myerson

Tech Lite

In this issue:

www.myerson.co.uk

0161 941 4000

Welcome to the Myerson 2020 Vision Tech Lite Newsletter.

Introducing this edition of Tech Lite is Carla Murray, a partner in our Corporate Commercial department. In this edition, we set out our 2020 vision for Tech this year and review the previous decade. Find out more in the video below.

At Myerson we have the experience and expertise to provide advice to those working within the IT, IP and Data Protection industries, in this issue our experts look at:

Tech-ing into the Next Decade

Normally at this time of the year we make a number of predictions for the year ahead and reflect on the results of our crystal ball gazing from the year before.

However, as we have entered a new decade, we take a look back over our past articles and consider what's ahead for the twenty twenties.

Migration to the cloud

We entered the last decade talking about the benefits of cloud computing. Over the last 10 years we have seen businesses slowly adopting cloud based solutions, with Cloud Industry Forum noting an 83 % increase in businesses using cloud from 2010-2017.

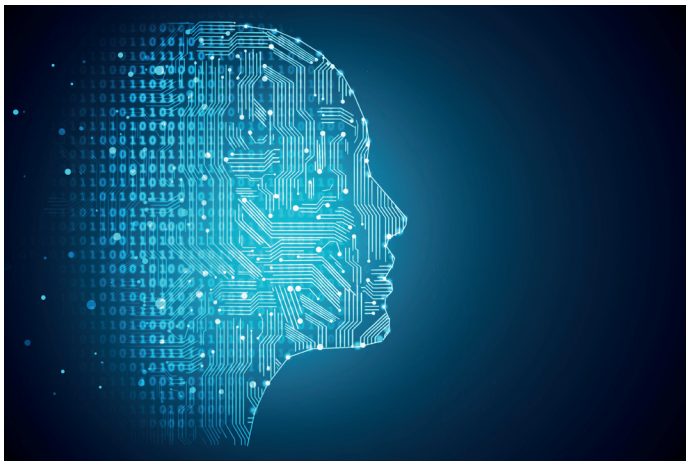
We haven't seen an instant "big bang" move to the cloud, but rather a gradual transition normally when businesses are moving software/service providers or are looking to implement new services/infrastructure.

We see this transitional process continuing, but we don't think we will see the end of the more traditional on site/licensing structures just yet.

Surge of Blockchain platforms?

Surprisingly, nearly all of the top 10 Blockchain platforms have been around since the early part of the last decade, and they don't just relate to Bitcoin. Despite this, we haven't seen Blockchain adopted as the norm in businesses.

Over the next decade, as we move towards smart contracts, Blockchain will become ever more prevalent, not least because of the chain of thought that Blockchain (or a similar technology) is the answer to data privacy and security risks. We anticipate Blockchain will be most active in the RegTech and FinTech sectors (regulatory/ finance/insurance) and the Healthcare sector.



Artificial Intelligence

At the beginning of 2018 we posed the question **"Are robots taking over?"**

Whilst we are not at the stage of Lost in Space, with robots intrinsically linked to humans, we're not far from it.

Tech Lite

Over the next decade we certainly anticipate that AI and machine learning will continue rapidly advancing and possibly displace the need for human labour/skills in certain tasks, streamlining businesses and creating efficiencies. But what robots won't do is take the place of human empathy and personal interaction, which businesses still need to thrive, otherwise it would be like replacing your dog with a dogbot?

Businesses will need to consider and exploit what differentiates them from their competitors which may include the adoption of AI to retain a competitive edge.

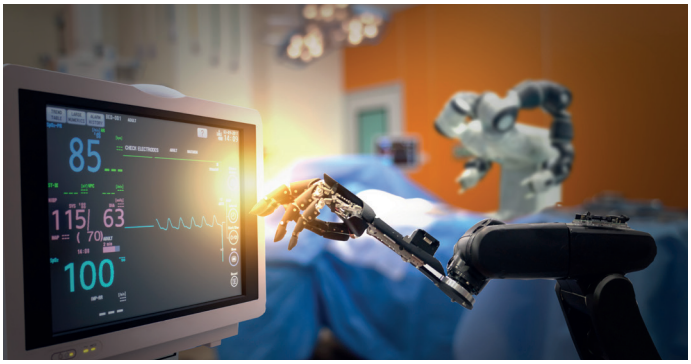
Agile business models and virtual sites

We believe that businesses will integrate more agile offerings not only into how their services are delivered but also how their employees work.

