e-commercelaw&policy

THE JOURNAL FOR THE ONLINE BUSINESS INDUSTRY
NOVEMBER 2013 VOLUME 15 ISSUE 11
WWW.E-COMLAW.COM

FPS Economy launches suit against ISP levy

Belgium's Federal Public Service Economy (FPS Economy) regulator announced on 30 October that it will sue Sabam, the Belgian association of authors and publishers, unless Sabam ends its own legal bid, begun in May, which would require three Belgian ISPs to pay a levy for providing access to copyrighted works online.

"The FPS' position is that there is a legal framework to protect copyright online and that we should enforce it to the fullest extent," said Hakim Haouideg, Partner at Field Fisher Waterhouse.

FPS Economy has accused Sabam of violating the E-Commerce Directive, in particular Article 12, which provides exemption of liability for copyright infringement for ISPs under set conditions. "In Sabam's reasoning, providing internet access to someone is the same as providing him/her with a satellite TV subscription. There is a fundamental difference: ISPs are not making any communication to the public," explains Haouideg.

Provided it wins its suit against Sabam, FPS Economy will charge Sabam €100,000 for each day that Sabam continued its own action against the ISPs.

IN THIS ISSUE

EU data protection revisions not in tune with e-commerce

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs voted to adopt a revised Compromise Text for the proposed General Data Protection Regulation on 21 October, which includes proposals to allow transfers of data outside the EU if both organisations hold a valid European Data Protection Seal.

"One of the changes proposed most likely to be welcomed by users and providers of cloud services is the proposal to allow transfers of data from EU controllers to recipients outside the EU if both organisations hold a valid European Data Protection Seal," said Nick Mathys, Senior Associate at White & Black Legal LLP, "this could prove to be a pragmatic solution for users and providers of cloud services who have the resources to devote to obtaining certification."

Organisations with a Seal, valid for a maximum of five years, would benefit from being able to provide a lawful basis for transfers outside the EU, where both the EU controller and the recipient outside the EU have valid Seals. "The provisions on the Seal and the rules on standardised information policies were both surprising, as they were suddenly included without earlier discussion," said Dr Jörg Hladjk, Counsel at Hunton & Williams.

"The Compromise Text introduces a number of interesting elements but it is still not very well tailored to the e-commerce and digital world," said Rocco Panetta, Partner at Panetta & Associati Studio Legale. "In seeking to protect citizens from the perceived ills of online behavioural analysis or ill considered uploads on social platforms, the balance has swung too far to protectionism, when in many instances rather than causing detriment, the processing creates benefits for the citizen," adds Paula Barrett, Partner at Eversheds.

The EP will now negotiate with Member States. If no agreement is reached before Parliamentary elections in May 2014, the full EP will vote on the Regulation. "The key point in terms of the negotiations to come is that there is seemingly a big difference between the position of the EC/EP, which favour much heavier regulation, and the Council of the EU, which is comparatively pro-business. It is unclear how much ground the Council will be able to claw back to reflect the more business-friendly approach," adds Mathys. "If it can't and the final text stays close to that adopted by the EP on 21 October then compliance costs are likely to significantly increase for many online businesses."

Illinois Supreme Court throws out 'click-through' tax statute

Illinois' Supreme Court affirmed on 18 October that Illinois' Main Street Fairness Act 2011 - a 'click-through' nexus statute requiring out-of-state internet sellers to collect sales tax if they commission to Illinois affiliates who link to the retailer's website - is preempted by the federal Internet Tax Freedom Act (ITFA) and is therefore unenforceable.

"The ITFA prohibits the imposition of a tax targeted at internet commerce," said Jeffrey Reed, Associate at Mayer Brown. "Since the Illinois statute on its terms applies only to the online retailer/weblink fact pattern, it violates the federal statute."

The Court did not comment on whether the Illinois statute violated the Commerce Clause of the US Constitution. "The ITFA is a temporary moratorium," said Sylvia Dion, Founder at PrietoDion Consulting Partners LLC. "Once it is lifted, Illinois' 'click-through' nexus provision will again be valid and the same Commerce Clause challenge will present itself."

The ruling contrasts with a 28 March decision by the New York Court of Appeals, which found that a near identical state tax law does not violate the Commerce Clause. "Although the decisions are in conflict, they are based on different principles," explains Dion. "Meaning for US retailers, there is a lack of guidance to rely on."

"Amazon has asked the US Supreme Court to review the New York case," adds Reed. "But the Court has not shown much interest of late in addressing state tax nexus cases."

e-commercelaw&policy

THE JOURNAL FOR THE ONLINE BUSINESS INDUSTRY
VOLUME 15 ISSUE 11 NOVEMBER 2013
WWW.E-COMLAW.COM

Editorial: Building trust in the Cloud

The European Commission set up an expert group for the creation of a set of cloud computing contract terms in October, a key action in its strategy for unleashing the potential of the cloud in the EU.

Tasked with assisting the Commission in identifying 'safe and fair contract terms and conditions for cloud computing services for consumers and small firms,' the development of an expert group, comprised of individuals and organisations of cloud service providers, customers and legal practitioners, responds directly to stakeholder concerns surrounding cloud computing contracts and aims to ensure that the inclusion of fair contract terms becomes best practice and serves to significantly improve confidence in cloud services.

The intention to create an expert group was announced by the Commission in September 2012 as part of its Communication on 'Unleashing the Potential of Cloud Computing in Europe,' which identified problems with cloud contracts as a key area in which action should be taken.

The Commission specifically stated that 'Problems with contracts were related to worries over data access and portability, change control and ownership of the data. For example there are concerns over how liability for service failures such as downtime or loss of data will be compensated, user rights in relation to system upgrades decided unilaterally by the provider, ownership of data created in cloud applications or how disputes will be resolved.'

Amongst its tasks, the expert group will have to consider how the development of new cloud contract terms will interact with the proposed Common European Sales Law (CESL), which is currently being developed.

The expert group's work will now begin: it is expected that a policy paper will be released in Spring 2014 that will include suggestions on model contracting clauses for cloud services.

In other attempts in the drive to increase trust in European cloud computing, the Commission announced the launch of Cloud-for-Europe (C4E) on 14 November, an initative which forms part of the European Cloud Partnership. C4E is driven by public sector organisations from European countries and it is hoped will help build trust in European cloud computing, by defining public-sector requirements and use-cases for cloud computing through direct involvement with the IT and telecoms industry to boost the uptake of the cloud in the public sector.

CECILE PARK PUBLISHING
Managing Editor Lindsey Greig
lindsey.greig@e-comlaw.com
Editor Sophie Cameron
sophie.cameron@e-comlaw.com
Associate Editor Simon Fuller
simon.fuller@e-comlaw.com
Subscriptions Adelaide Pearce
adelaide.pearce@e-comlaw.com
telephone +44 (0)20 7012 1387
Design MadeInEarnest
www.madeinearnest.com

E-Commerce Law & Policy
is published monthly by
Cecile Park Publishing Limited
17 The Timber Yard, Drysdale Street,
London N1 6ND
telephone +44 (0)20 7012 1380
facsimile +44 (0)20 7729 6093
www.e-comlaw.com

Spotify playlists and the battle for compilation infringement

On 2 September dance music label Ministry of Sound ('MOS') launched proceedings against the music streaming service Spotify, asking the UK High Court for an injunction in order to force Spotify to remove playlists made by Spotify users that exactly match the content and sequencing of MoS' dance music compilation albums. MOS' complaint is that these user playlists infringe on MOS' copyright in its track listings. Vanessa Barnett and Victoria Holvik, of Charles Russell, discuss MOS' action and the challenges that lie ahead for MOS in attempting to prove that track listings of compilation albums are in themselves deserving of copyright protection.

