

September 2017

Page

- 1. Limitation clauses**
Unclear limitation clauses – Royal Devon and Exeter NHS Foundation Trust v ATOS IT Services UK Ltd [2017] EWHC 2197 (TCC) 3
- 2. Contractual discretion**
Rationality in exercise of discretion – Watson and others v Watchfinder.co.uk Limited [2017] EWHC 1275 5
- 3. Exclusion clauses**
Excluding liability for negligence was reasonable – Goodlife Foods Ltd v Hall Fire Protection Ltd [2017] EWHC 767 (TCC) 7
- 4. UCTA**
African Export-Import Bank v Shebah Exploration & Production Company Ltd 9
- 5. Contractual interpretation**
Interpretation of uncertain provisions – Kitcatt and others MMS v UK Holdings Ltd and others [2017] EWHC 675 11

Supreme Court decision on conflicting contractual standards – MT Højgaard A/S v E.On Climate and Renewables UK Robin Rigg East Ltd [2017] UKSC 59 13

GB Building Solutions Ltd (in administration) v SFS Fire Services Ltd (t/a Central Fire Protection) 2017 EWHC 1289 15
- 6. Assignment**
Effective assignment and notice – General Nutrition Investment Company v Holland and Barrett International Ltd and another [2017] EWHC 746 (Ch) 17
- 7. Service provider liability**
EU proposal provides clarity on incoming requirements for digital service providers 19

The purpose of these snapshots is to provide general information and current awareness about the relevant topics and they do not constitute legal advice. If you have any questions or need specific advice, please consult one of the lawyers referred to in the contacts section.

8. Terms and conditions

Thousands agree to clean loos and hug stray cats for free WiFi 21

9. Data protection

Government publishes the Data Protection Bill 23

Data Protection Working Party adopts Opinion 2/2017 on data processing at work 25

ICO publishes updated Subject Access Code of Practice 27

ICO fines Boomerang Video Ltd for failure to prevent cyber attack 29

ICO issues fines for emails asking customers to change marketing preferences 31

10. ASA

New BCAP guidance on advertising of high fat, salt and sugar (HFSS) products 33

ASA Ruling on John Lewis Partnership plc t/a John Lewis – misleading pricing of products advertised as free in bundle promotions 36

Inspop.com Ltd t/a Confused.com (5 July 2017) – ASA decision on “No.1 claims” 38

ASA publishes report on gender stereotyping in advertising 41

ASA Ruling on SKY UK Ltd t/a Sky – “Super Reliable” broadband 43

ASA Ruling on British Telecommunications plc t/a BT – prominence of qualifications to headline claims 45

Limitation clauses

Unclear limitation clauses – Royal Devon and Exeter NHS Foundation Trust v ATOS IT Services UK Ltd [2017] EWHC 2197 (TCC)

The question

Will an ambiguous limitation of liability clause be valid and enforceable?

The facts

Royal Devon and Exeter NHS Foundation Trust (the **Trust**) entered into a contract for the provision of a computer system by ATOS IT Services UK Ltd (**Atos**). However, the Trust claimed that there were defects in the system provided, and that Atos had failed to remedy them, and proceeded to terminate the contract. The Trust claimed damages and argued that the limitation of liability provisions were unenforceable as they were ambiguous and uncertain.

Atos' aggregate liability was stated not to exceed: "*for claims arising after the first 12 months of the Contract, the total Contract Charges paid in the 12 months prior to the date of that claim.*"

The Trust argued that this made it unclear whether there was a single limitation cap or a separate cap for each claim. Atos argued the reference to "claims" should be read as "*claim*".

The decision

The Court rejected the Trust's argument that the provision was incapable of being construed and therefore unenforceable. The Court applied usual contractual interpretation principles (*Arnold v Britton*, *Rainy Sky* and *Wood v Capita*). The Court must ascertain the objective intentions of the parties by reference to what a reasonable person, having the background knowledge, would have understood the agreement to mean in the relevant factual and commercial context.

There were two competing interpretations and so it was open to the Court to prefer the option that made commercial sense, this case that the parties had intended an aggregate cap on liability.

The Court also noted it will try and give effect to terms agreed by parties where possible, and will be reluctant to decide a contractual provision is void for uncertainty (*Whitecap Leisure v Rundle* [2008] EWCA Civ 429).

Why is this important?

This decision again highlights the importance of precise drafting, particularly limitation clauses. It is also a good example of contractual interpretation where the Court prefers the interpretation that makes commercial sense (ie a *Rainy Sky* approach).

Any practical tips?

Be careful with your drafting! Take particular care with layered limitation clauses. Continue to bear in mind that recitals and acknowledgements within an agreement may assist the Court with identifying the commercial context.

Contractual discretion

Rationality in exercise of discretion – Watson and others v Watchfinder.co.uk Limited [2017] EWHC 1275

The question

What limits apply when an option is subject to the board's consent?

The facts

Watchfinder (**WF**) entered into a services agreement with another Adoreum Partners (**AP**) and granted options over its own shares to three of AP's directors. The option agreement provided: *"The option may only be exercised with the consent of a majority of the board of directors of the Company."*

When the directors attempted to exercise their share options, WF refused to issue the shares, on the basis that its board of directors did not consent. The directors claimed for specific performance. WF argued that the option gave the board an unconditional right to reject any exercise of the share options.

The decision

The Court held that the clause in the option agreement could not be interpreted as an unconditional right to reject any exercise of the options. Otherwise the options, which were part of the overall deal, would be worthless – this was against commercial common sense.

The provision could not be disregarded entirely and, although unusual, it must have been intended to impose some form of restriction on the options.

The Court held that, as a matter of construction or implication, the board had a duty to exercise its discretion over the option in a way which was not arbitrary, capricious or irrational in the public law sense (see *Braganza v BP Shipping [2015] 1 WLR 1661*). This must involve a proper process, taking into account the relevant matters and not irrelevant matters, and without reaching a decision no reasonable board could have reached.

In this instance, there had been no proper exercise of discretion. There had been barely any considered exercise of discretion – there were no discussions, relevant matters had not been considered, the board wrongly thought it had an absolute veto, and the decision was arbitrary.

Why is this important?

This case shows the reluctance of the Court to allow an absolute discretion, particularly where this would result in an uncommercial outcome, as well as the importance the Court places on proper process and how any contractual discretion is exercised.

Any practical tips?

Clearly identify provisions in an agreement where discretion may be exercised (e.g. discretion, election, consent, etc.) and state whether this will be sole/absolute, reasonable, etc. Even “absolute” contractual discretion is subject to proper process (considering relevant matters and disregarding irrelevant matters) and must not be not arbitrary, capricious or irrational. Consider stating what process will be followed and what matters will be taken into account.

At the point discretion is being exercised, ensure the decision makers know what they must do, that contractual/proper processes are followed and record a (rational or reasonable!) basis for the decision.

Exclusion clauses

Excluding liability for negligence was reasonable – Goodlife Foods Ltd v Hall Fire Protection Ltd [2017] EWHC 767 (TCC)

The question

Can a widely-drawn exclusion of liability which excludes liability for all negligence be reasonable under the Unfair Contract Terms Act 1977 (UCTA)?

The facts

Goodlife contracted with Hall Fire to design, supply, install and commission a fire detection and suppression system at Goodlife's frozen food production factory. A fire broke out at the factory, which Goodlife claimed led to £6 million of property damage and business interruption losses. Goodlife claimed that Hall Fire was liable for the losses caused by the fire, as it happened as a result of a failure or malfunction in the fire suppression system. The claim was in negligence rather than breach of contract for limitation reasons.

Hall Fire sought to rely on the exclusion clause contained in clause 11 of their standard terms and conditions, which stated that:

“We exclude all liability, loss, damage or expense consequential or otherwise caused to your property, goods, persons or the like, directly or indirectly resulting from our negligence or delay or failure or malfunction of the systems or components provided by us for whatever reason “.

