Technology update

2016 has been a very eventful year. The impact of numerous legislative changes as well as, of course, some very significant political changes will be felt by the UK's technology sector for many years to come. It remains to be seen whether the impact will have an overall positive effect.

In this issue of the Travers Smith Technology Update we have chosen a few recent legislative and case law developments and sought to highlight the impact of these on the technology sector.

We wish you all a merry Christmas and a prosperous 2017.

Dan

Dan Reavill
Head of Technology Sector

E: Dan.Reavill@traverssmith.com
T: +44 (0) 20 7295 3260

Winter edition

EDITORIAL

Is London's crowning glory under threat from Brexit?

The UK tech sector has been the crowning glory of our economy over the last decade and maintaining this success will be vital for the UK post-Brexit. Policy announcements over the previous weeks, such as the rebuilding of the Varsity Line and an assurance from the Prime Minister that she will continue to seek concessions to innovation in the tax system, show that protecting the industry from some of the potential negative effects of Brexit is important to Theresa May's administration. However, the Government will need to listen and engage with tech businesses to ensure that this important industry is protected and continues to attract both talent and investment from overseas. Below are three of the most important issues facing the UK tech sector as a result of Brexit.

Recruitment

Brexit could make it more expensive and more complicated for UK tech businesses to attract and maintain overseas talent. Most tech sector companies employ software developers from the European Union and there is a worry that the added hurdles that Brexit will present to recruitment of overseas talent will lead to a "brain drain" of skills in this area. This problem is likely to be twofold. First, the administrative complications involved in recruiting EU citizens following Brexit may well place an expensive administrative burden onto tech companies, particularly start-ups, for whom new young talent is essential. The second issue is more subtle, which is that European workers may now feel unwanted in the UK; something that will almost certainly be exploited by foreign tech companies seeking to recruit from the same talent pool.

Fintech

The UK has been at the forefront of the development of fintech, supported by Government initiatives to encourage investments in this fast-growing area. But with Brexit threatening the all-important "passporting" scheme within the financial services industry, this may change. Passporting has been essential to UK-established fintech companies, helping them to easily expand their businesses overseas. It also enabled non-EU businesses to set-up a single base in the UK from which to provide regulated services throughout the EU. Without these concessions such businesses may have to set up a further subsidiary within the EU from which to service the European market.

Data Flows

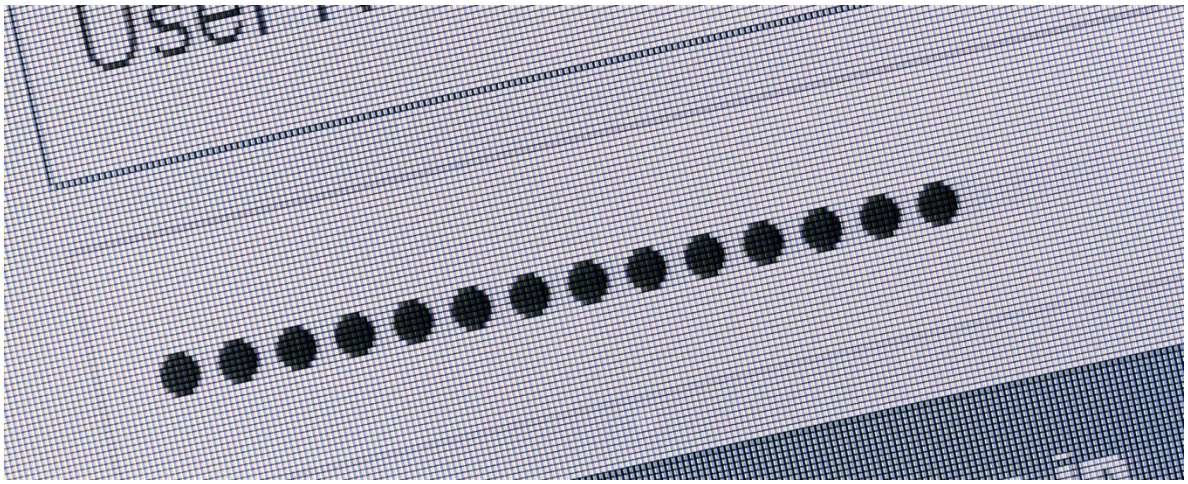
Technology businesses rely heavily on personal data and depend on the ability to transport data internationally. Brexit threatens UK tech companies' ability to rely on this free movement of data, which could impede our competitiveness. The new European General Data Protection Regulation ("**GDPR**") is likely to come into force before Brexit, and to maintain free movement of data in and out of the UK, the Government will need to keep GDPR (or something very similar) in force post-Brexit. This is because, once the UK exits the EU, the best way to ensure continuing rights of data flows from the EU would be to receive a decision of "adequacy" by the European Commission. This decision is made in respect of countries that the EC feels provide an adequate system of data protection legislation – and this usually involves rather close imitation of Europe's own laws. But the Government may face push-back on this approach from those for whom the Vote Leave campaign hinged on sovereignty and a desire to reject European laws.

