e-commercelaw&policy

THE E-COMMERCE NEWSLETTER FOR ONLINE BUSINESS
MAY 2013 VOLUME 15 ISSUE 05 **WWW.E-COMLAW.COM**

Google offers concessions to antitrust probe

Google formally submitted a number of concessions to the EC made public on 25 April in an attempt to end the EC's antitrust investigation into its search practices.

"The main concern was that Google was unfairly biasing search results to list its own services above rivals," said Paul Stone, Partner at Charles Russell. Google's concessions bundle seeks to remedy this by, *inter alia*, clearly displaying the search services of competitors, and marking results so users can identify which are promoted by Google.

Google's move follows the FTC investigation, which found that Google does not illegally manipulate search results. "The US investigation couldn't find any evidence to support concerns in this area; this may have influenced the EU to accept separate labelling requirements for Google's own services, rather than requiring changes to Google's search algorithms," believes Stone.

The viability of Google's offerings will now be evaluated via a month-long market test phase. "It remains to be seen whether Google's competitors think this goes far enough to allay their concern," explains Stone.

IN THIS ISSUE

US Congress "unlikely to enact cybersecurity legislation this year"

The US House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA) on 18 April, but the bill seems likely to fail again in the Senate due to privacy concerns, with the Senate concentrating on writing a new bill aimed at strengthening US cybersecurity.

"The word on the street is that CISPA will never hit the Senate floor," said Michelle Cohen, Member at Ifrah Law. "If it does, it likely will be voted down."

CISPA is aimed at aiding the investigation of cyber threats against the US by allowing a greater level of information sharing between businesses and government agencies. In particular, businesses would be granted legal immunity under CISPA with regards to the passing of personally identifiable information, and have no obligation to anonymise the information. The bill has thus attracted opposition on privacy grounds, which may be addressed in a Senate-drafted bill.

"The House rejected amendments that would have limited the amount of personally-identifiable information being shared," explains James Shreve, Associate at BuckleySandler. "I expect the Senate bill to permit or even require that data shared regarding cyber threats be scrubbed of personal information. Some opponents of CISPA are seeking to limit the immunity granted by the bill to entities participating in threat sharing, although limiting immunity may decrease the willingness of entities to share threat information."

Presuming the Senate does not vote on CISPA and a new bill is created, privacy may not be the only issue on the agenda. "The key sticking point in Congress still seems to be whether the federal government should only encourage private-sector entities to voluntarily take certain actions or precautions, or whether the government ought to compel such entities to do so," said David Ransom, Partner at McDermott Will & Emery. "My view is that Congress is unlikely to enact cybersecurity legislation this year, because Members will not be able to bridge the voluntary-compulsory divide. The major caveat to this prediction is if the nation suffers a significant cyber attack."

"Since Senate legislation is likely to differ fundamentally from the House bill, reconciling the bills may take time making it possible that a bill will not go to the President until 2014," adds Shreve, who believes that "There is definitely room for compromise here in spite of the harsh language used by CISPA supporters and opponents."

UK's move to license 'orphan' works results in "hysteria"

The Enterprise and Regulatory Reform Act (ERR), which received Royal Assent on 25 April, provides the Secretary of State with the power to introduce licensing of copyrighted material, which has no identified owner and which currently cannot be digitised or used without permission until the term of copyright expires, the licensing of so-called 'orphan' works.

"The new licensing powers represent significant changes in the landscape of copyright licensing in the UK and a shift in favour of users of copyright works, at the potential expense of copyright owners," said Mark Owen and Adam Rendle of Taylor Wessing. "It is evidence of a general paradigm shift in UK copyright law, from being a property right which authors can use to control uses of their creativity to becoming, instead, a bargaining tool around which as wide a range of uses can be made of their works."

Although the ERR does not define the specific rules and procedures necessary for licensing orphan works, the Act does state that orphan works can only be licensed if a 'diligent search' has been made for the original author, which has been independently verified. "The secondary legislation will provide more detail about what a diligent search involves and the criteria the 'independent authorising body' will take into account when deciding whether such a search has been completed," adds Owen. "Some works, particularly digital works stripped of ownership infor-

Continues on page 02

Continues from page 01

mation, are easier to orphan than others and the requirements of a diligent search are likely to reflect that. It is likely that rights ownership registers will arise where would-be users will have to search."

Following the passing of the ERR, photographers raised concerns about the current technology and practices that strip identifying metadata from digital files, which would result in their works being treated as orphan works. In response to those concerns, the IPO released a note on how the ERR will affect photographers, clarifying the application of the ERR to photographs online and the consultation process that will precede the secondary legislation. "It is fair to say that there has been a degree of hysteria about the extent to which orphan works provisions will remove copyright protection in photographs posted online. In fact, copyright will continue to subsist in those photographs, and a third party will not be able to reproduce them without having conducted an independently verifiable diligent search to find the owner," said Andrew Tibber, Senior Associate at Burges Salmon. "The key to ensuring that copyright owners are treated fairly will be to establish clear and rigorous guidelines on how to conduct a diligent search - something which a working group of rights-holders, including the Association of Photographers, is currently helping to define."

Another measure regarding copyright contained with the ERR, which caused controversy, involves the enabling of the Business Secretary to amend exceptions to copyright through new regulations contained in a statutory instrument rather than through an Act of Parliament. "Legal commentators expressed concerns about making changes to copyright law through regulations which are not subject to the same level of debate and scrutiny as Acts of Parliament," explains Dr Myles Jelf and Tom Ohta of Bristows. "These provisions were significantly curtailed in the ERR in its final form, which effectively removed the proposed ability to amend the exceptions via secondary legislation."

"There are many crucial details about how the orphan works provisions, and other copyright changes introduced by the ERR, will work in practice," concludes Owen. "We expected these to be contained in new Statutory Instruments to be introduced by October but there are rumours that these may be delayed."

CECILE PARK PUBLISHING
Managing Editor Lindsey Greig
lindsey.greig@e-comlaw.com
Associate Editor Sophie Cameron
sophie.cameron@e-comlaw.com
Editorial Assistant Simon Fuller
simon.fuller@e-comlaw.com
Subscriptions David Guati
david.guati@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

Supreme Court's landmark ruling in the Meltwater case

Is reading material on an internet web page an act which requires authorisation from the owner of copyright in the material? This was the question before the Supreme Court in the recent NLA v. PRCA dispute (the 'Meltwater case'). The case concerned the application of the temporary copies exception in Article 5(1) of the Information Society Directive (implemented in the UK by s.28A of the Copyright, Designs and Patents Act 1988) to temporary copies which are stored in a browser cache and produced on screen when an end user views a web page. Ben Allgrove, Michael Hart and Nicole Fairhead, of Baker & McKenzie, who acted for Meltwater and the PRCA in these proceedings, discuss the legislative background to the Meltwater case and the wider impact of the landmark ruling issued by the Supreme Court.

The Supreme Court ruled that such copies are exempted from copyright infringement by the temporary copies exception, and therefore do not require authorisation from the copyright owner. However, the Supreme Court has referred this point to the Court of Justice of the European Union ('CJEU') for a preliminary reference before making its final order on the appeal, highlighting that it is an issue with a transnational dimension which has "important implications for many millions of people across the EU making use of what has become a basic facility." The final decision in the case will therefore turn upon whether the CJEU agrees with the Supreme Court's clear view that the appeal should be allowed.