Goodlife challenged the incorporation and enforceability of clause 11.

The decision

The Court decided that:

- the clause was not particularly unusual or onerous, but in any event it had been sufficiently drawn to Goodlife's attention. Goodlife had the opportunity to read the terms and conditions and it has access to appropriate advice
- the court agreed with Goodlife that the exclusion did purport to exclude liability for personal injury or death (which is not permitted under section 2(1) UCTA). The question was then whether this rendered the whole exclusion clause unreasonable and of no effect
- Goodlife tried to rely on the Court of Appeal decision in *Stewart Gill v Horatio Myer [1992] EWCA 6* as authority that severance of the offending part of the clause was not

permissible. However, the Court distinguished *Stewart Gill* and relied instead on the Court of Appeal decision in *Troxel Products Ltd v Merrol Fire Protection Engineers*, which held: “[I]f part of a term is ineffective by reason of section 2(1), the remainder can nevertheless be upheld as reasonable”. The Court stated (obiter) that it would have found, if necessary, that the clause could not have been severed and so would have been unreasonable

- Goodlife further submitted that clause 11 was unreasonable because its scope was extremely wide and therefore Goodlife received very little benefit/protection.

Interestingly, whilst the Court accepted the clause was wide, it considered this was a fair allocation of risk between parties of equal size and bargaining power. This was particularly the case where Goodlife was likely to have its own insurance and, if there was a shortfall, it could have protected itself by additional insurance (Hall Fire offered to arrange cover for an additional payment within its terms). Goodlife was not being deprived of all recourse or being left with an insurable risk.

Why is this important?

This case demonstrates that Courts will not necessarily find widely drafted exclusion clauses to be unreasonable under UCTA and how the Courts will interpret broad exclusions of all negligence.

It also shows that the availability of other remedies or recourse, including insurance, will be relevant to whether the exclusion is reasonable.

Any practical tips?

Regardless of the Court's decision to uphold Hall Fire's exclusion clause, best practice is to expressly carve out matters that cannot be excluded/limited (e.g. death/personal injury caused by negligence, fraud, etc.). Exclusions/limitations should be divided into separate clauses/sub-clauses so they are severable if necessary. Ensure there are other effective remedies available, whether within the agreement or externally (e.g. insurance), particularly where exclusions apply.

UCTA

African Export-Import Bank v Shebah Exploration & Production Company Ltd

The question

What does “*deals on the other's written terms of business*” in section 3 of the Unfair Contract Terms Act 1977 really mean? Put another way, when are standard terms subject to the UCTA reasonableness test?

The facts

The claimants were the lenders under a loan agreement for \$150m. The defendants defaulted (save for one \$6m repayment) but contended they were entitled to set off their counterclaims against their accepted liabilities to the claimants under the facility agreement. The claimants argued that the defendants had no right of set-off as the facility agreement contained provisions expressly excluding any right of set-off. The defendants argued that they were dealing on the claimants' “*written standard terms of business*” within 5.3 UCTA, such that the claimants could not rely on the set-off provisions except in so far as that provision satisfied the requirement of reasonableness.

The decision

The Court of Appeal summarised the relevant law around reliance on section 3 UCTA. The party relying on a term must establish that: (i) the term is written; (ii) the term is a term of the business; (iii) the term is part of the other party's standard terms of business; and (iv) the other is dealing on those written terms of business. To do this, the party must show that the other party “habitually” uses those terms of business. Longmore J also held that: “*it is relevant to inquire whether there have been more than insubstantial variations to the terms which may otherwise have been habitually used by the other party to the transaction. If there have been substantial variations, it is unlikely to be the case that the party relying on the Act will have discharged the burden on him to show that the contract has been made 'on the other's written standard terms of business'*”.

There was: “*no requirement that negotiations must relate to the exclusion terms of the contract, if the Act is not to apply*”.

Why is this important?

Knowing when UCTA is, or is not, likely to apply can be critical, especially here where \$144m (the remaining loan) is at stake. The case shows that strong evidence is needed to show that

a complex agreement like a loan facility (even if based on an industry template) is made on a party's standard written terms.

Any practical tips?

Model form contracts and standard written terms are a common feature of the legal landscape. Be aware when such agreements are likely to be subject to UCTA and its reasonableness tests, and how far negotiations (whether or not relating to exclusion clauses) may start moving the UCTA dial.

Contractual interpretation

Interpretation of uncertain provisions – Kitcatt and others MMS v UK Holdings Ltd and others [2017] EWHC 675

The question

How will a Court interpret a clause that is uncertain or which appears to be unworkable?

The facts

Kitcatt sold their advertising agency to MMS (a subsidiary of Publicis Groupe SA). Under the sale agreement, Kitcatt was entitled to deferred consideration from the buyer. The amount depended on how Kitcatt performed following its merger with Digitas, a marketing agency within the Publicis group.

The sale agreement contained a warranty that MMA/certain persons were not aware:

“of any facts or circumstances that could reasonably be expected to have a material adverse impact upon the Operating Income and/or Revenue in 2012 or 2013 (being a reduction of at least 20% in the case of Operating Income and 10% in the case of Revenue) including, without limitation:(i) the resignation or expected loss of any client of Digitas; or (ii) any significant current or threatened litigation involving Digitas.”

Digitas lost a significant amount of work from a key client such that there was no deferred consideration. Kitcatt claimed for breach of warranty. MMS argued that the warranty provided no reference point which would allow a comparison to be made and so it was void for uncertainty. Also if the terms 'Operating Income' and 'Revenue' were given their defined meanings the clause became meaningless.

The decision

The Court found that the warranty was enforceable and had been breached. The key points were:

- the defined terms 'Operating Income' and 'Revenue' should not be applied. The parties intended the warranty to be enforceable and so the definition should not be incorporated. The definitions clause also provided a definition would apply, *“unless the context requires otherwise”*. The Judge noted *“a definition should be the servant of clarity, not a dictator of absurdity”*

- the Court applied *Arnold v Britton* and found that the relevant background knowledge and overall purpose of the clause included that the deferred consideration was partly dependent on Digitas' performance; and the warranty was an important part of the whole deal
- against that background, the Court could construe the clause as providing for a comparison between the information that had been disclosed and if the loss of the Digitas client had been disclosed. This gave effect to the purpose of the clause and made commercial common sense
- for these reasons, the Court rejected the argument that this was a meaningless clause to which it could not give effect – as had been held in *Prophet v Huggett [2014] EWCA Civ 1013*. The Court was reluctant to decide that an important clause, central to the deal, was unenforceable.

Why is this important?

This case is another good example of the Court being reluctant to find an important clause is void for uncertainty or because it is meaningless. Instead, the Court will seek to interpret the clause to give effect to its purpose and the objective intentions of the parties.

Any practical tips

Be careful with your drafting – especially on key provisions, e.g. payment terms. Double check definitions, especially when used in different parts of the agreement or for different purposes. If the drafting is unclear, the Court will construe the clause to reflect what it thinks the parties intended – so review recitals, etc.

Contractual interpretation

Supreme Court decision on conflicting contractual standards – MT Højgaard A/S v E.ON Climate and Renewables UK Robin Rigg East Ltd [2017] UKSC 59

The question

How will the Court resolve conflicting contractual standards, e.g. between general obligations and specified international standards?

The facts

MT Højgaard (**MTH**) was engaged by E.ON to design, manufacture and install the foundation structures for 60 offshore wind turbines for the Robin Rigg wind farm in the Solway Firth in Scotland.

The agreement contained various general obligations on the provision of the services, e.g. due care and diligence, works to be fit for purpose, and a 'design life' of 20 years.

The agreement also included detailed technical requirements, including that the design of the foundations be in accordance with an international standard published by Det Norske Veritas DNV – a leading classification and certification agency. The international standard DNV-OS-J101 (**J101**) was intended to deliver a service life of 20 years, subject to a small failure rate of less than 0.001%.

