RPC

Commercial law snapshots

Google Training - Summer 2021

ADVISORY | DISPUTES | REGULATORY | TRANSACTIONS

Contents

Commercial

Court of Appeal holds that notice of tax covenant claim is valid, despite lack of detail

Dodika Ltd and others v United Luck Group Holdings Ltd [2021] EWCA Civ 638

The question

Was the notice of a potential claim invalid because it failed to provide "*reasonable detail*"?

The key takeaway

Whilst notice clauses in contracts are intended to provide sufficient information to the recipient, adhering to notice requirements should not result in "empty formalism". The Court should be slow to conclude that a notice is invalid if it does not spell out what was already known to the recipient and what constituted "reasonable detail" depends on the background context, including the recipient's knowledge.

The background

Under a sale and purchase agreement (**SPA**), United Luck Group Holdings (**ULG**) was the buyer of the issued share capital of an English company, Outfit7 Investments Ltd. Dodika Ltd (**Dodika**) was one of the sellers and warrantors.

Under the SPA, Dodika gave ULG a tax covenant, under which it agreed to pay an amount equal to any potential tax liability of a group company arising out of post-completion matters. To claim under the tax covenant, ULG had to give written notice to Dodika by 1 July 2019 stating, "*in reasonable detail*" various things such as "*the matter which gives rise to such a Claim*".

ULG gave notice to Dodika via its solicitors on 24 June 2019 (the **Notice**), referring to a Slovenian tax investigation into a group company's transfer pricing practices which launched in July 2018.

Dodika argued that the Notice was invalid as it failed to state the matter giving rise to the claim and the amount claimed in reasonable detail. At first instance, the High Court agreed that the Notice did not comply with the SPA requirements. ULG appealed the decision.

The decision

(i) What was the "matter" giving rise to the Claim?

The Court of Appeal agreed with the judge that the *"matter"* giving rise to the claim was based on the factual reasons why a tax liability had, or may have, accrued pre-completion, rather than the existence of the tax investigation itself.

(ii) Did the Notice state the matter *"in reasonable detail"*?

However, despite the decision on (i) above, the Court of Appeal held that the Notice did state the matter in reasonable detail. The SPA did not specify exactly what information the Notice must contain and the requirement for *"reasonable detail"* was dependant on all circumstances, including the recipient's knowledge. Dodika were assumed to know the reasons why the Slovenian tax authority thought that the transfer pricing may be too low, and the Notice did not need to contain more detail than it did. The additional detail sought by Dodika was of a generic and limited nature and already known to them.

Why is this important?

If a contract prescribes that certain information must be included in a notice, failure to include that information will result in the notice being invalid and it is no answer to say that the recipient already knew it. However, where the contract does not specify precisely what is required (as was the case here), the Court will be reluctant to conclude that a notice is invalid if it does not spell out what was already known to the recipient.

Any practical tips?

When drafting notice provisions, ensure that they are workable and ideally specify what must be included. Where notice provisions are less specific, the level of information to be provided in the notice will depend on the circumstances.

When drafting a notice, ensure that all the requirements are fully satisfied – if something is expressly prescribed, it must be included. Doublecheck timing, content and service of the notice. And do not leave notices until the final deadline – allowing time for any issues to be remedied if necessary.

Summer 2021

Commercial

Courts reluctant to interpret standard entire agreement clauses to exclude misrepresentation claims

MDW Holdings Ltd v Norvill & Ors [2021] EWHC 1135 (Ch)

The question

Will a standard entire agreement clause protect a seller from liability for misrepresentation?

The key takeaway

The Courts are reluctant to interpret standard entire agreement clauses as excluding liability for pre-contractual misrepresentation.

The background

GD Environmental Services Ltd (**GDE**) operated a waste management business, processing various wet and dry waste including cess waste and leachate. These activities were subject to applicable regulations and environmental permits. GDE did not have active facilities to treat wet waste so it was taken to Dwr Cymru Welsh Water's (**DCWW**) treatment works for processing.

Between 2013 and 2015, samples gathered by both GDE and DCWW revealed that the leachate discharged exceeded prescribed limits. Despite DCWW providing GDE with an improvement plan in May 2015, further samples still contained restricted contaminants. GDE requested an increase in contaminant limits, although it was not approved by DCWW.

In 2015, the Buyer (**MDW**) agreed to purchase the share capital of GDE from the Sellers. Before entering the SPA, MDW submitted a legal due diligence request, including various environmental questions. The Sellers' response stated that there were no outstanding investigations/enforcement actions and said nothing about ongoing breaches.

The SPA was signed on 14 October 2015 and included general and detailed warranties relating to GDE's environmental permits and compliance records. The warranties were subject to contractual limitations on the Sellers' liability, including a provision excluding warranty claims unless written notice was given within two years of completion. Clause 7.7 stated that nothing would exclude the Sellers' liability for claims arising from dishonesty, fraud, wilful misconduct or wilful concealment. The SPA also contained a standard entire agreement clause.

In August 2017, the Buyer notified the Sellers of its claims under the SPA regarding trade effluent consent breaches which the Sellers had failed to disclose. The Buyer wrote to the

Sellers again in October 2017 indicating that the claimed amount was in excess of £1m. A letter of claim followed on 17 January 2019, seeking damages for breach of warranties and for pre-contractual misrepresentation.

The Sellers argued several contractual defences, including that the warranty claims were barred by limitation because the Buyer had not initially summarised the amount claimed, and that the entire agreement clause extinguished all prior representations.

The decision

The court rejected the Sellers' arguments and ruled in favour of the Buyer. The notification limitation in the SPA set a low threshold and the Buyer had provided a summary of its claim so far as was reasonably practicable at that time. In any event, clause 7.7 allowed the Buyer to pursue its breach of warranty claims regardless of notice limitation, as breaches of warranty had occurred as a result of wilful misconduct on the part of those controlling and running GDE.

Having found in favour of the Buyer regarding its primary warranty breach claim, the Court went on to consider misrepresentation. It found that the purpose of the entire agreement clause was to make it clear that nothing said, written or done prior to the SPA created any contractual liabilities. Nothing in the SPA stated that there had been no reliance on a representation or that liability for representation was excluded. The statements made by the Sellers were actionable misrepresentations and had induced the Buyer to enter the SPA.

Why is this important?

The courts have again rejected the argument that a standard entire agreement clause excludes a party's liability for misrepresentation.

Any practical tips?

If you wish to exclude liability for pre-contractual misrepresentations, you should include additional contractual wording. This might include statements concerning:

- non-reliance (a party has not relied on any representations in entering an agreement)
- non-representation (a party has not made representations leading up to the agreement)
- express exclusion of liability for misrepresentation (regarding pre-contractual statements)
- an express waiver of non-contractual remedies.

Note that such exclusions will not be effective for fraud/fraudulent misrepresentation, and such exclusions are also subject to the reasonableness requirement under s. 3 Misrepresentation Act 1967/Unfair Contract Terms Act 1977.

Summer 2021

Commercial

Standard exclusion clauses and liability caps interpreted without presumption even for fundamental or deliberate breach

Mott Macdonald Ltd v Trant Engineering Ltd [2021] EWHC 754 (TCC)

The question

Do special rules of interpretation apply to clauses excluding or limiting liability where there has been a deliberate and repudiatory breach of contract?

The key takeaway

The correct approach to determining a clause seeking to exclude liability is "*simply one of construing the clause, albeit strictly, but without any presumption".* If an exclusion clause is sufficiently clear, it will apply to deliberate or fundamental breaches even if that appears unfair or unreasonable. If the parties intended to exclude "*fundamental, deliberate and wilful*" breaches of contract, clear contractual wording was required.

The background

Trant Engineering Limited (**Trant**) engaged Mott MacDonald (**Mott**) to provide engineering consultancy design services to Trant for works to upgrade an RAF military base in the Falklands for the Ministry of Defence (**MoD**).

A dispute then arose regarding the scope and value of work to be provided by Mott and, in 2017, the parties entered into a Settlement and Services Agreement (**SSA**) to resolve the dispute and govern the services to be provided by Mott. As well as terminating the proceedings by way of a consent order, the SSA contained three clauses which limited Mott's liability in the event of a breach: (i) a liability cap limiting Mott's liability to £500,000; (ii) an exclusion clause; and (iii) a net contribution clause.

Another dispute arose when Mott revoked the passwords given to Trant to access the modelling database, preventing Trant from accessing the design data. Trant then failed to make certain payments and Mott issued proceedings for payments due of c. £1.6m.

Trant counterclaimed for £5m for the cost of redoing the work required and reflecting the possible sums payable to the MoD as a result of Mott's breaches. Trant argued that Mott had "*fundamentally, deliberately and wilfully"* breached the SSA in refusing to complete the design

deliverables required; provide native data files or calculations; or carry out independent reviews of its designs, in order to pressurise Trant to pay sums that they claimed were not due to Mott.

Mott denied the breaches and sought to rely on the SSA's exclusion and limitation clauses. Trant argued that express language was required to limit liability in the event of "*fundamental, deliberate or wilful*" breach.

The decision

Exemption clauses, including those purporting to exclude or limit liability for deliberate and repudiatory breaches, were to be construed by reference to the unambiguous language used by the parties and the normal principles of contract construction, to give effect to the parties' intention. There was no presumption against the exclusion of liability and no particular form of words was required to achieve the effect of excluding liability.

Although the exclusion was potentially wide-ranging in its effect, it did not preclude all of Mott's liability or reduce Mott's obligations to a "*mere declaration of intent".* A breach still had adverse consequences for Mott.

If an exclusion clause is sufficiently clear, it will apply to deliberate or fundamental breaches even if that appears unfair or unreasonable. If the parties intended to exclude "*fundamental, deliberate and wilful*" breaches of contract, clear contractual wording was required. The court was not responsible for rescuing Trant from a bad bargain.

Why is this important?

This judgment makes it clear that that exclusion and limitation clauses will be construed by the Court by reference to normal principles of contractual construction, regardless of whether there has been a deliberate or wilful breach.

Any practical tips?

If it is intended that a party in breach should not benefit from limitation or exclusion clauses in particular circumstances, eg in the event that the breach is deliberate or wilful, this must be clearly stated in the contract.

These carve outs can be particularly important for long-term or high value contracts where a party might otherwise consider it commercially beneficial to simply walk away and pay (capped) damages, instead of continuing to perform the contract.

Summer 2021

Commercial

High Court denies applicability of an exclusion clause due to convoluted terms and conditions

Green v Petfre (Gibraltar) Ltd (t/a Betfred) [2021] EWHC 842 (QB)

The question

In what circumstances will website terms and conditions effectively exclude liability?

The key takeaway

Those providing online services to consumers are not precluded from the possibility of excluding liability, provided that the exclusions are clearly drafted, transparent, fair and adequately signposted.

The background

Mr Green had been a Betfred customer since around 2006 or 2007. Having played Blackjack on an online platform hosted by Betfred for several hours, Mr Green's total winnings were shown as £1,722,500.24. When he tried to withdraw them several days later, Betfred stated that due to a "glitch" (in this case, an undiscovered fault where much better odds were applied for continuous play), he could not be paid out.

Mr Green issued a claim for his winnings by way of summary judgment, arguing that Betfred had breached its promise that customers could withdraw funds at any time from their account so long as all payments had been confirmed. In its defence, Betfred argued that the applicable contract terms excluded them from liability to pay Mr Green's winnings in these circumstances, relying on exclusions for errors or malfunctions set out in the relevant website terms and conditions (**T&Cs**), the End User Licence Agreement (**EULA**) and the individual game rules.

The decision

The Court granted Mr Green's application and rejected Betfred's submission that the case was unsuitable for summary judgment. The case involved the resolution of short points of contractual construction. English common law of contract is founded on principles of offer, acceptance, intention to create legal relations, consideration and certainty. Website contracts fall squarely within these principles.