With technology comes flexibility and efficiencies, and we have seen that it can be just as easy (sometimes even easier) to work off site or from home rather than on site.

In the ever-changing commercial environment, businesses need to be quick to adapt, modify and change. Therefore, adopting an agile business methodology is likely to become the norm – with businesses adopting more diverse tech, they can continue to meet client requirements and employees' desires to have more flexible working arrangements, avoiding the work life balance 'juggling act'.

Automated heathcare



As mentioned, AI is becoming increasingly sophisticated, creating efficiencies in terms of time and lowering costs.

The use of AI in healthcare has the potential to transform some of the common issues faced by the healthcare sector. From apps which encourage healthier lifestyles, to using AI to improve early detection of diseases, the benefits of tech to the healthcare profession ranges from encouraging improvements to individuals' lifestyle prioritising health, to prevention of life-threatening diseases.

The potential here for tech to take centre stage is immeasurable. Already we are seeing healthcare providers offering free wearable devices in a bid to encourage healthier lifestyles. We anticipate that everything from healthcare research, training and patient treatment will adopt some form of AI in the next decade, such adoption bringing with it benefits to healthcare professionals and patients alike.

Privacy legislation keeping pace with emerging technology?

As much as we'd love to see this and despite advances in technology, this is still very much one for the future and a long way off.

Technology doesn't stay static and advances rapidly, however the same cannot be said for the rules and regulations governing such technology/services.

Law is notoriously slow at reacting to events/circumstances rather than seeking proactive change. The rules and regulations that protect personal data have struggled to keep pace with technological advances. One area in particular is the privacy issues caused by the collection and use of Big Data.

At the start of the last decade we queried the extent that the Privacy Electronic Communications Regulations (PECR) would alter how cookies are used, yet here we are entering a new decade awaiting updated legislation on this.

Tech Lite

We have recently seen case law further alter how consent must be obtained where all but non-essential cookies are used. We see this cycle continuing unless legislation changes pick up pace.

The questions and issues posed by the use of Big Data, e.g. geo-location services, have not been fully addressed despite the number and types of devices increasing with the ability to know your precise location and track you at all times. Whether it's the black box fitted to your car for your car insurance, Strava (or other fitness tracking apps), your gas and electricity supplier, so you can optimise you home heating, or Facebook following where you are via your smart phone.

Driverless Cars

Any car built in the last decade will have some automation, whether it's automatic lights, driver assist or early warning and collision systems. We have yet to see fully automated vehicles on the motorways and in our cities and towns (other than the testing of a few pod buses used to navigate Olympic Park and trial bus routes).

The technology requires further development and issues such as liability/responsibility need to be fully mapped out, therefore we are being a little more conservative than the Government (whose plans were to have such vehicles on the road as early as next year).

We expect to see automated vehicles hitting our roads by 2025, not least because there is still a lot to do to ensure that the law is up to date with this technology. We expect to see further updates in this area from the Law Commission over the next 6-12 months.

ICO Fines

Data privacy and the rights of individuals have taken centre stage. We've had a number of high profile data beaches, cyber-attacks and seen the ICO issue its largest fines.

Hot on the heels of the implementation of the GDPR, we will no doubt over the next decade (if not the next 12 months) see our first multi-million pound super fine issued by the ICO. It is simply a matter of time.

As we know the ICO has issued Notice of Intent to fine – Marriot £99 million and British Airways £183 million for their data breaches, although we are yet to see what the final figures will be.

Brexit

At the start of 2019, we boldly predicted that Brexit would or would not happen in 2019. We start the beginning of the year off knowing that Brexit has happened and as we move through the transitional period, we will be issuing regular updates on the effects and legal implications of Brexit and what steps businesses need to take.

Final Thoughts

The last decade has seen technology revolutionising not only businesses but our daily lives.

Over the next decade the advances in tech will no doubt be even more staggering but such developments will inevitably bring with them new challenges to businesses and legal compliance. Our specialist tech team will continue to monitor and blog on such advances, offering unique insights into the legal issues they may raise. Of course, only time will tell whether our latest predictions will come true.

Tech Lite

Copyright Ownership of Software Programs and Applications

What is copyright?

There are two common misconceptions about copyright:

1. it protects ideas;
2. it only arises if it has been registered somewhere.

Copyright in fact protects the physical form of an idea rather than the idea itself.

Copyright automatically arises when pen is put to paper (or a document is saved on the system), provided that the piece of work falls into one of the categories listed below and is original.

