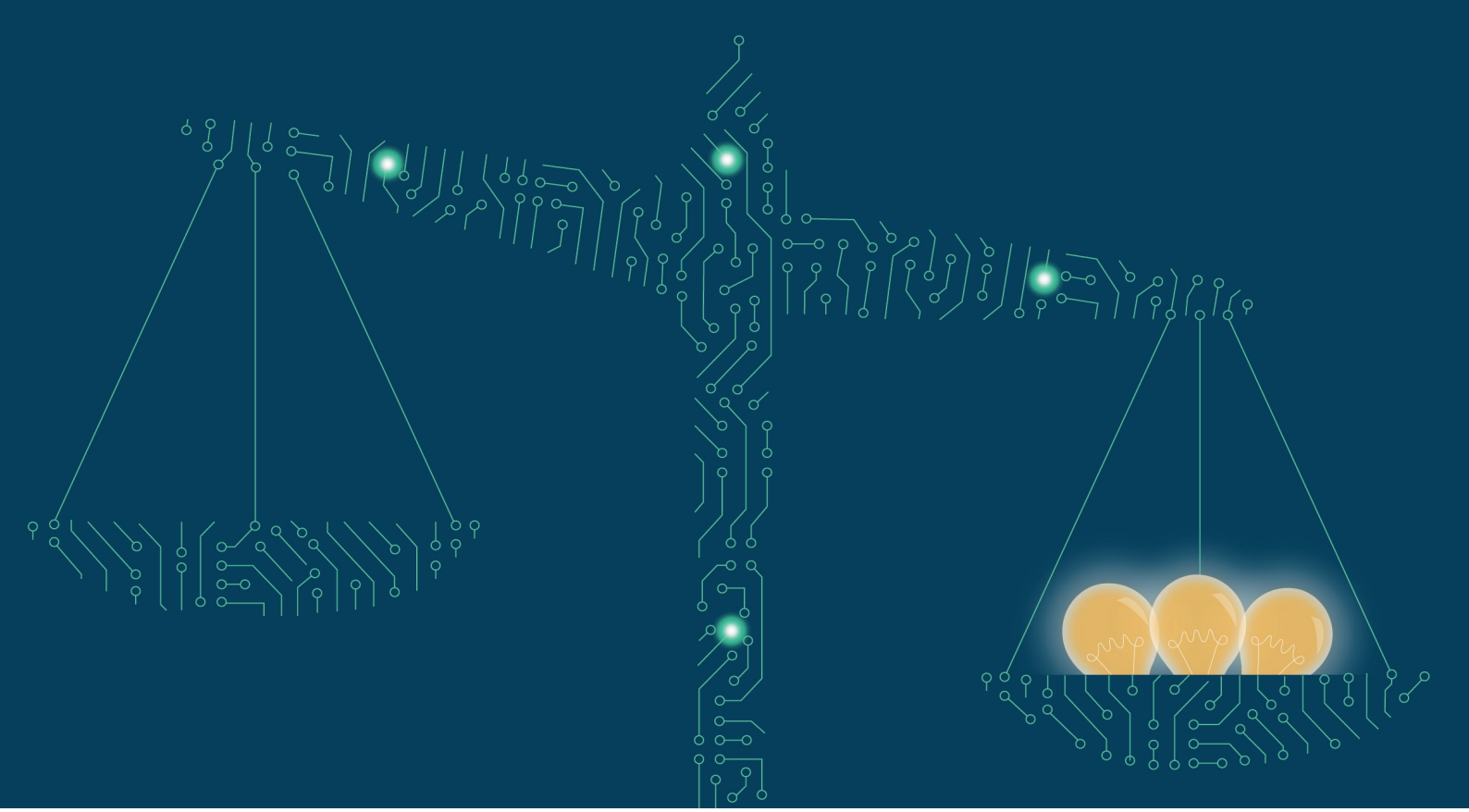

TECHNOLOGY DISPUTES
THE WAVE OF THE FUTURE

Joel Smith, Andrew Moir, Ina vom Feld, Alexandra Neri, Kate Macmillan, Peter Dalton, David Webb and Rachel Montagnon of Herbert Smith Freehills explore some of the major themes that have evolved around technology-related disputes.

How technology will shape the future is a perennial question across all walks of life. When it comes to legal matters, the question often becomes more focused on what sort of disputes will arise due to these advances in technology. That is a separate, and perhaps more pressing, question for those involved in risk assessment and planning.

This article considers the major trends and themes that have evolved in this area and which are driving technology-related disputes across a number of sectors:

- Data class actions and their potential to shape the digital landscape, and the gathering and storage of critical data-sets against a backdrop of regulatory and cyber security issues.
- The huge increase in the use of, and investment in, algorithms and artificial intelligence (AI) and whether the current systems of intellectual property rights (IPR) can accommodate them satisfactorily.
- The key role played by copyright in relation to internet content and how this develops in the UK and the EU after the Brexit transition period.
- The impact of the Supreme Court's recent decision on fair, reasonable and non-discriminatory (FRAND) licensing terms and how this may affect technology licensing disputes overall and the interoperability of technology in general.
- The rise in the use of trade secret laws to protect and enforce rights in relation to new technology in the face of increasing theft or misappropriation of critical know how and confidential information.