Facts of the case

Meltwater News is an online media monitoring service which monitors the online press for its customers ('end users') by reference to pre-set search terms. The monitoring is effected by internet search technology which scrapes and indexes publisher websites and then provides a list of results in a search report which includes the full headline of each article, the opening words of each article, and text either side of each appearance of the search term. The search reports are both sent by email to Meltwater's end-users and made available on Meltwater's website. Importantly, Meltwater's service only does this for sites which are not behind a paywall (unless it has a deal in place with a publisher whose site is behind a paywall).

Meltwater and the Public Relations Consultants Association ('PRCA') made a reference to the UK Copyright Tribunal challenging the reasonableness of licensing terms for online media monitoring services and their customers sought by the Newspaper Licensing Agency ('NLA'), representing major UK newspaper publishers.

In the context of this reference, the NLA claimed that, in addition to any licence held by Meltwater, end-users also required a licence due to the following three acts of copying: (1) the copy of Meltwater's alert email held on the user's computer containing search results; (2) the temporary copy of the search results in the RAM and on screen on the user's computer when the user viewed search results on Meltwater's website; and (3) the copy of the article in the RAM and on screen on the user's computer when the user clicked on a link and viewed an article on the publisher's website. The PRCA claimed in defence that (2) and (3) were temporary copies within the terms of the exception in s.28A CDPA / Art 5 (1) Information Society Directive. It was this defence that the Supreme Court considered.

Legislative background

Article 5(1) of the Information Society Directive (Directive 2001/29) provides that:

'Temporary acts of reproduction referred to in Article 2 [which provides for the reproduction right], which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:

(a) a transmission in a network between third parties by an intermediary, or

(b) a lawful use

of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.'

The Supreme Court's ruling

The Supreme Court, in a

unanimous judgment delivered by Lord Sumption, took the view that the temporary copies exception applies to the temporary copies necessarily made in a browser cache and on-screen when a web page is accessed and viewed.

This is contrary to the position taken by both Proudman J at first instance and the Court of Appeal below, that any 'consumptive use' of copyright material, including reading or viewing such material, precluded the application of the temporary copies exception and, as such, it could not apply to temporary copies created in the course of internet browsing as these are made for the very purpose of enabling their viewing by end-users.

The CJEU's rulings in both the FAPL[1] and Infopaq II[2] cases, which came after the Court of Appeal's decision, cast doubt on this approach. Applying these rulings, the Supreme Court took the view that making internet browsing an infringing activity would be "an unacceptable result making infringers out of the many millions of ordinary users of the internet across the EU who use browsers and search engines for private as well as commercial purposes."

Its reasoning on the legislative intent behind the Article 5(1) exception and its application to internet browsing was very clearly set out in the judgment and is summarised below.

Legislative intention behind the temporary copies exception

The NLA had claimed that the Article 5(1) exception only applied to copies made in the course of transmission of the material within a network, for example in the caches of intermediate routers and proxy servers. The Supreme Court found this was "an impossible contention" and that recital 33 of the Directive "expressly envisages" that the exception should "include acts which enable browsing [i.e. end user browsing] as well as acts of caching to take place."

The scope of the exception was wider than processes enabling "a transmission in a network between third parties by an intermediary," as provided for by Art 5(1)(a): it also, by virtue of Art 5(1)(b), extended to processes allowing the "lawful use" of a work, which "necessarily includes the use of the work by an end-user browsing the internet." Therefore, for the exception to be coherent, it must apply to the ordinary technical processes associated with internet browsing.

Application of Art 5(1) and the Infopaq conditions

In Infopaq I[3] the CJEU had set out the following conditions to be satisfied for acts of temporary copying to fall within the Art 5.1 exception:

(1) the act is temporary;

(2) it is transient or incidental;

(3) it is an integral and essential part of a technological process;

(4) the sole purpose of that process is to enable a transmission in a network between third parties by an intermediary or a lawful use of a work or protected subject matter; and

(5) the act has no independent economic significance.

According to the Supreme Court these are not free standing requirements, but are "overlapping and repetitive, and each of them colours the meaning of the other" and as such "have to be read together to achieve the combined purpose of all of them".

In terms of their application to the facts, the court gave the following guidance:

- Temporary, transient or incidental.

The Supreme Court took the view that the dispute turned on these first two conditions. 'Temporary' and 'transient' mean the same thing, and are intended to exclude from the exception acts which constitute permanent copying, for example downloading. Judged in the light of the normal operation of a computer or its browser, the ordinary processes of caching and browsing could be distinguished and came within the exception. It is irrelevant to this assessment that there are artificial ways of extending the period for which temporary cached copies are stored, as "there is a difference, which is fundamental to the object of article 5.1. between a discretionary decision to extend the duration of what remains an automatic process, and the storage of a copy of material in the course of browsing in a manner which will ensure that it is permanent unless and until a discretionary decision is made to delete or destroy it."

The copies were "incidental" as they were "for the purpose of enabling a lawful use of the copyright material, i.e. viewing it."

- Integral and essential part of a technological process.

The caching of material and its reproduction on screen is a basic feature of the design of modern computers and is necessary to allow the internet to function "correctly and efficiently". As such, the making of such copies is "manifestly" an integral and essential part of a technological process.

- Lawful use.

Lawful "means lawful apart from any lack of authorisation by the copyright holder." The Court highlighted that "it has never been an infringement, in either English or EU law, for a person merely to view or read an infringing article" and this equally applies to the viewing of content on a web page.

- No independent economic

significance.

This condition does not mean that the copy must have entirely no commercial value at all. The copy must have no independent commercial value additional to that which is "derived from the mere fact of reading it on screen." The copies at issue in this case satisfied this requirement for the same reasons as temporary copies stored within a decoder and on a television screen in the context of broadcasts, which were held by the CJEU in the FAPL case to be an "inseparable and non-autonomous part of the process of reception of the broadcasts transmitted containing the works in question....performed without influence, or even awareness, on the part of the persons thereby having access to the protected works" and were therefore "not capable of generating an additional economic advantage going beyond the advantage derived from mere reception of the broadcasts at issue."

Effect of Article 5(5) of the Directive

Art. 5(5) (often referred to as the 'three step test') provides that the Art. 5(1) exception 'shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.'

The Court, consistent with the CJEU's approach in FAPL and Infopaq II, clarified that this provision simply requires Article 5(1) to be as narrowly construed as is consistent with its purpose. As such, if all five conditions are met, no additional restrictions are imposed by Art 5(5).

Anomaly with FAPL

The CJEU, in its decision in FAPL, had held that temporary copies stored within a decoder and on a television screen in the context of broadcasts were protected by the temporary copies exception. The Court acknowledged there was no rational distinction to be drawn between viewing copyright material on a television screen and on a computer. Should this be upheld by the CJEU, this will remove the anomaly in the law created by the conflicting decisions of the CJEU in FAPL and the decisions of the lower courts in the present case.

If, as many commentators anticipate, the CJEU agrees with the Supreme Court's decision, this will provide welcome clarification once and for all that simply reading or viewing material on the internet is not an infringement of copyright.

An online piracy charter?

The Court emphatically rejected the notion that the application of the temporary copies exception in this case would lead to an "internet piracy charter." Rightsholders continue to have causes of action against pirates and intermediaries which are used to disseminate infringing material and the Supreme Court believes that allowing the appeal will not alter the status quo.