The battle for music and film (and the associated revenue) has long been bitter, emotional and polarising. When entertainment turned digital the established industry took it to a whole other level. Napster, Pirate Bay, Kim Dotcom: these are all milestones along the way.

For the past ten years or so, the skirmishes have really been in three areas: rightsholders enforcing their rights, infringers infringing them and consumers (often) stuck in the middle. The narrative developed that if consumers could access legal digital entertainment products with the same ease as file sharing, then things would change. To a certain extent, they have: legal downloads and subscription services are now commonplace. Most of these subscription services also have a social element, allowing sharing, connecting, experiencing. In particular, with reference to Spotify, the service allows playlists to be shared. And so the next battle begins...

Last month Ministry of Sound ('MOS') filed a claim with the High Court against Spotify. It is reported that the claim alleges that Spotify has infringed MOS' copyright in the track listings of its dance music compilation albums. Essentially, Spotify users have publicly posted playlists on the Spotify platform that reproduce track listings of MOS albums, both in respect of the tracks featured and their order. A number of these playlists were also named using the name of the relevant MOS album.

Further, it is reported that users of the Spotify service could use these playlists to listen to the same tracks featured on the MOS albums in the same order but without having to purchase the MOS album. As MOS does not own copyright in the tracks themselves, it is unlikely that any copyright licence fees are paid to MOS as a result of this use (although it is assumed that licence fees would still be payable to the artists, performers, recording companies, composers, lyricists, publishers etc. who own the copyright in these tracks).

MOS reportedly sent several notices to Spotify asking it to remove the playlists but to no avail. Had Spotify done so, it may have been able to take advantage of the hosting defence which is available to internet service providers if their platform or service is being used by others to infringe copyright. In order to use this defence however the provider must show that it has taken reasonable steps to stop the infringement when put on notice of it. In this case, it appears that Spotify did not take action at all.

If and when this case is eventually argued before the Court, the first hurdle that MOS will need to overcome is to establish that the track listings of its compilation albums are in and of themselves literary works deserving of copyright protection. Compilations may currently be protected under UK copyright law as literary works in one of two ways - either as a database or as a compilation other than a database - provided in each case that the compilation is sufficiently 'original.'

Databases are legally defined as being a collection of independent works, data or other materials which are arranged in a systematic or methodical way, and are individually accessible by electronic or other means. Unfortunately, there has not been any case law to date to offer practical guidance on when a compilation should be considered as other than a database.

The MOS albums do appear to be collections of independent works (being either the musical tracks themselves or simply the titles to those tracks appearing in the track listing) and one would assume these works are arranged in a systematic or methodical way, for example to ensure that the beat of an earlier track blends seamlessly with the next. The works are also individually accessible by electronic means through various media (CDs, MP3 downloads, etc. using the track listing as an index).

There could potentially be an argument that the works are not independent of each other if the tracks included on the MOS albums were mixed so that the music is continuous and each track leads into the next (possibly by creating a derivative work of one or both of the original tracks), but if that was the case, it seems more likely that MOS would claim for infringement of these derivative works rather than simply the track listings.

On the assumption that the track listings do qualify as databases in accordance with the definition set

out above, the next hurdle facing MOS is in the EU Database Directive 1996, which was intended to harmonise the legal protection of databases throughout the EU. Recital 19 to this Directive sets out that 'as a rule' the compilation of several recordings of musical performances on a CD does not meet the conditions for copyright protection although there is no explanation in the recital of why this is. Presumably, the EU legislators felt that in the main, the selection and arrangement used in compiling these CDs was banal and not sufficiently creative to be an intellectual creation of its author. Whilst the recitals to the Directive do not have legal force in the same way that the enacting provisions in the Directive do, recitals are persuasive and are intended to be used to aid with the interpretation of the Directive and the understanding of the reasons behind the enacting provisions.

The burden will be on MOS to show why its compilations are the exception to the rule laid out in recital 19 and are works deserving of copyright protection. It is worth noting that historically the level of originality that needed to be shown in order for a compilation to attract copyright protection was not that high - many different types of compilations have been deemed worthy of copyright protection (including trade brochures, lists of stock prices, an electronic circuit diagram etc).

Indeed, in Ray v. Classic FM, a case relating to the ownership of copyright in a catalogue of over 50,000 classical music tracks (amongst other works), the Court stated in its judgment that there could be no doubt that copyright existed in all the works, including the catalogue.

However, the catalogue in that case and the track listings that are presently being considered are rather different. First, the catalogue was far larger than MOS' track listings and took several years to produce. Second, the catalogue was created to assist Classic FM in building a database and contained much more information than simply the names of the different tracks. The MOS albums on the other hand, whilst much shorter, are intended to have a pleasurable aural effect by the very fact of the selection and arrangement used in creating the track listing, which arguably should speak to more creativity, not less.

Proving sufficient originality is the key for MOS and a number of judgments have been handed down by both UK Courts and the Court of Justice of the European Union on how to interpret the 'author's own intellectual creation' originality test.

Finally, Ray v. Classic FM may not be that helpful because it makes no mention of the Database Directive, the test of whether a work qualifies as a database (or a compilation other than a database) or whether the work is sufficiently 'original'. This may be because the case was decided only two months after regulations implementing the Directive into UK law came into force and the Courts were yet to take on board the scope of these regulations. Its utility as a precedent therefore may be limited for MOS in its current claim.

Proving sufficient originality is the key for MOS and a number of judgments have been handed down by both UK Courts and the Court of Justice of the European Union (CJEU) on how to interpret the 'author's own intellectual creation' originality test. It is worth noting however that these judgments have dealt with different types of works other than databases, including computer programs, photographs and titles and extracts from articles.

To apply the cases decided thus far, the track listing must in its 'choice, sequence and combination' demonstrate originality (Infopaq International A/S v. Danke Dagblades Forening). The choices must have been made 'freely and creatively' by the author, thus stamping the track listing with his/her 'personal touch' (Painer v. Standard Verlags GmbH) and the choices must not be 'dictated by technical considerations, rules or constraints which leave no room for creative freedom' (Bezpecnostni Softwarova Asociace - Svaz Softwarove Ochrany v. Ministerstvo Kultury).

Clearly, whether or not MOS will succeed in arguing that the track listings for its compilations are sufficiently original to deserve copyright protection will be decided by the evidence given at trial. How in practice the individual tracks are selected and then arranged for a particular album by an author, how free and creative these choices were and how this illustrates the author's judgment, taste and discretion, will be crucial in establishing whether these track listings are indeed its author's own intellectual creations.

It will be very interesting to keep an eye on this case if it does go to trial, especially as the Courts may decide to make a reference to the CJEU for further guidance on the level of originality required for a musical compilation to be deemed worthy of copyright protection (despite recital 19 of the Database Directive). In addition, it is likely that MOS will be motivated to appeal any decision not in its favour as any decision by the Courts that these track listings do not attract copyright could have far reaching effects for MOS' business model, not to mention the music industry as a whole. Both parties involved are keeping their cards very close to their chest - and more will be revealed when we can access the Particulars of Claim.

Vanessa Barnett Partner
Victoria Holvik Associate
Charles Russell
Vanessa.Barnett@charlesrussell.co.uk
Victoria.Holvik@charlesrussell.co.uk

The draft EU data protection package and online business

After treading a rocky road to reach this point, the Civil Liberties, Justice and Home Affairs Committee of the European Committee adopted its own proposed draft of a new Data Protection Regulation on 21 October. The new draft aims to modernise the law around data protection throughout the EU and will, if implemented, have substantial consequences for online business. Samantha Sayers and Phil Lee of Field Fisher Waterhouse analyse the key features of the Compromise Text agreed on by the Committee and its potential effects on e-commerce.