DATA CLASS ACTIONS

The world is undergoing its fourth industrial revolution and stands on the cusp of a fifth, driven largely by the generation, analysis and use of data. Technology is disrupting everything: economic systems, democratic debate, social norms, international relations, as well as legal and regulatory systems. Data class actions are an important tool in the fight to create a digital world which is beneficial for individuals.

A European approach

There is a fundamental difference between the EU and the US around issues such as the right to privacy, freedom of speech and the free flow of data. The EU considers that action to protect European values on these points is an urgent priority. The President of the European Commission (the Commission), Ursula von der Leyen, has said that "We have

to move fast or we will have to follow the way of others who are setting these standards for us" (*https://ec.europa.eu/info/sites/info/files/soteu_2020_en.pdf*).

There have already been some legal challenges which have had a significant influence on the British data protection landscape, such as *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* and the right to be forgotten or, more recently, Mr Maximilian Schrems's challenge to the privacy shield (*C-131/14, see News brief "Google decision: the right to be forgotten", www.practicallaw.com/3-568-9605; Data Protection Commissioner v Facebook Ireland and Maximillian Schrems C-311/18, see News brief "Schrems II and data transfers: cast adrift in a sea of uncertainty", www.practicallaw.com/w-027-1214*).

The EU clearly sees European data class action claims as a key part of achieving a digital age based on European values. These values are likely to play an important part in driving the direction of travel of EU regulation and law in this area. The General Data Protection Regulation (*2016/679/EU*) (GDPR) contains provisions that support these principles including:

- Representative actions (*Article 80*).
- Provisions on liability and compensation (*Article 82*).
- Rights in effective judicial remedy (*Articles 78 and 79*).

There has been an increase in claimant firm activity, the availability of, and interest in, litigation funding and high-profile claims as a result of increased awareness. In short, there has been a significant increase in data class activity across Europe (*see box "Data class actions in France"*).

Interestingly, the Dutch are leading the way. In 2019, the Dutch Senate approved the Wet afwikkeling massaschade in collectieve actie (translated as the Act on Redress of Mass Damages in a Collective Action) (WAMCA), which provides a regime for collective actions for damages that makes the jurisdiction an attractive one for large-scale international collective actions.

The first data class action under the WAMCA has been brought by the Privacy Collective, a Dutch consumer privacy non-profit organisation, in relation to the use of third-party cookies that help track and target internet users. The claimants are seeking €500 in compensatory damages for each user who did not consent to the use of their sensitive personal data. Reports suggest that a similar case will be filed in the UK.

Data class actions in France

France has had a specific regime for class actions related to consumer and competition law since 2014 (*Law No 2014-344*). In 2016, this regime was extended to include data protection class actions (*Law No 2016-1547*). Since June 2018, consumers have been able to seek injunctive relief in a class action as well as compensation for the damages suffered, including mental distress. In order to bring a data class action, the claimant has to prove a breach of the General Data Protection Regulation (*2016/679/EU*) (GDPR) or French data protection law, and the other consumers in the class must be in a similar situation.

While there have not been many data class actions, there are two notable cases currently pending in France:

- *Internet Society France v Facebook*, where Internet Society France asserts in seven causes of action that Facebook has breached the GDPR and seeks €100 million in damages.
- *UFC-Que choisir v Google*, where the UFC-Que Choisir group alleges that Google infringed the GDPR by exploiting the personal data of its users, particularly those using Android mobile devices, and asks Google to compensate users for up to €1,000. There are around 28 million Android users in France who could be eligible for compensation.

The reason why there have not been that many data class actions in France can be explained by the French regime being introduced only recently and the requirement that a class action must be filed by a licensed association, which has to meet specific conditions; for example, associations, consumer protection groups or trade unions that have been registered for at least five years for the purposes of protecting the privacy and personal data.

A proposed law on a new set of rules for class actions in France was presented to the French National Assembly on 15 September 2020. The Assembly representatives putting forward the proposal are arguing that the present system is not working effectively as only 21 class actions, including 14 consumer cases, have been brought since 2014, and not a single company has yet been held liable.

UK position

In the UK, this type of claim has been brought under the group litigation order (GLO) or representative action procedure (*see feature article "Class actions in England and Wales: key practical challenges", www.practicallaw.com/w-015-9333*). The GLO procedure is suitable where it is possible to identify multiple claimants and where there are common issues of fact or law in each claim. A court order is needed to start a GLO. The representative action procedure is suitable where it is difficult or impossible for all of the parties affected by a claim to be parties to the proceedings, but where there is a common interest, a common grievance and a potential remedy that would be beneficial to everyone. A court order is not needed to issue a representative action claim.

