EVERSHEDS SUTHERLAND

Commercially connected: November 2019

Welcome to the Eversheds Sutherland monthly commercial law update, covering both case law and regulatory development as well as progress on Brexit. *This report is intended to give you a general overview of legal developments in certain areas. It is provided for information purposes only and is not intended to be comprehensive or to constitute advice on which you may reply.*

Topics covered

Click on your topic of interest below:

- Brexit
- Commercial – general
- Consumer law
- Cyber security
- Data protection and privacy law
- IP
- IT
- Public sector
- Focus on disruptive tech

Brexit

Development	Summary	Links
UK failure to nominate a candidate for the European Commission	The European Commission has issued a letter of formal notice to the UK for breaching its EU Treaty obligations by failing to put forward a candidate for the European Commission. This letter is the first step in the Commission's infringement procedure.	Press release European Commission infringement procedure
EU Regulations for a no deal Brexit	The following Regulations have been published in the OJEU and will apply on a no deal Brexit: • Regulation (EU) 2019/1795 which extends Regulation (EU) 2019/501 on ensuring basic road freight and road passenger connectivity until 31 July 2020 and Regulation (EU) 2019/502 on basic air connectivity until 24 October 2020 • Regulation (EU) 2019/1796 which allows the European Globalisation Adjustment Fund to be used to support workers and self-employed persons who are made redundant as a result of a no-deal Brexit • Regulation (EU) 2019/1797 which extends Regulation (EU) 2019/498 on fishing authorisations to enable EU and UK fishermen to keep accessing each other's waters during 2020.	Regulation 2019/1795 Regulation 2019/1796 Regulation 2019/1797
Brexit SIs issued in November 2019	Brexit SIs issued this month that are likely to be of interest to commercial practitioners include: The European Union (Withdrawal) Act 2018 (Exit Day) (Amendment) (No. 3) Regulations 2019 (2019 No. 1423) which amend the definition of exit day in the European Union (Withdrawal) Act 2018 to 31 January 2020 in order to reflect the current extension to the Article 50 period. The Freedom of Establishment and Free Movement of Services (EU Exit) Regulations 2019 (2019 No. 1401) which dis-apply provisions on freedom of establishment and free movement of services which would otherwise continue as directly effective rights in domestic law under the European Union (Withdrawal) Act 2018. This will ensure that post Brexit EU nationals will be unable to rely on these rights to challenge any UK law or policy which places restrictions on their access to the UK internal market.	
Guidance on tariff quota claims under transitional simplified procedures	The government has issued guidance on making tariff quota claims under transitional simplified procedures.	Guidance

Brexit

Development	Summary	Links
International agreements on a no deal Brexit	Click on the links to see the government's latest status updates on international agreements and UK trade agreements with non-EU countries on a no deal Brexit.	Guidance on international agreements; Guidance on UK trade agreements

Commercial – general

Development	Summary	Links
Claims for breach of collateral warranty	**New York Laser Clinic Ltd v Naturastudios Ltd** provides a helpful statement of the law on tripartite collateral warranties. The defendant was the UK distributor of laser hair removal devices. It made statements to the claimant, who owned laser hair removal clinics, about the qualities and performance characteristics of the devices. In reliance on those representations the claimant decided to buy six devices. It bought them via a hire purchase company and so the sale contracts were between the defendant and the third party hire purchase company and not between the claimant and defendant. The statements turned out to be false and the claimant brought successful claims against the defendant for negligent misstatement and breach of collateral warranty. A collateral warranty is a promise with contractual force which leads to a contract being entered into. The judgment clarified that where a collateral warranty is given to a third party rather than to a contracting party, the requirements for a claim for breach of that collateral warranty are as follows: • A warranty is given to a third party ("TP") by a contracting party ("CP1"). • The warranty is intended to have contractual force. • TP provides consideration to CP1. • In reliance upon the warranty TP causes another person ("CP2") to enter into a contract with CP1. • The warranty was inaccurate; there is no need for the warranty to have been made fraudulently or negligently or even for CP1 to know that it is false. • TP suffers financial loss as a result. • There are no relevant exclusion clauses. In determining this case the court also concluded that where there is a breach of a collateral warranty about the quality or anticipated performance of the thing to be supplied, the claimant can recover either: (i) the loss caused by the breach (to be put back into the position it would have been in if the contract had never been made); or (ii) loss of the profits that it would have earned if the warranty had been true. However, if the warranty was only to the effect that reasonable care was taken in relation to an estimate given, then only the losses in category (i) can be recovered.	Judgment
No set off clause does not preclude defence by way of the prevention principle	In dismissing an application for summary judgment in **TMF Trustee Ltd v Fire Navigation Inc**, the High Court considered the interplay between the prevention principle and a no set-off clause.	Judgment