MTH performed the works in accordance with J101 but, due to an error in the international standard, the design did not have a service life of 20 years. The remedial work cost over €26 million and the parties disputed which of them was liable (or who bore the risk of an error in J101).

At first instance, the Technology and Construction Court (**TCC**) held that MTH was responsible for the necessary remedial work for breaching the 'fitness for purpose' obligation and the requirement the design life would be 20 years. The Court of Appeal overturned this decision but awarded E.ON only nominal damages of £10 (as the breach of a separate testing obligation would not have revealed the error in J101).

The decision

In a unanimous decision, the Supreme Court overturned the Court of Appeal and restored the earlier decision of the TCC. The key points were:

- the Court decided that there was a contractual duty that the design would give a lifetime of 20 years and this has been breached (whether this was expressed as a warranty that the foundations would have a lifetime of 20 years or as a contractual term that they had been designed to last 20 years was irrelevant to the outcome)
- the Court cited the case of *Cammell Laird v The Manganese Bronze and Brass Co [1934] AC402*, to confirm that a contractor is required to “*be bound by his bargain even though he can show an unanticipated difficulty or even impossibility in achieving the result desired*” – in this case relying on the J101 standard
- the Court held that where there are apparently inconsistent provisions or standards, rather than concluding that they are inconsistent, the proper interpretation is that the more higher standard must prevail and the less rigorous standard will be treated as a minimum requirement. In this case, the minimum requirement was J101 and MTH was held to the higher standards of a design life of 20 years.

Why is this important?

This Supreme Court decision confirms how the Courts will seek to resolve apparent conflicts between different contractual provisions/standards so as to give effect, if possible, to all parts of the contract. Instead of finding only one of the standards will apply, the Court can resolve the apparent conflict by applying the higher standard, with the other(s) acting as minimum requirements.

Any practical tips

Consider how general obligations and specific standards will interact and whether they are consistent. This can be particularly challenging for technical or complex projects (with detailed schedules – that may or may not be subject to legal review).

For example in software agreements, these issues are often avoided by not providing general obligations such as “satisfactory quality” or “fitness for purpose”, with standards being tied to performance in accordance with technical specifications (and often further qualified by “in all material respects”).

If there is a risk of inconsistency, consider provisions dealing with precedence/hierarchy of clauses, defining minimum requirements and/or acknowledging that compliance with technical standards will satisfy general obligations.

Contractual interpretation

GB Building Solutions Ltd (in administration) v SFS Fire Services Ltd (t/a Central Fire Protection) 2017 EWHC 1289

The question

When using defined terms in a contract, how careful do you need to be in their consistent application?

The facts

GB Building Solutions (a main building contractor) (**GB**) engaged SFS Fire Services (**SFS**) as a subcontractor to design and install a sprinkler system in a Manchester office development. The building was flooded before practical completion of the main contract works.

The case turned on whether the flooding took place before or after the “Terminal Date” – the practical completion of the subcontractor’s work. If before, GB would be barred from bringing an action because flooding was a “specified peril” and under the contract “specified perils” were covered by the contractor’s all risks insurance so the subcontractor would have no liability for remedying the damage. A core difficulty was that the definition of “Terminal Date” referred to the “date of practical completion of the Sub-Contract Works”. Note that “practical completion” here was lower case, whereas there was a definition of “Practical Completion” in the Schedule which was the “issue of the Certificate of Practical Completion pursuant to the Main Contract”. GB claimed that where “Practical Completion” was capitalised it was to be used as a defined term and, where it was not, practical completion was a matter of fact. SFS instead claimed that “Practical Completion” applied to all instances of practical completion.

The decision

The High Court applied the principles of construction as set out by the Supreme Court in *Wood v Capita* by which the court adopted “*the iterative process by which each suggested interpretation is checked against the provisions of the contract and its commercial consequences are investigated*”. As the judge stated, “*there may often be provisions in a detailed professionally drawn contract which lack clarity and the lawyer or judge in interpreting such provisions may be particularly helped by considering the factual matrix and the purpose of similar provisions in contracts of the same type*”. It followed that the judge preferred GB’s interpretation that the definition of Terminal Date in the Schedule referred to practical completion without capitalisation and the definition of Practical Completion in Schedule 1 did

not apply. Hence the flooding occurred after the Terminal Date and GB could bring its action for the flood damage.

Why is this important?

The case is a clean application of *Wood v Capita*, by which contractual interpretation is determined by a review of the contractual wording and the commercial consequences of each suggested interpretation. It also shows that particular care must be taken when drafting key definitions, and ensuring that they are applied consistently throughout.

Any practical tips?

Draft with clarity! If you use defined terms, use them consistently throughout. Otherwise the court may decide that the use or not of capitalised terms was intentional within the contract wording, and this might well prove costly.

Assignment

Effective assignment and notice – General Nutrition Investment Company v Holland and Barrett International Ltd and another [2017] EWHC 746 (Ch)

The question

What is the effect of not giving notice of an assignment of contractual rights?

The facts

The original licensor, GNIC Arizona, assigned its rights under a trade mark licence to General Nutrition Investment Company (**GNIC**). GNIC Arizona was then dissolved as part of a group restructure. The licensee and other contracting party was Holland and Barrett International Limited (**H&B**). H&B was not given notice of this assignment to GNIC and so there was only an equitable assignment of rights, not a legal assignment.

The licence agreement provided the licensor with certain termination rights and so GNIC (as the new licensor) served a number of notices on H&B purporting to terminate the licence agreement for breach, which H&B contested.

The decision

The Court considered whether there had been a valid assignment of the licence agreement from GNIC Arizona to GNIC. The Court confirmed there had been no legal assignment because H&B had not been provided with notice.

The Court held that the notices of termination served by GNIC, which was an equitable assignee only, were invalid because no notice of assignment had been given to H&B and so GNIC could not exercise those contractual rights in its own name. The key points were:

- the Court followed *Warner Bros Records v Rollgreen [1976] QB 430*, in which the Court of Appeal held that an equitable assignee could not exercise an option in its own name. The Court considered the same reasoning applied to the termination rights – these were substantive contractual rights, not merely procedural issues
- GNIC was attempting to change the contractual relationship through the termination, and H&B was entitled to know whether GNIC was able to exercise those rights. H&B did not know because no notice had been served
- the notice could have been provided by either GNIC Arizona or GNIC (although it was of course in GNIC's interests to ensure notice was given).

Why is this important?

Whilst an equitable assignment is binding as between the assignor and assignee, this case is an important reminder that notice should be provided to the other contracting party so that there is a legal assignment and the assignee can exercise its contractual rights against that other party.

Any practical tips

If the benefit of an agreement is being assigned, check the assignment clause to confirm this is permitted and ensure that notice of assignment is given to the other contracting party. Remember that an assignment will only transfer the benefit, not the obligations or burden, of the agreement.

Service provider liability

EU proposal provides clarity on incoming requirements for digital service providers

The background

The Network and Information Security Directive was passed in 2016 and is due to be implemented into UK law by 9 May 2018. It aims to increase the level of cybersecurity across the European Union. As part of that strategy, digital service providers (**DSPs**) will be required to manage the risks posed to the security of their network and information systems, and to notify the authorities in the event that incidents have a “substantial impact” on the provision of their service.

The Directive provides for the imposition of “dissuasive” penalties on DSPs who fail to meet their obligations.

The development

In September 2017 the European Commission published proposals which clarify the Directive's impact on DSPs.

DSPs must take “appropriate”, systematic measures to ensure the security of their network and information systems, taking into account incident handling, business continuity management, monitoring, and compliance with international standards. The proposals elaborate on how companies must take each of these elements into account, and provide a useful starting point for organisations who wish to start formulating compliant policies.

The proposals also lay down the criteria for determining if an incident is categorised as “substantial”. An incident will be substantial if it results in any of the following:

- the service provided by the DSP is rendered unavailable for more than 5,000,000 user hours, being the total number of users affected for a period of sixty minutes
- a “loss of integrity, authenticity or confidentiality” of data affecting more than 100,000 users
- an effect on public safety
- material damage of over €1,000,000 for at least one user
- an effect on at least two Member States.

