MOORE BLATCH

TECH UPDATE

Summer 2017

VIRTUAL REALITY:

FACEBOOK AND OTHERS LOSE $500 MILLION

WI-FI PROVIDERS:

ARE THEY LIABLE FOR THE ACTIONS OF THEIR USERS?

BREAKING RECORDS FOR ALL THE WRONG REASONS

LESSONS TO BE LEARNT FROM TALKTALK

VIRTUAL REALITY:
FACEBOOK AND OTHERS LOSE $500 MILLION

A US Court has recently ordered social media site Facebook, virtual reality headset developer Oculus, the co-founder of Oculus and the former CEO of Oculus to pay Zenimax Media Inc $500 million after finding the defendants unlawfully used virtual reality technology belonging to Zenimax and the co-founder of Oculus broke a confidentiality agreement with Zenimax.

Facebook acquired Oculus in 2014. One factor leading to the acquisition was due to its advances in virtual reality headset technology. The jury found that Oculus carried out software copyright infringement when it used source code belonging to the video game developer id Software which is owned by Zenimax, to launch its own virtual reality headset.

It was alleged that the co-founder of id Software took intellectual property belonging to id Software before he left the business to join Oculus as its Chief Technology Officer.

Whilst the jury found that none of the defendants misappropriated trade secrets belonging to Zenimax, a co-founder of Oculus was found to have breached a confidentiality agreement with Zenimax in the early days of building the Oculus headset.

Part of the $500 million damages were made up of the following:

- $200 million in respect of breaching the confidentiality agreement; and
- $50 million in respect copyright infringement.

It is unclear whether Facebook and Oculus will be appealing the verdict and whether the finding affects Oculus selling any further virtual reality headsets which are based on the technology originally derived from id Software. However, the case highlights the importance of ensuring any intellectual property used to develop software is developed independently of any intellectual property belonging to a third party and the importance of ensuring confidentiality agreements are adhered to even when employees leave a business.

Jasnoop Cheema
Solicitor
020 3818 5436
jasnoop.cheema@mooreblatch.com

MOBILE COMMUNICATIONS TECHNOLOGY IP COMPANY RECEIVES SIGNIFICANT FUNDING

AccelerComm Ltd, a company specialising in mobile communications technology, has received significant investment from leading intellectual property commercialisation company IP Group plc.

AccelerComm provides technology which overcomes the problems associated with the next generation of wireless communications (i.e. 5G). Moore Blatch provided the legal support to AccelerComm for the capital investment from IP Group. This is the third university spin-out transaction that Moore Blatch has advised on in the last 12 months; last year providing legal support for venture capital investment to BluPoint Ltd, another University of Southampton spin-out.

David Bright, partner, Moore Blatch said: "In the past few years we have seen a significant increase in technology related transactions. This is the third university spin-out that we have advised on in the past 12 months and we expect this type of transaction to become much more common. UK universities lead the way in many types of research and development, and by creating spin-out businesses they are able to commercialise this work, which is much more desirable than seeing the hard work picked up by businesses that had no role in its development. However, the legal issues can be very complex involving the university, the founders and an investment company with intellectual property, and particularly patent, considerations."

AccelerComm exhibited at Mobile World Congress in Barcelona from 27 February to 2 March 2017.

David Bright
Partner
023 8071 8035
david.bright@mooreblatch.com

BREAKING RECORDS FOR ALL THE WRONG REASONS

LESSONS TO BE LEARNT FROM TALKTALK

In what has become a stark reminder to all companies to take appropriate measures to protect customer data, TalkTalk has been fined a record £400,000 by the ICO for cyber security failings which Information Commissioner Elizabeth Denham has said, *"allowed hackers to penetrate TalkTalk's systems with ease".*[1]

In particular, TalkTalk was held to be in breach of the seventh principle of the Data Protection Act 1998 (DPA). The seventh principle requires companies to take, 'appropriate technical and organisational measures… against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'.[1]

The DPA contains provisions as to the level of security companies should implement in regards to the protection of data.

"The measures must ensure a level of security appropriate to – (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and (b) the nature of the data to be protected".

Oversights revealed

Between the 15th and 21st of October 2015, hackers were able to bypass TalkTalk's security systems and access the personal data of 156,959 customers. They were able to gain access to customer names, addresses, dates of birth, phone numbers and email addresses. And for 15,656 customers, the hackers were able to access bank account details and sort codes.

