MOORE BLATCH

TECH UPDATE

Spring/Summer 2019

CAN WE SUE OUR NEW ROBOT OVERLORDS?

THE RISE IN AI AND LEGAL LIABILITY

GETTING OUT OF ONEROUS CONTRACTS

THE BREXIT AFFECT

MOORE BLATCH'S TOP TIPS FOR SUCCESSFUL TRANSACTIONS

FIVE KEY TIPS

CAN WE SUE OUR NEW ROBOT OVERLORDS? THE RISE IN AI AND LEGAL LIABILITY

The rapid development of artificial intelligence (AI) and machine learning applications is seeing exciting new technologies being introduced to the market across a wide variety of sectors.

However, it is also bringing some worrying problems. What are some of the legal risks associated with AI and machine learning and what should you do to protect your business from these risks?

Alan Turing, considered by many to be one of the founding fathers of AI, published a paper in 1950 which discussed the possibility of machines which think and learn. Since then, the massive increase in computer processing power, the availability of large amounts of data and the reduction in cost of computing equipment and storage has enabled the growth of AI and machine learning.

In its Industrial Strategy White Paper, the Government defined artificial intelligence as "Technologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition, and language translation". The paper also defined machine learning as "a type of AI that allows computers to learn rapidly from large datasets without being explicitly programmed".

True AI is one that does not rely on pre-defined behavioural algorithms to reach decisions and meanings but can learn on its own and improve and enhance its capabilities and knowledge from past knowledge and decisions. Whilst true AI is still in its infancy, we are seeing advancement towards true AI in the form of machine learning software that uses complex behavioural algorithms and vast datasets to improve their skills and adapt themselves to our requirements.

Examples of this type of AI can be seen in:

- Home personal assistants like Apple's Siri, which uses machine learning to improve its ability to predict and understand questions and requests.
- Apple's HomePod which uses deep learning models and online learning algorithms to enhance and decipher speech and remove echo and background noise.
- The use of AI algorithms to improve diagnostic accuracy in breast cancer detection and reduce the number of false negatives.

However, despite the benefits of AI, some worrying problems have also arisen:

- Amazon ceased use of an internal AI tool it had created in 2014 to sort through job applications, after they found out that the tool had taught itself to prefer male candidates over female candidates and penalised CVs that included the words "women's".
- In autumn 2016, computer scientist Professor Vincent Ordonez noticed a pattern of gender bias in some guesses made by image recognition software he was building. In investigating the cause of the bias, he and his team tested two large collections of photos used to train image recognition software. He discovered these research collections displayed notable gender bias in their depiction of activities such as cooking and sport.
- Soon after Microsoft launched its AI chatbot called Tay into social media, it tweeted wildly inappropriate words and images. Peter Lee, Corporate VP, Microsoft Healthcare wrote "We are deeply sorry for the unintended offensive and hurtful tweets from Tay, which do not represent who we are or what we stand for, nor how we designed Tay." he explained "a coordinated attack by a subset of people exploited a vulnerability in Tay". Microsoft deactivated Tay within 24 hours of its launch.

It is clear that a regulatory framework is needed for successful and safe implementation of AI systems. Governments and collaborations of businesses and experts around the world are recognising the benefits of AI technology and the challenges associated with its use and are taking steps to research and recommend policies and laws on the use of AI technology. Examples of these include:

- The UK government advisory body, Centre for Data Ethics and Innovation, which has been tasked with investigating and advising on how we can maximise the benefits of AI and other data-enabled technologies.
- The Joint Research Centre (the European Commission's science and knowledge service), in collaboration with the European Institute of Innovation & Technology, is seeking to identify legal and regulatory challenges that using AI technology may bring for start-ups and research projects.
- The European Commission's High-Level Expert Group on Artificial Intelligence is tasked with advising the Commission on how to address AI challenges and opportunities through policy development and legislation.

Who is responsible for an AI system that causes damage or harm?

In legal terms, AI systems do not have legal personality in their own right; rather the business or individual that owns the AI or supplies the products and services that the AI system produces will be legally responsible for the AI system.

It is these businesses or individuals - not the AI itself - that will be the ones responsible for any wrong-doing or harm committed by the AI, or caused by any output of the AI system.

What are some of the legal risks arising from using AI systems?