If an incident is categorised as substantial, DSPs must notify it to their competent authority. If the DSP cannot show that it has effective security measures in place, a substantial incident is

likely to trigger a fine or other penalty. The nature of enforcement will be left up to Member States, and the UK has proposed incorporating the cybersecurity law into the same framework as the EU privacy law – which allows for fines of up to 4% of global revenue.

Why is this important?

These proposals provide greater clarity on a law which may have far-reaching impacts for DSPs. The underlying Directive creates an entirely new area of exposure for DSPs, which going forward will need to consider their relationship with the competent authority in addition to their customers. It is useful to have more detail on what will constitute “appropriate” measures under the legislation.

DSPs with a greater user-base should take particular note. A cyber incident at a large DSP, which may have millions of daily users, could easily trigger the proposed criteria to qualify as “substantial”.

Any practical tips?

Organisations should begin reviewing the measures they have in place to ensure the security of their network and information systems. It is essential that procedures are fully compliant with the law from its implementation date onwards. In the UK this will be on or before 9 May 2018.

Although the proposals are still in draft, they are unlikely to see any significant revisions before being published. Once the proposals are finalised, national legislation cannot impose more stringent requirements. Creating processes which comply with the EU law will therefore **at least** comply with requirements of the UK law when it comes into force, and may even go beyond it.

The last thing any organisation needs after suffering a major cyber incident is the threat of regulatory action, and the bad publicity and potential fines which go with it. Putting the right systems in place now will avoid these headaches, and make good commercial sense in any event.

Terms and conditions

Thousands agree to clean loos and hug stray cats for free Wi-Fi

The question

Does anyone read terms and conditions? And what might this mean for the concept of “unambiguous consent” under the GDPR?

The background

In an “experiment”, Purple, a Wi-Fi hotspot provider, added a clause to its terms and conditions that required 1,000 hours of community service from those who wanted free Wi-Fi. The definition for community service included the following tasks: “*cleaning portable festival lavatories, hugging stray cats and dogs and painting snails’ shells to brighten up their existence*”.

Only one person out of 22,000 noticed the clause, despite it being there for two weeks, and was awarded a prize for their attentiveness.

Purple’s experiment follows a similar stunt in 2014, when cyber security firm F-Secure included in their terms and conditions that users had to hand over their first-born child “*for the duration of eternity*” in exchange for free Wi-Fi. Six people signed up.

Why is this important?

Whilst Purple’s intention is not to enforce the community service, the experiment highlights an important issue for both users and Wi-Fi providers alike.

For users, the statement is clear – users are still not reading terms when they sign up to access free Wi-Fi and are unaware as to what they are agreeing to, how much data they are sharing and what license they are giving to providers. As the CEO of Purple observed, “*the experiment shows it’s all too easy to tick a box and consent to something unfair*”.

For Wi-Fi providers, the deadline to become General Data Protection Regulation (GDPR) compliant is looming large – all EU hotspot providers must meet the rules by 25 May 2018. One of GDPR’s headlines is the introduction of “unambiguous consent” which must be obtained before users’ personal or behavioural data can be used for marketing purposes.

In the light of GDPR, Purple has asserted that it is the first Wi-Fi provider to be compliant by modifying its privacy policy to be clearer, simpler and shorter, thereby encouraging users to

review the policy before accepting free Wi-Fi. Further, its “access journey” has been modified so as to provide better clarity as to how user data will be used, for what purposes and by whom. Finally, it has a “Profile Portal” so that users know that they can control how their data is being used.

Any practical tips?

For users of hotspots, it is imperative to read, read and read again the terms and conditions pertaining to the provision of goods and services before clicking “accept”. In the case of F-Secure, it was against public policy to enforce a clause where users were expected to give up their first born child. Likewise, there is no suggestion that the Courts would enforce Purple's clause in the light of the fact that such an unexpected and onerous clause was not clearly highlighted in the terms and conditions. However, every case will be judged on its facts and it cannot be assumed that the Courts will be sympathetic to users who claim terms are onerous/contrary to public policy if in fact those terms are commonly found in the industry and are contained in the provider's standard, unmodified terms and conditions in plain English.

For providers of Wi-Fi, in line with GDPR requirements, terms and conditions need to be very clear on what data is being collected, the reasons for collection, the intended use of such data and the ability for the user to opt-in for any marketing, as well as providing them clear instructions on how they can opt-out at any time. Good practice would also dictate that onerous/unusual terms are highlighted so as to encourage transparency and trust between the user and the service provider.

Data protection

Government publishes the Data Protection Bill

The development

The UK government published the Data Protection Bill (**Bill**) on 14 September 2017. The Bill will replace the Data Protection Act 1998 (**DPA**) and transfer the General Data Protection Regulation (**GDPR**) into domestic law (with a few derogations, as discussed below). Post-Brexit, the Bill will continue to regulate data protection in the UK.

The changes

By now, most enterprises will be familiar with the obligations and restrictions imposed by the GDPR (effective from May 2018). However, as anticipated when introducing any EU regulation, the localised UK Bill contains some agreed nuances. Here are some of the highlights.

Exemptions

As in the DPA, certain groups may be exempt from the application of the GDPR. Generally these exclusions protect individuals that process personal data as a necessary element of their profession, including:

- journalists, who are allowed to process personal data on grounds of freedom of expression and to expose wrongdoing
- scientific/historical research organisations
- anti-doping bodies to enable them to protect the integrity of sport
- financial services firms that process personal data to investigate terrorist financing or prevent fraud.

Additionally, subject to obtaining explicit consent or inclusion in an employee related policy, the Bill allows employers to process sensitive personal data (called “special categories of personal data” under the GDPR) and data relating to criminal convictions.

New offences

The Bill also includes some additional criminal offences in relation to data protection. These are important for organisations to consider; otherwise they may find themselves inadvertently committing offences, as follows:

- altering, defacing, destroying or concealing information with the intention of preventing its disclosure as part of a valid subject access request

- knowingly or recklessly re-identifying individuals from de-personalised (ie anonymised or pseudonymised) data, without the consent of the controller or the data subject
- intentionally or recklessly obtaining personal data unlawfully (i.e. without consent).

Other points to note

In addition to the above, it is also worth noting the following:

- the fines under the Bill are essentially the same as set out in the GDPR, a maximum of £17m or 4% of global annual turnover
- a child in the UK for the purposes of providing consent to data processing is an individual younger than 13 years of age. If a child is under 13, companies will need to obtain consent from a person with “parental responsibility” for that child.

Any practical tips?

As anticipated, there are no real ground-breaking differences between the GDPR and the Bill. In particular, with the new offences in mind, it will be important to carefully document consents for processing and also to keep a solid audit trail when responding to subject access requests. This is also important in the context of the GDPR's accountability principle in relation to record keeping.

We also recommend that organisations stay eagle-eyed for any further developments in this area, especially with the Bill going for its second reading in the House of Lords on 10 October 2017.

Data protection

Data Protection Working Party adopts Opinion 2/2017 on data processing at work

The question

How do new technologies affect the balance between employers and employees in the debate over legitimate data monitoring interests vs the privacy expectations of individuals?

The background

The Article 29 Data Protection Working Party (**WP29**) is a group of representatives from each EU Member State, charged with providing the European Commission with independent advice on data protection matters. The WP29's latest Opinion builds on its previous publications (Opinion 8/2001 on the processing of personal data in the employment context, and the 2002 Working Document on the surveillance of electronic communications in the workplace) by adapting its guidance to the context of modern technologies which have altered the methods by which employers can process employees' personal data at work.

The development

The aim of the Opinion is to assess the balance between the interests of employers and the privacy expectations of employees by outlining the risks posed by new technologies, and undertaking an assessment of proportionality. To this end, the Opinion states that in all cases employers should consider whether:

- the processing activity is necessary, and if so, the legal grounds that apply
- the proposed processing of personal data is fair to the employees
- the processing activity is proportionate to the concerns raised
- the processing activity is transparent.

