Data Protection in the Time of the Pandemic

Roundtable Series Report

Between September and December 2020, the Centre for Information Policy Leadership (CIPL)[1] and the Centre for Civil Society and Governance (CCSG)[2] at the University of Hong Kong hosted a series of three roundtables entitled "Data Protection in the Time of the Pandemic". This series was sponsored by Facebook and aimed to create a forum for key stakeholders, including data privacy regulators, industry leaders, academics and members of civil society, to exchange views and share perspectives on important privacy issues facing industry and governments as they responded to the pandemic and its impact on work, society, health and innovation. In particular, the roundtables examined how COVID-19 has had an impact on organizational initiatives to use data for good, share data responsibly and ethically deploy AI solutions.

This Roundtable Series Report provides a summary of key takeaways from each of the roundtables and highlights the latest thinking on these topics as COVID-19 continues to drive digital transformation and organizations continue to leverage data to fight the pandemic, think about other pressing humanitarian issues and find responsible data solutions to today's unprecedented data challenges.[3]

Key Takeaways from the Roundtable

Using Data for Social Good

1. **To facilitate speed to market when it comes to using data for social impact, we need pre-approved methodologies and ready-made solutions to enable quick response rates** (e.g. regulatory guidance, template agreements, appropriate governance

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 80 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see informationpolicycentre.com.

[2] Established in December 2002, the Centre for Civil Society and Governance is the first research centre in Hong Kong dedicated to enhancing knowledge of civil society - its nature, constituents, dynamics, roles (in particular its contribution toward governance) - and to contributing to the attainment of a sustainable society through forging community-based, innovative solutions to inform policy deliberation and collective action. For more information, please see https://ccsg.hku.hk/.

[3] Please note that this report generally does not attribute specific statements to specific individuals or organizations. In the few instances that it does, the organization that made the statement is specifically noted.

mechanisms, common terminology and shared and trusted platforms that link different forms of data).

2. **Using data for social good requires data protection authorities to re-examine and re-interpret certain data protection obligations and engage with organizations in respect of their new data philanthropy processes** (e.g. through consultations, regulatory sandboxes, roundtables and conference discussions).

3. Sharing data across borders from one market can aid social impact initiatives in other markets and **data protection should not act as a barrier to the responsible cross-border sharing of data** for such beneficial initiatives.

4. **There are already a panoply of governance processes and techniques that can be used to protect privacy when using data for good** (e.g. differential privacy, anonymization, pseudonymization, company guidelines and codes of conduct, external guidelines and codes of practice, advisory boards, risk assessments and other guardrails, data management techniques, increased transparency and clear retention periods).

5. **It is imperative that we make initiatives that use data for social good as trustworthy and transparent as possible** (e.g. communicate if personal or only non-personal data are being used for the initiative; shine a light on pre-data sharing processes and controls, and legal processes that organizations must follow before sharing data; communicate how the organization is thinking about the privacy aspects involved in the initiative; work with researchers and civil society who can then provide insights to government rather than providing data directly to government bodies).

Sharing Data Responsibly

1. **There are a multitude of benefits to data sharing** (e.g. provides greater access to data, supports innovation and improvement of service and facilitates data for social good) **but there are also key challenges** (e.g. establishing trust between data sharing partners, ensuring legal compliance, data sharing negotiation hurdles and operationalizing data sharing agreements).

2. **There are an increasing number of data sharing frameworks and structures which can aid organizations in efforts to responsibly share data with industry members, governments and civil society** (e.g. IMDA Trusted Data Sharing Framework, Japan's Trusted Personal Data Management Service, proposed-EU wide "data spaces") **as well as legislation facilitating data sharing** (e.g. Finland's Act on the Secondary Use of Health and Social Data").

3. **To fully enable effective and responsible data sharing, we need a global system or framework for cross-border data transfers. In addition, there is a need to address**

the issue of data localization and concerns surrounding unlimited government access to data.