In the UK, data claims to date have been brought under data protection law, misuse of private information or breach of confidence (or misuse of confidential information, as Lord Justice Arnold recently stated it should be called (*The Racing Partnership Ltd & Others v Sports Information Services Ltd [2020] EWCA Civ 1300; see "Equitable duty of confidence: betting data", Bulletin, Commercial law, this issue*)). It seems clear that, while the GDPR will have a central role, so too will the English laws of privacy and misuse of confidential information, not only in relation to liability but also in relation to remedies.

It is important to clarify that the model of data protection in England and Wales is not like the one in EU and UK competition law that allows for follow-on or piggy-back litigation, where the regulator's decision is binding and anyone who chooses to bring a claim does not need to establish liability and the court is able to move straight on to issues of causation and loss.

However, claimant firms are issuing class action claims within hours of the fact of a data breach coming into the public domain. This is made possible by the requirement under Article 34 of the GDPR that, if there has been a data breach that presents a high risk to individuals, the data controller must tell those individuals about it, which makes the event public knowledge. Claimants can then issue but not serve a claim, giving them a few months to establish the facts and whether the claim is viable. The purpose of issuing the claim is for the claimant to get their foot in the door.

Obviously, this does not happen in all cases; it depends on the data breach being significant enough that the claimants think that it is economically viable to run the claim. But it is a significant issue for many businesses that suffer data breach incidents.

Until there is clarity on what these claims are worth there is going to be a continuing trend for claims to be issued speculatively. The most significant recent decision on class data actions in the UK considered only liability and not quantum (*Various Claimants v WM Morrison Supermarkets Plc [2020] UKSC 12; see feature article "Data class actions: the outlook after Morrison", www.practicallaw.com/w-026-2617*) (*see "Damages" below*).

Ultimately, the true game-changer in this area may be political initiatives, such as GAIA-X, an EU project to develop common requirements for European data infrastructure. There have been suggestions in recent months about the UK becoming some sort of halfway house between the EU and the US positions on data protection. However, that would require legislation and there have not been any specific proposals regarding divergence yet.

Damages

The question of what damages might be claimed, and for what are individuals being compensated, is an important issue and one area where the EU approach differs substantially from that of the US. EU law recognises that it can be devastating for people when they lose control of their private information.

The principle of recovering damages for loss of control of information is now firmly established. This has been seen in both misuse of private information and data protection claims, which is not surprising given that both causes of action are based on the right under Article 8 of the European Convention on Human Rights (ECHR) to respect for private and family life.

Article 82 of the GDPR refers to compensation for material or non-material damage. But even before the GDPR came into force, it was recognised expressly that the UK's narrow interpretation of the Data Protection Directive (*95/46/EC*) was incorrect and that damages were available for mere distress caused by a breach (*Google Inc v Vidal-Hall [2015] EWCA Civ 311; see News brief "Claims for misuse of information: the DPA comes of age", www.practicallaw.com/6-610-3046*).

Even if quantum is quite low for each person who suffers loss of control, the number of claimants involved in a class action can make this type of claim very costly to any business. For example, the aggregate value of the Dutch Privacy Collective claim may be €10 billion because it applies to a large volume of potentially affected data subjects.

The misuse of data or information can cause a wide range of potential harms, a list of which appears in Recitals 75 and 85 to the GDPR. These refer, among other things, to physical, material and non-material damage, discrimination, identity theft or fraud, financial loss, damage to reputation, significant economic or social disadvantage. If the harms caused are serious, the damages will be significantly greater than the amounts due for mere loss of control.

A good example is *TLT and others v Secretary of State for the Home Department*, which concerned the publication of information about asylum seekers and their families (*[2016] EWHC 2217 (QB)*). The High Court held that the data breach had prompted a rational fear in one of the claimants that he would be targeted by the Iranian authorities to the point where he felt compelled to relocate his entire family and that, accordingly, he should be compensated. In that case, the size of the award was £12,500.

The misuse of data, particularly when it comes to the unlawful profiling of individuals, which is very topical currently, might give rise to some substantial harms and damages that will match these in scale.

PROTECTION OF ALGORITHMS AND AI

One of the fastest moving areas of technological development has to be AI and the exploding use of algorithms. Given that these are likely to underpin high-tech developments over the next decade, it is important to consider whether it is possible to adequately protect algorithms and ideas created by AI with the current IPR systems.

Nature of AI

AI is generally used to describe machines and systems that carry out tasks commonly associated with intelligent beings, without direct human oversight. It is this which makes it such a significant issue; the ability of AI to do things without involving human control or instruction, including generating IP, or infringing others' IPR, independently of any direct human decision making.

The widespread use of AI raises issues which have not had to be dealt with before from an IP perspective and comes down to a fundamental issue: whether AI is just a tool that is used by humans in the same way as other software might be (and, therefore, from a legal standpoint lacks any independent character of its own with its actions attributable to a human operator or owner), or whether its ability to behave autonomously changes the way that legal systems must deal with it. This poses a particular difficulty for IP policy makers.