Louisa Chambers
Partner, Commercial, IP & Technology

E: louisa.chambers@traverssmith.com
T: +44 (0)20 7295 3344

Hannah Duke
Associate, Commercial, IP & Technology

E: hannah.duke@traverssmith.com
T: +44 (0)20 7295 3101



Cyber Security Directive

Autumn and Winter have seen a flurry of high-profile cyber security attacks on British businesses (see next article for details of the TalkTalk incident and the revelation that a security breach at Tesco Bank led to suspicious transactions taking place on circa 40,000 accounts in November). The Government has responded to the increased threat with a £1.9 billion commitment to cyber security defences, but the law is also developing in this area.

The GDPR will seek to bolster security requirements for data controllers and data processors, but another piece of EU legislation is also tackling this issue. The Network and Information Security Directive (the "**Cyber Security Directive**") came into force in August this year and the 21 month period for it to be transposed into English law is now underway.

The Cyber Security Directive imposes security standards on the IT Systems of two main categories of organisations: (i) providers of "essential services" in the health, transport, energy, water, financial services and banking sectors; and (ii) the providers of "digital services" (meaning online marketplaces, search engines and cloud computing services). This may sound similar to data protection legislation, but importantly, the Cyber Security Directive applies to all IT systems and data (rather than just personal data) at the relevant organisations.

Whilst the Cyber Security Directive looks to have a broad scope, it does not apply to all businesses that fall within the relevant categories listed above. Instead, each Member State will have a 27 month period (ending in November 2018) to establish whether a business in the relevant sector is subject to the implementing legislation in that Member State. This will be done in one of two ways: each Member State will either (i) set objective criteria (e.g. number of users) or, (ii) rather unusually, elect which specific organisations (from within the categories mentioned above) will fall within the scope of the implementing legislation. The Government is still consulting as to its approach on defining whether organisations will be "in" or "out" but the Cyber Security Directive is certainly something that a business operating in the sectors referred to above should keep abreast of.

As an aside, it is worth mentioning that Brexit could have an impact on the implementation of the national legislation effecting the Cyber Security Directive in the UK. The 27 month period referred to above would bring us to November 2018 and a withdrawal from the EU could take place in March 2019 (if the Government's position on triggering Article 50 in March next year is maintained). Whilst this potential date for Brexit is after

the deadline date for the implementation of the Cyber Security Directive in the UK, it is sufficiently close that the Government could take a stance on not implementing it. There is obviously a degree of guess-work on this point at present but, as with most things Brexit related, things will hopefully become clearer over time.

In any event, our view is that it is likely that even if a decision was taken not to implement the Cyber Security Directive in the UK, something similar would be needed in its place – cyber security is a key priority for the UK and it seems unlikely that the Government would allow the UK to fall behind its European neighbours in its regulation.

