Horizon Scanning Series

The Effective and Ethical Development of Artificial Intelligence: An Opportunity to Improve Our Wellbeing

GDPR and Regulation

This input paper was prepared by Nick Abrahams and Monique Azzopardi on behalf of Norton Rose Fulbright

Suggested Citation

Abrahams, N and Azzopardi, M (on behalf of Norton Rose Fulbright) (2018). GDPR and Regulation. Input paper for the Horizon Scanning Project "The Effective and Ethical Development of Artificial Intelligence: An Opportunity to Improve Our Wellbeing" on behalf of the Australian Council of Learned Academies, www.acola.org.

Horizon Scanning Report on AI for Australian Commonwealth Science Council

1 Introduction

Artificial intelligence (**AI**) is no longer a fiction. It has become a legal reality that regulators around the world are still grappling to regulate and fully understand.

This paper covers the current regulatory landscape outside Australia and New Zealand that is likely to be relevant to the use and deployment of AI in Australia and New Zealand. Its focus is on the regulations and corresponding legal issues associated with AI in a general sense and without reference to any specific application of AI or the use of AI in a particular industry. However, it is important to note that industry specific laws and regulations will be relevant to AI's deployment and use in Australia and New Zealand, especially in more regulated areas such as the finance, healthcare and insurance industries.

2 What overseas regulations around AI and data are likely to impact on AI in Australia and New Zealand

Overseas privacy regulations; namely the new EU General Data Protection Regulation (**GDPR**), is likely to have one of the largest impacts and restraints on the use of AI in Australia and New Zealand. Other laws and regulations may also be relevant depending on the specific application and reach of the AI technology and what its capabilities are.

Contextualising AI – why privacy regulations will be relevant

To understand the relevance of privacy laws and regulations, such as the GDPR, it is necessary to firstly understand the data-centric aspects of AI. Data has been described as the fuel for AI. Using specific algorithms or rules, AI systems collect, sort and break-down datasets to analyse them and make forecasts and decisions.[1] As technology that collects, processes and develops data, which may include personal data, privacy legislation will be relevant to AI's application and use.

The GDPR governs the collection and processing of "personal data" which is defined in Article 4(1) of the GDPR as:

> "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

One may initially query how an overseas regulation is relevant to countries such as Australia and New Zealand. The answer is due to the GDPR's expanded extra-territorial reach. In broad terms, the GDPR may apply to an entity not incorporated in the European Union (**EU**) where that entity:

- has an establishment in the EU (for example, a branch office);
- processes personal data of individuals who are in the EU where such processing is related to the offering of goods or services to those individuals; or

[1] Government Office for Science, "Artificial Intelligence – Opportunities and Implications for the Future of Decision Making" available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf (accessed 19 July 2018).

- processes personal data of individuals who are in the EU where such processing is related to monitoring the behaviour of those individuals as far as their behaviour takes place in the EU.

Importantly, Australian and New Zealand entities do not need to have a physical presence in the EU to fall within the ambit of the GDPR. Moreover, Australian businesses of any size may need to comply with the GDPR, as opposed to the limited exemptions from the *Australian Privacy Act 1988* (Cth) (**Australian Privacy Act**) for certain small businesses which have an annual turnover of $3 million or less.

Whilst the GDPR shares a number of requirements with other privacy laws, such as the Australian Privacy Act, the GDPR introduces a number of new requirements that will likely have a significant compliance impact for Australian and New Zealand entities who are captured by the new regime. For example, the GDPR introduces increased accountability and transparency around the processing of personal data and enhanced data subject rights (such as the right "to be forgotten" and the right of data portability). It also introduces a new definition of consent. Of course, the specific application of the GDPR to AI will turn on the nature, scope and context of the data processing through AI systems, amongst other factors.

The use of AI and machine learning will likely present a big challenge for entities in terms of their compliance with privacy regimes, such as the GDPR. Such regimes are focussed on transparency of processes and systems around datasets containing personal data. However, it is often difficult to obtain this transparency and to fully understand how AI systems work and the full extent of their decision making capabilities. The potential risk of AI systems going rouge and the robots taking over is another concern, which is perhaps fuelled by science fiction movies rather than reality. However, these are some of the reasons why AI is an area that requires more onerous requirements and oversight under various regulatory frameworks. The regulatory implications and impacts of AI are discussed further below.

To lessen the impact and reach of the GDPR and other regulations governing personal data use, Australian and New Zealand entities may consider it prudent to minimise or completely remove the processing of personal data from AI's capabilities; for example, pseudonymising or de-identifying data before it is inputted into AI systems. However, this may not always be practicable. Furthermore, de-identification (such as removing a person's name) will not be a panacea if AI's functionalities are sophisticated enough to combine datasets together to re-identify datasets or reasonably ascertain the identity of a person based on one or a combination of datasets in its systems.