4. **Open data can be useful to increase access to data but it is important to consider privacy risks that stem from open datasets**.

5. **There is a lot of promise for data portability in empowering consumers to share their data,** including through initiatives like The Data Transfer Project and frameworks like India's Data Empowerment and Protection Architecture (DEPA), **but many logistical, operational and compliance questions remain**.

Responsible and Ethical Deployment of AI

1. **Regulators are developing frameworks, guidance documents and toolkits that are assisting organizations to develop, train and deploy their AI applications in responsible and ethical ways** (e.g. Singapore PDPC's Model AI Governance Framework, the UK ICO's guidance on data protection and AI and the ICO's AI and Data Protection Risk Mitigation and Management Toolkit).

2. **While AI might increase productivity and provide many benefits to society, we need to consider ethical issues such as the protection of workers and those with less bargaining power, as well as issues around bias and discrimination and other forms of social injustice.**

3. **It is important to recognize that AI itself can be used to build trust** (e.g. AI can be deployed to identify and combat fraud at scale).

4. **There are several accountable AI practices that organizations can employ to address ethical issues associated with AI** (e.g. ensure appropriate leadership and embed a culture of ethical and responsible development of AI throughout the DNA of the organization; consider the impact of the AI on individuals and society; consider the impact on society of not using data; utilize different forms of impact assessments, including automated decision impact assessments and ethics/human rights impact assessments; utilize data trusts).

5. **Policy prototyping programs can provide evidence-based policy input to policymakers either to improve existing governance frameworks or inform new ones as we seek to ensure appropriate approaches to achieving ethical AI.**

I. Roundtable 1 – Using Data for Good: Unleashing the Power of Data during the Pandemic and Beyond

On 10 September 2020, CIPL and CCSG hosted its first joint roundtable on "Using Data for Good: Unleashing the Power of Data during the Pandemic and Beyond". This virtual roundtable gathered stakeholders to discuss how we can unleash the power of data both in the context of addressing the immediate crisis posed by the pandemic and in the future to responsibly tackle real world issues in line with data protection policy and legal requirements.

Representatives from the Singapore Personal Data Protection Commission (PDPC), the University of Hong Kong, National Tsing Hua University, Facebook, Mastercard and GSMA participated in the roundtable, which comprised several keynotes followed by a panel discussion.

COVID-19 has highlighted the importance of using data for social good. During the roundtable, organizations reported that one resounding change compared to pre-COVID times is that there is now enormous interest from governments and policymakers for access to data to serve public interest objectives. In the early stages of the pandemic, there was a surge of requests for data to understand population mobility to coordinate an appropriate public health response. Public health officials wanted to be able to answer questions such as whether people were adhering to social distancing and lockdown orders, and at what rates?

This led to many organizations sharing datasets from their company externally where such data can be used for social impact purposes. Such sharing aims to empower the work of data partners, including academics, researchers, civil society organizations, government bodies and policymakers, and to make data more publicly available. However, organizations had to address a multitude of privacy concerns and act with agility to ensure they could responsibly use and share data for social good for the welfare of humanity.

The sections below outline the key issues, solutions and takeaways from this roundtable:

A. <u>Response rate and speed to market</u>

- In times of crisis, companies can find themselves at a privacy crossroads – they can either control access to a dataset and make sure it only goes out to a small number of researchers, or they can invest heavily and push themselves on the transparency and privacy side to scale rapidly and make datasets publicly available.

- COVID-19 has identified a need for faster approvals of research partners. From an accountability perspective, many organizations put their research partners through heavy privacy and security scans and vetting processes to understand who is going to have access to the shared data, how results and data will be published, what the legal contractual processes are, etc. Normally, this can take several months, but during the pandemic that had to be accelerated without compromising on due diligence checks. This

is where pre-approved methodologies and guidance for sharing data for social good would be very useful.

- A single data for social good initiative can involve many different parties and an organization will have to have agreements in place with all relevant actors to enable the initiative to move forward. Building an approved methodology or crafting other ready-made solutions will enable such relationships to be established and approved more expediently when time is of the essence.