The WP29 utilise a number of example scenarios in which new technologies, or the development of existing technologies, may cause high risks to the privacy of employees.

One such scenario is the processing of data through the monitoring of employee social media accounts. Whilst we now live in a society in which the vast majority of individuals have publicly-available social media profiles, employers should not mistake availability of access with permission to process. The screening of an employee's information regarding friends, opinions, beliefs, and so on "*should not take place on a generalised basis*". Similarly, during the recruitment process, employers may only collect data from social media if it is relevant to

the performance of the job being applied for. The applicant must be informed, and the information deleted once the process is finalised.

A new tendency for employers to provide employees with wearable devices (tracking health and activity) has also been scrutinised. The Opinion serves as a reminder that the processing of health data is prohibited under the Data Protection Directive.

The Opinion also considers the scenario of monitoring of employee ICT usage at home. The advent of remote working has created an increased risk of unauthorised access or hacking of devices. Employers are warned against deploying software packages that monitor keystrokes, capture screens or enable webcams – whilst designed to provide security, the data processing involved is very unlikely to have a legal ground.

Why is this important?

The crucial concept at the heart of the WP29's Opinion is that due to the power imbalance between employer and employee (given the employee's financial dependence on the employer) it would be rare to see an employee giving legally valid and explicit consent to the processing of data by their employer. Similarly, an employee may not feel comfortable in revoking or refusing consent. Overcoming this issue would require a truly exceptional circumstance in which there would be no consequences connected to the acceptance or rejection of the processing by the employee.

Any practical tips?

From an employer's perspective, the key message is this: just because you can process data, doesn't mean you should! Consideration must always be given to the principles of proportionality, transparency, fairness and subsidiarity. Does the need for data processing outweigh the privacy rights of employees? Realistically it seems that the answer will, except in exceptional circumstances, be "no".

Data protection

ICO publishes updated Subject Access Code of Practice

The question

How should data controllers respond to subject access requests (**SARs**)?

The background

The Information Commissioner's Office (**ICO**) has updated its Subject Access Code of Practice, originally published in 2013, to reflect the guidance of the Court of Appeal in *Dawson-Damer v Taylor Wessing [2017] EWCA Civ 74* and *Ittihadieh v 5 – 11 Cheyene Gardens [2017] EWCA Civ 121*.

The development

Arguably the most important development outlined in the amended Code relates to the “disproportionate effort” exception. By way of reminder, section 8(2) of the Data Protection Act states that the obligation to supply a requestor with a copy of the requested information in permanent form does not apply where doing so would involve disproportionate effort.

The ICO attempts to codify the developments made by the Court of Appeal in the *Dawson-Damer* and *Ittihadieh* cases with regard to the exception. The Code states that:

- difficulties throughout the process of complying with a request (e.g. in locating the requested information) may be taken into account when assessing disproportionate effort
- the data controller should assess each request, balancing the effort in complying against the potential benefits the requestor might gain from the information
- the burden of proof is on the data controller to show that all reasonable steps in order to comply with the SAR have been taken, and that further steps would be disproportionate
- even if there is a demonstrable disproportionate effort in providing permanent form copies, a data controller must try to provide the information in some other way.

Additional amendments to the Code require that data controllers:

- co-operate with the applicant – in other words, to engage with the requester about the information they require
- disregard the purpose of the SAR – the Code clarifies what we learned in *Dawson-Damer*: the applicant's collateral purpose (other than seeking to check or correct their personal

data) in making the SAR is irrelevant to the obligation of a data controller to comply with the request

- beware of ICO enforcement – the ICO will now have the power to serve enforcement notices if it considers that an organisation has failed to comply with the subject access provisions. However, it will only take action if it is reasonable to do so, and it will not require organisations to take unreasonable steps to comply.

Why is this important?

Whilst attention is currently focused on the upcoming GDPR, the ICO reminds us that the Data Protection Act and the associated cases are the current law. The revised Code is important not only because it reflects up-to-date case law, but also because it gives an indication of how the ICO expects to see SARs dealt with in practice, particularly where requests are likely to involve extensive search efforts.

Any practical tips?

If you are wondering how to respond to a SAR, read this Code! Following the guidance, and even reflecting its language and tone in dealing with applicants may make a huge difference if your response is ever investigated. Remember that SARs become free (i.e. no £10 payment required) when the GDPR lands – and when something becomes free, it becomes very popular. So the sooner your business starts dealing with SARs in the correct way, the better placed it will be in dealing with what may become a tsunami of SAR requests post May 2018.

Data Protection

ICO fines Boomerang Video Ltd for failure to prevent cyber attack

The development

On 27 June 2017, the Information Commissioner's Office (**ICO**) fined Boomerang Video Ltd (Boomerang) £60,000 after an investigation found that the SME had failed to take basic steps to stop its website being attacked.

The facts

Boomerang enables customers to rent video games through a payment application. A third party company developed the website in 2005 but Boomerang failed to identify a coding error on the login page. Boomerang's website was subject to a cyber-attack in 2014, in which 26,331 customer details could be accessed. The attacker used a common technique known as an SQL injection to access the data.

The decision

The ICO's investigation found that Boomerang had failed to comply with the Data Protection Act 1998 (**DPA**) for the following reasons:

- Boomerang failed to carry out regular penetration testing on its website that should have detected errors
- the firm failed to ensure the password for the account on the Wordpress section of its website was sufficiently complex allowing the attacker to upload a web shell onto the server
- Boomerang had some information which was stored unencrypted, and that which was encrypted could be accessed because it failed to keep the decryption key secure
- encrypted cardholder details and CVV numbers were held on the web server for longer than necessary

Whilst the ICO took into account several mitigating features, it also took into account the following aggravating features:

- Boomerang was not aware of the security breach until over one month after the attack, when it was notified by its customers
- Boomerang had assessed itself to be compliant with the "Payment Card Industry Data Security Standard" despite not carrying out penetration testing on its website
- Boomerang received almost 1,100 complaints and enquiries as a result of the cyber-attack.

The ICO considered that Boomerang's contravention was serious, that it ought to have been aware that contravention would have occurred, that there was "no good reason" to explain why reasonable steps had not been taken to prevent the contravention and such contravention was likely to cause substantial damage and distress. A monetary penalty was therefore issued under s.55A of the DPA.

The ICO said in its Monetary Penalty Notice:

"Boomerang Video failed to take basic steps to protect its customers' information from cyber attackers. Had it done so, it could have prevented this attack and protected the personal details of more than 26,000 of its customers".

Why is this important?

As organisations look to prepare themselves for the introduction of the General Data Protection Regulation (**GDPR**) in May 2018, the fine provides a timely reminder of the existing requirements which must be met to protect customer information from data breaches. If businesses are judged to have contravened data protection legislation, then the ICO will not hesitate to hand out penalties designed to be taken seriously. It is also probably worth noting that for the most serious violations of the forthcoming GDPR, the ICO will have the power to fine companies up to €20m or 4% of a company's total annual worldwide turnover for the preceding year. Add in the loss of consumer trust, plus the potential for civil claims for data violations (e.g. for distress), and the total cost/damage could prove substantial, if not terminal to smaller companies.

Any practical tips?

Ensure the tech teams are aware of the knock on effect of a failure to fix common coding errors. And if you're buying a company, make sure that the corporate team focuses on including the relevant representations and warranties to enable recovery should the worst happen (e.g. from a data hack) post acquisition.

Data protection

ICO issues fines for emails asking customers to change marketing preferences

The development

The ICO has fined Moneysupermarket.com and Morrisons Supermarket a total of £90,500 for emails sent to customers who had previously opted out of marketing messages.