With such a regulatory framework in place, it will be important for Australian and New Zealand entities who are captured by it to implement appropriate technical and organisational measures to comply. Certainly, there is a "big stick" incentive to do so. The penalties are severe for non-compliance with the GDPR with fines of potentially up to €20 million or 4 per cent of annual worldwide turnover (whichever is higher), for certain contraventions. Moreover, where an AI system causes a data breach involving personal data there are legal obligations to report certain breaches under both the GDPR and Australia's new notifiable data breach regime. Data breaches, whether caused by humans or machines, can be a public relations nightmare for any entity.

As a result of the GDPR, it is expected that there will be a natural flow-on impact as to how Australian and New Zealand entities manage and process personal data, whether or not they are captured by the GDPR regime. Compliance with regulations such as the GDPR could set the benchmark or norm for personal data processing and compliance within Australia and New Zealand.

3 **What are the regulatory implications for the use of AI by transnational corporations for Australia and New Zealand (data ownership; profiling)?**

There are several regulatory implications involved in the use of AI by corporations, whether they be transnational or not. We have seen above that a corporation that is not transnational could still be caught by an overseas regulation such as the GDPR.

Automated decision making and profiling

One of the touted benefits of AI and machine learning is its capacity to learn and make decisions without any human involvement. AI can also be used to "profile" individuals. Article 4(4) of the GDPR describes profiling as:

> "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

However, the use of automated decision making and profiling comes with some drawbacks and concerns. Errors or biases in collected or shared data or in AI's automated decision making or profiling processes may lead to incorrect decisions, profiles or classifications being made,[2] which can have an adverse impact on the individual concerned and on the integrity of these processes more generally.

It comes as no surprise that automated decision making and profiling is subject to restriction and increased oversight under the GDPR. Subject to some exemptions, under Article 22 of the GDPR, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling if it "produces legal effects concerning him or her or similarly significantly affects him or her". In other words, a data subject cannot be subject to a decision that is made without any human involvement. In broad terms, the exceptions to this are decisions that are necessary for contractual performance between the controller and the data subject, authorised by Union or Member State law to which the controller is subject, or made with the data subject's explicit consent. Even where a relevant exception applies, entities using automated decision making are still required to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. This includes, a series of rights under Recital 71 of the GDPR in relation to profiling; including the right to an explanation of a specific decision and the right to challenge the decision. Additional restrictions also apply where decisions are made based on specific categories of personal data (for example, personal data revealing racial or ethnic origin, political opinions or religious or philosophical beliefs).

Furthermore, Articles 13(2)(f) and 14(2)(g) of the GDPR requires data controllers who use personal data to make automated decisions to notify individuals about the existence of automated decision-making, including profiling and "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

The difficulties of complying with these obligations when using AI has been extensively reported in the literature. The complexity of AI and their associated technologies may make it difficult to understand how decisions and profiling are being undertaken by AI systems.[3]

Amongst other factors, Australian and New Zealand entities should identify any wholly automated decisions that they undertake using AI, and consider whether it is possible to change the process so that there is meaningful human involvement (for example, have a sufficiently qualified and skilled human review the machine's decision), or ensure that they can satisfy one of the available exceptions under the GDPR.

A data protection impact assessment may also be required. Article 35(1) of the GDPR requires that where a type of processing, and in particular where using new technologies, is likely to result in a high risk to the rights and freedoms of a person, a data protection impact assessment must be carried out. In particular, Article 35(3) of the GDPR expressly requires that a data protection impact assessment is undertaken when carrying out a "systematic and extensive evaluation of personal

[2] Article 29 Data Protection Working Party, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679" (adopted on 3 October 2017) available at https://www.pdpjournals.com/docs/887862.pdf (accessed 17 July 2018).
[3] *Ibid*.

aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person."

3.1 Data ownership and rights

In the age of "big data", data has become a very valuable asset. AI's data generating capabilities present some commercial opportunities for the use and leverage of that data. However, the current regulatory issue is that many laws do not recognise data itself as a type of property that can be owned and sold. Data can only be truly owed where it constitutes IP, such as copyright or a trade secret. However, as discussed below, there are difficulties with data constituting a work protected by copyright due to the absence of a human author.

Nevertheless, people still have rights associated with certain datasets; for example, where the data is their personal data, confidential information or where there exists a statutory right (for example, a right to access data under freedom of information laws). These rights are derived from a combination of contract, common law and statute.

The GDPR includes enhanced rights, including data portability rights. On the legislative agenda in Australia is the new "Consumer Data Right" to permit certain consumers open access to specific types of data and greater data portability over those datasets. This would extend to data held or generated by AI systems. Under this proposed legislation, the consumer would have a greater ability to access certain data concerning them. At present, the legislation is likely to apply to banks, utilities and telecommunication companies but may be extended beyond these sectors.