Impact of the case

Although this is not yet a final decision, pending the preliminary reference to the CJEU, the Supreme Court's reasoning is consistent with the CJEU's previous rulings, notably in the FAPL and Infopaq II cases. If, as many commentators anticipate, the CJEU agrees with the Supreme Court's decision, this will provide welcome clarification once and for all that simply reading or viewing material on the internet is not an infringement of copyright.

Should the Supreme Court's decision be upheld, this is also expected to have an impact on the Copyright Tribunal's view on what constitutes reasonable licensing terms for online media monitoring services and their customers, in particular the level of royalties as the number of restricted acts licensed under the NLA's scheme would be materially reduced.

Ben Allgrove Partner
Michael Hart Partner
Nicole Fairhead Trade Marks Practitioner
Baker & McKenzie
Ben.Allgrove@bakermckenzie.com
Michael.Hart@bakermckenzie.com
Nicole.Fairhead@bakermckenzie.com

*Disclosure - B&M acted for Meltwater and the PRCA in these proceedings.

1. Football Association Premier League v. QC Leisure & Others, combined cases C-3403/08 and C-429/08.
2. Infopaq International v. Danske Dagblades Forening, Case C-302/10.
3. Infopaq International v. Danske Dagblades Forening, Case C-5/08 [2010] FSR 20.

The Trademark Clearinghouse: the ambitions and the issues

The Internet Corporation for Assigned Names and Numbers (ICANN) has launched the Trademark Clearinghouse, which aims to provide a database for the registration of trade mark data for brands prior to the release of 1,930 top-level domains this spring. While ICANN intends the Clearinghouse as offering a means for individuals and companies to protect their brands against the unwanted attention of cybersquatters, the Clearinghouse may be undermined by a number of factors, explains Scott B. Gardiner of D Young & Co.

With the launch of up to 1,930 new generic top-level domains ('gTLDs') just weeks away, the Internet Corporation for Assigned Names and Numbers' (ICANN) Trademark Clearinghouse is paving the way for what will be the biggest expansion of the domain name system since the inception of the internet...and for the inevitable scramble for second-level domain names that will ensue!

For those who may not yet be aware, having gone live on 26 March 2013, the Trademark Clearinghouse (the 'TMCH') aims to serve as a 'central repository of verified rights information' (as so phrased by ICANN), which facilitates the authentication and dissemination of such information to new gTLD registries. In simple terms, the programme will operate to store trade mark data submitted to it by rights-holders who either have an interest in registering a domain name with a new gTLD registry, or have an interest in preventing the registration of a potentially infringing domain name with one of the new gTLD registries.

New gTLD registries are expected to include such top-level domain names as '.store,' '.shop' and '.book,' with a number of companies competing to run these registries in what are being referred to as 'string contentions.' It is anticipated that in order to resolve these string contentions, auctions will take place, with the highest bidder being granted the exclusive right to operate the relevant extension either on an open or a closed registration basis. Once all operators have been selected, it is thought that the total number of brand new gTLDs will be around 1,000.

Aside from 'top-level disputes,' there will undoubtedly be an even greater number of disputes arising in relation to the registration of second-level domain names (the bit before the second dot) and, as a result, ICANN has devised a programme that it hopes will mean that rights-holders are better able to ensure that their brands' reputations will not be tarnished online by a third party's opportunistic registration (and associated use) of infringing domain names.

Sunrise periods and Trademark Claims Services

Having noted the concerns of rights-holders, ICANN is requiring that all new gTLD registries must (for 30 days before their domain names are offered to the general public) allow rights-holders to submit an application for the registration of a domain name which corresponds to a mark in which they hold rights (predominantly, unregistered or registered trade marks). This 30 day window is referred to as a 'Sunrise period.'

During any Sunrise period and for at least the first 60 days of a registry's period of open registration (which is referred to as the 'Trademark Claims Service' period), new gTLD registries must link to the Trademark Clearinghouse so as to ensure that domain name applicants' rights are checked against the (verified) trade mark information registered with the TMCH. The requirement to have rights information submitted to (and verified by) individual new gTLD registries is intended to be eliminated as the TMCH will adopt a central role in verifying trade mark data on behalf of the many new registries which this expansion of the domain name system will see created.

During the Trade Mark Claims Service period, applicants for a second-level domain name will receive a notification in circumstances whereby their applied for registration may infringe a mark registered with the TMCH. Should the applicant proceed in registering that domain name, the rights-holder of the corresponding mark will be so notified, enabling them to take remedial action. Simple!

Whilst the aims and objectives of the TMCH are admirable, it is to be asked to what extent the programme will afford adequate protection to rightsholders? Although we support the ambitions of the programme, we consider that its value may be undermined by four key factors.

'Identical matches'

In short, the TMCH programme will only permit Sunrise applications to be made in relation to applied for domain name registrations that are an 'identical match' to a mark registered with the Trademark Clearinghouse. Similarly, in relation to the TMCH's Trademark Claims Service (which notifies rights-holders upon the registration of a potentially infringing domain name), notifications will only be

provided where the newly registered mark is an 'identical match' to the mark registered with the TMCH. The contentious issue of 'typo squatting' (the practice of registering a misspelling of a famous brand name as a domain name) is therefore beyond the scope of the TMCH.

Cost

Whilst at face value, registering a mark with the TMCH appears relatively inexpensive (the cost of registering an individual mark on an annual basis being low), for rights-holders with a number of sub-brands, costs may prove prohibitive. This is exacerbated further by the system being restricted to 'identical matches,' both in respect of Sunrise registrations and its Trade Mark Claims Service, forcing rights-holders to register a greater number of marks than might otherwise be required or be desired. Indeed, ICANN appears to have (in principle) recognised that for those rights-holders hoping to register a significant number of marks with the TMCH, costs may be a deterrent to registration. As a result, a discounted pricing structure has been made available, offering discounts based upon the number of marks registered with the TMCH. However, it is unlikely that the size of these discounts will be viewed by rights-holders as being particularly persuasive when deciding whether or not to go forward with the programme.

Absence of a registration 'blocking' service

Having already acknowledged that the TMCH will only generate notifications for rights-holders where a third party attempts to register a domain name which is an 'identical match' to a mark registered with the TMCH, it is disappointing to also learn that the programme will not itself prevent the registration of a potentially infringing domain name (although admittedly such a service would be difficult to administer). Instead, in order to 'pick up' the infringing domain name, rights-holders will be required (themselves) to take their own enforcement action at an additional cost. To do so in relation to a potentially large number of registered domain names may prove phenomenally expensive and it may well be the case that for many rights-holders, the costs associated with taking enforcement action may mean that this is not a realistic option.

Whilst at face value, registering a mark with the TMCH appears relatively inexpensive (the cost of registering an individual mark on an annual basis being low), for rights-holders with a number of sub-brands, costs may prove prohibitive.

Length of the Trademark Claims Service period

Whilst individual gTLDs may decide to provide for a rather more generous Trademark Claims Service period (although I think it unlikely), the minimum length of this period has been set by ICANN at only two months. Coupled with the 'identical match' criteria, this is particularly disappointing news for rights-holders, who may lose the opportunity to be notified of a great number of potentially infringing domain name registrations. Do we not think that intentional infringers will be wise to this and, as a direct consequence, decide to postpone any adverse registrations until a given Trademark Claims Service period has expired?

Sunrise or sunset for rights-holders?

