FutureTech: How ‘future’ it is and what there is to worry about

There are lots of technology buzz words circulating, such as: ‘Cloud Computing’, ‘Agile Development’, ‘AI’, ‘Blockchain’ and ‘Crypto’. However, it is important to note that this does not mean that all such technologies have only just materialised, *writes Jagvinder Singh Kang, Partner, International & UK Head of IT Law at Mills & Reeve – and qualified software engineer*.

Cloud Computing or SaaS has generated a considerable amount of media attention in the last few years, and you would be forgiven for thinking that it was something new.

However, I have been advising on Cloud Computing arrangements for about two decades – previously it was called ‘ASP’ or ‘Application Service Provider’ models – and the National Institute of Standards and Technology formally defined ‘Cloud Computing’ and ‘SaaS’ about a decade ago in September 2011.

Therefore, one might wonder if it has been around for so long, why is it only in recent times catching the media attention? Certain ‘FutureTech’ is simply pre-existing technology concepts implemented with the benefit of greater computer processing power, storage, network speeds and bandwidth, to provide greater amenity.

Yet, it is not just Cloud computing which has been around for many years, as AI (or Artificial Intelligence) has also been around for decades. Combining AI with the increased processing power of the Cloud though, allows a significant realisation of benefits, as illustrated by the collaboration between the All England Lawn Tennis Club and IBM in respect of Wimbledon.

IBM’s AI technology uses machine learning and neural networks

to analyse videos of tennis players and associated crowd noise to generate ‘excitement scores’.

This combination is then used to allow the system to automatically identify match highlights within two minutes of a match being completed, to automatically serve up content to tennis fans. The benefits of such automated analysis is clear in terms of time and labour efficiency.

However, one of the problems with the use of AI and machine learning in particular is the introduction of bias into decisions which are made by systems, whereby the outcome may not reflect the desired outcome. This can be attributed to a number of issues, including the breadth of the data set used for training the system, or the personal views of the programmers implementing the underlying algorithms, or other external factors.

Staying with the IBM and Wimbledon ‘excitement scores’ example, IBM seeks to remove biases, such as may be introduced from fan favourite players having larger supporters compared to other players.

As more cheering may have to do with favouring the player, rather than the player having more ‘exciting shots’ compared to a lesser known player. Also, larger courts may amplify the sounds to generate more perceived ‘crowd excitement’ than smaller courts. Consequently, IBM processes initial automated outcomes through additional processing which seeks to remove such biases based on pre-programmed attributes.

This ‘de-biasing’ might not appear to the average individual to be that significant, as after all it is in the context of video highlights footage. However, it becomes particularly important when it gives rise to decisions about individuals which can adversely affect them – one only has to think about such biases occurring with the use of facial recognition systems, loan application decisions or recruitment decisions,

to understand the need for careful use of AI based systems.

In addition to data protection obligations with regard to the use of AI, which extend to transparency and accuracy of processing of individuals' data, the European Commission has also proposed a legal framework to regulate the use of AI, by considering the risks which the systems that use AI pose.

For example, the European framework is seeking to generally prohibit the use of real-time facial recognition systems for law enforcement purposes in publicly accessible places, whilst for other high risk systems, such as AI systems used as safety components in vehicles or medical devices, there will be mandatory requirements, including those relating to assessing risks and mitigations.

Consequently, it remains to be seen whether such accountability will transpire to be a good thing, or whether it will stifle the speed of innovation. If at this point, we return to our IBM and Wimbledon example again, there's yet another pitfall which 'FutureTech' brings.

IBM has confirmed that in one of the Wimbledon championships going back a few years ago, it used its AI to stop almost 200 million cyber security events.

Unfortunately, this is a reminder that cyber risks are now an inherent aspect which all businesses will need to deal with – more so with COVID bringing remote working to the masses, coupled with the adoption of the 'Internet of Things' or 'IoT' devices.

Cyber attacks are on the increase, whether from phishing attacks or ransomware, they are not going to go away. Unfortunately, as we have seen in the US recently, infrastructure ransomware attacks, such as the Colonial Pipeline incident which significantly disrupted fuel supplies, or the ransomware attack on one of the world's largest meat suppliers, JBS, are making criminal organisations determined

to move to more lucrative targets.

Ironically, technology innovation is also teaming up to make cyber attacks more difficult to trace, due to criminals shielding behind crypto-currencies, such as BITCOIN, for ransom payments – albeit that in the Colonial Pipeline case, some recovery of the ransom has been made.

Consequently, businesses cannot wait for a cyber attack to happen and then respond. They need to prepare their defences in advance. If they are hit with an attack, they need to ensure that they act in a timely manner from an operational and regulatory perspective.

In addition to the operational, financial and reputational impact to an organisation, there is also the impact to affected individuals, whether staff, consumer customers, patients or others, which businesses need to address.

As a data protection and cyber law specialist, I would also remind organisations that they need to take into account the UK GDPR – as in certain cases, this initiates a 72 hour countdown for notifications to the data protection regulator (namely the ICO) as well as affected individuals.

Such timings must be adhered to, to seek to avoid even more adverse financial consequences from regulatory fines and enforcement actions.
In closing, 'FutureTech' may not be 'brand new', but it is more powerful than it was before, so it offers great advantages for organisations, but only if it is used with appropriate responsibility and caution.

• Jagvinder Singh Kang is presenting a live TECHtalk webinar on 'Dealing with Cyber-breaches – a Data Protection perspective' at 10am-11.15am on Wednesday 30 June 2021 at a discounted rate for Business Weekly readers.

Visit www.bit.ly/techtalkplus quoting BW2021 or you may

contact Jagvinder for assistance with any IT, Data Protection or Cyber law advice by emailing Jagvinder.SinghKang [at] Mills-Reeve.com