Deloitte Risk Advisory Pty Ltd
ACN 611 748 184
Grosvenor Place
225 George Street
Sydney, NSW, 2000
Australia

Phone: +61 2 9322 7000
www.deloitte.com.au

2 October 2018

Mr Edward Santow
Human Rights Commissioner
Australian Human Rights Commission

By email: tech@humanrights.gov.au

Dear Mr Santow

Human Rights and Technology Issues Paper: Submission

Thank you for your invitation to comment on the **Human Rights and Technology Issues Paper** (the Issues Paper). As a staunch advocate of human rights, Deloitte is delighted to contribute to the public discourse on this topical and vital issue. Our comments, in line with our specialisation, are primarily focused on the privacy implications of emerging technology. We have provided our views in response to a select number of the available consultation questions below.

Introduction

Deloitte endorses and celebrates the responsible development of new technologies that contribute to the empowerment, equitable distribution and accessibility of necessary services and conveniences. We note that technological advances have transformed and will continue to transform vital services such as medicine, transport, food production and distribution and more broadly, improve accessibility to necessary services.

We also note that new technologies are changing the face of existing industries and services such as the finance, banking, advertising and legal industries. For example, analytical and tracking technologies now routinely enable the provision of 'tailored services' to serve clients in a more efficient and accurate manner. Mobile apps enable instant and remote access to finances, and multiple programs permit instant, high quality audio visual communication overseas and in remote rural areas. On the legal front, the advent of the 'Online Court' and

'Online Registry'[1][2] has heralded an enormous shift in the procedural norms of the Local Court, enabling practitioners and litigants to manage evidence, documentation and preliminary proceedings online. Further, current technology now enables the automated creation and execution of contracts directly between parties, and there is reason to believe that in the near future, technological solutions may replace the traditional face to face legal consultation in a number of contexts[3]. The accessibility, cost, efficiency and other implications of this move are manifold.

However, Deloitte also notes that technological development is not without risk. As noted by the Australian Human Rights Commission, "new technologies are causing us to rethink our understanding of particular human rights"[4], and Deloitte believes technological changes should be accompanied by robust safeguards and regulation to appropriately and thoroughly mitigate or address the risks involved.

Consultation Questions

What types of technology raise human rights concerns? Which human rights are particularly implicated?

Technologies that rely on personal information and their impact on the right to privacy

It arguable that all technology has a potential human rights impact. However, certain types of technology and their potential uses pose a greater risk than others. As the Commission noted, "new technologies do not inevitably threaten human rights, but the problem of dual affordances or multiple uses, is particularly acute with new technologies."[5] As also noted in the Issues Paper, the demand for personal information is currently at unprecedented levels. Thus the risk to privacy has increased at an equally unprecedented rate, as "where personal information is misused, the consequences can be grave."[6]

We believe that the right to privacy, which is underpinned by the right to equality and non-discrimination, the right to freedom of expression, the right to information and safety for children, the right to freedom from violence and the right to a fair trial and procedural fairness, should be a key consideration when considering the regulation of emerging technologies.

Considerations of autonomy and self-determination are vital in any discussion of privacy. However, a discussion of the potential risks to the safety and wellbeing of the individual is equally important. Personal information may be used in a manner which results in physical, psychological, financial or emotional harm to the individual, such as in the provision of contact

---

1 Law Society of NSW Litigation Law and Practice Committee 'Online Registry and Online Court? We've got your queries covered' *Law Society Journal NSW* (July 2018). At https://lawsociety.cld.bz/LSJ-July-2018/84

2 NSW Courts and Tribunals 'Online Registry', at https://onlineregistry.lawlink.nsw.gov.au/content/

3 Melissa Coade 'Illuminating the Future of Law', *Law Society Journal NSW* (August 2018). At https://www.lawsociety.com.au/sites/default/files/2018-07/Illuminating%20the%20future%20of%20law.pdf

4 The Australian Human Rights Commission, Human Rights and Technologies Issues Paper, July 2018, at 4.1.

5 Ibid, at 4.1.

6 Ibid, at 3.4.

details to person who may pose a safety risk to the individual.[7] Furthermore, personal information may be used against individuals on a discriminatory basis on an as yet unprecedented scale. These risks may be exacerbated by risk assessments that do not adequately consider non-mainstream cases, wherein a loss of privacy may result in a devastating impact. The protection of individual privacy must be a key factor and driving principle in any discussion on the responsible regulation of technology.

