Recommendations for the creation of a governance framework for the protection of personal data used in the development of AI systems

2021 Digital Society Research Grant
21-DSRG-01

Researchers:
Assoc Prof Jaspal Kaur Sadhu Singh
Darmain Segaran
Arthi Ganesen (RA)

1. RESEARCH OBJECTIVES AND METHODOLOGY

RESEARCH OBJECTIVES

1. To identify the privacy risks resulting from the use of Big Data in AI systems to produce results through inferential analytics and automated data processing

2. To review existing law
   - Weaknesses
   - Coverage
   - Incompatibility with BDA & AI
   - Amendments

3. To explore and assess how legal frameworks in other jurisdictions have adopted (or otherwise) in managing the risks of BDAs to the data privacy legal regimes in place

4. To formulate recommendations for adoption in a self-governance data privacy framework by deployers (users) of AI

Concepetual Framework & Research Methodology

Conceptual Framework

The RALC (Restricted Access/Limited Control) Theory & The Just-Consequentialist Theory

Qualitative Legal Research for the Main Research Objectives

Doctrinal Legal Research when examining the national legislation, mainly the Personal Data Protection Act 2010

Comparative Legal Method when reviewing and exploring legal frameworks in other jurisdictions

Quantitative Research for the Dipstick Survey

Research Design: The research design is a non-experimental correlational quantitative survey.

Measurement: The survey was done through an ad hoc instrument consisting of a total of 8 structured response format items.

Data Analysis: Using descriptive statistics.

2. THE RESEARCH PROBLEM

The Research Problem

Data privacy laws were not designed to provide for the processing of personal data for inferential analytics or automated decision-making resulting from the use of Artificial Intelligence (AI) systems. Inferences drawn from Big Data, which are large data sets, do not fall within the sphere of traditional principles of the individual's right to privacy.

This research aims to make recommendations for the creation of a governance framework for the protection of personal data used in the development of AI systems. The data privacy governance framework must serve to manage the requirement of data privacy and protection standards without acting as an impediment in the use of AI systems.

Classes of Data: Novelty of the problem

Big Data	• extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions
Provided Data	• Provided by individuals
Observed Data	• Recorded automatically
Derived Data	• Produced from other data in a relatively simple and straightforward fashion
Inferred Data	• Produced by using a more complex method of analytics to find correlations between datasets and using these to categorise or profile people

3. FINDINGS OF SURVEY

Part A	Utility of the system		Question 1	Did you know why this particular system was deployed in this specific area?
			Question 2	Did you know the business model concerning this system (e.g. how it creates value for the organisation)?
			Question 3	Did you make clear to users what the purpose of the AI system is and who or what may benefit from the product/service?
Part B: Section 1	Transparency and Explainability	Pillar 1 *Explainability*	Question 4	Did you know the extent to which the outcome made by the AI system can be understood?
			Question 5	Did you ensure that an explanation as to a certain outcome can be made unde explanation?
			Question 6	Did you design th from the start?
			Question 7	Did you assess w the interpretabilit
			Question 8	Did you have acc
		Pillar 2 *Communication*	Question 9	Did you commun or any other mea system and not w
			Question 10	Did you label you
			Question 11	Did you put in pl reasons and crite clearly and intelli
			Question 12	Did you establish individuals' feedl this feedback to a
			Question 13	Did you also con risks, such as bia
			Question 14	Did you clearly c potential shortcor
Part B: Section 2	Privacy and Data Governance	Pillar 1 *Respect for Personal & Data Protection*	Question 15	Depending on the allow others to fl protection issues data collection (fi processing?
			Question 16	Did you build in personal data dep consent and the p
			Question 17	Was an officer re deployment of th
		Pillar 2 *Quality & Integrity of Data*	Question 18	Is the system alig Protection Act (M data privacy i.e. (
			Question 19	Did you establish storage, processir
			Question 20	If you are using e control of the quality of the external data sources used?
		Pillar 3 *Access to Data*	Question 21	Did you assess who can access individuals' data, and under what circumstances?
			Question 22	Did you ensure that these persons are qualified and required to access the data, and that they have the necessary competencies to understand the details of data protection policy?

Part B: Section 2	Privacy and Data Governance	Pillar 1 *Respect for Personal & Data Protection*	Question 15	Depending on the use case, did you establish mechanisms that allow others to flag issues related to privacy or data protection issues concerning the AI system's processes of data collection (for training as well as operation) and data processing?
			Question 16	Did you build in mechanisms for notice and control over personal data depending on the use case (such as valid consent and the possibility to revoke, when applicable)?
			Question 17	Was an officer responsible for data privacy involved in the deployment of the AI system?
		Pillar 2 *Quality & Integrity of Data*	Question 18	Is the system aligned with the principles of the Personal Data Protection Act (Malaysia) and widely adopted protocols for data privacy i.e. GDPR and ISO 27701/27001?
			Question 19	Did you establish oversight mechanisms for data collection, storage, processing and use?
			Question 20	If you are using external data in the AI system are you in control of the quality of the external data sources used?
		Pillar 3 *Access to Data*	Question 21	Did you assess who can access individuals' data, and under what circumstances?
			Question 22	Did you ensure that these persons are qualified and required to access the data, and that they have the necessary competencies to understand the details of data protection policy?

