28 May 2020

AIBotics 2020

Personal Data Protection Commission
Ministry for Communications and Information

Email: DataRegulation@mci.gov.sg

Dear ***Sirs***

Response to the Invitation on
Public Consultation for Personal Data Protection (Amendment) Bill

APARA (Asia Pacific Assistive Robotics Association) is a non-profit organization and has been founded with the intent to help users of technology place emphasis on the Augmentation of Human Potential. In particular, we study the aspects of the Ethical and Responsible use of AI and Robotic applications. APARA collaborates with counterpart industry associations with a common cause as well as with research institutes and universities on practical research and development projects.

A Strategic Committee on the Ethical and Responsible use of AI (ERAI) was established on 17 January 2020. Through this strategic committee, APARA engages with industry leaders, both locally as well as overseas to place a heavy emphasis on how users of technology can adequately understand and adopt good practices in ethical and responsible. We believe it is not a function of simply complying with a document of governance but the success of such a practice involves:

- **Awareness**
- **Assimilation**
- **Adoption**
- **Acceleration**

Herewith, we submit our response to the public consultation on the draft Personal Data Protection (Amendment) Bill as attached. Thanking you in advance,

Yours Sincerely,

Kat Ong (Ms)
Secretariat
Asia Pacific Assistive Robotics Association
Email: secretariat@apara.asia

Public Consultation for Personal Data Protection (Amendment) Bill

Submitted by

ERAI

Ethical and Responsible Use of AI Committee (ERAI)
Asia Pacific Assistive Robotics Association (APARA)

Email: erai@apara.asia

Chairman:	Mr Teng Chuan Hiang
Members:	Mr Adrian Chan
	Mr Eitan Netzer
	Dr Lim Chong Hee
	Mr Julian Tan
	Mr Roland Yeow
	Mr Amritanshu Roy
Advisor:	Mr Oliver Tian

1. Introduction

The motivation of our submission for this public consultation paper is to better link aspects of data protection to the individual and without stifling the adoption of artificial intelligence (AI). Singapore's economic growth in the next 20-30 years will hinge heavily on the adoption of AI, and data is a mandatory ingredient for this technology work successfully. It is worth to highlight that AI has several unique characteristics from a technology standpoint and one of them is the implementation cycle. It is not the same as the traditional IT implementation methodology. Neither is true in regards to the benefits of AI where the magnitude of change is profound as well as the impact on the results. AI implementation is sharp to the point and development lifecycle can be 50% shorter to realise. With a powerful technology deployed in a shorter time with higher impact, there is potential exposure when unethical behaviour pervade the use of this technology. Our Committee Members deliberated and would like to share such an innovation process below which gives us a good understanding of the implementation lifecycle.

