FAST Legal Update

Federation Against Software Theft

FAST Legal Update
Member Bulletin May 2016

Contents

FAST Legal Update

Federation Against Software Theft

1 Personal Intro

1.1 Every month I update you on key legal developments affecting our sector. But I am not going to focus solely on IP law. It is clear from the business activities that many of our members are involved in that there are several legal developments that will have an impact on everything that we in the industry are engaged in at the moment. I aim therefore to bring you each month the legal headlines on issues for you to be aware of plus an update on Legislation, Case Law and Consultations. I will also be including a monthly book recommendation touching upon the themes we will be exploring each month. If you have any questions please contact me directly at FAST. I look forward to hearing from you.

Julian Heathcote Hobbins
General Counsel at FAST

2 Monthly Introduction

2.1 Another busy month has seen key developments in the Digital Single Market and the law on data protection more generally. Although some of the DSM initiatives are slowing down we will keep you up to date with developments as the DSM will have an impact on our sector. There are significant developments in the law on data protection which may have an impact on you if you are processing personal data. We also have a quick look at issues for you to be considering now if the vote goes in favour of Brexit. In the Legislation update we focus on trade secrets, e-signatures and copyright infringement. In the case law update there has been a recent decision that offers guidance on when standard terms contracts are not standard terms contracts. And there are a few consultations open which you should be aware of including one on a proposed software publisher's code of conduct! Thoughts on a postcard please… Finally given the developments this month in the law on data I have put "Big Data, does size matter?" by Timandra Harkness on my reading list.

3 Headline Stories

3.1 **Brexit: What will the impact be on your business?** If we have a vote to leave the EU on 23 June 2016 this may have a significant impact on your commercial relationships and contracts. It is not clear yet what would happen in a two year EU exit negotiation. It may therefore be advisable to start scoping out a contract review exercise now to check your contracts so that you are able to appreciate the full extent of any risks you may be facing in the event of Brexit:

3.1.1 **Performance:** Do any of your contracts rely upon some aspect of EU law or the single market, such as free movement of goods or workers? If so would the other party be able to claim that the contract is frustrated or that performance is excused by force majeure as a result of Brexit? Alternatively could they seek to rely on force majeure if the contract will no longer be profitable due to changes in tax structures? What are the risks you are facing here?

3.1.2 **Personal data:** Do you process or transfer personal data under any of your contracts? If you do then after Brexit the automatic transfer of personal data to the UK under such contracts will not be automatically permissible until the EU are satisfied that UK law offers sufficient safeguards. What impact could this have on the contracts you have in place with your customers and your suppliers?

3.1.3 **EU Regulations:** EU Regulations which have direct effect within the UK will no longer apply. The UK government will have to decide whether or not to replicate such legislation. It may also choose to repeal legislation enacted under EU Directives, such as TUPE and consumer rights legislation. You may wish to consider reviewing your contracts to take advantage of any such reforms.

Of course there may be a vote against Brexit. At this point in time it is only important to identify the issues that may affect you if there is a vote for Brexit. If so we will have more detailed proposals over the year in terms of issues that you may wish to consider.

3.2 **Plans by the European Commission to regulate Online Digital Platforms have been leaked!** As part of the Digital Single Market the European Commission has had a "communication" entitled "Online Platforms and the Digital Single Market" leaked prior to its scheduled publication on May 25th 2016. The communication indicates that the Commission is intending to regulate online platforms. They define online platforms as undertakings that are "capable of facilitating direct interactions between users via online systems and that capitalise on data driven efficiencies enable by network effects" (?). The paper goes onto argue that regulation is necessary to ensure a level playing field for comparable services; to ensure that online platforms behave responsibly; to maintain transparency and fairness needed for maintaining user trust; to encourage open fair, and non-discriminatory markets for maximum innovation. However the British government disagrees and in their consultation response argued that the European Commission should focus on applying existing laws to online platforms rather than creating platform specific rules. It is difficult to see how regulating online platforms will achieve the objectives stated above, or indeed if the case has been made out at all to justify such intervention. You can read the leaked paper here and we will keep you up to date if any plans do emerge for the regulation of online platforms.