FOR FURTHER INFORMATION, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

James Longster
Senior Associate, Commercial, IP & Technology

E: james.longster@traverssmith.com
T: +44 (0)20 7295 3496

Protecting personal data after Tesco Bank and TalkTalk

The UK data protection regulator (the ICO) has now completed its investigation of the TalkTalk cyber-attack, and its report makes difficult reading for TalkTalk. Unfortunately, lessons may still not have been learned as reports of the recent cyber-attack on Tesco Bank suggest that the bank ignored warning signs that its vulnerable software (apparently in mobile apps) was being targeted by cyber criminals. We await to see whether these reports will prove justified.

£400k fine imposed on TalkTalk

The ICO has fined TalkTalk £400,000 (or £320,000 if paid by 1 November). This is the highest fine yet levied by the ICO. The ICO press release comments that TalkTalk had security failings which allowed the attacker to access customer data (including bank account details) "with ease", and that TalkTalk could have prevented the attack in October 2015 if it had taken basic steps to protect customer's information.

Recently appointed Information Commissioner, Elizabeth Denham, commented: "Hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk could and should have done more to safeguard its customer information…Cyber-security is not an IT issue, it is a boardroom issue."

Hacking often succeeds because of basic human error. So it has proved with TalkTalk. The ICO found that in spite of TalkTalk's expertise and resources, when it came to the basic principles of cyber-security, TalkTalk was found wanting. The ICO report says: "*For no good reason, [TalkTalk] appears to have overlooked the need to ensure that it had robust measures in place…*"

How did TalkTalk get hacked?

The attacker used a common technique known as SQL injection (to which known defences exist) to access data via three webpages which proved vulnerable – TalkTalk was unaware of the webpages, inherited in a 2009 acquisition, or that they enabled access to a database holding customer information. Moreover, TalkTalk was unaware that the installed version of the database was outdated, was no longer supported by the provider and was affected by a bug to which a fix was available. That fix (well publicised in 2012) would have prevented the successful attack. The company also suffered two earlier attacks in July and September 2015 (of which at least one was successful) which it failed to respond to.

What could TalkTalk have done better?

According to the ICO, TalkTalk should have been able to:

- Spot the web pages it had overlooked;
- Secure or remove them;
- Ensure adequate testing and monitoring (and react to threats quickly); and
- Apply the bug fix available since 2012 or upgrade to a newer version of software unaffected by the bug.

Previous highest ICO fines

- £250,000 on Sony Computer Entertainment Europe for failure to take adequate measures to protect against hacking (2013)
- £325,000 on Brighton Sussex University Hospitals NHS Foundation for failure to wipe hard disks containing sensitive patient data (2012)

These risks were well known by 2015 and the errors were classic stuff, so it is not surprising that a fine has resulted. We regularly see similar errors. Nonetheless, the ICO response is unusually forthright and, with the size of fine imposed, may mark the start of a more deterrent approach from this traditionally light-touch regulator – although the cost of resolving the incident, which TalkTalk has put at about £60m, might itself be quite an incentive to keep security up-to-date. It is a reminder of the importance of proper cyber-security for all businesses, no matter how large or small.

What about Tesco Bank?

The reports circulating about what may have happened at Tesco Bank suggest further ways in which the bank could potentially have done more:

- Analysts of online data had apparently found evidence of Tesco Bank customer account details being traded on the "dark web". Cyber security experts are routinely able to monitor such activity and, as good practice evolves, it must be arguable that holders of financially sensitive personal data, such as banks, have an obligation to positively monitor for such evidence of possible vulnerabilities in their security systems;
- A mobile app testing firm claims to have uncovered and told Tesco Bank of vulnerabilities – only to be rebuffed. Tesco Bank seems to get a lot of similar offers of support from consultants and seems understandably wary of engaging with such vested interests. However, no business can afford to be complacent, and if warnings are made their credibility must still be assessed and, where credible, taken seriously, if the business is to remain compliant with its legal obligations.

Higher fines in future?

As a footnote, it should be added that from May 2018 the new GDPR will have effect. While the basic obligation to ensure "appropriate" data security remains unchanged, the level of potential fines will increase substantially – to a maximum of the higher of 4% of worldwide annual turnover and EUR 20,000,000. A boardroom issue indeed.