`The AI Innovation Process

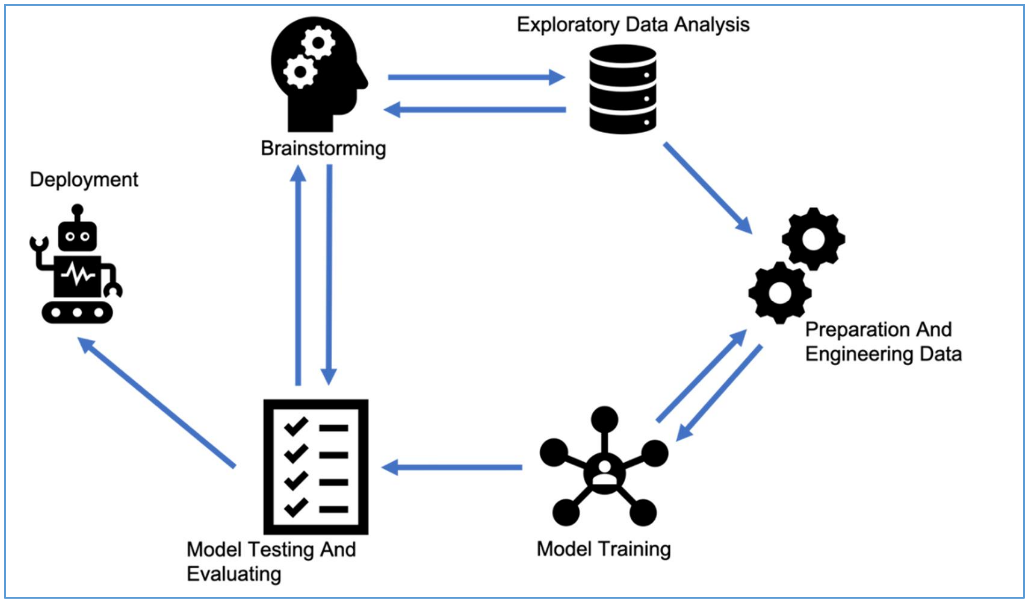

Exploratory Data Analysis
Brainstorming
Deployment
Preparation And Engineering Data
Model Testing And Evaluating
Model Training

Diagram adopted from CoreAI

The mission of **ERAI** is to help the constituents of societies to embrace AI more readily to advance our cause. We believe there is a vital need for **trust** between organisations who implement AI and consumers who uses the AI. We help the public grasp the concepts of AI in relation to their use, so they understand the **risks** involved. This is achieved by **simplifying** the information produced by different publications into laymen terms for easy understanding and to resonate with their use.

Policymakers and stakeholders must abridge with the advancements of technology. It is important for any agencies not to lag behind in its full appreciation of the impact that technology is having on societies. For example, with the advance capabilities of AI, it is no longer sufficient to anonymize data. AI system is fully capable of piecing fragmented data together to make a prediction of who the person is, and accuracy is quite high.

The strength of a policy framework is as good as the degree of adoption and user practice. Enforcement and incentives can further enable the success of such policy deployment.

2. Strengthen Accountability

1. We propose that the strengthening of accountability put strong emphasis on organisations that are using AI or intend to use AI for their business purposes. These organisations should understand how the existing legal framework applies to their use of data for AI, and that they support appropriate programmes to educate the people who are entrusted to discharge this responsibility. Establishing clear standards and guidelines with reference to data protection accountability and how AI will be adopted are crucial to creating a transparent system. Stringent auditing standards with proper documentation is essential to maintaining a high level of trust for everyone concerned. **Institutional framework created to support these initiatives can lead to job creation both for the private and public sectors**.

2. Similar to financial accountability, organisations should treat data as an important asset when their business relies heavily on data collection and processing to function optimally. At Google and Facebook, without the data they possess and are still collecting, their operations cannot function optimally and may be incapacitated to grow. A "data value" can be attached to this data asset to exemplify the critical importance of data. **Again, this is another job growth potential for the policymakers to consider.**

3. Some organisations that by the nature of their business collect huge amount of personal data such as chat messages, like WhatsApp, must adhere to a more stringent standard. The same should apply to organisations who intend to use AI to process such data. Private chats should be strictly out of bounds unless a court order is served for criminal charges. But we have to be careful how such orders are carried out because as more instances will be exposed, and there must be further considerations to mitigate the risks of destabilising the system of trust.

4. Data security requirements should be clearly stated so that organisations are aware of the minimum security standards to protect the data from hacking. Any basic tier of hosting offered by data centres such as AWS should clearly comply with such data security requirements and if an exception is required there should be a process to make such requests with proper authorization. Businesses that operate in areas affected by these policies should have the clear understanding of their obligations and responsibilities on data collection and usage. Different types of business collecting different types of data, and their intention to use the data, should be transparent and make available for audit.

