

SPRING 2015

Technology update



Welcome to the latest edition of the technology update which aims to provide you with up-to-date information about issues affecting businesses in the technology sector.

I am delighted that since our last edition, John Warchus has joined our commercial and technology team as a partner. John brings with him 25 years of experience and knowledge of the law in the area of information technology and intellectual property and will be working principally out of our Richmond and City offices.

In this edition we discuss why it is important to make sure that your cloud services provider has adequate security arrangements. We also look at the court of appeal's decision on Topshop's use of Rihanna's image, the new copyright exceptions for personal copying, parody, and quotation and the financial conduct authority's review of swap contracts.

If you have any comments or suggestions for topics that you would like to see in future editions, please contact me on 023 8071 8078.

Kind regards

Dorothy Agnew

Partner
023 8071 8078
dorothy.agnew@mooreblatch.com

Recent deal

We recently acted for Liberata UK Limited in relation to its purchase of Trustmarque. Liberata is a business process outsourcer based in Central London with 14 offices around the UK.

Trustmarque is a Microsoft enterprise partner and major technology service provider to the NHS, healthcare trusts, local government and financial sector. Trustmarque is a £100million turnover business employing over 200 people in London, Manchester, Edinburgh and Glasgow and was acquired by Liberata in just 7 days.

Dermot Joyce, Chief Executive Officer of Liberata commented: "I would like to thank Peter Jeffery and his team for a speedy resolution of a highly complicated and highly charged transaction."

Peter Jeffery, Partner in Moore Blatch's corporate department commented: "The UK technology sector is buoyant and dynamic, with a rich mix of mergers, joint ventures, restructures, relocations and disposals. We are adept at bringing together all the disciplines that ensure speedy resolutions in every legal area, however complex."

New exceptions in UK intellectual property law already outdated?

In October last year UK intellectual property law received a much needed update, when exceptions for personal copying, parody, and quotation came into force.

Stemming from the 2011 Hargreaves report, the changes brought about by The Copyright and Rights in Performances (Personal Copies for Private Use) Regulations and The Copyright and Rights in Performances (Quotation and Parody) Regulations 2014 aim to bring our IP laws into the 21st century, supporting the reasonable use of creative content, without undermining copyright's important role in supporting the creative industries.

Many would have been blissfully unaware that personal copying of legally purchased media (CDs, ebooks etc.) had up until October been unlawful. Changes to the law now allow you to make personal copies to any device that you own, or a personal online storage medium, such as a private cloud, without fear of prosecution. It is however still unlawful to allow others access to the copies you make, including, for example, by allowing a friend to access your personal cloud storage.

The new parody and quotation exceptions that allow people to use copyright material without permission from the owner are subject to the concept of "fair dealing". Whilst comedians all across the country will no doubt be relieved by the prospect of performing without the threat of litigation, the lack of a UK definition of parody and the hazy concept of 'fair dealing' fail to clarify what is acceptable and difficulties remain especially where it is hard not to "reproduce a substantial part", such as with the use of images.

So while it may have taken decades to reach this point, this must be seen as a positive step for UK consumers. However, with the shift towards streaming media one wonders whether the changes have come too late.

Dorothy Agnew, Partner and Ben Kerley, Trainee Solicitor

How secure is your data?

Insecure data could damage your business

Business are using cloud services for data storage, corporate websites, payment processing, sales, marketing and many other business activities. Using cloud services provides flexibility and potentially lower costs, but how secure is your data?

A recent survey on information security commissioned by the department for business innovation and skills, clearly demonstrates the continuing risks associated with doing business online. The survey findings noted that cyber attacks have continued to grow in frequency and intensity over the last year with the focus shifting back towards large organisations. Most worryingly most of the affected companies were penetrated not just once but once every few weeks during the year. There has also been a significant rise in the cost of individual breaches, the worst nearly doubling over the last year. Attacks from outside the organisation continue to cause most security breaches and malicious software is increasingly the means for such attacks. One of the 6 key observations of the year was that 70% of organisations keep their worst security incident under wraps. So what's in the news is just the tip of the iceberg.

In addition to the cost of recovering from a breach, large penalty fines imposed by the Information Commissioner's Office (ICO) for security breaches in recent years serve as a salutary warning that businesses should not treat data security lightly.

Under current UK data protection legislation businesses can be liable for fines of up to £500,000 for data protection breaches. However, the European Commission's recent proposals for a comprehensive reform of the European Union's data protection legislation include proposals for fines of up to 2% of global annual turnover for businesses who fail to comply with the rules.

Other risks associated with security breaches include damage to reputation and adverse media coverage of the security breach. A security breach can also cause significant business disruption, both from the breach itself and remedial action to prevent it recurring.

When purchasing cloud services what are some of the factors that businesses need to consider?