FOR FURTHER INFORMATION, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Alistair Wilson
Consultant, Commercial, IP & Technology

E: alistair.wilson@traverssmith.com
T: +44 (0)20 7295 3345

Use of social media in advertising

In June 2016 guidelines on the publication by businesses of online reviews and endorsements were issued by the International Consumer Protection and Enforcement Network (presided over at that time by the UK's Competition and Markets Authority). The guidelines were published in light of research which showed that (i) marketing businesses were more likely to use individuals with social media influence (e.g. bloggers/vloggers) than traditional celebrities when advertising online and (ii) it was not always clear to consumers that the adverts were "paid for advertising". Adverts which are not clearly identifiable as such are likely to breach consumer protection law and advertising standards and the CMA has recently taken action against numerous companies in the UK to ensure that online advertising is clearly labelled.

The guidance from ICPEN states that individuals endorsing certain goods or services online must:

- disclose clearly and prominently whether content has been paid for;
- be honest about other commercial relationships that might be relevant to the content; and
- give genuine reviews on markets, businesses, goods or services.

The CMA have stated that the business being promoted, the marketing companies arranging the promotion and the publishers of online content all need to play their role and maintain trust online by ensuring that advertising and other marketing is clearly distinguishable from editorial content.

Separately, investigations by the CMA found that numerous companies were publishing fake reviews on their websites or "cherry picking" more favourable customer reviews for publication. For example, Wool Overs staff were instructed to publish only a selection of reviews on its website and none below "four stars". Practices such as these are considered to be deceptive by the CMA since they can have the effect of distorting people's natural buying decisions and reap commercial rewards for the wrong reasons. In an open letter to retailers dated 11 August 2016, the CMA stated that:

"*If your business's website allows people to review products or services – whether they are yours or someone else's – you should publish all genuine, relevant and lawful reviews. If the way you manage or present reviews misleads consumers, your business could be in breach of the Consumer Protection from Unfair Trading Regulations 2008 (CPRs), which prohibit unfair commercial practices that distort consumers' decisions.*"

Whilst the CMA's approach to misleading advertising practices, to date, has focussed on: (i) educating businesses (by way of open letters published online) and (ii) obtaining undertakings from companies breaching the legislation (i.e. that the company will refrain from such practices in future), it does have the power to enforce consumer protection law (which may lead to civil or criminal proceedings). It is also worth noting that an advertisement that breaches the CPRs is likely to breach the UK Advertising Codes which contain similar industry rules on making sure that marketing communications are easily identifiable.

FOR FURTHER INFORMATION, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Ashley Avery
Associate, Commercial, IP & Technology

E: ashley.avery@traverssmith.com
T: +44 (0)20 7295 3340

Direct Marketing – death of the soft opt-in?

Much has been said recently regarding the implementation of the GDPR and how it will have a significant impact on businesses. One point that has not received as much attention as it should, and this is partly because of a lack of information on the point from the Regulators, is the impact of the GDPR on the "soft opt-in" for marketing mailing lists (which is found in the Privacy and Electronic Communication Directive ("**PECR**")).

People involved in marketing will be familiar with the soft opt-in but, by way of summary, the soft opt-in currently enables a business to market its own goods and services to an individual without obtaining his/her consent where that individual has bought (similar) goods and/or services from the business.

The soft opt-in is used by a wide variety of businesses throughout a multitude of sectors and is a key element of some businesses' marketing strategies. GDPR is however unequivocal in its requirement for unambiguous and informed consent. Therefore the big question is: can GDPR and the soft opt-in co-exist?

Whilst it is possible that the soft opt-in *could* be retained as an exception to the need for consent, this seems unlikely given that there is an ever-increasing focus on obtaining "positive" or "opt-in" consents. The European Commission is currently reviewing PECR in light of GDPR and we expect a statement on the position soon. Until we have that additional information, we are in the dark on this point but many businesses are preparing for marketing strategies where a soft opt-in is not permitted.