In view of the above identified shortfalls (and at least in respect of the TMCH's Trademark Claims Service), many rights-holders may consider a trade mark watching service to afford greater (and less expensive) protection for their intellectual property rights. Whilst in some respects this may be true, it must be stressed that for those rights-holders who are looking to secure early registrations with many of the new gTLDs, registering a mark (or marks) with the TMCH may be prudent in order to take advantage of the Sunrise registration periods that will be offered by each of the new registries. In requiring rights to be registered with (and verified by) the TMCH, the need to submit trade mark data to individual registries is removed which, in itself, may present some cost and time savings.

Of course, the true benefit of registering marks with the TMCH is yet to be seen and we keenly await developments in this area.

Scott B. Gardiner Legal Assistant
D Young & Co
sbg@dyoung.com

Prof. Viktor Mayer-Schönberger of the Oxford Internet Institute

Big data, the book and the need for regulation

Sophie Cameron spoke to Viktor Mayer-Schönberger, Professor of Internet Governance at Oxford University and co-author of the recently published 'Big Data: A Revolution That Will Transform How We Live Work and Think,' written with Kenneth Cukier, Data Editor of The Economist, about the potential for big data to change the world, and the need for regulation.

How will big data change the world as we know it?
By providing us with insights into a reality that we have not had – and through these insights enabling us to make predictions. For instance Google can predict the spread of the flu down to regions in the US by looking at what people search for online. Logistics companies change parts in their fleet before they break – predictive maintenance – using big data analysis; and financial services providers are able to predict whether an individual will likely take her medication on time by solely looking at her financial history. Such empirical analysis will take over from human intuition and hunches.

Which countries are investing in big data and why?
There is a vibrant and fast growing big data ecosystem in the US in Silicon Valley, in and around Seattle. Angel investors and venture capitalists there have realised the potential. Europe is quite a bit behind. Most surprising perhaps is the amazing interest in big data in China, where it is seen as a tool for further economic growth and embraced by the digital sector and government technocrats alike.

Is regulation necessary in this space to protect the consumer?
Yes. We suggest in our book that safeguards need to be put in place to ensure that big data does not control us. We are particularly concerned about what we call probabilistic predictions when they are abused to punish or stigmatise people.

You mention in the Big Data book that the value of data is in its secondary uses, with that in mind do you think that evolving data protection regulations threaten the potential of big data?
Yes. With big data we will realise that much of the value of data lies in its reuse. If that reuse requires data users to go back to individuals and ask them to consent, a significant portion of big data's potential will remain untapped. That is not necessarily a problem of future, but of already existing data protection statutes.

What can be done to harmonise the need for privacy protection and the need to innovate with big data?
We need to reconsider whether our current standard model of protecting privacy, namely to rely on informed (through 'notice') consent is appropriate. In our book we suggest that an alternative way forward is to focus on data user accountability: those who benefit most from big data, the data users, should also be held responsible for how they use the data.

Is technology advanced enough to protect privacy online?
No. And it never will be – because the problem is less technology itself, but the interaction of humans with technology.

What needs to be done to reduce the risk of data breach and the loss of sensitive personal information?
With big data, the problem of data breach shifts – at least to an extent. If one has a small data set, it can be 'stolen' easily and swiftly. If the data set is very, very large and comprises billions of data points in an unstructured database, 'stealing' it takes much, much longer, and thus increases the chances of detection. Moreover, if the dataset is not well structured, stealing only a small part of it will reveal less information than when it is structured. That should not make us complacent in the big data age, but it implies that the data breach problem does not necessarily increase drastically as we move into the big data age.

Do you think 'the right to be forgotten' is feasible and necessary in an increasingly online world?
It depends what we mean by the 'right to be forgotten'. If it means that individuals can rescind their consent to the concrete processing of their personal information, then this has been feasible (and law in Europe) for well over a decade. That is the essence of what the European Union is suggesting currently, and something that experience has shown is feasible, and in many direct transactions potentially useful. It also does not fundamentally undermine big data. If one, however, means a 'right to be forgotten' that would create a technical infrastructure to ensure that one's personal information automatically vanishes wherever it is stored if the individual so desires, then this will remain science fiction.

How integral will the law be in the success or failure of big data?
If we want to reap the benefits of big data without also being exposed to some of its most troubling dark sides, we need to put legal safeguards in place – to protect privacy, but especially to ensure human free will and competitive data markets.

Why did you see the need to write a book on big data?
Because big data is going to affect everyone, we need to know about it – and have an informed discussion about the need for any safeguards to be put in place.

Viktor Mayer-Schönberger Professor of Internet Governance and Regulation
Oxford Internet Institute / Oxford University
Viktor.MS@oii.ox.ac.uk

The Unfair Commercial Practices Directive review

In March 2013 the European Commission issued its review on the application of the Unfair Commercial Practices Directive ('UCPD') five years after its entry into force. The Report gathered feedback on the effectiveness of the UCPD across the EU and provided a summary of actions for the Commission to maximise the UCPD's benefit to consumers, primarily through coherent application and improved enforcement. Aonghus Martin, an Associate at Marriott Harrison LLP, discusses the Report in detail and the focus for the UCPD going forward.

Scope of the UCPD

The UCPD[1], which was adopted in 2005 to facilitate and encourage cross border trade whilst safe guarding consumer interests[2], covers the totality of business-to-consumer ('b2c') transactions from advertising through to after sales, both offline and online, and applies to goods and services. The Report touched upon the theme of expanding the scope beyond b2c transactions, i.e. to also cover, b2b, c2c (e.g. via trading platforms such as eBay) and c2b. For example, many consumers have sold antiques and jewellery (e.g. gold) to traders and have been misled by the representations made by traders, e.g. as to the value of the items. Whilst some Member States are in favour of legislation to expand the scope, the UK suggested an extensive approach to expanding the scope (i.e. a wide interpretation of the existing regime). However, the Commission commented in the Report that it is not keen on this approach and is against expanding the scope of the UCPD to include c2b, b2b and c2c transactions.

Principle-based approach

The UCPD is a principle-based piece of legislation allowing for flexibility to cope with new selling methods, products and marketing techniques. Traditionally English law has steered away from principle-based legislation but the implementation of the UCPD has proved effective in allowing Member States to adapt their assessments of evolving practices, in addition to the 'Black List' of banned behaviours[3]. An example of its evolution is the prohibition of the practice of making attractive offers to consumers when the trader is not able to supply the product in the quantities or scale expected based on the scale of advertising (e.g. traders making attractive offers using third party aggregators).

Misleading practices

The ability to clamp down on misleading practices has been a useful tool in dealing with 'copycat packaging'. 'Copycat packaging' refers to the practice of designing the packaging of a product to give it the general 'look and feel' of a competing well-known brand. Previously, 'copycat packaging' fell outside of trade mark and counterfeiting protections.

A misleading practice occurs when information is deceptive and causes (or is likely to cause) the average consumer to take a different transactional decision than they would have taken otherwise. One of the world's largest electronic providers fell foul of this when offering its paid-for-warranty for products, some of which it failed to sufficiently inform consumers was already covered by their statutory rights[4].

Price comparison websites

The UCPD has proved to be an effective tool in curbing such misleading practices from price comparison websites. Various Member States highlighted problems in relation to transparency and incompleteness of the information provided, i.e. incomplete information (e.g. delivery costs) makes any comparison unfair. It also found that some price comparison websites were not impartial and misled in relation to whether the traders paid to have their products listed or to receive priority.