On 21 October 2013, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) voted in favour of adopting a European Data Protection Regulation (Regulation) and proposed its own draft reflecting the different views of the Parliament's political groups (Compromise Text). This is a significant development, as the draft will ultimately replace the now seriously out-dated 1995 Data Protection Directive and directly implement throughout the whole of the European Union (EU) much-needed modern measures to govern data protection.

The road to this point has not been easy and further challenges lie ahead if the draft is to be finalised before the May 2014 European Parliament elections. After overcoming the already troublesome path to reach this milestone, the text will now be subject to potentially difficult negotiations between the European Commission and the Council of the EU before being finalised. The EU bodies will be faced with the difficult task of reviewing a draft which has already been subject to significant amendments since the Commission's original January 2012 draft, as it also incorporates the very different proposals contained in the Council's May 2013 draft. Elements of both proposals would fundamentally have very different impacts on e-commerce businesses, depending on which position is finally reached.

In addition to the potentially difficult negotiations that lie ahead, numerous Member States, particularly the United Kingdom and Sweden, have publicly criticised the latest proposal. The UK in particular is pushing for a 2015 deadline, sparking fresh fears that the Commission would effectively be sent back to the drawing board. However, EU national leaders have firmly stated that: 'The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015.' Therefore, if all goes as planned, businesses would be expected to comply with the new regime as early as 2016 or 2017 following the two year grace period.

Key features of the Compromise Text

The latest Compromise Text has retained many of the provisions originally proposed by the Commission in 2012 and seems to have taken into account some (although not all) of the concerns raised by global businesses since then. On the whole, the latest amendments strictly regulate businesses' use of personal data and include increased penalties for non-compliance. Although the Compromise Text is not yet finalised and could change again, as currently drafted some proposals significantly affecting businesses include:

1. Territorial scope

The amendments to Article 3 of the Regulation mean that the law will apply to businesses outside of the EU so long as they are processing personal data related to individuals established within the EU. This includes businesses processing personal data in order to offer services to data subjects in the EU or where the data subjects are being monitored. Ultimately, this means that most website operators anywhere in the world could be captured and be directly subject to EU law. In reality, it is difficult to see how EU authorities will effectively monitor and enforce the Regulation against non-EU businesses. (Article 3)

2. Increased fines

Another significant impact on businesses is the potential introduction of massive fines and sanctions. Those businesses that do not comply with the Regulation could be subject to fines of up to €100million or, if larger, 5% of annual worldwide turnover. This is a significant increase from the original 2% proposed. LIBE has also introduced written warnings for first offences and regular data protection audits, as an alternative to the standard financial sanctions previously proposed. (Article 79)

3. Increased threshold for appointment of Data Protection Officers (DPO)

The Compromise Text also introduces a requirement for all businesses processing personal data relating to 5,000 or more data subjects in any consecutive 12 month period to appoint a DPO. The Text also introduces a two or four year minimum term for the DPO, depending on whether it is an employee or contractor

relationship. The DPO must also meet the following minimum criteria in order to be appointed: (i) have professional qualities, and (ii) have expert knowledge of data protection law and practices in order to meet the detailed requirements of the Text. (Article 35)

4. Distorted scope of international data transfers

The criteria for assessing adequacy has been amended, blurring the lines of what is acceptable in relation to data transfers to non-EU countries. However, there may be a glimpse of hope for businesses as those that frequently transfer personal data from EU to third countries may be able to transfer data more freely if both the EU-based data controller and the non-EU recipient have been granted a valid European Data Protection Seal. (Article 41)

5. 'One stop shop' versus 'lead authority'

The 'one stop shop' mechanism has been replaced by the concept of a 'lead authority,' which will be responsible for consulting with the other competent authorities, taking their opinions into account and working towards an agreed position. This is unlikely to meet the wishes of global businesses but should go someway towards streamlining the compliance process and increasing efficiency. (Article 54)

6. European Data Protection Seal (certification by authority or third party)

The Compromise Text has been redrafted to encourage businesses to certify their data processing with a supervisory authority by allowing businesses to request the supervisory authority to audit their processing. When granted, the certification would be valid for up to five years and recorded on a public register. The primary benefit of this proposal is that it potentially provides businesses with lawful grounds for international transfers. (Article 39)

The 'lead authority' concept is unlikely to meet the wishes of global businesses but should go someway towards streamlining the compliance process and increasing efficiency.

7. Data breaches to be reported 'without undue delay'

The proposal now requires notification 'without undue delay' as opposed to 'within 24 hours' where there has been a data breach. There is also an obligation on supervisory authorities to maintain a public register of the types of breach notified. This will place greater emphasis on the compliance function of most businesses to ensure internal policies and procedures are implemented and maintained in order to respond quickly to a data breach. (Article 31)

8. Consent must be freely given

The Compromise Text provides that consent must be freely given and shall be obtained for a specific purpose. When the previous draft was being debated, businesses had raised concerns regarding the obligation to obtain 'explicit' consent as it was felt that this may not be achievable in many cases. This concept has been retained by the Compromise Text, so unless this is removed in the final stages, businesses and websites that currently rely on implied consent will face an insurmountable challenge. (Article 7)

9. Icon based privacy notices

A new concept in the Compromise Text is the requirement for information to be provided to individuals in two ways: (i) in a yes/no icon based table; and (ii) in a detailed notice. As a result, it is highly likely that businesses will need to update all of their existing transparency mechanisms in order to meet this additional obligation, incurring unavoidable external costs. (Article 13)

10. Privacy impact assessments (PIAs)

Businesses will also need to complete PIAs at least annually and in certain situations the data protection officer or supervisory authority will need to be consulted. This is another example of increased administration and costs for businesses as a result of the proposals. (Article 32)

Although the latest draft of the EU Data Protection Regulation has many benefits for businesses, it also presents numerous challenges. The next few months will be crucial to determine whether the new data protection regime ends up being fit for purpose or a regulatory nightmare.

Samantha Sayers Member of the Privacy & Information Law Group
Phil Lee Partner
Field Fisher Waterhouse LLP
Samantha.Sayers@ffw.com
Phil.Lee@ffw.com

Recent amendments made to Serbia's e-commerce law

Amendments to the Law enter into force

Serbia's Law on e-commerce ('the Law') (Official gazette RS 41/2009) was enacted in June 2009 and is based on the EU Directive on e-commerce (2000/31/EC). It has been applicable since 10 June 2009 and marked the first time that the internet based economy has been regulated in Serbia and service providers have been held accountable; consumers are now better protected. Before we look at some of the recently implemented amendments to the Law let's see what the current framework holds.

The first section of the Law sets the groundwork in terms of the Law's applicability and exceptions (not applicable in areas such as games of chance) and defines the main terms used throughout the text. For example, an information society service in this context is defined as a service which is provided remotely at the service user's personal request for a fee via electronic equipment for processing and storing of data and specifically sale of goods and services via the internet, offering of data and advertising via the internet, electronic search as well as enabling search of data and services transmitted via an electronic network, enabling of network access or storage of service users' data. Also, a service provider is a legal entity or entrepreneur which provides information society services. Finally, an electronic contract is defined as a contract which the legal or natural persons conclude, send, receive, terminate, cancel, adhere to and display electronically using electronic means. It should be noted that the provision of services is not regulated i.e. permits are not required except that a service provider must be a registered company.

The following section sets the specific requirements that apply to e-commerce and other service providers in relation to the right of a consumer to be sufficiently informed about the provider's business. This includes the obligation of the provider to present prices and charges clearly and unequivocally. Also, a so-called 'commercial message' is defined and its proper usage specified, including restrictions applicable to unsolicited advertising (prior consent is required/opt-in model). The third section of the Law defines the meaning of a contract in electronic form i.e. an electronic contract. The validity of an e-contract, including electronic offer and acceptance, shall not be disputed because of its electronic form alone. Exceptional situations in which e-contracts are not legally valid are specifically defined e.g. transfer of ownership in real estate. If a signature is required for an e-contract to be valid, an electronic message signed with a qualified electronic signature shall suffice.