5. These increased standards of accountability will inevitably increase the cost of doing business. Consideration for SMEs should be thought through to help them mitigate these increases in costs. We must try to help these companies comply with higher standards and yet allowing them to grow their business. If would be disastrous if more legislations kill entrepreneurship and small businesses since they are often the ground where new ideas are sowed to spur growth. **Promoting the use of AI in this regard actually serves both purposes, adhering to higher standards and advancing capabilities.**

6. Relevant and strong incentives should be given to organisations to remain vigilant and comply with the stipulated standards. Clear examples of such behaviour should be communicated to the public so these organisations has a distinction from the rest. The "stick alone" approach handicaps the balance of the "carrot and stick" model, hence discouraging successful deployments. Make certification mandatory for data officers and other AI related roles but provide financial support them with subsidies. **Mandate any company who has intention to use data for AI to undergo certification on ethics and responsible use of this technology along with higher standards for data protection requirements.**

7. Accompanying the accountability framework, there should be a technology framework in the form of a recommendation table to help organisations build better IT infrastructure to stay relevant to the accountability requirements. This also helps the organisations to build better IT infrastructure to support its data management requirements with proper documentation and process. Data management framework can help many organisations improve their data management practices internally. This will inevitably strengthen accountability with clarity for enforcement purpose.

ERAI and APARA can play a role to support and facilitate the above suggestions on accountability.

(The rest of the page is intentional left blank.)

3. Enabling Meaningful Consent

1. All data privacy policies provided by any organisations operating in Singapore should be centrally vetted and approved by PDPC. The data privacy policy agreement should not be an agreement that differs from organisation to organisation, at least at the fundamental level. This is an essential service the authority can provide to its citizen and alleviate this burden on the individual having to read such agreement which no one really does before accepting the data privacy policy. If there is a need to deviate from the standard terms of data privacy policy, these terms should be appropriately communicated to PDPC and then presented to the individual as an exception to the normal terms. When accepted, the individual must know that it is not outside the purview of PDPC to protect the individual.

   If one tries to read the data policy of Facebook, you can be assured of a convoluted experience navigating the different legal document. No individual is capable of dealing with such complex legal agreement just to use some basic services. This kind of business which is monetarizing data individually and collectively should be scrutinised by the appropriate authority before it is released to the public for use. We have to consider the risks of data abuse and misuse as our top priority to protect the public before any economic consideration. Moreover, no individual is capable of taking the organisations to task if there are any violations.

2. Consenting to the collection of data must be accompanied by a similar and notably easy process of deleting the data or at least have the assurance that when the individual request it to be deleted, it will be done. This requirement should be clearly stipulated but also applied only when it matters. Any individual should have the right to make this request when the person no longer wish to deal with the organisation and it is the duty of the organisation to ensure that this task is carried out as part of the accountability approach.

3. PDPC should consider using AI provided as a service to assist the individual to understand the risk factors of some of the terms of use and data privacy policy meted out by these organisations. This can be a national infrastructure to help the less informed or knowledgeable to deal with complex issues beyond their capabilities. AI technology, today, has the capability to “crawl through” text and highlight specific terms to the user in consultation. Such an App can be made available as a public tool for convenient download which dovetails PDPC’s effort to generate greater appreciation of data policies.

4. If the data collected is going to be used by AI system, this type of consent should be made explicit. AI system can deployed a different level of capabilities to use the data to serve the individual better or to abuse it in the case of unethical practices.

5. It is important that the individual understand the risks involved when companies intend to use AI and that the trust must be established before going further. To mitigate these risks on behalf of the individual, certifications and audits can be introduced for companies who are using AI. There are international ethical standards and methods to ensure that AI systems are implemented in compliance with these standards. Ethics can be cultural specific, hence there is a need to localize some of these standards.

ERAI and APARA would be able to assist and support programs on the meaningful content enablement.

4. Increasing Consumer Autonomy

1. There should be a national infrastructure and mechanism to allow for data to move from one organisation to another. Just like roads and bridges, this infrastructure should be managed by the state. Technology in this area is matured and robust but only when it is well managed and designed. Private sector or educational institutions can be roped in to support this infrastructure as usual but careful consideration on security is required. In fact, it is worth considering to assert that education institutions manned by professors will have an inert higher standards of adherence to manage such an important infrastructure.

2. Consumers should be empowered to exercise this right and the functions to transfer data or delete data should be **a mandatory built-in function** in any systems. However, since data is an asset to any organisations, such a design has to implement these functions with careful thoughts. There must be proper guidelines what, when and how the data is transferred without impeding the organisations ability to perpetuate. A useful consideration is to classify and/or declassify data accumulated and valuated to support data transfer.

