Making privacy core business

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000

Privcore

Artificial Intelligence
Strategic Policy Division
Department of Industry, Innovation and Science
Via email: artificial.intelligence@industry.gov.au

30 May 2019

Dear Department of Industry, Innovation and Science,

Submission:
Consultation on Artificial Intelligence, Australia's Ethics Framework - A Discussion Paper

Introduction

Thank you for the opportunity to participate in the consultation on Artificial Intelligence, Australia's Ethics Framework – A Discussion Paper (the Discussion Paper). This submission focuses on the privacy aspects raised in the Discussion Paper. Privacy concepts and risk mitigation strategies and tools are important to understand and can be built upon to assess Artificial Intelligence (AI) systems that process personal information.

The intention of this submission is to highlight Privcore's main points concisely, as my fellow privacy professionals, Anna Johnston, Nicole Stephensen and Nicole Hunt have gone into great detail on a number of privacy matters affecting the Discussion Paper. As such, Privcore does not intend to delve into the same level of detail, though reaches similar conclusions.

Privcore's submission covers five areas and makes five recommendations:

- Leveraging existing work being undertaken (impacts Discussion Paper Question 6)
- Privacy failing to keep up with technology, or technology failing to keep up with privacy? (impacts Discussion Paper Question 6)
- Consent to use or disclose personal information provides little privacy protection (impacts Discussion Paper Questions 3 and 4)
- Consumer research – privacy awareness levels on the increase (impacts Discussion Paper Question 2)
- AI principles – enforcement and going beyond minimum legal obligations (impacts Discussion Paper Questions 1, 5, and 7)

About Us

Privcore's team with 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens.

Annelies Moens, CIPT, FAICD, CMgr FIML, a privacy professional practising since 2001 founded Privcore. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She had the benefit of resolving hundreds of privacy complaints whilst working at the Australian privacy regulator and consults globally on privacy.

Annelies also studied artificial intelligence and machine learning at tertiary level, is a qualified legal practitioner and holds an international MBA. Her bio is available at: www.privcore.com/bios.

Leveraging existing work being undertaken

Privcore acknowledges the extensive research undertaken by the authors of the Discussion Paper to identify and locate relevant materials; this research is valuable. As mentioned in the Discussion Paper, a number of organisations globally are developing AI frameworks and principles. In Australia alone, the Victorian Privacy Commission and the Australian Human Rights Commission with the World Economic Forum have already, or are, completing work in this area. The latter are undergoing a similar consultation process exploring models of governance and leadership on artificial intelligence in Australia.

Recommendation One: Leverage existing work both locally and internationally to ensure consistency rather than having disparate AI principles, frameworks and governance models developed.

Privacy failing to keep up with technology, or technology failing to keep up with privacy?

The Australian Privacy Principles (as well as most other privacy principles globally) are deliberately technology-neutral and designed to be able to be applied in multiple contexts. If legislators had to draft specific laws every time there was a new technology, we would never be able to advance at the pace to which we are now accustomed. What matters is how these laws are interpreted, applied and enforced in new contexts. This is where privacy regulators play an important educational role and where more mainstream (rather than outlier) decisions need to reach the public to enable the increased understanding of privacy regulation as it is applied in practice by regulators.

Page 7 of the Discussion Paper states that "privacy measures need to keep up with new AI capabilities" and goes on to discuss biometrics implying that we have had rules for collection and use of fingerprints, but not other forms of biometrics. Sensitive personal information in the *Privacy Act 1988* (Cth) includes biometric information that is to be used for the purpose of automated biometric verification or biometric identification.

Additionally, the Discussion Paper when referring to the Cambridge Analytica and Facebook case study states on page 28 that: "For industry, the incident serves as an example of the cost of inadequate data protection policies and also demonstrates that it may not be sufficient to merely follow the letter of the law". Facebook is currently being investigated by privacy regulators globally and those regulators are finding that Facebook was in breach of privacy law. See for example, the findings of the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia where it advised that Facebook had committed serious contraventions of Canadian privacy laws and failed to take responsibility for protecting the personal information of Canadians. The Office of the Australian Information Commissioner is also investigating Facebook in relation to this matter as are other jurisdictions.

Recommendation Two: Determine what, if any, privacy measures, their interpretation, application and enforcement in Australia are inadequate in the context of AI.

Consent to use or disclose personal information provides little privacy protection

There is a major misconception that the consent process is fundamental to protecting privacy as expressed on pages 28 and 64 of the Discussion Paper. That is a flawed understanding of privacy legislation, exhibited unfortunately by many entities. Indeed, to the contrary, (whilst counterintuitive to non-privacy experts) consent processes are more likely to lead to privacy and social licence issues, as consent is an exception that should be used in limited circumstances. Its overuse and inappropriate implementation in the digital world does little to build trust. How purported "consent" is sought is also problematic from a privacy and social licence perspective (consider bundled consents, consent in terms and conditions, forced consent in order to use service etc). A good discussion of the use of consent can be found in "The Pathologies of Digital Consent" by Neil Richards and Woodrow Hartzog, forthcoming Wash. U. L. Review (2019).

For example, an organisation bound by the *Privacy Act 1988* (Cth) that decided to collect more information than it reasonably needed for its functions or activities would likely breach the collection principle (APP 3). Seeking consent from individuals to use or disclose that personal information which had been unnecessarily collected would not rectify the breach of the collection principle. This type of scenario would commonly be seen in the downloading of apps onto mobile phones. Quite often, when installing apps, users are asked to "consent" to the app accessing identity, contacts, location, photos etc, when there is no apparent reason for the app to collect all this personal information for the purported function that it offers to its users.