How should Australian law protect human rights in the development, use and application of new technologies? In particular:

a) What gaps, if any, are there in this area of Australian law?

Privacy regulation

As noted above, the right to privacy is a vital element of when discussing technology and human rights.

Currently, Australian privacy law, and consequently Australian privacy regulation, is multi-jurisdictional. The *Privacy Act 1988* (Commonwealth) regulates Commonwealth agencies and private sector organisations with an annual turnover of over 3 million dollars per annum. In addition, Victoria, New South Wales, Queensland, the Australian Capital Territory, the Northern Territory and Tasmania have introduced legislation to regulate privacy in all state-based organisations. South Australia has issued an administrative instruction, which directs its state agencies to comply with a set of Information Privacy Principles, whilst Western Australia has not introduced any privacy specific legislation (although there are some privacy-based principles in its *Freedom of Information Act 1992* (WA)).

As with any multi-jurisdictional scheme, there are significant differences in regulatory involvement and oversight, accountability requirements, enforcement action and mandatory reporting between each jurisdiction. This has led to a number of gaps in privacy regulation. For example, the recently introduced Notifiable Data Breach (NDB) Scheme[8] requires all private health service providers to notify the federal regulator and affected party of all eligible breaches, whilst no equivalent requirement exists for state health bodies. This has created a gap in relation to the reporting and management of data breaches between the federal and state jurisdictions, and thus ultimately, potential differences in regulatory oversight and ultimately privacy practice and accountability by regulated entities.

Additionally, small businesses (businesses that earn three million dollars or less per annum) are not currently subject to any consistent regulatory scheme. For example, a small NSW business which provides private health services may be subject to both the NDB scheme and the *Health Records and Information Privacy Act 2004* (NSW) in relation to its handling of health information; however the remainder of its personal information-related activities will remain unregulated. Conversely, other small businesses who do not fall within scope of state health legislation are entirely unregulated. Victoria and the ACT have similar health-record

[7] Josh Robertson 'Commissioner 'orders review' into officer who leaked woman's address to allegedly abusive partner', ABC News, 11 May 2018. At http://www.abc.net.au/news/2018-05-11/officer-who-leaked-womans-address-has-pay-docked-no-charges/9748818

[8] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Commonwealth)

privacy legislation and thus the current approach in NSW, Victoria and the ACT requires many private health providers to comply with both state and Commonwealth legislation. This gap poses significant risks to the privacy (and consequently, other related human rights) of individuals whose information is handled by unregulated entities, and additionally imposes duplicate obligations on private health providers, resulting in additionally resourcing and administrative burdens.

Additionally, with the recent introduction of the NDB scheme, a number of entities who are not considered Australian Privacy Principle (APP) entities are subject or partially subject to the scheme in relation to part (for example, relating to tax file number handling) or the entirety of their dealings. Thus, the entities in question are expected, in practice, to implement and operate under the Scheme and the APPs whilst not actually being subject to the APPs. This inconsistent application of privacy law is likely to result in inconsistent privacy practices and uncertainty around accountability and regulatory requirements.

We suggest that Australian privacy law should be streamlined to facilitate uniform or similar regulation across jurisdictions. Unregulated entities should be brought under the aegis of an existing privacy regulatory scheme or law, and unregulated states should consider the introduction of privacy legislation to regulate the handling of personal information. Additionally, current regulators should consider the formation of an Australian Governmental Privacy Council, to facilitate uniformity of approach and the streamlining of Australian privacy regulation (for example, they may provide guidance around dual obligations). This council may wish to consider the creation of a principles-based privacy code or equivalent, to which all member-bodies are subject in relation to regulatory functions and activity. The council would not be required to provide guidance material on individual privacy legislation; rather, the individual regulators should each seek to update and provide greater visibility of their existing guidance to stakeholders.

National security surveillance

As the capacity of technology increases, so too does its capacity to capture and process information, often automatically. Additionally, the quantity and fields of 'information about personal information' (or metadata) will continue to expand as technology evolves.