The Court found that the exclusion clauses that Betfred sought to rely on did not cover the circumstances of this case. Further, the clauses were opaque and difficult, making them unclear to the average and informed consumer and therefore unenforceable. In particular:

- the relevant clauses of the T&Cs did not cover a failure to pay out winnings at all, nor did it deal with errors or glitches in the system that were undetectable to either party
- the exclusion clause contained in the EULA sought to avoid liability for obvious failures of connection but made no reference to the voiding of a bet or non-payment of winnings in these circumstances, and
- the EULA was long, complex, repetitive and obscure and had the appearance of a standard form software licence agreement (which was not a natural place to determine the rights and obligations of parties to a gaming contract). The layout and terminology used (including typographical errors and absent or inconsistent numbering) also made it unclear as to what a player was obliged to agree to, or where to find it.

Regardless of their true meaning, none of the terms relied upon by Betfred to exclude liability were sufficiently brought to Mr Green's attention to be incorporated into the gaming contracts he entered. Instead, the relevant clauses were buried amongst other materials, making it unlikely that Mr Green would have been able to easily spot the key terms before agreeing to them. Betfred's failure to signpost the exclusion clauses and explain their consequences to Mr Green was inconsistent with the fairness envisaged by the Consumer Rights Act 2015.

Why is this important?

This decision reiterates the need for clear and unambiguous terms and conditions at the outset, particularly for consumer contracts. It does not preclude the possibility for online providers to exclude liability, if exclusions (and the T&Cs in general) are clearly drafted and adequately signposted.

Any practical tips?

All online service providers should ensure their terms and conditions are clearly and carefully drafted, so that they are easy to follow, onerous provisions are highlighted/brought the counterparty's attention, and (for consumer contracts) that they comply with applicable consumer legislation.

There are many practical solutions, but the judge suggested that it may be prudent to include a full "click and scroll" mechanism before a website user makes a contract via the platform.

Summer 2021

Commercial

Terms implied into a break right limited the capability to exercise the right

Wigan Borough Council v Scullindale Global Ltd and others [2021] EWHC 779 (Ch)

The question

Can terms be implied to limit the timeframe in which a contractual right can be exercised?

The key takeaway

The courts are willing to imply terms, even if they are not necessary to meet the 'business efficacy' test, where those terms are so obvious that it "*goes without saying*" that the parties would have proceeded on the basis that they existed.

The background

The case concerned a home owned by Wigan Borough Council (**WBC**) called Haigh Hall. In 2015 WBC granted planning consent to redevelop the property into a hotel and wedding venue. WBC then granted a lease over the property to Scullindale Global Ltd (**SGL**) for a term of 199 years for a premium of £400,000.

The lease contained some milestones that required SGL to redevelop the property within a specific timeframe, along with acquiring the proper planning permissions. The lease also contained a break right for WBC, which was exercisable "…*at any time*" with two months' notice if SGL failed to meet those specific milestones (deemed to be an **Event of Default**). The lease also stipulated that WBC should pay compensation to SGL if the break right was exercised.

In September 2019 WBC purported to exercise the break right and gave notice to SGL to terminate the lease two months later. SGL remained at the property after the termination date and WBC subsequently claimed that they were trespassing and therefore liable for damages for trespass or mesne profits. SGL argued that the lease was still in place as WBC had not served the notice exercising their break right within a reasonable time, and that their redevelopment of the property had been completed by the time the break right notice was served.

The decision

The High Court found that WBC's break right notice was effective.

The court rejected SGL's suggestion that the words "*at any time*" should be construed as requiring notice to be served "*at any reasonable time*", "*at any time whilst an Event of Default persists*" or "*at any time between 23 May 2018 and subsequent completion of the Development in accordance with the Planning Permissions*". SGL had argued that an implied limitation to the right was necessary to meet the business efficacy test or to reflect the reasonable expectations of the parties.

The court did not agree – SGL could serve a notice on WBC at any time after an Event of Default, making time of the essence for the exercise of the break right. The failure to serve a notice at that point by WBC would make the right lapse. Because of this the implied term was not necessary to satisfy the business efficacy test.

However, the court decided that it *was* necessary to imply a limitation on the break right because it was so obvious as to "*go without saying*" that both parties had proceeded on the basis that a break notice could only validly be served at any time whilst an Event of Default still persisted.

Even with this implied limitation on the break right, the court deemed the notice to be valid because the development was not completed in accordance with the planning permissions by the required completion date and/or the break right notice date. The court also required that WBC pay compensation based on the value of the Property at the break date.

Finally, the court considered the matter of damages for trespass or mesne profits. WBC had not suffered any financial loss, nor had SGL received any financial benefit from the continued possession of the property after the break right date, so the court did not order any damages or mesne profits to WBC.

Why is this important?

The decisions confirms that the courts may be willing to imply terms where those implied terms satisfy only the requirement of "obviousness", not "business efficacy"; although the judge acknowledged that in practice it is likely to be a rare case when only one of those requirements is satisfied.

Any practical tips?

When considering the exercise of a contractual right, consider whether there should be any limitations, eg if the trigger event has passed, duration, new circumstances, etc. This particularly relevant if a "trigger" event can happen at any point during a long-term agreement. Those limitations should be expressly included in the contract to avoid the uncertainty of implied terms.

Summer 2021

Commercial

Search engines can infringe sui generis rights when copying databases if it adversely affects database maker investment

SIA "CV-Online Latvia" v SIA "Melons" Case C-762/19

The question

Does the copying of a website's database by a search engine infringe database rights?

The key takeaway

If the copying of a database has an adverse effect on the database creator's investment, the copying can infringe the (*sui generis*) database rights in the database.

The background

The Claimant, SIA CV-Online Latvia (**CV-Online**), created and operated a website that included a database containing job advertisements published by employers. The site also contained "microdata" metatags, which were invisible to users, but allowed internet search engines to better identify the content on the site and to index it correctly. For each of the job postings the "microdata" contained the keywords "job title", "name of the undertaking", "place of employment" and "date of publication of the notice".

The Defendant, SIA Melons (**Melons**), operates a website containing a search engine specialising in job advertisements, which allowed users to search several websites containing job advertisements following certain criteria. The website then produced links to various websites with relevant job advertisements, including CV-Online's website. When a user clicked one of the links it would take them to the relevant job ad on that specific website.

CV-Online sued Melons for breach of the *sui generis* database right under Article 7 of the EU Database Directive, alleging that Melons "extracted" and "re-utilised" a substantial part of the contents of their database.

The decision

The Court of Justice of the EU (**CJEU**) held that internet search engines that copied and indexed whole or substantial parts of a database freely available online, and then allowed its users to search the database on its own website, amounted to "extracting" and "re-utilising" the content within the meaning of Article 7.

However, databases would only be protected by Article 7 if there had been qualitatively or quantitatively a substantial investment in the obtaining, verification or presentation of the contents of the relevant database (including any associated metadata). The CJEU assumed that this was the case in terms of CV-Online's website.

In terms of "extraction" and "re-utilisation", the CJEU considered that this would encompass any act of appropriating and making available to the public, without the database maker's consent, the results of their investment that deprived the database maker of revenue that should have enabled them to redeem the cost of the investment.

Why is this important?

The CJEU's decision sets clear boundaries on the copying of databases by search engines if the copying negatively effects the database maker's investment in the creation of the database. The CJEU highlighted the need to balance the interests of both parties, namely, to protect the investment in the database but also users' and competitors' capability to access the information contained in those databases and the possible creation of new innovative products based on that information.

Any practical tips?

Search engines will be able to continue to utilise the contents of these types of databases, so long as there is no negative impact on the revenues of the database holder. Search engines can still identify and index content; but activities that deprive the database owner of the benefits of its investment in the database are not permitted.

Summer 2021

Commercial

High Court determines that an "unusual" and "exorbitant" exclusion clause in standard terms and conditions fails the UCTA reasonableness test

Phoenix Interior Design Ltd v Henley Homes Plc & Anor [2021] EWHC 1573 (QB)

The question

When is an exclusion clause in standard terms and conditions considered to be unreasonable?

The key takeaway

Any unusual or onerous exclusions or limitations in terms and conditions need to be visible and well-signposted to the other party. If not, they can be deemed to be unreasonable and unenforceable.

The background

The Claimant, Phoenix Interior Design Ltd (**Phoenix**), brought a claim against the Defendant, Henley Homes Plc (a property development group) (**Henley**), with respect to unpaid invoices for interior design services. The parties' relationship spanned some 10 years, and Phoenix had been retained to provide furniture and fittings for a new "high end" apartment hotel in Scotland.

Phoenix presented Henley with its design concept, and hard copies of its terms and conditions were made available at the presentation. Subsequently, a revised proposal was sent to Henley via email with the terms and conditions provided "overleaf". There were further revisions of the design over some time, which all referred to the same terms and conditions, but no new copies of the terms were provided with those revisions.

A dispute then arose between the parties concerning the quality and suitability of the products and design provided by Phoenix; whether the works were signed off by Henley and whether completion had occurred. Phoenix asserted that a "five-star specification" was not part of the contract and sought to rely on its terms and conditions, in particular its exclusion clause, which provided that it was not liable under its warranty if the total price of the goods had not been paid by the due date for payment.

Henley disputed Phoenix's assertions, arguing that Phoenix's performance had been defective to the point that completion had not occurred, and the invoice balance was therefore not due.

The decision

The High Court held that Phoenix's terms and conditions had been incorporated into the contract. Among other factors, Henley was provided a copy of the terms at the presentation and in subsequent email correspondence, and signed copies of the agreement referred to them (even though they were not provided overleaf). Henley had not attempted to incorporate its own terms and had simply accepted the agreement.

In the agreement, Phoenix had warranted that the goods would correspond with their specification. However, the exclusion clause that Phoenix sought to rely on was unreasonable because:

- there was no good explanation for why an anti-set off clause would not have sufficed
- it was an unusual clause tucked away "in the undergrowth" of the standard terms and conditions without any highlighting of the consequences, which were also not obvious
- the clause was potentially exorbitant because the consequence of the slightest delay or deduction might bar all rights of redress against the claimant relating to the quality of the goods supplied
- it was very difficult for a customer without an independent certifier to say when there had or had not been completion, and
- payment was due on the date of completion as opposed to a number of days following it.

Why is this important?

The case is a clear reminder to draw attention to particularly unusual or exorbitant clauses within terms and conditions and make the consequences of non-compliance clear to the other party. Don't simply assume that the other party is aware of them. The more visible and well-signposted the clause, the greater the likelihood that the supplier can successfully rely on them.

Any practical tips?

Make sure that any unusual or onerous terms, including exclusions and limitations of liability, are visible and clearly marked/brought the attention of the other party in standard terms and conditions (and not hidden in the small print).

Make it easy for the other party to have access to the standard terms and conditions and ensure that they are properly incorporated into any agreement (ideally with some method of express acceptance).

Summer 2021

Data

UK gains adequacy for EU-UK data transfers, despite opposition from LIBE Committee

The question

What were the grounds of objection by the EU's Civil Liberties, Justice and Home Affairs Committee (the **LIBE Committee**) to the EU's decision to grant the UK adequacy for EU-UK data transfers?

The key takeaway

Despite protest from the LIBE Committee, on 28 June 2021 the European Commission (**Commission**) adopted its draft adequacy decisions in respect of both the GDPR and the Law Enforcement Directive, meaning that personal data can continue to flow freely between the UK and EU. This means that UK businesses and organisations can continue to receive personal data from the EU and EEA, without having to put additional arrangements in place with European counterparts.

The background

The EU General Data Protection Regulation (**GDPR**) sets out the requirements for the processing of personal data and its free movement within the EU and EEA. Under the GDPR, data can be freely transferred between Member States and EEA countries. For third countries, which now include the UK following Brexit, an adequacy decision of the EU Counsel is required to allow the free flow of data between the UK and EU. After the UK's exit from the EU, a six month "bridging" period was put in place while the EU assessed whether the UK should receive an adequacy decision that would allow data to flow freely from the EU to the UK.

The development

On 11 May 2021 the LIBE Committee announced that it had passed a resolution evaluating the Commission's approach on the adequacy of the UK's data protection regime. This raised concerns around the implementation of the UK's data protection framework, especially in the light of *"…broad exemptions in the fields of national security and immigration, which now also apply to EU citizens wishing to stay or settle in the UK, and… a lack of court oversight of data policies, as well as wide executive powers"*. This resolution followed the LIBE Committee's earlier non-binding opinion (published on 5 February), which concluded that the UK data protection regime was inadequate and would fail to protect the data of EU citizens.