The facts

Moneysupermarket.com sent an email informing customers that it had updated its privacy policy and terms and conditions. The email included a section titled “Preference Centre Update” which invited customers to change their marketing preferences to receive “*personalised news, products and promotions*”. All 6,788,496 recipients of the email had previously opted out of receiving direct marketing emails.

Morrisons Supermarket sent a similar email to 130,671 customers who had previously opted out of receiving marketing related to their Morrisons More Card (though they had opted in to marketing for online groceries). The emails were titled “Your Account Details”, and offered to send money-off coupons, extra More points, and the “*latest news*” from Morrisons if the customers changed their preferences.

The decisions

The ICO found that both Moneysupermarket.com and Morrisons Supermarket had breached their obligations under the Privacy and Electronic Communications Regulations 2003 (**PECR**) and fined the companies £80,000 and £10,500 respectively. The ICO restated its view, affirmed in other recent cases, that organisations cannot e-mail an individual to ask for consent to future marketing messages. Such an email is itself sent for the purposes of direct marketing and is subject to the same rules as other marketing e-mails.

ICO Head of Enforcement Steve Eckersley said “*organisations can't get around the law by sending direct marketing messages dressed up as legitimate updates. When people opt out of direct marketing, organisations must stop sending it, no questions asked, until such time as the consumer gives their consent. They don't get a chance to persuade people to change their minds*”. The fact that marketing only constituted one section of the emails sent by Moneysupermarket.com was irrelevant. Mr Eckersley added that emails sent “*under the guise of “customer service”, checking or seeking their consent, is a circumvention of the rules and is unacceptable*”.

Why is this important?

There is growing pressure on organisations to sort out their marketing consents ahead of the GDPR coming into force on 25 May 2018. If they don't, the concern is that their ability to continue using their core databases may be severely compromised under the GDPR's tougher data regime. It explains why businesses are contacting customers now to try and maintain their marketing reach in the future. These fines (just like the recent ones against Flybe and Honda) are a reminder that customers who have opted out of marketing messages are off limits – at least from direct marketing messaging to get them to opt back in (whether dressed up as customer service or otherwise).

Any practical tips?

Be strong with the marketing teams, whatever the temptation to “refresh” marketing consents, or you could end up with a decent fine. And don't forget that the ICO guidance on direct marketing still applies (for now) and that the ICO also published draft guidance on consent under the GDPR at the end of March 2017. This, and the draft ePrivacy Regulation (published by the European Commission on 10 January 2017), are essential reading materials if you are advising on the ongoing viability of marketing databases ahead of the (now fast-approaching) GDPR D-Day.

ASA

New BCAP guidance on advertising of high fat, salt and sugar (HFSS) products

The question

How can an HFSS product advertisement be differentiated from a brand advertisement (to which the HFSS restrictions do not apply)? And what is the approach of the Broadcast Committee of Advertising Practice (**BCAP**)?

The background

On 8 December 2016, the Committee of Advertising Practice (**CAP**) announced tough new rules banning the advertising of HFSS food or drink products in children's media. The new rules are now applicable across all non-broadcast media, including in print, cinema and, more importantly, online and social media. The rules followed a full public consultation and research showing that youngsters aged 5 to 15 are spending approximately 15 hours per week online. The introduction of the new rules is intended to help protect children's health and well-being.

The new CAP rules are briefly summarised as follows:

- advertisements which directly or indirectly promote an HFSS product are not allowed to appear in any children's media
- advertisements for HFSS products are not allowed to appear in other media where children make up over 25% of the audience
- advertisements for HFSS products cannot use promotions, licensed characters and celebrities popular with children.

It is worth noting that the above restrictions do not apply to brand advertising that do not have the effect of promoting a specific HFSS product. However, it is acknowledged that differentiating an HFSS product advertisement from a brand advertisement is not always easy.

The development

In view of the recent development of the CAP rules, the BCAP revised its "Guidance on identifying brand advertising that has the effect of promoting an HFSS product" (the **Advertising Guidance**) which came into effect alongside the new rules on 1 July 2017.

The Advertising Guidance set out various scenarios where it was difficult to distinguish between HFSS product advertisements and brand advertisements.

The scenarios

Product reference is an important factor to determine whether an ad amounts to an HFSS product advertisement. If an ad refers to or prominently features an identifiable HFSS product, it is likely to be regarded as an HFSS product advertisement.

Where the information provided by a product advertisement is not sufficient for the audience to identify the product as one that can be nutrient profiled, the advertiser needs to satisfy the Advertising Standards Authority (**ASA**) that its range of that type of product is mainly non-HFSS (ie a range under which more than 50% of the products sold are categorised as non-HFSS under the nutrient profiling scheme) to avoid the HFSS restrictions.

The direct response mechanic contained in the advertisement (such as telephone numbers and interactive links) is another indicator. An advertisement is unlikely to be regarded as an HFSS product advertisement if it does not contain any direct response mechanic relating to a specific HFSS product.

If an advertisement features a brand name which does not promote a specific HFSS product and the brand is synonymous with an identity other than the provision of HFSS products, it will not be considered an HFSS product advertisement. In determining whether the brand is synonymous with the identity other than the provision of HFSS products, the ASA will take into account the company's provision of non-HFSS products or goods and services other than food and soft drink products, or its association with significant initiatives relating to education, sport, community etc.

However, if a brand advertisement features, say, a celebrity or a brand-generated character which is strongly associated with a specific HFSS product, it can still be subject to the HFSS restrictions.

Why is this important?

As organisations look to comply with the new rules, the Advertising Guidance provide a timely note on the factors that the ASA will take into account when deciding whether an ad is subject to the HFSS restrictions. Those who are responsible for reviewing marketing materials should now have a better idea on how the ASA draws the line.

Any practical tips?

When reviewing materials for promotion of HFSS products, check through the restrictions imposed by the CAP Code (in particular, section 15) and BCAP Code (in particular, sections 13 and 32) as well as the Advertising Guidance. However, bear in mind that the list

of scenarios in the Advertising Guidance is not exhaustive and it is for the ASA to decide on a case-by-case basis whether an advertisement has the effect of promoting an HFSS product.

Always keep a check on all marketing materials, including those in social media (especially in platforms where youngsters make up a large portion of audience) to ensure that they comply with the CAP Code and the BCAP Code.

ASA

ASA Ruling on John Lewis Partnership plc t/a John Lewis – misleading pricing of products advertised as free in bundle promotions

The question

When is it misleading to claim that an item, purchased as part of a bundle, is “free”?

The complaint

On 15 February 2017, John Lewis offered on its website an LG TV 55B6 with a “FREE LG SH7 sound bar” for £1,999.

The complainant, who understood that the TV had previously been available for £1,749 without the sound bar, and that the sound bar was sold separately for £259, challenged whether the “FREE” claim was misleading.

The response

John Lewis said that in the month prior to 14 February 2017, the TV had received a discount of £250, partially funded by the manufacturer. That financial support was withdrawn on 15 February 2017 and the TV reverted to its original selling price of £1,999. Also on 15 February 2017, however, the manufacturer offered financial support for another promotion. This was a bundle which included a free sound bar worth £259.99. John Lewis confirmed that the TV without the sound bar was available for £1,999, and provided evidence of the selling price since May 2016.

John Lewis considered that the price of the TV had not been inflated to cover the cost of the sound bar, as the support from the manufacturer was only available when the TV was bought as part of the bundle.

The decision

The ASA upheld the complaint.

It considered that consumers would interpret the “FREE” claim to mean that the **usual** selling price of the TV was £1,999, and that the sound bar had been added at no extra cost. In particular, the ASA considered that consumers would expect that the price immediately before the promotion would have been £1,999, with no sound bar included.

In fact, the promotion under consideration had immediately followed another promotion, where the TV was offered for £1,749. Having reviewed evidence of the TV's selling price, the ASA noted that the price of the TV had changed regularly since May 2016, and had often been available for £1,749. It therefore found that £1,999 was not the usual selling price.