The 2015 amendments to the *Telecommunications (Interception and Access) Act 1979* (Commonwealth), or TIA, require Australian telecommunications providers to collect and retain specified types of telecommunications data (or 'metadata') for a minimum period of two years. Whilst the TIA requires providers to comply with the Privacy Act in their handling of personal information, a lack of clarity in the definition of personal information- and whether metadata may itself be considered personal information- may cause uncertainty in the handling of personal information requests. We note that the Australian Federal Court recently ruled[9] that personal information does not include metadata; however, we also note that guidance from the Australian Privacy Commissioner suggests that a number of forms of metadata should be considered personal information.[10] Such uncertainty may cause in

[9] *Privacy Commisioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017)

[10] https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information

difficulties in the enforcement of data subject rights, as demonstrated in the overturning of the Privacy Commissioner's original decision in the matter of *Ben Grubb v Telstra*[11] by the Administrative Appeals Tribunal.

We suggest that the following criteria be revised against a human rights framework and clearly defined in legislation:

- the type of government agencies that may access personal information (such as metadata) for security reasons. This will require clear definition of key terms such as 'metadata', 'personal information', security reasons' and 'law enforcement agency';
- the means by which a matter will be found to be a 'national security risk' which outweighs the personal right to privacy; and
- How the information will be transmitted to law enforcement authorities.

Additionally, Australian legislators should consider the benefits of legislation which deals specifically with privacy in electronic communication (such as the the e-Privacy directive[12]). Such legislation better caters to the specifics of personal and non-personal data in this context and should, together with existing privacy legislation, form the protective framework against which all new technology should be held.

b) what can we learn about the need for regulating new technologies, and the options for doing so from international human rights law and the experiences of other countries?

The General Data Protection Regulation and its harmonisation of multiple data protection laws across multiple jurisdictions provides a possible mechanism for the harmonisation of existing Australian privacy laws. Australian regulators should consider whether the creation of a single privacy code or framework should be created for the purpose of harmonising privacy laws in Australia.

Furthermore, the European e-Privacy Directive[13] provides a live example of a means by which specific regulation of privacy in a technological context (specifically, in this instance, privacy in the context of electronic communications) may be undertaken, in conjunction with existing privacy legislation. Australian legislators should continue to observe the progress of this directive in the near future, and ultimately consider whether or not an equivalent of the directive should be introduced as a means of providing clear, specialist guidance on matters of technology and privacy.

c) what principles should guide regulation in this area?

In keeping with the significance of privacy and its related rights, we believe that the key principles which should govern the development of any technology should include:

- Transparency
- Accountability

11 http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2015/35.html

12 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*

- Equality
- Fairness
- Safety
- Purpose limitation
- Efficiency
- Accuracy
- Innovation

4. In addition to legislation, how should the Australian government, the private sector and other protect and promote human rights in the development of new technology?

Human rights cannot be upheld by the use of legislation alone; industry engagement and participation are key. To that end, Deloitte supports:

I. The creation of a joint government and private industry expert body. This body would be responsible for providing on-request assistance and information on industry-specific queries related to human rights to technology companies when sought; and

II. The introduction of a co-regulatory system which involves the use of a voluntary trust mark and compliance scheme. Much like the Information Security Management Systems (ISO) standards, the technological trust mark would require compliance with publicised, specific standards (which should contain specific requirements around the use of personal information and the protection of personal privacy). Compliance with these standards would be assessed by the body in paragraph I, and certification could be renewed for an agreed predetermined period (such as annually, biannually or as required). Additionally, this body would facilitate industry engagement and a practical means of ensuring that emerging technology is developed in accordance with human rights principles.

Final Thoughts

We welcome the growth of Australian technological innovation and development, and its potential for enormous benefit and growth. Concurrently, we strongly support the responsible creation and enhancement of laws and other regulatory frameworks, to be developed alongside technology, to ensure that human rights and freedoms of individuals are protected.

We thank you for the opportunity to comment on the Issues Paper, and look forward to reading your findings.

Yours sincerely,

[redacted] [redacted]

David Owen

Partner

Michele Bahari

Privacy and Data Protection Manager