RPC

Snapshots for Meta

WINTER 2023

KEY UK AND EU DEVELOPMENTS FOR META'S COMMERCIAL LAWYERS

The UK's Online Safety Act: new Ofcom guidance

PLUS

What the AI is going on...? Latest updates

New amendments to the Digital Markets, Competition and Consumers Bill

ASA report on Intermediary and Platform Principles Pilot

Welcome to the Winter 2023 edition of Snapshots for Meta

We aim to cover everything Meta's lawyers need to know in the UK and EU from the previous quarter (well, almost!). We hope it hits the spot, as we aim to address most of the key changes affecting Meta, including data, digital, consumer and advertising developments as well as the latest UK commercial case law. Please do let us know if you have any feedback or queries.

Best wishes
Olly

Olly Bray
Senior partner
oliver.bray@rpc.co.uk

WITH THANKS TO OUR FANTASTIC CONTRIBUTORS

- Sofia Gofas
- Andy Hodgson
- Hettie Homewood
- Sophie Hudson
- Dan Jackson
- Rebecca James
- Tom James
- Nick McKenzie
- Will Monaghan
- Aiswarya Nadesan
- Dorian Nunzek
- Abigail Pipkin
- Mia Pullara
- Anila Rayani
- Lydia Robinson
- Carla Skelton-Garcia
- Laura Verrecchia
- Ed Warren
- Mars Yeung

EDITORIAL

Sub-editors Olly Bray, David Cran, Joshy Thomas, Praveeta Thayalan and Laura Verrecchia.

Design Rebecca Harbour

Contents

"The UK, EU and US have all adopted different approaches when it comes to regulating AI, with the UK taking a more "hands off approach" when compared to its European neighbours and our friends across the pond."

What the AI is going on … September to November 2023

September

ChatGPT gets an update: all seeing, all hearing

OpenAI announced that ChatGPT can now see, hear and speak, as the company rolls out new voice and image capabilities.

October

Microsoft 365 follows suit with upgrading Copilot

Are all those meetings adding up? Fear not, AI assistant Microsoft 365 Copilot can now attend meetings for you and report back its conclusions and findings. If this is not enough, it can provide a "snapshot" of the meeting; think a quick recap of the main highlights.

The Law Society's recommendations on the Government's AI white paper

The Law Society has highlighted its recommendations that were made in response to the government's white paper on AI regulation in June 2023. The Law Society stated that it believes there to be a need for further clarity on legislation, procurement practices and how discrepancies across sectors will be mitigated.

November

UK AI summit: too many cooks?

Nick Clegg, speaking on behalf of Meta, voiced his concerns over how confusing the global approach to AI was becoming. He highlighted the new UN panel, the publishment of a G7 Code, Biden's US executive order, the UK summit conclusions and that the EU was continuing to work on a new AI Act. It simply, in his view, does not fit together. governments and regulators need to focus on key definitions that will help shape AI governance.

AI regulation: who will come out on top?

The UK, EU and US have all adopted different approaches when it comes to regulating AI, with the UK taking a more "hands off approach" when compared to its European neighbours and our friends across the pond. All three have announced plans to open an "institute" or "office" to oversee AI. The UK's "institute" will "independently and externally evaluate, monitor and test" AI models, whereas the others will act as a regulator and play a part in determining future regulations.

Grok launch: Elon's at it again

Elon Musk's xAI has released its first AI model, named Grok, which has "real-time access" to information from his social media platform X. This access, according to Musk, gives the chatbot an edge over competitors that have largely relied on older archives of internet data.

OpenAI plans to launch custom versions of ChatGPT: an "app store" like never before

Called GPTs, the apps will be adapted and tailored for specific applications, turning the chatbot interface into a digital platform similar to iOS and Android. The Microsoft-backed AI company plans to collate the best apps and eventually split revenues with the most popular GPT creators.

The Artificial Intelligence (Regulation) Bill is introduced: if you won't regulate, we will

A Private Members' Bill, the Artificial Intelligence (Regulation) Bill (AIRB), was introduced in the House of Lords on 22 November 2023 to create an AI Authority, which would collaborate with relevant regulators to construct "regulatory sandboxes for AI" and consult on as well as monitor other regulatory frameworks. The AIRB also affords the Secretary of State the power to add other functions to the AI Authority's remit.

If passed, in its current form, the AIRB would require any business which develops, deploys and/or uses AI to appoint an AI Officer to ensure the:

- safe, ethical, unbiased and non-discriminatory use of AI
- data used by the business in any AI technology is unbiased, as far as reasonably practicable.

AI leaves white collar workers feeling exposed

The Department for Education has published a report, "The impact of AI on UK jobs and training", which looks into the jobs and industries it expects will most likely be "exposed" to AI. The report states professional occupations are most exposed to AI, with manual work and those typically associated with lower wages being the least exposed. In particular, the report states that the finance and insurance sector have the highest exposure to AI than any other sector, with law and accountancy trailing not too far behind. The report focuses on "exposure" and not on whether AI will enhance or replace jobs, stating AI is expected to complement most jobs and industries – so all hope is not lost (just yet).

AI Safety Summit and the Bletchley Declaration

The question

What is the impact of the UK's recent AI Safety Summit on the governance of AI systems around the world?

The key takeaway

Representatives of 28 countries as well as other tech companies, academia, and civil society leaders signed the Bletchley Declaration to establish shared agreement and responsibility on the risks and opportunities presented by frontier AI.

The background

As various governments seek to harness the great economic and social potential of AI-driven technology, there has been a coinciding push to put in place the necessary legislative framework to protect the interest of countries, businesses and individuals. In the UK, the government framed its pro-innovation approach to AI regulation in the White Paper it published in March 2023 (covered in our previous Snapshots). This was followed by the UK hosting the AI Safety Summit in Bletchley Park on 1 and 2 November 2023. The summit coincided with the US Government's publication of an executive order on AI safety and the G7's International Code of Conduct on AI.

The development

As part of the summit, the participating 28 countries signed the Bletchley Declaration on AI Safety. The declaration recognises the positive potential impact that AI can have on the world and calls for the alignment of AI development with values that prioritise safety, human-centric design, trustworthiness, and responsibility. In particular, the declaration notes the specific risks presented by frontier AI models - highly capable general-purpose AI models that can perform a wide variety of tasks and for which the potential for intentional misuse and unforeseen consequences are not fully understood.

Significantly, as part of the Bletchley Declaration, leading AI companies such as OpenAI, Google DeepMind, Anthropic, Microsoft, and Meta agreed to allow governments to test their latest models before they are released to the public.

Governments have also agreed to share the results of their evaluations with other nations and to collaboratively develop AI standards over time, thus establishing a foundation for future advancements in international AI safety efforts. As part of the UK's input into the development of the global understanding of AI, the Prime Minister announced that the existing UK Frontier AI Taskforce is to be renamed the AI Safety Institute, with its focus shifting to advanced AI safety for the public. The newly named institute will be in charge of conducting evaluations on AI systems, research into AI safety and sharing developments in the AI sphere with the government and other players in the field.

Why is this important?

The summit reflects the global ambition to regulate AI in a way that promotes its use for economic and societal benefit, whilst balancing the safety concerns. Governments have differing opinions on where to position their respective AI frameworks, with the UK currently taking a less aggressive approach to regulation. However, the summit highlights the importance of a unified and cooperative approach to monitoring the use of AI between countries and the biggest actors in the AI sphere. The summit also marks the commencement of a sequence of discussions among the 28 participating countries. The Republic of Korea has committed to jointly organising a virtual summit on AI within the next six months. Subsequently, France is set to host the next in-person AI safety summit in the Autumn of 2024.

Any practical tips?

The UK Government has come under some criticism for its light-touch approach to AI regulation thus far. Whilst there are no indications that it is likely to alter its "pro-innovation" approach, it is evident that AI is an area of particular interest for the government and naturally we are likely to see further initiatives and legislation as AI's influence continues to grow. Businesses developing AI technologies (particularly those engaged in frontier AI) should be wary to the fact that further laws governing AI are inevitable, and governments have expressed their desire to be involved in the testing of such products.

Companies operating across multiple jurisdictions will have to be cognisant to the patchwork of legislatives frameworks that are springing up across the UK, EU and the US and differing approaches to regulation.

G7 AI Regulation: a new international code of conduct on regulating AI

The question

What is the impact of the G7's new voluntary AI code of conduct?

The key takeaway

Voluntary guidance published by the G7 encourages responsible development of generative AI. Further regulation on a national level should be expected in response.

The background

At the G7 Summit on 19 May 2023, the G7 countries established the G7 Hiroshima Artificial Intelligence Process to promote controls for advanced AI systems on an international level. This is one of several multi-national initiatives around regulating AI; others include the OECD Global Partnership on AI and the Bletchley Declaration agreed by 28 countries at the UK's AI Summit (discussed in a separate Winter 2023 Snapshot).

The development

On 30 October 2023, the countries in the G7 announced the International Guiding Principles on Artificial Intelligence and the International Code of Conduct for Advanced AI Systems (the Code) aimed at companies developing advanced AI.

The Code's purpose is to encourage a collective response to the development of trustworthy AI by setting out a non-exhaustive list of voluntary commitments by companies including:

- taking a preventative approach to risks, particularly by developing recognised processes to test and record them
- considering impact beyond the initial development phase by analysing potential harm to the end-user and society
- creating an open dialogue between developers and society, with developers sharing testing reports and concerns, and their own codes of conduct with government bodies or relevant academics
- being alive to the surrounding social context and the need to use AI to aid global challenges, for example, improving public education. TheCode also gives specific examples of improving knowledge around climate change
- acknowledging privacy and IP rights by implementing training measures and privacy policies.

The Code is likely to be developed in the future following further stakeholder discussion.

Why is this important?

The development of the Code and its international background shows that the international community will respond to growing calls to regulate AI. The Code comes in addition to other responses referenced above, including the EU's more stringent AI Act (discussed in previous Snapshots). The Code is another example of regulation and a sign of more to come, albeit in different forms.

Any practical tips?

Whilst it is currently voluntary, companies developing advanced AI systems should consider ensuring their models are compliant with the Code, as there are likely to be reputational pressures – not least from the public - to demonstrate that AI is safe and trustworthy. Developers should also be alive to the prospect of more regulation at a national level and the challenges with responding to different obligations from different countries if working cross-jurisdictionally.

President Biden's Executive Order: how the US is planning to tame AI

The question

What is the impact of the Biden administration's recent Executive Order on AI?

The key takeaway

The Biden administration has recently issued an Executive Order on Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, outlining a comprehensive approach to AI governance.

The background

AI has been at the forefront of the public consciousness in the last year, promising efficiency and innovation while also causing concerns about security, safety and ethical implications. Different approaches have been taken to AI regulation around the world, for example the draft EU AI Act and the UK AI White Paper (both reported in previous Snapshots).

In October 2022, the US signalled its own approach to AI regulation in a Blueprint for an AI Bill of Rights. This sets out a list of five principles that should guide the design, use, and deployment of automated AI systems to protect the public, including:

- safe and effective systems
- protection against algorithmic discrimination and ensuring that algorithms and systems should be used and designed in an equitable way
- data privacy
- notice that automated systems are being used and an explanation of why and how it impacts you
- ensuring the availability of human alternatives to AI, consideration, and fallback.

The development

The Executive Order follows on from the Blueprint by expressing the US's commitment to establishing clear principles for the governance of AI systems. These principles identify potential harms to protect citizens from, marking a big step in addressing the ethical considerations surrounding AI development and deployment. Significantly, the Executive Order takes a proactive stance by requiring that developers of the most ground-breaking AI systems share safety test results with the US Government before making products and services generally available to the public. Simultaneously, the National Institute of Standards and Technology (NIST) has been entrusted with the responsibility to develop new standards, tools, and tests to guarantee the safety of AI systems. These standards will be applied by the Department of Homeland Security which will also establish an AI Safety and Security Board.

The Executive Order also includes actions to:

- protect citizens from AI-enabled fraud and deception by establishing standards and best practices for detecting AI-generated content and authenticating official content
- establish an advanced cybersecurity programme to develop AI tools to find and fix vulnerability in critical software
- set out a framework to develop standards for biological synthesis screening, thereby protecting against the risks of using AI to engineer dangerous biological materials, and
- develop a National Security Memorandum that directs further actions on AI and security.

Why is this important?

