Your World First

C/M/S/
Law.Tax

Artificial Intelligence

Does your business really need AI?

Where the business case and control parameters are proven and effective, AI can demonstrably deliver significant productivity, efficiency and accuracy gains. However, as tempting as it may be for organisations in increasingly competitive marketplaces to jump headfirst into adopting or deploying AI, should your company 'take a breath' before diving in? This paper outlines the main points from the recently released National Cyber Security Centre guidance on assessing intelligent tools for cyber security – a valuable opportunity for businesses of any size to reflect on how they should (or equally, should not) adopt or deploy intelligent technologies.

Can AI really help my business?

Will it really bring any benefit? What factors should you consider in selecting a solution? How can you compare tools when you might not understand how they actually work? Is your organisation comfortable with the various risks adopting AI may bring?

Key to selecting the right intelligent tool for your business is an understanding of the kinds of issues you are intending for the tool to solve. In some cases, augmenting existing processes may provide a satisfactory result. If not, when you start shopping around for a new solution, detailed knowledge of your 'issue' (including any potential effects of the proposed solution being incorrect) will provide a useful basis for comparing AI tools. Comparing smart technologies may not be a simple proposition. Unlike more mature software markets, intelligent tools vary hugely in their features and level of customisation required. Instead, expect a more resource-heavy process where your business should converse with vendors and take time to assess options available; running the same task and analysing side-by-side results might be the best way to compare.

Nature of the technology

AI tools range from full automation to supplying individuals with information to supplement their own decision-making. Choosing where your organisation sits on this continuum will be a question of balancing several factors. On the one hand, full automation will limit the risk of, for example, user error or the introduction of human bias. On the other, full automation means that your company needs to be comfortable giving full responsibility to a tool, which in some cases may be 'black boxed'. You may be unable to fully understand how it comes to its decisions. In these situations, your business will need to consider whether the corresponding lack of transparency or apparent lack of control poses an unacceptable operational risk.

You may need to consider governance processes and resourcing, alongside ethical and legal considerations, not least any applicable data protection restrictions. The GDPR, for instance, restricts the use of algorithms in certain instances. You may need to design control frameworks and give thought to how technological and organisational measures need to adapt to the intelligent tool's learning over time and to changes to its risk profile. You should consider how temporary unavailability of the tool may affect your business, and what continuity measures should be put in place.

Driven by data

Understanding how a product deals with your information is an essential factor in selecting your AI tool. In many cases the decision-making quality of the AI tool will only be as good as the data fed into it. Many vendors synthetise data across their customers and/or third party sources, which has the benefit of allowing the smart technology to 'learn' from a larger data set. However, this does impose some risk. For example, use of the third party data may (if unrepresentative) introduce a bias. A number of considerations relevant to the implementation of SaaS agreements apply equally to the deployment of AI. For example, ensuring data is secure in transit and at rest, controlling where your data will be stored and undertaking appropriate due diligence on the vendor.

When it comes to your own data set, knowing what makes high quality data will improve your output. Ensuring your data set is comprehensive, diverse and accurate will help you get the best return from your AI tool.

Overall gain in security?

Following implementation of your AI tool, you should adopt a process of evaluation to ensure the tool remains within the scope of work it was specifically obtained for. Assessing whether the data does 'enough' to provide you sufficient information to make the decisions the tool was deployed for should be an ongoing consideration. Importantly, having a 'plan B' – fixes and fallbacks for where the tool is down – will enable your business to continue to operate in case of failure.

Should you do it?

Businesses need to consider carefully whether the introduction of AI is the right choice, before undertaking an exercise to adopt it. In many cases, this will require significant investment, both in terms of capital and resources. Adapting existing processes and procedures may bring similar benefits without the added risk and outlay associated with the introduction of a smart technology. However, the desire of many businesses to implement or deploy AI is rightfully driven by the positive change that many have witnessed it bring across industries. In each case, the National Cyber Security Guidance is a valuable reminder to undertake appropriate diligence prior to, and ensuring an appropriate governance and control framework is in place following on-boarding a new smart technology.

Contacts

Dr Rachel Free
Partner
T +44 20 7067 3286
E rachel.free@cms-cmno.com

Ian Stevens
Partner
T +44 20 7367 2597
E ian.stevens@cms-cmno.com

Elizabeth Vincent
Associate
T +44 20 7367 2195
E elizabeth.vincent@cms-cmno.com

© CMS Cameron McKenna Nabarro Olswang LLP 2019. 1907-0102194-1