Legislative protection

The current legislative framework in the UK was established in a different era of computing. Computer-implemented innovations are usually protected by copyright, the expression of the innovation being in the source code, user interfaces, art assets and databases that exist in the software. Where possible, patents may be sought to protect the functionality of the software but these are subject to some quite stringent legal hurdles. Further, the substantive legislation governing those rights pre-dates the modern computer age let alone the types of AI innovations that are now arising, and does not provide satisfactory cover in terms of protection or enforcement.

The main pieces of legislation involved, the Copyright Designs and Patents Act 1988 and the Patents Act 1977 (1977 Act), have been updated since they came into force. There have been attempts to amend and supplement this legislation, both at the UK and EU levels, to retrofit it to deal with digital technology developments with a degree of success. However, it is fair to say that there has always been some disquiet about whether these adaptations of the law really go far enough and deal properly with the issues at hand.

For example, in copyright law, there was a great deal of case law during the 2000s that dealt with how far copyright could be used to protect software. When taken together, this resulted in a relatively restricted interpretation of the extent to which copyright can protect software beyond the direct copying of assets. This has made it quite difficult to protect software and buyer copyright in the absence of some obvious copying of source code or theft of other assets.

The cases effectively limited copyright to the literal copying of specific elements of software such as the source code, art assets and sounds, and excluded more generalised claims seeking to protect the functionality and processes contained in software (*for example, Navitaire Inc v Easyjet Airline Co and Another [2004] EWHC 1725, www.practicallaw.com/2-200-2402; Nova Productions Ltd v Mazooma Games Ltd and others [2007] EWCA Civ 219, www.practicallaw.com/7-314-1956; SAS Institute Inc v World Programming Ltd [2013] EWHC 69 (Ch), www.practicallaw.com/8-524-3749*).

Equally, while patents can theoretically protect the functionality of computer-implemented inventions and are therefore a valuable right in the field of software, there have been strong arguments on both sides as to whether patents are a suitable tool for protecting software (*see box "For and against patenting software"*).

For and against patenting software

Opponents to software patents point to issues such as the 20-year monopoly that is granted for patents, which in software terms effectively covers two generations of development. Opponents claim that it hinders innovation to wall off software behind patents and so potentially prohibits additional innovation by a third party for such a length of time.

Equally, it can be difficult to draft precise patent claims in respect of software (and there is of course a potential patentee interest in not doing so), which has led to issues around the breadth of historic patents. Due to the breadth of their claims, patents that were granted in the early 2000s can still apply to software today even though that software and the underlying processes may not have been conceived of at the time of filing.

On the other side of the debate, software developers and software owners point to the difficulty of obtaining patent protection and the costs of doing so. They are also concerned by the unsatisfactory unpredictability with which software patents are granted or not granted. It is hard to know which way an examiner will go on any particular case and results vary widely between jurisdictions, which is far from ideal.

AI as an inventor

AI is posing specific problems because of its potential to make independent decisions and, potentially, to innovate for itself. For example, who is responsible when an AI product independently does an act that infringes IP? Is it possible for the owner of the AI be held to have done the act, even though they may have been unaware that the AI was doing it? And, if AI invents something, who is eligible to own a patent, or indeed any other IPR over that invention, if anyone?

For a long time these were speculative questions, but there is now ongoing litigation about the ability of AI to be an inventor. The High Court recently held that an AI called DABUS could not be an inventor for the purposes of the 1977 Act, with the result that the invention was potentially incapable of patent protection because there was no one capable of applying for the patent (*Thaler v The Comptroller-General of Patents, Designs and Trade Marks [2020] EWHC 2412 (Pat); www.practicallaw.com/w-028-0539*). The question was also heard before the European Patent Office, which refused two European patent applications naming DABUS as inventor, and the US Patent and Trademark Office, which similarly declined to grant patent applications in the US. In each case, the finding was essentially the same: only natural persons can be named as inventors on a patent.

One unanswered question is whether the owner of the AI should be held to be the inventor. This position would fit with the model of AI as a tool, but it may not reflect reality. In the DABUS cases, the AI had been fed with data relating to a particular field and left to generate the invention independently. Its owner's evidence was that he had nothing to do with conceiving the invention and so it would be wrong for him to claim to be the inventor in a patent application. While this point was not determined, on a logical and potentially policy level, crediting an invention, and granting potentially expansive IPR, to an inventor who has had no creative or technical input into generating the invention, seems difficult to justify.

Potential change

A recent announcement from the European Competition Commission has created waves in the technology world. Commissioner Margrethe Vestager has announced that the Competition Commission will announce draft rules on 2 December 2020 to require dominant technology companies to explain how their algorithms work, so as to make sure that companies are held responsible for decisions made by those algorithms. This move could require disclosure of what are closely guarded secrets for the technology giants.

