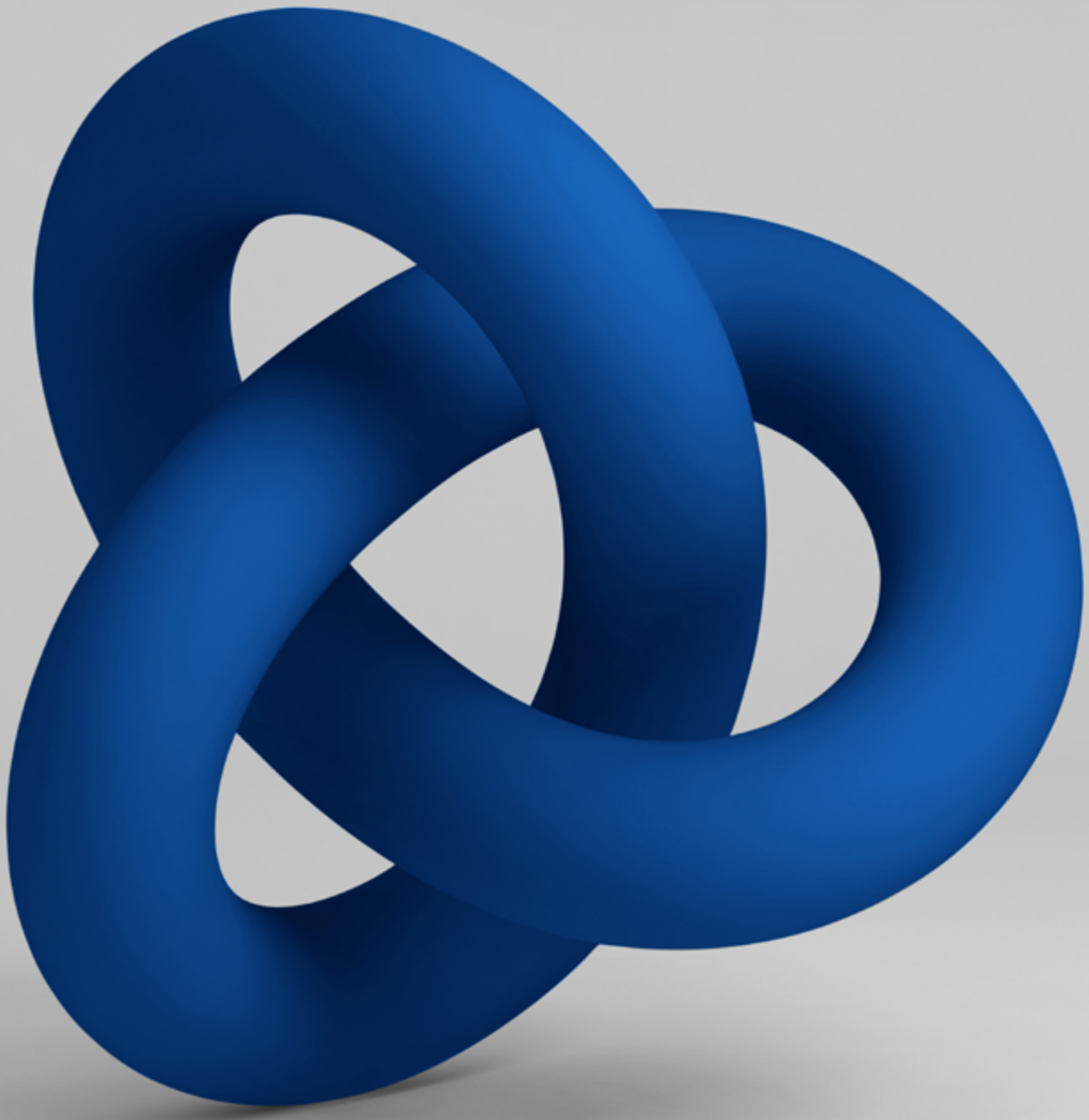
Baker McKenzie.



Trust Continuum

Leveraging Technology to Promote Employee Trust

Fostering employee trust is a critical component to overall business success. In light of the COVID-19 pandemic and as some workforces shift toward more permanent remote operations and day-to-day interactions are regularly buttressed by technology, this trust needs to be nurtured and guarded.

