World Law Group

New Paradigms for Addressing Emerging AI & Data Protection Issues

April 15, 2020

World Law Group – Quick Facts

Why World Law Group

- WLG is ranked one of a few “Elite” (Band 1) law firm networks, according to Chambers and Partners
- Qualified, trusted advisors
- Global coverage and local expertise
- Seamless client services
- Established in 1988, our firms have been working together for more than 30 years

Our Global Network of Premier Local Firms

Argentina: Alfaro-Abogados
Argentina: Bruchou, Fernández Madero & Lombardi Abogados
Australia: MinterEllison
Austria: CMS Reich-Rohrwig Hainz
Belgium: CMS Belgium
Brazil: TozziniFreire Advogados
Canada: Davies Ward Phillips & Vineberg LLP
Canada: Goodmans LLP
Cayman Islands: Campbells
Chile: Urenda Rencoret Orrego y Dörr
China: Zhong Lun Law Firm
Colombia: Philippi, Prietocarrizosa Ferrero DU & Uría
Costa Rica: Arias
Denmark: Bech-Bruun
England: Gowling WLG
Finland: Castrén & Snellman
France: Soulier AARPI
Germany: CMS Hasche Sigle
Germany: Taylor Wessing
Greece: Bahas, Gramatidis & Partners
India: AZB & Partners
India: Vaish Associates
Indonesia: Makarim & Taira S.
Ireland: Mason Hayes & Curran
Israel: Herzog, Fox & Neeman
Italy: Gianni, Origoni, Grippo, Cappelli & Partners
Japan: City-Yuwa Partners
Korea: Bae, Kim & Lee LLC
Luxembourg: Arendt & Medernach
Malaysia: Shearn Delamore & Co.
Mexico: Santamarina y Steta S.C.
The Netherlands: CMS Netherlands
Norway: Advokatfirmaet Schjødt
Paraguay: Gross Brown
Poland: Sołtysiński Kawecki & Szlęzak
Perú: Payet, Rey, Cauvi, Pérez Abogados
Philippines: SyCip Salazar Hernandez & Gatmaitan
Portugal: PLMJ
Russia: CMS Russia
Singapore: WongPartnership LLP
South Africa: ENSafrica
Spain: Cuatrecasas
Sweden: Setterwalls
Switzerland: CMS von Erlach Poncet
Taiwan: Formosa Transnational
Thailand: Chandler MHM Limited
Turkey: Hergüner Bilgen Özeke
UAE: Al Tamimi & Company
Uruguay: Guyer & Regules
USA – California: Greenberg Glusker LLP
USA – District of Columbia: Arnold & Porter
USA – Florida: Greenberg Traurig PA
USA – Georgia: Miller & Martin, PLLC
USA – Illinois: Drinker Biddle & Reath LLP
USA – Massachusetts: Locke Lord LLP
USA – Texas: Hunton Andrews Kurth LLP
USA – Washington: Lane Powell PC
Venezuela: D'Empaire
Vietnam: VILAF

Panelists

Chung Nian Lam

WongPartnership LLP, Singapore

chungnian.lam@wongpartnership.com

Monique McAlister

Goodmans LLP, Toronto, Canada

mmcalister@goodmans.ca

Vivian Gazel

Arias, San Jose, Costa Rica

Vivian.Gazel@ariaslaw.com

New Paradigms for Emerging Issues

Topics:

- What are key areas that regulators are looking into?
- How are people reacting to these emerging issues?
- As AI and big data applications impacting life and liberty become more pervasive, what are the legal and ethical issues that need to be addressed?