- Inadequate knowledge can cause mistakes in results. Inherent biases in the datasets used can cause biases and discrimination in results.
- A business that uses an AI system to provide information and advice to its customers could be liable to those customers for loss or damage that they suffer if the system gives misleading or inaccurate advice.
- An AI system that publishes untrue statements that cause or are likely to cause serious harm to the reputation of an individual could expose the owner or operator of the system to a claim for defamation.
- A business that uses an AI system to filter a shortlist of candidates could be liable for discrimination if in selecting candidates the system deselects or disregards candidates, on the grounds of their race, gender or age in the same way as if it had been a human doing the selection.

What steps can businesses take to reduce these legal risks?

When developing or acquiring an AI technology, or when contracting with an organisation to use their AI system, consider taking the following action:

1. **Due diligence:** Conduct due diligence on the system itself and the underlying data used to teach the systems; find out whether the AI system's learning has been supervised or unsupervised.

2. **Testing:** Test AI systems thoroughly for bias and discrimination.

3. **Specification:** Carefully review specifications of the AI system. Understand the limitations of the system (where does its knowledge and its ability to learn begin and end).

   Understand what controls are in place in the AI system to prevent it from learning bias and discrimination and ensure continued compliance with data protection, employment and other relevant laws.

4. **Legal compliance:** Seek contractual assurances that the AI system does not and will not operate in a way that could cause your organisation to break current laws (including laws regarding discrimination and data protection).

5. **Insurance:** Ensure that you or your provider of the AI system has appropriate insurance to protect your business from some of the legal risks associated with AI systems that cause harm or damage.

6. **Support:** Consider obtaining support and maintenance for the AI to ensure that it continues to operate properly and within agreed parameters.

7. **Take-down:** If you discover that your AI system is operating unlawfully or causing harm, make sure that you can take your AI system offline quickly to prevent further damage.

8. **Oversight:** When implementing and using AI tools which are used to provide advice or are interacting with your customers, consider overseeing and managing their performance and output in a similar way to how you would oversee and manage a new member of staff.

Over the next few years, we expect to see a rapid increase in the number of businesses using AI and machine learning applications. Some of these will undoubtedly bring positive benefits to businesses and consumers alike.

There are also some worrying problems with this type of technology. A robust legal framework will help build trust in the use of AI systems, however, this may take time to develop. In the meantime, businesses should take proactive steps to reduce the legal risks.

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

GETTING OUT OF ONEROUS CONTRACTS - THE BREXIT EFFECT

Whatever your views on Brexit, the ongoing saga is recognised in many quarters as being bad for UK Plc due to great uncertainty as to whether Brexit will actually take place, and if so, on what terms the UK will leave the EU.

In particular, many businesses are worried that existing contracts will be adversely impacted by one or more "Brexit factors" such as a fall in Sterling, a rise in interest rates or the imposition of customs tariffs, making their contracts more expensive to perform and/or less profitable. In the worst cases, some contracts may become loss-making.

Against this backdrop, what does English law say generally about a party's right to terminate an agreement where it becomes more onerous or loss-making?

This right to terminate an agreement is covered by a principle called "frustration" – a principle recently invoked in probably the largest case to come to the courts involving the impact of Brexit on a commercial contract (Canary Wharf v European Medical Agency).

Simply put, the concept of frustration is that in rare situations, where a supervening event occurs without fault by either contracting party which would make enforcement of the contract unjust because circumstances have changed so radically, the contract will be automatically terminated and the parties will have no further obligations (or liability) to each other.

In the Canary Wharf case, the EMA had entered into an expensive 25-year lease in 2014 and now argued that the lease had been frustrated by Brexit due to:

- supervening illegality (it argued that EU law did not allow it to maintain a lease outside the EU); and
- failure of a common purpose – the intent was to provide a lease for the headquarters of the EMA which was now not possible.

Decision

The High Court was not impressed by these arguments and dismissed EMA's case, confirming that the lease had not been frustrated. This decision was based on a mixture of the facts and law: in relation to the facts, the Court did not accept that EMA could not deal with the lease under EU law, and felt that the EU itself could do more to allow the EMA to make use of the lease.

On a narrower legal point, it felt that supervening illegality under a foreign law was not part of the frustration test under English law and so was legally irrelevant in any event.

As for the common purpose argument, the Court pointed out that there was no real common purpose given that the parties had their own, opposing commercial aims. Moreover, there was evidence that EMA had benefited from a lower rent on the basis that it did not have a break clause in the lease – and so allowing the EMA to terminate early now would be unfair to Canary Wharf.