While it does not appear that the US intends to pass any all-encompassing legislation on AI in the next few years (such as the EU AI Act), the Bill of Rights and Executive Order signify that it is actively considering the development and application of new standards. It remains to be seen the form these standards will take, whether these will be legally-binding or recommended, and how the US Government intends to enforce these standards.

Any practical tips?

Businesses developing foundational models and other powerful AI systems should review the new processes in place to provide safety test results to the government before public release. Otherwise, businesses looking to develop, procure, or use AI in the US should keep an eye on further developments, especially any new standards issued by NIST in the future.

New amendments to the Digital Markets, Competition and Consumers Bill signal a lighter touch approach towards CMA enforcement action

The question

How do amendments to the Digital Markets, Competition and Consumer Bill (**DMCC**) impact the Competition and Markets Authority's (**CMA**) ability to take regulatory enforcement action against companies designated as having Strategic Market Status?

The key takeaway

Under new amendments to the DMCC, the CMA will be required to ensure that any enforcement action is proportionate and does not impose unnecessary burdens on businesses operating within the UKs pro-competition regime.

The background

As well as marking the beginning of a new era of enhanced consumer protection in the UK, the DMCC is also set to introduce a new regulatory regime to address concerns around competition in the UKs digital industry and to regulate the companies active within it.

Under the DMCC, the CMA will be able to designate large digital companies as having Strategic Market Status (**SMS**) where: (i) its activity is linked to the UK and meets conditions of having substantial and entrenched market power, and a position of strategic significance; and (ii) it has a turnover exceeding £1billion in the UK or £25billion globally. Where a company is designated as having SMS, they will also be required to abide by the DMCC's code of conduct. The CMA will also have powers to make Pro-Competitive Interventions (**PCIs**) in order to address potentially adverse effects on competition. PCIs will allow the CMA to intervene in the market quickly and flexibly to promote competition. PCIs can take the form of an order from the CMA that imposes a conduct requirement on a company or a recommendation to a regulator of steps that should be taken in order to address a competition concern.

The development

Recent amendments proposed by the UK Government have solidified proposals for the introduction of an appeals process for all regulatory decisions (excluding fines). This means that tech firms designated as having SMS will be able to challenge PCIs on proportionality grounds. This approach enables regulators and relevant tech firms to work together to ensure that competition is maintained throughout the market on an ongoing basis by virtue of ongoing discussions, rather than allowing legal challenges to cause the pro-competition regime that the DMCC seeks to introduce, to become bogged down as challenges to regulatory decisions work their way through the court system.

Furthermore, under the DMCC, the CMA has the ability to impose significant fines for anti-competitive behaviour that could reach into the billions of pounds. The amendments will allow companies to challenge these fines "on their merits" as a means of ensuring that regulatory fines are properly balanced by allowing significant checks and balances. The updates to the DMCC will also allow firms to challenge fines on the substance of the decisions, as well as scrutinising the process taken in order to reach the decision.

Another core element of the proposed legislation is limiting the CMA's ability to impose a conduct requirement or a PCI unless it is demonstrably proportionate to do so. The CMA must also be able to present significant evidence that suitably demonstrates the proportionality of the CMA's decision.

Why is this important?

The proposed updates to the DMCC highlight the government's "functional" regulatory approach that seeks to work with businesses rather than stifling the pro-competition environment the government seeks to foster. Additionally, the proportionality requirements for enforcement action taken by the regulator will ensure that any enforcement action does not have an overly restrictive effect on companies within the digital environment.

Any practical tips?

Whilst those companies that are likely to be designated as having SMS will already be aware of this, it is becoming increasingly important for companies to monitor the DMCC's progress through Parliament to ensure that they are adequately prepared to comply with their incoming obligations. These new amendments will be particularly well-received by the platforms who do not want investigations or enforcement action to unnecessarily slow down their business plans, noting that many have already built in – or are building in – processes, including establishing specific working groups, to work with the CMA in the event of a PCI or a fine.

Reduced scanning obligations proposed for interpersonal communications services

The question

What are the consequences of the recent amendments to the EU's draft legislation to combat Child Sexual Abuse Material (**CSAM**) on private messaging companies?

The key takeaway

The proposed version of the law narrows obligations on interpersonal communication services, such as webmail messaging services and internet telephony, to scan their services. It introduces targeted detection through judicially backed time-limited orders and excludes end-to-end encryption from the scope of the detection orders.

The background

On 11 May 2022, the European Commission adopted a proposal for a new law to prevent and combat child abuse, as part of a greater collective EU action to tackle child sexual abuse material online. The Commission proposal would require internet providers to assess whether there is an important risk of their services being misused for online child sexual abuse and to take appropriate steps to mitigate these risks. The proposal has been subject to contentious debate, due to concerns regarding privacy and security.

The development

On 14 November 2023, lawmakers at the European Parliament agreed on a series of amendments to the draft legislation in an attempt to strike the right balance between protecting children and protecting privacy. The draft Parliament position is currently pending endorsement by the plenary.

To avoid blanket scanning of messages, the amended position proposed targeted detection for CSAM, through the introduction of time-limited orders that judicial authorities could issue to digital messaging providers for detection and take-down of CSAM.

The Parliament position further specifies that the orders must be issued as a last resort, where mitigation measures are not effective and if there is "reasonable grounds of suspicion a link [...] with child sexual abuse material".

Importantly, the amendments also ensure that end-to-end encrypted private message services fall outside the scope of the detection orders.

Why is this important?

Under the draft position, private messaging services will face narrower obligations with relation to interpersonal communications, which is essential to safeguard end-to-end encryption of user's communications. The amendments also ensure that online service providers are not made subject to general obligations to monitor the data that they transmit or store for their users.

Any practical tips?

Practical steps for platforms to consider taking include:

- conducting risk assessments to identify whether and to what extent their services are likely to be misused for online child sexual abuse
- reviewing their existing technologies and considering how they can establish processes and systems to ensure compliance with the safeguards foreseen by the law
- considering whether they will be regulated by the Online Safety Act and, if so, assess any intersection between their obligations under the Online Safety Act and the draft CSAM proposal.

New development: government makes changes to voluntary code of practice for app store operators and developers

In our Spring 2023 Snapshots, we reported on the Department for Digital, Culture, Media and Sport's (**DCMS**) voluntary code of practice for app store operators and developers (the **Code**).

In October 2023, the Department for Science, Innovation and Technology (**DSIT**) made amendments to the Code, notably extending the implementation period of the Code by nine months following concerns regarding barriers to implementation and lack of clarity for some of the Code's provisions. The eight principles stipulated by the Code must now be implemented by June 2024. DSIT has said that it shall use the extended implementation period to improve monitoring and increase engagement.

Other key changes include:

- a reformed appeals process allowing developers one week to challenge the removal of a malicious app from an app store (Principle 1)
- the requirement for users to be able to delete their data on an app is removed; now developers must only provide means for users to request deletion (Principle 2)
- all vulnerability disclosure processes must now be accessible from the app store. The 15-day time limit for the developer to acknowledge a vulnerability report has been removed (Principle 3)
- it is no longer mandatory for operators to remove an app which has not been updated for two years (Principle 4)
- if a developer challenges the removal of an app not considered malicious, users shall not be notified of the removal until the appeals process ends (Principle 5)
- a reformed process for personal data security incidents (Principle 8).

Clearview AI cleared of £7.5m ICO fine for processing data outside the UK

The question

Just how did the processing of personal data by Clearview AI (**Clearview**) fall outside the scope of UK GDPR?

The key takeaway

The decision of the First-tier Tribunal (General Regulatory Chamber) (the **Tribunal**) stated that, while Clearview was processing personal data related to the monitoring of UK data subjects, because Clearview was not processing the personal data for commercial purposes and Clearview's client base was exclusively comprised of non-UK criminal law enforcement agencies, national security agencies, and contractors associated with those agencies, Clearview's processing of personal data fell outside the scope of UK GDPR.

The background

On 18 May 2022, the Information Commissioner's Office (**ICO**) issued an enforcement notice and a monetary penalty notice against Clearview for numerous alleged breaches of GDPR and UK GDPR and imposed a fine on Clearview of over £7.5m.

The ICO's notices related to Clearview's compilation and operation of a database of over 20 billion images of individuals' faces which were automatically scraped from the internet. These scraped images enabled Clearview to generate coordinates (vectors) of individuals' faces. Clearview's clients could then upload an image of an individual to Clearview's system. Clearview's system would generate vectors of that individual's face from the uploaded image and use a facial recognition system to find similarities between the uploaded image and other images scraped from the internet to deliver comparisons to Clearview's clients.

This enabled Clearview's clients to identify an individual or to assess what an individual was doing at a particular moment in time (ie the time the image was scraped) through the objects or activities which appeared in the image. Clearview's clients could also undertake successive searches of the same image over time which, the ICO argued, provided Clearview's clients with the potential to monitor the behaviour of the pictured individuals.

The development

The Tribunal found, given the size of the database, and that between June 2019 and March 2020 Clearview had offered its service to law enforcement and government agencies in the UK, that it was reasonable to infer that some images of UK residents were contained in Clearview's system. Further, it was found that the images held in Clearview's database constitute personal data and the vectors derived from the image of an individual's face constitute special category data under UK GDPR.

Additionally, the Tribunal found that, while every photographic image of an individual will reveal something about that individual (eg that they were alive when it was taken), "monitoring" of an individual by Clearview's clients could include:

- establishing where an individual was a particular point in time
- watching an individual over time by repeated uploading of the same image
- using the results produced to provide a narrative about the person in the images at the different times
- combining the results with information obtained from other forms of monitoring or surveillance.

The Tribunal also stated that an image which revealed an individual's "behaviour" could include:

- where they are
- what they are doing (including what they are saying/have said, what they have written, their employment or their pastimes)
- who they associate with in terms of relationship
- what they are holding or carrying
- what they are wearing (including items indicating cultural or religious background or belief).

Given the above, the Tribunal found that Clearview's service itself did not monitor the behaviour of individuals because generating vectors of individuals' faces from their scraped images did not monitor the behaviour of those individuals.

However, the Tribunal determined that, as there was such a close connection between the creation, maintenance and operation of Clearview's database, and the monitoring of the behaviour of individuals which was being undertaken by Clearview's clients, Clearview's activities were "related to" the monitoring of individuals' behaviour. Further, the Tribunal found that, even though it was unlikely that UK data subjects' images would be produced as part of a search carried out by Clearview's clients related to crimes which occurred in their respective jurisdictions, Clearview's system would nonetheless process the personal data of UK individuals.

Nonetheless, the Tribunal was satisfied that all of Clearview's clients carried out criminal law enforcement or national security functions. As such, the Tribunal found that, as the acts of foreign governments fell outside the scope of European Union (EU) law, and it was not for one government to bind or control the activities of a foreign state, Clearview's processing fell outside the scope of EU law before the UK's exit from the EU, and therefore it did not constitute "relevant processing" as required under Article 3(2) UK GDPR for the UK GDPR to apply.

As such, the UK GDPR did not apply to Clearview's processing of personal data in this case and the ICO did not have jurisdiction to issue the enforcement notice or monetary penalty notice against Clearview.

Why is this important?

On 17 November 2023, the ICO released a statement announcing that it sought permission to appeal the Tribunal's decision. The basis for the ICO's appeal is that the Tribunal erred in finding that "Clearview's processing fell outside the reach of UK data protection law". Notwithstanding the ICO's appeal, the decision nonetheless reinforces the position that, where an organisation is not established in the UK and has no clients in the UK, if it provides commercial services which are related to the monitoring of the behaviour of individuals living in the UK, it will fall within the territorial scope of UK GDPR and the jurisdiction of the ICO.

Any practical tips?

It's rare for any organisation which processes the personal data of UK individuals to avoid the scope of the UK GDPR, particularly where an element of the processing is for commercial purposes. The factual matrix behind this decision – the processing of data by companies outside the UK for purposes related to foreign criminal law enforcement or national security functions – is narrow, but it is nonetheless interesting to see where a gap in the reach of the UK GDPR may be. It is of course safest always to consider the processing to be caught and work backwards from there, rather than the other way round.

ICO issues preliminary enforcement notice against Snap for its "My AI" chatbot

The question

How can organisations who wish to join to the world of generative AI ensure that they adequately assess the risks from the perspective of the Information Commissioner's Office (**ICO**)?