Maximum harmonisation

One area which has resulted in tension between certain Member States and the UCPD is with regard to laws around sales promotions. The full harmonisation of the UCPD (confirmed in the 'Total Belgium' case[5]) restricts Member States from having (or adopting) stricter rules (even if it increases consumer protection)[6]. Many Member States would like to see sales promotions carved out of the scope of the UCPD, while others have asked for further guidance on this. The Report commented that most concerns could be addressed by increasing legal certainty and uniform application in this area. One of the key methods of achieving uniform application is the development of the UCPD database and Guidance document. There has been some case law in which the ECJ has ruled that the following national provisions are not compatible with the UCPD:

- A general prohibition on combined offers;
- A general prohibition on commercial practices under which the participation of consumers in a prize competition or lottery is made conditional on the purchase of goods or services;
- A general prohibition on

announcements of price reductions during the period preceding sales; and

- A prohibition to announce 'clearance sales' without obtaining the prior authorisation of the competent local administrative authority.

UCP database

In December 2009, the Commission issued a database and Guidance document to support the uniform application and convergence of practices in relation to the UCPD. This made all relevant materials concerning the UCPD accessible to the public, including national decisions, case-law and legal literature[7]. The Guidance document aimed to clarify key concepts and provisions perceived as problematic. It had no formal binding legal status; however, it has been widely used in court proceedings. It is intended to be a living document evolving as new unfair commercial practices emerge. Eventually, it will be replaced by a new Consumer Law Database, which will be regularly updated with materials and input from national enforcers and other stakeholders.

Misleading sales promotions

With regard to sales promotions, the Commission recently organised a workshop to tackle the issue of misleading environmental claims (also known as 'greenwashing'). The UCPD is used to tackle such claims that products or services are 'eco-friendly' etc. This is an important area given the drive for consumer preferences to contribute to the development of a more sustainable economy[8].

Environmental claims can be difficult to verify and assess and therefore the Commission has provided the following guidance, stating that environmental claims must be:

The good news for traders is that the Commission does not deem it appropriate to amend the UCPD at present. Rather, the Commission is focussing on several activities to help promote and stimulate cross-boarder trade with particular attention on problematic sectors such as travel and transport, digital services, financial services and immovable property.

- specific, accurate and unambiguous; and
- backed up with scientific evidence and be able to provide such evidence in an understandable way if the claim is challenged.

Curbing misleading environmental claims has been a success for the UCPD. It shows the ability of the UCPD to fill gaps in consumer protection laws where there was no specific legislation to deal with the practice.

Conclusion

The good news for traders is that the Commission does not deem it appropriate to amend the UCPD at present. Rather, the Commission is focussing on several activities to help promote and stimulate cross-boarder trade with particular attention on problematic sectors such as travel and transport, digital services, financial services and immovable property. The Report set out the following actions to continue the fight against unfair and unscrupulous practices:

- improve the enforcement activity at a cross-border level and promote additional coordinated enforcement 'sweeps'[9];
- regularly update guidance and databases to share best practice;
- develop indicators to detect shortcomings that require further action;
- specific consideration to be given to practices targeting vulnerable consumers, e.g. elderly and minors;
- stronger enforcement against price comparison websites which fail to disclose the identity of the trader operating the site, if traders pay a fee or the site has a bias towards certain partners; and
- establish regular thematic workshops and training between national enforcers and the judiciary.

The Commission did comment that recent research suggests that consumers are at present (and even more so in future) likely to purchase products and services across borders (which brings greater variety and lower prices for consumers)[10]. This is due, in part, to the success of the UCPD in simplifying the regulatory environment by replacing the previous fragmented regulations of Member States with one set of fully harmonised rules.

Aonghus Martin Associate
Marriott Harrison LLP
Aonghus.Martin@marriottharrison.co.uk

1. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market.
2. The UCPD was supposed to be implemented by Member States by 2007. The UCPD was implemented in the UK on 26 May 2008 via the Consumer Protection from Unfair Trading Regulations.
3. Recently, the ECJ clarified that the banned practices of informing a customer they have won a prize, and obliging them to incur costs, is strictly prohibited and includes the cost of a stamp.
4. Decision of the Italian Antitrust Authority (AGCM) PS7256 - Comet-Apple Prodotti in Garanzia Provvedimento n. 23193, 27 December 2011.
5. Joined Cases C-261/07 and C-299/07 VTB-VAB NV v. Total Belgium, and Galatea BVBA v Sanoma Magazines Belgium NV, 23 April 2009.
6. There is a six year grace period for Member States to repeal existing contradictory local laws. The maximum harmonisation rule does not apply to financial services and immovable property.
7. https://webgate.ec.europa.eu/ucp/public/index.cfm?event=public.home.show
8. The Report is in line with the Europe 2020 Strategy and the European Consumer Agenda.
9. The CPC (Consumer Protection Cooperation) Regulation establishes a cooperation framework linking enforcement authorities in the Member States to form an EU-wide CPC-Network.
10. However, the growth in online cross-border shopping is still some way behind online domestic growth.

Slovenia's data retention regulations called into question

Data retention and the principle of proportionality and privacy

Slovenia's Electronic Communications Act ('ZEKom-1'), which came into force on 15 January 2013, awaits its first review by the Constitutional Court. In March the Information Commissioner requested a constitutional review in connection with a supervisory proceeding against the second largest MNO in Slovenia[1], and challenged the provisions of ZEKom-1 on data retention. The Commissioner established that, for the purposes of the state, the operator stores and retains on a daily basis millions of personal details, but receives only 700 court orders per year for disclosure. The Commissioner therefore holds that the regulation of data retention does not respect the principle of proportionality and the constitutional right to privacy.

The Directive 2006/24/EC of the European Parliament and of the Council on the retention of data was transposed into the Slovene legal system with articles 162-169 of the ZEKom-1 and with the law on electronic communications. The article 163 of the ZEKom-1 however broadens the scope of data retention beyond the scope that is foreseen by the Directive. ZEKom-1 allows the retention of data for the purpose of (i) investigating all criminal offences, instead of only serious criminal offences as foreseen by article 1 of the Directive, (ii) ensuring national security, constitutional order, and security, political and economic interests of the state, and (iii) national defence.

The Commissioner argues that data retention in general does not constitute a necessary and appropriate measure for achieving the objective as foreseen by article 1 of the Directive, and finds that the state did not demonstrate the impossibility of achieving the same objective with lesser or without interference with the right to privacy. Available data shows that the extent of criminal offence prosecution has not changed since the implementation of data retention, and the state continues to successfully prosecute criminal offences without using retained data. The Commissioner therefore noted that data retention is not a necessary measure. She furthermore noted that, due to the possibility of falsification of data, the expectation of its public benefit is based on an erroneous belief that digital data is always trustworthy.

The Commissioner also established that the authorities often tend to request the operators to disclose the retained data for purposes outside of the scope of the ZEKom-1, including for litigation, prosecution of minor offences and labour disputes, which represents an additional risk to privacy.

The Commissioner holds that the current rules on data retention are interfering with the right to privacy of communications. The right to privacy of communications may be restricted when provided by law and only on the basis of a court order - a principle which is not respected in the ZEKom-1. The Commissioner also holds that data retention is interfering with the freedom of movement and expression. She noted that some of the data discloses the position of the affected individual, which might lead to monitoring of movement, and may affect the way individuals express themselves.