Further, the third section sets out obligations of e-commerce service providers in relation to consumer protection issues such as the obligation to inform the consumer about the nature of the transaction and steps required to conclude the contract, the contents of the contract and the applicable terms and conditions etc. prior to entering the contractual relationship. Finally, providers are required to enable consumers to access the text of the contract, reproduce, re-use and locally store the same. The rule on when an e-contract is concluded is based on the Law on obligations and its 'reception theory.' An e-contract is concluded at the time the offeror receives an electronic message containing the offeree's statement of acceptance. Such acceptance is deemed received only if the offeror can access the message containing it.

The fourth section of the Law sets out the liabilities of service providers towards consumers and state regulators. This includes limitation of service provider's liability for the content of messages transmitted through its networks if specific requirements are met (a mere conduit theory, take down procedure etc.), for temporary and permanent storage of such content and for linking to other service providers' content. In the fifth section of the Law the supervision and inspection procedures are defined. Finally, the sixth section sets out the penalties of up to 1,000,000 RSD (currently cca. 10,000 EUR) applicable to service providers in breach of the Law (up to 50,000 RSD for the responsible person of the legal person) as well as the penalty of suspension of all commercial activities for up to six months in the case of repeated or significant breaches.

Amendments to the Law entered into force on 8 November 2013 and are centred on further harmonisation of the Law with the EU framework. The main points to note are the widening of the applicability of the Law to foreign service providers that are not based in Serbia but target Serbian consumers as well as the significant increase in the upper limits of penalties from 1,000,000 RSD to 1,500,000 RSD applicable to service providers in breach of the Law and from 50,000 RSD to 150,000 RSD for the responsible person of the legal person. Finally, at a justified request from a third party a court can now order a temporary measure against a service provider such as the removal of disputed content.

Alex Petrovic Partner
Joksovic, Stojanovic & Partners Law Office
alex@jsplaw.co.rs

The Hotham case: analysing the scope of the DMCA

Can the Digital Millenium Copyright Act ('DMCA') be used to remove content that may not infringe copyright interests, but that the 'copyright owner' disapproves of? What options are available to an internet service provider that receives such a takedown request? A recent incident involving a blogger, the organisation 'Straight Pride UK' and online service provider WordPress brings these questions to the forefront as Kathy Ossian of Ossian Law PC explains.

A key purpose of the DMCA[1] is to provide copyright owners with a way to seek removal of infringing content from a website. At the same time, the Act affords the site's service provider immunity from vicarious infringement through safe harbor provisions. To avail itself of the DMCA's safe harbor provisions, a service provider that receives a takedown request conforming with the statutory requirements must act 'expeditiously to remove, or disable access to' the content[2].

Most online service providers also give the poster of the content notice of the request and an opportunity to provide a counter-notice showing that the content does not infringe[3]. The DMCA specifically prohibits any material misrepresentation that online content is infringing (or has been improperly removed) and provides civil remedies for damages and attorney fees incurred by the alleged infringer, copyright owner and/or service provider injured as a result of such a misrepresentation[4].

As a practical matter, a takedown request culminating in the removal of content espousing a contrary view from the person or entity seeking its removal may also garner considerable publicity in the form of the re-posting of the content on other sites.

The Hotham-Straight Pride controversy

This summer, Oliver Hotham, whose blog[5] is hosted by WordPress[6], learned of Straight Pride UK, an organisation apparently advocating for 'straight equality.'[7] Hotham sent Straight Pride a letter identifying himself as 'a freelance journalist' and asking questions about the organisation[8].

Straight Pride responded by emailing Hotham a document entitled 'Press Release.' Hotham made some organisational and grammatical changes to the answers. He also noted that the organisation failed to answer two of his questions - one on the bullying of LGBTI and the other relating to other 'pride' movements. Hotham sent Straight Pride an email offering a second opportunity to respond and stating that if they didn't do so, he would 'make it clear in the article' that they were avoiding the questions. Hotham waited two days and, having received no response, published his blog article about the organisation called 'Oliver Hotham, - It's Great When You're Straight...Yeah,' including his edited versions of the answers to the remaining questions.

Soon after the publication of the article, Straight Pride's Press Officer, Nick Steiner, emailed Hotham; Steiner told Hotham that he did not have consent to publish the answers. Steiner requested that Hotham take down the article within seven days or Straight Pride would send a DMCA takedown request to WordPress to have it removed. Hotham did not remove the article, so Straight Pride sent the blogging site's US based operator, WordPress, a DMCA takedown request.

Article removal

True to its 'Digital Millennium Copyright Act Notice,'[9] WordPress removed the content in response to Straight Pride's takedown request that, at least on its face, satisfied the statutory requirements, including verifying the accuracy of the request under penalty of perjury[10]. WordPress also notified Hotham of his right to submit a counter-notice to WordPress if he believed the copyright infringement notice 'was submitted in error.'[11] In taking these actions, WordPress was complying with the safe harbor provisions of the DMCA and WordPress' own posted procedure for addressing DMCA takedown requests.

The next move belonged to Hotham. As he explained in his follow-up article, submitting a counter-notice would require him to consent to jurisdiction 'for any judicial district in which [WordPress] may be found' and this was not something that UK-based Hotham was willing or able to agree to[12]. Thus, WordPress did not restore the article. Nevertheless, Hotham's original article was reposted hundreds of times by others and can easily be found online through a browser search of the article name.

In a statement afterwards, WordPress General Counsel Paul Sieminski stated "[w]e think this was a case of abuse of the DMCA and we don't think that taking it down was the right result. It is censorship using the DMCA."[13] Straight Pride issued its own statement, reiterating that its communication with Hotham was not intended for publication, and that the article 'caus[ed] a great deal of illegal Harrassment and unwanted contact.'[14]

Options for online service providers

Could WordPress have handled the

Hotham/Straight Pride matter differently? Probably not - to maintain its safe harbor status under the DMCA, WordPress must afford a presumption of validity to any takedown request that, on its face, meets the statutory requirements.

The opportunity for the poster to submit a counter-notice provides the means to sort out those DMCA requests that are attempts at censorship from legitimate reports of copyright infringement. Where, as with Hotham, the poster chooses not to file a counter-notice, it is not surprising that the takedown request will prevail.

Faced with conflicting DMCA notices and counter-notices, an online service provider will likely let the parties fight directly. An example is a lawsuit between two bloggers on opposite sides of a home birthing debate[15]. Crosely-Cocoran, a midwife, posted a photo of herself on her blog in a graphic hand pose with the caption that she was giving Tuteur, a physician, 'something else to go back to her blog and obsess about.' Tuteur then copied the photo and posted it on her own blog without Crosely-Cocoran's express permission.

Crosely-Cocoran submitted a DMCA takedown request to Tuteur's web host. Tuteur filed a counter-notice. The web host notified both parties that it was up to them 'to pursue legal action.' The current lawsuit commenced whereby Tuteur alleges that Crosley-Cocoran made a material misrepresentation in her takedown request in violation of Section 523(f) of the DMCA. Crosley-Cocoran filed a motion to dismiss, which the court denied, leaving open the potential for Crosley-Cocoran to face damages under Section 512(f)[16].

Deterring manipulation of the

The opportunity for the poster to submit a counter-notice provides the means to sort out those DMCA requests that are attempts at censorship from legitimate reports of copyright infringement.

DMCA takedown process

The Hotham/Straight Pride controversy and the Tuteur/Crosely-Cocoran lawsuit illustrate how the DMCA takedown process can extend beyond copyright infringement issues. Under the safe harbor provisions of the DMCA, an online service provider has little discretion to act outside of the requirements of the Act and the provider's own posted procedures.