The key takeaway

Organisations should ensure that the risk assessment which they conduct, prior to their implementation of generative AI technologies, adequately addresses both the benefits and the risks which such technologies pose to data subjects, especially where a portion of those data subjects are children.

The background

On 6 October 2023, the ICO announced that it had issued a preliminary enforcement notice against Snap Inc. and Snap Group Limited (**Snap**), alleging that they had failed to adequately evaluate the risks which were associated with Snap's rollout of its AI-powered chatbot "My AI".

"My AI" was the first generative AI technology to be built into a messaging platform in the UK when it was launched on 27 February 2023. "My AI" was originally launched for Snapchat+ subscribers as a feature of the Snapchat app, but it was later rolled out to all Snapchat users on 19 April 2023.

The tool, which is powered by OpenAI's GPT technology, is a chatbot which can be used by Snapchat users to answer such questions as: what gift to buy, what hiking trip they should go on at the weekend, or what they should make for dinner. As a Snapchat user uses "My AI" it becomes more personalised over time, learning more about the user, and making users feel as though they are chatting with a friend.

The development

Following its investigation, the ICO provisionally found that the risk assessment, which was carried out by Snap prior to the rollout of the "My AI" feature, did not sufficiently evaluate the risks which are associated with the implementation of generative AI technology, especially given that the technology would be used by Snap to process the personal data of children aged 13-17. To stress, the ICO's findings are provisional, and Snap will have an opportunity to respond to the ICO before a final decision is made, or any fine is imposed. The preliminary enforcement notice outlines the potential actions which Snap could take to address the ICO's concerns. Of course, if the ICO chooses to issue a final enforcement notice, Snap could be prevented from processing UK users' personal data for the purposes of the "My AI" feature.

Why is this important?

The preliminary notice issued by the ICO emphasises the importance for organisations of conducting fulsome risk assessments before launching a product which incorporates new, innovative technologies. These risk assessments should analyse both the benefits and the risks which may be posed by new technologies to all categories of data subject concerned. According to the ICO's "Generative AI: eight questions that developers and users need to ask" (see here), the ICO emphasises that conducting an adequate Data Protection Impact Assessment (**DPIA**), and keeping the DPIA updated as the processing of personal data evolves, will assist organisations with assessing and mitigating any data protection risks before they start processing personal data.

Any practical tips?

The preliminary enforcement notice issued by the ICO is an important reminder that organisations need to be live to the privacy risks which are posed to their data subjects by the implementation of generative AI technologies. As a starter, any organisation which is considering developing or implementing generative AI technology should consider:

- the ICO's "Generative AI: eight questions that developers and users need to ask" (see here)
- the ICO's updated guidance on "AI and data protection" (see our Summer 2023 Snapshot article here)
- the ICO's guidance on "Data protection by design and by default" (see our Summer 2023 Snapshot article here).

ICO publishes guidance to ensure lawful monitoring in the workplace

The question

How can employers monitor their workers whilst maintaining their trust and complying with data protection regulation?

The key takeaway

On 3 October 2023, the UK's Information Commissioner's Office (**ICO**) issued new guidance – "Employment practices and data protection: monitoring workers" (the **Guidance**) – to help businesses interpret the law on monitoring in the workplace. The Guidance aims to provide employers with greater certainty, to protect employees' data protection rights and help employers build trust with their employees, service users and customers.

The background

The Guidance replaced the Employment Practices Code of 2011 and was published after a 3-month consultation period. The consultation revealed that almost one in five people feel like they are being monitored and 70% of the public would find it intrusive for their employers to monitor them.

The issuing of the Guidance comes in response to an increasing number of businesses implementing new technologies to monitor their workers since a rise of remote working following the Covid-19 pandemic. The UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA**) do not prohibit business from monitoring their workers using new technologies but highlights that they must do so without infringing their privacy rights as well as having lawful grounds to do so.

The development

The Guidance focusses on how employers can apply best practice and remain transparent and fair while monitoring their workers. Monitoring can take many forms, including tracking the worker's keystrokes and calls, taking screenshots, recording webcam footage and audio recordings, or using new technology which monitors and tracks activity.

When identifying whether a lawful ground for monitoring a worker applies, the ICO encourages business to thinks about why they want to monitor the workers and document all the grounds that apply. They do not suggest having a one-size fits all policy. The ICO states that monitoring workers under the legitimate interests ground is the most flexible basis and could apply in a wide range of circumstances. This entails monitoring workers where it is necessary for the business' own legitimate interests or those of a third party.

The Guidance also reflects on new tools and technologies, as well as the potential of AI. It discusses automated monitoring tools, meaning those that do you not use any human involvement. Uses include those for security purposes, managing workers' performance and monitoring attendance and sickness, for example if a worker is away from their desk.

The Guidance also looks at biometric data, being someone's unique personal data, including fingerprints, iris scanning, retinal analysis and facial/voice recognitions. This type of data is unique under data protection law as its status can change depending on the use of it. For full coverage on the ICO's draft guidance on biometric data and biometric technologies, see our Autumn 2023 edition of Snapshots.

Why is this important?

Non-compliance with data protection regulation can have wide ramifications. The Guidance shows how the ICO expects companies to comply and provides a frame of reference for businesses that do want to monitor their employees.

Any practical tips?

The Guidance is particularly helpful for its wide range of examples throughout, which companies and individuals are encouraged to review and compare to their own practices to ensure they any monitoring of employees is conducted lawfully. There are also a useful set of baseline checklists at the end of the Guidance.

ICO publishes its draft "Data Protection Fining Guidance" for public consultation

The question

How will the Information Commissioner's Office (**ICO**) calculate the amount of a fine under the UK GPDR and the Data Protection Act (**DPA**) 2018?

The key takeaway

The ICO has published its draft "Data Protection Fining Guidance" (the **Guidance**) for public consultation (see here). The Guidance addresses: (i) the ICO's power to impose fines, (ii) how a fine may arise, and (iii) how the ICO calculates the amount of a fine under UK GDPR and the DPA 2018. Importantly, the Guidance clarifies that, where the ICO finds that the "same or linked processing operations" infringe more than one provision of UK GDPR, the overall fine imposed will not exceed the maximum amount applicable to the most serious of the individual infringements.

The background

On 2 October 2023, the ICO published the Guidance for public consultation. In the Guidance, the ICO explains that it may only exercise its power to impose fines under Article 58(2)(i) and Article 83 UK GDPR by giving a penalty notice to a controller or processor in accordance with section 155 of the DPA 2018. Further, the Guidance states that it updates and replaces the sections of the Regulatory Action Policy which were published on 7 November 2018, and which currently set out how the ICO determines: (i) when to issue a penalty notice, and (ii) the amount of a fine under UK GDPR and the DPA 2018. The consultation closed on 27 November 2023.

The development

The key sections of the Guidance set out: (i) the infringements of the UK GDPR and the DPA 2018 for which the ICO may impose a fine, (ii) the factors which the ICO may have regard to when deciding to issue a penalty notice, and (ii) how the ICO determines the amount of a fine.

The infringements for which the ICO may impose a fine

Here, the Guidance provides that the ICO may choose to impose a fine where a controller or processor has not complied with the provisions of UK GDPR or the DPA 2018 in relation to:

- the principles of processing
- the rights conferred on data subjects
- the obligations placed on controllers and processors, or
- the principles for transfers of personal data outside the UK.

Further, the ICO may impose fines where a controller has failed, or is failing, to comply with a requirement to pay a data protection fee, or other charges, to the ICO. The Guidance also explains that the ICO may choose to impose a fine on a person for a failure to comply with their requirements under the DPA 2018 including a failure to:

- provide information which the ICO reasonably requires to assess compliance with the UK GDPR or the DPA 2018
- permit the ICO to inspect or examine documents, information, equipment, or material for the purposes of assessing compliance with the UK GDPR or DPA 2018, or
- comply with a requirement set out in a previously issued ICO penalty notice.

The factors which the ICO will consider when deciding to issue a penalty notice

In determining whether to issue a penalty notice, the Guidance states that the ICO must have regard to Article 83(1) and Article 83(2) UK GDPR, or section 155(3) DPA 2018. The factors which the ICO will have regard to include:

- the nature, gravity and duration of the infringement(s), the purpose of the processing, the number of data subjects affected by the infringement(s), and the level of damage suffered
- whether any infringement(s) were intentional or negligent
- any action taken to mitigate the damage suffered by data subjects
- the degree of responsibility of the controller or processor (given the technical and organisational measures which they have implemented)
- any relevant previous infringement(s) by the controller or processor
- the degree to which the controller or processor cooperated with the ICO to remedy the infringement(s) and mitigate adverse effects
- the categories of personal data affected by the infringement(s)
- the manner in which the infringement(s) became known to the ICO
- any other applicable aggravating or mitigating factors.

Determining the amount of a fine

The Guidance states that, to calculate the amount of a fine, the ICO will consider:

- the seriousness of the infringement(s)
- the worldwide annual turnover of the controller or processor (where the controller or processor is part of an "undertaking")
- where the starting point for the fine should be (in consideration of the above points)
- adjusting the fine in consideration of any aggravating or mitigating factors
- whether imposing the fine would be effective, proportionate, and dissuasive.

Further, the Guidance states that the maximum fine which the ICO can issue will also depend on whether the controller or processor forms part of an "undertaking" (eg the controller is a subsidiary of a parent company). This affects the maximum fine which the ICO can impose as follows:

FINE TYPE	NOT AN "UNDERTAKING"	UNDERTAKING
Standard maximum fine	£8.7m	£8.7m or 2% of worldwide turnover in the preceding financial year, whichever is higher
Higher maximum fine	£17.5m	£17.5m or 4% of worldwide turnover in the preceding financial year, whichever is higher

Why is this important?

Once finalised, the Guidance will provide controllers and processors with a means of estimating the fines that they may face where something goes wrong. Further, the Guidance sets out the key points which the ICO will have regard to when evaluating new and existing infringements for which a notice of intent to impose a fine has not yet been issued.

Any practical tips?

As the Guidance provides controllers and processors with a means of assessing what factors the ICO will consider when determining whether to impose a fine, organisations should stress-test their playbooks, processes and training against it to ensure that they continue to do everything possible to prevent, or at least mitigate, the level of fines they could be exposed to where something goes wrong.

DATA

EU Advocate General's opinion on data subjects' rights to compensation for non-material damage under the GDPR

The question

Does the theft of an individual's sensitive personal data by a wrongdoer give rise to compensation for non-material damage under Article 82 EU General Data Protection Regulation (**GDPR**), if the wrongdoer has not used, or taken steps to use, the sensitive personal data for any purpose?

The key takeaway

The opinion handed down by EU Advocate General (**AG**) Michael Collins states that, under GDPR, the possession of personal data by a wrongdoer, without any steps being taken by the wrongdoer to use the personal data to impersonate a data subject, does not constitute "identity theft". However, the opinion provides that the theft of a data subject's sensitive personal data may give rise to a right to compensation under Article 82 GDPR where: (i) there is proof that GDPR has been infringed, (ii) actual damage has been suffered by the data subject, and (iii) there is a causal link between the GDPR infringement and the damage the data subject has suffered.

The background

On 26 October 2023, the AG published its opinion on the Court of Justice of the European Union's (CJEU) website. The opinion, which the judges of the CJEU will consider before making a final decision, concerns the cases of *JU v Scalable Capital GmbH* (Case C-182/22) and *SO v Scalable Capital GmbH* (Case C-189/22).

These cases relate to claims by data subjects for the pain and suffering (ie non-material damage) which they claim they suffered following the theft of their sensitive personal data by unknown wrongdoers from a trading application managed by Scalable Capital. As such, the local court in Munich sought the CJEU's guidance on: (i) the interpretation of the concept of "non-material damage" under Article 82 GDPR, and (ii) what constitutes "identity theft" under Recital 75, GDPR.

The development

In relation to the interpretation of the concept of "non-material damage" under Article 82 GDPR, the AG's opinion concurs with the preliminary ruling of the *CJEU in UI v Österreichische Post AG* (see our Summer Snapshot here). As such, the AG has reiterated that to receive an award of compensation for non-material damage under Article 82 GDPR, a data subject must demonstrate that: (i) they have suffered damage, (ii) there has been an infringement of the GDPR, and (iii) the infringement is linked to the damage the data subject suffered.