- Sharing data speedily from one market can aid social impact initiatives in other markets. During the early stages of the pandemic, US and EU governments and organizations were particularly interested in the health and economic impacts of the pandemic in Asia to inform local response and measures once COVID-19 reached their shores.

- Datasets for research need to be built for purpose and during COVID-19, there were many different requests coming from civil society, researchers and the public sector for different types of datasets that were not sufficiently specific. For example, "mobility data" can be interpreted in many different ways. Broad requests for location or mobility data or other vague requests slows down the conversation. It is important to improve governance mechanisms and relationships so that organizations can have these conversations quickly and arrive at requests that are more definitive which will enable them to respond definitively as well.

B. <u>Modernized guidance and interpretation of traditional privacy principles</u>

- COVID-19 has pushed policymakers to dig deep into various policy toolkits to revitalize the economy. It has also pushed business owners to think outside the box to identify new ways to ensure commercial relevance and viability. Similarly, the pandemic is pushing data protection authorities (DPAs) to re-examine and, sometimes even re-interpret, existing data protection obligations to support economic recovery and data uses that benefit society.

- DPAs have been and should continue to go beyond principles and concepts that have been discussed at a high level in decades past. This includes engaging with specific business processes and the technology itself, either through consultations, regulatory sandboxes, roundtable and conference discussions and in the context of resolving complaints. This enables DPAs to provide administrative, hands on and step-by-step guides that operationalize and translate data privacy requirements and concepts into actionable tasks for organizations.

C. <u>Cross-border data flows</u>

- As organizations assist in the fight against the present and future crises, it may be necessary for them to share data for good to overseas entities. Moreover, as they recover from the pandemic, they will naturally seek new opportunities and some of these,

including for SMEs, will be in overseas markets. Data protection should not act as a barrier to sharing data abroad and regulators have a responsibility to enable, facilitate and support responsible cross-border sharing of data.

D. Governance processes and techniques to protect privacy when using data for good

- ***Differential Privacy*** – When using data for social impact, organizations can apply a differential privacy framework to preserve user privacy. This involves adding a certain amount of random noise to datasets and being explicit about the re-identification risk for each individual within the dataset. It also involves excluding data points from a dataset where the risk for re-identification exceeds certain thresholds.[4]

- ***Anonymization*** – Organizations often anonymize data that is subsequently used for social impact initiatives as this minimizes the risk of processing and enables greater possibilities to share data.

- ***Pseudonymization*** – Pseudonymization is a useful technique when using data for social impact that enables de-identification and aggregation of data so that important and interesting patterns can be discerned for research and societal advancement.

- ***Company Guidelines and Codes of Conduct*** – Organizations can create internal privacy guidelines for staff to follow with respect to using and sharing data for social impact. They may also create or re-emphasize company codes of conduct on data sharing or good data handling practices.

- ***External Guidelines and Codes of Practice*** – External industry and regulatory guidelines and codes may also assist efforts to use and share data for social impact. For example, during COVID-19 app developers consulted the UK Information Commissioner's Office (ICO) guidance document that set out its expectations on how contact tracing solutions may be developed in line with the principles of data protection by design and default.[5] In addition, the ICO recently released a new Data Sharing Code of Practice[6] as COVID-19 brought the need for fair, transparent and secure data sharing into sharper focus.

- ***Advisory Boards*** – Internal and external advisory and review boards can provide an additional layer of oversight before embarking on data for social impact initiatives.

---

[4] Facebook made use of differential privacy with respect to using mobility data to assist the response to COVID-19. See "Protecting privacy in Facebook mobility data during the COVID-19 response", available at https://research.fb.com/blog/2020/06/protecting-privacy-in-facebook-mobility-data-during-the-covid-19-response/.

[5] COVID-19 Contact tracing: data protection expectations on app development, UK ICO, May 2020, available at https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf.

