HERBERT SMITH FREEHILLS

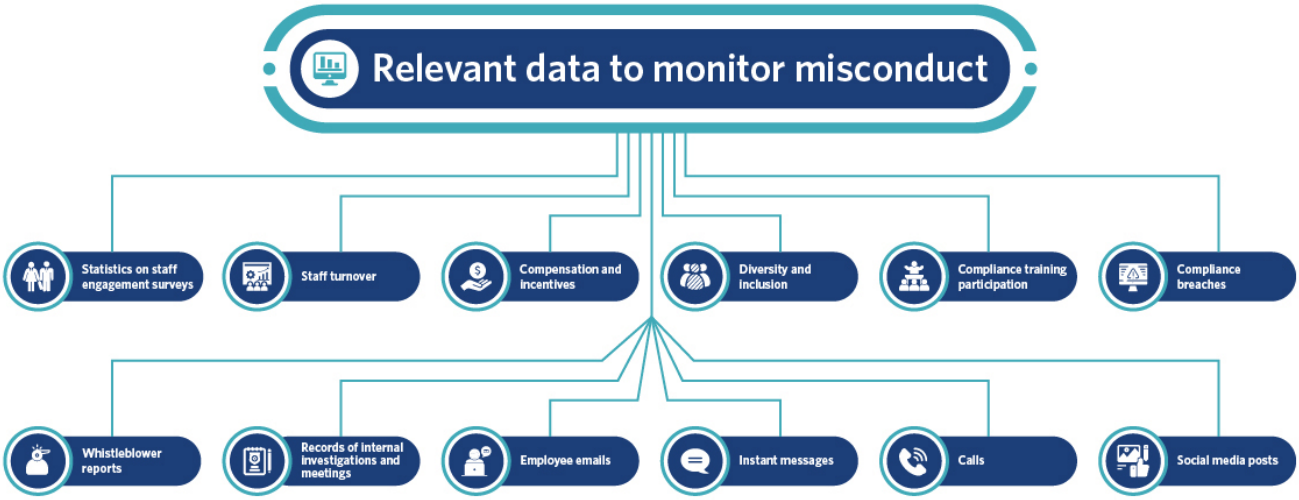
CAN PREDICTIVE ANALYTICS PREVENT EMPLOYEE MISCONDUCT?

21 July 2020 | Insight
– By **Tim Leaver, Michael Gonski and Tess Lumsdaine**

The appeal of data tools in unearthing misconduct is clear. So are the risks if employers fail to tread carefully

With predictive policing and crime forecasting gaining attention, although not always good, it is not surprising that businesses are considering how to deploy analytics in their fight against employee misconduct. Certainly, financial regulators have encouraged organisations to become more sophisticated in how they use both quantitative and qualitative data to identify the drivers of misconduct and to develop methods to adjust employees behavioural norms.

The appeal is clear: if businesses can use data to identify and address misconduct far earlier, let alone prevent it from occurring, they may limit regulatory, financial and reputational fallout. While the opportunities this presents for organisations are attractive, the legal, ethical and operational considerations are complex, particularly so when using predictive analytics in the context of employee misconduct.



Predictive analytics is a process by which new and historical data are drawn upon to detect patterns and trends with a view to forecasting events and behaviours. While commonly used to observe and anticipate consumer and community behaviours, it is increasingly being experimented with by organisations in relation to their employees. In the employment context, relevant data may range from statistical data drawn from employee engagement and turnover, compensation and incentives, diversity and inclusion, training participation rates and compliance breach records to qualitative data such as transcripts of investigation interviews, meetings, whistleblower reports as well as emails, instant messages, calls and social media. Increasingly data is also being drawn from employee computer and smart phone usage logs, CCTV and wearable devices. As technology becomes more sophisticated, data points will increase.

Through statistical modelling and AI, it may be possible to discern patterns within the data which are typically associated with conduct risk. For instance, using AI to review text or voice records may pick up key words in customer interactions which, when reviewed with trade data and computer and phone logs, may indicate potential misconduct. Through machine learning organisations may uncover relationships between data sets and conduct which were previously overlooked or misunderstood.

Legal implications of predictive analytics

The ways in which predictive analytics may be used as part of workforce management are limitless. Where trends associated with conduct are identified, organisations can take early steps to identify and respond to misconduct at an early stage. They may also intervene and mitigate against such misconduct occurring through increasing compliance controls or training.

More difficult questions arise if organisations rely on data when taking actions in respect of employees identified as high risk but against whom no finding of misconduct has been made. For instance, how should data that suggests an individual is a higher compliance risk be taken into account in the context of an internal investigation into misconduct?

In jurisdictions such as Australia and the United Kingdom, employees may challenge the lawfulness of disciplinary decisions on the basis that the processes lacked procedural fairness or the decision was not based upon a valid reason. Decisions underpinned solely by predictive analytics will not hold up in such circumstances. Where the data suggests possible misconduct, as opposed to evidencing that misconduct has occurred, it should prompt further investigation. In the absence of evidence of actual misconduct, an individual would be unable to respond to the allegations levelled against them and thus be afforded procedural fairness.