The fact that the lower prices had been driven by financial incentives, which had been offered by the supplier to both John Lewis and other retailers, did not alter the ASA's findings. Indeed, it considered that those previous reductions had undermined the expectations consumers would have about the sound bar being added without the price being increased. The reductions also contributed to the finding that £1,999 was not the usual price for the product.

The ASA found that the claim was misleading, in breach of CAP Code rules 3.1 (Misleading advertising) and 3.24.2 (Free).

Why is this important?

The decision, whether you consider it **sound** or not, is a useful clarification on the ASA's approach to misleading pricing when items are offered “free” as part of a bundle. What matters is the customer's impression of the “usual” price for the products in the offer. The usual price is determined by reference to historic prices for the products, and in particular the price immediately before the promotion.

Any practical tips?

Think like the customer! To avoid adverse rulings from the ASA, companies should always view their offers from the customer's perspective. Remember – the customer will usually not be aware of behind-the-scenes financial incentives, which would otherwise provide a perfectly good explanation for price fluctuations.

ASA

Inspop.com Ltd t/a Confused.com (5 July 2017) – ASA decision on “No. 1 claims”

The facts

Confused.com, a comparison site, ran a campaign comprising of five adverts in total, all which stated that it was “*No. 1 for car savings*”.

The complaint

Gocompare.com, a competitor, challenged whether the five adverts could be substantiated and were therefore misleading, as each advert gave the impression that consumers could save more money at Confused.com than its competitors.

The response

Confused.com stated that it had undertaken a market review and compared the number and type of car-related services available through them and the next three largest UK price comparison sites. The sites were then ranked by the **total number of opportunities** to save on car related products and Confused.com argued that it offered savings on 23 of those products.

In order to mitigate any risk, Confused.com said that it had taken care to explain the comparison was not based on price, the adverts themselves did not claim that it offered greater savings on individual products and the claim did not indicate that consumers would take up all of the opportunities to save. In addition, Confused.com added that all the adverts carried a qualification to explain that being “No.1” was based on the opportunities to save on car-related products. Furthermore, Confused.com had involved Clearcast to ensure the basis of its claim was clear.

Clearcast asserted that due to the fact that Confused.com had provided substantiation and had included a qualifying statement on the adverts, Confused.com could carry a No.1 claim. Furthermore, Confused.com had given assurances to Clearcast that it would monitor the market and make regular changes to the adverts as appropriate.

The decision

The ASA upheld the complaint.

The ASA considered that the claim “*No. 1 for car savings*” would generally be understood by consumers to mean that if they purchased car-related products through Confused.com, then

they were likely to save more money compared to buying via competitor sites. This is because consumers use comparison sites to find the best value deal on what product or service they are interested in buying.

The format of each advert was different and the reason to uphold varied depending on the format. In summary, the ASA made the following findings for each advert:

- the paid-for search result on Google gave the overall impression that Confused.com saved consumers more on their car insurance compared to their competitors. There was no qualification that “*No. 1 for car savings*” related to the number of car products on which Confused.com compared prices
- the email repeated the “*No. 1 for car savings*” three times at the top of the email as well in the body of the text. It was only further down that the advert said “*No one offers drivers more opportunities to save on their car*” with a hyperlink to a page that told drivers about opportunities to save. The ASA said that the “*No. 1 for car savings*” claim was not explicitly linked to the number of products on which Confused.com compared prices
- the TV advert featuring James Corden was acknowledged to contain a qualification in small text about the opportunities to save on car-related products; however, the voice over and prominent on-screen text stated “*No. 1 for Car Savings*” and that “*Drivers Win*”. The advert did not highlight that Confused.com was “*No. 1 for Car Savings*” because it compared more products than its competitors. To underscore this point, Confused.com was presented with market research asking participants to assess the “*No. 1 for car savings*” claims (including the on-screen text with the qualification about opportunities to save on car related products). Less than 5% of participants considered the claim fitted the definition which Confused.com had provided
- regarding the website, the ASA acknowledged that an attempt had been made to explain the qualification of the claim under the title “*how we fare against other price comparison sites*” and “*when it comes to car savings, Confused.com is the place to come to...no one offers drivers more opportunities to save than us!*” However, the page did not explicitly state that the “*opportunities to save*” meant that they compared more products than competitors
- the newspaper advert was acknowledged to include the qualifying sentences “*no one offers drivers more ways to save on their car*” and “*No. 1 for car savings – based on opportunities to save on car-related products*”, but the ASA found that the position of the qualifying sentences, both on the page and in the wraparound, diminished the likelihood of it impacting significantly on consumers' overall impression of the advert.

The ASA ruled that the adverts could not appear in their current form and not to repeat the claims unless they could be substantiated.

Why is it important?

The adverts ran contrary to a key principle of the ASA that marketing communications must not materially mislead or be likely to do so. They must not mislead by hiding or omitting material information or presenting it in an unclear, unintelligible, ambiguous or untimely manner. The ASA not only considered that the qualifier “*no one offers drivers more opportunities to save on their car*” was ambiguous but that, in the absence of any reference to the comparison with Confused.com’s three largest competitors in the majority of the adverts, consumers would interpret a “No.1” claim to be a comparison with the entire market.

Furthermore, the decision received publicity from the press and online community which a brand like Confused.com might not have welcomed, given its focus on championing the consumer and helping them find the best possible deal to save on their car.

Any practical tips?

This decision underscores the need for the consumer to be able to make an informed choice when they are choosing goods or services. Therefore, when undertaking an ad campaign in any format, advertisers should be careful to ensure that (a) they understand how consumers will likely interpret the claim being made (b) the substantiation matches the claims and, if necessary (c) the claims are clearly and properly qualified to ensure transparency and non-ambiguity.

ASA

ASA publishes report on gender stereotyping in advertising

The question

How far do advertisers need to go in ensuring that ads avoid harmful gender stereotypes?

The background

Following public backlash to the now infamous Protein World “Beach Body Ready” advertising campaign, in 2016 the ASA launched a project to consider whether current advertising regulation does enough to address the potential for harm and offence caused by gender stereotyping in ads. This project formed the foundation of the “Depictions, Perceptions and Harm” Report published in July 2017.

The development

The Report found that gender stereotypes have the potential to cause harm by inviting assumptions that might negatively restrict how people see themselves and others. Such assumptions are ultimately detrimental not only to individuals, but more widely to society and the economy. Though advertising is only one of many factors that contribute to the proliferation of gender stereotypes, the ASA and CAP consider that the Report provides a case for tougher regulation to tackle the use of potentially harmful gender stereotypes in ads.

The six categories of gender stereotypes identified within the Report include:

- roles – occupations or positions usually associated with a specific gender
- characteristics – attributes or behaviours associated with a specific gender
- mocking people for not conforming – making fun of someone for behaving or looking in a non-stereotypical way
- sexualisation – portraying individuals in a sexualised manner
- objectification – depicting someone in a way that focusses on their body parts
- body image – depicting an unhealthy body image.

Rest assured that the ASA does not expect the removal of any kind of depiction of men and women in traditional gender roles – for instance, it would be unrealistic to censor ads depicting a woman cleaning or a man doing DIY. The evidence suggests, however, that the following might be classed as problematic:

- ads depicting families creating mess while a woman has sole responsibility for cleaning it

- ads suggesting an activity is inappropriate for one gender because it is stereotypically associated with the other
- ads featuring men trying and failing to undertake simple parental or household tasks.

Why is this important?

Currently, the CAP Code catches ads that are likely to cause “*serious or widespread offence*”, and the ASA has in the past ruled against ads which sexualise women or depict an unhealthy body image. However, there is no direct rule preventing gender stereotyping within the UK Advertising Codes. Based on the strength of evidence in this Report, CAP is in the process of developing new standards for ads that feature stereotypical gender roles or characteristics.

Campaigns promoting stereotypes can already face public backlash, but in future, an upheld complaint could magnify the public relations damage by validating what might otherwise be written off as a few anonymous voices on Twitter.