Perhaps the threat of court enforcement of statutory damages for a material misrepresentation in the DMCA takedown process, such as those under consideration in the Tuteur case, may serve as a deterrent to this type of behaviour. The re-posting of the content in question, as played out by Hotham's article, appears to remain an even more practical, affordable and expedient deterrent.

Kathy Ossian Founder and CEO
Ossian Law PC
kathy@ossianlaw.com

1. Pub. L. 105-304 (8 October 1998). This article focuses specifically on DMCA Title II, also known as the Online Copyright Infringement Liability Limitation Act, 17 U.S.C. 512 ('OCILLA') which offers a safe harbor to online and internet service providers against liability for copyright infringement if they follow the OCILLA's safe harbor guidelines.
2. 17 U.S.C. 512.
3. For e.g. Vimeo.com's DMCA Notifications and Counter-Notifications Process at http://vimeo.com/dmca and Twitter's Copyright and DMCA policy at http://support.twitter.com/articles/15795-copyright-and-dmca-policy
4. 'Any person who knowingly materially misrepresents under this section (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misrepresentation, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner . . . or by a service provider, who is injured by such misrepresentation . . .' 17 U.S.C. 512 (f)
5. http://oliverhotham.wordpress.com
6. WordPress's site is found at http://wordpress.com and is owned by Automattic Inc. Automattic is referred to as WordPress throughout this article.
7. When Hotham first contacted Straight Pride, the organisation had a website located at www.straightprideuk.com. The site appears to have no content as of 14 October 2013.
8. The source for the recitation of facts in this section is largely taken from Hotham's blog and the updated article 'The sordid tale of how I was censored by StraightPride UK' found at http://oliverhotham.wordpress.com/2013/08/11/the-sordid-tale-of-how-i-was-censored-by-straight-pride-uk/
9. http://automattic.com/dmca/
10. WordPress' DMCA notice states that: '[y]ou must include: A physical or electronic signature of the copyright owner or a person authorized to act on their behalf; Identification of the copyrighted work claimed to have been infringed; A description of the nature and exact location of the content that you claim to infringe your copyright, in sufficient detail to permit Automattic to find and positively identify that content. For example we require a link to the specific blog post (not just the name of the blog) that contains the content and a description of which specific portion of the blog post - an image, a link, the text, etc - your complaint refers to; Your name, address, telephone number and email address; A statement that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and A statement that the information in the notification is accurate, and under penalty of perjury, that you are either the copyright owner or a person authorized to act on their behalf.'
11. WordPress' Counter-Notice policies and form are found at http://automattic.com/dmca/dmca-counter-notice/
12. http://oliverhotham.wordpress.com/2013/08/11/the-sordid-tale-of-how-i-was-censored-by-straight-pride-uk/
13. A. Hern, 'WordPress pulls interview with anti-gay group Straight Pride UK' (13 August 2013): http://www.theguardian.com/technology/2013/aug/13/wordpress-straight-pride-uk
14. See B. Smith, 'Straight Pride UK update: official statement' (12 August 2013) found at http://ciswhitefemale.wordpress.com/2013/08/12/straight-pride-uk-update-official-statement/ where the entire Straight Pride official statement is posted.
15. Tuteur v. Crosley-Cocoran, Civil Action No. 13-10159-RGS.
16. Ibid., 'Memorandum and Order on Show Cause Response and Defendant's Motion to Dismiss' (10 September 2013): https://www.eff.org/sites/default/files/tuteur_order.pdf

Platform price parity clauses: various UK-led investigations

The Office of Fair Trading concluded in August its formal investigation into Amazon's use of platform price parity clauses; these stipulated that third-party marketplace sellers would not be able to sell products at prices any higher than the lowest price the product was sold for by that seller on other non-physical sales channels. Diarmuid Ryan of Squire Sanders discusses the investigation and other regulatory action on pricing clauses.

On 29 August 2013, the Office of Fair Trading ('OFT') announced[1] that it was minded to close its investigation into the platform price parity clause ('PPPC') imposed on third parties selling on Amazon's Marketplace platform, in light of Amazon agreeing to unilaterally end its price parity policy in the EU.

It has been clear for some time that 'most favoured nation' pricing clauses ('MFNs') can fall foul of the prohibition of anticompetitive agreements in Article 101 TFEU[2]; see the 2004 Hollywood studios case[3]. Only recently has scrutiny of MFNs become a regular feature of regulatory enforcement activity, particularly in the UK, and the reasons for concern have begun to be systematically set out, although there remains uncertainty.

The Amazon case

Since May 2010, third party sellers trading on the Amazon.co.uk Marketplace platform were required to agree to a PPPC guaranteeing that product prices offered by the sellers on the Marketplace should not be higher than the lowest price offered by the seller for the same product on any other non-physical sales channel, whether the seller's own website or on other online sales platforms.

Following numerous complaints by sellers, in October 2012 the OFT opened a formal investigation of Amazon's PPPC under Article 101 TFEU. The German Federal Cartel Office ('FCO') has also been investigating in parallel and in close cooperation with the OFT. The OFT's announcement identifies concerns with Amazon's PPPC, namely that the PPPC's effect may be to: (i) raise online platform fees; (ii) curtail the entry of potential entrants; and (iii) directly affect the prices which sellers set on platforms (including their own websites), resulting in higher prices for consumers.

Amazon then informed the OFT and the FCO of its plans to unilaterally withdraw its Marketplace PPPC in the EU (but not elsewhere) from 30 August 2013. The FCO's 27 August 2013 announcement states that the FCO is 'currently assessing whether the measures will be sufficient in their form, content and scope for the proceedings against the company to be terminated. One precondition for this is that the company gives up its price parity clause for good and there is no risk of any repeat action.'

PMI market investigation

On 5 July 2013, the Competition Commission ('CC') published an annotated issues statement[4], summarising its thinking on the issues raised by its ongoing market investigation into private motor insurance ('PMI'), including that most (91%) PMI policies sold on price comparison websites ('PCWs') are subject to a PPPC restricting the insurance provider's ability to offer the same policy for less via its own website (narrow scope MFN) or via another channel (wide scope MFN).

The CC believes that the narrow scope MFNs are likely to have few anticompetitive effects but that the wide scope MFNs might: (i) create upward pricing pressure on the 'cost per acquisition' fees charged to providers by PCWs and therefore on the levels of PMI premiums charged by providers; (ii) increase PMI levels directly; (iii) restrict entry; and (iv) lead to excessive spending on advertising. While the CC indicates that the wide scope MFNs may also give rise to some benefits, namely improving the value of a PCW search for consumers (as they know they are getting a competitive price) and by allowing PCW firms to earn a return on their investment, it states that some other devices might achieve these benefits without causing the anticompetitive effects of MFNs. However, the CC's issues statement states that it has 'not yet formed a view on the balance of the possible anticompetitive and pro-competitive effects.'

Hotel online booking

On 9 August 2013, the OFT published[5] its intention to accept binding commitments from two hotels and two online travel agents ('OTAs') to resolve the OFT's investigation into restrictions imposed on the OTAs not to discount the daily room rates set by the hotels. Under the commitments package, for the next three years, the OTAs can offer discounts (funded by their commission/margin) off hotel headline room rates to 'closed groups' of UK customers who have made one non-refundable booking. The OTAs will be able to widely publicise (including on PCWs) the general availability of closed group discounts but will only be able to disclose specific closed group rates/discounts to closed group members.