Development	Summary	Links
	The prevention principle is, broadly, that a party is excused from its breach of contract where its performance is prevented by the other party. In this case the claimant argued that the defendant was not entitled to rely on the prevention principle to avoid making contract payments to the claimant because the contract contained a no set-off clause. The court disagreed and found that the defendant had an arguable defence to the claim. This was on the basis that earlier case law makes it clear that the prevention principle gives rise to a defence to liability for the breach itself, not merely a defence by way of set-off to an obligation to pay monies due.	
Legal statement on cryptoassets and smart contracts	Following a consultation launched in May 2019, the UK Jurisdiction Taskforce has published a (non legally binding) legal statement on cryptoassets and smart contracts, concluding that: • cryptoassets are to be treated in principle as property; • a smart contract may satisfy the basic requirements of a legal contract under English law and so it is capable of having contractual force; and • a private key which is intended to authenticate a document can in principle meet a statutory requirement for signature. For more information click on the link to an Eversheds Sutherland briefing by James Burnie.	Legal statement Eversheds Sutherland briefing
2019 bribery risk matrix	TRACE, the world's leading anti-bribery standard setting organisation, has released the 2019 TRACE bribery risk matrix which measures business bribery risk across 200 jurisdictions, as well as a bribery risk typology and interactive map.	TRACE press release
The Cross-border Parcel Delivery Services (EU Information Requirements) Regulations 2019	The Cross-border Parcel Delivery Services (EU Information Requirements) Regulations 2019 came into force on 23 November 2019. These Regulations ensure that the UK complies with Article 8 of the Cross-border Parcel Delivery Services Regulation (EU) 2018/644 which requires member states to take all measures necessary to ensure that the Regulation is implemented and to lay down rules for infringement that are effective, proportionate and dissuasive. The purpose of the EU Regulation is to improve cross-border parcel delivery services by improving transparency and regulatory oversight of the sector. After Brexit this EU Regulation will be revoked in the UK.	Regulations

Development	Summary	Links
EU Enforcement and Modernisation Directive	As part of the EU's "New Deal for Consumers", the European Economic and Financial Affairs Council has adopted a directive that is intended to modernise consumer protection law and update it for the digital age. The Directive is colloquially known as the Enforcement and Modernisation Directive but its full title is "Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules". It amends the current Unfair Commercial Practices Directive, Consumer Rights Directive, Unfair Contract Terms Directive and Price Indications Directive. The Directive will come into force 20 days after it is published in the OJEU. Member states will have to adopt and publish compliance measures 24 months after it comes into effect and those measures will start to apply six months later. The Directive includes provisions on the following: • member states are required to impose penalties for breach of national consumer protection law of up to 4% of the trader's annual turnover in the relevant member states; • a right for consumers to seek redress directly from traders; • new information obligations for online traders, in particular regarding the criteria used to rank search results, the verification of online reviews, the status of the seller and personalised pricing based on automated decision making; • the Consumer Rights Directive is amended to apply to both digital content and digital services provided in exchange for personal information; • an obligation on online marketplaces to inform consumers of whether the responsible trader in a transaction is the seller and/or the online marketplace itself; • clear information provision obligations in respect of price reductions; and • an obligation on the Commission to ensure that consumers can use the single digital gateway to access up to date information about EU consumer rights and to submit a complaint through the Commission's Online Dispute Resolution platform.	Directive