As a result of this breach of security TalkTalk revealed in May that the hack had cost the company £42m as well as 101,000 subscribers who left the company following the attack coming to light.

For TalkTalk this was a lesson in due diligence, as the facts of the case reveal a series of oversights by TalkTalk that, should they have been rectified, would have saved the company from all the subsequent grief.

The first oversight occurred when TalkTalk purchased Tiscali's UK operations in 2009. TalkTalk failed to identify that the system employed by Tiscali was outdated and vulnerable to cyber-attacks.

The second oversight was TalkTalk's failure to take a proactive stance on monitoring activity on its database to discover vulnerabilities.

The third oversight, which would have been remedied should TalkTalk have taken appropriate action concerning the first two issues, was that Tiscali's infrastructure included outdated database software which found sensitive information available via the internet. This made it particularly vulnerable to cyber-attacks, in particular an 'SQL injection', which was used to extract the aforementioned personal data.

In a 'salt in the wounds' moment, not only was the vulnerability exploited by the hackers identified in 2012, a fix was also developed and available in 2012.

A fourth and final oversight was TalkTalk's failure to adapt and update its systems after two previous cyber-attacks; one successful SQL injection on the 17th July 2015 and another attack between the 2nd and 3rd September 2015.

As a result of these oversights the hacks exposed well over 100,000 customers' personal data and led to what has been the ICO's biggest fine to date.

Lessons to be learnt

The overriding lesson to be learnt from this case was summed up by Ms. Denham, "Today's record fine acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers"

In its report the ICO said of the record breaking fine, that the, *"underlying objective… is to promote compliance with the DPA and… to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data".*

If anything should be taken from this case it is the need to be aware of, understand and take seriously the DPA. In this case one should not interpret the vagueness of 'appropriate… measures' referred to within the aforementioned seventh principle, as an excuse to apply the bare minimum cyber-security, but as a constituent element to be taken very seriously, lest one wishes to find themselves in a similar position as TalkTalk.

However, companies should also look forward to and be prepared for changes made within the EU's General Data Protection Regulation (GDPR), scheduled to become effective on May 25th 2018.

Besides from laying out new legislation to be aware of and comply with, one should take particular note to the punishment afforded to breaches of the GDPR. Article 83 section 5 grants the ability to apply fines which dwarf the current maximum ICO fines of £500,000, by increasing the maximum fine to €20m or, in particularly serious cases, 4% of global turnover.

In light of this, companies which process large amounts of personal data would do well to ensure all their systems are up to date and comply with the GDPR sooner, rather than later. And if companies are to learn from TalkTalk's mistakes it would be wise to not only ensure IT systems are up to date, but also staff are familiar with and have a healthy respect of the new legislation.

Finally, it is worth noting that while Britain's decision to leave the EU earlier this year may mean that, once Britain has formally left the EU, the GDPR may not apply to companies storing domestic data, it will still apply to those companies storing data from the EU. It is also important to note that the triggering of article 50 in March this year marks the start of two years of negotiations over a deal for Britain's exit from the EU. This means Britain will be fully subject to the GDPR when it comes into effect.

Dorothy Agnew
Partner, Southampton
023 8071 8078
dorothy.agnew@mooreblatch.com

[1] *TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack- 5th October 2016* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/
[2] *Data Protection Act 1998 https://ico.org.uk/media/action-weve-taken/mpns/1625131/mpn-talk-group-plc.pdf*

ANTI-MONEY LAUNDERING REGULATIONS

CHANGES MAY SOON AFFECT ONLINE LETTINGS BUSINESSES

There are an increasing number of businesses solely providing lettings services via online platforms and apps. Businesses purely providing lettings services should be aware the Government recently underwent a consultation in relation to the proposed Fourth Money Laundering Directive which when introduced as legislation will change how lettings agents currently carry out and assess anti-money laundering checks on landlords and tenants.

The Directive will apply to businesses which do not deal with the sale or purchase of properties but help to govern the landlord and tenant relationship – this will therefore also apply to businesses which provide lettings services via online portals or apps.

Currently the Anti-Money Laundering Regulations apply to estate agents which handle high risk property transactions or incorporate lettings as part of its business.

At the moment the Anti-Money Laundering Regulations do not apply to lettings, however if the Directive is approved then the regulations applicable to estate agents may be amended in the near future to also apply to lettings.