[6] Data Sharing: A Code of Practice, UK ICO, December 2020, available at https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/.

- ***Risk assessments and other guardrails*** – Using personal data for social good can be challenging and organizations can minimize the risks through risk assessments and other appropriate guardrails. Some organizations report that oftentimes researchers will say that if they had access to the raw data, they would be able to do so much more with it for social good. However, privacy rules and company dedication to privacy protection prevents such sharing. As such, the development of a universally accepted methodology would enable organizations to responsibly address these limitations and ensure greater data use while still ensuring high levels of privacy protection.

- ***Data Management*** – Accuracy, completeness and consistency of data play an important part in using and sharing data for social good, apart from basic responsibilities related to privacy, security and data protection. If an organization does not understand how accurate its information is, that plays a huge role in the data outcomes of using that data for research and the subsequent impact it has on individuals.

- ***Transparency*** – Industry has been overly reliant on consent and it is important to understand that the average consumer may not be able to comprehend data for social good uses that are buried in consent forms. We need to split transparency from consent and need mechanisms that explain these data uses as they are happening or as part of the context of a data use.[7] Organizations may seek to use just-in-time or dynamic notice which will be much more effective for both the individual and the organization in processing data for social impact.

- ***Retention Periods*** – It is very important to make sure that data shared for social impact purposes is time bound or, alternatively, be very clear about how it will be used in future.

E. Building trust around data for social good initiatives

It is imperative that we make initiatives that use data for social good as trustworthy and transparent as possible so that people understand what is really happening and what is involved with the initiative. Below are some consideration to achieve this:

- Much of the data used for positive social impact is non-personal data – communicating instances of this upfront, where possible, will go a long way in reassuring skeptics and cautious users about an organization's data sharing practices.

- Most organizations go through a whole process before sharing data for good and have policies, procedures and controls in place to ensure that data does not end up in the wrong hands. In other words, organizations do not hook up a hose to the data they control and give it out freely. Moreover, in addition to accountable governance processes, there are also legal processes in each jurisdiction that organizations must follow before transferring and sharing data. Shining a light on these processes and better

[7] See, for example, Privacy Matters: Data for Good, available at https://about.fb.com/news/2020/06/privacy-matters-data-for-good/.

communicating about them will improve user, customer and government trust levels around social impact initiatives.

- On the opposite end of the spectrum, one hurdle that arose when COVID-19 started to claim lives was a public perception that we cannot let privacy stand in the way of preventing the spread of the disease and more deaths. It is equally important to communicate that thinking about the privacy aspects of using data for social good is a way to enable those uses to happen and we can achieve both – privacy protection and appropriate and responsible use of data for societal benefit. There is a moral imperative to use data you hold to help society but also the moral imperative to protect privacy.[8]

- It is important that we enable sharing of data with governments and state bodies for research as well as other public interest reasons but we need to make sure this does not creep into state surveillance, which has been a legitimate concern among the general public.

- One way that companies can ensure appropriate protection against government access to data when sharing data for social good is to work with researchers and civil society organizations that governments already have relationships with. By empowering those groups with new datasets and capabilities, the government doesn't need to produce a new legal mechanism by which to even accept data from a company. You simply empower the channel or local actors (e.g. civil society, academia, etc.) that the government already turns to.

F. Wish list for the future

- Pre-approved and developed methodologies, guidance and other ready-made solutions for using and sharing data for social good.

- Shared and trusted platforms that link different forms of data.

- Skills and capacity building in governments (e.g. many government bodies requesting data for social good do not have data science expertise in their teams).

- Data and digital education for individual data subjects and society to enable a more sophisticated understanding about what is happening in our modern digital ecosystem.

- Capacity, skills and talent in big data and analytics to make use of all the available, open and shared data.

[8] See "Aggregated mobility data could help fight COVID-19", an op-ed from leading epidemiologists at the start of the pandemic exemplifying this (April 2020), available at https://science.sciencemag.org/content/368/6487/145.2/tab-article-info.