One of the most fundamental privacy tenets is to minimise data collection, a concept which is not discussed in the Discussion Paper. This is one of the key considerations for AI which uses large amounts of personal information.

Recommendation Three: Obtain and ensure advice from privacy experts and regulators is acted upon and understood by those developing AI principles and ethics frameworks.

Consumer research – privacy awareness levels on the increase

Australians are not as privacy naïve as Chapter 3 of the Discussion Paper implies as primary research quoted in the Discussion Paper on pages 27-29 suggests otherwise. We are reaching a tipping point with the general population in Australia distrusting media, government, business and NGOs as evidenced by the 2019 Edelman Trust Barometer.

Chapter 3 of the Discussion Paper on Data governance incorrectly summarises research commissioned by the Consumer Policy Research Centre of Australia. The Discussion Paper suggests that most people think that when a company has a privacy policy, it means the site will not share their personal information with other websites or companies. The Discussion Paper also suggests on page 27 that most people think that all mobile/tablet apps only ask for permission to access things on their device that are required for the app to work. The cited research from the Consumer Policy Research Centre entitled "Consumer data and the digital economy: emerging issues in data collection, use and sharing" actually suggests the opposite at page 29 (as shown in the table reproduced below (emphasis added)):

Table 1. Australian consumer knowledge about data collection and sharing.

	True	False	Don't know	Correct answer
Companies today have the ability to follow my activities across many sites on the web*	91%	2%	7%	True
In store shopping loyalty card providers like Flybuys and Everyday Rewards have the ability to collect and combine information about me from third parties	73%	4%	23%	True
Some companies exchange information about their customers with third parties for purposes other than delivering the product or service the customer signed up for	88%	2%	10%	True
All mobile/tablet apps only ask for permission to access things on my device that are required for the app to work	26%	47%	27%	False
When a company has a privacy policy, it means the site will not share my information with other websites or companies*	19%	59%	22%	False

*Questions derived from Turow et al (2005)

Likewise, when the Discussion Paper reports on statistics from the Office of the Australian Information Commissioner on data breaches at page 29, it incorrectly shows that human error is the cause of 59% of data breaches, when in fact the cited source shows that human error only accounts for 36% of the causes of data breaches in the period April-June 2018. Human error continues to represent only a third of causes for all notified data breaches based on the OAIC annual statistics to date.

The OAIC also produces Australian Community Attitudes to Privacy surveys, the last of which was conducted in 2017. It shows that Australians are increasingly concerned about the privacy of their personal information.

Recommendation Four: Ensure appropriate representation of consumers' privacy views.

AI principles – enforcement and going beyond minimum legal obligations

Principles without enforcement or other ramifications if principles are not followed become feel-good exercises with little practical outcome for individuals. As such, Privcore suggests that thought should be given to what happens when harms occur due to AI ethics principle(s) not being implemented.

Privcore suggests that AI in particular needs to be assessed when the probability of the individual being aware of the autonomous processing is low and the potential harm from false positive or false negative decisions is either medium or high as per the below table developed by Privcore.

Table: When AI Needs to be Assessed. Developed by Privcore.		Harm resulting: False Positive or False Negative Decision		
		High	Medium	Low
Probability of individual being aware of the autonomous processing	High			
	Medium			
	Low			

Consideration, at the outset should be given to whether an AI system is in fact the most appropriate tool for the problem being addressed since bias, amongst other issues, is a massive issue in machine decision making (and human decision making). AI can be biased, leading to discrimination and reintroducing stereotypes if not carefully assessed and analysed (consider for example the use of female voice assistants). Algorithmic Impact Assessments, much like Privacy Impact Assessments can help identify and minimise such risks. Principle 5 on Fairness suggests that AI systems must not result in "unfair" discrimination. This implies that discrimination that is fair is acceptable. Legally, some forms of discrimination are never acceptable.

Any principles referring to minimum compliance standards or complying with the law do not fit in ethical frameworks. Complying with the law should be seen as a hygiene factor and not part of an ethical framework which arguably should go beyond the minimum requirements of law. In particular, the third core principle for AI titled "Regulatory and legal compliance" and the fourth principle titled "Privacy protection" fall into this category.

Principle 2 on Do no harm is limited to civilian AI systems and excludes military uses of AI which the Discussion Paper indicates on page 9 are out of scope. Should an ethical framework not aspire to what is permitted or not permitted in all AI systems regardless of deployment?

Principle 1 on Generates net-benefits states that "The AI system must generate benefits for people that are greater than the costs". This is not measurable or specific enough, nor does it consider distribution of those benefits or costs. Most AI systems are set up to generate or save money for a certain group of people as the ultimate goal, even if there are also altruistic purposes served.

Privcore agrees that core principles for AI must include 6. Transparency & Explainability; 7. Contestability and 8. Accountability.

Recommendation Five: Develop within the AI Ethics Framework the consequences of not adhering to AI principles and ensure the AI principles go beyond minimum legal requirements.

Conclusion

There are many human rights, governance and privacy concepts, if correctly interpreted and applied that are useful to build upon to develop AI ethical principles and assess AI's risks and benefits to the relevant populations. Accordingly, closer engagement with human rights, governance and privacy experts will enhance the work being done by the CSIRO, Data 61 and the Department of Industry, Innovation and Science on developing Australia's AI Ethics Framework. Privcore would be pleased to contribute to these developments.