In light of possible changes of applicability to lettings agents, coupled with the on-going risk of cyber security and fraud, businesses which deal with landlords and tenants online should have appropriate procedures in place which will allow them to determine the identity of landlords and tenants which they deal with.

Jasnoop Cheema
Solicitor
020 3818 5436
jasnoop.cheema@mooreblatch.com

WI-FI PROVIDERS

ARE THEY LIABLE FOR THE ACTIONS OF THEIR USERS?

Many cafes, restaurants, hotels and shops provide free Wi-Fi to customers, this may often be provided free of charge with no or only basic security, sometimes there may be no password to connect the Wi-Fi or the password may be the name of the establishment.

As the provider, it is difficult to control the actions of users on an unprotected Wi-Fi, and the users could be infringing the copyright of others without the provider's knowledge or control.

Can such business owners be liable for the activities of their users on their Wi-Fi?

The recent decision of the European Court of Justice (ECJ) in McFadden v Sony Music Entertainment Germany GmbH has clarified the position for providers of both password-protected and unprotected free Wi-Fi.

Tobias McFadden ran a business selling and leasing lighting and sound systems in Germany. As part of his business, Mr McFadden provided free Wi-Fi as a way of promoting his business to prospective customers in his locality.

In September 2010, the Wi-Fi network provided by Mr McFadden was used to make recorded music available to the general public free of charge on the internet without the permission of the rights holders. Sony Music, who had produced the music recording, gave Mr McFadden formal notice of its rights over the recording.

In response to the formal notice, Mr McFadden sought a declaration before the Munich Regional Court that he had not committed any infringement. Sony made several counterclaims against Mr McFadden seeking damages for the infringement of its rights over the recording, an injunction and costs. The Court dismissed Mr McFadden's action and upheld the counterclaims of Sony Music.

The question that was referred to the ECJ was whether Mr McFadden was able to rely on the mere conduit defence for information society service (ISS) providers under the E-Commerce Directive. Under the mere conduit defence, internet service providers, website providers and some telecoms providers have a defence from copyright infringement and defamation if they are just acting as a "mere conduit" of information passing through their service.

In order to rely on the defence, the provider must prove that they did not:

- initiate the transmission
- select the receiver of the transmission; or
- select or modify the information contained in the transmission.

In Mr McFadden's case, The ECJ held that:

- Mr McFadden was not liable for infringement. The provision of a free-unprotected Wi-Fi service fell within the remit of the mere conduit defence, as the service was used to advertise the business.
- Significantly, the E-Commerce Directive did not prevent a person harmed by the infringement from seeking injunctive relief along with payment of associated costs.
- Any imposed injunction could include (a) examining all communications passing through the Internet connection (b) terminating the connection and (c) password protecting.

Consequently, business owners offering free wifi should look to follow these key steps in order to minimise liability for infringement:

1. Password-protect your Wi-Fi.
2. Have terms of use of your Wi-Fi – which make it clear that copyright infringement and other unlawful activity is not permitted.
3. Deal with any objections to material transmitted through the service promptly.

This is good news for retailers and all other business owners who provide free Wi-Fi for their customers. However, it doesn't mean that they are completely safe. Retailers should follow the key steps above to ensure that they fall within the scope of the regulation and can therefore rely on the mere conduit defence.

Dorothy Agnew
Partner, Southampton
023 8071 8078
dorothy.agnew@mooreblatch.com

GENERAL DATA PROTECTION REGULATIONS: A SUMMARY

The new General Data Protection Regulation (GDPR) will become directly applicable in all member states on 25 May 2018. It will create clarity for businesses by establishing a single set of rules across the EU.

The GDPR will replace our existing data protection legislation and will change the rules concerning processing of personal data.

These changes will significantly impact businesses that process personal data. Set out below is a summary of the key concepts of the new GDPR:

1. When does it apply?

The GDPR takes effect from 25 May 2018.

2. Who does it apply to?

The GDPR is a single legal framework that applies across all EU member states. Non-EU data controllers and data processors will be subject to the GDPR if they offer goods/services to data subjects in the EU or if they monitor data subjects' behaviour and this takes place within the EU.