The LIBE Committee called for the Commission to amend its draft adequacy decisions in respect of both the GDPR and the Law Enforcement Directive, so that the decisions reflect CJEU court rulings and address European Data Protection Board concerns raised in opinions 14/2021 and 15/2021 (both opinions recommended the adoption of an adequacy decision, but highlighted some shortcomings in the UK data protection regime, including agreements between the UK and US allowing for surveillance of personal data).

The LIBE Committee urged the Commission to withdraw its draft adequacy decisions without first agreeing an action plan for the UK to address the perceived issues in its data protection regime, including access to personal data for surveillance purposes. However, despite these objections, the EU Commission ultimately adopted the UK adequacy decision on 28 June 2021.

Why is this important?

Failure to obtain an adequacy decision would have been disastrous for UK businesses over a wide range of industries. Analysts warned that the absence of an adequacy decision could have cost UK firms up to £1.6bn in compliance costs or higher prices for goods and services.

Any practical tips

The UK's adequacy decision comes as a huge relief for UK businesses who work closely with EU Member States.

However, the topic of international data transfers remains a "live" one, as all eyes are now on the UK's Information Commissioner (**ICO**) as to whether it will adopt the EU's new Standard Contractual Clauses (**SCCs**) published on 4 June 2021. These new SCCs become mandatory after 27 September 2021 for new agreements (ie the old SCCs can be used up until this date for new agreements). For any pre-existing agreements using the EU's old SCCs, there is a transition period until 27 December 2022, after which the new SCCs will have to be incorporated.

The ICO has previously stated that it only recognises the EU's previous SCCs (valid as at 31 December 2021) as an adequate means of international data transfer from the UK and that it is looking towards developing its own UK SCCs for such transfers. The current situation leaves businesses with somewhat of a challenge - by needing to continue to use the old EU SCCs for transfers outside the UK and the new EU SCCs for transfers outside the EU. Clearly this is far from ideal. While we await an update from the ICO, it makes sense to get ready for the changes to come – for example, by conducting an audit of your contracts to determine which involve international data transfers and, more specifically, which involve data transfers from the UK and which from the EU in order to be ready for the eventual outcome.

Summer 2021

Data

EU Commission publishes final versions of its new Standard Contractual Clauses

The question

What is the impact of the new Standard Contractual Clauses (**SCCs**) on companies and data transfers?

The key takeaway

The new SCCs will become mandatory after 27 September 2021 for new agreements (ie the old SCCs can be used up until this date for new agreements). For pre-existing agreements using the old SCCs, there will be a transition period until 27 December 2022, after which the new SCCs will have to be incorporated.

The background

The old SCCs came into force along with the General Data Protection Regulation (**GDPR**) in May 2018 and provide contractual clauses that are pre-approved by the EU that can be incorporated into contractual arrangements to enable compliance with international data transfer requirements.

Following the EU Court of Justice's decision in *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (Case C-311/18) (**Schrems II**), the EU set out to update the old SCCs to enable lawful transfers of personal data to non-EU countries.

The development

The key changes to the new SCCs include:

- one single entry-point covering a broad range of transfer scenarios, instead of separate sets of clauses. A new 'modular' approach gives greater flexibility for complex processing chains by offering the possibility for more than two parties to join and use the clauses, and
- a practical toolbox to comply with the Schrems II decision, giving an overview of the different steps companies have to take to comply with the decision. There are also examples of possible 'supplementary measures', such as encryption that companies can take where needed.

The two key dates to note are:

- **new agreements**: the old SCCs can be used until 27 September 2021, after which the new SCCs will become mandatory for all new agreements, and
- **existing agreements**: a transition period of 18 months for controllers and processors that are using the old SCCs in existing agreements, which will remain valid until 27 December 2022, provided processing operations remain unchanged and are subject to appropriate safeguards.

Why is this important? And what about Brexit?

The new SCCs provide companies with greater flexibility over data transfers, in particular in connection with complex processing chains. The new toolkit also enables easier compliance following the Schrems II decision to ensure that international data transfers are compliant with the GDPR.

In light of Brexit, however, the new SCCs do not form a part of retained EU legislation in the UK, and how far the UK's Information Commissioner (**ICO**) officially adopts the new SCCs remains to be seen. The ICO is currently considering preparing the UK's own bespoke SCCs (ie under the UK GDPR). In the meantime, UK businesses are left with a challenge, given that the ICO has previously stated that it only recognises the EU's previous SCCs (valid as at 31 December 2021) as an adequate means of international data transfer from the UK. This means that (for now at least) those businesses are left with the need to continue using the old EU SCCs for transfers outside the UK and the new EU SCCs for transfers outside the EU.

Any practical tips?

- Review your existing data protection agreements and transfer arrangements to ensure that: (a) any processing operations remain unchanged and are subject to appropriate safeguards to benefit from the transition period (ie until 27 December 2022 for those agreements already using the old SCCs); and (b) you have a clear understanding as to which arrangements involve transfers outside the UK and which relate to transfers outside the EU
- For transfers outside the EU, ensure that the new SCCs are incorporated into your new data protection agreements where necessary (ie from 27 September 2021), and
- For transfers outside the UK, keep alert to developments within the UK and any potential divergence from the EU approach in relation to any UK SCCs.

Summer 2021

Data

European Parliament asks European Commission for guidance post-Schrems II

The question

Where next for Schrems II? Or rather, how will the European Commission (**Commission**) respond to the European Parliament's call for guidance following the CJEU decision in *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (Case C-311/18)?

The key takeaway

The European Parliament has passed a resolution calling on the Commission to issue guidelines on how to make data transfers compliant with recent CJEU case law and the European Data Protection Board's (**EDPB**) decisions.

The background

The decision in Schrems II was yet another blow for the legal framework surrounding international data transfers. In the decision, the CJEU invalidated the Commission's adequacy decision for the EU-US Privacy Shield Framework, which was used by over 5,000 companies to conduct data transfers between the EU and US. The decision also cast doubt over other personal data transfers between the EU and US due to the US government's access to private sector data.

Since the decision, the Commission has recently incorporated changes into documents such as the new Standard Contractual Clauses to consider the impact of the decision. However, MEPs have requested further guidance in several areas, including on the implementation of guidance from the EDPB.

The development

The European Parliament has called on the Commission to incorporate the EDPB's recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. It has asked the Commission not to conclude new adequacy decisions with third countries without considering the implications of CJEU rulings and ensuring full General Data Protection Regulation (**GDPR**) compliance. In addition, MEPs have called for data storage capabilities to be developed within Europe to achieve true autonomy in data management through additional investment.

The Commission had expressed disappointment with the Irish Data Protection Commissioner (**IDPC**) because of its decision to initiate a civil claim in Schrems II, rather than independently

triggering enforcement procedures based on GDPR rules. MEPs also criticised the IDPC's long processing times and called for infringement proceedings to be issued against it.

Finally, MEPs have asked EU Member States to stop transfers of data that could be accessed in bulk in the US if the Commission reaches an adequacy decision regarding the US.

Why is this important?

The ball is now in the Commission's court to issue guidance on how best to manage data transfers and enforcement in a post-Schrems II world.

Data transfers to the US remain under significant scrutiny with a strong desire to avoid any adequacy decisions based on a system of self-certification (such as the Safe Harbour and Privacy Shield frameworks). One rapporteur stated that the Commission could not afford to repeat the mistakes of the past and bear witness to a possible "*Schrems III*" case. It is particularly concerned with the use of mass surveillance technologies in the US and compliance with EU law, which puts the spotlight on the Biden administration's approach to privacy and national security over the coming months and years.

Any practical tips?

Keep looking to include terms within your agreements to anticipate additional measures flowing from Schrems II. Above all, keep an eye out for further announcements by the Commission on its forthcoming guidelines and how best to ensure compliance with international data transfers.

Summer 2021

Data

ICO fines American Express for blurring service emails with marketing emails

The question

What is the difference between service emails and marketing emails, and what happens if you get it wrong?

The key takeaway

Take great care to avoid including marketing material in service emails to customers who have not consented to marketing communications. If the material is targeted at specific individuals and advertises any of the business' goods or services, or contains any significant promotional material aimed at encouraging customers to purchase extra products or services, it is highly likely to be subject to the strict rules on consent-based direct marketing.

The background

The Information Commissioner's Office (**ICO**) has fined American Express Services Europe Limited (**Amex**) £90,000 for sending more than four million unsolicited marketing emails to its customers.

Over a 12-month period, between 1 June 2018 and 31 May 2019, Amex sent over 50 million service emails to its customers. These emails prompted complaints from customers who were disgruntled at receiving marketing material contained within these emails, despite having opted out of marketing communications.

The ICO's investigation

The ICO was prompted to investigate as a result of complaints from five Amex customers in 2019. They asserted that they were receiving marketing emails despite having opted out of them. Amex rejected the complaints, alleging that the emails were service emails, not marketing emails and as such were not covered by the specific rules around electronic marketing.

The ICO found that Amex had sent over 50 million service emails to its customers, and that over four million of those emails were marketing emails. The emails in question included details of the rewards of shopping online with Amex, advice on how to get the most out of using the card and encouragement for customers to download the Amex app. They were designed to encourage customers to make purchases on their cards which would benefit Amex financially, and therefore amounted to a deliberate action for financial gain by the company.

Amex argued that customers would be disadvantaged if they were not informed about campaigns, and that the emails were a requirement of its Credit Agreements with customers. The ICO disagreed, and fined Amex £90,000 for its conduct in sending the unlawful marketing emails.

Why is this important?

Amex's case highlights the importance of being vigilant on what can be a fine line between a service email and a marketing email. Service messages contain routine information, such as changes to terms and conditions and payment plans, notice of service interruptions, or information around product safety. By contrast, direct marketing is any communication of advertising or marketing material that is directed at specific individuals. This distinction is critical, and the latter should only be sent to those who have given their consent to receiving marketing emails – noting the strict rules which apply to direct marketing messages under Regulation 22 of the Privacy and Electronic Communications Regulations 2003 (**PECR**).

The maximum fine for a breach of PECR is £500,000. The fact that Amex were fined £90,000 on this occasion shows that the ICO take these kinds of complaints seriously, even in circumstances where only a handful of complaints were received. It considered the breach to be serious and therefore worthy of a noticeable fine.

Any practical tips?

All companies should familiarise themselves with the differences between a service email and a marketing email and thereby ensure that their email communications with customers are compliant with PECR. The ICO has published helpful guidance on the difference between marketing and service emails, which can be used as a point of reference. See the ICO's draft Direct Marketing Guidance for the latest on this.

It is also prudent for companies to regularly revisit and monitor their procedures to ensure that marketing messages are not inadvertently slipping into service emails, at least not to customers who have not consented to receive them.

Summer 2021

DATA

Data Sharing Code of Practice goes before UK Parliament

The question

What does the Data Sharing Code of Practice (the **Code**) mean for companies that deal with personal data?

The key takeaway

The Code does not mark a huge leap from the previous data sharing code, but it serves as a helpful and useful guide for organisations to help ensure compliance when sharing any personal data with third parties.

The background

In May 2021 the UK government placed the Code before Parliament for consideration as a statutory code of practice under s.121 of the Data Protection Act 2018. The Code is a practical guide for organisations about how to share personal data in compliance with data protection law. Unless amended or rejected by Parliament, the Code will come into force after 40 sitting days.

The development

The Code has been in development with the UK government and the Information Commissioner (**ICO**) for some time, but finally has reached its apparent final form. The last data sharing code was published almost 10 years ago, and the Code now seeks to update it to reflect key changes in data protection laws and the ways in which organisations share and use personal data.

The Code compiles all of the practical considerations that companies need to take into account when sharing personal data with other parties, bringing together existing items of ICO guidance in relation to ensuring a legal basis has been satisfied for said transfers, and supplementing this with new guidance.

