

A reflection of FIMA Connect 2024

08 May 2024  Kay Chand

Kay Chand, Partner in Browne Jacobson's digital and sourcing practice, participated in a panel discussion titled "Ensuring Ethical Usage of AI/LLMs: How to Choose the Right Architecture and Partners" at the FIMA Connect 2024 event. In this article, Kay shares her insights and reflections on the topics discussed.

The Regulatory Landscape

We are very early days in terms of regulatory development and approach for the UK but what is already clear is that the EU and UK are taking different approaches. The EU will legislate the technology categorising it as high or low risk. It will even ban certain types of AI technology.

We know that at the moment, the UK is leaving this to the regulators such as the FCA and ICO, and will take an approach based on use cases.

Therefore it could be argued that the EU approach is that AI is something that we need to be fearful of and treated with caution. Whilst the UK, whilst not throwing caution to the wind, is taking very much a pro-innovation approach. Although there are some recent murmurings that this approach may be starting to shift somewhat.

The Consumer Duty is based around principles of:

- good faith
- fair value
- good Customer outcomes

Therefore ensuring accuracy and reliability of the AI technology and eliminating bias will be key in ensuring compliance. This will involve continuously testing the AI technology and ensuring appropriate KPIs are in place with service providers in order to measure the level of accuracy and reliability such as the accuracy of automated decisions, probably assessed against some pre-determined criteria.

Security processes and procedures will also need to be updated to manage new and emerging threats such as through increased fraud of customer bank accounts through sophisticated scams for example using deep fakes technology.

Supplier Onboarding

In addition to the questions already asked by the procurement teams of financial institutions as part of the supplier onboarding process, many of which will still be relevant, one of the things to ask is whether the proposed solution is actually utilising AI. This might not be clear and so it will be for the customer to drill down by asking the right questions in this regard to determine the extent to which AI is being used in the solution.

Customers should also be asking on what data the AI has been trained, is it open or closed data and from which third party sources. This could have implications for ownership of generative IP created from the AI that customers ought to have early site of in order to avoid complex issues later down the line. This could also have implications for bias if the data on which the solution has been trained is flawed.

Other questions to ask might be how has the AI been tested and how often and what commitments will be given to ongoing testing.

Customer's may also wish to request a request a longer term pilot to given them time to properly test the system before making a commitment on a long term procurement. This will most likely be on a non-production environment.

The supplier might also be asked what service levels it is willing to sign up to for example regarding accuracy and reliability and what ongoing testing and monitoring will the supplier provide.

Thinking further down the line, will new versions and releases be tested with the same rigour?

AI will require closer and more frequent monitoring in my view as it will continue to learn from the data fed into it and at any given time, the results and accuracy could become skewed. Therefore greater governance will need to be applied and supplier should be asked about their governance commitments.

BCDR planning, processes and procedures should probably also require consideration from a new lens. Typically we have thought about a disaster as a flood or fire. But what if the system went rogue and let's say incorrectly rejected a vast amount of lending applications in a short time. Would that constitute a business continuity or disaster event such that the automated decision making is paused and an alternative system kicks in?

What processes and procedures should be built in to keep the system in check? This may result in a more robust governance regime with more frequent meetings with service providers and the provision of additional management information for example on automated decisions.

Consideration will also need to be given to financial risk and the risk of reputational damage and what commitments the supplier is willing to give in this regard.

Key contact

Kay Chand

Partner

Kay.Chand@brownejacobson.com

+44 (0)330 045 2498

Related expertise

Services

Data protection and privacy

Intellectual property

Regulatory