Development	Summary	Links
Council of European Energy Regulators' guide on bundled products	The Council of European Energy Regulators has published a guide on bundled products. The Guide is intended to be used by companies who offer bundled products and their regulators, regardless of what sector they are in, in order to promote a consistent approach and to better protect consumers. Bundled products are packages of combined goods and/or services whether within one sector or across multiple sectors (eg internet + fixed telephone + TV + mobile telephony services; banking + travel insurance). Key principles for companies offering bundled products include transparency, keeping it simple, communication of clear and understandable contract terms and conditions and allowing the customer the possibility of switching out of a bundle. The three principles for regulators overseeing and regulating sectors with bundled products are to educate companies on the applicable rules and obligations, to monitor bundled products and to cooperate across sectors with relevant authorities.	Guide
BEIS report on safety of electrical goods in the UK	The Business, Energy and Industrial Strategy Committee has published a report on the safety of electrical goods in the UK, a follow-up to its January 2018 report. The report is a damning indictment of Whirlpool's approach to its defective tumble driers. It also heavily criticises the Office for Product Safety and Standards ("OPSS") which, the report says, did not deliver in dealing with the Whirlpool issue; has not yet delivered a fully operational and credible hub for consumers to register their electrical goods and access information on recalls, a comprehensive injury database or indelible marking for electrical goods; and has not made sufficient progress on the sale of recalled second-hand electrical goods or those that do not meet safety standards. The report also states that in order for the OPSS to fulfil its remit effectively it needs to be armed with a full array of powers including powers to impose civil sanctions. The recommendations set out in the report include the following: • The government should review the funding of Local Trading Standards and their current ability to carry out surveillance and enforcement activities at a local level and contribute to data sharing at a national level; • The OPSS should work with online market place platforms to produce a more proactive approach to ensure that electrical goods are not sold online until their safety has been established; • The OPSS must deliver the changes to the product safety system already identified; and • The government should seriously consider making the OPSS an independent and fully transparent body.	Report

Consumer law

Development	Summary	Links
Ofcom paper on regulation of online services	Ofcom has published a paper entitled "an economic perspective on the challenges and opportunities in regulating online services". The findings set out in the paper include the following: • the characteristics of some online services can generate market failure which harms consumers and society in several ways, eg online services can be concentrated with a few big players thereby limiting competition; and some online services are incentivised to maximise the capture of data and attention which can lead to the promotion of addictive behaviour or the spread of harmful content which, in turn, may limit users' exposure to a variety of views; • online services pose particular challenges for regulators due to their global nature, fast pace of change, complexity of online business models, scale of online content and variety of services available online; and • interventions to address harms should be carefully designed to overcome these challenges and avoid undesirable unintended consequences.	Ofcom paper on online market failures and harms
CJEU decision on extent of courts' obligation to examine fairness of contract terms	The CJEU has held that a national court's obligation to examine the fairness of terms in consumer contracts, even where unfairness has not been pleaded, extends to requiring a trader to produce a copy of relevant documentation.	Judgment
Which? agenda for the next UK government	Consumer group Which? has published its "agenda" for the next UK government, setting out what it wants that government to deliver for consumers. At a headline level this includes: • **Better connectivity** – a strategy to deliver an improved digital infrastructure; • **An enforcement system fit for purpose** – a stronger Consumer and Competition Authority to proactively lead on the enforcement of consumer rights and fair trading law; the Office for Product Safety and Standards to be an independent arms' length product safety regulator and reform of the alternative dispute resolution (ADR) system to make it more robust; • **Greater protection from online harms and insecure products** – place more responsibility on online platforms and marketplaces to prevent scams, fake reviews and the sale of unsafe products, and ensure that security is built into the design of connected devices; • **Banking services that work for everyone** – ensure continued access to cash and ensure everyone is protected from Authorised Push Payment fraud (where people are tricked into sending money to a fraudster);	Which? agenda

Development	Summary	Links
	• **Fair and transparent pensions** – enable everyone to understand their pensions savings, address the pensions gender gap and ensure that all retirement income products are value for money; and • **A future trade policy and food strategy that delivers for consumers** – pursue a trade policy underpinned by world-leading consumer standards, consumer rights and enhanced choice and deliver a national food strategy that maintains the UK's high food standards.	