For those asking what implications rapid digitalization might have on employee trust, businesses need to reframe the age-old debate of humans vs. machines and instead look deeply at the human component of the data that feeds these technologies to identify the inherent risks within them.

Two notable areas of risk include the potential of data privacy breaches arising from the use of technology and the entrenching or accentuating of existing structural biases and distrust through AI algorithms.

Businesses should look to deploy new technologies critically and mindfully, using the related insights from technology as a vehicle for building trust.

In this paper, we explore:

1. the inherent value of employee trust to businesses;
2. what the current landscape and risks for emerging workplace technology look like;
3. the key tenets around responsible technology deployment; and
4. how organizations can leverage technology and its related insights better to promote employee trust.

1. Exploring the Value of Employee Trust

For those seeking to integrate Environmental, Social and Governance (ESG) principles in their overall business strategies, the COVID-19 pandemic has spotlighted the social aspect of ESG as well as the critical roles of both employees and a culture of trust.

In assessing a company's key stakeholders, in most companies with a workforce, employees will likely be considered as such. There are established links between **trust, employee engagement** and **business performance.**

The legal implication of considering employees as key stakeholders, is that, in many jurisdictions, directors will have a fiduciary duty to take account of the employee voice when considering any major decisions.

There are three key characteristics of companies that foster a culture of employee trust:

Accountability

Transparency

Delivery on promises

Further to these three characteristics, fostering employee trust goes beyond organizations having a one-way line of communication with their employees, but rather fully engaging with them in order to understand the full spectrum of their needs, concerns and aspirations.

The more effectively that companies are able to engage with their employees, the better that they can understand what motivates them and feed this back into their business strategies. This in turns creates a virtuous circle upon which trust can be built. The outcome for businesses is that building employee trust through better engagement and clearly incorporating feedback into decision-making can positively impact overall success, boosting both profitability and productivity.

In looking at how technology fits into this equation, the same characteristics that should be used to promote employee trust also apply to the deployment of technology: new technologies should be deployed transparently, with accountability and companies should routinely gather employee feedback in order to ensure the technology is delivering on its promise.

2. Assessing Emerging Workplace Technology and Risks

The rapid digitalization of many workplace functions, accelerated by the COVID-19 pandemic, poses a threat to employee trust through its potential — if used incorrectly — to perpetuate existing bias and inequity, result in breaches to employee privacy, break down accountability and create a false sense of trust.

Perpetuating bias and inequity

The promotion of fairness and equity within the workplace is a critical lifeline for employee trust; however, the lived reality is that the uncritical deployment of emerging technologies is more likely to entrench or accentuate existing structural biases than to remove them.

One particular area of concern is the use of AI, or more usually machine learning, which relies on pre-populated algorithms and other data input in order for machines to "learn" how to make decisions and carry out certain cognitive tasks typically done by humans to save time and improve efficiency.

However, there is concern about the implications of its unregulated usage, particularly when it perpetuates bias and inequity within the workplace or is perceived to do so.

Gartner has predicted that through 2022, 85 percent of AI projects will deliver erroneous outcomes due to bias in data, flawed algorithms or — perhaps most telling — the teams responsible for managing them. The reason for this latter risk is that most organizations are not well prepared for implementing AI as they lack internal skills in data science. Consequently, they have to rely a high degree on external providers, who are not familiar with their organizations and data, to fill the knowledge gap.

Without transparency and the necessary oversight, companies are at risk of encoding their own bias into algorithms.

Emerging Tech Applications in the Workplace: Human Resources and AI

The human resources (HR) field has been flagged as a particularly high risk area for AI oversight and regulation.

In HR, AI is currently used for tasks such as talent acquisition, administrative duties and employee training.

While these tools can save time and improve efficiency, some experts are concerned about the implications of unregulated AI usage when it comes both to undermining employee trust and to perpetuating bias and inequity within the workplace.

In HR, AI systems are built using pre-existing training data, which can include biased human decisions or reflect historical inequities in hires. Used incorrectly, this data can reinforce these inequities.

It is one thing to acknowledge potential biases in an AI-driven CV or resume sorting system; however, in correcting for that bias, there is a risk that organizations might falsely conclude that this has solved the problem of diversity in their workforce.

The legal industry's progress on gender bias is a salient reminder that it is not just hiring bias that is a problem. For example, while the majority of new graduates starting in law firms in many countries are now female, the female percentages at partner, and in particular equity partner, are not showing sufficient or material change.