This debate is creating a lot of discussion in legal and technology circles, and appears to be generating some wider legislative momentum. The World Intellectual Property Organisation is undertaking a broad consultation process into how IPR should dealt with in AI, and whether legislative changes are necessary (*www.wipo.int/about-ip/en/artificial_intelligence/call_for_comments/*).

In September 2020, the government issued a similar public consultation (*www.gov.uk/government/consultations/artificial-intelligence-and-intellectual-property-call-for-views*). Both consultations ask far-reaching

questions about how AI should be protected, how the IP system should deal with the acts of AI, and what the moral and commercial considerations are for IP protection for these 21st century developments.

COPYRIGHT AND DIGITAL CONTENT

The issue of who is liable for, or responsible for enforcement against, the unauthorised use of content on social media and other content sharing sites has been an increasingly hot topic for a few years. This arises from the fact that the business model of these sites is based on sharing and making available content that is created not by the sites, but by their users: the content providers.

Article 17 of the Digital Copyright Directive (*2019/790/EU*) (Article 17) (Copyright Directive) (formerly Article 13) relates to underlying platforms' responsibility to police content that is posted or uploaded by users and was hugely controversial at the time it was introduced. It polarised discussions between rights holders, users and platforms. Nevertheless, it was adopted in 2019 and national compliance among EU member states is not required until June 2021. The UK government announced that it would not implement the Copyright Directive before the end of transition period after the UK had left the EU.

Addressing deficiencies

The Copyright Directive affects online content sharing providers and service providers. In particular, there are obligations to address what people have called the value gap: that is, the fact that the users who provide content do not get any compensation or benefit from service providers in relation to the content they are posting or uploading. The Copyright Directive also seeks to address the failures of the notice and takedown procedure, such as the need to keep notifying a platform of repeated infringements to get individual postings taken down, without the ability to require the service provider to search and locate similar infringements, now or in the future.

The key requirement in the Copyright Directive is the obligation to negotiate a licence agreement with the rights holders for the material on the platform or with the collecting societies who represent them. Service providers are effectively required to enter into licensing arrangements with their users and have various obligations to use best efforts to prevent making infringing content available.

In essence, service providers will be liable as primary infringers for acts of communication to the public unless they can demonstrate that:

- They have used best efforts to obtain a licence for the content.
- They have used best efforts to ensure the unavailability of the content once rights holders have notified them, and provided information about the offending or infringing content.
- They have acted expeditiously on receiving that notice to disable or remove the content, and used best efforts to prevent any future uploads (*Article 17(4)*).

So for service providers that do not want to, or cannot, obtain a licence agreement, the content provider will have to demonstrate that it has made its best efforts to obtain authorisation from the rights holders but was unable to identify or locate them. This involves demonstrating best efforts to identify copyrighted content for which the rights holders have transmitted fingerprints or relevant information, and showing, following notification, that they have blocked access or removed content, while preventing its subsequent republication, if the rights holder has provided the relevant information.

Practicalities

The so-called take-down obligation in Article 17 will not be a problem for service providers such as YouTube, because large content platforms already have the tools and the necessary processes to block and filter. The rights holder is able to notify and provide those platforms with their record of the copyright work and large platforms have the fingerprinting tools that enable them to keep the content off their platforms.

More recently established platforms, such as TikTok or the smaller platforms, have not yet developed the necessary tools to track illegal content and to take it down following a notification and are also not able to prevent the reposting of the same content on the platform by another user.

Although Article 17(4) recognises that upload filters are not required, in practice it is difficult to see how filtering technology cannot be at least part of the solution. However, there are a lot of concerns about so-called over-blocking (that is, blocking material which should not be blocked) and what happens if legitimate material is removed or disabled, including material that might be protected by copyright limitations or exceptions.

Issues with implementation

Member states will now have to implement the Copyright Directive in their national legislations and, in this respect, the devil really will be in the detail (*see box "Implementation of the Digital Copyright*

Implementation of the Digital Copyright Directive in Germany

The German Federal Ministry has published its latest draft legislation to implement the Digital Copyright Directive (*2019/790/EU*). This is just one example of the sort of implementing legislation that is being crafted and there may be very different results in different jurisdictions.

Some interesting points that have arisen in the German legislation are, for example, that there is a proposal about having a de minimis use, rather like an exemption for non-commercial minor uses. A de minimis use could be 20 seconds of material, 1,000 characters of text or a small image of 250kb. However, this has been opposed by rights holders groups. Nevertheless, there would be some mandatory remuneration for the content provider.

The German legislature is considering a system where, if content is potentially going to be blocked, then the content provider is given the option to flag their content as being either contractually authorised by licence or by virtue of a copyright exemption, like parody, as a way of avoiding over-blocking. It is also looking at making it mandatory to have a form of complaints procedure that is not automated but has people dealing with complaints if material is over-blocked.