3.2 Data quality and security

AI systems do not simply process data, they also create new datasets, which may include the generation of data based on personal data. Entities utilising AI will need to audit and assess the correctness and quality of those datasets. Where the datasets include any personal data, entities will need to ensure compliance with applicable privacy legislation and associated privacy principles, such as APP 10 under the Australian Privacy Act. Under APP 10 entities governed by the Australian Privacy Act must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that they collect, use or disclose is accurate, up-to-date and complete. A broadly similar principle is included in Article 5 of the GDPR.

Persons that collect and use data have a custodianship role, especially where that data contains confidential information or personal data. Under the Australian Privacy Act entities must take reasonable steps to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. "Reasonable steps" in the context of AI might include implementing systems around information and communication technology security,[4] and regular testing of the AI system's security controls and systems.

3.3 Consent

If AI systems are collecting personal data on behalf of an entity, consent will be required. This may pose difficulties when AI is involved. While AI systems can accommodate a "tick a box" approach to consent (that is, they can work out whether or not someone has ticked the "I agree" box), they may struggle to comply with the onerous consent requirements under the GDPR.

The GDPR requires consent to be freely given, specific, informed, and an unambiguous indication of the data subject's wishes. While AI systems may be intelligent in many respects, they may lack sufficient emotional intelligence to recognise the emotions and intentions of humans. It may therefore be more difficult for AI systems to discern whether or not consent is free or represents an unambiguous indication of someone's wishes.

3.4 Intellectual property (IP)

[4] Office of the Australian Information Commissioner, "Chapter 11: APP 11 — Security of Personal Information" available at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information (accessed 18 July 2018).

There are a number of regulatory issues associated with the protection of AI systems and technologies and their outputs. There is a question as to whether AI as computer implemented algorithms meet the high thresholds of being "novel" and containing an "inventive step" to be eligible for patent protection. At least in Australia, courts have confirmed mere ideas, methods of calculation, systems or plans, and certain computer-implemented business methods are not patentable subject matter. For AI, this means that automating individual processes may not be sufficient to constitute a manner of manufacture or patentable subject matter unless the automation is an invention in and of itself.

Secondly, there is a question as to whether any data or works produced by AI systems constitutes a original work protected by copyright. Certainly under the *Australian Copyright Act 1968* (Cth), copyright does not protect data alone but rather the way it is collected and put together. Compilations of data can be protected under copyright law but only if it passes the originality test. This is a barrier with AI created works which are created without the input of a qualified person. Under Australian law, copyright does not exist in a work that is made by a machine and is effectively "authorless" – a human author is required.

3.5 Competition law

In the competition law space, concerns have been raised about the market power that technologies such as AI can give entities. The reason for the concern in this area is that AI can use algorithm pricing systems to gather and leverage vast datasets. In the right market conditions, such pricing algorithms may be used to engage in and sustain collusion or other anti-competitive practices that are prohibited at law.[5] The Australian Competition and Consumer Commission has noted:

> "…a profit maximising algorithm will work out the oligopolistic pricing game and, being logical and less prone to flights of fancy, stick to it… [I]f similar algorithms are deployed by competing companies, an anti-competitive equilibrium may be achieved…"[6]

Complicating the area further is the fact that the use of AI may mean that businesses would not know how or why their machines reach a certain conclusion.[7]

3.6 Liability

AI creates a liability conundrum. While some AI systems are often seen as acting autonomously and independently, they are not human. In such a scenario who should be liable where an AI system goes wrong and causes an accident or other liability: should it be the programmers, manufacturers and developers of the specific AI system or someone else? The conundrum also arises from the complexity of AI systems and the interdependency between their different components, parts and layers.[8] Australia is yet to establish meaningful precedents to address the appropriate allocation of risk and liability between the various actors involved in the development and deployment of AI systems.

4 Conclusion

The regulatory issues and implications related to the use of AI by transnational corporations and other entities are complex and varied. As disruptive technologies such as AI become more prevalent, we are likely to see increased regulation in this space.

Nick Abrahams (Partner) and Monique Azzopardi (Senior Associate)
Norton Rose Fulbright Australia
24 July 2018

[5] Rod Sims, "The ACCC's Approach to Colluding Robots", delivered at the Can Robots Collude? Conference (16 November 2017), available at https://www.accc.gov.au/speech/the-accc%E2%80%99s-approach-to-colluding-robots (accessed 18 July 2018).
[6] *Ibid.*
[7] *Ibid*.
[8] European Commission, "Commission Staff Working Document: Liability for Emerging Digital Technologies" (Final) available at https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies (accessed 18 July 2018).