Cyber security

Development	Summary	Links
DCMS call for evidence	The Department for Digital, Culture, Media and Sport has issued a call for evidence as part of its Cyber Security Incentives and Regulation Review 2020. The purpose of the Review is to assess where existing incentives and support have delivered the greatest improvements and where there are observable impacts of the existing regulatory framework (including GDPR and the NIS Regulations) and, looking forward, to consider which additional incentives and regulation would most effectively support the economy to overcome cyber security risks and help to integrate cyber security within operational risk management. The call for evidence focuses on four issues: barriers to effective cyber risk management; commercial barriers and incentives for investing in cyber security; access to the right information for effective cyber risk management and areas of focus for future policy and regulatory intervention. The call for evidence closes on 20 December 2019.	Call for evidence
NCSC CyBOK	The NCSC has issued CyBOK Version 1.0, a freely available cyber security body of knowledge which aims to codify that knowledge. It comprises 19 knowledge areas grouped into the five broad categories of systems security; infrastructure security; software and platform security; human, organisational and regulatory aspects; and attacks and defences.	Cyber Security Body of Knowledge
Government guidance on non-UK digital service providers and the NIS Regulations post Brexit	The government has issued guidance on what non-UK digital service providers operating in the UK will need to do post Brexit in order to remain compliant with UK law, namely: • appoint a UK representative and confirm this in writing following the ICO registration process; and • comply with the UK Network and Information Systems Regulations 2018 (as amended) even if already complying with the domestic law transposed from the NIS Directive in an EU member state.	Government guidance
European Commission report on identification of operators of essential services under the NIS Directive	The European Commission has published a report assessing how EU member states have identified operators of essential services that have to put cybersecurity measures in place and report cyber incidents under the NIS Directive, focusing on the extent to which methodologies are consistent across member states.	Press release

Cyber security

Development	Summary	Links
ENISA report on good practice for security of IoT	ENISA, the European Union Agency for Cybersecurity, has released a report entitled "Good Practices for Security of IoT" which is intended to promote security by design for Internet of Things ("IoT") devices and their ecosystems. The report focuses in particular on software development guidelines for the full life cycle of a device including: • analysis of security concerns in all phases of the software development life cycle; • detailed asset and threat taxonomies; • concrete and actionable good practices to enhance cybersecurity; and • mapping of ENISA good practices to related existing standards, guidelines and schemes. The target audience for the report is IoT software developers; IoT platform, software development kit and application programming interface developers and consumers; and IoT integrators.	ENISA good practice for security of IoT
Updated FCA guidance on cyber resilience	The FCA has updated its cyber resilience guidance to include a link to a new self-assessment questionnaire (CQUEST) created jointly by the FCA and the PRA. CQUEST is intended to help firms and regulators understand the firms' cyber resilience capability at a high level and it is made up of multiple-choice questions such as: • does the firm have a board-approved cyber security strategy? • how does it identify and protect its critical assets? • how does it detect and respond to an incident, recover the business and learn from the experience? The answers are intended to provide a snapshot of a firm's cyber resilience capability and to highlight areas for further development.	FCA cyber resilience guidance
DHSC issues third progress update on actions taken to boost cyber resilience in the health and care industry	The Department of Health and Social Care ("**DHSC**") has issued a progress report on its ongoing work to enhance cyber resilience across health and care. The report explains that DHSC's main priorities over the past 12 months have been strengthening national leadership for cyber security, supporting local organisations to address cyber security threats and applying clear cyber security standards across the system. The report also sets out the key priority of the NHSX – an initiative comprised of teams from DHSC and NHS England and Improvement – to develop a 'Cyber Security Strategy' in 2020 which will provide a framework for prevention of and protection from cyber security risks in the health and social care industry. DCMS also announced that over £250 million will	DHSC report

