IP & Media News

Our newsletter on recent developments November 2016

Hyperlinking

Following earlier updates on the rulings in Svensson C-466/12 and Bestwater C348/13, which clarified that it is not copyright infringement to link or embed a work already online, as there is no new public; the ECJ has now clarified that this remains the case even where the original upload linked to is itself infringing. The court ruled that any liability requires knowledge of the infringement, which most linkers will lack. However, where the link is for profit/commercial purposes, knowledge will be presumed (on the basis that businesses should check rights) and the business user must rebut knowledge. This is still a sensible and reasonably generous approach in line with actual usage in modern web and social media which rely on sharing. See GS Media C-150/16.

A Digital right for Press Publishers

The IPO is currently consulting on a new copyright right for press publishers in their published content. Germany introduced this right and Spain also attempted it (leading Google News to withdraw its services there). The Commission has decided on it and we expect to see it enacted. We attended meetings between on and offline publishers held by the Institute for Advanced Legal Studies last year when the temperature of industry was taken here and the issues explored.

The intention is to protect and assist publishers with bricks and mortar costs and, in particular, employees, in an industry under threat, from aggregators and bots

and content farms. In large part the issue was exacerbated by the ruling in Meltwater C 360/13 which clarified, that just as it is offline, reading or browsing online is not an exclusive right and is not infringing. The difficulty expressed by publishers was that while this made sense in relation to human readers, issues arose in relation to machine readers –which combined with the right to hyper link to works online (as above) –saw expensive news content reused by these new market entrants. Contrary arguments concerned preferring incumbents at the expense of disrupters and legislating about actors instead of conduct. If enacted it will be a limited right to authorise digital use of their particular publication/edition. The new right will have a 20 year term and operate like other 'related rights' or entrepreneurial copyrights such as those enjoyed by broadcasters in their broadcasts. See https://www.gov.uk/government/news/call-for-views-modernising-the-european-copyright-framework

Internet Intermediaries/ISPs

The same package of copyright reforms proposes to require ISPs to “co-operate” with rightsholders over measures to protect their works and including as to content recognition. The draft reads:

"Art 13: Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with rightholders, take measures to ensure the functioning of agreements concluded with rightholders for the use of their works or other subject-matter or to prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers. Those measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate. The service providers shall provide rightholders with adequate information on the functioning and the deployment of the measures, as well as, when relevant, adequate reporting on the recognition and use of the works and other subject-matter."

Readers will recall that currently under the Ecommerce Directive, there can be no general obligation on ISPs to monitor their systems/services for intellectual property infringements and that this has prevented ISPs from being required to filter content on their systems in a generalised way and has also ensured that Blocking Orders granted to date have been targeted and focused on specific URLs rather than broader measures. A general duty to cooperate may sound harmless enough but commentators are already concerned that this may mean inspection software on users devices, with the serious implications that has for privacy and expression. This debate is not new and in East Germany, in the 1970-80s rather than allow rightsholders to search homes for infringing cassette tapes, a general levy on blank cassettes for personal use was introduced --later adopted across Europe. Readers will recall that here the government's proposal for a general personal use/format shifting exemption was defeated on judicial review due to the failure to include such a remuneration scheme.

The Commission is also exploring “follow the money” redress schemes whereby platforms and ISPs may have to disgorge advertising revenue derived from infringing works--again likely to fall within the ambit of “co-operation.” Other proposals of note include a “joint referral platform” in order to prevent Takendown materials from being posted elsewhere. The context for this is currently Terror related materials but the language is wide enough to encompass criminal content more generally and possibly scaled infringement. This is a very early stage but the direction of travel is worrying given we have no accessible “put back” right, as enjoyed in the US models.

Digital Economy Bill 2016

Although its long been an offence to publish pornography online to those under 18, see R v Perrin (2002), this is now being regulated and sections 15-25 of the DEB impose an obligation to prevent access to the under 18s including by use of age verification technology. The Bill also provides for a regulator of age verification, this is expected to be the BBFC. Indeed proposals are for Blocking Orders against sites which fail to verify age. The Bill also deals with other miscellaneous matters and section 77 also provides for the laying down of a Direct Marketing Code of Practice, previously a self regulatory measure, now being given statutory force. Controversially it includes new laws allowing debts to, and fraud on, the public sector, namely HMRC, to be published. The current version of the Bill before Parliament is at http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0087/cbill_2016-20170087_en_1.htm

IPB

The Investigatory Powers Bill was passed last week and will receive Royal Assent later this year.

This is just in time before DRIPA (Data Retention and Investigatory Powers Act 2014) sunsets (which in turn temporarily replaced the Data Retention Directive struck down in Digital Rights Ireland, Cases C-293/12 and C-594/12).

We discussed the Bill in this year's earlier update. Our final view was the only meaningful protection was proper judicial authorisation and scrutiny via judges sitting in a court. However, now the IPB has passed, its business as usual and the Investigatory Powers Tribunal is what we now have.