The OFT's notice refers to the fact that the hotels had also agreed

'room rate most favoured nation clauses' with the OTAs, guaranteeing the OTAs booking rates no less favourable than the lowest booking rate displayed by other online distribution outlets. Such clauses are somewhat similar to a PPPC, albeit there is a fundamental difference in that the OTAs are not just the platform on which the hotels sell their rooms but are resellers in their own right.

The OFT explicitly did not investigate the room rate MFNs and its notice states that it has made no assessment of whether MFN provisions may infringe Article 101 TFEU. However, the OFT notes that the commitments given by the hotels/OTAs include a commitment to remove/not include any provisions in current/future commercial arrangements between them 'that could undermine the new discounting freedoms provided for by the commitments. This could include amending any MFNs if necessary.' The OFT's notice goes on to state that having regard to the 'present specific legal and economic context,' the OFT is unlikely, for the duration of the commitments, to investigate any MFN clauses which do not undermine the principles underpinning the commitments.

Most obviously, this leaves open the possibility that the OFT will subsequently object to the room rate MFNs on the grounds that they reduce the level of price competition between OTAs. Further, the OFT's notice goes on to emphasise that the OFT will consider investigating MFN clauses in other industries where there are reasonable grounds for suspecting that the clauses, in their specific industry context, infringe UK/EU competition law. Therefore, the OFT's notice raises a clear flag that MFNs/PPPCs will continue to be of interest to the OFT as a potential concern under the competition rules.

The Amazon, PMI and Hotel Online Distribution cases all indicate that PPPCs are viewed with some suspicion by the UK competition authorities.

The Lear report

On 10 September 2012, the OFT published a report by Lear[6] reviewing the competition law treatment of 'price relationship agreements' ('PRAs'), i.e. agreements whereby sellers agree to link their prices to other prices charged for the same or similar products, including PPPCs (or 'across platforms parity agreements').

The Lear report identifies the fundamental interest that a platform is likely to have in ensuring that sellers price competitively, as this is key to ensuring the platform is attractive to buyers. The report identifies potential benefits/efficiencies and potential competition concerns that PPPCs may give rise to.

On the one hand, PPPCs may be seen as beneficial if they are used as a means to credibly inform buyers that all the goods/services sold on that platform are competitively priced (this benefit will only arise if the low-fee platform's PPPC is publicised and higher-fee platforms do not also impose a PPPC on sellers). They can also be justified if they prevent other platforms from free-riding on the investments of a higher quality/reputation platform. On the other hand, PPPCs may deter entry of more efficient platforms by preventing sellers from charging lower prices on new platforms, reducing the ability of new platforms to attract sellers and, in consequence, to attract buyers via lower transaction fees. PPPCs can also soften transaction fee competition between platforms by lowering the incentive of rival platforms to reduce fees. The PPPC prevents the seller from charging a higher price on the higher-fee platform, so the seller will have to spread the higher transaction fee across the prices charged on both platforms, depriving the lower-fee platform of the price advantage it would otherwise enjoy from charging a lower fee and so reducing its incentives to charge a lower fee in the first place. Finally, PPPCs can facilitate collusion both between platforms and between sellers, by improving the ability of platforms and sellers to monitor rivals' pricing and to enforce collusive outcomes.

Conclusion

The Amazon, PMI and Hotel Online Distribution cases all indicate that PPPCs are viewed with some suspicion by the UK competition authorities, albeit they are not treated as 'by object' (i.e. automatic) infringements of the Article 101(1) prohibition and there is a recognition (consistent with the Lear report findings) that their proper assessment involves a complex and detailed balancing of possible anticompetitive and pro-competitive effects in the specific relevant economic and legal context. Unfortunately, none of these cases provide a detailed final consideration of such clauses, although the CC's PMI report should do so in due course. In the meantime, firms should approach such clauses with care.

Diarmuid Ryan Partner
Squire Sanders LLP
Diarmuid.Ryan@squiresanders.com

1. See: http://www.oft.gov.uk/news-and-updates/press/2013/60-13
2. Treaty on the Functioning of the European Union.
3. See: http://europa.eu/rapid/press-release_IP-04-1314_en.htm
4. See http://www.competition-commission.org.uk/assets/competitioncommission/docs/2012/private-motor-insurance-market-investigation/130705_annotated_issues_statement.pdf
5. See http://www.oft.gov.uk/shared_oft/ca-and-cartels/oft1500.pdf
6. Laboratorio di economia, antitrust, regolamentazione.

The Unified Patent Court and its potential for abuse by trolls

The creation of a single court in which patent disputes for the whole of Europe can be decided has caused significant concern for companies across a wide variety of industries regarding the potential for abuse of the system by so-called patent trolls. Hiroshi Sheraton, Partner at McDermott Will & Emery UK LLP, reflects on those concerns and the obstacles to the widespread adoption of the Unified Patent Court.

On 24 September 2013, a group of the world's largest and best-known companies from a variety of industries wrote an open letter[1] to the highest bodies within Europe to express concern over the proposed rules of the Unified Patent Court that could, they say, lead to 'significant opportunities for abuse' and 'an unfair litigation system being too advantageous for patent proprietors.' The threat identified by the authors, which included Adidas, Apple, Deutsch Poste, Samsung and Telecom Italia, was that of patent trolls or (using more sensitive terminology) PAEs - Patent Assertion Entities.

Two particular aspects of the UPC rules were identified as being problematic: the procedures for 'bifurcation' (i.e. hearing issues of infringement and validity separately) and the rules concerning the granting of injunctions in patent cases.

The objections regarding bifurcation were that the rules are not sufficiently clear as to when, where and how validity should be determined and that it should be made easier for defendants to obtain a stay of infringement issues until validity has been finally decided. The authors state that the rules will 'allow plaintiffs to obtain a quick infringement ruling, along with an injunction barring products from most of the European market, before any determination of whether the patent in question is actually valid.' Consequently, 'unprincipled plaintiffs would be able to extract substantial royalties (through settlements or verdicts) from European and other companies based on low-quality, and potentially invalid patents.'

With respect to the granting of injunctions, the authors point out that 'rigid application of an injunction rule could enable unprincipled litigants to "hold up" manufacturers by making unreasonable royalty demands for even a single trivial patent on a complex product. A rule that does not offer sufficient guidelines on when to grant injunctions will create strong incentives for abusive behaviors.'

However, neither bifurcation nor injunctions are new to the European patent system. Bifurcation is the norm in German patent cases and, generally speaking, if a patent holder obtains a finding of infringement, the courts will award an injunction to stop the infringement. Instead, the concerns expressed are perhaps best placed in the dual context of the US patent litigation system, where PAEs accounted for nearly 60% of patent litigation in 2012, and in the fragmented patent litigation system that prevails in Europe.

The introduction of the Unified Patent Court will change the landscape for patentees seeking to assert their rights in Europe. Current patent litigation in Europe must be conducted on a nation by nation basis, but the UPC will give a single case far greater geographic reach. Even allowing for the absence of Spain and Italy from the system, the UPC will have jurisdiction over a population of around half a billion residents. This brings its potential commercial power to a level comparable with that of US district courts.

The diversity of approaches within Europe is exemplified by the way in which the English and German courts address issues of validity. Whereas English legal sensibilities consider it desirable to hear questions of infringement and validity together, the German *landesgericht* (for infringement) and *bundespatentgericht* (for validity) have co-existed in harmony for many years dealing with different issues. The concern expressed in the letter thus appears to arise from the attempt in the UPC rules to allow flexibility in approach without clear indications of what the 'new' approach under the UPC should be rather than from the idea of permitting bifurcation *per se*.