The updated Code is lengthy, so the following is a flavour only of some of the useful practical guidance it provides:

- **conducting data impact assessments**: organisations should conduct these when considering sharing personal data, allowing for the assessment of risks of the sharing of data to be identified and safeguards to be put in place where needed

- **clarification on the responsibility of the disclosing party for the recipient's processing of personal data**: the Code attempts to clarify the extent to which an independent controller, which discloses personal data to another controller, is responsible for the recipient's processing of that personal data. The Code notes that an organisation should not provide personal data to another if it does not have visibility over the measures, they are taking to protect the data during the process
- **due diligence in data sharing during M&A**: the Code notes that the parties involved in a M&A transaction need to ensure that due diligence extends to examining issues pertaining to the transfer/sharing of personal data in connection with that transaction, and
- **sharing of personal data in databases and lists**: recipients of a database or list of personal data from another party have the responsibility to establish the provenance or integrity of the data they receive, and ensuring that all compliance obligations have been met prior to exploiting or otherwise using the data.

The Code also briefly discusses guidance on automated decision-making and the difference between anonymised data and pseudonymised data, and how these need to be dealt with in a data sharing context.

Why is this important?

The ICO, Elizabeth Denham, said the publication of the Code was not a conclusion, but a milestone, and that it *"demonstrates that the legal framework is an enabler to responsible data sharing and busts some of the myths that currently exist"*. As such, it is a highly useful tool for organisations in ensuring that their data sharing arrangements are above board, both currently and moving forwards.

Any practical tips?

Remember to consult the Code when considering any data sharing arrangements, as well as the ICO's data sharing information hub. The latter provides targeted support and resources, including:

- data sharing myths busted
- data sharing code: the basics for small organisations and businesses
- data sharing FAQs for small organisations and businesses
- case studies
- data sharing checklists
- data sharing request and decision forms template
- sharing personal data with a law enforcement authority toolkit
- guidance on sharing personal data with law enforcement authorities, and
- guidance on data sharing and reuse of data by competent authorities for non-law enforcement purposes.

Summer 2021

Data

First-tier Tribunal grants Ticketmaster stay of its appeal on an ICO fine pending a parallel group action

The question

Can an appeal of an ICO fine be stayed pending the resolution of concurrent group action proceedings in the High Court?

The key takeaway

The case highlights the possibility of staying ICO actions where concurrent litigation is taking place in the High Court. It also provides practical pointers on contracting arrangements with third parties around the all-critical area of data security.

The background

Ticketmaster had contracted Inbenta Technologies Ltd (**Inbenta**) to provide a chatbot which Ticketmaster used on its website, including the payment page. The JavaScript code for the chatbot was hosted on Inbenta's server. An attacker managed to infect the code with a scraper that collected users inputted personal data including names, payment card numbers, expiry dates, and CVV numbers.

Following this breach the ICO issued Ticketmaster a fine of £1.25m, as it found that the implementation of the code by a third party for the processing of personal data was a known security risk and that Ticketmaster was in breach of Articles 5 and 32 of the General Data Protection Regulation (**GDPR**). In the ICO's view Ticketmaster had failed to adequately to address the security of the chatbot and its implementation into Ticketmaster's own infrastructure, and to ensure on-going verification of security to an acceptable level.

Ticketmaster subsequently appealed the ICO's decision to the First-tier Tribunal on several grounds, claiming, among other things, it had not breached the GDPR and that the attack was not foreseeable. However, Ticketmaster sought a stay in terms of its appeal in the light of ongoing group action proceedings in the High Court in relation to the same cyber-attack by a group of c. 800 customers who were affected by the data breach.

The development

In an unusual turn of events, the First-tier tribunal has stayed Ticketmaster's appeal of the ICO fine pending the conclusion of the High Court case. The First-tier tribunal considered that on balance, the Tribunal would be materially assisted by a substantive judgment from the High Court proceedings, and that those proceedings would be likely to determine points on

common issues of law. The stay was granted until 28 days after the High Court's judgment is handed down. It is unlikely, therefore, that Ticketmaster's appeal will be heard until late 2023.

Of separate, but equally important interest, the aspects of the High Court case which are relevant to Ticketmaster's appeal before the Tribunal include: Ticketmaster's vetting of Inbenta; each party's responsibilities for the security of the chatbox; Inbenta's awareness of the chatbox on Ticketmaster's payment pages; the reasonableness of the scope of Ticketmaster's integrity monitoring and so on.

Why is this important?

Although the stay in the case is very unusual, and companies involved in litigation with the ICO should not assume that this will happen in most cases, the decision does highlight the opportunity for organisations to delay enforcement action where this might be needed.

Any practical tips?

Should any fines be levied against you by the ICO for a major data breach, consider whether the ICO actions can be stayed if any concurrent High Court action has been initiated in order to minimise legal costs in the considerations of similar or the same issues by both the Tribunal and/or the High Court. The case also provides practical pointers on what to look for in your contracting arrangements with third parties, and being clear as to where responsibilities on such key aspects as data security.

Summer 2021

Digital

European Commission proposes new rules on AI

The question

How will future EU regulations affect the development of artificial intelligence (**AI**)?

The key takeaway

The European Commission's new draft regulations set specific standards and obligations on the developers of AI systems, particularly those which fall into a high-risk category. Developers of these systems will need to pay very close attention indeed to the new rules in order to avoid crippling fines in the future – being up to €30m or 6% of a company's total worldwide annual turnover, whichever is higher.

The background

Published in April 2021, the new draft regulations seek to turn Europe into *"the global hub for trustworthy AI"*, and to *"guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU"*. This is a big development in the legislative landscape for AI and developers will need to pay close attention to them to ensure compliance in the future.

The development

The regulations follow a risk-based approach depending on the level of risk in the use of AI in each particular context. The higher the risk, the stricter the rules. The categories include high-risk, limited risk and minimal risk, with the clear focus on high-risk systems. The latter are those where the AI creates a high risk to the health and safety or fundamental rights of natural persons. These include:

- employment, worker management and access to self-employment (eg CV-sorting software for recruitment)
- safety components of products (eg AI application in robot-assisted surgery)
- law enforcement that may interfere with people's fundamental rights (eg evaluation of the reliability of evidence), and
- administration of justice and democratic processes (eg applying the law to a concrete set of facts).

Developers of high-risk AI systems will have to adhere to specific obligations before they can be placed in the European market. These include:

- adequate risk assessment and mitigation systems run throughout an AI system's lifecycle
- high quality datasets used in training of an AI system to minimise discrimination and risks
- logging of the AI's activity to ensure traceability of results throughout its lifecycle
- designing and developing the system in a way which ensures transparency of its operation and use to the end-user, and
- appropriate human oversight of the AI system during the period of its operation.

Some high-risk systems will be outright banned, if they are deemed a clear threat to the safety, livelihoods and rights of people. Limited and minimal risk AI systems will have fewer, if any, obligations to comply with. A good example falling within the limited risk category are chatbots (being systems that interact with natural persons), where developers will have to only adhere to transparency obligations, informing users that they are interacting with a machine. Those deemed as minimal risk AI systems include AI-enabled video games or spam filters, which can be used freely and will not be regulated.

Non-compliance with the regulations can result in hefty fines for developers. Non-compliance with provisions on prohibited AI practices or data and governance obligations can incur fines of up to €30m or 6% of a company's total worldwide annual turnover, whichever is higher. An infringement of any other requirements (eg for activity logging, transparency or human oversight) can incur a fine of €10m or 2% of a company's total worldwide annual turnover.

Why is this important?

The draft regulations show clear intent by the EU for the setting of strong, robust standards for the development of AI, as most clearly witnessed by the potentially massive fines of up to 6% of worldwide turnover.

Any practical tips?

Any developers of AI, currently or in the future, must become familiar with the draft regulations as soon as possible, especially understanding which risk category their systems may fall into. If there's a chance of being deemed the provider of a high-risk system, then taking steps to hardwire in the necessary protections could prove critical in avoiding huge regulatory fines down the line.

Summer 2021

Digital

UK government publishes draft Online Safety Bill

The question

How could the Online Safety Bill (the **Bill**) affect online companies, in particular 'big tech'?

The key takeaway

The Bill sets out the proposed framework for the first regulatory regime specifically targeted at online tech firms in the UK and the provision of online services.

The background

The UK government has recently published a draft of the Bill, which is set to impose a duty of care on certain online service providers to take responsibility for the safety of their users in the UK. The Bill also appoints Ofcom as the regulator for this new duty of care.

The Bill aims to tackle illegal and harmful content, including racism, fraud (such as romance scams and fake investment opportunities), as well as illegal terrorist and CSEA content, while attempting to not curtail freedom of expression.

The development

The Bill gives Ofcom the power to oversee and enforce the legislative framework and requires Ofcom to prepare Codes of Practice to assist service providers in complying with their duties of care. It also extends Ofcom's general duties under s. 3 of the Communications Act 2003 to online safety matters and expands Ofcom's existing duties in relation to the promotion of the media literacy of members of the public. It also gives Ofcom the power to require the production of information by service providers and to investigate compliance with the Bill where needed.

The Bill extends and applies to the whole of the UK, but also has extraterritorial application to services based outside the UK where users in the UK are affected. However, the duties of care only apply to the design and operation of the service in the UK and to users in the UK. These duties of care will apply to providers of services that allow users to upload and share user-generated content (user-to-user services) and search services. There are, however, exemptions. These relate to services meeting certain conditions (eg internal company message boards and news publishers' websites).

Companies within the scope of the Bill will also have to provide mechanisms to allow users to report harmful content or activity and to appeal against the takedown of content. Certain companies, as

dictated by Ofcom, will also need to publish transparency reports setting out what they are doing to tackle online harms. These reports will then be published on the Ofcom website.

Why is this important?

A wide range of businesses potentially fall within the scope of "user-to-user services" covered by the Bill, ranging from the social media 'tech giants' to smaller review websites, independent forums and online marketplaces. Many will therefore have to prepare for the passing of the Bill in order to be compliant from day one.

Penalties for non-compliance can be steep and go beyond even those under the GDPR. Ofcom will be able to issue fines of £18m or 10% of qualifying worldwide revenue, whichever is higher. It will also be able to take enforcement action, which may include business disruption measures in relation to ancillary services. Senior managers of companies could also be liable for criminal sanctions if they fail to comply with Ofcom's information requests.

Any practical tips?

Providers of user-to-user services and search engines will need to carefully consider whether they fall within scope of the Bill and to review the codes of practice (to be issued by Ofcom in the near future). The risks of non-compliance are just too great, being some of the largest fines in regulatory history.

Summer 2021

Digital

UK Law Commission launches call for evidence on digital and crypto assets

The question

How ready is English law to accommodate emerging technologies, in particular digital assets?

The key takeaway

By instigating the Law Commission's consultations on digital assets and electronic trade documents, the UK government has shown a desire to support digital trade and the adoption of emerging technologies. The Commission's call for evidence (published April 2021) includes considering the benefits of giving greater certainty around the legal status of digital documents and assets, which is good news for a variety of digital business stakeholders, such as those engaged in international trade and non-fungible tokens (**NFTs**).

The background

The Commission was asked by the Ministry of Justice (**MoJ**) and the Department for Digital, Culture, Media and Sport to recommend law reforms that will ensure English law accommodates electronic trade documents and digital assets. In September 2020, the Commission announced it had started analysing English law in the context of digital assets and smart contracts. The Commission recognises that English law needs to evolve to support an increasingly digital world. For example, it notes that the current law does not adequately enable international trade using electronic documents; a digital document is not currently recognised as something that can be "possessed" and therefore it cannot be classified as a formal document of title. This issue can cause significant difficulties in the process of international trade and its financing. This digital assets project is intended to build on the Commission's electronic trade documents consultation and considers other areas such as cryptoassets (which will draw on the conclusions of the UK Jurisdiction Taskforce's significant Legal Statement on cryptoassets and smart contracts).

The MoJ asked the Commission to include the following points in its investigation into digital assets, namely: the current state of the law; recommended solutions to the problems caused by the lack of recognition of digital assets as "possessable"; recommendations to ensure the law provides legal certainty and predictability around digital assets; and areas of future consideration.