- International and collaborative platforms to unleash the power of data to benefit the global community.

II. Roundtable 2 – Sharing Data Responsibly: Lessons from the Pandemic for the Future

On 29 October 2020, CIPL and CCSG hosted the second joint roundtable in this series on "Sharing Data Responsibly: Lessons from the Pandemic for the Future". This virtual roundtable gathered stakeholders to discuss the role of data sharing in the post-COVID world and how we can strike an appropriate balance between data protection concerns and the need to share data for the benefit of society, the economy and the data ecosystem as a whole. The discussion also focused on whether the pandemic has impacted data sharing by consumers and concerns around government use of data that is transferred for purposes of fighting COVID-19, as well as the role of data portability in addressing such concerns.

Representatives from the Singapore Infocomm Media Development Authority, the Personal Information Protection Commission of Japan, Facebook, Naspers Group, Trilegal, Sitra and the Internet Society of Hong Kong participated in the roundtable.

Data sharing means initiatives that require positive data sharing between and among businesses and governments, and empowering individuals to share and move their data, including through data portability rights. Post-COVID, the appetite and need for data sharing is going to increase. The big question is how do we share data in ways that protect privacy rights and individual autonomy while also enabling us to leverage and use data.

The sections below outline the key issues, solutions and takeaways from this roundtable:

A. Benefits of Data Sharing

- Increases data flow by providing greater access to data.
- Supports innovation and the improvement and delivery of products and services, including AI solutions.
- Facilitates data for good initiatives and data use in the public interest.

B. Challenges for Data Sharing

- Establishing trust between partners (i.e. concerns around how the data will be used, whether the data partner knows how to handle the data, the potential for breaches to occur, etc.)
- Ensuring legal compliance (questions around whether legally an organization can share and exchange personal information, cross-border data sharing issues, etc.)
- Negotiation hurdles (e.g. valuing data to be shared, completing legal agreements, etc.)

- Operationalizing data sharing agreements (e.g. use of intermediaries, format of data, standards to adhere to, etc.)

C. Frameworks for Data Sharing

- The Infocomm Media Development Authority (IMDA) of Singapore has developed a Trusted Data Sharing Framework[9] which is designed to help users understand key considerations to enable data sharing. It also provides assurance for individuals that data is handled responsibly and gives them greater confidence in service providers. It is Asia's first comprehensive framework for trusted data sharing.
    - The framework includes business, legal and technical considerations and tools. It comprises four components:
        - (1) Data sharing strategy;
        - (2) legal and regulatory considerations;
        - (3) technical and organization considerations;
        - (4) operationalizing the data strategy.
    - The framework also puts forward three data valuation approaches – a market approach, cost approach and income approach.
- In addition to regulatory frameworks, some countries are implementing legislation to facilitate data sharing (e.g. Finland's Act on the Secondary Use of Health and Social Data[10]).
- Moreover, there are initiatives to create EU wide "data spaces" in Europe which aim to make better use of publicly held data for research for the common good, support voluntary data sharing by individuals and set up structures to enable organizations to share data.[11]

[9] Trusted Data Sharing Framework, Infocomm Media Development Authority, June 2019, available at https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf.
[10] Act on the Secondary Use of Health and Social Data, available at https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf.
[11] See Data sharing in the EU – common European data spaces, available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Legislative-framework-for-the-governance-of-common-European-data-spaces.

- In Japan, the Trusted Personal Data Management Service (TPDMS)[12] is a service to utilize systems, including a Personal Data Store, and manage personal data based on entrustment agreements on data utilization with individuals. Such personal data is provided on behalf of the individuals to third parties in accordance with the instructions of the individuals or pre-specified conditions. TPDMS is a voluntary mechanism to certify business operators meeting a certain standard. Certification serves the purposes of enabling individuals to choose a reliable/trusted service with whom to engage in a data entrustment agreement.