1. **Pre-contract due diligence:** carry out pre-contract due diligence on your chosen cloud services provider. Are the security arrangements adequate for your purposes? Is the provider financially secure and does it have a good

reputation in the industry? Where will your data be stored – for example will it be stored on servers in the UK or in the US or India or elsewhere in the world? Any pre-contract assurances given by the provider about the service should be clearly documented in your agreement with the provider.

2. **Third party service providers:** It is not unusual for cloud service providers to use third parties to store data and to provide other features of the service. If your data is going to be stored by a third party outside the UK or the European Economic Area is this acceptable to you/ your customers? Does the third party give adequate assurances about security? Your data could be at risk if the IT security of the service provider's suppliers is lax.



3. **Supplier security obligations:**

- What security systems does the cloud service provider have in place? Do they protect you, and them, from viruses, rogue code execution, unauthorised access, and social engineering?
- If the cloud based service is web-based, how is it protected from Denial of Service (DoS) attacks, which are often part of a wider targeted hacking attempt.
- If the cloud provider uses outside software, what is the process and schedule for updating this with the latest security updates? This is especially important as the time between an exploit being discovered and used is being compressed.
- Loss or corruption of data can significantly disrupt a business, with critical customer and accounting records being key targets. Reinstatement or restoration of data can be costly and time consuming. What back-up and business continuity arrangements will the supplier provide? How often is this backup taken? What happens if the data is corrupted, can the IT service provided restore the position to the last backup?
- What are the plans in place in event of a physical problem with the data centre(s), such as fire or flood?

Make sure security features and processes of the cloud service are clearly documented in your agreement with the service provider.

4. **Right of audit:** Consider seeking a right to audit your service provider's security arrangements from time to time during the service term.
5. **Customer retained risks:** make sure that you understand what expectations the supplier has about how you will assist with security such as password management. You may need to work with the service provider to agree customer security obligations that are appropriate and proportionate to the type of cloud services that you are seeking from the supplier.
6. **Data protection:** even though you are using a cloud service provider to store your customer data and other personal information you are likely to remain the data controller of such information and as such will be responsible for compliance with the Data Protection legislation. You should take steps to ensure that the cloud services provider gives you adequate commitments about its processing of such personal information.

Using cloud services can bring many benefits such as flexibility and reduced cost but care should be taken to ensure that your data is well protected as a security breach can damage your reputation and cause your business significant disruption and cost.

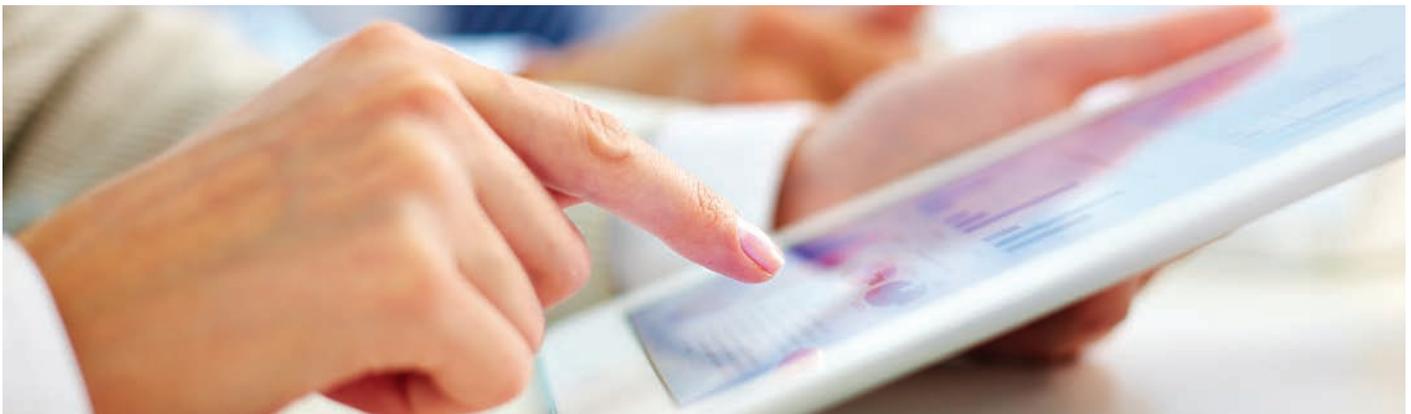
Dorothy Agnew, Partner and Elizabeth Cooke, Legal Assistant

Recent ICO Penalties

In February 2015 the ICO fined Staysure.co.uk Limited £175,000 after IT security failings let hackers access customer records. The ICO reported that more than 5,000 customers had their credit cards used by fraudsters after the attack on Staysure.co.uk.

In March 2014, The British Pregnancy Advice Service was fined £200,000 by the ICO. In March 2012 the BPAS's website was attacked. As a result of insecure collection of website data the attacker – an anti-abortion campaigner – was able to gain access to the website CMS which contained details of over 9,000 users; data included their name, data of birth address and telephone numbers. The ICO's report stated that "Some of the call back details were from individuals whose ethnicity and social background could have led to physical harm or even death if the information had been disclosed by the attacker."