3.3 **The need for Standards in the Digital Single Market:** The European Commission in a "communication" on April 19th said it plans to prioritise ICT standardization, by encouraging standards organizations to work more across borders and sectors. The Commission identified 5G, the Internet of Things, cloud computing, big data and cybersecurity as areas that need urgent standardization. This has already led to much discussion. Interested parties have aired their concerns about the dangers of either not getting the standards right, or failing to act quickly enough, or stifling innovation by setting standards which fail to allow innovative companies to be commercially rewarded for their efforts. All these themes were discussed at a recent conference details of which can be seen here. But nothing concrete has yet been proposed in terms of the actual standards to be adopted in the areas outlined above. There remains a tension between companies needing to commercially protect their intellectual property through proprietary software licensing, and a public need to have agreed standards that everyone can benefit from. Resolving this tension will be among the biggest challenges facing the Digital Single Market Initiative.

3.4 **EU - US privacy shield: continuing uncertainty over transatlantic data flows. What are the latest developments?** The European Commission declared the US Safe Harbour agreement invalid in October 2015. In February 2016 the European Commission announced that it had reached agreement on a new EU-US 'Privacy Shield'. But there remains uncertainty over transatlantic data flows. The new Privacy Shield will eventually replace the old Safe Harbor agreement. The Article 29 Working Party published its Opinion on the draft agreement on 13 April 2016. While the Working Party recognised that the Privacy Shield is a significant improvement to the Safe Harbor framework, it still has concerns about certain commercial and national security aspects of the Privacy Shield. However the Opinion of the Working Party is non-binding so the European Commission could still proceed to finalise the adequacy determination. The next step is for the European Commission to consult a committee composed of representatives of the EU Member States before issuing its final decision.

3.5 **Do you encrypt your customers' personal data?** The Information Commissioner Office (ICO) has issued guidance on encryption which is deemed to be an "appropriate technical and organisational measure" to ensure companies do not lose, destroy or damage personal data. The guidance does not suggest that all personal data should be encrypted but does suggest a risk based approach should be adopted. Key recommendations include

3.5.1 a need to have an encryption policy in place and guidance to assist staff in understanding it.

3.5.2 encypting personal data where its loss would result in damage or distress to individuals.

3.5.3 using encryption when transmitting sensitive personal data over the internet.

4 Legislation Update

4.1 **Are you ready for the GDPR?** The GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), was published on May 4th and will come into force on May 25th 2018. You now have two years to make sure that you are able to comply with the new data protection regime.

4.2 **Ten years in prison for infringing copyright.** The government intend to change the law so that someone who is engaged in online software piracy could receive up to ten years in jail. This will offer software providers greater protection than before. The decision follows a consultation carried out by the Intellectual Property Office last year. As a result of the consultation the government intends to "introduce to Parliament at the earliest available legislative opportunity re-drafted offence provisions in relation to sections 107(2A) and 198(1A) of the Copyright Designs and Patents Act 1988 (CDPA), in addition to increasing the maximum custodial sentence to ten years in sections 107(4A) and 198(5A) of the CDPA" (see https://www.gov.uk/government/consultations/changes-to-penalties-for-online-copyright-infringement#history. Under section 107(2A) a person commits an offence if they knowingly infringe copyright in a work by communicating the work to the public in the course of business or to such an extent as to affect prejudicially the owner of the copyright. Section 198(1A) contains the equivalent provisions in relation to performers rights.

4.3 **Trade Secrets Directive has a narrow definition of trade secret?** The European Parliament has adopted a new directive on Trade Secrets which will contain a much narrower definition of "Trade Secret" than is consistent with the UK's approach to confidential information. This means that when you draft confidentiality agreements you will need to have a wide definition of confidential information so as not to be caught by a narrow statutory definition when it comes into force. It is expected that the European Council will approve the Directive at the end of May 2016 and it will therefore come into force in each member state approximately two years later. The Directive aims to introduce minimum uniform rules on trade secrets across the EU. The Directive defines trade secret as information which is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret. The Directive also allows employees to disclose trade secrets in order to reveal "misconduct, wrongdoing or illegal activity" without having to show, unlike under current UK employment law, that he or she was acting in the public interest.