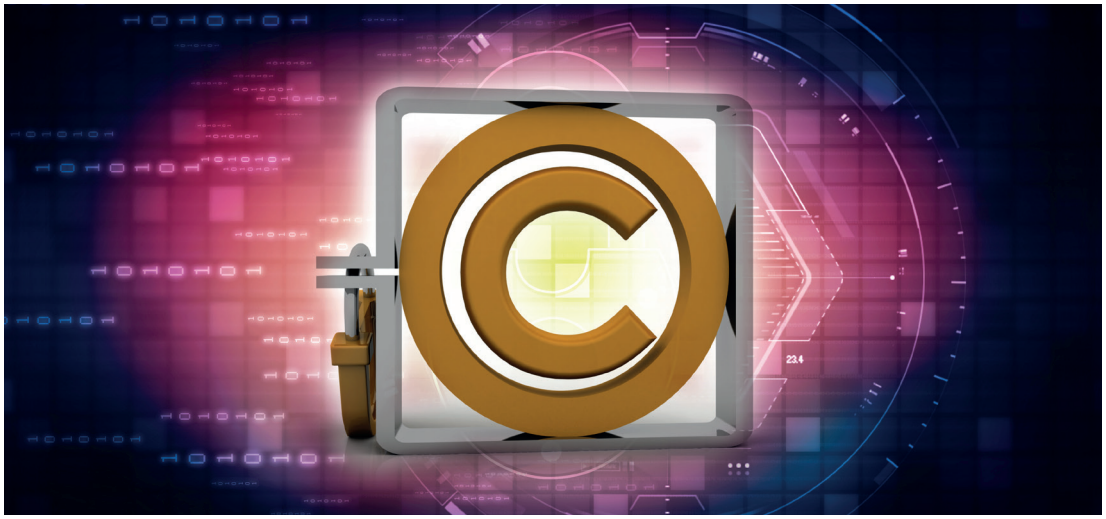
The categories of work protected by copyright are:

- literary, dramatic, musical or artistic works;
- sound recordings, film and broadcasts; and
- typographical arrangements.

Are software programs and applications protected by copyright?

Software programs and applications can be protected by copyright. Copyright may arise in relation to:

- the source code or object code;
- the preparatory design material leading to the development of the program or application;
- the general structure, sequence and organisation of the program/application;
- screen displays or other visual elements;
- on-screen text;
- music created by the program/application.



Tech Lite

Who owns copyright?

Generally, the owner of copyright will be the author/producer of the works. However, this is not always the case as the following exceptions can arise in the tech sector:

1. a program/application is created by a developer in the course of their employment. The employer will own copyright of the program/application;

2. a program/application is created by a third party developer. Unless there is a contract in place with the third party developer which assigns copyright to your business, the third party developer will own the copyright of the program/application;

3. if you develop your program/application prior to establishing your business structure or you do not have a service agreement in place with your company and you (as an individual) develop a program/application, you are likely to own the copyright;

Joint Ownership of Copyright

The question of ownership may be further complicated if a team of programmers are involved in developing the program/application. This can lead to joint ownership of copyright.

1. A work of joint authorship can arise where work is produced by a collaboration of people.

2. A collaboration can arise where people undertake jointly to create the copyright work with a common design as to its general outline and where they share the labour of working it out.

3. Joint authors must have contributed a significant amount of the skill which went into the creation of the work.

4. There is no requirement that the authors must have intended to create a work of joint authorship.

5. The respective shares of the joint authors do not need to be equal, but can reflect, pro rata, their contributions.

Why is it important to own copyright?

It's important to understand who owns the intellectual property rights in the programs/applications used within your business, not only because they will be an asset of the business but they may be critical to your business operations.

If you are looking to have a program/application developed, either for use in your businesses day-to-day operations or to licence and exploit it commercially, it's imperative you own the rights to the copyright, as otherwise your business may find that it is restricted in what it can do with the program/application.

If you are going to the expense of paying for development then you may want to ensure that you end up owning the thing you are paying to be developed

Out-Smarting Devices - The Government Announces Plans For New Legislation To Bolster Security Of Smart Devices

The Internet of Things (IoT) is a system of interrelated computer devices which allow data to be transferred without human-human or human-computer interaction. As illustrated by the onset of 'home hubs' like Alexa, to home security systems such as Ring, the IoT has an increasing presence in modern life.