Development	Summary	Links
	be invested nationally by 2021 to improve cyber safety across the health and care system.	
Europol's strategic report on spear phishing highlights frequency of attack	The European Cyber Crime Centre ("**EC3**") of Europol published a '*Law Enforcement and Cross-Industry Report on Spear Phishing*', which has been established as one of the most prolific cyber threats in the EU. The report provides suggestions as to how to prevent, respond to and investigate spear phishing attacks. The report recommends two main technical defences against phishing threats which organisations can implement: (1) IT security policies, and (2) anti-phishing software. Public awareness by both individuals and businesses and employee training are crucial to identifying and reacting to spear phishing attempts. EC3 provides case studies on entities which have successfully implemented and executed incident handling procedures and methods for cooperation with law enforcement, such as the 'E-Crime Task Force' in the Netherlands.	EC3 press release

Data protection and privacy law

Development	Summary	Links
Council of the EU publishes revised draft ePrivacy Regulation	The Presidency of the Council of the European Union has published a revised draft of the ePrivacy Regulation (the "**Regulation**"). By way of reminder, the Regulation will sit alongside the GDPR and is intended to repeal and replace the existing ePrivacy Directive 2002/58/EC (as amended) which governs – among other things – the confidentiality and security of communications services, the use of cookies and location data and the sending of direct marketing communications. It is broader in scope than the ePrivacy Directive and aims to cover communications provided by a wider range of providers, including over-the-top service providers (such as instant messaging apps), Voice over Internet Protocol platforms and machine-to-machine services (such as the Internet of Things). The new draft provides clarification on a number of issues including cookies, data retention periods, child protection and consent when processing data from terminal equipment.	Revised draft (8 November 2019)
EDPS issues Opinion on e-evidence legislation proposals	The European Data Protection Supervisor ("**EDPS**") published Opinion 7/2019 on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters (the "**Opinion**"). The Opinion considers the European Commission's proposals to introduce two new proposals: (i) a Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters; and (ii) a Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. The Commission intends for the proposals to accelerate the process of securing and obtaining electronic evidence, which may be used in criminal proceedings, across EU borders. The EDPS acknowledges and supports the Commission's objective of ensuring that effective tools are available to law enforcement authorities to investigate and prosecute criminal offences, including the aim of proposals to accelerate and facilitate access to data in cross-border cases by streamlining procedures within the EU. However, the EDPS also highlights the need to respect the Charter of Fundamental Rights of the EU and the EU data protection framework at all times. Among others things, the EDPS suggests that the definitions of data categories in the proposed Regulation should be clarified. In addition, the EDPS makes recommendations on: the authenticity and confidentiality of orders and data transmitted, the limited preservation under European Preservation Orders, the data protection framework applicable, the rights of data subjects, data subjects benefiting from immunities and privileges, the legal representatives, the time limits to comply with European Production Orders and the possibility for service providers to object to orders.	Opinion

Development	Summary	Links
ICO calls for statutory code of practice on live facial recognition	The Information Commissioner Elizabeth Denham has written a blog post discussing the use of live facial recognition ("**LFR**") technology and has issued an opinion on the use of live facial recognition technology by law enforcement in public places ("**Opinion**"). The Commissioner reflects on the ICO's investigation into the use of LFR by the Metropolitan Police Service and South Wales Police In the post, the Commissioner calls for the government to introduce a binding statutory code of practice on the deployment of LFR. In addition, she emphasises that "*more work should be done by a range of agencies and organisations including the police, government and developers of LFR technology to eliminate bias in the algorithms, particularly that associated with ethnicity*". The Opinion makes clear that there are well-defined data protection rules which police forces need to follow before and during deployment of LFR and sets out the practical steps police forces must take to demonstrate legal compliance. Police forces must be able to show that LFR technology is strictly necessary, balanced and effective in each specific context in which it is deployed. The Opinion collates the findings of the ICO's investigation, the current landscape in which the police operate, and the recent judgment from the High Court in **R (Bridges) v The Chief Constable of South Wales**. The ICO noted that while public support for LFR to catch criminals is high, it is less so in relation to the private sector operating the technology in a quasi-law enforcement capacity. The ICO is separately investigating the use of LFR in the private sector, including where it is used in conjunction with law enforcement. It will report its findings in due course.	Blog post Opinion
Information Commissioner invites views on the ICO's application for powers under POCA	The Information Commissioner has announced that the ICO is consulting on proposals for it to be granted access to investigation and other associated powers under the Proceeds of Crime Act 2002 ("**POCA**"). The ICO's consultation suggests that, without being granted the powers it is applying for, there may not be sufficient deterrent against criminal activity involving personal data. Under the Data Protection Act 2018, criminal breaches can only be punished by a fine. The level of fine may well be below the gain the individual enjoyed as a result of the criminal activity and it follows that there remains a financial incentive for crime in this area. If it is successful in its application for POCA powers, the ICO will be able to apply to the court for various orders, undertake investigations, gain access to information and seize assets (amongst other things). Asset recovery will be considered '*in all cases where offenders have benefitted from criminal conduct*'.	Press release Eversheds Sutherland briefing