3. Consumer autonomy also comes with user awareness and perceive value of data. Consumers today may not be fully cognizant of the value of data which they offer and the damages associated with data abuse. Consumers have a *'right'* to know.

APARA would be keen to support and facilitate outreach programs to increase consumer awareness and levels of consumer autonomy.

5. Strengthening Effectiveness of Enforcement

1. Prevention is definitely better than cure. The approach to enforcement is prevention and to strengthen prevention we should consider the use of AI to police other AI systems. AI can efficiently scan any systems to detect weakness in the system when we can define what constitute a weak system.

2. While we are supportive that the PDPC enact specific legislatures to punish perpetrators of the new law, positive reinforcement programs can lend to be more effective outcome, too. Stricter laws and heavier punishments should be meted out to the perpetrators who abuses data by using AI. The magnitude of damage caused AI is far greater than when it is caused by conventional methods. This piece of legislature by no means is easy and needs careful considerations as abuses of data by AIs system less directly implicated but yet can be human like in terms of intelligence factors.

3. Similarly, enforcement could also refer to a system of data maturity credits which recognizes companies which execute exemplary practices of data management and demonstrates credible behavior to be role models for other companies to follow.

ERAI, under the auspices of APARA and guidance of PDPC, can drive a program to acknowledge exemplary use cases.

6. Statement of Interest

Ethical and Responsible use of Artificial Intelligence (ERAI) under APARA is a strategic committee with interest to promote the use of AI in a responsible and ethical manner. We act as a bridge to promote trust in the use of AI by educating the three constituents of our society; Community, Government and Businesses. Set up in January 2020, ERAI aims to:

a) ***To consider and recommend practical guidelines for the ideation, planning, development and adoption of AI and Robotic innovations***

b) ***To support, validate and extend existing governance framework on AI innovations without hampering progress***

c) ***To raise awareness and recommend critical competencies on the practical aspects of AI and Robotic Innovations***

7. Further Comments

Data misuse in the conventional method is not as severe as abuses discovered in AI systems. Data protection in the context of AI usage needs more thorough and careful thoughts to ensure consumers are protected. At the same time, legislature shouldn't stifle innovation by organisations. A balanced approach will not cut the job, but a principled approach is a better choice to tackle the issue. This could mean little and/or no compromise on the outcome but deciding what to protect and what is less important mitigating along the way.