A recent study carried out by the Waste and Resources Action Program (WRAP) found that each UK household will own an average of 10 to 15 IoT devices by the end of this year, with approximately 75 billion devices worldwide by 2025.

These products are purchased not just for their appearance but also as an aid to improve our quality of life, for example by easing the burden of daily tasks. However, does this increase in available devices bring with it a significant increased risk to personal data?

Smart doorbell maker Ring has come under scrutiny and faced questions over its handling of video footage, including:

- failing to inform consumers that their footage would be reviewed by others;
- permitting unnecessary access to footage; and
- not storing footage in an encrypted format.

The Government is finishing new legislation to improve the security standards of household IoT devices. Following the Department for Digital, Culture, Media and Sport's (DCMS) review and consultation on this area, the Digital Minister, Matt Warman MP, set out the DCMS's regulatory proposals on 27th January 2020, stating that:

"the DCMS will implement a staged approach to ensure that manufacturers have 'sufficient time' to implement the proposals effectively and sustainably".

The first stage of this new legislative approach will be to ensure that manufacturers comply with the existing Code of Practice for Consumer IoT Security so that "strong cyber security is built into these products by design" which echoes obligations under the General Data Protection Regulation and Data Protection Act 2018 which requires controllers to consider privacy by design.

What is not clear though is how onerous this regulatory burden will be for technology manufacturers, although the DCMS's response to the consultation is that it will advocate for "further requirements to be mandated" where necessary.

Tech Lite

The DCMS has outlined that all consumer smart devices sold in the UK are to adhere to the following IoT security requirements:

1. all consumer internet-connected device passwords must be unique and not resettable to any universal factory setting;

2. manufacturers of consumer IoT devices must provide a public point of contact so anyone can report a vulnerability and such reports must be acted on in a timely manner; and

3. manufacturers of consumer IoT devices must explicitly state the minimum length of time for which the device will receive security updates at the point of sale, either in store or online.

The measures are sensible given existing household devices have:

- been listening and recording private conversations around the home; and
- been hacked and locked people out of their homes.

Although manufacturers will be required to comply with any new and existing legislation and updates to existing codes of practice, the DCMS has not confirmed who will police compliance or what the penalties will be for manufactures who fail to comply. Therefore, the effectiveness of such measures will remain to be seen.

This aside, manufacturers of technical devices should not be complacent and should, if they aren't already, start to consider whether their contracts (including terms and conditions and supply contracts), processes and procedures need to be amended and updated to reflect the evolving regulatory requirements.

It will also be interesting to see whether the Information Commissioner's Office will be called upon to police this area to protect consumers data. If so, then manufacturers need to be alert to the possibility of the hefty fines that the ICO can impose (up to 4% of global turnover in certain cases) for failing to comply with data protection legislation.

Recognising The Potential of Crypto-assets and Smart Contracts

The UK jurisdiction taskforce of the LawTech Delivery Panel recently produced a 46-page report (the Report), in which it made potentially important conclusions regarding the enforceability of smart contracts and recognition of crypto-assets.

This article considers smart contracts and crypto-assets in a little more detail, including some of the ways in which they could be used in the technology sector and some of the issues which may arise with them.

What is a smart contract?

A smart contract is an agreement written in computer code which runs on a decentralised network such as Blockchain and is capable of self-executing when certain conditions are met.

As smart contracts are capable of automating execution via Blockchain or other similar technology, this can greatly reduce the centralised administrative burden and cost of managing the process.

Additionally, because Blockchain transactions are encrypted once they are approved, a permanent record of the transaction will be saved which can be relied on in the future, thereby reducing the risk of inaccuracies and fraud.

Blockchain technologies could be used to record an undisputable history of all aspects of a contract, including:

- the interpretation of the code which forms the basis of the operative provisions of the contract;
- the execution of the contract (and verification of electronic signatures via encrypted records);
- the monitoring and performance of the contract (including performance of key milestones); and
- the triggering and authorising of automated payments.

What does the Report say?

The Report made two key findings:

1. Crypto-assets (including virtual currencies) can be treated, in principle, as property; and

2. Smart contracts are capable of satisfying the requirements as being binding and enforceable contracts under English law.

The Chancellor of the High Court, Sir Geoffrey Vos, described this as a "watershed moment for English law... No other jurisdiction has attempted anything like it".

Indeed, the Report has been very warmly received by commentators, who see this as an innovative development and one which will place English law and jurisdiction ahead of the competition for agreements based on encryption technologies.