3. If I'm relying on consent to processing, what form consent is acceptable?

Like the current data protection legislation, processing of personal data under the GDPR must meet one of the fair processing conditions. Consent is one of these conditions. Under the GDPR consent to the processing of an individual's personal data must be freely given, specific, informed and unambiguous and must be shown by clear affirmative action. An individual's explicit consent is still required to process certain categories of personal data. The burden of proof will be on the business to show that consent was validly obtained. Where content is relied upon it will need to be obtained to all processing purposes and may be withdrawn at any time. Consent to processing/using an individual's data may not be a condition to signing a contract or providing a service. If there is a "clear imbalance" between the parties, consent is presumed not to have been given freely.

4. How do I work out if my processing is lawful?

Businesses are responsible for assessing the degree of risk that their processing activities pose to data subjects.

Data protection by design and by default is a requirement under the GDPR. When deciding on the way a data controller will process personal data and when processing personal data the business must put in place appropriate technical and organisational measures to implement the data protection principles and to put safeguards in place to protect the privacy of the data subjects.

Businesses must perform privacy impact assessments before carrying out processing that uses new technologies. The national public authority responsible for monitoring the application of the GDPR (supervisory authority)will publish a list of the kind of processing activities that require a privacy impact assessment. Privacy impact assessment will be required where processing is likely to create a high risk to people's rights and freedoms, particularly where the processing uses new technologies. Where an impact assessment indicates that processing would result in a high risk to individuals, then business must consult with the NDPA before the processing takes place. Standardised icons may be used to indicate important features of the data processing activities.

5. What if I operate out of several offices in the EU?

Where a business has several offices in different EU countries, the business's main office where cross-border processing is involved will be the one responsible for processing activities.

6. Do I still need to notify/register?

Businesses are no longer required to register their processing of personal data. Instead of registration businesses must keep detailed documentation that records their processing activities. The information that they record is specified in the GDPR. Data processors must keep a record of their processing activities – the GDPR specifies what this record must contain. These obligations do not apply to organisations that employ fewer than 250 people unless the organisation is processing sensitive personal data or the processing is likely to result in high risk to individuals.

7. Do I need to appoint a data protection officer?

In some circumstances controllers or processors must appoint a data protection officer. Almost all public authorities and organisations that systematically monitor individuals on a large scale (including those using big data analytics for online behaviour tracking or profiling) must appoint a data protection officer.

8. Do data processors have to comply?

Yes Data processors must meet certain compliance obligations under the GDPR.

9. Do I need to notify breaches?

Businesses must notify the supervisory authority of data protection breaches without undue delay and where feasible within 72 hours. If the breach is likely to result in high risk to individuals then (subject to certain exceptions) data subjects must be informed without undue delay.

10. What is Pseudonymisation?

The GDPR introduced a new concept of Pseudonymisation. Pseudonymous data – that is data which has been processed so that it can no longer be attributed to a specific individual without additional information – is personal data but is subject to fewer restrictions if the risk of harm is low. Any "key" that is required to identify data subjects from the coded data must be sept separate and secure to prevent accidental re-identification of the coded data.

11. Are BCRs recognised?

The GDPR formally recognises binding corporate rules. These will require the supervisory's authority's approval, but the approval process should be less onerous.

12. What rights do individuals have?

Individuals have the right to access their data. Businesses must reply to data subject access requests within one month from receiving the request and must provide more information than they have to provide under the current data protection laws.

Individuals have the right to request that businesses delete their personal data in certain circumstances.

Individuals have the right to object to the processing of their personal data eg to profiling.

Data subject have the right to obtain a copy of their personal data from the data controller in a commonly used and machine-readable format and to transfer those data to another controller.

13. What are the maximum fines for non-compliance?

For data controllers there are 2 tiers of fines that can be imposed on data controllers and data processors for breach of the GDPR. These maximum fines will be up to 2% of annual worldwide turnover of the preceding financial year or 10 million euros (whichever is greater) or up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is greater).

Fines for non-compliance by data processers of their obligations are up to 2% of annual worldwide turnover of the preceding financial year or 10 million euros (whichever is greater).

14. What are the powers of the data protection authorities?

The supervisory authority's powers will include power to carry out audits, require information to be provided and obtain access to premises.

Many businesses will need to make changes to their IT systems and their privacy policies to comply with the new data protection regulations. Effecting and implementing these changes may take time. Businesses should take steps now to prepare for the new regulations so that they are able to comply with the new regulations once they take effect.

Dorothy Agnew
Partner, Southampton
023 8071 8078
dorothy.agnew@mooreblatch.com

MOORE BLATCH

www.mooreblatch.com