Protecting confidential information in an AI-led and augmented reality

13/04/2020

*By **Charlotte Walker-Osborn,** Partner and international head of artificial intelligence, international head of technology sector, Eversheds Sutherland (International) LLP*

Across the banking sector, the Bank of England and the Financial Conduct Authority predict that firms' utilisation of artificial intelligence (AI) solutions will triple in the next three years (BoE and FCA Joint Report on Machine Learning in UK financial services, 2019).

Firms are data-rich.This makes AI and more basic machine learning an obvious technological advancement, in processes such as fraud detection, anti-money laundering, decision-making, personalised financial planning.

So, how do firms protect the confidential information and data that is processed by AI technology?

Generally, AI technologies evolve through use. Training an existing model on new data gives rise to a new model whose properties and behaviour are modified by that data.

Often, for firms, that data is confidential in nature and it may also contain personal data. It is critical both to protect the confidentiality of the original data the AI will process (input data) and to protect the confidentiality of any derived data/output data the AI generates. It is also imperative to comply with privacy rules (which is outside the scope of this article).

Ultimately, the most pragmatic way from a legal standpoint is to protect the firm's and its customers' confidential information is through contractual obligations Such a concept is easy to convey in relation to input data.

Where the AI platform and data belong to different parties, the question arises as to which party should own the new intellectual property in the trained model and any derived data. There is no set rule. As with the fee structure, this is ultimately a commercial discussion between the parties. But, even if the firm does not own the derived data, it is important that the derived data can not be utilised in such a way (particularly with third parties) that the original confidential information can be derived or accessed by others. Again, setting this concept out in the contract will be key so ensure that the confidentiality obligations apply to all data, including the derived data.

Intellectual property – closing the loop-hole

If the AI company is to own the intellectual property in the derived data orhas a wide license to keep using it, it is imperative that the obligation to protect the confidentiality of the input data takes precedence above these rights.

As an overarching point in relation to data, intellectual property law struggles globally to deal with AI technologies.It is therefore likely that there will be new laws arising in many countries over the coming years.

A closed solution for your firm

Do not forget that it is possible to procure, build and contract for use of AI solutions which only process your firm's data or to procure an instance/version of the solution which – even if it has utilised other firms' data and/or public data – is a private version/instance for your firm. As a result, the confidential information and data your firm adds into the solution will only improve the instance of your firm's AI and, if contracted for in this way, cannot be used by other firms, third parties or even the AI company going forwards. This is an ultimate way for protecting confidentiality but has pros and cons, depending on what the AI is for.

Complying with new laws and guidance in this area

There are several laws and guidance notes already in place or coming into force which touch on obligations of confidentiality and protecting data, including from the UK Information Commissioner's Office, the European Commission and UK government.Guidance will emanate from the FCA increasingly over the coming years. It is important to keep a watching brief on these, to comply with them and place (where relevant) obligations on your AI provider to comply with them or help your firm do so in order not to breach applicable laws. This includes, where personal data is concerned, carrying out assessments as to whether data can be anonymised. If data is anonymised, clearly, this is a technical step that can assist greatly with protecting confidentiality.

AI technology and cyber-security

AI technologies reside on servers, whether on-premise or in the cloud. It is critical that a detailed analysis takes place early on for the technology set-up, data flows, and security arrangements. The analysis is broadly the same as for other technology projects, but is a critical step given the large amounts of potentially confidential information and personal data along with the potential sensitivity of the data and the results.

Close governance, transparency and auditability around the use of data/confidential information throughout the project is vital.This right should be contracted for, including how confidential information/data is treated at the end of the project (which may, depending on the solution, include expunging the data).

Conclusions

There are many technical, data governance and contractual steps which firms can and should take to protect the confidential information of both their firm and their customers when adopting AI solutions. The above is merely a snapshot of the key points. Ultimately, detailed analysis of the confidential information being placed in the systems and how derived data is created and used is at the heart of this. More than ever, contracting carefully around ownership, licensing, treatment/processing and usage of this confidential information is crucial, as is close governance of the project throughout.

‹ Implementing new technology and the need for updating management styles
› How COVID-19 killed cash and what will repace it.

Implementing new technology and the need for updating management styles

13/04/2020

*By **Roel Jansen,** Head of Marketing and Business Development, five°degrees*

'Evolve or become irrelevant' has been the mantra in the banking and finance sector for some time now. The challenge of updating legacy systems and transitioning to more agile, innovative technology has been at the forefront of most banks' priorities within recent years.