How can smart contracts be utilised in the technology sector?

Smart contracts have huge potential in the technology sector and are already being utilised, particularly in areas which rely on process-based decision making.

By way of example, the fintech sector alone could take significant advantages of smart contracts by improving processes and creating efficiencies for businesses, such as the automation of insurance (including claims handling and transferring policies), stock trading platforms, payment software and risk management tools.

What are the legal issues around smart contracts?

Whilst smart contracts can streamline the contractual process, the use of code invariably lacks the precision and complexity which the English language is able to convey in a complex contract and they arguably remain better suited to simple transactional contracts.

An example of this may be where a non-exhaustive list of circumstances (such as events which may frustrate a contract, or which may give rise to a termination event) is required. Whilst this can be expressed in a written form to convey the general principle (including non- exhaustive lists and guiding principles), the use of code can lack flexibility in this regard and may not prove to be a sufficient alternative on more complex arrangements.

Conclusion

The Report is a positive development in this exciting area of technological advancement.

However, smart contracts remain a developing area, both in terms of utilisation and enforcement.

Whilst there is significant potential in the use of smart contracts for determination of pre-agreed conditions to "self-execute" a simple contract, more complex agreements may be difficult to govern, and whilst the recent report suggests that smart contracts may be enforceable, they remain very much untested at the present time.

Trends in IT Outsourcing

Outsourcing has long been a common strategy businesses adopt when looking to reduce their overheads (including their headcount). IT outsourcing has been key for many businesses looking to increase their efficiency and pass some of the responsibility and risk involved in the management of IT systems to a third-party supplier.

Whilst this trend for outsourcing IT continues, there have been key changes in the sector over the last couple of years. Previously businesses tended to outsource responsibility for all their IT needs, and now we are seeking a more fragmented approach with businesses outsourcing some IT systems to a variety of suppliers and while retaining responsibility in-house for other aspects.

Why is IT outsourcing becoming more fragmented?

There has been a shift to sourcing IT from multiple suppliers (also known as multi-sourcing). This allows businesses to become more adaptable and agile. The flexibility of multi-sourcing means businesses can take advantage of innovative new technologies as and when they become available compared to a traditional single IT supplier structure which can be inflexible and slow to adapt. The competition between suppliers of IT systems also means businesses can take advantage of cost reductions.

Multi-sourcing has grown as businesses become more tech savvy and look to adopt increasingly advanced IT systems in-house. This has led to a better understanding of the available opportunities that a multisource model can offer. Increased in-house capability also means that business IT teams can manage the complexities of multi-sourcing.

What are the risks involved for businesses?

The key risk inherent in multi-sourcing is integration: the customer will ultimately be responsible for ensuring that all the suppliers and services involved work together. If things go wrong, the risk is that suppliers blame each other and disown responsibility. This can be a significant obstacle to getting issues resolved and appropriate remedies provided, leaving a gap that the customer is left to pick up.

The customer may also be expected to take on an increased burden of responsibility under their contracts with suppliers. The contracts needed to ensure multi-sourced systems operating together can lead to a complex framework of contracts for businesses to manage. Contracts will be needed with each supplier and should detail how the suppliers will interface not only with the customers system but third party suppliers and set out how the parties will cooperate with each other at an operational level.

Unless your contracts are appropriately drafted to cover this, it can make it difficult to manage changes in suppliers or services during the lifetime of the systems and to deal smoothly with exiting the arrangements when the time comes.

Conclusion

Although there are risks inherent in the multisource model and it may not be appropriate for all organisations, for an increasing number of businesses, the flexibility and increased control of multi-sourcing outweigh any potential downsides.

As technological innovation continues apace, for the time being at least this looks like a trend that is set to continue.

Because life is rarely **black** and **white.**

You know technology, we know technology law.
Get a lawyer who you can trust.

Call us today or visit our website
0161 941 4000
www.myerson.co.uk

myerson

Myerson Solicitors award winning law firm proudly ranked 'Top Tier' by The Legal 500.

THE TIMES Best Law Firms 2019 In co-operation with statista

ML AWARDS 2018 WINNER LAW FIRM OF THE YEAR MEDIUM

The LEGAL 500 UNITED KINGDOM LEADING FIRM 2019

Myerson Solicitors LLP
Grosvenor House, 20 Barrington Road, Altrincham WA14 1HB
Tel: 0161 941 4000 | lawyers@myerson.co.uk
www.myerson.co.uk | @myersonllp