In relation to what constitutes "identity theft" under Recital 75 GDPR, the AG's opinion provides that the GDPR does not explicitly define the concept of "identity theft". However, the AG's opinion also states that a "systematic interpretation of Recital 75" supports the view that "identity theft" occurs where a wrongdoer misuses a data subject's personal data in order to "feign" that data subject's identity. As such, the opportunity for a wrongdoer to use certain personal data to impersonate a data subject in the future, without any intention or steps being taken to do so, does not constitute "identity theft" because it only presents an abstract possibility that damage might occur in the future.

Given the above, the AG has opined that, where the points under *UI v Österreichische Post AG* can be demonstrated by a data subject (as detailed above), a data subject will be entitled to compensation for non-material damage under Article 82 GDPR.

Therefore, an award of compensation for non-material damage under Article 82 GDPR is predicated on whether a data subject can demonstrate that an infringement of the GDPR has occurred, and that the data subject actually suffered damage due to that infringement. As such, this will come down to the particular facts of the case in question.

Why is this important?

While the opinion of the AG is not binding on the CJEU, or applicable to the UK, it will be considered by the judges in the CJEU before they make a final decision in these two cases. As such, it provides organisations with a useful example of what the courts could require a data subject to prove in order to ground a claim for non-material damages under Article 82 GDPR.

Further, once a final decision in these cases is made by the CJEU, the decision will represent a persuasive authority and is likely to inform how the UK courts, and the Information Commissioner's Office (**ICO**) will respond to similar compensation claims by UK data subjects.

Any practical tips?

While the AG's opinion is not binding in the UK, UK organisations should still consider tracking the progress of cases concerning claims by data subjects for non-material damages under Article 82 GDPR. These cases provide a feel for how the UK courts (and the ICO) may respond to similar claims against their UK controllers – and in turn help assess potential exposure to the ever-present threat of class actions by aggrieved data subjects.

New development: EDPB provides clarification on tracking techniques covered by the ePrivacy Directive

On 14 November 2023, the European Data Protection Board (**EDPB**) adopted a set of new guidelines (the **Guidelines**) on the technical scope of Article 5(3) of the ePrivacy Directive (the **ePD**). The Guidelines seek to elucidate the scope of the ePD and its applicability to emerging tracking tools. While the effective use of Article 5(3) is widely recognised and applied to certain tracking technologies like cookies, further clarity was needed regarding the application of this provision to new tracking methods, in order to remove ambiguity for data controllers and individuals.

The Guidelines clarify that the scope of Article 5(3) of the ePD extends beyond cookies and will also apply to emerging tracking methods. In doing so, the EDPB identified four key elements for the applicability of Article 5(3), offering a detailed analysis of each: "information", "terminal equipment of a subscriber or user", "gaining access" and "stored information and storage". Further, the Guidelines also examine a number of specific use cases, including URL and pixel tracking, local processing, tracking based on IP, intermittent and mediated Internet of Things reporting and unique identifier collection.

In the UK, the Privacy and Electronic Communications Regulations (**PECR**) implement the ePD, with Article 5(3) of the ePD being reflected as Section 6 of the PECR. PECR complements the general data protection regime, (under the Data Protection Act 2018 and the UK GDPR) and stipulates specific privacy rights on electronic communications. Whilst the new Guidelines are not directly applicable to PECR, given that the UK has left the EU, they may offer further guidance into newly emerging tracking tools. For further information on Section 6 of PECR, the ICO has published guidance on the use of cookies and tracking technologies.

CONSUMER

CONSUMER

Ofcom issues draft guidance and launches consultation on the Online Safety Act 2023

The question

What can platforms expect from Ofcom, as it steps into its new role regulating compliance with the Online Safety Act 2023 (the **Act**)?

The key takeaway

Ofcom is deploying its new resources and increased headcount to implement a fast-moving approach to regulation, and has already issued draft compliance measures and guidance on risk assessments and record keeping for industry review.

The background

After years of debate and parliamentary review, the Act came into force on 26 October 2023. It will impose requirements on firms to take steps that will aim to protect children and adults from all manner of online harms, ranging from content promoting suicide, to human trafficking communications, to child pornography. Read more about the Act here.

Much of the Act requires secondary legislation from the Secretary of State before it is effective, and Ofcom (as promised) is taking an active role in guiding what that secondary legislation, and later Codes of Practice, may look like.

The development

Mere days after the Act received Royal Assent, Ofcom launched the first of four consultations on how the Act will be implemented and enforced. The regulator is calling for industry input on measures it believes firms should implement, and also on draft guidance that will seek to inform and direct firms when they are considering how to implement the proposed measures which include:

- measures proposed for user-to-user (**U2U**) services
- measures proposed for search services
- draft guidance on risk assessments and reviews
- draft guidance on record keeping duties.

Proposed measures

The proposed measures are wide-ranging and comprehensive. For U2U services, they are split into the following headings:

- Governance & Accountability
- Content Moderation
- Automated Content Moderation
- Reporting and Complaints
- Terms of Service
- Default Settings and Support for Child Users
- Recommender Systems
- Enhanced User Control
- User Access.

Search service measures currently overlap slightly with the U2U proposals, although naturally there are deviations:

- Governance & Accountability
- Search Moderation
- Search Automated Content Moderation
- Reporting and Complaints
- Publicly Available Statements
- Search Design.

Not all of the measures suggested by Ofcom are intended to apply to all firms. Instead, a firm will be required to implement more measures based on the size of the service provided, and the risk profile of that service.

This means a firm providing "larger services" (ie one serving an average user base greater than 7m users per month in the UK) will be subject to higher standards than a firm providing "smaller services" (ie less than 7m users). Further, a service's risk profile will fall into one of three categories: (1) low risk; (2) specific risk; and (3) multi risk.

Draft guidance

Based on the current guidance, all firms (irrespective of size), will be under a duty to carry out a "suitable and sufficient" risk assessment. These risk assessments will need to be reviewed annually, but also whenever Ofcom makes an update to the risk profile of the relevant services, or the firm makes a significant change in relation to the design or operation of its services.

The guidance in relation to record keeping is currently quite vague and fairly uncontroversial, providing that risk assessment records must be kept in a durable, easy-to-understand format for at least 5 years. They must also be kept up to date, including making any necessary amendments when Ofcom issues new Codes of Practice – and it appears there will be many of those to come.

Why is this important?

The Act imposes broad compliance duties on firms providing online services. Larger firms are subject to heavier regulatory burdens, but even smaller companies are subject to a large portion of the measures Ofcom expects to see from complying businesses.

The consultation represents an opportunity to engage with Ofcom and to provide input that will be necessary to ensure the regulation and enforcement of the Act is done sensibly and practically. Non-compliance with the Act can incur criminal liability in some cases, and Ofcom has powers to fine firms up to 10% of global turnover.

Finally, whilst the guidance may be in draft form, it still offers useful insights into the approach Ofcom will be expecting firms to take when they conduct their risk assessments and the measures they are expected to put in place, as required by the Act.

Any practical tips?

- Respond to the consultation.
  It represents a critical opportunity for businesses to have their say on how this critical piece of legislation will be interpreted and enforced by Ofcom.
- Review the draft measures and consider their application to your business.
  Although not yet binding, it offers an insight into the sorts of measures which will need to be implemented once Ofcom is clear on what it wants to see. If your current processes fall short of the draft measures, the sooner you can identify your weak spots and areas for improvement, the better.
- Look out for future Ofcom activity.
  Ofcom has been clear that it is working quickly on this and expects to launch four consultations on the Act in total. There is more to come, so keep it on your radar.

Last chance saloon: EU consumers only have one opportunity to withdraw from auto-renewing subscription contracts

The question

When do EU consumers have a right to withdraw from subscription contracts? And how will this differ to the UK's approach under the new Digital Markets, Competition and Consumers Bill (**DMCC**)?

The key takeaway

The European Court of Justice (**ECJ**) has confirmed that EU consumers only have a right to withdraw from subscription contracts at the start of the contract, provided consumers have been clearly informed of their right to withdraw. This means that customers do not get a further right to withdraw when a free trial period ends or when a subscription automatically renews. This position marks a significant difference to upcoming new UK legislation aimed at dealing with subscription traps.

The background

As we reported in our Summer Snapshots, the European Commission has been developing its consumer rights agenda and seeking to improve consumer protection measures.

On 5 October 2023, the ECJ held that Article 9(1) of the Consumer Rights Directive (**CRD**) granting the "14 day cooling off period" must be interpreted to mean that consumers only have one window within which to withdraw from distance contracts that include a free trial period and if consumers have been informed in a "clear, comprehensible and explicit manner" that payment is required after the trial period ends.

This ruling was made following a request from the Supreme Court of Austria on whether Verein für Konsumenteninformation (**VKI**) was correct in asserting that Sofatutor GmbH, a German business offering a 30-day free trial for access to its education services, should be ordered to inform its customers of the "conditions, time limits and procedures" for exercising their right to withdraw from subscriptions as the trial was approaching its end.

The development

One opportunity to withdraw

VKI argued that a correct interpretation of Article 9(1) CRD would grant consumers a right to withdraw not only when their 30-day free trial with Sofatotur started but also when the trial ended and the contract converted into a paying subscription, as well as whenever that subscription automatically renewed again in future.

However, although the ECJ found that the extension of an existing fixed term contract could give rise to a renewed right to withdraw, this was not implicit in a contract that includes a free trial period, or automatic renewals, when consumers have been informed from the outset that these are features of the contract.

Requirement to inform

The ECJ's decision also highlights the importance of Article 6(1)(h) CRD's requirement for consumers to be informed of the "conditions, time limit and procedures" for exercising their right to withdraw from distance contracts within 14 days. The purpose of this right is to give consumers an opportunity to examine and understand the services they are receiving and which they need because the contract is being agreed remotely. Consequently, if this information is not provided, or the terms of a contract change significantly when a free trial period ends, then a new right to withdraw may emerge.

Why is this important?

This decision is interesting as it will represent a post-Brexit divergence between the EU and the UK on the topic of subscription contracts – see the UK's incoming DMCC, which we covered in our Summer Snapshots.

Under the DMCC, consumers will have the right to cancel a subscription contract during both an initial free trial period and again during a "renewal cooling off period" which starts when a free trial ends. Further renewal periods will also start "at any time" another renewal payment is due, such as when subscriptions automatically renew. The planned rules also ensure that UK consumers receive a second renewal period if businesses follow a "freemium" model, such as by giving limited access to their service during a free trial and saving their full offering until a paid subscription starts.

Additionally, whilst those trading in the UK will also be required to inform consumers of their right to withdraw from subscription contracts, failure to comply with this obligation is set to become a criminal offence. Comparatively, the CRD takes a much more lenient position of only extending consumers' withdrawal periods by up to 12 months if they are not correctly informed.

Any practical tips?

Whilst this decision allows businesses operating in the EU to be clear that offering free trials and auto-renewing subscriptions will not create new rights for consumer to withdraw from contracts, it also highlights that businesses should provide clear terms governing the entirety of such contracts as soon as any free trials begin.

The key piece to watch here, however, is that businesses operating in both the UK and the EU should be aware of the upcoming divergence that the UK's DMCC will bring. Businesses may want to consider using separate terms for governing such contracts in the UK and the EU, much as this may feel like a practical headache to implement. On the flip side, if businesses wish to only use one set of terms across both jurisdictions then they will need to comply with the UK's upcoming, and much more consumer friendly, requirements.

CONSUMER

European consumer group files greenwashing complaint over water bottle recyclability

The question

Will a consumer group complaint about recyclability and the use of green imagery on water bottle packaging be successful in proving a breach of EU regulations against greenwashing? And what will this mean for wider industry using recyclable or recycled packaging?

The key takeaway

The Bureau Européen des Unions de Consommateurs (**BEUC**), the European consumer organisation, has filed a complaint to European authorities against a number of drinking water bottle traders about claims of their products' recyclability. The BEUC has stated that "such claims do not comply with the EU rules on unfair commercial practices".

The background

The vast majority of consumer-facing advertising, sales and marketing legislation within the EU currently falls under the Unfair Commercial Practices Directive (2005/29/EC) (**UPCD**). December 2021 saw updates made to its detailed guidance. Key changes included, among others, guidance on:

- the need for relative statements
- avoiding distorting claims
- the meaning of labelling schemes, certificates and logos.

In further efforts to combat "greenwashing", in September 2023, the Green Transition Directive was provisionally agreed.
This will ban practices such as making a generic environmental claim if it cannot be demonstrated in accordance with the requirements set out in "Regulation (EC) 66/2010 (EU Ecolabel), officially recognised eco-labelling schemes in the Member States, or other applicable Union laws".