Data protection and privacy law

Development	Summary	Links
ICO issues new guidance on special category personal data, including template appropriate policy document	The ICO has published new guidance on the processing of special category personal data, including the lawful basis requirements under Article 6 and Article 9 GDPR, and potentially Schedule 1 of the Data Protection Act 2018. The ICO has also provided a template "appropriate policy document", which is a short document outlining the compliance measures and retention policies with respect to the processing of criminal offence data and special category personal data under certain conditions, required under Schedule 1 paragraphs 1(1)(b) and 5.	Blog Guidance Appropriate policy document template
ICO submits final version of Age Appropriate Design Code of Practice to Secretary of State	On 22 November 2019, the ICO submitted its final version of the Age Appropriate Code of Practice to the Secretary of State for it to be laid in Parliament. Due to certain limitations during the pre-election period, the code is unlikely to be submitted before the new government is formed and the final version will be published after that. The ICO was required to prepare the code under section 123 of the Data Protection Act 2018. The aim of the code is to provide practical guidance on how to design data protection safeguards into online services and ensure they are appropriate for use by children, as well as meeting children's development needs. For the purposes of the code, a child is anyone under the age of 18.	ICO statement
Joint Committee on Human Rights calls on government to shift responsibility of cyber safety from individuals onto tech companies	The Joint Committee on Human Rights has published a report entitled '*The Right to Privacy (Article 8) and the Digital Revolution*' which calls for more "robust regulation" governing how personal data is collected and used by companies through web-based services. The report warns of the "darker side" to the personalisation of online content – the potential for groups of people to be discriminated by being excluded from the opportunity to see certain advertisements – as well as the dangers of drawing inaccurate inferences from data in order to tailor products and services to certain people. The Committee urges the government to reconsider its decision to exclude data protection from the scope of their new regulatory framework outlined in their recently published Online Harms White Paper. The report also highlights that the commonly used "consent model" is flawed in that it assumes that the individual is fully aware of how their personal data will be used and relies on the individual having necessary expertise to understand the risks that may be involved in what they are consenting to.	JCHR report

Development	Summary	Links
EDPS issues guidance on controller, processor and joint controller concepts for EU public bodies	The EDPS has published guidance on the concepts of controller, processor and joint controllership in the context of the processing of personal data by EU public bodies in accordance with Regulation (EU) 2018/1725. Although the guidance is aimed at EU institutions, bodies, offices and agencies it contains commentary on the different obligations attached to each role and some illustrative case studies and checklists which may be of interest to organisations more widely.	Guidance
EDPB publishes agenda for its 15th plenary session	The European Data Protection Board held its 15th plenary meeting on 12 and 13 November 2019. The agenda included, among other things: • **report on the third annual review of the EU-US Privacy Shield** (the EU-US framework for the transatlantic transfer of personal data), which was subsequently published on 18 November. This included concerns as to the substantial compliance checks required by the main principles of the Privacy Shield and comments as to the need to assess further the Privacy Shield requirements in relation to HR data and processors; • **its draft guidelines on data protection by design and default** – a consultation on these guidelines subsequently began on 20 November and will end on 16 January 2020; and • **its guidelines on the territorial scope of the GDPR**, which it subsequently published in final form on 12 November.	Agenda Third annual joint review of the EU-US Privacy Shield Draft guidelines on data protection by design and default Finalised guidelines on territorial scope