AI Ethics Maturity of Data Protection and Governance

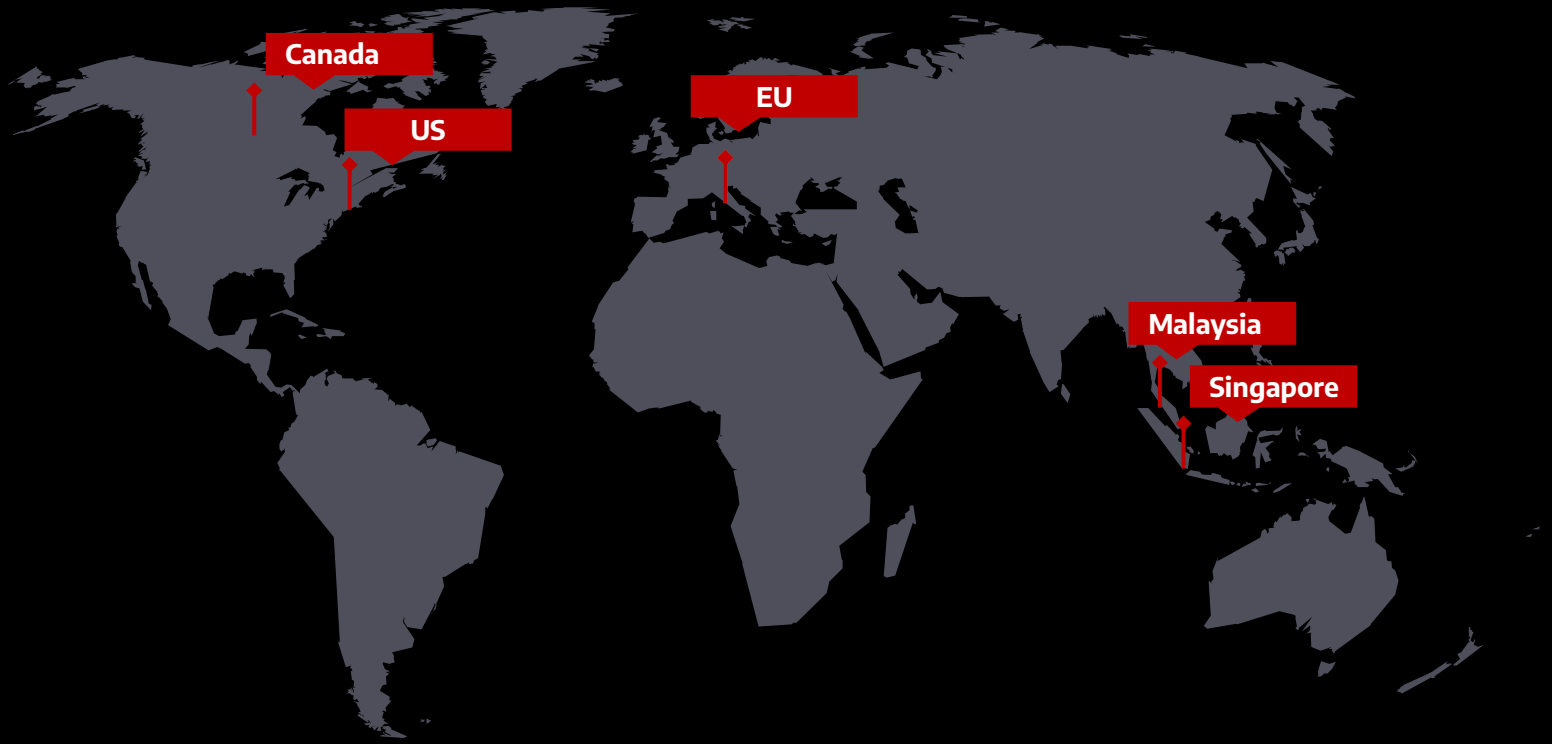
The Survey results are available at https://www.ai-doctrina.info/malaysian-ai-ethics-maturity-report-2021

There are several anomalies within the DIS and AI Maturity measurements. By anomalies, the researchers have found that there were industries that were categorised as DIS that did not perform well in the adoption of ethical principles, and conversely, in non-DIS, there were indications of good ethical practices

4. SUMMARY OF RESEARCH FINDINGS

OUR RESEARCH

COMPARATIVE STUDY



Data Protection Laws – Legal Responses to Big Data and AI

Malaysia

PDPA 2010

X Anonymised data (√ in Codes)

X Profiling

? Processing

? Consent

? Notice

EU GDPR

√ Profiling

Anonymised data

X Right to explainability

? Consent

? Notice

Proposals – AI Law

Classification of Data Practices

Singapore

PDPA 2012

Amendments in 2020

√ Deemed Consent

√ Transparency – Legitimate use

? Notice

Canada

PIPEDA 2000

? Valid consent – different forms of consent

Proposal - Bill C-12

Exceptions to obtaining consent

Profiling

De-identified data

Automated decision-making

US

Proposals

Data Protection Act 2021

The GOOD AI Act 2021

Threats presented by AI & BDA to DPL

Scope of personal data

Definition excludes anonymised data.