These amendments form part of the EU's drive to tackle misleading environmental claims, an issue identified in the EU's 2019 Green Deal. In March 2023, the Commission put forward a Green Claims Directive, which would impose new regulations businesses seeking to substantiate and communicate explicit environmental claims.

The development

The BEUC has raised a complaint with the EU Commission about green claims made by major water bottle traders. The complaint follows a report carried out by BEUC together with non-profit ClientEarth and NGO ECOS - Environmental Coalition on Standards. The consumer group contends that the recyclability claims are misleading consumers. The BEUC stated: "The beverage industry resorts to recyclability claims that according to our research are too vague, inaccurate or/and insufficiently substantiated".

Their complaint focuses on three key green claims:

- "100% recyclable" depends on many factors outside of the manufacturer's control, including the available infrastructure, the sorting process and the recycling process
- "100% recycled" suggests that the bottle in its entirety is made from recycled materials, when bottle lids cannot be made of recycled materials by EU law and some brands also add non-recycled plastic to the body
- use of green imagery, such as closed loops, green logos or nature images, promotes the idea that the products have environmental neutrality or even a positive impact on the environment.

The group is therefore calling for an investigation into these claims by the European Commission and the network of consumer protection authorities.

Why is this important?

Consumer groups are calling on authorities to take action, using existing regulations to target potential greenwashing and misleading statements across the EU. While new EU directives relating to green claims are on the table, it will take some time for these to be enacted by Member States and further time for enforcement action to be taken. The BEUC's complaint argues that current regulations cover a number of the green claims made by major traders in the drinks industry that require enforcement today.

Any practical tips?

The BEUC's complaint is a reminder that attacks on greenwashing can come from all directions, not just the regulators initiating their own investigations. Consumer groups are also forcing the pace of change, here in an action which may have far-reaching consequences for any business with recyclable or recycled packaging.
The message is clear, namely that greenwashing remains one of the hottest topics in the consumer sphere right now, and businesses must approach any green claim (wording, imagery or otherwise) with extreme care and (very early) input from their legal teams.

Platforms with Irish HQs win EU case to follow Irish law

The question

Do platforms have additional regulatory obligations in EU states, even if they don't have a registered office there?

The key takeaway

Tech companies are not required to abide by additional regulatory obligations in EU countries where they are not based, according to a recent ruling by the European Court of Justice (**ECJ**) concerning Austrian laws.

The background

Many tech companies, including Meta, Google and TikTok have their EU headquarters in Ireland, and are subject to Irish laws. They are protected under the EU's E-Commerce Directive, as companies are free to provide online services from a Member State to other Member States through the "country of origin" principle. Member States may not restrict this freedom unless very specific requirements are met, meaning a company headquartered in Ireland would not usually be subject to additional regulatory laws in Austria if they are providing online services there.

However, an Austrian law, imposed in 2021, required communications platforms to set up mechanisms to ensure reporting and verifying for potentially illegal content and provide regular, transparent publication reports of illegal content. The punishment for not doing so was a fine of up to €10m. Soon after their attempt to enforce the law, an Austrian court faced fightback from the tech companies who insisted that they should not be subject to the laws of a country where they are not established. The matter was referred to the ECJ who ultimately agreed with them.

The development

The key takeaways of the decision are:

- in 2021 Austria passed a law that would oblige tech companies to set up mechanisms to ensure reporting and verifying for potentially illegal content and provide regular, transparent publication reports of illegal content. This applied to companies providing online services in Austria, even if they were not physically headquartered in Austria
- Google Ireland, Meta Platforms Ireland and TikTok, all based in Ireland, brought a claim arguing that this was contrary to EU law
- the ECJ agreed that EU Member States may not oblige communication platforms which are based in other Member States to follow general and abstract obligations
- the ECJ agreed with the tech companies over their concerns about the "principle of control in the member state of origin" and that a contrary decision would undermine the "mutual trust between member states and contravene the principle of mutual recognition"
- the ECJ also highlighted that the rules pursuant to the Austrian law "would ultimately amount to subjecting the service providers concerned to different legislation" that would generally undermine the free movement of goods and services across the EU.

Why is this important?

This decision is an important reinforcement of the "country of origin" principle, particularly where individual EU member states (as here with Austria) seek to impose their own additional regulatory requirements and fines.

Any practical tips?

Although the ECJ decided in the platforms' favour in this instance, it goes without saying that the EU terrain remains an incredibly challenging one for them with the slew of EU regulation coming their way or already landed – not least the Digital Services Act, the Digital Markets Act and the Omnibus Directive to name just a few. Getting their arms round these at speed remains the priority and a huge practical challenge.

New development: European Parliament adopts draft report to address the addictiveness of digital platforms

Earlier this year, the European Parliament published a draft report (the **Report**) on the addictive design of online services and consumer protection. The Report has now been adopted, with overwhelming support (38 votes in favour, none against and 1 abstention), by the Internal Market and Consumer Protection Committee (**IMCPC**) of the European Parliament. The IMCPC had repeatedly expressed concern over the addictive design features of certain digital services and called for the promotion of ethical design by default. The adoption of the Report signals the European Parliament's intent to address the addictive nature of digital services like online games, social media, streaming platforms and online marketplaces which have the potential to abuse users' vulnerabilities.

For full coverage on the European Parliament's draft report on the addictive design of online services and consumer protection, see our Autumn 2023 Snapshots.

ASA publishes final report on Intermediary and Platform Principles Pilot

The question

How have the main digital platforms responded to the ASA's year long Intermediary and Platform Principles Pilot initiative (the **IPP**)?

The key takeaway

Ten of the largest companies in digital advertising, including Google, Meta and TikTok, were found to support the ASA in its self-regulation of advertising, including by: (1) raising awareness of rules for online advertising; and (2) removing ads that were persistently non-compliant. The pilot has enhanced the existing self-regulatory system for responsible online advertising.

The background

The IPP was devised as a global first to explore transparency and accountability in the UK's online advertising system. It ran for one year from 1 June 2022 to 1 June 2023 and required participating platforms to follow six key Principles:

- to bring the requirement for CAP Code compliance to advertisers' attention
- to ensure policies require ads aimed at a UK audience to comply with the CAP Code
- to assist the ASA in promoting awareness of the ASA system to the public and advertisers
- to make advertisers aware of the tools that support requirements to minimise young people's exposure to ads with age-targeting restrictions
- to act swiftly to remove non-compliant ads where the advertiser fails to act
- to respond in a timely way to reasonable requests for information from the ASA to assist in investigation of suspected breaches of the CAP Code.

At the end of the pilot, all ten participating companies provided comprehensive submissions supported by evidence which allowed the ASA to assess the extent to which they had implemented the Principles.

The development

The independent findings of the report demonstrate that, unequivocally, the participating companies implemented the Principles. In doing so, they raised awareness of advertising rules and took the relevant action where non-compliant ads were identified online. The ASA considers that the IPP has established the ability of the Principles to enhance the existing system of self-regulation whereby relevant companies in the online advertising supply chain support the ASA in securing responsible and safe online advertising.

Why is this important?

Online advertising is recognised as a cornerstone of innovation, customer engagement and competitive prices. Alongside a pro-tech approach to governing digital technologies, the Government is making ongoing considerations as to whether regulators are sufficiently equipped to address harms that can arise from online advertising, particularly high risk areas (eg alcohol and gambling) or illegal online advertising.

A number of digital regulation reforms have been developed as part of the Plan for Digital Regulation, including the Online Safety Act, the Digital Markets, Competition and Consumer Protection Bill, and the Data Protection and Digital Information Bill. Legislative reform has been proposed in the Online Advertising Programme following concerns about the lack of transparency and accountability across key areas of the online advertising supply chain. The Government's July response to the Online Advertising Programme consultation concluded that a tailored and proportionate approach to regulating online advertising, by ensuring regulators have the necessary tools to oversee and ensure compliance, is most appropriate. Particular recognition was paid to the IPP and the substantial work of the ASA.

Whilst the Government's response does not suggest the IPP eradicates the need for further regulation in online advertising, it does highlight the significant positive progress made by the pilot for the advertising industry. It described the results of the pilot as a "helpful step forward" for some of the largest firms to explore how better outcomes can be achieved in online advertising.

Any practical tips?

The report sets out both the good practices observed and identifies areas where the ASA considers there is potential for ongoing consideration which online advertisers should be aware of.

Examples of good practice by online advertisers such as Google, Meta and TikTok include:

- the use of prominent and direct hyperlinks to the CAP Code
- additional methods of raising awareness of the CAP Code and relevant guidance
- the swift removal of all notified non-compliant ads
- the use of CAP Code training for advertisers.

ASA bans misleading Emma Mattress ads on "independent" mattress review website

The question

How did ads for Emma mattresses on a review website fall foul of the CAP Code for being misleading, when the landing page included information about the website being owned by a subsidiary of Emma?

The key takeaway

The owner of Emma Matratzen GmbH t/a Emma Mattress (**Emma**), a bed brand, has been criticised by the ASA for potentially misleading customers with two YouTube advertisements, which appeared to be for an independent mattress review website, when the website was actually owned and operated by a subsidiary of Emma.

The background

Two paid-for ads for a mattress comparison website, top5bestmattresses.co.uk, were shown on YouTube in May 2023. The ads were:

- a video showing a person in a t-shirt with the text "Top 5", who then said: "Today, we'll be testing the UK's most awarded mattress: the Emma original". The person then showed an Emma mattress, explained the positive qualities of the mattress and concluded with saying: "Our verdict: we love Emma and everything about it. Try it and tell us how your first nights were with it. See you in the next review"
- a static image showing a person lying on a mattress highlight the different layers, a mattress with an award ribbon above, and a mattress coming out of a box. Below this image was the text: "Exclusive Deals and Coupon Codes – Spring Sales: Up to 55% ... compare popular beds brands in 2023. Check out exclusive deals and discount codes ... www.top5bestmattress.co.uk/".

Four complaints were made about the two ads, by consumers who understood that www.top5bestmattress.co.uk, was owned by Emma. The complaints challenged whether the ads made clear their commercial intent.

The development

Emma argued that it was evident that www.top5bestmattress.co.uk belonged to a company owned and controlled by a subsidiary of Emma. While acknowledging that the ads themselves lacked any kind of explanatory text, they highlighted that the landing page of www.top5bestmattress.co.uk included information about it being owned by a subsidiary of Emma.

However, the complaints were upheld by the ASA and the ads were held to have breached CAP Code (Edition 12) rules 2.3 (Recognition of marketing materials), and 3.1, 3.3 and 3.9 (Misleading advertising). The ASA considered that both ads would suggest to consumers that www.top5bestmattress.co.uk was an independent mattress review site, which was clearly untrue as it was a subsidiary of Emma. The ASA took into account that there was a disclaimer on the landing page that www.top5bestmattress.co.uk was a subsidiary of Emma, however, they held that this information should have appeared in the ads themselves as this information was material to a consumers' understanding of the ads and the partiality of the comparison website, thus influencing their consumer decision-making. Moreover, the ASA held that both ads implied that independent reviews of different mattresses and mattress brands could be found at top5bestmattress.co.uk when this was not the case. Therefore, they concluded that the ads omitted material information, did not make clear their commercial intent, and were likely to mislead consumers.

Why is this important?

The ruling highlights the importance of advertisers making clear their commercial intent. In this case, the consumer could have been led to believe that they were being advertised an independent mattress review website, when it was essentially, an ad for Emma. The fact that the ads were held to be both unrecognisable as marketing materials for Emma and misleading advertising practices, highlights that the ASA will take complaints regarding ads without clear commercial intent seriously and brands should ensure best efforts to avoid misleading consumers.

Any practical tips?

The key here is transparency. Any company or brand wishing to advertise their products or services must ensure that they do not mislead consumers, that their ads are clearly recognisable as marketing materials for that product or service and that their commercial intent is made clear.

ASA stands against complaints about Dove's body image awareness campaign

The question

How can advertisers approach campaigns on potentially sensitive topics such as the effect of social media on young people's body image?

The key takeaway

The ASA did not uphold complaints about an emotive ad campaign raising awareness of the impact of social media on mental health in young people. Despite the ad's potentially upsetting content, the ASA held that Dove had approached the topic responsibly and had limited the likelihood of young children viewing the ads.