The development

The Commission's consultation asks for evidence and views on the following issues:

- **possessability** – the legal and practical implications if digital assets were possessable,
- **transferability** – analogies between the transfer of digital assets and other legal transfers (eg cash or bank transfers)
- the **mechanics of cryptoasset transfers** on the blockchain
- the distinction between **ownership and possession** and whether this distinction is helpful in the context of digital assets
- **classification of digital assets as goods** and practical consequences, also in the context of key legislations such as the Sale of Goods Act 1979, Supply of Goods and Services Act 1982 and the Consumer Rights Act 2015
- **title transfer** – whether it is possible to transfer good title to a digital asset
- transfer of **tokenised assets** and the relationship between a digital asset token and its underlying asset
- **security** and whether the difficulties of controlling a digital or crypto asset reduces the efficacy of a mortgage or charge
- **bailment** – whether it would be a practical or useful concept if digital assets were considered possessable
- **conversion** of digital assets and how it could arise in practice, and
- comparison with **other jurisdictions**.

Responses will be accepted until 30 July 2021. The Commission then intends to publish a consultation paper by the end of this year.

Why is this important?

The Commission's project show the UK government is serious about supporting digital commerce and mining the benefits of emerging technologies. Responses to the call for evidence will help the Commission identify gaps in the law, determine whether English law can accommodate the use of digital assets, and help direct law reforms. Greater certainty about the legal status of digital assets would also create a strong foundation for increasing adoption.

Any practical tips?

Stakeholders and market participants who are well versed in the technical and practical aspects of digital asset dealing are encouraged to contribute their evidence and views to the consultation. Despite previous consultations, digital assets still exist in an area of major legal uncertainty; those at the coal face are best placed to help legislators navigate it and to enable the law to develop in the best way to support adoption of these technologies. Above all, the anticipated reforms should give confidence to stakeholders and market participants; so, watch this space as the Law Commission starts to grapple with the difficult questions relating to digital assets and processes, paving the way for greater adoption in the commercial world.

Summer 2021

Digital

Facebook combats fake reviews following CMA pressure

The question

What does the CMA's prompting of Facebook to take action over fake reviews signal to the online marketplace in terms of potential future action in this area?

The key takeaway

Social media platforms and other similar online service providers need to consider the extent to which they offer a platform for individuals or businesses to sell fake reviews, and the steps they need to take to curtail this type of activity.

The background

In January 2020, following an investigation by the Competition and Markets Authority (**CMA**), Facebook committed to efforts to identify and remove both groups and pages on its site where misleading reviews were being sold. This commitment was also extended to Instagram in May 2020.

Fake and misleading reviews are already illegal under The Consumer Protection from Unfair Trading Regulations 2008; however, the CMA was not convinced that enough has been done by many internet giants to combat fake reviews. A follow-up investigation in early 2021 into Facebook found further evidence that the illegal trade in fake reviews was still occurring on both Instagram and Facebook, causing the CMA to intervene again.

The development

As a result of Facebook's crackdown, more than 16,000 groups were removed from the platform for trading fake reviews, as well as the creators being either suspended or banned outright. To build upon their current systems, Facebook also implemented further changes, namely:

- suspending or banning users who repeatedly create Facebook groups and Instagram profiles that promote, encourage or facilitate fake and misleading reviews
- introducing new automated processes that will improve the detection and removal of this content
- making it harder for people to use Facebook's search tools to find fake and misleading review groups and profiles on Facebook and Instagram, and
- putting in place dedicated processes to make sure that these changes continue to work effectively and stop the problems from reappearing.

Why is this important?

As the Chief Executive of the CMA notes: *"…never before has online shopping been so important…fake and misleading reviews are so damaging – if people lose trust in online reviews, they are less able to shop around with confidence, and will miss out on the best deals"*. This is noted as being particularly important in light of research which found that more than three quarters of shoppers are influenced by reviews when they shop.

Social media platforms and businesses both need to be critically aware of reviews on their websites and ensure that they are acting in a way that promotes public confidence, in order to avoid similar scrutiny from the CMA and ensure they act within the confines of the law. This is against the backdrop of the new Digital Markets United, which was set up within the CMA in April 2021, and provides a framework for governing the behaviour of platforms that dominate the market.

Any practical tips?

All platforms and businesses offering similar opportunities for the sale of fake reviews are likely to risk action in the future. This is particularly the case given the EU's forthcoming Omnibus Directive in May 2022, which highlights online reviews as a target area of concern. Identifying checks and controls now in order to monitor and verify reviews is increasingly becoming a business necessity if sanctions from the CMA and other regulators across the EU are to be avoided and public confidence in reviews is to be retained.

Summer 2021

Digital

European Commission looks to strengthen the Code of Practice on Disinformation

The question

What steps are being taken to strengthen the EU Code of Practice on Disinformation (the **Code**)?

The key takeaway

While the Code has been adopted on a self-regulatory basis by the relevant signatories, the European Commission's recent guidance (May 2021) shows that sweeping reforms and updates are needed to make it truly effective at halting the flow of disinformation.

The background

The Code is a 2018 regime introduced for online platforms and the advertising sector which outlines a list of commitments for signatories to implement in order to help stop the spread of disinformation. It was designed as a self-regulatory system and signing up is voluntary.

Under the Code, disinformation is defined as *"verifiably false or misleading information"* manufactured for monetary gain or to deceive the public, ultimately causing harm. Measures to tackle disinformation under the Code include ensuring transparency on political advertising, the closure of fake accounts and the demonetization of accounts which peddle disinformation.

The Code also includes a section dedicated to assessing its success, which included an initial assessment period of 12 months, culminating in a report published in September 2020. It found that the Code needed to be strengthened and more effectively monitored. The report set out that, while the Code is an effective tool in stemming the flow of disinformation, it fell short in a few key areas, including: inconsistencies in application across platforms and Member States; a lack of uniform definitions; gaps in scope; limited participation; and lack of independent oversight.

The development

In response to the report, the European Commission published a communication in May 2021 setting out guidance on strengthening the Code in order to address its weaknesses. The guidance sets out steps which should be taken by stakeholders to strengthen the Code, including the following three key areas to be addressed:

- **reinforced commitments -** to achieve the Code's objectives

- **broadening participation** - while the current signatories include major online platforms, there is a need to ensure that other established platforms, as well as emerging ones, sign up in order to ensure that a broad and united front is presented against disinformation, and
- **tailored commitments** - in order to facilitate broader participation, the Code should include commitments that are tailored to the specific services provided by certain platforms. The guidance and steps taken by the Commission also aim at evolving the existing Code of Practice towards a co-regulatory instrument foreseen under the Digital Services Act.

To achieve the above goals, the Commission also set out various steps that should be taken to help strengthen the Code, namely:

- **demonetising disinformation**: the Code should strengthen the commitments made by signatories designed to defund the accounts of those disseminating disinformation on their own platforms as well as third party websites
- **commitments to address advertising containing disinformation:** under the strengthened Code, the signatories should be committing to design and implement advertising policies that adequately addresses the misuse of their advertising systems via disinformation. Signatories should work to ensure that they have adequate resources to ensure that these policies are properly enforced. Alongside this, signatories should ensure that political advertising comes with sufficient labelling, verification as well as transparency commitments
- **integrity of services:** the updated Code should include provisions that provide for enhanced coverage of current and future forms of manipulative behaviour that can be leveraged in order to spread disinformation. This includes: ensuring that the signatories agree on a cross-service understanding of the kinds of manipulative behaviour that may be used by those attempting to spread disinformation; the introduction of expanded and firmer commitments to limit the effectiveness of techniques used to spread disinformation including hack-and-leak operations, account takeovers, impersonation and deep fakes; a commitment to continued re-evaluation and assessment to ensure that the Code can continue to adapt to combat new threats
- **empowering users:** the Code's commitments to empowering users should be expanded and enhanced to cover a broad range of services, including mechanisms by which users can appeal against actions taken by signatories as well as increased protections for children
- **empowering the research and fact-checking community**: steps should be taken to strengthen the Code by allowing access to the platforms' data by the research and fact checking community (whilst also being mindful of any data protection concerns) as well as increasing collaboration, and
- **ongoing monitoring:** as mentioned above, the Code should include a robust monitoring system to ensure that it is fit for purpose. Any monitoring system should provide for the regular assessment of the signatories' implementation of their commitments under the

Code. In particular, the signatories should ensure that they all provide information and monitoring data in standardised formats.

Why is this important?

The publication of the Commission's guidance highlights a revitalised crackdown on the spread of disinformation, whilst reinforcing that the onus of policing the spread on disinformation is on the very platforms that are used by malicious actors. The steps outlined will strengthen the Code and increase the responsibility on the signatories to ensure that adequate steps are taken to combat the spread of disinformation. Consistent monitoring and reviewing on the effect of the Code will help ensure that it continues to evolve to counter new threats of disinformation which may emerge.

Any practical tips?

Working to ensure that the relevant internal procedures and policies are put in place in order to enact the recommendations put forward by the Commission will go a long way to combatting the spread of disinformation. Ideally, collaborating with other signatories, including via working groups, will help ensure consistency in implementation and ongoing effective management.

Summer 2021

Consumer

UK government policy on cyber security legislation for connected consumer products

The question

What will the UK government's future legislation on cyber security over connected products mean for manufacturers, retailers and distributors?

The key takeaway

A new robust scheme of regulation is on the way to protect consumers in a fast-developing world of connected products – think smart TVs, wearables, smartphones, connected fridges/doorbells and digital assistants (like Google Assistant, Siri and Alexa). Manufacturers and distributors of these products all need to pay close attention to the new rules, in particular the government's mantra of "security by default".

The background

The UK government ran a consultation in mid-2020 on new proposals for UK legislation on the cyber security of connected products (ie the Internet of Things) in an attempt to make items like TVs, cameras and household appliances which connect to the internet safer and more secure. The consultation ended in September 2020, and the government provided its response in the form of a policy paper in April 2021. This in large part references the earlier "Code of Practice for Consumer IoT Security" published by the Department for Digital, Culture, Media and Sport and the National Cyber Security Centre in October 2018 (the **Code**).

The development

Following the consultation and the subsequent responses from third parties, the government has now signaled its intention to put forward legislation to create a new robust scheme of regulation to protect consumers from insecure connected products. The new legislation will apply to all consumer connected products such as smart speakers, smart televisions, connected doorbells and smartphones; however, some devices will be exempt due to the specific circumstances of how they are constructed and secured, including desktop computers and laptops.

The new security requirements will align the UK with existing international standards and aims not to unnecessarily burden manufacturers with new requirements to those they might already be complying with. Any non-compliant products will not be able to enter the UK market. Three key security requirements being proposed by the government pick up on those identified in the previous Code, namely:

- a ban on universal default passwords
- implementation of means to manage reports of vulnerabilities, and
- transparency on the minimum time period during which a product will receive security updates.

The UK is set to also create a regulatory body to oversee the enforcement of the requirements, which will have powers to investigate allegations of non-compliance and to take steps to ensure compliance. The government has not announced any levels of potential fines, but they may end up being steep given the raft of other new regulations now adopting GDPR-level penalties for non-compliance.

The legislation will require manufacturers to publish a publicly available declaration of conformity and to act if they place a product on the market that is not compliant. Distributors (including wholesalers and retailers) of such products will also be subject to new obligations, including a requirement to verify that the manufacturers of consumer connected products they are working with have published a declaration of conformity. There will be two routes to compliance under the new regulations, namely (i) implementation of security requirements derived from and aligned with the top three guidelines from the Code of Practice for Consumer IoT Security and key provisions within the ETSI European Standard; and (ii) compliance with other relevant standards, as designated by the UK government in the future, that can be implemented in lieu of the security requirements in the legislation.

Why is this important?

The government's response shows a clear intent to regulate connected products and to provide consumers with a safer experience when using such devices, while trying to not burden manufacturers and wholesalers with new requirements they have not complied with. While the new legislation is set to be broad and cover many types of devices, it still acknowledges the challenges of its application to devices like laptops and desktops, which will be exempt.

Any practical tips?

