Partners in Performance®
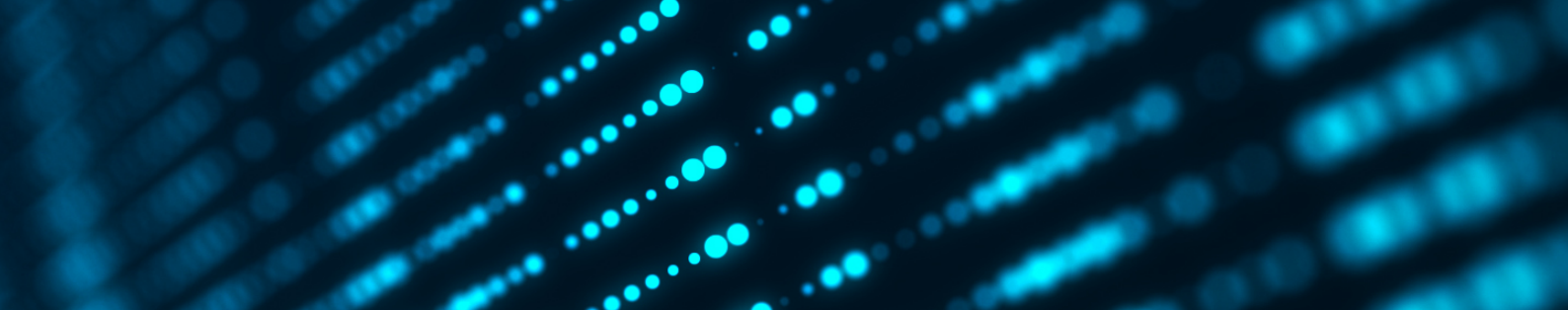*Unleashing potential* | Lasting impact

Navigating the ethical concerns of AI and data use

Data and AI offer significant benefits, but their widespread use creates new organisational challenges and security risks. Setting ethical boundaries is crucial for avoiding adverse outcomes. Furthermore, educating staff and having regular ethics discussions on data ownership, privacy controls and accountability is imperative to thrive in an ever evolving technological landscape.

The benefits of data analytics and artificial intelligence (AI) in driving productivity, creating valuable insights and improving service outcomes are extensive. AI is expected to be utilised at every level of high performing organisations within the next few years.

Boards and CEOs face a challenge in understanding the full extent data and AI software are used by staff to perform their role, creating new risks to manage. Most organisations have been improving internal data access controls over recent years, however the risk extends far beyond whether the user can use the data. Instead, it relates to how data is used and should it be used for that purpose.

While the word 'ethics' is thrown around a lot, real conversations about what is ethical behaviour in a rapidly changing data ecosystem are rare. When it comes to your organisation's data and AI strategy, going beyond "Can I?" to "Should I?" is vital.

Data privacy regulations provide "Can I?" boundaries, but regulators are finding it challenging to keep up with the pace of innovation as it can take years for governments to develop and finalise privacy legislation. These regulations will need to keep evolving as technology use and capabilities grow.

Setting ethical boundaries for data and AI – why does it matter?

Just as data analytics has permeated every facet of organisations, AI is similarly about to explode with potentially far greater consequences. AI will expose any inappropriate or ill-considered data use. If data hasn't been properly controlled then it could lead to unintended adverse customer outcomes, reputational damage and financial consequences. Organisations must ask themselves:

• What legal or regulatory obligations must they meet?

• What are the possible customer or employee outcomes from collecting, storing and using the data? Could they be adversely impacted?

• What data governance and AI frameworks are in place, including for systematic deletion of data?

Organisations who cannot answer these questions and do not set explicit boundaries around data and AI leave these decisions to the discretion of staff and suppliers. Their risk appetite and ethical boundaries may be surprisingly different than those of organisational leaders. This can result in missed opportunities due to uncertainty around what is acceptable. It can also lead to inappropriate data use. Relying on existing codes of conduct is insufficient for addressing these risks, and generic data principles often have minimal impact on behaviour.

This is especially pertinent for internal data privacy controls. Only those who need the information to fulfil their responsibilities should have access to it, proactively containing the security risk.

Managing the issue of bias in data and AI

The pervasive issue of bias in AI looms large. The web of unknown inputs from various data sets gives rise to a pressing concern: the potential for explicit and implicit bias. Biases entrenched within the underlying data can subtly infiltrate the algorithm, leading to unintended consequences. Amazon famously trained an AI tool to vet applicants and speed up the recruitment process, using internal data that stemmed from submitted resumes over the last decade. A problem arose when the algorithm prioritised male candidates and penalised resumes with the word 'women's' (such as 'women's chess club'), as the data set was biased due to male dominance in the technology field. While Amazon edited the algorithm to remove this bias, it had no guarantee the AI would not devise another biased way to sort candidates, ultimately leading them to scrap the project.

Furthermore, the reliance on secondary sources and data sets can introduce questionable logic and biases into conclusions. Discerning what constitutes a legitimate source and understanding the rationale AI employed to reach a conclusion becomes crucial for organisations committed to ethical decision-making. Overcoming these challenges requires transparency, ongoing scrutiny and testing to build trust into AI tools, as well as the development of robust frameworks and guidelines.

What is the impact of setting ethical boundaries for data and AI?

Every company is likely to set different thresholds and build unique frameworks, depending on the nature of their products, services, customer profile and brand promise. However, similar questions on data and AI use are likely to appear for all organisations in this development, key among them:

1. How are you using data and AI in your organisation and for what purpose?

2. What data is collected and stored and why?

3. How long is data stored for and why?

4. Have your expectations and standards been communicated to staff and suppliers? Can you prove they are adhering to your expectations?