Directive in Germany"). There are many questions about balancing implementation with the Charter of Fundamental Rights of the EU, the ECHR (such as the right to freedom of expression and a fair trial), the e-Commerce Directive (*2000/31/EC*), which does not require service providers to monitor their networks, and the GDPR, in terms of the disclosure of user information.

The Commission went through the process of stakeholder consultations in the process of drafting Article 17, but despite this, it does seem to have polarised the debate further. The Commission is now producing guidance on how Article 17 should be applied, which might be issued by the end of 2020.

The French government wants to allow smaller or newer service providers time to adapt and to take the opportunity to configure their set-ups to the new obligation in order to maintain competition in the sector. This may be a factor involved in the Copyright Directive's limitation of provisions of Article 14 of the e-Commerce Directive, the so-called "hosting defence", which states that the service provider has no obligation to control what happens on its platform. Under the Copyright Directive, those providers have the obligation to be aware of copyright content that is stored on, or accessed through, their platforms.

There are some distinctions, however, because platforms are only required to block access and remove content once the rights holder has sent the platform operator the relevant information.

If the content service providers are less than three years old, have an annual turnover of less than €10 million, and receive less than five million visitors a month, then a lighter regime will apply under Article 17(6).

Content-sharing services across the EU will have to provide to rights holders, at their request, adequate information on the functioning of the services' procedures and information about the use of content covered by the licensing arrangements.

TECHNOLOGY LICENSING AND FRAND DISPUTES

The field of telecommunications, and other fields where industry technology standards are developed and may be covered by essential patents, are a source of substantial licensing disputes. A critical issue in these disputes is in which jurisdiction is the litigation conducted and, therefore, which court determines the terms of the technology licensing.

The Supreme Court's judgment in *Unwired Planet* certainly puts the UK courts in a good position to take jurisdiction for FRAND disputes in virtually all circumstances (*Unwired Planet International Ltd and another v Huawei Technologies (UK) Co Ltd and another; Huawei Technologies Co Ltd and another v Conversant Wireless Licensing SÀRL; ZTE Corporation and another v Conversant Wireless Licensing SÀRL [2020] UKSC 37; see News brief "FRAND patent licensing: Supreme Court stays the course", www.practicallaw.com/w-027-5139*).

UK jurisdiction

Once an infringement of UK patent rights has been established and the infringer is seeking to rely on a FRAND defence in order to avoid an injunction, then the UK courts will go through the exercise of determining the terms of a FRAND licence. As *Unwired Planet* shows, that licence can be for the standard essential patent (SEP) holder's global portfolio of SEPs.

For the UK to be seised with jurisdiction it first requires the SEP holder to choose to litigate in the UK. The UK is certainly an attractive jurisdiction for SEP holders given that it allows them to short circuit the need for litigation in each individual jurisdiction and the royalty rate determination in *Unwired Planet* was considered favourable to the SEP holder. There is still scope for implementers to avoid a UK-determined FRAND licence but only if they waive their FRAND rights and accept an injunction in the UK, which might not be a commercially feasible approach for the larger players in the UK market.

Forum shopping

Although the UK has taken a very broad approach to jurisdiction it looks like other territories, such as the US, Germany and possibly China, will also seek to undertake determinations of global FRAND licence terms. In those circumstances, forum shopping may become a lot more common, with each party trying to get global licence terms determined in the jurisdiction that they think will be most favourable to them.

This inevitably brings up the possibility of there being simultaneous proceedings in the UK and other national courts. It seems that the UK will not give up jurisdiction to other courts in those circumstances. In *Conversant*, which was before the Supreme Court alongside *Unwired Planet*, the main grounds for the court refusing to give up jurisdiction was that Huawei had failed to show that the Chinese courts could determine the terms of a global FRAND licence.

This still leaves open the question of what happens when there is another national court that can determine global licence terms. The Supreme Court in *Unwired Planet* suggested that the key issue in dispute in these kinds of FRAND cases are the UK patent rights, and that the FRAND determination is just a necessary consequence of the infringer having raised a FRAND defence.

As a result, the FRAND issues were not of primary importance when considering jurisdiction in *Unwired Planet*. If that is the approach that the court takes in the future, then arguably there are no circumstances in which the UK courts will give up jurisdiction to another national court because the appropriate jurisdiction to consider the infringement of UK patent rights will always be the UK.

This does seem to be the approach that has been taken in *Phillips v TCL* (*[2020] EWHC 2553 (Ch)*). In *Phillips*, the UK courts were first seised, but the High Court suggested that even if they had not been, the UK courts could still have proceeded with a determination of global FRAND licence terms even though there were concurrent French proceedings that would apparently also determine the terms. There is therefore a clear risk of inconsistent judgments being issued by different national courts in the future.

This suggestion from the judge in *Phillips* was obiter, so the question remains, if proceedings commenced first in time in another national court are already at fairly advanced stage and it is clear that those proceedings can result in the determination of the global licence, whether in all those circumstances the UK courts might be willing to stay the FRAND aspect of the dispute pending judgment from the foreign court.