- Ensure that current safety standards are equivalent or exceed those which will be required by the new legislation and implement cyber security measures in line with the intended requirements should any gaps exist
- Review existing reporting on compliance and produce any requisite declarations of conformity, ensuring that these are publicly available, and
- Above all, see compliance as an opportunity to build trust with your existing and future customers – it's hard to see brands who fail to gain consumer trust surviving given the potentially "intrusive" nature of a connected device within the home environment.

Summer 2021

Consumer

CMA to publish "greenwashing" guidance in Autumn 2021

The question

What measures will regulators introduce to prevent businesses from misleading consumers about their products' "green" credentials?

The key takeaway

The Competition and Markets Authority (**CMA**) will issue its final guidance on how to avoid "greenwashing" in August or September 2021. With increasing interest in brands' environmental credentials, marketing and legal teams should ensure they get to grips with the guidance in good time, in particular its six core principles, which include a focus on ensuring substantiation with credible and up to date evidence of any eco-friendly claims.

The background

The CMA first launched its investigation into how consumers can be protected from misleading green marketing campaigns in November 2020. So-called "greenwashing" occurs when unsubstantiated claims are made about a product's ethical credentials to deceive consumers. The investigation followed increased concerns that the recent boom in consumption of environmentally friendly and ethical goods might encourage businesses to make false promises about how green their products really were.

The investigation focused on:

- how claims about the environmental impact of products are made
- whether these claims can be substantiated with evidence
- to what extent these claims influence people to purchase products, and
- whether consumers are misled by a lack of information on a product's environmental impact.

Behaviours such as exaggerating a product's environmental impact or using misleading packaging for a product were highlighted by the CMA as issues with greenwashing.

In May 2021, draft consumer protection law guidance was published along with a call for responses from interested parties. The CMA's consultation ended on 16 July 2021.

The development

Following its consultation this summer, the CMA will issue its final guidance in August or September 2021. The draft guidance will set out six principles designed to help businesses make environmental claims while complying with existing consumer protection law. Businesses are advised that any claim made about a product or service's environmental credentials must:

- be truthful and accurate
- be clear and unambiguous
- not hide important information that would prevent a consumer from making an informed choice
- make only meaningful comparisons
- consider the total impact of a product across its life cycle, and
- be substantiated with credible and up to date evidence.

The guidance will focus on UK marketing practices, but the CMA is also looking to be a leader in investigating green product claims being made globally, particularly where the products are for sale to UK consumers.

Why is this important?

At present, the six principles are likely to be issued as guidance aimed at helping businesses to avoid greenwashing their products. However, following a joint investigation with the International Consumer Protection Enforcement Network in February 2021, the CMA suggested that it would act against businesses that makes misleading sustainability claims.

Any business looking to promote products on the basis that they are good for the planet should therefore pay close attention to the new guidance when it is published.

Any practical tips?

Even before the guidance is published, it would be wise to consider the CMA's six principles for compliance before making any claim about a product/service's green credentials, including:

- be transparent in the language you use
- don't hide information, and
- if you're making a specific claim about the product, make sure you have the evidence to back it up.

Summer 2021

Consumer

CMA targets anti-virus software companies on subscription auto-renewals

The question

What consumer rights concerns have the Competition and Markets Authority's (**CMA**) recent enforcement actions raised, especially with regards to automatic subscription renewals?

The key takeaway

Auto-renewals remain under the regulatory spotlight, with the CMA recently acquiring undertakings from McAfee Ireland Limited (**McAfee**) and NortonLifeLock Ireland and UK (**Norton**) to combat their subscription practices which the CMA deemed potentially unfair for consumers.

The background

The CMA began an investigation into the anti-virus software sector in 2018 in the light of concerns that some companies may not be complying with consumer protection laws. The investigation focused particularly on the fairness of: (i) whether automatic renewal is set as the default option; (ii) whether notification of renewal is sent and, if so, the timing of the notification; and (iii) when renewal payments are taken and whether the renewed subscriptions are charged at a different price to the original subscription.

The development

Following the investigation, both McAfee and Norton gave voluntary undertakings to the CMA in May and June 2021 respectively. The undertakings seek to make changes so that automatically renewing contracts is easier for consumers to understand and exit. More specifically, the undertakings include:

- giving customers whose contract has auto-renewed an ongoing right to exit the contract and obtain a pro-rata refund of the amount they have been charged, after their existing refund window has expired (also extended to customers who asked for a refund in 2020, but were refused) – the right will be available to consumers from 24 August 2021 onwards
- making refunds available through an automated system to make it simple and easy
- ensuring customers are made aware, up front, that their contract will auto-renew, the price they will be charged for the product upon renewal and when the money will be taken
- where the price will be higher on auto-renewal, not giving the impression that the initial price represents a saving by comparison, and

- contacting customers who have not used their product for a year to advise them of the fact and make their options clear, including the ending of their subscription.

Following the above undertakings, the CMA ended its investigations into the anti-virus sector.

Why is this important?

The CMA's actions show clear intent to crack down on automatic renewals that are not compliant with consumer protection law. This is relevant to all businesses, not just those engaged in anti-virus software.

Any practical tips?

The undertakings give a clear indication of the types of steps the CMA expects companies to be taking when providing auto-renewals. Consider checking:

- the extent to which your consumers are subject to auto-renewals and whether there is a right to exit
- whether consumers are appropriately informed, and are aware, that their contract will auto-renew, the price (including any future increases to the renewal price) and when any payments will be charged, and
- if consumers are contacted where they have not used your product for over a year, and whether there are processes to advise them of this and make their options clear to them.

Summer 2021

Consumer

CMA continues consultation on potential harms caused by algorithms

The question

What competition and consumer harms are the Competition and Markets Authority's (**CMA**) finding in the operation of algorithms, and how is it seeking to address these?

The key takeaway

Following the conclusion of the consultation, the CMA is now looking into ways in which it can mitigate and remedy the harms it outlined in its earlier research paper on algorithms.

The background

The CMA has been investigating algorithms and how they can reduce competition and harm consumers for some time, having published a research paper on the topic in January 2021. The paper sought to analyse algorithms and their impact from a competition and consumer perspective. The harms identified include:

- personalisation (which is hard to detect by consumers or others and targets vulnerable consumers)
- exclusion or reduction of competition through algorithms (eg through preferencing your own services over others), and
- failure to prevent harm through the overseeing of platforms using algorithms.

In conjunction with the review, the CMA called for evidence in a consultation. It published the evidence that was submitted in June 2021.

The development

Most of the 35 respondents agreed with the CMA's assessment of the potential harms, but did note that: there are several nuances to the harms identified; some harms were missing (including use of consumer data); and there is a need for legal analysis, empirical evidence, and a proportionate approach for any investigation into the harms in the future.

The CMA will publish its next steps and potential future intervention soon, once all the evidence has been reviewed. However, as highlighted in the research paper, potential future steps being considered by the CMA include:

- ordering firms to disclose information about their algorithmic systems to consumers

- requiring a firm to disclose more detailed information to approved researchers, auditors and regulators, and to cooperate with testing and inspections. Cooperation may involve providing secure access to actual user data, access to documentation and internal communications on the design and maintenance of the algorithmic system, and access to developers and users for interviews
- imposing ongoing monitoring requirements and requiring firms to submit compliance reports, providing ongoing and continuous reporting data or API access to key systems to auditors and regulators
- requiring firms to conduct and publish algorithmic risk assessments of prospective algorithmic systems and changes, and/or impact evaluations of their existing systems, and
- ordering firms to make certain changes to the design and operation of key algorithmic systems and requiring them to appoint a monitoring trustee to ensure compliance and that the necessary changes are made.

The CMA has also flaunted the possibility of further investigations before any of the above steps are taken, so that it can better understand the use of algorithms in various marketplaces and what might therefore be appropriate given their use in various contexts.

Why is this important?

Algorithms are near ubiquitous in most technologies and services these days and are an integral part for many making their services as valuable as they are (such as Google Search). The CMA's consultation shows clear intent in regulating the algorithm space, and to provide further transparency in how they work, which raises challenges for those who want to keep them proprietary and confidential. It is clearly in the interests of all affected parties to ensure that they follow the developments in this space and to feed into any possible future investigations so that their position can be better understood and any regulations shaped in a way which both protects consumers whilst also allowing algorithms to be used in the best, most useful way possible.

Any practical tips?

- If your business runs on or utilises algorithms, follow the CMA's investigations closely
- Consider engaging in early dialogue with the CMA to help ensure future compliance and to limit any potential exposure of proprietary technologies and/or confidential information, and
- Consider if any immediate steps need to be taken with the design and operation of your algorithmic systems in order to get ahead of the regulatory requirements (and likely investigations) which will inevitably follow in this space.

Summer 2021

Advertising

Sexualisation and objectification in advertising

The question

Where does the ASA draw the line between "sexy" advertising and sexual objectification?

The key takeaway

Sexual imagery is allowed in advertising – just make sure you don't cross the line into sexual objectification. Warning bells should go off if you're intending to use disembodied bodies in your ad, or sexualised imagery in a situation not relevant to the product.

The background

In February 2021 the Committee of Advertising Practice (**CAP**) published an advice note on the compliance risks associated with treating a person as an object of sexual desire in marketing communications.

Sexual objectification is not allowed by the ASA and is in direct contravention of both the CAP and BCAP Codes. The advice note highlights a general rule that if an ad is likely to have the effect of objectifying someone by using their physical features to draw attention to an unrelated product, then this has the potential to lead to harm, such as body image issues, as well as the potential to negatively impact a person's mental health. However, the note does point out that sexual imagery itself does not necessarily constitute objectification and points to certain complaints whereby the ASA found that whilst the ads featured potentially "distasteful imagery" they fell on the right side of the line between "sexy" and "sexist".

The development

The advice note helps to clarify the distinction between what is "sexy" without being classed as objectification and what would stray over the line into being sexist. It does so by highlighting certain upheld rulings across two key areas: (i) disembodied bodies (ie those ads that reduced a person to a body or a body part); and (ii) appropriate dress (ie the appropriateness of clothing, or lack thereof, is dependent on the situation and how the person in little clothing is portrayed).

Disembodied bodies

The note details several rulings that help to illustrate what would be objectification.

The ruling on Lewis Oliver Estates Ltd related to an ad for an estate agency which featured the image of a topless man's torso and thighs with the tagline "wow what a package" placed over the man's crotch. The ASA stated that the image in no way related to the services being

advertised and that, while the pose was “mildly suggestive”, the man was portrayed in such a way which invited viewers to focus on his body.

In the ruling on Silks (Glasgow) Ltd, a lingerie store, the ad featured an image of a woman wearing lingerie in a sexually suggestive pose. This, combined with the fact that the model’s head was not shown, led the ASA to rule that the image invited viewers to view the woman as a sexual object. The fact that the model was only wearing lingerie had no impact on the ASA’s decision because this was relevant to the business and the products being advertised.

The note further illustrates the fine line between compliance and non-compliance referring to a full-page print ad for a perfume. The ad featured a topless woman with a fully dressed man covering the woman’s breasts and stomach with his arms. The ASA did not consider this ad to breach the CAP Code due to the image being highly stylized, the woman’s face was visible, and she appeared confident, in control and unified with the man as a couple. It also considered the image to be typical of perfume ads and not out of place in magazines and newspapers aimed at general readers.

Dress appropriately

The note distinguishes that lack of clothing does not necessarily result in sexual objectification, which the ruling on Fontem Ventures BV (trading as Blu) highlights. The ad featured a naked woman positioned so that the top of her buttocks was visible as she looked back over her shoulder. The ASA considered that the tone of the ad was sensual and sexually suggestive to the point that some may find it distasteful, but that the ad was not sexually explicit. However, importantly, the ASA did not think that the ad portrayed the model as a sexual object and as such this was just on the right side of the line.

Conversely, in their ruling on Croftscope Ltd (trading as BOCA), the ASA determined that an advert for toothpaste, which featured the image of the body of a naked woman wearing only a pair of strappy heels, reclining in a chair with one leg placed on top of a table by the window and the other on the ground placed significant emphasis on the model’s body in a highly sexualised manner, therefore inviting viewers to view her as a sexual object.