Commentary

In some ways the decision was not that surprising given that frustration is rare and very much "the exception to the rule" that clear contractual obligations need to be honoured by the parties: the Court was clearly influenced by earlier decisions which had stressed that the change in circumstances had to be so drastic that it would be positively unjust to enforce the original contractual terms.

Drafting escape routes to deal with Brexit

In order to try to protect your organisation's commercial position, either generally or specifically in relation to Brexit, there are two broad approaches that could be taken:

- **Specific events/consequences:** this would mean drafting, on a case-by-case basis, for certain consequences to flow from specific events. In the case of Brexit, for example, it could well be that a specified change in interest rates or the value of sterling would lead to a specific increase/decrease in the price of goods. Alternatively, if this is seen as too tough by the party that will need to pay an amended price to that originally agreed, the consequence could be an obligation to negotiate pricing (or any other term) and in the event of no agreement, either party having the right to terminate without any liability.

- **Triggering events for renegotiation/termination**: this approach would mean carefully defining an event or circumstance that would require the parties to negotiate an amendment to part of the agreement. If an agreement was not possible or not made within a reasonable period, either party would have the right to terminate without liability to the other.

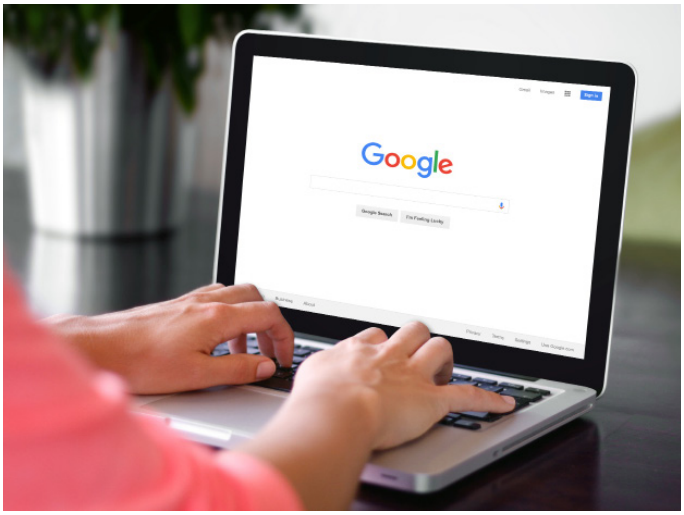
The key implication from Canary Wharf v EMA is that those arguing that Brexit is a frustrating event will themselves be frustrated by the Court's likely refusal to agree.

Far better than relying on the narrow principle of frustration would be to insert express clauses that either allow specific consequences to flow from a Brexit event or a more general obligation to renegotiate parts of the agreement, failing which the parties can terminate without further liability to each other.

John Warchus
Partner
020 8332 8631
john.warchus@mooreblatch.com

GOOGLE HIT WITH LARGEST EVER GDPR FINE OF £44 MILLION

Earlier this year, Google was fined £44 million (50 million euros) by the French data regulator for breaching the data protection rules under GDPR. To date, this is the largest fine issued since GDPR came into force.



Why was Google fined?

In May 2018 the General Data Protection Regulation (GDPR) came into force, requiring each European Union member state to introduce GDPR into their national legislation.

As soon as GDPR came into force, complaints against Google, citing failings to meet fundamental principles under GDPR, were filed by two privacy rights groups.

Google was subsequently fined by the French regulator principally for two main failures under the new regulations: lack of transparency and not obtaining valid consent for personalised advertising.

Essentially, the regulators found that individuals were not sufficiently informed about how Google collected data to personalise advertising.

Why is this fine significant?

At £44 million, this fine is the largest ever to be issued under GDPR. Considering that under the previous Data Protection Act 1998, the maximum fine that was permitted in the UK was limited to £500,000, Google's fine is comparatively large.

However, it could have been much worse. Under GDPR, the maximum fine is limited to the higher of £20m or 4% of annual global turnover; which means that for Google, the fine could have been closer to £4 billion.

The level of the fine issued against Google is a reflection of the gravity of Google's failings to meet the requirements which were introduced under GDPR. Even though the French regulator fined Google, the principles under which Google was fined against also apply to businesses processing personal data in the UK.