However, this situation is so far untested and it seems likely that there will be a lot more jurisdictional tussling in the coming years.

Other FRAND-favourable jurisdictions

In Europe, Germany and the UK are considered to have the leading patent courts. Following

Unwired Planet, it is interesting to consider the German courts' potential reaction.

There is competition between the national courts for SEP patent litigation. For example, the Munich court is innovative with new patentee-friendly ideas. It is also possible to obtain a worldwide FRAND portfolio licence in Germany through the enforcement of SEPs. However, it is not the court that decides on the licence terms or sets the royalty rate directly, but the parties themselves under the pressure of a possible injunction.

If the defendant does not accept what the court considers a FRAND proposal from the SEP holder and does not make a counter-offer which is FRAND, it will be injuncted in Germany. This is a pressure point for industries that are based in Germany. For example, the connected and autonomous vehicle (CAV) FRAND cases, which primarily take place in Germany are driven by the fact that there is a large number of car manufacturers there and they are therefore under threat from actions in Germany more than they would be in the UK. However, given the decision in *Unwired Planet*, some businesses might consider it more efficient to come before a UK court that is willing to set the licence terms itself.

The German courts are certainly considering this situation. The Munich court has a two-hearing system: at the first hearing, the court gives its impression of the proposals from the parties and the court tells them where it sees the "story" of the case going; then there is a pause between the first and the final hearings. During that time, the Munich court offers a mediation through another judge, separate from the infringement case panel, so that the parties, in light of the suggested direction of travel from the infringement court, can agree on FRAND licence terms. Mediation can also be performed through other bodies. Given that this current method of handling these disputes is effective, it seems unlikely that the German courts will develop a system where the courts themselves set the licence terms.

Overall, in the CAV cases, and also in other recent patent cases, the German system is showing itself to be favourable to patentees, as well as the German courts drawing inspiration from the UK courts. For example, the German Federal Supreme Court has recently cited *Unwired Planet* and the requirement that a willing licensee must be willing to take a FRAND license whatever the FRAND license terms may be (*Sisvel v Haier KZR 36/17*). This is a clear influence from the UK.

Related information

This article is at practicallaw.com/w-028-3689

Other links from uk.practicallaw.com/

Topics

Confidentiality	topic/7-103-1304
Copyright	topic/0-103-1270
Data protection: general	topic/1-616-6550
Patents	topic/2-103-1306
Restraint of Trade, Confidentiality and IP	topic/2-103-2061
Rights of data subjects	topic/6-616-6190

Practice notes

Automated vehicles: legal and regulatory framework	w-013-2663
Demystifying artificial intelligence (AI)	w-008-5369
Digital Copyright Directive: key provisions	w-019-6934
GDPR and DPA 2018: claims for compensation	w-018-4325
GDPR and DPA 2018: enforcement, sanctions and remedies	w-005-2487
Overview of privacy law	1-507-0879
Patent infringement	0-592-4826
Patent infringement: remedies: injunctions	w-008-8500
Protecting trade secrets: overview	w-021-1676
Protecting confidential information: overview	8-384-4456

Previous articles

Data class actions: the outlook after Morrison (2020)	w-026-2617
Patent licensing: what next for FRAND? (2019)	w-018-7499
GDPR one year on: taking stock (2019)	w-020-0982
Class actions in England and Wales: key practical challenges (2018)	w-015-9333
Artificial intelligence: navigating the IP challenges (2018)	w-015-2044
Data use: protecting a critical resource (2018)	w-012-5424
Trade secret protection: guarding against a global threat (2017)	5-637-7032
Trade secret protection: the regime in key jurisdictions (2017)	0-639-0286
Employee monitoring: the value of being prepared (2016)	3-629-9945
General Data Protection Regulation: a game-changer (2016)	2-632-5285

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

PROTECTION OF TRADE SECRETS

There has been a great increase in interest in the protection of technology and business practices through trade secrets. Trade secret protection has become a key issue, as shown by a survey by Euromoney Investor, which said that 48% of senior executives now saw it as a critical issue ahead of patent strategy (*https://assets.euromoneydigital.com/a4/85/4f0872014c7e9e3aebe0c3ba42e2/the-board-ultimatum-protect-and-preserve-final.pdf*).

This may be, in part, because there are various issues with the process of obtaining patents and limitations on what protection they can afford. Many businesses do not want to share the details of their technology as they would need to in order to gain patent protection, especially if it is not readily accessible by viewing or reverse engineering the product. The pace of change in technology research and development is extremely rapid. Development cycles are becoming shorter and shorter, and developers are looking for the more flexible protection that trade secrets can offer across multiple markets.

Disadvantages of patents

The costs of patenting are high, given the time and the skill involved, as well as the prior art searches, sophisticated claims drafting, examination and the costs of dealing with any opposition proceedings and registering

in multiple jurisdictions. There is then the obvious downside of patents in that the claims and specifications of the invention are put in the public domain and the period of protection is finite: in most cases, a maximum of 20 years from first filing.