The note also highlights that the appropriateness of the lack of clothing is also dependent on the situation. In its ruling on Meridan BP the ASA censured an ad for building products and materials which featured a woman with an exposed midriff and a tool belt. This was done on the basis that it was unlikely to be recognised as typical or appropriate attire in which to undertake building work, and that the sexualised image bore no relevance to the products being advertised and as such was sexually objectifying.

Why is this important?

The note helps to clarify what sexual imagery is acceptable, and what isn't, in advertising. The main theme is that advertisers should keep sexualised imagery relevant to the product in order to avoid complaints or negative rulings.

Any practical tips?

Don't put unnecessary focus on body parts and keep the use of sexual imagery relevant to the product or service being advertised. And consider yourself lucky if you're in the fashion or perfume industry – you're likely to have more leeway than if you're advertising building products.

Summer 2021

Advertising

Advertising cryptocurrencies – staying on the right side of the regulatory line

The question

What are the key issues to be alive to when advertising cryptocurrencies and NFTs?

The key takeaway

Be careful when advertising cryptocurrencies and NFTs and ensure that enough information is given to consumers on the technologies, how they work and the potential fluctuation in their value.

The background

In the past couple of years some cryptocurrencies like Bitcoin have reached dizzying monetary heights. The resulting spike in popularity has led to increased marketing of this emerging technology to a wider audience.

In response, the Advertising Standards Authority (**ASA**) published a guidance note in April 2021 advising crypto businesses on what they need to think about when it comes to advertising their digital assets.

The development

The ASA first notes that cryptocurrencies are currently not regulated by the Financial Conduct Authority (**FCA**), so any advertisements should not imply that they are. Even though platforms where these currencies are sold might be regulated by the FCA, care must be taken so that this distinction is made in any ads involving these platforms. The aim is that consumers clearly understand the lack of regulation around the cryptocurrencies.

The volatility of cryptocurrencies' value presents a difficulty in advertising. The ASA states therefore that advertisers must make clear that the value of investments is variable and, unless guaranteed, can go down as well as up. Consumers need to be made aware of the possibility of their investment losing value, as well as potentially increasing in value. The ASA also notes that small print within an ad disclosing this might not be enough to comply, ie clear signposting is needed.

The CAP Code also requires that advertisers explain products in ways that are easily understood by those they are addressing. Cryptocurrencies and blockchain can be very difficult to understand for the average consumer, so advertisers need to make sure any advertisements are clear on what they are and how they work.

The ASA also discusses the emergence of NFTs, or non-fungible tokens, which have also risen in popularity recently. NFTs are often sold in relation to digital artworks, and it needs to be made clear to consumers that they may be buying a method of tracking ownership of the artwork but might not include the ability to share or commercialise the artwork.

Why is this important?

The complexity and novelty of new technology – especially one which carries risk and which many consumers do not fully understand - raises challenges in the communication of specifics and functionality, which leaves the door wide open for unintentional non-compliance. The ASA's new guidance note is a solid starting point for staying on the right side of the regulatory line.

Any practical tips?

Don't forget the ASA's guidance when advertising cryptocurrencies and/or NFTs. Above all, given the complexities, err on the side of caution by being as clear as possible when explaining how cryptocurrencies and/or NFTs work.

Summer 2021

Advertising

Ofcom consults on advertising on video-sharing platforms

The question

What measures are likely to be put in place on the advertising of video-sharing platforms (**VSPs**), like YouTube and TikTok?

The key takeaway

With heightened focus on the safety of users of VSPs, changes are likely to be made to the advertising standards for VSPs. Ofcom has launched a consultation, which spans proposed guidance and required monitoring measures.

The background

In late 2020, certain changes to the Communications Act 2003 (the **Act**) came into effect. The Act implemented several regulatory requirements for VSPs based in the UK, and obligated Ofcom to ensure their enforcement. Ofcom is therefore responsible for the regulation of VSPs, including advertising on such services.

The purpose of these amendments is to protect VSP users from harmful content, including several specific requirements relating to potential harm from advertising on these platforms.

The development

Ofcom has sought to reflect the distinction between two different types of advertising in the Act, namely advertising under the control of the VSP provider and advertising embedded within shared content uploaded onto the VSP (ie not under the control of the VSP provider).

For advertising controlled by the VSPs, VSPs have a legal responsibility to ensure that the ads meet certain standards. Ofcom proposes that for the day-to-day administration of advertising the Advertising Standards Authority (**ASA**) will be designated to fulfil this role, with Ofcom as the statutory back-stop regulator. Additionally, Ofcom is proposing the addition of a VSP annex to the CAP Code.

For advertising not controlled by VSPs, VSPs are required to take appropriate measures to protect their users, which will be enforced by Ofcom. Ofcom is proposing guidance on compliance, which will contain information covering the meaning of “control” and how to comply with the non-controlled-VSP rules.

In summary, Ofcom's consultation covers five primary areas:

1. Proposed guidance surrounding how Ofcom will determine if a VSP has control over advertisements on their platform
2. Proposed guidance surrounding how Ofcom will seek to regulate the circumstances where VSPs have been found to be in control of advertisements on their platform
3. The involvement of the ASA as a co-regulator where VSPs have been found to control advertisements on their platform
4. The proposal for measures to be taken by VSP providers in order to appropriately monitor and regulate advertisements not controlled by the VSP, and
5. Proposed guidance on how Ofcom will seek to regulate non-VSP controlled advertisements.

Why is this important?

Earlier this year in May, the UK government published the draft Online Safety Bill (**the Bill**). The Bill aims to establish a new regulatory framework capable of tackling harmful online content. When the Bill enters into force, it will supersede many of the provisions of the Act and repeal those dedicated to advertising requirements.

In publishing this Bill, the UK government has also stated that, in the context of advertisements, the regulation of VSPs shall continue to fall to the responsibility of the ASA and Ofcom.

Through the creation of these proposals Ofcom has pre-considered and factored in the above, providing these amendments in compliment of the future regulation of the subject and potential provisions that may arise. Ofcom is seeking to adopt a collaborative approach allowing providers and regulators to work together ensuring that the advertising standards will be held in the best interests of both VSP users and the public.

Any practical tips?

The deadline for responding to the consultation is **28 July 2021.** If you're a VSP, keep a close eye on developments, noting that a summary of Ofcom's findings is due shortly after the consultation end date.

Summer 2021

Advertising

ASA research into racial and ethnic stereotyping in ads

The question

To what extent do racial and ethnic stereotypes, when featured in ads, contribute to real world harms and how might this type of stereotyping be regulated in the future?

The key takeaway

The Advertising Standards Authority (**ASA**) is looking to gather evidence on racial stereotypes in ads, what real world harm they result in and how best to combat these harms.

The background

Following the tragic death of George Floyd in May last year and the resultant rise of the Black Lives Matter movement, racial stereotypes and other challenges facing ethnic groups has been pushed into mainstream consciousness. This has prompted a serious review of various aspects of modern-day life, from the workplace to sports fields. These reviews have assessed how race can affect the treatment of people and the role racial stereotypes play within that. The current willingness of society to reflect on the impact of racial prejudices and ethnic stereotypes is unprecedented and is prompting many institutions to change their processes to combat the effects these have on people and help limit the harm to individuals subject to those racial stereotypes. This willingness of businesses as well as institutions to critically assess themselves regarding racial and ethnic stereotypes has been shared throughout different industries. However, it has been particularly pronounced within advertising due to its pervasive nature in modern life.

An example of the challenges faced by advertisers can be seen in Sainsbury's last Christmas campaign, in which an ad depicting a black father singing the "Gravy Song" received a tirade of racist comments on social media culminating in some consumers threatening to boycott the supermarket. These draconian attitudes towards race shown in the backlash to the ad can result in harm to those people subject to the perceived stereotype within the ad and effect people's day to day lives.

The ASA is aware of the potential harm to individuals and is committed to limiting that harm, which has prompted its research into the subject matter to assist in future regulation.

The development

On racial and ethnic stereotypes, the ASA has not been shy of interventionist measures. For example, in 2017 it banned an online ad for Paddy Power which contained a tag line relating to the skin colour of the boxer Floyd Mayweather. The ad was deemed to insinuate that gamblers should bet on the outcome of a bout with reference to the fighter's skin colour.

This appetite to critically assess ads in relation to racial and ethnic stereotypes, combined with the recent increase in racial awareness from the public, has led the ASA to put the whole advertising industry under the microscope. As such, they are requesting quantitative and qualitative evidence relating to the real-world harm racial and ethnic stereotyping in adverts can cause. They are particularly interested in:

- the depiction of race and ethnicity in advertising, including examples of racial and ethnic stereotypes
- how the issues of objectification and sexualisation relate to race or ethnicity in advertising
- how particular cultures, or racial and ethnic groups with religious affiliations, are portrayed in advertising, and
- the use of humour relating to race or ethnicity in advertising.

This call for evidence follows the Committee of Advertising Practice's launch of a consultation on the introduction of new rules on harm and protected characteristics and the results of the ASA's collated evidence will inevitably feed into this consultation.

Why is this important?

The evidence received by the ASA should enable them to better understand the current issues surrounding race in 2021. While also providing them with an awareness of the specific harms that can relate from racial and ethnic stereotypes in ads and in turn enable them to mitigate those harms where possible. It is possible that the evidence will provide instances where individual ads, which appear be on the right side of the line in isolation, may be contributing to a cumulative effect of offence or harm on individuals. These outcomes will allow the ASA to gain a greater understanding of racial and ethnic stereotypes in advertising, enabling them to better police those stereotypes and reduce the harm to individuals.

Any practical tips?

- Review any ads featuring racial or ethnic stereotypes, even if inadvertent, and ensure that they comply with both the regulations and with general good taste.
- Look out for the ASA's output from its investigations, which are expected later in the year once the review has concluded.

Summer 2021

Advertising

How not to run an influencer prize promotion

The question

If you're an influencer with a substantial following, and you plan on running a free prize draw, how careful do you need to be in selecting the winner from the (likely) huge number of responses?

The key takeaway

Influencers have to follow the rules like everyone else. Just because you're an individual doesn't mean you don't need to think very carefully about how you administer a prize promotion in a way which meets the requirements of the CAP Code. There is a lesson for brands in here too. If you engage influencers to run promotions for/with you, you need to ensure they know exactly what they need to do to – not only from an advertising disclosure perspective, but also from an administrative perspective.

The ad

In September 2020, Love Island alumni Molly-May Hague offered one of her five million Instagram followers the opportunity to win almost £8,000 of designer goods. To be in with a chance to win, Instagram users had to subscribe to Ms Hague's Instagram and YouTube accounts, "like" the Instagram post in question, tag a friend, and follow her tanning brand "Filter By Molly-Mae" on Instagram. The competition post attracted around 1.2 million likes and almost three million comments. The CAP Code provides that *"promoters of prize draws must ensure that prizes are awarded in accordance with the laws of chance and, unless winners are selected by a computer process that produces verifiably random results, by an independent person, or under the supervision of an independent person"* (rule 8.24).

The complaint

Following the close of the competition, the ASA received over ten complaints from individuals who questioned whether all the entrants were included in the final prize draw. They challenged (i) whether the promotion was administered fairly, and (ii) whether the prize was awarded in accordance with the laws of chance.

The response

Ms Hague responded to the allegations stating that the post didn't incentivise any engagement with a brand of product and therefore didn't come under the CAP Code's rules on promotions. Despite this, Ms Hague qualified that during the process of selecting a winner, she had instructed a member of her team to pick a group of participants at random, and under the

supervision of an independent person. Due to the high number of entrants prohibiting the use of computer software, the profiles were manually selected from a hat and verified as meeting the entry requirements. From the pool of 100 randomly selected entrants, Google's number picker was used to select a final winner. Ms Hague claimed that she had no part in the selection process and that the independent person who oversaw the process had no affiliation with either her management team, the brand or the promotion. She was also candid in admitting that the response to the promotion had been *"overwhelming and unexpected"*, and that she had endeavored to deal with it in the best way possible.