Key Areas for Regulators - Singapore

Reviews will support objectives of supporting data-driven innovation yet strengthening organizational accountability and consumer trust

- Enhancing data security
  - Mandatory breach reporting, treatment of ID numbers, cloud services
- AI governance frameworks
  - Model Governance Framework 2.0, Trusted Data Sharing Framework
  - Responsible use of biometric technology
- Data portability and data innovation
- Potential updates to the PDPA
  - Enhancing enforcement, accountability, bases of handling personal data

Key Areas for Regulators – Costa Rica

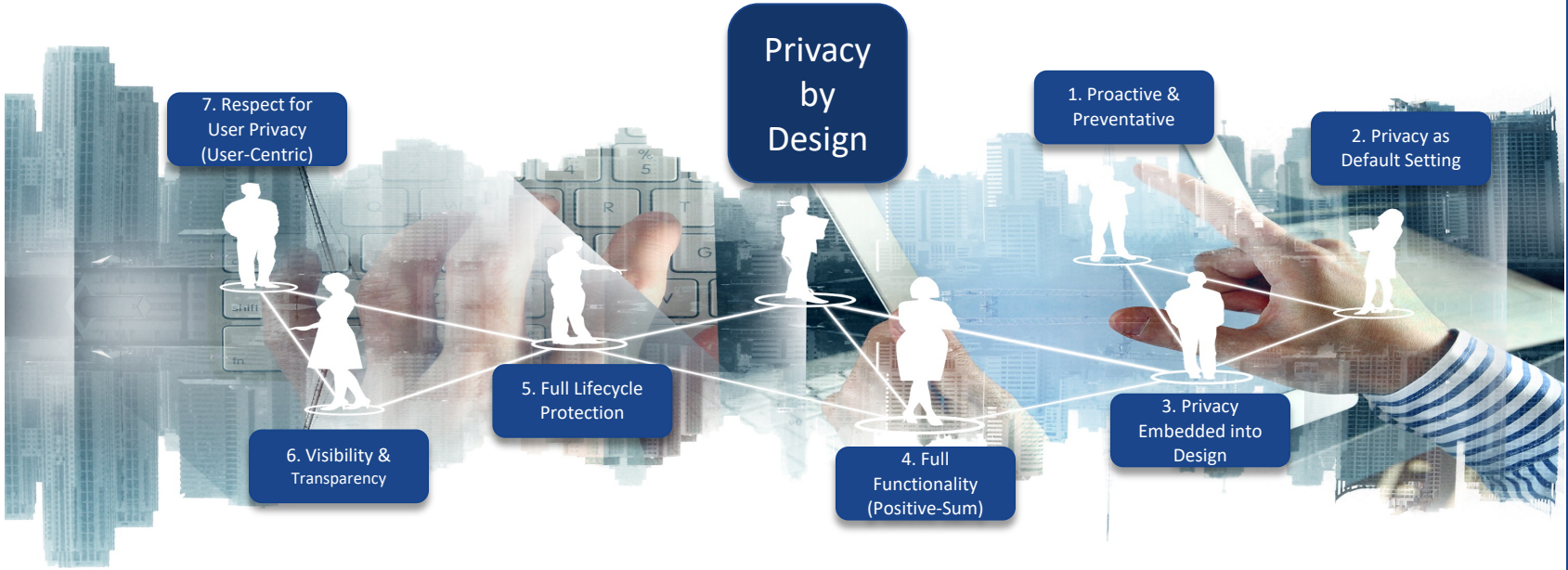
- Costa Rican Data Privacy Acts dates 2011 and its regulation from 2013, they do not foresee specific provisions on AI.
- The Data Protection Authority (PRODHAB) has mainly focused on addressing claims and has not yet addressed specific challenges that AI faces.

Key Areas for Regulators - Canada

- Consultation by Office of the Privacy Commissioner of Canada (OPC) on the treatment of AI under Canada's federal private sector privacy statute, the Personal Information Protection and Electronic Documents Act (PIPEDA).
- AI presents fundamental challenges to foundational privacy principles in PIPEDA: (a) limiting collection; (b) purpose specification; (c) retention period; (d) consent; and (e) transparency.
- OPC proposals:

1. definition of AI to clarify applicable legal rules
2. rights-based approach - data protection principles protect a broader fundamental human right to privacy
3. right to object to automated decision-making and not to be subject to decisions based solely on automated processing
4. right to explanation and increased transparency re: automated processing
5. Privacy by Design and Human Rights by Design in all phases of processing and data collection
6. compliance with purpose specification and data minimization principles should be realistic and effective
7. alternative grounds when obtaining meaningful consent is not practicable
8. flexibility in using non-identifiable information and protect against re-identification
9. ensure data and algorithmic traceability
10. mandate demonstrable accountability for the development and implementation of AI processing
11. empower OPC to issue binding orders and financial penalties for non-compliance

Privacy by Design – 7 foundational principles



Developed in 2009 by Ann Cavoukian, Ph.D., Former Information & Privacy Commissioner for Ontario, Canada

Emerging AI & Data Protection Issues

- How to balance privacy rights and public health during the COVID-19 pandemic?
- Can human rights and dignity be preserved when using automated processing and decision-making?
- Should technological advancement be suppressed by privacy rights?
- Does public interest disclosure trump proprietary algorithms?

Emerging Issues & Reactions

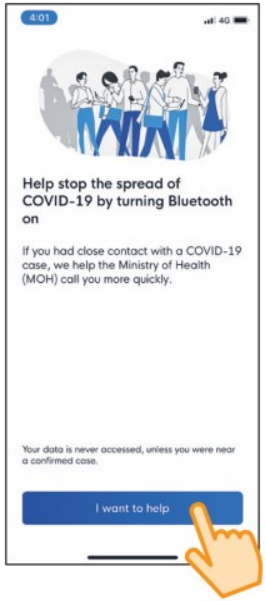
- Balancing privacy and public health during the COVID-19 pandemic
  - Singapore: TraceTogether app for contact tracing minimises the collection of personal data, uses temporary IDs, lack of consent for handling of personal data for contact tracing within emergency exception
  - Costa Rica: Although privacy laws apply, informing the people about the situation is necessary. Therefore, anonymization of data is key during this time.
  - Canada: OPC - "During a public health crisis, privacy laws still apply, but they are not a barrier to appropriate information sharing." Hesitancy re: collection, retention and abuse of biometric data.
- Automated processing and decision-making
  - Singapore: Model Governance Framework released to guide organizations on approaches to AI adoption
  - Costa Rica: Our Government has implemented an app that helps individuals report their symptoms and medical history and AI is used to determine whether the individual could be a risk patient and the Health Authorities can monitor this individual closely.
  - Canada: Federal government criticized for lack of transparency in COVID-19 modelling. Now using a private company's big data analytics platform to help model and monitor spread of COVID-19, and inform government decision-making. AI not yet used to make decisions on allocation of healthcare resources.

What is TraceTogether and how does it work?

TraceTogether is a contact-tracing smartphone app that enables the Ministry of Health (MOH) to quickly track people who have been exposed to confirmed coronavirus cases.

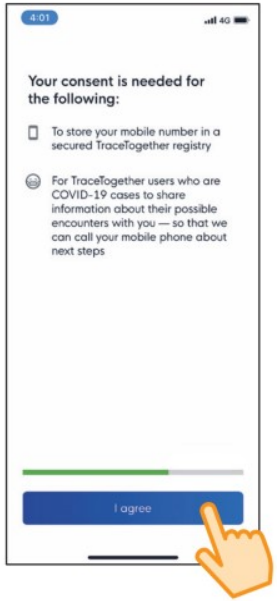
1 Users here can download the app on the Apple App Store or the Google Play Store.

SCAN TO DOWNLOAD

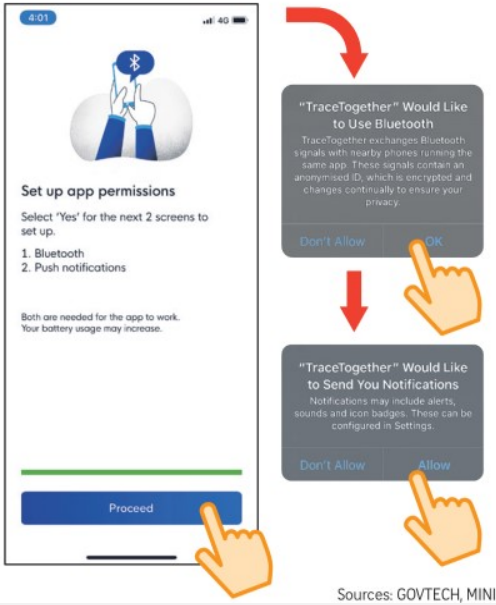


2 Users have to input their mobile phone number for MOH to be able to contact them quickly. The number is the only data collected by the Government through the app.