The background

In June and July 2023, Unilever ran a TV and video on-demand advertising campaign in support of their brand, Dove, and their Self-Esteem Project initiative. This initiative was to raise awareness of the impact of social media on a range of mental health conditions, with the ads in question focusing on body image issues.

The long-form ad began with a disclaimer reading "Sensitive Content. The following film features real stories about body appearance that may be upsetting to some viewers". This was followed by home videos of a real person, "Mary", taken during her childhood. The videos showed various scenes of Mary suffering from body image issues caused by social media, leading up to scenes of her in hospital in an Eating Disorder Unit with an IV drip. This was followed by on-screen text stating "The cost of toxic beauty content is greater than we think" and "Mary in recovery from an eating disorder". Finally, a group of young women were shown in recovery from a variety of mental health conditions such as self-harm and depression, with the on-screen text "Social media is harming the mental health of 1 in 2 Kids. Join us to protect their mental health. 2023 Dove Self-Esteem Project Research for Kids Mental Health".

The ads received 136 complaints from the public that the ads were irresponsible and distressing, in particular to those affected by the issues portrayed, and were inappropriate for children to see. Some also challenged whether the ads where appropriate to be shown during the TV program Love Island, which had been specifically targeted.

The development

Unilever's response to the complaints pointed out the background to the ad's creation, which involved consulting a range of relevant experts, charities and focus groups. The content warning was added as a result of that consultation, and Unilever were satisfied that they had approached a difficult subject in a sensitive manner.

The ASA held that a content warning would not necessarily remove the potential for the ads to cause distress. It also found that the content of the ads was emotive and could cause significant emotional impact, both to sufferers of the conditions referenced and to a wider audience. However, it also noted that the ads aimed to raise awareness of the issues and provide support to sufferers. This message was likely to be understood by viewers and the ads were unlikely to encourage copy-cat behaviour. Therefore, the ads were deemed not irresponsible and not likely to cause unjustifiable distress.

Unilever had also taken steps to avoid children seeing the ads, which the ASA felt may have been upsetting to them. It had requested that the long-form ad not be shown before 9pm, and the short form not before 6pm, as well as manually reviewing the surrounding programming to ensure it was appropriate. Clearcast did not apply the timing request strictly, but the ASA was satisfied that Unilever's clear efforts were sufficient.

Finally, the ASA noted that Love Island was broadcast after 9pm and had been chosen by Unilever because the show had been at the centre of relevant cultural debates, meaning the audience was likely to directly understand the themes of the ad. It was not inappropriate to place the ads during Love Island.

Why is this important?

This case is a reminder of just how much care is needed for campaigns dealing with highly sensitive topics. Equally, how a carefully judged campaign aimed at raising awareness of an issue and directing those affected to support can be allowed on air despite being potentially distressing to the audience.

Any practical tips?

Advertisers looking to address sensitive topics should approach them with extreme care and be sure not to seem to encourage unsafe behaviour. The content of the ad itself is critical (content warnings alone may not be enough), as well as paying close attention to when the ads are shown including the surrounding programming. Discussing proposed ads with relevant experts, charities and focus groups to ensure they hit the right balance is also key.

Low to no tolerance: new ASA rules on advertising alcohol alternatives

The question

How is the ASA approaching the regulation of the fast evolving market of alcohol alternative products?

The key takeaway

The ASA has announced specific new rules on the advertising of alcohol alternative products (ie low-and-no-alcohol drinks), which are due to come into force on 14 May 2024. Accompanying the rules is detailed guidance to help advertisers understand where the boundaries are likely to lie in judging whether ads are compliant with the rules. The development was needed due to the expansion in the low-and-no-alcohol alternatives market in recent years, a sector which was not as prevalent when the alcohol rules in the CAP and BCAP rules were first introduced. The new rules include requirements that ads that depict low-or-no alcohol products in a way which have the effect of promoting an alcoholic drink must fully comply with the CAP and BCAP's alcohol rules.

The background

The new rules have been developed in order to keep pace with evolution in the market for low-and-no-alcohol drink alternatives. These are drinks at or under 0.5% ABV (no alcohol) or between 0.5% and 1.2% ABV (low alcohol) and which, unlike traditional soft drinks, are intended specifically to be consumed as alternatives to alcoholic drinks in situations where alcohol might normally be consumed. They can either be standalone beverages or low-or-no-alcohol versions of an alcoholic drink, for example, a non-alcoholic beer.

Ads for alcohol alternatives are frequently similar to those of alcoholic drinks, often depicting or referring to alcoholic drinks. These ads raise concerns about inadvertently encouraging inappropriate consumption of alcohol. Where an ad for an alcohol alternative may have this effect, it now must comply with the advertising rules relating to alcoholic drinks.

The development

Following a public consultation earlier this year, the CAP and BCAP codes are to be updated with changes due to come into force on 14 May 2024. Under these new rules, which are accompanied by guidance, an ad will be subject to the new rules if it is likely to be understood by the audience as being for a product that is an alternative to alcohol.

Circumstances likely to be interpreted as advertising alcohol alternatives include: use of "non-alcoholic" or other statements that indicate ABV at or below 0.5%; references to consuming the drink instead of alcohol; presentation in a style associated with alcohol; shared branding with an existing alcoholic drink, and consumption of the product in a setting where alcohol consumption is prominent. Ads with features which may have the effect of promoting alcoholic drinks or a wider alcohol brand must comply in full with the alcohol advertising rules.

Why is this important?

Businesses which produce low-and-no alcoholic beverages, whether as stand-alone products or as alternatives to alcoholic products within their range, need to pay very close attention to the new rules, which are now almost as strict as those governing the advertising of alcohol itself. The key test is whether an ad is "likely" to be understood by audiences as being specifically for an alternative to alcohol, which is a low bar to meet. Key provisions include:

- if an ad for an alcohol alternative refers to or depicts alcohol, the references or depictions must comply with the rules relating to responsible portrayal of alcohol consumption
- where alcohol alternatives share the same brand as an alcoholic drink, care must be taken not to refer to the brand name without reference to the alcohol alternative
- ads for alcohol alternatives must include a prominent statement of their ABV or non-alcoholic status; and must not be directed to or likely to appeal particularly to people under 18, whilst people shown drinking or playing a significant role in the adverts must not seem to be under 25.

Any practical tips?

Promoters of alcohol alternatives are advised to familiarise themselves fully with the relevant rules and guidance of the CAP and BCAP Codes, which can be found here. They will come into force on 14 May 2024, meaning advertisers currently have a six-month grace period to educate their marketing teams so that they can be fully implemented into their marketing strategies and campaigns in good time.

COMMERCIAL

Exclusion clauses: loss of profits and wasted expenditure

***Pinewood Technologies Asia Pacific Ltd v Pinewood Technologies PLC* [2023] EWHC 2506 (TCC)**

The question

What factors does the court take into account when construing an exclusion clause that covered loss of profits and wasted expenditure, and how does the court approach arguments on whether UCTA applies where the parties are dealing on standard terms of business that have been subject to some negotiation?

The key takeaway

Even where there is an imbalance in the parties' bargaining power, where the language of an exclusion clause is clear and explicitly includes a reference to loss of profits, a court will not strain the language of the clause to hold it ineffective.

The background

Pinewood Technologies PLC (**Pinewood**) is a UK developer and supplier of a management system for motor dealers (the **DMS**). The dispute stemmed from two reseller agreements made between Pinewood and Pinewood Technologies Asia Pacific (**PTAP**), in which Pinewood designated PTAP as its exclusive reseller of the DMS in various territories outside the UK.

PTAP claimed that Pinewood had breached its obligations to develop the DMS for use in the specified territories, seeking damages for loss of profits and wasted expenditure, totalling an estimated US $312.7m. Pinewood denied the alleged breaches of the reseller agreements and PTAP's claims for damages for lost profits and wasted expenditure which it said came under the excluded types of loss in the reseller agreements (clause 16.2):

"… liability for: (1) special, indirect or consequential loss; (2) loss of profit, bargain, use, expectation, anticipated savings, data, production, business, revenue, contract or goodwill; (3) any costs or expenses, liability, commitment, contract or expenditure incurred in reliance on this Agreement or representations made in connection with this Agreement; or (4) losses suffered by third parties or the Reseller's liability to any third party".

Pinewood's position was also that its liability was subject to general liability limits under clause 16.3 of the reseller agreements. It counterclaimed for unpaid invoices due under the reseller agreements. PTAP defended the counterclaim by claiming an equitable right to set off amounts it claimed were owed to it based on its initial claim, arguing that the no set off clause contained in the reseller agreements either didn't apply to equitable set offs or was an unfair term under UCTA 1977 (not meeting the requirement of "reasonableness").

The court was asked by Pinewood to:

- construe the provisions of the exclusion clause to find whether PTAP's claim was excluded by clause 16.2 as a claim for "loss of profit" or alternatively for "any costs or expenses…incurred in reliance on" the reseller agreements
- declare that Pinewood's liability was limited by clause 16.3 of the reseller agreements to £134,528 in respect of the first agreement and to £0 in respect of the second agreement
- enter summary judgment on Pinewood's counterclaim for outstanding sums due under the reseller agreements on the basis of a "no set off" provision in clause 8.10 of the reseller agreements.

The decision

Construing the exclusion clause

The court rejected PTAP's arguments that, as a matter of principle, the exclusion clause could not apply to the non-performance of contractual obligations or to repudiatory breaches of contract, but said that it will be a question of construction in every case whether the exclusion clause covers the breach or, in the case of clause 16.2, the loss in question. Losses pleaded by PTAP which did not fall under the specified losses in clause 16.2 could be caught by clause 16.3. The language of the exclusion clause was held to be "clear and unambiguous" and the intention of the clause was clearly to "exclude the specified heads of loss arising by reason of any liability on the part of Pinewood". It did not serve to remove all of PTAP's substantive rights and remedies because PTAP's claim for incurred costs, while limited by clause 16.3, was not excluded.

The court also rejected PTAP's argument that the exclusion clause was only intended to cover indirect or consequential losses, in line with the second rule of *Hadley v Baxendale*. This was held to be supported neither by the surrounding provisions in the contract or the language of the clause itself.

UCTA

The UCTA arguments centred on whether PTAP was dealing on standard terms of business and, if so, whether the provisions satisfied the "reasonableness" test.

The court held that it was apparent from the evidence that the reseller agreements had been the subject of negotiation, culminating in substantive amendments to the draft (which had started off in a standard form held by Pinewood on its internal system) originally provided by Pinewood. It was also clear that both sides had had access to legal advice. It could not be said that the terms were "effectively untouched" or that none of the changes was material or that the changes left the first reseller agreement unchanged and the fact that there was no negotiation of some of the clauses did not alter the position.

Set off

The court took a cautious approach to its interpretation of the clause restricting set off, again highlighting the importance of the requirement for clear and unambiguous wording, particular in circumstances such as here where the clause was asymmetrical.

Clause 8.10 provides that payment "shall be made in full without withholding deduction or set off, **including** in respect of taxes, charges and other duties" (**emphasis added**). The court agreed with Pinewood that it was clear from the use of the word "including," that "taxes, charges and other duties" are not exhaustive of the items which may not be withheld, deducted or set off against user account fees. It was also well established that "set off" meant both legal and equitable set off.

The court therefore granted reverse summary judgment in favour of Pinewood and summary judgment on their counterclaim.

Why is this important?

It confirms what we have seen with a whole host of judgments this year, the court will approach the exercise of construing an exclusion clause using the ordinary methods of contractual interpretation and on the basis that commercial parties are free to make their own bargains and to allocate risks as they think fit. In commercial contracts negotiated between business-people capable of looking after their own interests and of deciding how risks inherent in various kinds of contract can be economically borne, courts are reluctant to place a strained construction on words in an exclusion clause.

Any practical tips?

When structuring and negotiating an exclusion clause in a contract, consider:

- specifically referring to what kind of loss or expenditure is limited or excluded
- using clear and unambiguous wording
- setting out any exceptions to the exclusion clause to avoid uncertainty
- once negotiations are complete, read the words of the exclusion clause in the context of the whole exclusion clause, the contract as a whole, and the material background and circumstances appliable at the time the agreement was entered into.

Incorrect invoicing: claiming the difference between sums mistakenly invoiced and sums correctly due under agreement terms

Rolls-Royce Holdings Plc v Goodrich Corporation **[2023] EWHC 1637**

The question

When a supplier invoices a lower sum than the figure due under the agreement, can the customer defend a claim in debt based on incorrect invoicing?