The Court in its previous decisions held that the interference with human rights is admissible, if it is based on a legitimate, objectively justified aim and the interference is not excessive. The case law indicates that the Court may hold data retention as unconstitutional, since the Commissioner showed that the state is not at all able to demonstrate a successful use of the retained data, and the interference with the right to privacy therefore fails to comply with the principle of proportionality, which was also crucial in the Czech and German review of data retention. However, the state still has the opportunity to show that the concerns about dis-proportionality are unfounded.

Unlike in the case of the Austrian and Irish review of data retention, the Constitutional Court is not likely to request a preliminary ruling of the CJEU, since the Commissioner did not propose such a ruling and the validity and interpretation of the laws of the EU are not likely to be seen as relevant for the Constitutional Court to give judgment. The position of the Commissioner that the ZEKom-1 is unconstitutional, since it did not directly and completely implement the Directive, appears irrelevant, as the Constitutional Court has no jurisdiction regarding the conformity of the ZEKom-1 with the laws of the EU.

Although the Commissioner proposed that the Court handles her request with the highest priority, arguing that data retention interferes with the human rights of all users of electronic communications in Slovenia, if they act in accordance with law or not, it is - according to the case law of the Court - more likely that a ruling will not be seen before 2014. The Commissioner also proposed that the Court temporarily suspends the provisions on data retention. The Court normally suspends challenged provisions, if enforcement may lead to effects that are difficult to remedy. The Commissioner failed to substantiate which effects may occur by the time of the ruling and how the immediate cessation of retention could prevent such effects. As the retained data is relatively easy to delete, it is more likely that the Court will not follow the proposal on temporary suspension of respective provisions.

Retention of data is subject to constitutional reviews in a growing number of EU Member States. There are currently open review procedures in Austria, Ireland and Slovenia. While the courts of Austria and Ireland await a preliminary ruling of the CJEU, we will likely soon see a judgment of the Slovene Court, which could repeal the provisions transposing the rules on data retention from the Directive 2006/24/EC.

mag. Mitja Podpecan Senior Associate
Jadek & Pensa
mitja.podpecan@jadek-pensa.si

An extended version of this article can be found on the ecomlaw website.

1. https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1155

The global fight against cyber crime: CERT, CISP and CISPA

The security of cyberspace is now a hot topic for governments across the globe, and different jurisdictions have adopted varying approaches to combating cybercrime, from information sharing federal bills in the US to the 'big picture' oriented Cybersecurity Strategy of the EU. Mark Surguy and Liz Fitzsimons, of Eversheds LLP, assess the mammoth task of tackling cybercrime and the latest governmental approaches.

Cyberspace does not recognise global boundaries, so the cyber threat applies to all countries, governments and peoples. Attacks allegedly by rogue states, state sanctioned bodies and criminals have been made against the private sector. The perpetrators benefit from the fragmented legal ecosystem, made up of multiple public and private legal entities, geographical boundaries and territorial jurisdictions, which underpins cyberspace. Lack of awareness of current threats and risks facilitates the progress of the cybercrime bandwagon.

Mandatory information sharing and breach reporting is currently rare. In Europe security breaches involving personal data must be reported to regulators by telcos and ISPs but otherwise, mandatory personal data breach reporting is the exception rather than the norm and is often limited to specific types of incident.

Surprisingly, since the US does not have federal data protection legislation regulating all types of personal data, they do take a stronger line on mandatory security breach reporting than Europe, although the position in the US requires consideration on a state-by-state basis, since there is no applicable federal law. Almost all states have laws requiring notification of security breaches (triggered by the incident hitting various thresholds connected to the type and amount of personal identifier information involved). However, the obligations vary from state-to-state and companies must be aware of the state law applicable to both themselves and the data subjects affected by a breach.

However, attacks on the cyber nervous system will not always involve personal data. There is separate European legislation not dependent on personal data and aimed at protecting critical European infrastructure, Directive 2008/114/EC, and there are other bodies to help deal with threats to networks and information security and to help combat cyber security threats. These include the European Police Office ('Europol'), the European Cybercrime Centre ('EC3'), the European Network and Information Security Agency ('ENSA') and the UK's Centre for the Protection of National Infrastructure ('CNPI').

Many if not all Member States are dealing with cyber threats and security, in terms of policy, guidance and detection along with local prosecution, but to date a joined-up approach has been lacking. Reducing the incidence of cybercrime and establishing a coherent defence requires systematic reporting of incidents to law enforcement agencies, where criminal intent is suspected.

So, would a compulsory system of reporting these incidents, at least by those at greatest risk of the most damage, improve the ability of others to better protect themselves against a similar attack? Such a regulatory approach is indeed the view of the EC, which recently published a proposal aimed at adopting a 'big picture' vision to manage and reduce the cyber security threat. Having undertaken impact assessment and consultation exercises, the EC released its new EU-wide Cybersecurity Strategy, aimed at 'An Open, Safe and Secure Cyberspace,' on 7 February 2013.

The EU strategy and proposed legislation will amongst other things require Member States to create a Computer Emergency Response Team ('CERT') responsible for protecting the providers of critical infrastructures from cyber attacks and for sharing information on incidents with law enforcement and data protection regulators. The thinking behind the new regime is that each Member State should have a central reporting authority to whom incidents can be notified. From these central bodies, Member States can disseminate information on incidents in order to generate early warning systems for other Member States. The idea is to improve co-operation on network infrastructure security within the EU and to create a culture of risk management and a better flow of information between the private and public sectors. The legislation also aims to establish a minimum common level of network security.

The EC intends to compel each Member State to have a minimum capability for dealing with network security issues and to facilitate information sharing between them. The new policy has five goals: achieving cyber resilience, drastically reducing cybercrime, developing cyber defence policy and capabilities, developing industrial/technological resources for cyber security and establishing a coherent EU policy on this topic which promotes EU values.

The plans target 'public administration' and 'market operators,' who will be compelled to implement 'appropriate technical and organisational

measures to manage the risks posed to the security of networks and information systems which they control and use in their operations,' bearing in mind the available technology and through a risk-based approach taking into account the risk presented by but also supplemented by the ability of the national authority to audit compliance by the public administration or market operator body. This will expressly impact e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores. It is not entirely clear how this will work if the provider is based outside the EU, as many are.

Supplementing this, the national authorities can issue binding instructions to the affected administrations and operators. This may lead to an element of micro management being imposed, with the EC and authorities being able to mandate minimum security requirements for certain bodies, dictated by their sector or importance to the digital economy.

There are gaps in the current arrangements. Does the existing mandatory security breach reporting across Europe really drive change and how much benefit actually results from these obligations? Barriers to information sharing about attacks and breaches are the fear of regulatory enforcement action, concern about reputational damage, and the risks from disclosing sensitive data. It needs to be clearer whether these proposed measures are aimed at punishment or information gathering and the improvement of cyber defences.

It also seems excessive to have yet another enforcement regime (if that is what it is), in addition to the two current legal regimes, especially when the proposed EU Data Protection Regulation already contains an EU wide mandatory reporting regime for personal data security breaches.

In practice, the sometimes slow to respond and bureaucratic EU regulatory system may not be as agile as is vital to counter the present threats. So would simply facilitating information sharing on cyber risks be a better approach?