The concerns over the ability of defendants to challenge the validity of patents held by PAEs also has parallels in the US. US patents are perceived by some as easy to obtain, particularly in the fields of software and business methods. Furthermore, juries in certain district courts have developed a reputation for being 'patent friendly.' These factors (amongst others) have undoubtedly led to the rise of the PAE stateside. It is easy to see how a bifurcated system, which has no regard at all to invalidity defences, could be seen as unfairly harming the interests of defendants by allowing 'bad' patents to be enforced aggressively. However, the question remains as to whether European Patents asserted by PAEs will be 'of low quality and potentially invalid' as suggested. The standards applied by the European Patent Office, particularly with respect to business methods and software

patents, are widely seen as more robust than those of the USPTO. Nevertheless, questionable patents could certainly create the type of injustice cited; further guidance and clarity on the circumstances in which courts should bifurcate and/or stay proceedings would undoubtedly assist in creating a satisfactory and workable litigation system.

A subtext raised by the authors' observations is the potential for forum shopping by patentees amongst local or regional divisional UPC courts which will have jurisdiction to determine infringement issues. The concern is that this may lead to the emergence of a patent-friendly, 'rocket docket' national or regional divisional court that will deal with infringement issues swiftly and robustly whilst bifurcating allegations of invalidity to a slower central division. Again, the history of PAE activities in the US may be instructive. The courts of the Eastern District of Texas have become a popular choice of forum for patent infringement cases in the US, and some fear the emergence of a similar regional division under the UPC. Further clarity in the rules for bifurcation and stays of infringement proceedings in the event of bifurcation will reduce the prospect of such a development by ensuring consistency of approach across Europe. Having a predictable and uniform approach to such issues (governed by clear rules of procedure and principle) will reduce the potential for one divisional court to become particularly attractive to PAEs.

The other concern expressed in the letter arises from the immense power wielded by the threat of effectively 'shutting down' a defendant by the awarding of an injunction. This problem has been demonstrated (and subsequently addressed) in the US patent litigation system. In January 2006, NTP, having succeeded in a patent case against RIM, threatened to obtain an injunction which would paralyse the entire US Blackberry email network. RIM settled the case before any decision on an injunction was given, for over $600 million (in contrast to a damages award for past infringement of $53 million), thus demonstrating the disruptive (and potentially extortionate) nature of a potential injunction. In May 2006, the US Supreme Court in eBay v. MercExchange changed the law to remove a presumption of an injunction being awarded particularly in cases involving PAEs. In Europe, different courts have adopted different approaches to the granting of final injunctions in patent cases. Whereas the English courts consider injunctions to be an equitable remedy which require an assessment of all the circumstances of the case, other courts apply a less nuanced approach. As with the question of bifurcation, there is no clear guidance in the rules on the approach that the judges of the new UPC should follow.

Current patent litigation in Europe must be conducted on a nation by nation basis, but the UPC will give a single case far greater geographic reach.

The Unified Patent Court itself was, and always has been, a compromise born of political ambition. The desire to create a single court in which patent disputes for the whole of Europe can be decided has necessarily involved rules of procedure which permit varying national approaches to be adopted within a common framework. However, more clarity in how the judges of the UPC should approach the crucial questions of bifurcation and injunctions can only serve to improve the transparency of the proposed system and avoid a potentially damaging period of bedding down whilst the UPC formulates its approach. The earlier this can be achieved the better.

One of the greatest obstacles to the rapid and widespread adoption of the UPC system appears to lie in the uncertainties of the UPC rules themselves. A recent survey[2] of European users of patent litigation conducted by Legal Week showed that only 3% of respondents were most concerned with potential patent troll activities under the UPC, whereas a remarkable 57% were unable to say how likely they were to use the system and over a third felt unable to express an opinion at all about it.

In conclusion, whether or not the risks of patent trolls under the Unified Patent Court identified in the letter will come to pass remains to be seen. Certainly, the authors of the letter raise potentially real issues which may need to be addressed, but which also depend on other factors such as the quality of patents granted by the EPO and internal coordination and consistency of approach amongst judges of the new system. However, the issues raised and clarifications sought will be extremely valuable in making the UPC a success.

Hiroshi Sheraton Partner
McDermott Will & Emery LLP
hsheraton@mwe.com

1. Available at https://docs.google.com/file/d/0BwxyRPFduTN2NkpoN29UVm11OWc/edit?pli=1
2. http://www.legalweek.com/digital_assets/7210/LW_25.10.13_Benchmarker.pdf

Selling digital content online: the EC's compliance 'sweep'

The European Commission has taken some radical steps to ensure compliance by online providers of digital content following a 'sweep' of 330 websites that make available digital content across the EU. The sweep analysed areas such as contract terms and availability of contact information. James Gill and Bryony Compson, of Lewis Silkin LLP, examine the background to the sweep and its findings.

In June 2012, EU national authorities, who form part of the Consumer Protection Cooperation (CPC) Network, undertook, under the guidance of the European Commission, an EU wide screening of 330 websites selling digital content (such as digital games, books, music, films and videos) in 26 EU Member States, Norway and Iceland to assess compliance with EU consumer legislation[1]. The websites were selected on the basis of two main criteria: those with the best-selling or most popular products in their country and those in respect of which authorities had received complaints.

This 'sweep' was the sixth sweep since 2007 and occurred as a result of the European Commission's commitment to implement a coherent framework for building trust in the Digital Single Market for e-commerce and online services. In particular, the Commission has made a pledge to ensure that the Electronic Commerce Directive and other EU Directives protecting online consumers are correctly applied[2].

As part of this sweep, selected websites were checked to determine whether:

- information on key characteristics of the content was obvious and not hidden in small print;
- the provider's contact details were made easily available to consumers; and
- the websites had in place fair terms and conditions.

Findings

Of the 330 websites investigated, 172 were found to be non-compliant. Each non-compliant website operator was subsequently contacted. The Commission recently revealed that so far 116 of those websites are now compliant, 49 are still subject to further proceedings, five were not actually pursued due to the fact that their infringements were minor and two websites no longer exist.

The key areas in which the websites were non-compliant included:

- unclear and unfair contract terms: many of the websites did not make clear that consumers have the right to take legal action and also denied consumers the right to compensation in cases where digital content failed to work;
- unclear information with regard to the right to withdrawal: many of the websites did not make clear to consumers that the consumer would be unable to cancel a download once it had started; and
- lack of mandatory information: many of the websites did not provide the mandatory information required in respect of the trader's identity and method of contacting them, making it very difficult for consumers to contact the provider directly to make a complaint and/or receive after-care services.

A further simultaneous study[3] carried out by the national consumer enforcement authorities revealed that limited information, and in some cases no information, was provided to consumers about geographical restrictions that might apply in respect of their use of the digital content, such information being essential to consumers who travel in the EU and who expect to be able to access and use their digital content without restriction.

This second study also revealed that games advertised as 'free' often required some sort of payment at a later stage without this being clearly explained up-front. It was also found that such practices often target children directly, luring them into the games by advertising them for 'free,' but then asking them to pay to continue to use the game or to buy advanced features (e.g. better powers for their superhero, better castles for their kingdoms or better food for their virtual pet).

What does this mean for online digital content providers in the UK?

Interestingly, out of the 11 websites reviewed in the UK, all were found to be compliant with EU consumer protection legislation. Clearly, however, this is not a reason for all online providers of digital content in the UK to rest on their laurels!

Following the results of the sweep, Mr Neven Mimica, the European Commissioner for Consumer Policy, said: "Enforcement of consumer rights is a priority for me, including in the rapidly changing digital environment. I am pleased that this sweep addressed some of the most important issues related to digital content downloads. A year ago over 50% of the websites were not compliant, which is unacceptable. This figure is now down to 20%, and further results are expected. This is great progress but I will continue to fight for improvements."[4] This is a clear message that compliance in this area will continue to be regularly

monitored.