The development

Despite her explanation, the ASA noted that, following the close of the competition, Ms Hague had uploaded an Instagram story which clarified that the winner had been selected from a smaller shortlist of 25 profiles – the ASA was understandably *"concerned by the inconsistencies in the information provided"*. Ms Hague had failed to provide evidence that this smaller group had been chosen randomly using computer software or that the prize was awarded in accordance with the laws of chance and by an independent person or under the supervision of an independent person. The ASA considered that the characteristics of the post – namely its time limited nature, and the liking, tagging and subscribing – were indicative of a prize draw promotion and consequently brought under the scope of the CAP Code. Irrespective of Ms Hague's expectations of how many would respond to the post, the ASA considered that she should have anticipated the high response relative to her overall following. Consequently, the ASA upheld both complaints and found that the promotion has not been administered fairly.

Why is this important?

The ASA warned Ms Hague that she must ensure that any future promotions were administered fairly, and prizes awarded only in accordance with the laws of chance, under the supervision of an independent person. The results of this ruling have been widely publicised in the national press and some entrants were vocal in their criticism of the promotion, calling it "unfair" and a "scam". The case therefore serves as a timely reminder of the importance of adherence to the advertising rules, particularly to influencers and/or content creators but also the brands who may work with them on these types of promotions.

Any practical tips?

All promotions run via social media channels should be conducted very carefully and in compliance with the CAP Code. And always remember to watch your influencers, both from an advertising disclosure perspective and, as highlighted by the Molly-Mae case, the proper administration of those promotions.

Summer 2021

Advertising

#ad your advertising posts on social media

The question

How much more reminding do influencers, and the brands working with them, need to ensure that all social media posts which advertise products or services are tagged with #ad?!

The key takeaway

The ASA's ruling on Select Fashion is yet another reminder for both influencers and marketers to properly tag their social media posts with #ad. A brand can't simply rely on its contract with an influencer to absolve itself of responsibility and claim an omission is beyond its control – engagement is the key, ideally by marketing teams monitoring influencer activity to ensure that their influencers really understand what they need to do to comply with the rules on advertising disclosure.

The ad and the response

Influencers Mandi and Anna Vakili made two posts on their respective Instagram accounts, the first one featuring an image of Mandi and Anna sitting on a bed. Text caption underneath said: "*It's been a crazy year! But we have to focus on the positive moments, and me and Anna are over the moon about having a collection with @selectfashion…I've worked with them for a long time since Anna came from the island … Me and @annavakili_had so much fun working together and with @selectfashion team on this edit … Set your alarms for 7pm and head over to @selectfashion website or pop in store to check out our collection*". The second post yet again featured the sisters with the caption "*Same but different @selectfashion*" with a black heart emoji. A complaint was made alleging that the posts were not obviously identifiable as marketing communications and did not make clear their commercial intent.

The influencers responded by providing copies of their commercial agreements with Genus UK Ltd, trading as Select Fashion, which stipulated that the marketing posts were to be correctly tagged and identified as being part of a commercial arrangement. Select Fashion argued that the omission was beyond their control, and the influencers noted that the omission was an error, and this had been corrected, and the brands involved will be credited appropriately in future.

The decision

The ASA initially noted that the agreements required that all posts were to be properly tagged and that a representative from Select Fashion had to approve any posts before they are

published, being able to request reshoots if needed. Select Fashion were also to be noted as a business partner and tagged in the caption.

In their view, these factors established that Select Fashion had enough control over the content of social media posts, in conjunction with a payment arrangement, for them to be considered marketing communications falling within the remit of the CAP Code. This meant that the posts had to be obviously identifiable as ads.

Although the first ad referred to the clothing collection with Select Fashion, the second ad showed the sisters wearing outfits from the collection, and that Select Fashion were indeed tagged in both posts, this was insufficient to ensure the posts were obviously identifiable as ads. Further identifiers were needed to be placed upfront, such as #ad, making it clear to viewers that the posts were ads. Because of this, the ASA considered that the posts breached CAP Code rules 2.1 and 2.3.

Why is this important?

The ruling reminds both influencers and marketers that advertising posts must be labelled appropriately as ads, and that a simple omission will not excuse any non-compliant posts from ASA action.

Any practical tips?

It's simple – ensure your influencers always use #ad in all their advertising posts on social media. One simple step could be to ask your marketing team to sign up to the relevant social media accounts and actively monitor the posts – and if the team sees omissions from an ad disclosure perspective, asking the influencer to remedy immediately.

Summer 2021

The view from Asia

Tackling the issue of "doxxing" in Hong Kong

The question

What legislative changes are being considered in Hong Kong to address the rise in doxxing cases and the resulting harm caused to the affected data subjects?

Key takeaway

The Hong Kong Government has released significant proposals before the Legislative Council to criminalise unlawful doxxing acts and enhance the Privacy Commissioner for Personal Data (**PCPD**)'s capabilities to combat doxxing.

Background

Doxxing describes the act of unlawfully revealing personal information of a third party or his/her family to the public – usually through online platforms – without prior consent and with the intention to humiliate, intimidate, or cause psychological or bodily harm to the victims.

In recent years, Hong Kong has seen a rapid surge in doxxing activities. Between June 2019 and April 2021, the PCPD received nearly 6,000 doxxing-related complaints, and close to 1,500 cases have been referred to the police for criminal investigation. However, to date, there have only been a few convictions; although, in the event of a conviction, a custodial sentence is a real possibility.

Under section 64 of the Personal Data (Privacy) Ordinance (the **PDPO**), the conviction threshold requires the act to be "without the data user's consent" (such as improper disclosure of medical records of a data subject without the consent of the hospital as a data user). However, with the development of the internet and social media, most doxxing acts are recklessly dispensed, and repeatedly reposted online, making it difficult for law enforcement to trace and identify the data user and ascertain whether there has been any consent provided.

Additionally, under the current regime, the PCPD is required to refer cases to the Police and the Department of Justice for investigation and prosecution, which can delay the handling of doxxing cases.

The development

In the bid for stronger enforcement and protection over online data privacy, on 17 May 2021 the Government released a discussion paper containing proposed amendments to the PDPO before the Legislative Council (the **Proposed Reform**):

1. **Adding a "doxxing" offence under section 64 of the PDPO** which requires a person to obtain the data subject's consent and extend the protection to the data subject's immediate family members. The penalty for the existing offence under section 64 will tally with the new doxxing provisions. Any person who contravenes the doxxing offence is liable upon conviction to a fine of HK$1,000,000 (c. £93,000) and to imprisonment for up to five years, or on summary conviction to a fine of HK$100,000 (c. £9,300) and to imprisonment for up to two years
2. **Empowering the PCPD to carry out criminal investigations and initiate proceedings in its own name** to allow more effective collection of evidence for prosecution and to expedite the processing of doxxing cases
3. **Empowering the PCPD with statutory powers to demand rectification of doxxing contents** by serving a "Rectification Notice" on any person who provides services in Hong Kong to Hong Kong residents (including online platforms) and requiring the removal of the information unlawfully disclosed in an expeditious manner, and
4. **Empowering the PCPD with the power to apply to court or seek an injunction** if they believe that there is very likely to be large-scale or repeated doxxing acts against specific persons or groups.

The Proposed Reform will be formalised in an amendment bill (the Personal Data (Privacy) (Amendment) Bill 2021) (the **Amendment Bill**), which will be gazetted on 16 July 2021 and introduced into the Legislative Council for first and second readings on 21 July 2021.

Why is this important?

The Proposed Reform shows the Government's desire to combat the effective weaponizing of personal data. Subject to proper safeguards, the greater power to be conferred on the PCPD should help to expedite the processing of doxxing cases, improve the enforcement of doxxing offences and better safeguard the privacy interests of data subjects. The Proposed Reform is in tandem with the recent gazette of a three-phased new inspection regime under the Hong Kong Companies Ordinance, Cap 622, which aims to withhold certain personal information of directors and company secretaries from general public inspection to prevent the potential abuse of such data by eg doxxing.

Any practical tips?

Companies with an online geographical reach should keep informed of the upcoming implementation of the Proposed Reform and should be prepared for enhanced regulatory obligations coming into effect. As the Proposed Reform and the forthcoming Amendment Bill are yet to be finalised, the PCPD welcomes any views, proposals and recommendations that companies, or other stakeholders may have.

Summer 2021

The view from Asia

Singapore High Court denies first-ever private action brought under the PDPA

The question

What is the definition of "loss or damage", a threshold requirement which data subjects need to satisfy to pursue a right of private action under the Personal Data Protection Act 2021 (the **PDPA**)? Specifically, will emotional distress and/or loss of control over personal data suffered by data subjects fall within the definition of "loss or damage"?

The key takeaway

The Singapore High Court's decision to adopt a purposive and narrow interpretation of "loss or damage", which excludes emotional distress and loss of control over personal data, lowers the potential litigation risk arising from private actions under the PDPA by affected data subjects. They must now prove that the misuse of personal data results in financial loss, damage to property and personal injury, such as psychiatric illness, in order to pursue a private action.

Given the novelty and importance of the questions raised in the case, the respondent has since been granted leave to appeal to the Court of Appeal (Singapore's court of final appeal).

Background

Alex Bellingham (**Bellingham**), a marketing consultant, used personal data obtained from his former employers to market a new investment fund to Michael Reed (**Reed**). This prompted Reed, a client of Bellingham's former employers, to question how Bellingham was able to obtain his personal data. Reed subsequently joined Bellingham's former employers in court proceedings before the District Court for an injunction under the PDPA to restrain Bellingham from using, disclosing or communicating to any person, any personal data of Reed (alongside two other clients). The District Court granted Reed's injunction (but not Bellingham's former employers' application for the same as they were not the affected data subjects), which Bellingham subsequently appealed to the High Court.

Under the then-section 32 (now section 48O) of the PDPA, data subjects who suffer "loss or damage" directly as a result of contravention of specific sections of the PDPA have a right of private action to pursue monetary damages, injunctive relief and/or other remedies. However, as the PDPA does not define "loss or damage", the scope of the provision remained unclear until this decision.

The decision

In its decision on 25 May 2021, the High Court firstly found that Bellingham had breached Part IV of the PDPA by, among others, failing to obtain Reed's consent before using his name, email address and the fact that he was an existing investor of Bellingham's former employers to market investment services.

However, the High Court held that "loss or damage" must refer only to heads of loss or damage applicable to torts under common law – namely financial loss, damage to property and personal injury, including psychiatric illness. Broader concepts of emotional harm (such as humiliation, loss of dignity, injury to feelings and distress) and/or loss of control over personal data were not covered. On this point, the Court recognised that there is no general right to privacy under Singapore law, and they mainly relied on the statutory purpose and context of the PDPA to reach their decision.

On the facts, the High Court further found that Reed did not suffer any financial loss, psychiatric injury or nervous shock as a result of Bellingham's contraventions. As a result, the appeal was allowed, and the injunction was set aside pending the decision of appeal.

Why is this important?

This is the first ever decision by the High Court on the right and scope of a private action under the PDPA since its enactment in 2012. Of particular importance is the court's finding that the purpose of the PDPA was as much to enhance Singapore's competitiveness and position as a trusted business hub, as it was to safeguard individual personal data against misuse. The Court noted that the position in Singapore differed from the positions in other jurisdictions, such as the EU, where the data protection frameworks were driven primarily by the need to recognise the right to privacy.

Any practical tips

Where an individual cannot establish the threshold under section 32 (now section 48O) PDPA, remedies can still be sought through the Personal Data Protection Commission (**PDPC**), whose powers include giving directions to the infringer to (a) stop collecting, using or disclosing personal data; and/or (b) destroy all personal data collected in contravention of the PDPA. Regarding PDPC's regulatory powers, it has recently released a Guide on Managing and Notifying Data Breaches, with key information on the mandatory data breach notification obligations introduced under the newly amended PDPA, including the criteria, timelines and information to be provided when notifying data breaches. The Personal Data Protection (Notification of Data Breaches) Regulations 2021 sets out comprehensively such information, including the various classes of personal data deemed to result in "significant harm" to affected individuals if compromised in a data breach.

Summer 2021

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

Temple Circus99
Temple Way
Bristol BS1 6LW
T +44 20 3060 6000

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

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

DM 35216191

RPC