The key takeaway

Incorrect invoices rendered may not affect the obligation to pay the higher amount correctly due under the agreement.

The background

Rolls Royce and Goodrich Corporation (**Goodrich**) were involved in a joint venture whereby Goodrich manufactured and sold engine control equipment to Rolls Royce and provided aftermarket services for built plane engines.

Goodrich and Rolls Royce had agreed pricing provisions under the engine repair services agreement (the **Agreement**). Rolls oyce was required to include in its orders the price to be paid by it.

Clause 9.5 of the Agreement provided:

"[Goodrich] shall post invoices to [the RR Entities'] purchase accounts department at the address on the Order on the day on which the Aftermarket Services are despatched or completed. Providing the invoice is accurate, [the RR Entities] shall make payment to [Goodrich] on the fifteenth (15th) day of the second (2nd) month following the month in which the relevant Aftermarket Services are despatched, or completed in accordance with the lead times in the Contract. For the avoidance of doubt, an accurate invoice must include, amongst other things, the Order which relates to the invoice".

Rolls Royce issued orders for parts and incorrectly included in its orders a price lower than was provided for in the Agreement, for certain items. Goodrich did not acknowledge the error and subsequently issued invoices, which replicated the incorrect prices for the goods supplied. Goodrich subsequently claimed the difference between the amounts invoiced and the correct sums due from Rolls Royce as damages for Rolls Royce's breach of contract. Because a claim in damages requires loss to be proved and mitigation of loss, Goodrich also sought to advance a debt claim.

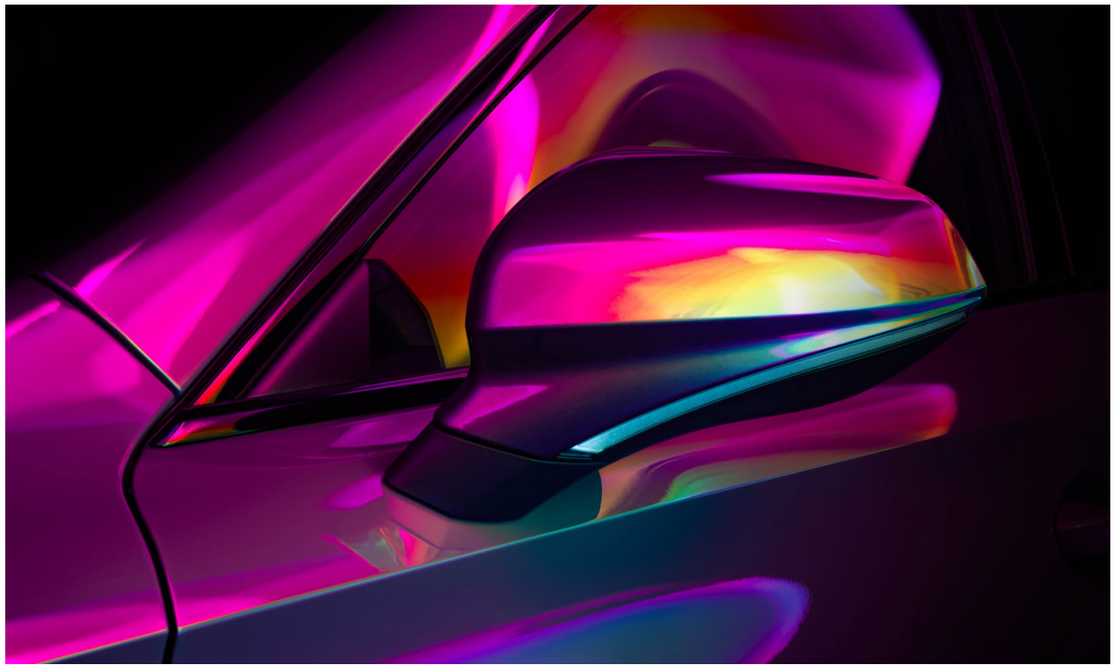
Rolls Royce's position was that the only amount due was that contained in the incorrect invoices which it had paid.

The decision

The court was satisfied that the specifying of the incorrect price by Rolls Royce in the order did not affect the price payable under the Agreement. Further, a debt claim did accrue despite the fact that Goodrich had not submitted invoices at the correct price. Clause 9.5 did not affect the point in time at which the debt arose because the clause linked the payment obligation not to the provision of the invoice as such, but to the time when the goods were despatched or the services completed. Goodrich was therefore entitled to bring an action for the price of the goods under s 49(1) of the Sale of Goods Act 1979 because the goods had passed to Rolls Royce.

Goodrich providing incorrect invoices was held to be no defence, enabling Rolls Royce to avoid paying the amount owed to Goodrich. Clause 9.5 did not expressly link the payment obligation to the rendering of an accurate invoice, but to delivery or completion of the services, and the words "provided the invoice is accurate" were intended to do no more than make it clear that an inaccurate invoice did not itself create a payment obligation which did not otherwise exist. The court considered that the parties could not have intended that the amount due for the supply of the spare parts would not become payable unless invoiced in full if the reason for the inaccurate invoice was Rolls Royce's own breach of contract in specifying the wrong price in the order. This would permit Rolls Royce to take advantage of its own wrong.

Under a separate clause, the court found that Rolls Royce was expressly obliged under the Agreement to specify the correct price in its orders. The price specified by Rolls Royce in its order for spare parts was highly likely to be the price invoiced by Goodrich, and assuming that specification of the correct price in the invoice was necessary for that price to be recoverable as a debt, the argument for interpreting the clause as imposing an obligation to specify the correct price was found to be particularly strong. As between Rolls Royce and Goodrich, Rolls Royce was far better placed to determine what the spare parts were being ordered for and therefore what price applied. Rolls Royce was therefore in breach of contract for specifying incorrect amounts on its invoices.



Why is this important?

While it's important to invoice the correct amount in accordance with the contract, this case highlights that invoicing (andbeing paid) an incorrect amount may not prevent suppliers from recovering the correct, higher contractual price for the items and services delivered.

Any practical tips?

If it is the intention of the parties that the passing of property or delivery of goods/ services do not provide the basis for price to become due, a clear provision to that effect should be included in the contract.

When using words such as "provided the invoice is accurate", bear in mind that the court found these words did no more than make it clear that an inaccurate invoice does not itself create a payment obligation which does not otherwise exist.

Consider whether the contract should include a mechanism for reconciling amounts payable, invoices and payments, whether there are any time limits after which amounts are deemed confirmed, and the consequences of any discrepancies.

"A party who fails to plead its entitlement to contractual interest in proceedings is not entitled to statutory interest."

Interest clauses: displacing the courts' wide discretionary powers to award interest on debt or damages

Rolls-Royce Holdings plc v Goodrich Corporation **[2023] EWHC 2002 (Comm)**

The question

What is the courts' approach to awarding statutory interest when a contract provides for contractual interest.

The key takeaway

A party who fails to plead its entitlement to contractual interest in proceedings is not entitled to statutory interest.

The background

Following the conclusion of *Rolls-Royce Holdings plc v Goodrich Corporation* [2023] EWHC 1637 (the **Judgment**), an issue arose between the parties as to whether, and if so for what period, Goodrich was entitled to pre-judgment interest on the sum of $112,285,440 awarded to it by the Judgment.

The agreement the subject of the original dispute (the **Agreement**) contained a contractual entitlement to claim interest, in clause 44:

"Interest on Late Payment

If R-R does not make payment in accordance with this Agreement, GR shall be entitled to recover (in addition to the principal sum owed) a sum from R-R equal to the interest which it pays or loses as the case may be in consequence of such late payment upon provision of evidence of such payment/loss. The amount recoverable for the first three months following such late payment shall not in any event exceed a sum equivalent to interest at 2.0% above the Bank of England's Base Rate on the overdue payment for the period between the dates on which such payment was due and not made. For these purposes, the Bank of England's Base Rate shall be that applicable at the date the overdue payment was due. The Parties acknowledge and agree that such payments are sufficient to compensate GR for any such late payment".

In the original proceedings for which the Judgment was given, no claim for contractual interest was pleaded. After the Judgment was handed down, Goodrich wrote to the Rolls Royce entities setting out the amount which they contended they were entitled to by way of statutory interest. Rolls Royce's response was to point to clause 44 (the first time the clause was raised in the entire litigation) which it claimed precluded a claim for statutory interest.

The decision

Section 35A of the Senior Courts Act 1981 gives the court the power to award interest on debts and damages. Section 35A(4) states that interest in respect of a debt shall not be awarded by the court for a period during which, for whatever reason, interest on the debt already runs.

Acknowledging that there had been no attempt to assert or prove any interest claim permitted by clause 44, the court held that no award of interest should be made under s 35A:

The effect of s.35A(4) is to prevent interest being awarded under s.35A when it is already "running" for some other reason on the debt. That could be because a contractual rate of interest is running or because it is a statutory debt on which interest runs. Section 35A(4) avoids interest being recovered twice on the same debt.

The court's reasoning was that the parties had by clause 44 reached an agreement as to when and in what amount interest should be paid, and it would be inappropriate to award statutory interest where the contractual conditions for the payment of interest have not been shown to be satisfied.

Why is this important?

It confirms the limits of the court's discretionary powers concerning statutory interest when a contract already contains provisions for interest. It reflects the principle that that if the parties have mutually agreed the terms of interest payment in a contract, the court will refrain from granting interest on an alternative basis. This extends to where the contract provides for interest to be payable in particular circumstances only or fixes the interest rate at a specific rate. In these cases, the court can only enforce that provision and its statutory power does not allow it to fix a different interest rate.

Any practical tips?

A contract will typically provide for contractual interest and the applicable rate. Consider whether there are any circumstances in which interest does not accrue/ is not payable. If the parties decide not to include an entitlement to interest, consider providing for this expressly.

If a monetary claim is pursued, ensure that it includes a claim for any available contractual interest.

SPA breach of warranty claim: interpreting a no material adverse change warranty

***Decision Inc Holdings Proprietary Ltd & Anor v Garbett & Anor* [2023] EWCA Civ 1284**

The question

How will the courts assess an alleged breach of a warranty that there had been no material adverse change in the financial prospects of a company?

The key takeaway

In assessing whether there had been a change in the company's prospects, it was necessary to evaluate the company's "prospects" using the two relevant dates (the Accounts Date and completion) as provided for in the SPA, and not focus on other dates not stated in the warranty, on historical information or on comparing different things (eg "the expectation that a reasonable buyer would have had" and the "actual" position) as at the same date.

The background

In October 2018, Decision Holdings entered into a share purchase agreement (**SPA**) with Mr Garbett and Mr El-Mariesh (the **Sellers**), pursuant to which Decision Holdings agreed to acquire all the shares in a company specialising in the design of enterprise performance management software (the **Company**) from the Sellers.

The SPA contained various warranties, including in clause 10.2, where the Sellers warranted that, "except as Disclosed", each of the warranties set out in schedule 4 to the SPA was true on the date of the agreement and the completion date. Schedule 4 provided:

"19 CHANGES SINCE THE ACCOUNTS DATE

Since the Accounts Date:

...

19.1.2 there has been no material adverse change in the turnover, financial position or prospects of the Company

....

20 FINANCIAL AND OTHER RECORDS

20.1 All financial and other records of the Company ('Records'):

20.1.1 have been properly prepared and maintained;

20.1.2 constitute an accurate record of all matters required by law to appear in them, and in the case of the accounting records, comply with the requirements of section 386 and section 388 of the CA 2006;

20.1.3 do not contain any material inaccuracies or discrepancies; and

20.1.4 are in the possession of the Company".

Clause 11 of the SPA imposed limitations on claims for breach of warranty, including an exclusion of the Sellers' liability for any breach of warranty claims not notified "in writing summarising the nature of the claim (in so far as it is known to the buyer) and, as far as is reasonably practicable, the amount claimed" by the buyer within 24 months of completion.

Prior to concluding the SPA, the Sellers supplied Decision Holdings with numerous positive pipeline documents (showing new and potential work) and a detailed profit forecast. Soon after the SPA was signed, Decision Holdings was sent the monthly accounts for the Company showing net losses after tax and overall poorer prospects. Revenues continued to be low with the company starting to make losses. Decision Holdings sent a formal notice alleging breach of warranties which the Sellers had given in the SPA. They later commenced breach of warranty proceedings alleging breach of warranties 19 and 20 on the basis that the Company's records were defective, and that there had been a material adverse change in the turnover and in the prospects of the Company.