This issue is prevalent beyond the legal industry too. According to **McKinsey & Company's 2020 Women in the Workplace** study, which tracks the progress of US corporations in regards to gender equity, for every 100 men promoted to manager in 2019, only 85 women were promoted. This number reflects a deeper issue around retention and progression for women in the workforce.

When considering the deployment of AI on the basis that it will help to combat bias, it is crucial that organizations look at the whole system into which that technology is being placed, which at times can be a difficult and uncomfortable conversation to have.

Breaching employee privacy

The lack of transparency around the use of employee data in workplace technology has resulted in the potential to cause long-term damage to employee trust. Beyond this, the risk of data privacy breaches directly arising from the use of technology adds another layer of concern.

Data privacy issues in relation to the workforce pervade the employee lifecycle, from the hiring process to various types of monitoring that might be implemented into an employee's day-to-day. Data rights have become an increasing point of focus for employees, in particular their rights of rectification, erasure and objection to data processing. Full transparency and avoiding improper use of data are critical components of avoiding backlash in this area.

Rapid developments in advanced data analytics, artificial intelligence and data capture have also created new opportunities for organizations to monitor their employees' productivity and work performance. In light of COVID-19 and a shift to remote working, technology such as email and internet usage monitoring, keystroke monitoring and remotely accessing webcams and microphones bring into question what employers can lawfully monitor.

In a stand-off between an employer's legitimate best interest for productivity and the employee's right to privacy, many of these monitoring technologies, if used to their full potential, are not EU General Data Protection Regulation (GDPR) compliant. Furthermore, beyond the regulatory pitfalls, the potential to erode employee trust may very well outweigh the benefits.

Breaking down accountability

Another risk of technology is breaking down accountability for decisions made within a company. Using technology as an end-all be-all decision maker within a company can have a de-humanizing impact for those affected.

While technology can provide detailed insights, data and analysis to support decisions and strategies, technology should augment rather than replace significant human decision-making processes.

This does, however, require two additional factors to be present:

- **a thorough understanding of the relevant technology element by the human decision-maker,** which proves to be challenging in most companies.
- **the discretion to ignore the recommendation and the time to make one's own decision.** In many situations, it might instead be easier to support the recommendation provided by the technology than to ignore or deviate from it, which will mean that this "human in the loop" will be less meaningful in practice.

Creating a false sense of trust

Misunderstandings toward technology can create false expectations around its infallibility.

Often, employee dissatisfaction and a lack of trust toward their human managers to be fair, informed and objective can lend itself to unmerited trust in current technology to make the "fair" decisions instead.

Whilst people may assume that technology is objective and free of the biases that affect human judgements, this is, however, not always true.

Society is structurally and inherently biased, and as a result, so are the algorithms and data that feed into these systems. It is critical for company decision makers to recognize that technology can never be divorced from the underlying context from which it is being deployed (namely, data input by and algorithms created by humans).

Ultimately, the deployment of new technology should not be considered a panacea to repair trust within a company as long as distrust still exists within the human chain of command. This becomes another issue of looking for the solution rather than diagnosing the problem at hand.

The Shifting Regulatory Landscape Around AI in the Workplace

Understanding the potentially negative impacts of uncritically deployed AI, multiple jurisdictions have either implemented or moved to implement legislation and frameworks around AI usage in the workplace, specifically:

- In Illinois, United States, the **Artificial Intelligence Video Interview Act** requires employers to:
  - notify applicants in writing before the interview that AI may be used to analyze their facial expressions and consider their fitness for a position;
  - provide applicants with information explaining how the AI in question works and what general types of characteristics it uses to evaluate them; and
  - obtain applicants' consent to use the AI program, as described in the notice, prior to the interview.
- In the EU, the European Commission has announced it will publish **its proposal for regulating AI** on 21 April 2021. The proposal is a follow-up to its White Paper on artificial intelligence, which was released in February 2020.
- In New York, United States, the proposed **bill** would require companies to disclose to candidates when they have been assessed with the help of software. Companies that sell such tools would be required to perform annual audits to check for discrimination within this technology.

3. The Tenets of Responsible Technology Adoption

While both organizational policies and government regulations are key in ensuring that workplace technologies are fairly deployed, ultimately, the onus falls on businesses to adopt new technologies critically and mindfully, providing the necessary frameworks and oversight to ensure that that they are deployed fairly and safely.