Equally, there are increasing numbers of court decisions challenging the validity of patents, which may expose businesses to unforeseen competition from the new entrants where the patents that were expected to protect new products are found to be invalid. There are areas where patent protection may be challenging to achieve or is limited where it is achievable, such as where patentability exceptions may apply, including in relation to software, biotech plant or animal engineering, or AI. In addition, there are specific changes in patent law, particularly in the US with inter-parties review, which have accelerated a switch to a focus on trade secrets.

Change in protection

At the same time as the increased desire to use trade secrets as a way of protecting inventions and technology, there has been an upgrade in the legal protection of trade secrets in many jurisdictions. The US Defend Trade Secrets Act of 2016 was matched by the EU Trade Secrets Directive (*2016/943/EU*), which has been in force from 2018 and, most recently, the China State Administration for Market Regulation has been working on draft provisions to protect trade secrets and provide remedies for infringement in China (*see feature article "Trade secret protection: the regimes in key jurisdictions", www.practicallaw.com/0-639-0286*).

Enforcement and remedies

Along with improvements in trade secret protection, there is also a move towards a focus on trade secrets enforcement. This seems particularly true in sectors like healthcare in relation to medical devices and in the automotive sector around driverless vehicle technology. The recent dispute in the US between Uber and the Google's self-driving car division, Waymo, over alleged access to trade secrets by an individual executive is an example (*Waymo LLC v Uber Technologies Inc, Ottomotto LLC, and Otto Trucking LLC Case No 3:17-cv-00939*). There is also interest in trade secrets in areas such as IT and computer technology development, professional services, financial trading (including algorithms), insurance, engineering and consumer product development.

The likelihood of obtaining early interim injunctive relief can be much higher in trade secret cases than in some patent cases, and damages obtained for claimants are certainly at a healthy level in the US. In the top ten trade secrets cases in the US over the last few years, the largest damages award is just short of $1 billion, which was in *DuPont v Kolan* and awards now regularly approach $100 million and average around $20 million (*Case No 3:09-cv-00058*).

In the EU, the Trade Secrets Directive has been very helpful to technology development by putting all member states on a level playing field and ensuring that there are adequate remedies throughout the EU. It is particularly important in the way that it extends those remedies to the infringing products that benefit from the trade secrets as opposed to only providing a remedy to the owner for direct use of the trade secret. In addition, the relief mirrors what is available under patent law, including the availability of both interim and final injunctive relief, damages and delivery-up or destruction of infringing products.

Implementation

The UK regime was already aligned with the requirements under the Trade Secrets Directive but other major EU jurisdictions, such as Germany, made some changes to the law to implement its requirements. For example, in Germany, there was previously no provision for confidentiality clubs which UK courts regularly put in place to ensure that confidential information is not revealed through the court process. Instead, confidentiality was safeguarded by other means, including non-disclosure agreements concluded outside of the court proceedings.

However, the definition of trade secret in the Trade Secrets Directive also creates difficulties in Germany and beyond, as information is only classed as a trade secret if all reasonable measures have been taken to keep it secret. This is new for Germany, as previously it was sufficient that the information was not public, and that the claimant had the intention to keep it secret and a justified interest in doing so.

Now the test has changed and its meaning will need to be tested. For the UK, this is also true, although there have already been a few cases assessing trade secret status (*for example, Trailfinders Limited v Traveller Counsellers and others [2020] EWHC 591 (IPEC)*). However, in the UK, the common law of confidential information has been retained in parallel and specifically allowed as an alternative or additional cause of action. In the UK, the remedies under the common law of confidentiality remain available in parallel to those available under the new trade secrets regime under The Trade Secrets (Enforcement etc) Regulations 2018 (*SI 2018/597*).

From the few cases heard so far in Germany since implementation in April 2019, it seems that the threshold applied by the courts has been high. For example, in a recent North Rhine-Westphalia employment court decision, the delay by a business in following up a previous employee who had taken confidential information and used it in his new employment, was assessed by the court to mean that the information was no longer a trade secret as reasonable steps had not been taken to protect the information (*file no 12 SaGa 4/20*). If the threshold remains at that high level, there may be problems with the regime for companies, which do not instigate suitable systems for designating and protecting trade secrets. This may affect SMEs more than larger companies that have more resources to deal with these issues. In any event, all companies need to revisit and, if necessary, improve their protection measures.

Joel Smith, Andrew Moir, Ina vom Feld, and Alexandra Neri are partners, Kate McMillan is a consultant, Peter Dalton is a senior associate, David Webb is an associate and Rachel Montagnon is a professional support consultant, at Herbert Smith Freehills.

This article is based on discussions at a webinar hosted by Herbert Smith Freehills LLP which brought together some of its leading technology disputes practitioners to discuss the issues.