It is also not clear how the new regime will work with the existing and already contemplated regimes. For instance, the proposal recognises that there will be an overlap of reporting obligations and enforcement action possible where personal data is involved. It does not explain whether the dual reporting obligation may lead to a double fine. It is also not clear whether meeting this directive's security requirements will automatically meet the security expectations of the data protection regulators. It may be better to build where necessary on current systems and laws, making use of the existing regulators to minimise costs and confusion.

In practice, the sometimes slow to respond and bureaucratic EU regulatory system may not be as agile as is vital to counter the present threats. So would simply facilitating information sharing on cyber risks be a better approach? This is the view in the US where on its second attempt through the House of Representatives, the Cyber Intelligence Sharing and Protection Act, ('CISPA') was passed on 18 April. CISPA will allow private companies to share customer information with legal impunity with a range of government agencies in the event of cyber threat. One of CISPA's co-authors, Mike Rogers, argued: "This is the answer to empower cyber information sharing to protect this nation, to allow companies to protect themselves and move on to economic prosperity." However, the bill has still to pass through the Senate, while the White House administration has threatened to veto the bill due to privacy concerns. The American Civil Liberties Union shares those concerns: "CISPA is an extreme proposal that allows companies that hold our very sensitive information to share it with any company or government entity they choose, even directly with military agencies like the NSA, without first stripping out personally identifiable information."

A more acceptable approach may be the UK government's launch in March of the Cyber Security Information Sharing Partnership ('CISP') between government, including the CPNI, and industry under which, in secret and by invitation only, partners can share information on cyber security threats. CISP will include support by expert analysts from GCHQ and MI5 in a fusion cell and will: "give government and industry a far richer, more immediate intelligence picture of the cyber threat," according to Sir Francis Maude. There is no privacy immunity under the UK approach.

To successfully protect our privacy and assets from criminals, we may have to be more open with each other and the government than we would ideally like. It is not certain whether we still need the EU proposed mandatory cyber security reporting regime in the light of developments. However, CISP does not obviously deal with how the intelligence gathered would be used for inter-governmental and international protection.

What is clear is that the bad guys will not wait for us to catch them up. They are a moving target which we need to get ahead of if the proposed strategies are to be delivered.

Mark Surguy Partner
Liz Fitzsimons Legal Director
Eversheds LLP
marksurguy@eversheds.com
lizfitzsimons@eversheds.com

Capitol Records v. ReDigi and the reselling of digital files

On 30 March 2013, a New York District Court handed down its decision in the case of Capitol Records v. ReDigi, finding that ReDigi, a service that offers an online marketplace for the reselling of mp3 files, was in violation of US copyright law. Samuel Fifer and Katherine L. Staba of Dentons examine the court's findings and explore how the digital redistribution conundrum remains unsolved.

While the average consumer rarely discerns between the paper and ink copy of their favourite novel and the version read on a tablet device, copyright law certainly does. The clash of these perceptions and rigid application of copyright law has recently been illuminated by the Southern District of New York's summary judgment opinion in Capitol Records, LLC v. ReDigi, Inc. (No. 12-CV-95; Mar. 30, 2013).

The dispute arose from ReDigi's online music resale marketplace that launched in 2011. The business model, as described by ReDigi, permits users to resell music purchased on iTunes or from another ReDigi user. The process of such resale is critical for understanding the nuances of the court's analysis: First, a user/seller wishing to sell one of its eligible songs uploads the file to ReDigi's 'Cloud Locker;' then, ReDigi validates that the uploaded file is a type that is 'eligible' for resale (e.g. from iTunes); validated files are then stored in the Cloud Locker and can be streamed by the seller or offered for sale in the marketplace, which terminates the seller's access to the file. Once a file is purchased, the buyer can stream it from or offer it for sale on the Cloud Locker, or download it to the buyer's device. Built into this process is ongoing monitoring by ReDigi to screen for sellers that attempt to maintain copies of the sold file in certain areas of their computer. The process attempts to migrate a user's file through the digital sphere so the file does not exist in multiple places at once.

Capitol Records, holder of numerous copyrights in such music, filed suit alleging multiple violations of the Copyright Act.

The Opinion

On 30 March 2013, the Southern District of New York ruled on the parties' cross motions for summary judgment, finding for Capitol Records on all asserted counts. In its opinion, the Court tackled the convergence of somewhat archaic copyright principles with new applications of existing technology. The court addressed each count separately, but the opinion centred on two issues: (1) whether ReDigi's services in facilitating the transfer of a digital music files over the internet constituted unauthorised reproduction within the Copyright Act, and (2) whether ReDigi's distribution activities were protected under the first sale doctrine. In answering these questions, the court focused on the peer-to-peer file-sharing precedent and, more specifically, the lifecycle of a transferred digital music file.

Looking to the technical lifecycle of a digital music file in ReDigi's marketplace, the court found reproduction rights violated at several different stages. Since, according to the court, the download of the digital music file necessarily created a new object on the user's hard disk, this embodiment of the file on the new hard disk is a reproduction (i.e., 'a copy') within the meaning of the Copyright Act. ReDigi's attempt to ensure that only a single copy of the file existed at any one time was irrelevant, as the relevant distinction was rather the requisite creation of a new material object, not the existence of additional material objects. In fact, ReDigi's argument that a file merely 'migrated' from one user to the other was rejected on the grounds that not only was a new material object created when the buyer downloaded the file, but reproduction also occurred at the outset of the service in the seller's original upload of the file to ReDigi's Cloud Locker. After finding infringement of Capitol Records' reproduction rights, the court swiftly held that ReDigi had similarly violated Capitol Records' distribution rights by admittedly selling digital music files.

Significantly, ReDigi's reliance on the first sale doctrine defence to excuse its infringement of Capitol Records' distribution right was rejected[1]. While the first sale defence was codified to limit a copyright holder's distribution rights after a copyrighted item is sold, it was held inapplicable to ReDigi's services because the digital music files sold by ReDigi were actually not the lawfully made articles, but rather were unauthorised reproductions. It was thus insignificant that only lawfully purchased files from iTunes were eligible for sale, as such particular digital music files could never, through use of ReDigi's marketplace, be transferred. Rather, files were reproduced at each stage in the sale process. Unmoved by ReDigi's contention that application of the doctrine's literal terms to technological changes creates a result that is misaligned with the basic purpose of the Copyright Act, the court instead differentiated between the nature of resale of physical and digital works: The justifications for application of the doctrine to the latter are not met because a resold digital work is no less desirable

than a copy of the new work, as it does not degrade and is thus indistinguishable from a new copy.

With no defences to excuse infringement, the court deftly found liability for both direct and secondary infringement. Constructing a service that was solely based on the resale of copyrighted content and brokering such sales made ReDigi an active participant in the infringement, despite the automation of the service, thus warranting a finding of ReDigi's direct infringement of both Capitol Records' distribution and reproduction rights.

Under theories of both contributory and vicarious liability, the court found ReDigi liable for secondary infringement[2]. Objective evidence showed that ReDigi had warned investors that the law was unsettled in the area, the Recording Industry Association of America had sent ReDigi a cease and desist letter in November 2011, and ReDigi had been involved in licensing disputes over use of song clips and cover art. ReDigi insisted that it had sought the advice of counsel, but declined to reveal any of this advice. Its 'sincere belief' in its legality alone was simply insufficient in light of such objective facts. Its supervision of and confirmation that its content was copyrighted and its hosting in the Cloud Locker marketplace ensured that infringement occurred, thereby negating any argument that the service was capable of substantial non-infringing uses. Accordingly, contributory liability was found. Applying the same objective facts regarding ReDigi's involvement in the sale of copyrighted works and financial gain from the service, the court found that 'clearly' ReDigi vicariously infringed Capitol's copyrights.