It is also important to note that it is generally thought that businesses will no longer be able to rely on marketing consents obtained pre-GDPR which do not comply with GDPR. Businesses would therefore need to obtain GDPR-compliant (i.e. "opt-in") consent from each customer who currently appears on their mailing lists solely because they once bought a similar good or service from that business. Obviously, this may not be easy to achieve in practice – and thus many businesses will either have to get very creative when it comes to finding ways to obtain "opt-in" consents or they are likely to find that their marketing mailing lists rapidly become a lot smaller.

FOR FURTHER INFORMATION, PLEASE CONTACT

James Longster
Senior Associate, Commercial, IP & Technology

E: james.longster@traverssmith.com
T: +44 (0)20 7295 3496

Tax issues for the tech sector

While the Autumn Statement did not announce tax measures specifically targeting the tech sector, it continued the focus on long term investment in high skills areas with changes that will improve the tax landscape for the technology sector. The 'good news' includes: a restatement of the government's business tax "roadmap" with the rate of corporation tax dropping to 17% by 2020; the helpful simplification of the capital gains tax exemption for trading groups (the Substantial Shareholding Exemption rules); and an announcement that the government will look at ways in which it can build on the introduction of the 'above the line' R&D tax credits. Finally, a new 16.5% flat rate of VAT will be introduced from April 2017 for any businesses which are "limited cost traders" (for example, such as fast growing, labour-only businesses).

The 'not so good news' includes the introduction of two new corporation tax regimes (both coming into effect from April 2017) which (i) limit the tax deductions that large groups can claim for their UK interest expenses, and (ii) restrict the amount of profit that can be offset by carried forward losses to 50%. Another (albeit fairly predictable) announcement is the abolition of Employee Shareholder Status schemes for any arrangements entered into on, or after, 1 December 2016.

Non-domiciled individuals may feel encouraged by the government's plans to relax the Business Investment Relief scheme from next year (making it easier for non-doms to invest in UK businesses), but non-doms may be less pleased to hear that from April 2017 individuals who have been UK resident for 15 of the last 20 years, or who were born in the UK with a UK domicile of origin, will be deemed UK domiciled for all tax purposes.

FOR FURTHER INFORMATION, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Simon Skinner
Partner, Tax

E: simon.skinner@traverssmith.com
T: +44 (0)20 7295 3242

Ed Humphreys
Associate, Tax

E: edward.humphreys @traverssmith.com
T: +44 (0)20 7295 3462

Spotlight on the "gig economy"- is the concert nearly over?

The last few years have seen significant growth in the so-called "gig economy" as businesses seek to manage fluctuating customer demand and rising costs by engaging individuals on an ad-hoc basis to work as and when required. To this end, there is an increasing use of self-employed, agency or casual/zero-hours workers. Technology has made these flexible working arrangements easier, with new digital platforms enabling businesses to resource jobs quickly, with less need for advance planning.

Around 7.1 million people, or 22.2% of workers in the UK are now in "precarious" employment (self-employed, temporary or zero-hours work)[1], with half of the self-employed being in low pay, (taking home less than two–thirds of median earnings)[2]. Two fifths of large organisations (those with 100,000 employees or more) expect to increase their use of contingent workers in the next five years[3].

Whilst many individuals are content with such flexibility, in recent months a growing number of workers and representative bodies are voicing their concerns over what they see as one-sided arrangements which deny important legal rights.

These concerns reached the Employment Tribunal for the first time recently, when Uber fought, and lost, a case brought by two of its drivers. The drivers successfully claimed that they were not "self-employed" as Uber described them, but workers, and therefore entitled to worker rights, including national minimum wage and paid statutory holiday. The Tribunal decided that the level of control exercised by Uber over its drivers was inconsistent with self-employment. The label they had been given did not reflect the reality.

Uber is reportedly planning to appeal the decision, so this may not be the last word on the matter, but the case is being widely reported and appears to have prompted other "gig economy" workers to question their supposed self-employed status.