Key tips to avoid breaches

As the first major fine under the GDPR, this record-setting fine is significant. If your business collects or processes personal data, it is important to consider the following tips:

Ensure your business is transparent:

- Make the essential information clear to understand; and
- Make it easy for individuals to find the essential information. Information disseminated across a range of documents will not meet this requirement and individuals should not have to take 5 or 6 steps to access the information.

Obtain clear consent from individuals:

- Avoid using sweeping statements to obtain consent;
- Avoid using pre-ticked boxes to indicate consent has been provided; and
- Sufficient and clear information should be provided so that individuals are clear what they are consenting to.

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

TRANSACTION TOP TIPS

We are seeing numerous transactions in the TMT sector, many of which are a consolidation of the market. Additionally, a number of these transactions are bolt-ons with businesses adding additional expertise.

With this in mind, here are my **top five tips** for successful transactions and scale ups:

1. **Planning**: Plan both the transaction itself and the post-transaction period well in advance. Seek professional advice at an early stage to assist with structuring the transaction to suit the future ambitions and intentions of your business. Set your goals for the transaction at the outset and stick to them.
2. **Due diligence**: Complete targeted due diligence with your overall goals in mind. Use due diligence as a 'getting to know exercise' and focus on understanding your key assets.
3. **Internal teams**: Ensure that your internal teams are experienced in managing transactions and have the authority to make decisions.
4. **External teams**: Appoint professional advisers that you have a good relationship with, and who inspire confidence. Speak frankly with your advisers and ensure that they take instructions, not give them.
5. **Momentum**: Maintain momentum. Allocate sufficient internal resource to ensure that the transaction is well prioritised.

Thomas Clark
Partner
023 8071 6104
thomas.clark@mooreblatch.com

WHO DO YOU PAY?

It is easy to forget that invoices were once sent by post - a cheque was raised, dispatched by post, and delivered by the supplier to their bank to deposit. The bank would check and confirm the recipient's name and the payment would be completed.

Invoices now arrive by email, specifying bank account details for electronic payment, with payments near-instantaneous. It is faster, but is it progress?

When processing electronic payments, banks neither check the payee name, nor have an obligation to do so (Tidal Energy Ltd -v- Bank of Scotland PLC, 2014). Only the sort code and the account number are actually required.

Criminals know this. They know that if they can swap the "real" bank details for those of an account they control, they can pocket the payments.

A recent report by UK Finance concluded that in 2018, about £93m was stolen in scams of this type. We anticipate this figure may even be on the low side. Yet the report also concluded that 40% of businesses were unaware of the risks.

The technology sector is particularly vulnerable to these scams. There are lots of invoices, involving large sums, with limited face-to-face contact with suppliers. It's easy for criminals to intervene. At risk are payments to your suppliers, and also invoices you send to your customers. While your customers would usually remain responsible for any misdirected invoice payments, you are nonetheless in an awkward position if they insist they paid in good faith.

But how could criminals swap the payment information without you knowing? Simple - they take advantage of the whole process being electronic. For example:

- Sending an email with replacement account details. This might allege that details on the original invoice were wrong, or that the supplier has just changed banks. Crucially, the payee name doesn't need to change for the scam to succeed.
- Intercepting the supplier's outbound invoice email, and changing the payment details, before it reaches the recipient. Neither the supplier, nor the recipient, might have any reason to suspect that the details have been changed (until it's too late).

These scams may seem obvious and crude, yet they are succeeding on a large scale. Fortunately, there are simple precautions that can help protect you:

1. **Avoid using public WIFI hotspots:** They make it easier for criminals to intercept communications, and expose your devices to a greater risk of being manipulated.
2. **Know your suppliers:** Maintain an internal record of contact and payment details.
3. **Verify any new or changed payment details by phone:** Use a phone number from your own records (not from an email, or from the internet).
4. **Check invoices. Did you actually make an order?** Is the amount correct? Criminals often research these details to make a scam more convincing, but basic checks are still worthwhile.
5. **Tell your bank urgently if you suspect you have been scammed:** Occasionally, it may be possible to freeze the payment.

Unfortunately, if the criminals do succeed, there may be little you can economically do. However, if the sums involved are significant, we'd recommend a prompt review of your options.

Looking to the future, work is ongoing on a system to enable bank payees to be verified. But until that system arrives, significant risks remain.

Andrew Reid
Associate solicitor
023 8202 5021
andrew.reid@mooreblatch.com

MOORE BLATCH

www.mooreblatch.com