3 During the initial set-up, users have to give their explicit consent to be able to use the app.



4 Users will then have to enable push notifications and location permissions, and keep the Bluetooth function on their phones turned on.



5 This is because the app uses short-distance Bluetooth signals that are exchanged between phones to detect other TraceTogether users in close proximity.

6

- Official contact tracers who call users will provide a code that users can match with a corresponding verification code on their app.
- Once authenticated, users will be given a PIN number that allows submission of logs when entered.
- Official contact tracers will not ask for personal financial details or transfer of money.

Sources: GOVTECH, MINISTRY OF HEALTH PHOTOS: GOVTECH STRAITS TIMES GRAPHICS

Model AI Governance Framework (SG)

Guiding Principles

Decisions made by AI should be **EXPLAINABLE, TRANSPARENT & FAIR**

AI systems should be **HUMAN-CENTRIC**

From Principles to Practice

Internal Governance Structures and Measures

- Clear roles and responsibilities in your organisation
- SOPs to monitor and manage risks
- Staff training

Determining the Level of Human Involvement in AI-augmented Decision-making

- Appropriate degree of human involvement
- Minimise the risk of harm to individuals

Operations Management

- Minimise bias in data and model
- Risk-based approach to measures such as explainability, robustness and regular tuning

Stakeholder Interaction and Communication

- Make AI policies known to users
- Allow users to provide feedback, if possible
- Make communications easy to understand

Source: *Model AI Governance Framework 2.0*, Singapore Personal Data Protection Commission

a. **Human-in-the-loop** suggests that human oversight is active and involved, with the human retaining full control and the AI only providing recommendations or input. Decisions cannot be exercised without affirmative actions by the human, such as a human command to proceed with a given decision.

   For example, a doctor may use AI to identify possible diagnoses of and treatments for an unfamiliar medical condition. However, the doctor will make the final decision on the diagnosis and the corresponding treatment. This model requires AI to provide enough information for the human to make an informed decision (e.g. factors that are used in the decision, their value and weighting, correlations).

b. **Human-out-of-the-loop** suggests that there is no human oversight over the execution of decisions. The AI system has full control without the option of human override.

   For example, a product recommendation solution may automatically suggest products and services to individuals based on pre-determined demographic and behavioural profiles. AI can also dynamically create new profiles, then make product and service suggestions rather than relying on predetermined categories.

   A machine learning model might also be used by an airline to forecast demand or likely disruptions, and the outputs of this model are used by a solver module to optimise the airline's scheduling, without a human in the loop.

c. **Human-over-the-loop** (or human-on-the-loop) suggests that human oversight is involved to the extent that the human is in a monitoring or supervisory role, with the ability to take over control when the AI model encounters unexpected or undesirable events (such as model failure). This approach allows humans to adjust parameters during the operation of the algorithm. For example, a GPS navigation system plans the route from Point A to Point B, offering several possible routes for the driver to pick. The driver can alter parameters (e.g. due to unforeseen road congestions) during the trip without having to re-programme the route.