Anonymised data lacks definition.

Whether proper anonymising standards have been imposed.

Does not include inferred data.

Consent & lawful processing

Whether consent extends to the processing performed in analytics.

Notice & purpose

Concerns around transparency of use.

Whether notice is sufficiently detailed.

Issues with unsupervised learning.

Automated decision-making

Issues of explainability and transparency.

Threats presented by DPL to AI & BDA

“Sharp-corners” dilemma

Difficulty in predicting insights that may be garnered.

Impractical to obtain consent for a specific purpose.

Data minimisation dilemma

Limitation imposed by necessity principle.

Analytics may discover corelations that may go beyond necessity.

Data retention & consent withdrawal dilemma

Limitation of deletion of data request or after use expires.

Undertake analytical processes afresh.

Automated decision-making

Onerous duty of explainability and transparency in low-risk systems.

RECOMMENDATIONS FOR INCLUSION IN THE GOVERNANCE FRAMEWORK

Graduated Consent

Though “just in time notifications”.

To seek consent to new uses of data as they emerge.

Improved definition of “processing”

To include inferential analytics or automated processing

Improved requirement for notice & transparency

Inclusion of standards of fair and transparent processing.

Comprehensive privacy notice and updates.

Right to explanation

Clear classification of data practices where such a right is essential.

Classification of risks based on data practices using automated decision-making.

RECOMMENDATIONS FOR INCLUSION IN THE GOVERNANCE FRAMEWORK

Algorithm that unlearns & prevents re-identification

Use of differential privacy

Privacy by design/default

By design - Using technical and organisational measures (pseudonymisation) to implement DPP

By default – only data which are necessary for specific purpose are processed. Ensuring data minimisation.

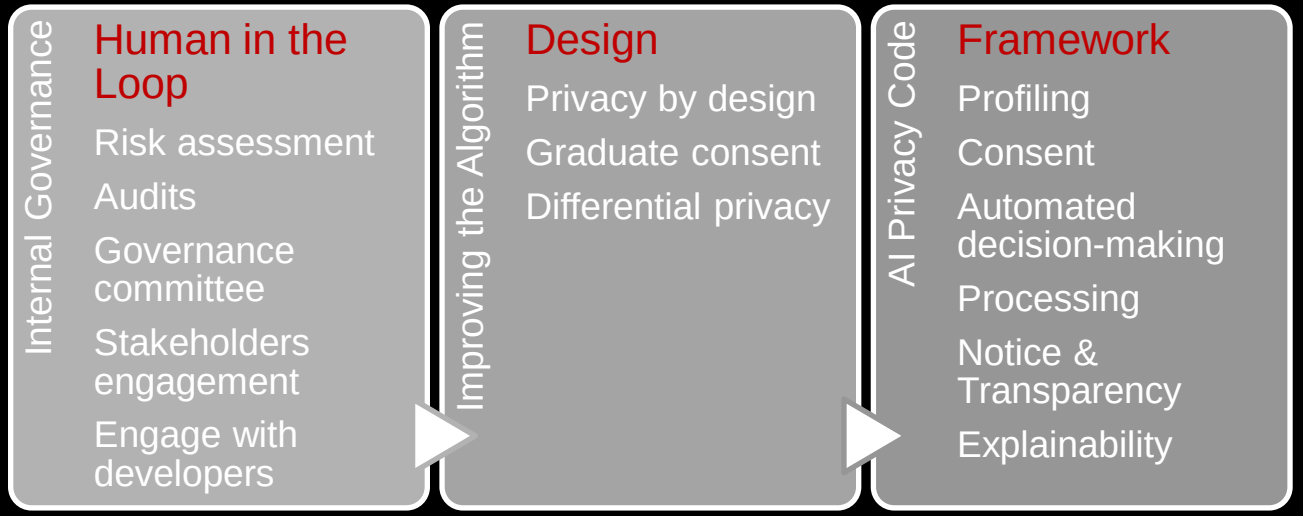
Human-in-the-loop

Human oversight & governance.

DPIA & HRIA

Regulator – e.g. AI Rights Commissioner

Graduated Adoption of Recommendations



THE TEAM

Assoc Prof Dr Jaspal Kaur Sadhu Singh
Lead Researcher

Darmain Segaran
Co-Researcher

Arthi Ganesen
Research Assistant

THANK YOU