[1] Office for National Statistics/John Philpott
[2] Resolution Foundation
[3] EY Global

Deliveroo faced protests from some of its couriers this summer after announcing changes to its payment scheme which the couriers claimed would significantly reduce their earnings. Now the Independent Workers Union is seeking trade union recognition to allow it to negotiate pay on the couriers' behalf – a claim which relies on the couriers being "workers" rather than self-employed as Deliveroo classes them. If they are in reality workers then the couriers would, like Uber drivers, have the right to the national minimum wage and paid holiday.

Hermes is reportedly facing an inspection by HMRC into claims that it may be paying less than the minimum wage to its couriers. Amazon was recently the subject of an undercover investigation by the BBC which revealed drivers claiming they were being paid less than the minimum wage. Both Hermes and Amazon class their couriers as self-employed, but critics claim that this is inconsistent with the level of control exercised over them.

The future

At the moment, the spotlight is firmly on businesses whose workers believe that the "self-employed" cap they have been given simply doesn't fit. Many claim that such organisations can't expect to have the best of both worlds – the lower cost of self-employment but the benefit of retaining control over their workers. If other prospective claims go the same way as the Uber decision (assuming it is upheld on any appeal), then this has significant consequences for the future of companies which operate in a similar way - which may need to change their entire business model.

But could there be another solution? Theresa May recently launched a review of employment practices, to assess whether employment law needs to change to keep pace with the growing "gig economy". The review will look at six key areas, including the appropriate balance of rights and responsibilities for new business models. It is possible that a new form of employment status could emerge to fit the "gig economy" and enable it to continue and expand. Watch this space….

In the meantime though, companies which use any type of contingent workers, including casual, zero-hours or agency workers, or self-employed contractors, would be well advised to carry out a review to assess how they use their workers, the terms on which they are engaged, whether they are still appropriate and the potential risks for legal claims, in order to decide whether any changes need to be made. Given the recent trend for challenges by contingent workers who believe they are being treated unfairly, any business which uses them needs to be prepared to respond to such a challenge.

FOR FURTHER INFORMATION, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Tim Gilbert
Partner, Employment

E: tim.gilbert@traverssmith.com
T: +44 (0)20 7295 3207

Anna West
Professional Support Lawyer

E: anna.west@traverssmith.com
T: +44 (0)20 7295 3316

The Digital Economy Bill – is it still alive?

In 2009, it was announced in the Queen's speech that legislation would be passed to support the development of the UK's communications infrastructures, in recognition of the growth of the global digital economy. Seven years on and the Digital Economy Bill has still not been passed into law, however it does continue to progress and evolve.

The latest draft of the Bill attempts to address a far broader range of issues than first anticipated, including areas such as age-related TV licence fee concessions and the regulation of both direct marketing and data sharing. It is apparent from the report of the final meeting of the Public Bill Committee that some MPs felt the scope of the Bill should have been extended further again. Several potential additions to the Bill were discussed, including a clause to address the issue of the growth in the use of digital ticketing software to purchase concert tickets in large quantities, and a clause to facilitate greater accessibility to e-books.

The comments made in the House of Commons by a number of MPs in their final review of the Bill echoed the sentiments of their colleagues on the Public Bill Committee, that opportunities for legislative action had been missed. For example, several MPs set out their concerns regarding the failure of the Bill to address the issue of poor internet access in rural areas. The Bill is now under review by the House of Lords.

Fundamentally, e-business, e-commerce and the infrastructure supporting them in the UK are areas which by their very nature are continually developing and expanding. When it comes to the Digital Economy Bill, it would seem that there are almost limitless topics that perhaps could and should be addressed. That being said, there is a risk in trying to legislate for such a fast-paced sector whilst progressing at such a slow rate. In other words, the Bill may already have become outdated before it has even passed into law.

FOR FURTHER INFORMATION, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Dan Reavill
Partner, Head of Technology Sector Group

E: dan.reavill@traverssmith.com
T: +44 (0)20 7295 3260

Sarah Robinson
Trainee, Commercial, IP & Technology

E: sarah.robinson@traverssmith.com
T: +44 (0)20 7295 3349