Government of Canada's Directive on Automated Decision-Making

- Effective April 1, 2019 – compliance by April 1, 2020

Our guiding principles

To ensure the effective and ethical use of AI the government will:

1. **understand and measure** the impact of using AI by developing and sharing tools and approaches
2. **be transparent** about how and when we are using AI, starting with a clear user need and public benefit
3. **provide meaningful explanations** about AI decision making, while also offering opportunities to review results and challenge these decisions
4. **be as open as we can** by sharing source code, training data, and other relevant information, all while protecting personal information, system integration, and national security and defence
5. **provide sufficient training** so that government employees developing and using AI solutions have the responsible design, function, and implementation skills needed to make AI-based public services better

Emerging Issues & Reactions (cont'd)

- Technological advancements vs. privacy rights
  - Singapore: Enhanced accountability measures and enforcement powers being introduced, balanced against data portability and innovation measures
  - Costa Rica: Most companies largely depend on Big Data to carry out their business and privacy laws are not being able to catch up with this new demand
  - Canada: Transparency, strict parameters, policies, checks and balances should be in place for facial recognition tools to prevent their abuse. Privacy commissioners investigating police's use of facial recognition technology in child exploitation investigations.
- Public interest disclosure vs. proprietary algorithms
  - Singapore: MGF promotes transparency
  - Costa Rica: There are no initiatives on this specific matter in Costa Rica.
  - Canada: Expert panel report on legislative review of the Broadcasting Act recommends that all media content undertakings (including foreign online streaming services such as Apple and Netflix) should have to report to the Canadian broadcasting regulator (CRTC) on algorithms, AI-based processes and consumption data used to make content recommendations and customize offerings.

New Portability & Innovation Obligations?

- New "**Data Portability Obligation**" that imposes on organizations, at the request of the individual, the obligation to transmit to another organization the individual's data in its control or possession in a commonly used machine-readable format.
- New "**Data Innovation Provisions**":
  - **Derived Data**: Derived personal data (i.e. derived data which constitutes personal data within the meaning of the PDPA) will not be subject to
    - access and correction obligations; and
    - proposed Data Portability Obligation.
  - **Business Innovation purposes**: Organizations may use personal data for "business innovation purposes" without notifying individuals of and seeking consent to use their data for these purposes. Such purposes will cover:
    - operational efficiency and service improvements;
    - product and service development; or
    - knowing customers better, but not extend to the use of data for sending direct marketing messages to customers.
  - However, for the collection or disclosure of personal data, whether for business innovation purposes or other purposes, organizations must still notify and seek consent, unless there is an applicable exception to consent.

Legal & Ethical Issues

As AI & big data applications impacting life and liberty become more pervasive, what are the legal and ethical issues that need to be addressed?

- Should governments dictate ethical standards in AI/data analytics (AIDA)?
  - What principles should apply?
  - Parallels with medico-ethical regimes?
- Universality of norms vs arms-race for technical superiority?
- Enforceability vs black-boxing?

AI/Data Governance Frameworks

- Examples of some Asilomar ethical AI principles:
  - **Liberty and Privacy:** The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.
  - **Shared Benefit:** AI technologies should benefit and empower as many people as possible.
  - **Shared Prosperity:** The economic prosperity created by AI should be shared broadly, to benefit all of humanity.
  - **Human Control:** Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.
  - **Non-subversion:** The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.
  - **AI Arms Race:** An arms race in lethal autonomous weapons should be avoided.

Human-centered AI

"To foster public trust and confidence in AI technologies and fully realize their potential, we are committed to a human-centered approach to AI, guided by the G20 AI Principles drawn from the OECD Recommendation on AI", including the following principles:

- inclusive growth, sustainable development and well-being
- human-centered values and fairness
- transparency and explainability
- robustness, security and safety
- accountability

G20 Ministerial Statement on Trade and Digital Economy, June 2019

Other Ethics Frameworks

- Institute of Electrical and Electronics Engineers ("IEEE") Standards Association's *Ethically Aligned Design*
- European Commission's Communication – *Building Trust in Human-Centric Artificial Intelligence*
- OECD's Recommendation of the Council on Artificial Intelligence

Panelists

Chung Nian Lam

WongPartnership LLP, Singapore

chungnian.lam@wongpartnership.com

Monique McAlister

Goodmans LLP, Toronto, Canada

mmcalister@goodmans.ca

Vivian Gazel

Arias, San Jose, Costa Rica

Vivian.Gazel@ariaslaw.com

Questions?