4.4 **Does your company use electronic signatures?** The EU "Regulation on electronic identification and trust services for electronic transactions in the internal market" ("e-IDAS Regulation") comes into force on July 1st 2016 and replaces the Directive on Electronic Signatures (1999/93/EC). The e-iDAS Regulation will harmonise different national rules on electronic signatures to increase legal certainty and trust. So if you do use electronic signatures you should be aware that changes will be made across three key areas of law governing online authentication:

4.4.1 **Trust services:** the e-IDAS harmonises the rules on providers of electronic services and introduces the concept of 'qualified' trust service providers.

4.4.2 **Electronic identification (e-ID) schemes:** the concept of mutual recognition is intended to facilitate more efficient interaction with public service providers.

4.4.3 **Electronic signatures:** a qualified electronic signature based on a qualified certificate issued in one member state will automatically benefit from mutual recognition in all other member states.

You should therefore review your current practices and procedures on e-signatures to check how they can benefit from the developments introduced and to see if you need to carry out any compliance activity.

5 Case Law Update

5.1 **How "standard" are your standard terms contracts?** In a recent High Court case the judge has made it clear that where commercial parties, represented by solicitors, have negotiated a contract based on a "neutral" industry model form, it will be difficult to argue that the resulting contract is made on the written standard terms of one of those parties. This is important because if it is not a standard terms contract then section 3 of UCTA would not apply. Under section 3 of UCTA a court can strike out clauses it considers unreasonable. So if you use any third party "neutral" industry model form which ends up being negotiated, as your standard terms contracts with any of your customers or suppliers, be aware that section 3 of UCTA cannot be relied upon subsequently to strike out any of the clauses as being unreasonable. The judgment was handed down in the case of *African Export-Import Bank v Shebah Exploration & Production Company Ltd [2016]*. In that case the court considered whether a loan agreement, based on the Loan Market Association's model form, should be treated as the lender's standard terms. The High Court found no evidence that the lenders routinely put forward industry standard terms, or that they refused to negotiate them and that as a matter of fact in this case they had been negotiated and were therefore not to be regarded as standard terms. Each case will turn on its own facts.

6 Consultations

6.1 **Unambiguous consent to process cookies?** As part of the DSM the European Commission has launched a consultation on the ePrivacy Directive, which needs to be amended before the GDPR comes into force. The consultation closes on July 6th 2016: https://ec.europa.eu/eusurvey/runner/EPRIVACYReview2016. The ePrivacy Directive sets out the rules for processing consents on cookies and for using online marketing communications. There is a danger it may be amended to introduce the unambiguous standard of consent required under the GDPR in relation to cookies. This consultation offers industry the chance to let the European Commission know how difficult if not impossible this would be in practice.

6.2 **The Telcos want to talk about codes of conduct for software publishers. What would you like to tell them?** The INTUG (International Telecommunications Users Group) has launched a Proposal for a Software Publishers' Code of Conduct. INTUG has now sent the proposal to many software companies in aid of supporting a constructive engagement with the software industry. These companies include: SAP, Oracle, Microsoft and IBM. More details can be found here: http://intug.org/2016/04/intugs-proposal-for-a-software-publishers-code-of-conduct-is-ready-for-discussion-with-software-publishers/

7 Monthly Book Recommendation

7.1 "Big Data, does size matter?" by Timandra Harkness. She starts with the basics – "what is data? And what makes it big?" She then outlines how big data is already being used today from the Internet of Things to smart cities via self-quantification and asks what else could it be used for? And is big data too big or not big enough yet? See more at: http://www.bloomsbury.com/uk/big-data-9781472920065/#sthash.oeV58ixZ.dpuf.