Similarly, issues may arise if organisations base promotion decisions upon predictive analytics. Any data may need to be viewed in a broader context which may not be captured. For example, if one data point drawn upon is high absenteeism, it is possible that these may be more prevalent for an individual with a disability or with carer's responsibilities, and decisions based on this may run the risk of unlawful discrimination. Analytics may also have a disparate effect on individuals from a particular cultural or ethnic background. For example, certain phrases or terms have a different meaning in a cultural context, however, analytics may not be sufficiently complex to pick up on cultural or regional nuances. In defending any allegations of unlawful discrimination, it may be difficult or undesirable (given the proprietary and confidential information involved) to break down how an algorithm has identified an individual or a group as being a higher compliance risk. This may mean it is difficult for companies to disprove that the decision did not take into account any protected attribute and was instead based on entirely non-discriminatory reasons. The challenges associated with bias in AI are widely known and are currently the subject of significant academic and legal debate across the globe. There is also discussion around regulation of AI in certain circumstances and a commitment by AI developers and users to adopt ethical guidelines. Both the US Equal Employment Opportunity Commission and the European Commission have raised concerns about the manner in which predictive analytics is used in the work context and employers are cautioned to proceed carefully.

Finally, organisations must consider how transparent they are in relation to monitoring of employees. Most forms of monitoring will involve processing personal data which, across Europe, is subject to significant restrictions under the General Data Protection Regulation and, separately, local employment law requirements. In some European jurisdictions, employee monitoring (let alone employee profiling) is prohibited and can result in criminal sanctions. In other jurisdictions, monitoring is permitted only if the employer has assessed that it's truly necessary and proportionate to achieve legitimate interests, and usually only if employees have been fully informed as to what monitoring is taking place and why. Some EU nations also require employers to consult with employee representative bodies before subjecting workers to surveillance measures.

Increasingly, we are seeing instances of employees challenging the decision to terminate their employment due to their refusal to agree to monitoring with cases in the US and Australia (see inset). The European Court of Human Rights has also been called upon to opine in the context of a dismissal based on employee monitoring.

ARIAS VS INTERMEX WIRE TRANSFER
In 2015, a former sales executive for money transfer service Intermex filed a state court lawsuit in California claiming that she had been fired after she disabled an app that tracked her movements 24 hours a day through her company-issued phone. Myrna Arias said she and her colleagues had been required to download the job management app and she had complained that monitoring her location during non-work hours was an invasion of her privacy. The case, in which the plaintiff claimed damages of more than US$500,000, was settled out of court.

FINGERPRINT SCANNER FALLS FOUL OF THE PRIVACY ACT
In early 2019, Australia's Fair Work Commission (FWC) heard a case brought by Jeremy Lee, who had been dismissed by his employer for refusing to provide his fingerprint for a new entry system used to check workers in and out of its site. Mr Lee argued that he should not be required to provide his fingerprint, on the grounds that the biometric data contained within it was 'sensitive data' under the 1988 Privacy Act and therefore could only be collected with his consent. Employers in Australia were granted an exemption from the Act for employee records when it was first introduced, over concerns of the cost of compliance. Mr Lee's employer argued that his fingerprint formed part of his employee record and should fall under the exemption. The FWC, though, found that the exemption wording related to personal information that is 'held' in an employee record – and as the employee's fingerprint had not yet been collected, it could not already be held and the obligations of the Act applied. The FWC found in the worker's favour and he was awarded compensation.
The above case studies appeared in our recent publication, **The Future of Work**

At a minimum, the process of determining and testing data parameters will be incredibly important – particularly so for organisations with diverse workforces or operating in different markets. Similarly, those reviewing and making decisions based on predictive analytics will need to thoroughly understand the predictive analytics process and be alive to the potential risks and broader context that may need to be taken into account. Periodic reviews will also need to occur to assess there has been any unforeseen, disparate or adverse impact which could potentially cause discriminatory outcomes and consider if further testing or refinement is required.

Even where laws are complied with, organisations will need to consider potential triggers for employee activism. We recently surveyed approximately 400 cross-sector C-suites globally for Herbert Smith Freehills' Future of Work report and 50% of respondents identified issues connected to the surveillance and monitoring of the workforce as a potential trigger for workforce activism. The survey results show that employers expect activism in the near future to be centred on technology-driven workplace issues such as the introduction of AI and automation, and the surveillance and monitoring of workers.

Given the significant disruption and reputational damage that workforce activism can cause, the approach that organisations take when conducting employee monitoring needs to be carefully balanced with the potential for backlash which may undo the benefits of embracing new technologies.

EXPLORE OUR CAMPAIGN

RELATED TOPICS

Data and privacy
Future Cities

FEATURED INSIGHTS

FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

BROWSE BY:

- TECH, DIGITAL & DATA

- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

RELATED ARTICLES

UPDATED: UK NATIONAL SECURITY ACT 2021 - WHAT INVESTORS NEED TO KNOW

Foreign investment: Rising tides of politics in regulation

Comply or Explain to climate-related reporting – A cross-industry roadmap

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

TIM LEAVER
PARTNER, LONDON

+44 20 7466 2305
tim.leaver@hsf.com

MICHAEL GONSKI
PARTNER, SYDNEY

+61 2 9225 5083
Michael.Gonski@hsf.com

TESS LUMSDAINE
SENIOR CONSULTANT, HONG KONG

+852 2101 4122
Tess.Lumsdaine@hsf.com