Any practical tips?

The ASA plans to report publicly on CAP's new standards before the end of 2017. This interim period presents a risk, in that the ASA has signalled heightened sensitivity but not yet provided its guidance. Advertisers should tread carefully, and keep an eye out for the new guidance towards the end of the year.

ASA

ASA Ruling on SKY UK Ltd t/a Sky – “Super Reliable” broadband

The facts

Two Sky adverts claimed that Sky's broadband services were “*super reliable*”.

The first, a TV ad, depicted an animated dog and was centred around the concept of it receiving an unreliable broadband service. The TV ad was accompanied by a voiceover stating “*switch to super reliable sky broadband*” and over screen text stating “*Super Reliable Sky Broadband*”. The second ad was a national press piece which featured the claim “*Super Reliable Sky Broadband Unlimited*”.

Virgin Media challenged whether “*Super Reliable*” was misleading and could be substantiated.

The response

Sky accepted that their reference to “*Sky Broadband*” in both ads was wide enough to encompass both their ADSL2+ and fibre broadband packages. They stated that they thought that consumers would take “*Super Reliable*” to mean that the service was very reliable and could be trusted to work well. They said that they did not consider this to be a comparative claim, and that more than one provider was able to make a “*Super Reliable*” claim.

Sky considered that they were able to substantiate the “*Super Reliable*” claims with evidence related to their overall performance and complaints performance. They relied on data from Ofcom's 2016 “UK Home broadband performance: The performance of fixed-line broadband delivered to UK residential consumers” Report. Sky said that they considered that factors most relevant when assessing overall reliability of a broadband service included latency, jitter, packet loss, peak time performance and daily disconnections. They therefore focussed on these aspects of the Report.

The decision

The ASA upheld the complaint. They considered that consumers would understand these claims to be general claims about the overall reliability of all of Sky's broadband packages, and would expect a “*super reliable*” service to deliver a consistent connection with very few interruptions or slowdowns. Accordingly, they said that they would expect to see evidence demonstrating that all of Sky's broadband services delivered consistency in all measurable factors of relevance. They were satisfied that the factors identified by Sky were the key

metrics relevant to consumers' expectations of "reliability" for broadband, and went on to examine whether evidence supplied sufficiently substantiated the "Super Reliable" claims.

The ASA concluded that the Ofcom data evidenced that Sky's fibre packages delivered consistency in all measurable factors of relevance, but that its ADSL2+ service failed to deliver consistency in peak time performance (i.e. one element). Since the claim "*Super Reliable Broadband*" was wide enough to encompass ADSL2+, it was considered misleading to describe Sky's broadband services generally as "*Super Reliable*".

For the TV ad, the ASA considered that the "*switch to super reliable sky broadband*" voiceover, coupled with the concept of an unreliable broadband service, did implicitly create a comparison in the mind of consumers of Sky vs other broadband providers. Having examined the Ofcom data, they said that this demonstrated that Sky's broadband packages delivered a similarly consistent connection to equivalent packages of competitors, but that Sky was not more consistent overall. This was therefore likely to mislead consumers.

Why is this important?

This is a further example of the very high levels of substantiation required for claims in the telecommunications sector. It also demonstrates that "switch" messaging is capable of being interpreted as encompassing a comparative claim, and so advertisers will need to ensure that they are able to substantiate superior performance/services with comparative data when making such claims.

Any practical tips?

Keep claims as specific as possible – allowing claims to be viewed as encompassing a number of services (each with varying levels of performance) will naturally make substantiation more difficult.

Watch out for subtle comparative claims in your advert – these will still need robust data in order to substantiate even if competitors are not specifically named in the ad itself.

ASA

ASA Ruling on British Telecommunications plc t/a BT – prominence of qualifications to headline claims

The question

What constitutes a sufficiently prominent qualification of a comparative advertising claim?

The facts

In July and August 2016, BT ran four ads for the BT Smart Hub:

- a TV advert (and identical YouTube ad) featured Ryan Reynolds stating: “*With the UK’s most powerful Wi-Fi signal, it can reach some serious distance*”. On-screen text displayed the phrase “*UK’s most powerful Wi-Fi signal versus major broadband providers*”. The ad then depicted Reynolds taking off in a helicopter, stating he still had Wi-Fi at 150 meters and 200 meters
- the BT website featured text including “*the UK’s most powerful Wi-Fi signal*” and “*better Wi-Fi coverage...faster Wi-Fi connections in more rooms than the latest hubs from other major UK broadband providers*”
- a radio advert stating: “*the UK’s most powerful Wi-Fi signal...could reach the length of at least 12 London buses*”.

Predictably, many of the major ISPs (including Virgin Media, Sky and TalkTalk) challenged the claims that the BT Smart Hub:

- has the “*UK’s most powerful Wi-Fi signal*”
- “*gives you better Wi-Fi coverage*”
- can reach distances of up to 200 metres or 12 London buses (i.e. 180 meters).

The response

BT rebutted the first and second complaints by detailing the robust testing to which the Hub had been subjected before any advertising claims were made. In order to ensure that their evidence was obtained in a context representative of general consumer use, BT’s testing took into account the relevance of testing network speeds, frequencies and devices, as well as the requirement to test in real homes as well as test homes. The claims were intended to relate only to the capabilities of the router, rather than overall broadband speed.

Further, the claim of being the “*UK's most powerful Wi-Fi signal*” was qualified in on-screen text and in the body of the website as being compared against major broadband providers. BT believed that the prominence of the qualification was sufficient and would not mislead.

In relation to the third complaint, BT submitted a test report to demonstrate that the Hub could reach the distances claimed when travelling through one wall and connecting to a tablet. The company noted that the helicopter and the buses were intended to illustrate the distances in a humorous manner, rather than being literal descriptions.

The decision

The ASA upheld the first and second complaints; the third was not upheld.

It was acknowledged that the evidence provided by BT demonstrated that the Hub's signal reached a greater distance than routers from other major broadband providers. That said, consumers would understand the “*UK's most powerful Wi-Fi signal*” to be a superiority claim. Whilst “*gives you better Wi-Fi coverage*” was seen as general in isolation, the combination of the two headline claims would be understood as whole-of-market comparisons rather than a comparison against major providers. The on-screen and webpage qualifications were not sufficiently prominent to make this clear to consumers. The overall effect was therefore misleading.

As for third complaint, the ASA concluded that whilst consumers would understand that the router could transmit a signal over a distance of 200 meters, it was unlikely that consumers would need the router to transmit such a far-reaching signal. As such, the adverts were likely to be understood simply as illustrating that the router could transmit a signal over a long distance, and it would be sufficient for BT to demonstrate that this was the case.

The ASA decided that the four adverts could not appear in their current forms.

Why is this important?

Interestingly, the main reason that the complaint seems to have been partially upheld is because the “*versus major UK broadband providers*” wasn't prominent enough (rather than BT not being able to substantiate the claims through testing). BT had jumped through all the hoops to ensure their statements were accurate, they fell at the final hurdle – the wording of the claims!

Conversely, it appears that claims overtly designed to be illustrative and fantastical in nature will be judged more benignly by the ASA, so far as the requisite test data can be produced to substantiate the core message as understood by the consumer.

Any practical tips?

When drafting a qualifying statement, ensure that it is clear and unambiguous so as to ensure it adequately disclaims the headline claim. In addition, ensure that the statement is in a prominent place for the consumer to view and digest.

For ISPs and router manufacturers specifically, the takeaway is that the ASA has accepted that claims about Wi-Fi signal strength and reach, where used appropriately, can be taken by consumers to mean just the performance of router (rather than a general claim about Wi-Fi performance which would be more difficult to substantiate). When making a claim about the performance of the router only, broadband speeds do not need to be taken into account.

One final point to note is that the adjudication makes clear that there is now a requirement to test in real homes as well as test homes. The ASA has confirmed that there is a need to demonstrate that evidence is obtained in a context representative of general consumer use.