Answering these questions helps build a framework for ethically managing AI and data while directly influencing customer, risk and financial outcomes as well as who the organisation attracts in terms of staff, customers and partners.
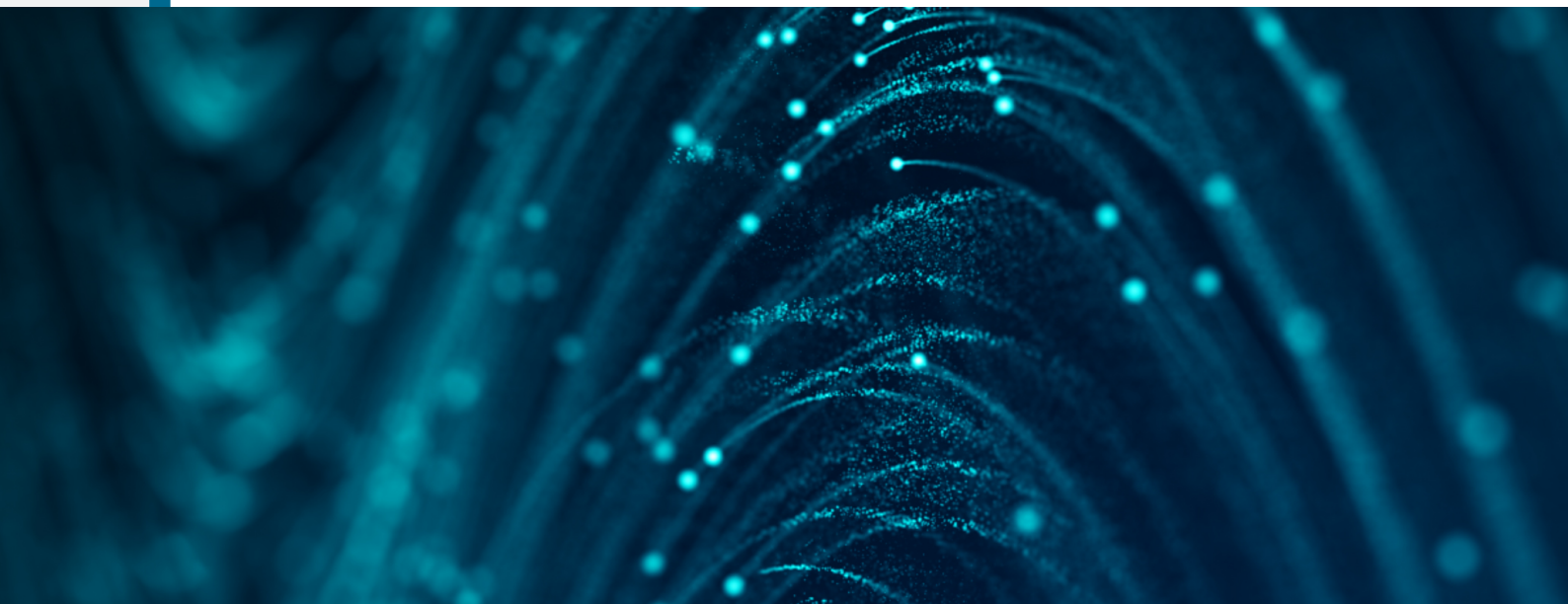
Driving ethical data and AI usage in your organisation

In an environment where regulations are unable to keep up with the pace of innovation or provide guidance on every scenario, and an executive's ability to control discrete actions is limited, how do you set boundaries to ensure your organisation behaves ethically when harvesting this immense value?

01 Perspective

Recognise that what one person deems as ethical behaviour, may not be ethical to someone else. Organisations need to be clear on their own perspectives.

02 Accept AI is a core part of your future

Agree a deliberate approach to bring AI into your organisation and keep tight controls. Adopt an explicit AI and data use governance framework that aligns to your business objectives and data strategy. Be deliberate in the data you generate and ensure you know the purpose and intent prior to creating it.

03 Set explicit and enforceable expectations

Set explicit expectations and standards for using data and AI and include these in your 'code of ethics', staff performance plans, supplier agreements and policies. Communicate these to staff and partners regularly and enforce clear consequences for those who breach the organisation's thresholds.

04 Recognise data is both an asset and a liability

The more data you store, the more expensive it is to protect. If data is used or manipulated in a way it shouldn't or if it is exposed publicly, the organisation will be held responsible. Proactively manage your liability, know the difference between data you use and data you need to store and don't hold onto data you don't need.

05 Educate your team

Include data and AI ethical case studies in training to ensure staff understand what is acceptable, and to get a pulse of the staff perspective vs. the organisation's perspective. Training materials should cover transparency between cause and inference, active awareness of bias and how to overcome or remove it, and explicit standards for ethical data use.

06 Embed the conversation

Data and AI usage requires the ethics conversation at all levels of the organisation, not just at the Board or C-Suite level, and it needs to be embedded within decision making and understood by all team members.

07 Evolve

Recognise data and AI will be used in ways which haven't been considered yet. These guardrails need to evolve over time to reflect changes and support organisational transformations.

Conclusion

Organisations need to be mindful of the potential adverse outcomes of data privacy and AI usage. To successfully integrate these evolving tools, they need to take appropriate measures to mitigate risks, respect privacy rights, and prioritise data protection and ethical practices by setting explicit boundaries, educating teams, and embedding ethics conversations at every level of the organisation.

About the author

Fiona Bench, Partner

Fiona Bench is a Partner and subject matter expert with over 15 years of leadership in financial services. She has a proven track record of driving business and technology outcomes in large, complex organisations and is adept at addressing challenges and managing risk in a changing regulatory and technological environment.