In January 2013 the ICO fined Sony £250,000 after the Playstation network was hacked, compromising the personal information of millions of customers. This included their dates of birth, account passwords and payment card details. The ICO investigation found that the attack could have been prevented if the software had been up-to-date. Technical developments also meant passwords were not secure.



Topshop loses in the Court of Appeal

Court of Appeal upholds the decision of the High Court that Topshop's use of Rihanna's image amounts to passing off

In 2013 the pop star Rihanna won her High Court claim against Arcadia, the parent company of Topshop, for passing off as a result of Topshop using her image on a t-shirt without her approval.

The High Court found that Topshop's use of the image was a misrepresentation that the t-shirt had been endorsed by Rihanna. In reaching this conclusion, the High Court relied on the following facts:

- The image was from a photograph taken during a video shoot for a single on Rihanna's Talk That Talk album, was very distinctive, and could be thought to be part of a promotional campaign; and
- Topshop had well-publicised links to a number of celebrities, including Rihanna, who was a well known music and style icon.

Topshop appealed against that decision. The Court of Appeal has now heard the appeal and given its judgment. It upheld the High Court's decision, although emphasised that the decision was very much dependent on its facts. The Court of Appeal highlighted that it was the combination of the facts present in this case which allowed the claim to succeed.

Consequently, this decision will not mean that every celebrity will succeed in an action for passing off simply because their image appears on a garment or any other merchandise. However, retailers should take care when using a celebrity's image without their approval.

Claire Haverfield, Partner and Hayleigh Sears, Trainee Solicitor

Technology firms face inflexible bank funding

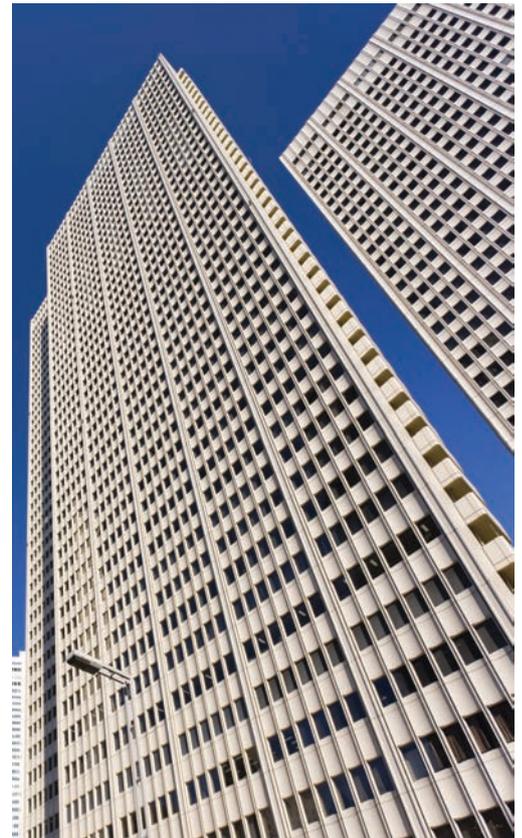
Price rises for comms and internet services providers have been predicted, as a consequence of this year's changes to VAT rules for EU online sales. A predicament arises for these providers – as to whether a price rise will affect their revenue positively - or negatively if their customers move elsewhere.

With significant property and infrastructure costs to be maintained, service providers might consider reviewing their finance arrangements to ensure they have the flexibility they need.

Many Tech SME's with property assets may have found that their finance arrangements include interest-rate fixing arrangements, known as "swap contracts", which can make it very expensive for them to refinance or relocate. The problem arises from exit costs, payable if the finance arrangements are terminated early.

The Financial Conduct Authority (FCA) has, this month, provided an update on its review of sales of "swap contracts" – revealing that hundreds of firms are still waiting for payouts due from their banks – with thousands of businesses yet to have their cases resolved. The FCA reports that some 29,568 swap contracts were sold, mainly to SME's, with over 90% of the cases they have reviewed having been found to be mis-sold. The FCA's review scheme is potentially closing to new cases on 31 March 2015.

Andrew Reid, Senior Solicitor



Please contact one of our team



Dorothy Agnew

Partner
023 8071 8078
dorothy.agnew@mooreblatch.com



Claire Haverfield

Partner
023 8071 6132
claire.haverfield@mooreblatch.com



John Warchus

Partner
020 8332 8631
john.warchus@mooreblatch.com



Jeremy Over

Partner
023 8071 8025
jeremy.over@mooreblatch.com



Sarah Crookall

Senior solicitor
023 8071 8044
sarah.crookall@mooreblatch.com



Rachel Mott

Solicitor
023 8071 8083
rachel.mott@mooreblatch.com