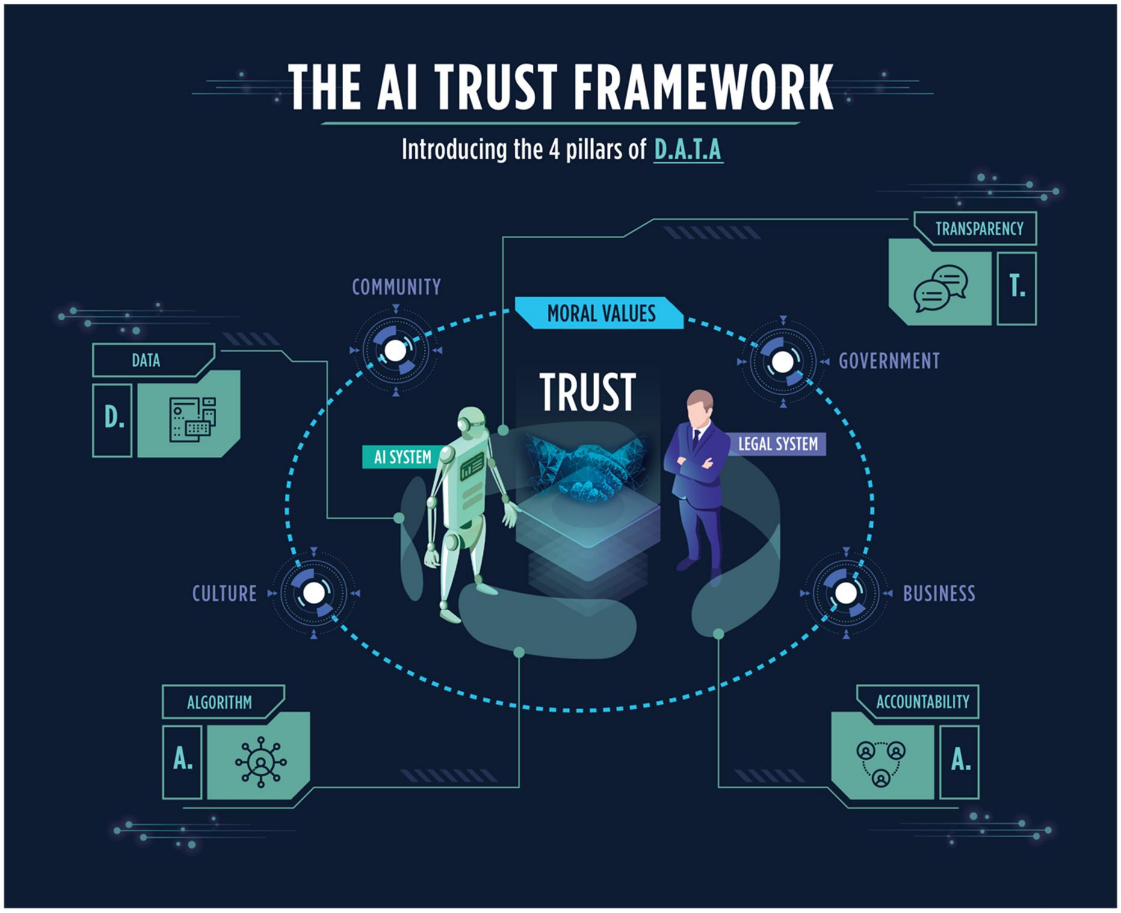
AI is more difficult to legislate considering the fact that AI is mimic of human like intelligence but yet does not have the conscience of a human to decipher right from wrong, autonomously. However, there are ethical AI concepts and methods to ensure this technology is used responsibly and ethically. We will face more dilemmas when we go deeper into the challenges of legislating AI and how data play a part in this entire system.

8. Conclusion

AI and data are going to fuel the future of our economies. It is more than a balanced approach - it must be a principled approach to weighing the issues. We should not compromise on data privacy protection as we can observe from what had happened when data is compromised at massive level committed by Cambridge Analytica. Neither can we compromise the free use of data for AI to serve our society better.

This outcome of free-flowing data for AI to use can only happen when people have trust in the system. Trust will be the most important currency, more important than data. As the world moved into the realm of AI, this phenomenon will accentuate the importance of trust. Without trust no individual will want to give their data to the organisation to keep and use. Only truly ethical organisations will earn and keep the trust to perpetuate their business and keep innovating with the data they collected using AI. The key characteristic of AI is the more data you feed it, the better the system performs. This incentive when fully realised and capitalised, is an incentive in itself to keep many organisations naturally morally good.

Appendix: The AI TRUST Framework



Design by Chuan Hiang and Esther Fang for ERAI - APARA

Data is the knowledge an AI system needs to acquire from the person and to serve them better. It is used to train the AI system to "know" you and it will be better with more data.

Algorithms is the "intelligence" needed to use the data to make prediction, extrapolation, deduction and inferences to build relationships for a predefined intended outcome.

Transparency is making the necessary provision for the AI system to be understandable and auditable by third party without exposing trade secrets when investigation is required. Contrary to the common notion that deep neural network is a black box, anything that is digital is traceable if proper documentation and audit trail data are captured.

Accountability is the standard by which entities can be held responsible for violating it. This calls for the community together with the practitioners of AI to come together to establish a gold standard for everyone to follow. The SGIsago presented at the World Economic Forum is an example of such documents for organisations to follow. There are other ethical standards including at the coding level for AI practitioners to set a higher standard of accountability.

(This is the end of the document.)