

AI Guides

AI & Privacy

Does AI have a privacy problem?

As AI becomes more popular, organisations are increasingly being forced to ask themselves how best to balance AI innovation with privacy law compliance. In its Human Rights and Technology discussion paper released December last year, the Australian Human Rights Commission (AHRC) highlighted the right to privacy as one of the key human rights affected by the rise of new technologies, and noted that the privacy risks posed by AI-informed decision making had become a major community concern. Although not all AI systems collect personal data, many do. And these systems can process personal information in volumes and at rates that were previously unimaginable.

How could your AI system cause you to breach privacy laws?

One of the key foundations of Australian privacy law is that personal information should be collected from an individual for a specific purpose, that purpose should be disclosed to the individual, and that information should only be used for that purpose, with limited

exceptions. Even businesses that don't use AI grapple with these limitations. But for organisations using AI, the difficulties are exacerbated.

In many cases, an entity won't be able to predict the relationships and correlations that a particular data set is going to reveal. In fact, the value of using AI regularly comes from subsequent uses of data. For example, an algorithm may discover an unexpected relationship in data collected for one purpose that is particularly valuable for another purpose. However, under Australian privacy law, an entity must not use the data for that new purpose unless it is satisfied that the new purpose would be within the "reasonable expectation" of the individuals from whom the data was collected. If not, it will have to seek consent from those individuals to use their data for the new purpose. Organisations that purchase data in bulk from third parties will need to go through a similar process.

Another core data protection principle that may conflict with businesses' use of AI is the "collection limitation", which only allows organisations to collect personal information to the extent "reasonably necessary" for their functions. But in the world of AI, there is almost no such thing as too much data. Many AI systems need large amounts of training data to "learn" from, and this may encourage organisations to collect more personal data than what is actually necessary for the particular project. It can also be difficult to predict when an algorithm has been adequately trained, and the use of any data after that point is arguably in breach of the collection limitation. To manage this, businesses should have procedures in place to help their engineers and developers assess and continuously reassess how much and what type of data is necessary for the particular project.

Australian regulators have also foreshadowed the introduction of a "right to be forgotten" (ie the right to have your personal information erased

on request), similar to the right provided under the EU's General Data Protection Regulation. If this proposal goes ahead, it raises another question – how do we teach an AI system to “forget”? Some have suggested that this might be impossible.

So what does the future look like for AI and privacy?

We are likely to see a regulatory response on some of these issues in Australia – for example, the AHRC has proposed that the Government should introduce laws regarding “explainability” of AI-informed decision making, and establishing a cause of action for serious invasions of privacy. If enacted, these

laws may force businesses to adopt much stricter procedures regarding their use of AI. In the meantime, businesses should be guided by the approach of regulators overseas. The Information Commissioner's Office in the UK is leading the charge in this regard, and has recently provided [guidance](#) on how to conduct a data privacy assessment for an AI system that processes personal data.

The AI Guides are authored by:



John Swinson
Partner, Brisbane
T +61 7 3244 8050
john.swinson@au.kwm.com



Rebecca Slater
Senior Associate, Brisbane
T +61 7 3244 8147
rebecca.slater@au.kwm.com



Kendra Fouracre
Senior Associate, Melbourne
T +61 3 9643 4105
kendra.fouracre@au.kwm.com

www.kwm.com

Asia Pacific | Europe | North America | Middle East

King & Wood Mallesons refers to the network of firms which are members of the King & Wood Mallesons network. See kwm.com for more information.

© 2020 King & Wood Mallesons