substantiating bold ad claims in the wake of rapid digital developments cutting across all providers.

Why is this important?

The ruling underlines the need for care in using consumer surveys to substantiate claims which require objective substantiation. It is the latest in a string of cases where mobile operators go back and forth with each other to get ads with bold claims pulled down by the ASA. This case was widely publicised and is a timely reminder of the impact of ASA adjudications on brand reputation.

Any practical tips?

Remember that any claims of being "the best" will be considered a claim against the whole market and will require significant objective substantiation. You also need to make it easy for consumers to see the information that verifies comparisons with competitors. If you are seeking to rely on a consumer survey in support of a claim, it's important to get into the detail of the survey to ensure it is capable of withstanding a level of objective (rather than purely subjective) interrogation. Put another way, check out the basis of the survey itself and ensure that it is robust enough to support the claim you are seeking to make.

Autumn 2021