ReDigi has stated its intention to the court to move for certification of the 30 March 2013 order for interlocutory appeal, but at the time of publication such motion has not been made.

Objective evidence showed that ReDigi had warned investors that the law was unsettled in the area, the Recording Industry Association of America had sent ReDigi a cease and desist letter in November 2011, and ReDigi had been involved in licensing disputes over use of song clips and cover art.

Observations

Judge Sullivan's statement at the outset of the hearing read: '[t]here are a lot of people who are very interested in what the law should be and what would be a wise way to arrange ourselves with respect to this kind of technology...but that's not really what we're here to decide today.' The court's opinion repeatedly suggested that ReDigi's legal position arising from its innovative technological services was not necessarily at odds with copyright principles but simply could not be aligned within the confines of the current Copyright Act. It can be argued that the court's mild chastisement of ReDigi to press its position through statutory amendment instead of in a courtroom was less a function of the necessity of a change to the legal landscape than a plea to cease the deluge of precedent-making, inconsistent and often thinly parsed decisions.

A statutory amendment is seldom swift, and would likely be rendered a relic of the past even more quickly than the current Copyright Act. Accordingly, a party's battleground still likely lies with making informed business choices to fall magically on the proper side of the hazy, ill-defined legal line. In ReDigi's case, business changes had already occurred by the time of the opinion; later versions of the service (not considered by the court) apparently omit the seller/user's original upload to the Cloud Locker. Whether such changes alone are sufficient to place the new version within the zone of the first sale doctrine is unknown.

The landscape of the digital resale market remains increasingly unclear. The court's opinion in ReDigi suggests that even where an entity takes steps to ensure that such resale transaction is compliant with business and legal morays and a single file 'migrates' digitally from seller to buyer, technological particularities may render the act infringing and, more specifically, outside the protections of the first sale doctrine. Looming on the horizon is the obstacle that traditional conceptions of 'ownership' of physical goods are not mirrored in the digital world. For example, iTunes subjects purchasers to rules restricting use to personal, non-commercial use on a limited number of devices[3]. Thus, consumers expect to be able to sell what they have purchased, but have we created a virtual marketplace that supports this conception? Undoubtedly, changes are in the future, whether within technological advances to circumvent infringement concerns, or on the statutory front. How the Second Circuit may act on appeal also is unknown and it may reframe the conversation entirely.

Samuel Fifer Partner
Katherine L. Staba Managing Associate
Dentons
samuel.fifer@dentons.com
katherine.staba@dentons.com

1. ReDigi also asserted the defence of fair use. Characterising ReDigi's service as "well outside the fair use defence," the court rejected ReDigi's argument that the uploading and downloading services were for personal use, finding each of the fair use factors weighed against a finding of protected use.
2. While Capitol Records also alleged a separate count for inducement of infringement, the court declined to settle the disagreement over whether such a count is a separate theory of liability, instead not reaching a decision on the claim in light of its finding of contributory liability.
3. http://www.apple.com/legal/internet-services/itunes/us/terms.html#SERVICE (last visited 6 May 2013).

HOT TOPIC: Online sales tax

E-Commerce Law & Policy explores the online sales tax debate in four jurisdictions.

United States

Since before the birth of the commercial internet, states and localities in the US have been prohibited under decisions of the US Supreme Court from requiring retailers with no physical presence in the jurisdiction to collect sales and use taxes from consumers. That may soon change. Skipping the usual committee process, the US Senate on 6 May passed the so-called 'Marketplace Fairness Act.' The bill would authorise states and US territories that satisfy certain basic criteria to impose a sales/use tax collection obligation on internet retailers and other remote sellers. Proponents argue that the bill 'levels the playing field' for online sellers and traditional bricks-and-mortar retailers. Critics charge that the legislation does not demand enough simplification of state tax codes and that the bill's 'small seller' exemption for businesses with less than $1 million in total US sales is too low. Many large US internet sellers already collect sales tax online but the bill, if enacted, will likely make sales tax on internet purchases ubiquitous. It will also subject ecommerce vendors to much greater sales tax compliance burdens. The legislation now moves to the US House of Representatives, where the prospects for its passage are less certain.

Matthew P. Schaefer Partner
Brann & Isaacson
mschaefer@brannlaw.com

India

In terms of Indian tax laws, business income of a non-resident e-commerce player will be taxed in India if it accrues or arises in India or is deemed to accrue or arise in India through a 'business connection.' As a concept it is similar to 'permanent establishment,' discussed in tax treaties, but is much wider and inclusive in scope.

As an observer at the OECD deliberations, India argues that a website may constitute a permanent establishment in certain circumstances. Depending on facts, an enterprise can be considered to have acquired a place of business by virtue of hosting its website on a particular server at a particular location.

However, in terms of decided cases, a website does not constitute a 'permanent establishment' unless the servers on which websites are hosted are also located in India. The principle applies to online commerce as well as to globally famous search engines.

Most of India's success in the last two decades has been through IT and ITES-based activities, and a considered e-commerce tax policy is the need of the hour.

Sunil Jain Partner
J. Sagar Associates
sunil.jain@jsalaw.com

France

The idea of a tax on data collection seems to have been put aside for technical and legal reasons. Fleur Pellerin, minister for digital economy, expressed in April her interest in having a tax on bandwidth.

The objective would be to tax the volume of digital information consumed in France by the operators, which allow them to reach French internet users. French ISPs would like to invoice operators, arguing that the evolution of the internet entails higher costs due to the increase of content sent by operators and advanced technical features required to allow proper use.

The government appointed the 'Conseil National du Numérique,' in charge of advising on issues of the digital sector, in order to organise a public consultation on the taxation and based on proposals including the Colin and Collin report. A summary document is expected on 15 July 2013.

The government wishes to include in the upcoming draft of Finance Act for 2014, the first measures that would allow, at a national level, the taxation of digital activities carried out in France.

Rui Cabrita Avocat à la Cour
Olswang France LLP
rui.cabrita@olswang.com

United Kingdom

One issue that everyone agrees on is that international tax rules are out of date and need to change to reflect modern business.

As with most other jurisdictions, the UK has adopted the OECD's model of taxing businesses that are managed and controlled in or that have a 'permanent establishment' in the UK. And therein lies the problem for the Government - without a permanent establishment there is nothing to tax.

Crucially, HMRC takes the view that 'a server either alone or together with web sites could not as such constitute a PE of a business that is conducting e-commerce through a web site on the server.' As a result, businesses selling to UK customers online are not subject to UK corporation tax simply because their servers are located in the UK. The UK Government, knowing that it cannot unilaterally change its approach, is taking the issue to numerous bodies, including the EU and OECD.

While some steps to bring UK tax in line with online businesses have been taken, this lags behind business developments.

Aredhel Darnley Senior Associate
Squire Sanders
aredhel.darnley@squiresanders.com

READ MORE EXCLUSIVE CONTENT ONLINE - www.e-comlaw.com/e-commerce-law-and-policy
Go to the website to read an article on the procedures of the **Unified Patent Court**, the extended version of the article on Slovenia's data retention laws and our **Editor's Insight** for May by Mark Bailey on **cyber risk and survivability**.