Development	Summary	Links
TuneIn radio breaches Copyright, Designs and Patents Act 1988	In **Warner Music UK Ltd and Sony Music Entertainment UK Ltd v TuneIn Inc**, the High Court held that a service enabling users to access music radio stations around the word via a website or app had communicated copyright works to the public contrary to section 20 of the Copyright, Designs and Patents Act 1988 ("CDPA") where: (a) the radio stations were not licensed in the UK or elsewhere; (b) they were licensed for a territory other than the UK; or (c) they were premium stations created exclusively for the service (a, b and c cumulatively being all accessible radio stations that were not licensed in the UK). The defendant's argument that it provided nothing more than a directory or search engine linking users to the relevant website failed. TuneIn intervenes directly in the provision of the links to the radio stations' audio streams in a manner that conventional search engines and hyperlinks on conventional websites do not. TuneIn's activity is targeted at users in the UK, thereby bringing into play the necessary territorial element for breach of section 20 CDPA. TuneIn was not entitled to rely on any of the "safe harbour" defences in the E-commerce Directive as none of these were relevant to its activities. As is expressly acknowledged in the judgment, this test case highlights the tension between the functioning of the internet on the one hand and the protection of IP rights on the other.	Judgment
Consultation on horizontal cooperation block exemptions	The European Commission has opened a consultation on the two Horizontal Block Exemptions: Regulation (EU) 1217/2010 for research and development agreements and Regulation (EU) 1219/2010 for specialisation agreements, together with the associated guidelines on the applicability of Article 101 TFEU to horizontal co-operation agreements. The purpose of the consultation is to collect evidence and views from stakeholders as part of the Commission's process of deciding whether to let the Horizontal Block Exemptions lapse, prolong them or revise them. The consultation closes on 12 February 2020.	Consultation

Development	Summary	Links
First annual self-assessment reports under Code of Practice on Disinformation published	The European Commission has published the first annual self-assessment reports by Facebook, Google, Microsoft, Mozilla, Twitter and 7 European trade associations regarding implementation of their commitments to tackle online disinformation under the self-regulatory Code of Practice on Disinformation. The Commission intends to present a comprehensive assessment of the Code of Practice in early 2020.	Commission press release
Survey relating to guidelines on the EU Regulation on promoting fairness and transparency for business users of online intermediation services	Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services, which comes into effect on 12 July 2020, sets out a legal framework for online intermediation services providers (such as online market places, online software application stores, online social media) and online search engines to use transparent terms and conditions for business users and to provide redress if those terms and conditions are violated. This includes a requirement to set out in the terms and conditions the main parameters that determine ranking of search results and the reasons for their relative importance. The European Commission has launched an online survey which it intends will help inform production of guidelines on ranking transparency. Responses are due by 12 December 2019.	Press release

Public sector

Development	Summary	Links
Revised procurement thresholds published	Revised procurement thresholds that will apply from 1 January 2020 have been published in the OJEU.	Revised procurement thresholds

Development	Summary	Links
Call for tenders for an international alliance for a human-centric approach to AI	The European Commission has announced a call for tenders for an international alliance for a human-centric approach to AI. The project objectives are to support the EU to: • develop responsible leadership in global discussions around legal and ethical aspects of AI; • create the conditions for the uptake of policies and good practices/standards that ensure an appropriate ethical and legal framework on AI; and • improve public awareness of the challenges and opportunities associated with AI. Applications must be made by 16 January 2020.	Commission call for tenders
LinkedIn report on AI Talent in the European Labour Market	LinkedIn has published a report on AI Talent in the European Labour Market which concludes that Europe has a smaller pool of AI talent than the US, but has strong ecosystems in place and that "with the right investments in training, further strengthening AI hubs and diversifying the workforce, policy leaders and businesses can help that talent diffuse across more industries and countries".	European Commission website

For further information, please contact:

Sara Ellis
Principal Associate PSL

T: +44 121 232 1062
M: +44 7827 954 720
saraellis@eversheds-sutherland.com

Claire Stewart
Principal Associate PSL

T: +44 20 7919 4856
M: +44 7867 155 050
clairestewart@eversheds-sutherland.com

Lizzie Charlton
Senior Associate PSL (Data Protection & Privacy)

T: +44 20 7919 0826
M: +44 7827 230 131
lizziecharlton@eversheds-sutherland.com

eversheds-sutherland.com