Organizations should regularly assess the impacts of deployed technologies, ensuring that the proper safeguards are being put in place.

One of the key points of focus is to create a workplace environment grounded in inclusivity and ensure that there is human accountability in working to reduce risk across all systems. This requires internal honesty about other structural biases that may exist in the system apart from the particular application of technology in question and full transparency around the criteria and data being used to feed algorithms.

Ensuring AI Best Practices: The Assessment List for Trustworthy AI (ALTAI)

Last year, the High-Level Expert Group on Artificial Intelligence (AI HLEG) presented a finalized **Assessment List For Trustworthy AI**. The list centers around seven key requirements for the deployment of trustworthy AI:

- human agency and oversight
- technical robustness and safety
- privacy and data governance
- transparency
- diversity, non-discrimination and fairness
- environmental and societal well-being
- accountability

Through this list, "AI principles are translated into an accessible and dynamic checklist that guides developers and deployers of AI in implementing such principles in practice. ALTAI will help to ensure that users benefit from AI without being exposed to unnecessary risks by indicating a set of concrete steps for self-assessment," **according to the EU Commission**.

Following such requirements ensures that relevant safety measures can be put in place in response to risk level changes and helps to generate trust amongst employees. This approach also aligns with the GDPR principle of accountability, whereby organizations acting as controllers are in the best position to assess, determine and document the level of risk raised by their own processing activities, and therefore should mitigate those risks accordingly.

4. Harnessing Technology as a Tool for Trust

While technology isn't a one-stop solution to promoting employee trust, businesses can harness technology and its insights in a way that is more likely to engender trust.

Businesses need to look at the problem that technology is trying to solve and see where it can be part of a larger solution, treating it as a tool, rather than an answer, in order to:

Spotlight gaps in employee trust & spark difficult conversations

Businesses can leverage data and other insights from technology in order to spark organizational change, as people are generally more receptive to data-driven decisions. However, as previously mentioned, businesses still need to take full accountability for decisions of critical business importance, especially those that have a direct impact on employees.

Mitigate pre-existing risks that might potentially erode trust

It is a fact that some existing human decision-making processes are not working to achieve stated goals. Despite the fact that technology has the potential to improve upon the current situation, it is often put under more scrutiny than existing human processes. Some balancing of the risks and opportunities of human vs. machine decision making is essential.

Businesses should be mindful of the opportunity costs of not using technology in specific situations, particularly those where the alternative poses greater risk than that posed by deploying a new technology. This could be reflected in the risk assessment in order not to discourage technology's net beneficial use.

Create a trust loop

Technology can add rigor around decisions that impact employees' day-to-day and, if structured well, can add transparency by enabling companies to scale insights from what is actually happening within the business.

By actively communicating and engaging employees through the insights provided by technology, a trust loop is then created.

Outlook and Takeaways

Accountability, transparency and delivery on promises are key components for businesses looking to foster long-term employee trust. The same characteristics around employee trust also apply to the deployment of emerging technologies.

Both organizational policies as well as government regulations are key in ensuring that workplace technologies are being fairly deployed. Emerging legislation around AI in the workspace, in particular, has made for a shifting regulatory landscape that organizations will need to navigate.

In addition, as the prospect of a single, coherent, global system of ESG reporting appears on the horizon, it becomes even more critical for companies to understand the concept of responsible AI and societal and governmental concerns regarding biases, misinformation and potential ethical breaches through unguarded use of AI. Implementing procedures for addressing this and preparing to be transparent about what has been done and with what impact, that is, describing a company's approach to responsible data management, will become critical.

Ultimately, businesses will need to adopt technology critically and mindfully, but also realize many of these issues encountered are oftentimes representative of larger issues within an organization. Accordingly, businesses also need to look internally at the whole system, ensuring that the overall culture is also one that is conducive to an environment of trust.

In the long-term, valuing employees as business stakeholders and taking these actions to enhance employee trust will offer long-term benefits.

Ben Allgrove
Partner
Ben.Allgrove@bakermckenzie.com

Beatriz Araujo
Partner
Beatriz.Araujo@bakermckenzie.com

Roderick Beudeker
Senior Associate
Roderick.Beudeker@bakermckenzie.com

© 2021 Baker McKenzie. All rights reserved. Baker & McKenzie International is a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner or equivalent in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.