Moreover, the draft Consumer Rights Bill, the Consumer Protection from Unfair Trading (Amendment) Regulations 2013 and the Consumer Contracts (Information, Cancellation and Additional Payments) Regulations 2013 are all expected to come into force in the UK in 2014. Online providers of digital content will then become subject to even more obligations in respect of the provision of digital content, and consumers will also acquire a right of private redress against providers who engage in misleading and/or aggressive practices. Together, these developments mean that online providers of digital content who operate in the UK need to be better prepared than ever to ensure that they can comply with all existing, and anticipated, consumer laws.

In light of the findings of the latest sweep and the expected changes to the consumer landscape[5], online providers should consider undertaking their own internal audits and making the necessary changes to their websites and related terms and conditions to ensure compliance, not least to avoid falling foul of future sweeps[6].

In particular, UK-based providers should ensure that:

- their websites clearly set out the consumer's legal rights (including the consumer's right to return and/or receive a refund/ price reduction/compensation). Consumers should also be made aware of how their actions may also affect their rights. For example, providers must inform consumers that they will lose their (currently seven working day, but soon to be 14 calendar day) right to cancel once they start to download digital content;
- all terms of sale and/or use relating to digital content are clearly set out and any onerous or unusual terms are expressly brought to the attention of the consumer (including any geographical restrictions regarding use of the digital content). Providers should also check the extent to which they seek to limit or exclude liability - where providers seek to exclude or limit their liability beyond their legal entitlement and thereby deprive consumers of the appropriate remedy, the enforceability of such clauses is likely to be subject to challenge;
- any information regarding the key characteristics, interoperability and functionality of the digital content is accurate and easily available to the consumer;
- consumers are made aware of any additional payments that may apply in the future, particularly in respect of games or apps that are marketed as 'free'; and
- the provider's identity and contact details are accurately and prominently displayed on the website.

In light of the findings of the latest sweep and the expected changes to the consumer landscape, online providers should consider undertaking their own internal audits and making the necessary changes to their websites and related terms and conditions to ensure compliance.

Those who provide digital content targeted at children will also need to bear in mind the findings and proposed principles set out in the OFT's recently published report in respect of app-based games and online games targeted at children[7]. For example:

- all information about the costs associated with a game should be provided clearly, accurately and prominently up front before the consumer begins to play, download or sign up to it, or agrees to make a purchase;
- the commercial intent of any in-game promotion of paid-for content, or promotion of any other product or service, should be clear and distinguishable from game-play;
- games should not include practices that are aggressive, or which otherwise have the potential to exploit a child's inherent inexperience, vulnerability or credulity; and
- games should not include direct exhortations to children to make a purchase or persuade others to make purchases for them.

Despite the Commission's own back-slapping announcement that improvements in consumer law compliance have been made in respect of the websites it previously swept in 2012, it seems pretty clear that online providers of digital content in the EU have their work cut out to achieve, and maintain, compliance with the myriad of existing, and anticipated, consumer laws.

James Gill Partner
Bryony Compson Associate
Lewis Silkin LLP
James.Gill@lewissilkin.com
Bryony.Compson@lewissilkin.com

1. EC Press Release: 'Better protection for EU Consumers downloading games, e-books, videos and music,' dated 14 October 2013.
2. Page 7 of Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A coherent framework for building trust in the Digital Single Market for e-commerce and online services {SEC(2011) 1640} {SEC(2011) 1641}: http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/COM2011_942_en.pdf
3. http://ec.europa.eu/consumers/enforcement/sweep/digital_content/docs/dcs_complementary_study_en.pdf
4. EC Press Release: 'Better protection for EU Consumers downloading games, e-books, videos and music,' dated 14 October 2013.
5. A summary of the anticipated changes can be found at http://www.lewissilkin.com/Knowledge/2013/September/A-new-era-for-consumer-rights.aspx
6. The Commission conducts a sweep approximately once a year.
7. OFT: Children's online games - report and consultation: http://oft.gov.uk/shared_oft/consumer-enforcement/oft1506.pdf; and Annex A: The OFT's proposed principles for online and app-based purchases http://oft.gov.uk/shared_oft/consumer-enforcement/oft1506a.pdf

HOT TOPIC: e-government

E-Commerce Law & Policy explores e-government developments in four jurisdictions.

Asia

E-government provides opportunities to improve existing services, to offer new services and to collaborate internationally. There are also opportunities for less developed countries to leapfrog into e-government environments, avoiding legacy infrastructure, which often encumbers other countries.

Filipino Government agencies launched an online engagement portal for the country's overseas citizens to engage in local developments, including investment opportunities, charitable activities and expertise and skills exchanges.

Thailand's government is planning a nationwide network of Wi-Fi hotspots, is promoting e-learning with tablet devices and has a comprehensive masterplan for ICT development.

Singapore topped global e-government rankings in 2012 and 2013. Its e-government deals with everything from immigration, taxes and communications to a real-time mobile app, which detects lightning across the island.

ASEAN Member States have agreed to adopt a haze monitoring system which compares high resolution satellite data with land use maps to help locate fires and manage pollution.

Matthew Hunter Associate
Olswang Asia LLP
matthew.hunter@olswang.com

Belgium

In August, the federal, regional and community governments concluded a cooperation agreement to harmonise their initiatives for an integrated e-government.

The use of commercial cloud computing services by government institutions have been subject to in-depth parliamentary discussions. To give governmental institutions a legally compliant framework to buy commodity services, the government has developed a G-Cloud framework.

Also, the Belgian Privacy Commission announced that it is preparing an opinion on using cloud services, in particular regarding the public sector risks.

The Brussels Region is enacting a law regulating e-communications between public authorities and citizens/companies. Without having to change existing laws, local authorities can apply functionally equivalent alternatives, taking into account cost, efficiency and security aspects. In a second stage, the relevant legal provisions will be amended. The uniqueness of this law is that local authorities receive a temporary mandate to deviate from existing legal provisions.

Geert Somers Partner
time.lex, ICT/IP and media law
geert.somers@timelex.eu

Serbia

The legal framework for e-government in Serbia has improved with the enactment of two laws, the Law on Accounting and the Law on amendments to the Law on Tax Procedure and Tax Administration.

The Law on Accounting came into force on 24 July and aims to further harmonise this area of law with EU legislation. It is now possible to sign official accounting documents with a qualified electronic signature, which will facilitate easier issuance and processing. Also, the archiving of accounting documents in electronic format has been regulated.

The Law on amendments to the Law on Tax Procedure and Tax Administration which will apply from 1 January 2014 introduces a new unified system for payment of withholding taxes whereby mandatory electronic filing will replace 35 individual filings. The savings in administrative costs are estimated at 1.5 billion RSD. Finally, mandatory electronic exchange of data between the Tax Office and other government bodies with a view of improving tax collection was introduced.

Alex Petrovic Partner
Joksovic, Stojanovic & Partners Law Office
alex@jsplaw.co.rs

US

In the last few weeks, e-government has been 'ailing' due to the failed rollout of the universal healthcare website.

www.HealthCare.gov, which launched on 1 October, implementing President Obama's seminal healthcare restructuring law, has been plagued by glitches, outages, and poor performance. 'ObamaCare' relied on the website to begin accepting American's enrolments. In fact, due to the website's issues, only six people were able to enroll for health insurance on the first day.

One North Carolina man reportedly entered his information and received eligibility letters for two individuals in another state. The site has also run slowly, rendering blank or frozen screens, making it difficult for individuals to enter their information. The Obama Administration has now brought in experts to fix the glitches and claims the site will work properly by the end of November.

While many Americans are comfortable with doing business online, the HealthCare.gov situation may erode that confidence. It goes almost without saying that private companies would easily be fined or hauled into an investigation if they exposed individuals' personal health information due to security lapses.

Michelle Cohen Member and Certified Information Privacy Professional US
Ifrah PLLC
michelle@ifrahlaw.com