The High Court found that the Sellers were liable to pay £1.31m in damages for breach of the no material adverse change warranty. The Sellers appealed.

The main issues for the Court of Appeal (**CA**) were narrowed down to whether the High Court's interpretation of, and approach to, the "prospects" limb of warranty 19 (the **Prospects Warranty**) was wrong and whether the formal notice given was adequate to notify the claim for the breach of the Prospects Warranty.

The decision

The CA overturned the decision of the court of first instance finding that its interpretation of, and approach to, the Prospects Warranty was wrong.

Under the warranty the Sellers had warranted that there had been no material adverse change in the prospects of the Company from the date of the last accounts (31 December 2017). For the warranty to have been breached, therefore, the Company's "prospects" must have worsened since 31 December 2017. It was necessary to evaluate the "prospects" at 31 December 2017 and those in October 2018, when the SPA was signed and completion occurred. Instead, the court had contrasted the actual position in October 2018 (not with that on 31 December 2017) but with the "expectation which a reasonable buyer would have had" derived from the agreed pricing structure for the transaction found in the SPA, which dated from October 2018, and so could not establish the Company's prospects as at 31 December 2017.

The court's approach was also wrong because the Prospects Warranty was concerned with what the Company's "prospects" in fact were on different dates (at 31 December 2017 and October 2018), not a comparison between different things ("the expectation that a reasonable buyer would have had" and the "actual" position) on the same date. It had also wrongly concluded that the Prospects Warranty had been breached by reference to what had already happened, not how the Company might fare in the coming period (ie the word "prospects" looks to the future).

The High Court had equated "prospects" with expected levels of Earnings Before Interest, Tax, Depreciation and Amortisation (**EBITDA**). The CA acknowledged that the meaning to be attributed to "prospects" may be affected by the context in which the word is used and, where used contractually, could potentially vary from one contract to another. In the context of the SPA, "prospects" was not easy to construe but the CA was not persuaded that it simply referred to EBITDA because had the parties had EBITDA in mind, they could have specifically used that term. Also, EBITDA featured elsewhere in the SPA in a number of places and the word "prospects", read naturally, meant "chances or opportunities for success" in a more general way.

The CA also overturned the High Court's ruling regarding the validity of Decision Holdings' notice of claim. According to the SPA, the notice was required to specify the claimed amount for each breach of warranty, not just a combined figure, as provided by Decision Holdings. The failure to adhere to this requirement rendered the notice defective, and consequently, the Sellers could not be held responsible for the alleged breach.

Why is this important?

Although the CA's finding was heavily influenced by the circumstances of the case and the specific SPA warranties, it offers a working example of how the courts are likely to interpret a material adverse change clause. It also serves as a further warning as to the need to serve notices that meet the contractual requirements.

Any practical tips?

To provide greater certainty, consider defining what is meant by material adverse change in an SPA making it clear which dates or events apply to measuring whether a change has occurred. If financial metrics are the intended measure (eg because that is consistent with how the company/business has been valued), specify those that will apply.

As material adverse change clauses can be somewhat uncertain, consider including targeted warranties in the SPA to deal with undisclosed loss or liability, changes to forecasts, future work pipelines, etc.

Ensure that where a clause specifies that notice of a claim must include required information (here the notice had to include, as far as reasonably practicable, the "amount claimed" in respect of each breach of warranty claimed, not just a total figure), it is workable in practice, and that any notice is drafted strictly in accordance with its terms. Ideally, do not leave the notice until the very end of the contractual limitation period – which invites risk as to the content and valid service of the notice.

COMMERCIAL

Excluding statutory implied terms: inequality of bargaining power considerations

***Last Bus Ltd v Dawsongroup Bus and Coach Ltd* [2023] EWCA Civ 1297**

The question

In what circumstances is it reasonable to exclude the statutory implied term as to quality?

The key takeaway

Whether the parties are deemed to be of equal bargaining power requires consideration of factors wider than the parties' size, long standing commercial relationship and the availability of alternatives to contract with. Inequality in bargaining power may be found where a party is trading on the counterparty's standard terms and no substantially different terms are available within the market, or where the effect of the term is that the party is left without a remedy.

The background

Last Bus brought a claim against Dawsongroup Bus and Coach Ltd (**Dawson**) for breach of various hire purchase agreements (the **Agreements**) relating to coaches which it claimed were defective. Last Bus's claim was that some of the coaches acquired under the Agreements were not of satisfactory quality because they were liable to catch fire, requiring Last Bus to implement a far more onerous and expensive maintenance regime than was originally anticipated. Last Bus claimed damages exceeding €10m.

The Agreements, which were on Dawson's standard terms, contained a clause 5(b), which purported to exclude the term as to satisfactory quality that would otherwise be implied by section 10(2) of the Supply of Goods (Implied Terms) Act 1973:

"The Customer agrees and acknowledges that it hires the Vehicle for use in its business and that no condition, warranty or representation of any kind is or has been given by or on behalf of the Company in respect of the Vehicle. The Company shall have no liability for selection, inspection or any warranty about the quality, fitness, specifications or description of the Vehicle and the Customer agrees that all such representations, conditions and warranties whether express or implied by law are excluded. Notwithstanding the foregoing provisions of this clause, nothing herein shall afford the Company a wider exclusion of liability for death or personal injury than the Company may effectively exclude having regard to the provisions of the Unfair Contract Terms Act 1977. The Customer acknowledges that the manufacturer of the Vehicle is not the agent of the Company and the Company shall not be bound by any representation or warranty made by or on behalf of the Vehicle manufacturer".

Dawson successfully obtained summary judgment of the claim against it – in its assessment, the High Court found that the parties were of equal bargaining power and that the term that was part of Dawson's standard terms of business was reasonable under UCTA 1977. Last Bus appealed.

The decision

The Court of Appeal (**CA**) allowed Last Bus's appeal finding that the High Court had taken the wrong approach in assessing reasonableness. Specifically, it was wrong to have approached the question of reasonableness on the basis that the parties were of equal bargaining power.

"Even where the parties are large commercial concerns and of equal bargaining strength as regards the price to be paid under the contract, that does not mean that they are of equal bargaining strength in respect of the terms. A supplier may be willing to negotiate the unit price, but will only supply on its standard terms, a position taken by all other suppliers in the market. That crucial distinction must, in my judgment, be borne in mind ...".

The CA found it was obvious that Dawson would not have contracted without the exclusion clause and the fact that there were no materially different terms available in the market should have contributed to the conclusion (at least arguably) that the parties were not of equal bargaining strength as regards clause 5(b).

The starting point for the court of first instance should have been that clause 5(b), contained in standard terms of business, purported to exclude any and all liability for the quality of the coaches supplied to Last Bus, leaving Last Bus without a remedy even if it received no value at all while having to pay for the hire. Prevailing caselaw made it clear that such clauses are prima facie unreasonable under UCTA 1977.

Why is this important?

It highlights a more nuanced approach to assessing UCTA 1977 reasonableness and whether parties are of equal bargaining power.

Any practical tips?

When contracting on standard terms, consider whether the parties on an equal footing as regards those terms and are other terms available in the market. Also consider whether there is any other remedy available, eg an alternative (limited) warranty in substitution for any excluded implied warranties or conditions.

Consider whether insurance is available/ should be obtained by the customer against the excluded risk (and if the contract should contain an appropriate recital/ acknowledgement to that effect). That may also be relevant to an effective allocation of risk and support arguments that the parties are of equal bargaining strength.

COMMERCIAL

Express and implied good faith obligations and relational contracts

***Phones 4U Limited (In Administration) v EE Limited and Ors* [2023] EWHC 2826 (Ch)**

The question

Did an express or implied general duty of good faith arise under a relational contract between parties who were also competitors?

The key takeaway

Where parties are not exclusive, but are in fact direct competitors, they are less likely to be considered to be in a relational contract. If an agreement expressly specifies a requirement to act in good faith in relation to a specific activity or on one party only, then a general duty of good faith is less likely to be implied.

The background

In September 2014 Phones 4U Ltd (**P4U**), suppliers of consumer connections to mobile networks in the UK, went into administration. The administrators of P4u brought proceedings against mobile network operators EE, Vodafone UK and O2 (the **MNOs**) and their parent companies. P4u claimed that the defendants engaged in anti-competitive collusion which caused it to enter into administration and also that its collapse was caused by a breach of contract on the part of EE (only the breach of contract claim is covered in this analysis).

The alleged collusion stemmed from suspicions that the operators did not renew their individual agreements with P4U following discussions with each other in order to strategically advance their own commercial aspirations and boost profits, and in breach of competition law. The administrators also claimed EE was in breach of an express and an implied obligation of good faith after EE announced to P4U in September 2014 that it would not be renewing its agreement after its expiry in September 2015.

The clause relied on stated:

"13.2 EE hereby undertakes and agrees that it will in good faith observe and perform the terms and conditions of this Agreement and in particular EE shall, and shall procure that its employees, agents and subcontractors will…

13.11 EE hereby undertakes and agrees with P4U that it will act in good faith and not carry out any activity designed to reduce or avoid the making of any Revenue Share Payment(s) to P4U as contemplated by this Agreement".

Relying on the case of *Yam Seng Pte Ltd v International Trade Corp Ltd* where the one year commercial distribution agreement in question was deemed to be a "relational contract", P4U contended that the clause 13 provisions should be construed in the light of the nature of the EE Agreement as a "relational contract", and therefore giving rise to a general duty of good faith.

The telecom companies denied the allegations claiming that the decisions were made independently and based on thorough commercial analysis.

The decision

The High Court dismissed the breach of contract claim against EE holding that the agreement between P4U and EE did not entail a general duty of good faith.

The court found that this was a professionally drafted and very full contract between sophisticated parties and that had the parties intended to impose a general obligation of good faith, they would have expressly done so. The court also found that if there was to be such an express, general good faith obligation on EE, the contract would also have imposed the same obligation on P4U. But while there was a corresponding obligation to clause 13.2 on P4U in clause 13.1, there was no equivalent to clause 13.11. Further, clause 13.11 followed clauses 13.8 to 13.10 which all related to matters affecting the occasioning of Revenue Share Payments. Accordingly, clause 13.11 was to be interpreted as applying the requirement of good faith to "activity designed to reduce or avoid" the liability under the agreement to make Revenue Share Payments, and not more generally.

On the question of whether the EE agreement was a relational contract and whether, if so, that impacted the construction of either of the clause 13 provisions, the court reasoned that the nature of the parties' relationship in the case relied on by P4U – Yam Seng (which involved an exclusive distribution agreement) was significantly different to the relationship between P4U and EE. Relational contracts required "a high degree of communication, cooperation and predictable performance based on mutual trust and confidence and involve expectations of loyalty which are not legislated for in the express terms of the contract but are implicit in the parties' understanding and necessary to give business efficacy to the arrangements". Examples included joint venture agreements, franchise agreements and long term distributorship agreements.

While the EE agreement had some features of a relational contract in that it was moderately long term and involved collaboration, it also had some major differences. EE was not only enabling P4U to supply connections to its network but was also in competition with the retailer to supply the connections to customers directly. This meant that it was only natural for EE to seek to reduce its reliance on indirect retailers and instead expand its direct retailing business. In Yam Seng, exclusivity was "a supporting indication, not a necessary condition, for a relational contract" but here the fact that the parties were in direct competition pointed away from the existence of a relational contract. The court found that this was not a relational contract but that even if it was, no duty of good faith would be implied. If the court was wrong on that then it considered that there was no duty of good faith by EE on the facts.

Why is this important?

The case shows the courts' reluctance to imply a general duty of good faith in commercial transactions between sophisticated parties, where the agreement has been professionally drafted and where the general duty is not reciprocated between the parties.

Any practical tips?

While courts may in some circumstances imply a general obligation to act in good faith, if that is what the parties intend, an express clause to act in good faith should be included in the contract.

A good faith clause should be drafted with the context of the agreement in mind and scoped accordingly (all of the agreement or only certain aspects?), for example to promote cooperation or prevent a party from acting in a way that is detrimental to the other. The parties may also consider including a (non-exclusive) list of examples of good faith behaviour.

If there are particular actions that are intended to be covered, it is preferable to have specific obligations dealing with them – although bear in mind that a general good faith obligation will not usually override these specific provisions.

COMMERCIAL

rpc.co.uk