The Tribunal held a few weeks ago in Privacy Int. v Secs of State for Foreign and Home, GCHQ and SIS [2016] UKIP Trib 15_110 that the UK government's bulk data programme (including for bulk personal and communications data) was unlawful until the avowal or disclosure of that programme to the public in the course of recent cases. This is follows logically from Liberty v IPT [2015] 3 All ER 142

(receipt of PRISIM and UPSTREAM data from the US was secret or “below the waterline,” so that only once the court was told did it become “prescribed by law” and foreseeable so before the avowal or disclosure there was a breach but not thereafter). That decision lead to publication of a Code of Practice and the PI case above. As the Tribunal in PI noted, other questions are still pending at EU level, including as to the adequacy of the UK approach to judicial authorisation and it left this to be dealt with at the same time as other adjourned questions. In a similar vein, the Advocate General in the Sec. of State for Home Dept. v Tom Watson & Ors C-698/15 case opined that the UK's bulk retention practices would be lawful only if strict requirements were met, including legislative authority (so that the practice and law is accessible and foreseeable and with adequate protection from arbitrary interference), due respect to privacy and data rights and limited to use in relation to, and as strictly necessary to, fight serious crime. The final decision of the ECJ is still pending. Advocate General Henrik Saugmandsgaard Øe was opined that a general obligation to retain data may be compatible with EU law subject to satisfying strict requirements. It was for national courts to determine, in the light of all the relevant characteristics of the national regimes, whether those requirements are satisfied. He considered only the fight against serious crime was capable of justifying a general obligation to retain data and no other measure or combination of measures could be as effective while at the same time interfering to a lesser extent with fundamental rights. We have to wait to see if the Court agrees with the Advocate General. Similar issues will be answered in Big Brother Watch v UK Application No. 58170.

These NGO driven cases bring helpful clarification and our public law is vastly improved by them, but the labyrinthine, byzantine complexity of the new codes and guidelines (set out in annexes to the PI judgment) ---render them impenetrable to most.

Privacy and suspicion/arrests

The court granted a privacy injunction to restrain publication of the fact that a businessman had been interviewed under caution but not arrested. See ERY v Associated Newspapers Ltd [2016] EWHC 2760 QB. It ruled he had an art. 8 of the European Convention on Human Rights, right to privacy in the fact of the interview which outweighed the Daily Mail's art. 10 right to publish it. It could publish the investigation into the two companies involved---in which there was a public interest —but due to the profile and connection of the man to the companies, that would necessarily implicate him. There is authority that there is no privacy in an arrest per se and it depends on the circumstances of the arrest, Axel Springer v Germany Application No. 39954/08 (2012) 55 EHRR 6, (the fact that the arrest took place in public would be a significant feature in what is always a fact sensitive exercise) and Mann J in Hannon v News Group Newspapers Ltd [2015] EMLR 1 at [101] (same). But this case breaks new ground and will have real implications for the press which focus primarily on accuracy/truth in these situations. What is surprising is that there was no real debate about the fact the man's art. 8 rights were implicated and they trumped the art. 10 rights of the paper and its readers. One of

the issues was whether the claim was in essence a defamation rather than privacy claim and an attempt to circumvent the rule against prior restraint of libel, the rule in Bonnard v Perryman [1891] 2 Ch. 269 (no injunctions to restrain libel only damages post publication as it is always possible to reframe and the courts should not become censors). This was dismissed as the court did not agree that the rule was engaged as the nub of the claim was not protection of reputation, although it was reputation based. Similar privacy issues arose in A v Norway No. 28070/06 (publication of police questioning of a convicted murderer recently released from prison in a high profile child abduction case-- causing loss of home and job and fear for life, was held to be a particularly grievous breach of art 8). Cases like these throw the law into stark relief and with the impact on individuals at times of extreme vulnerability. There is always a defamation risk in publishing about suspicion or investigation or even arrest prior to charge and a common approach is to wait until the police name an individual at charge and then include the police statement –which has statutory privilege. Indeed, Police Guidance and the Leveson Report recommend not naming those suspected/arrested unless there is a threat to the public. However, different forces have different approaches.

FOI

In Magyar Helsinki Bizottság v. Hungary, Application 18030/11, the ECHR held there is a right to information from public authorities under art. 10 of the European Convention on Human Rights. In the US, digital activists and academics are making FOI requests seeking disclosures of public/government deployment of algorithms for decisions impacting individuals, for example in relation to education (e.g. expected student performance -actual student performance =teacher performance) and probation and likelihood of offending. Naturally, as most of the software involved is off the shelf, the relevant department is not often able to comply and at this stage the purpose of the campaign is to raise awareness and question the use of unknowable metrics when applied to individuals.

Brexit

Readers will be aware that EU law is either direct law in member states (Regulations) or harmonising --requiring domestic implementation (Directives). Under discussion as away of dealing with Brexit is a Great Repeal Bill which would bring into domestic UK law, all EU law not already implemented domestically as a status quo measure, planning to leave reforms, if any, for the future. Its hard to see any point to any of it given on Human Rights, Data Protection, Intellectual Property, Banking and Finance, Environment and Defence, Security and Terror many other key areas, the UK via other treaty or reciprocity obligations will have to meet EU standards or essentially comply with EU law anyway—only in future it may not have any say in those laws. We look forward to the Supreme Court's clarification of

whether Parliament must vote to trigger Art. 50 TEU as the Secretary of State cannot do so under Royal Prerogative in Millar & Dos Santos v Sec. of State. [2016] EWHC 2768 (Admin). Lady Hale, the only Lady in the Supreme Court and an excellent academic mind, has suggested that the government may also have to replace the 1972 European Communities Act which took the UK into the EU. One does not have to be a constitutional law expert to see the merit in these arguments.

The ICO has advised that the UK will comply with the new General Data Protection Regulation (GDPR) passed in April this year and coming into force in 2018, whatever the outcome of Brexit. See the ICO guidance at http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0087/cbill_2016-20170087_en_1.htm Helpfully, it has also provided 12 step guidance on compliance: Preparing for the General Data Protection Regulation (GDPR) – 12 Steps to Take Now. We've discussed the features of the GDRP in earlier updates. Long an open question, it is now clear that dynamic IP addresses are personal data as clarified in Breyer v Germany C-582/14. This means those who collect or gather this information even unwittingly or in metadata or log form, need to notify with the ICO.

30th Flr, 40 Bank St, Canary Wharf, London E14 5NR
www.mcevedys.com | 020 7243 6122