D. Global Data Sharing

- We need a global system or framework for data sharing. Japan is in a unique position to share data given it has secured a reciprocal adequacy decision with the EU and is a participant in the APEC CBPR system which enables flows from Japan to the US and elsewhere. We need to bridge these systems to ensure data can flow around the globe. This might be achieved through a new or globalized cross-border privacy rules certification scheme (which current APEC CBPR participants are exploring).

- We also need to address issues around data localization and unlimited government access to data concerns, which have presented stumbling blocks for global data sharing. One forum for doing so could be the OECD.

E. The Promise of Open Data

- Open data responds to public demands for data. However, open data initiatives can often contain high levels of personal data (i.e. raw data without aggregation).

- In the early stages of the pandemic, people wanted information quickly. They wanted to know if their neighborhood had been hit by COVID-19 and how contagious the disease was. Asian governments were able to swiftly answer these data demands from individuals. One of the reasons for this is because Asian economies have been climbing open data ranking lists in the last few years (e.g. The Open Data Barometer[13] and the Global Open Data Index[14]).

- When authorities released data, civil society was able to put together tools to keep the public informed at record pace.

- Civil society advocates for transparency from government so it can have access to open data but it is equally important to consider privacy risks that stem from open datasets.

[12] See Trusted Personal Data Management Service, available at https://www.tpdms.jp/file/20190927-1presentation.pdf.
[13] The Open Data Barometer, available at https://opendatabarometer.org/?_year=2017&indicator=ODB.
[14] The Global Data Open Index, available at https://index.okfn.org/.

F. Data Portability

- Though there are different interpretations as to the meaning of data portability, one interpretation is that portability means the ability to take the personal data an individual shares with one service and move that data directly to another service.

- Portability is a legal right in a number of jurisdiction (e.g. under the GDPR, CCPA, and LGPD) and is finding its way into the privacy or consumer protection regimes of other jurisdictions (e.g. Singapore, India, South Korea, Australia, and Israel).

- Portability provides individuals with control over their information and facilitates informational self-determination. It also enhances competition through improving choice among services. Portability can also support public interest and research initiatives.

- The Data Transfer Project[15] is an open source initiative among Facebook, Google, Twitter, Microsoft and Apple that seeks to facilitate portability in a manner consistent with regimes like the GDPR and CCPA. It does this by taking advantage of existing public infrastructures to enable transfers.

- India has created the Data Empowerment and Protection Architecture (DEPA)[16]. This framework creates a consent manager to decouple consent from data flows. DEPA was first used by financial intermediaries who signed up to the consent manager. Through DEPA, individuals seeking a loan can share data through requests by banks for information (e.g. transaction history). This enables just in time consent for important financial decisions. One billion Indians are currently not participating in India's financial system. DEPA provides a way for them to enter the system.

- Although there is a lot of promise for portability, there are many questions that organizations are seeking guidance on, including:

    - What do we really mean by portability?

    - When a user directs someone to transfer data, is that considered portability (e.g. if a consumer consents to data sharing with app developers) or is portability a right that must be invoked for the direct benefit of the user?

    - What is the scope of data included?

    - What is data provided by a user – uploaded content only or also observed and inferred data?

[15] See Data Transfer Project, available at https://datatransferproject.dev/.
[16] See Data Empowerment and Protection Architecture: A Secure Consent-Based Data Sharing Framework to Accelerate Financial Inclusion, available at https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf.

- In addition to logistical and operational questions, there are also questions around data protection, including:
    - How do you ensure the privacy rights of individuals who are porting data are protected?
    - How do you tell individuals about portability and give them information about their rights and the controllers they may choose to port data to?
    - Who is responsible for actions of third parties that receive the data? Is it the transferring company or the third party that collects data via the portability regime? In other words, which controller is responsible for protecting the data before, during and after it is ported?
    - If data is misused once ported, how can individuals vindicate their rights?
    - Are self-regulation and/or sector-specific rules key to balancing the data protection risks of porting data to third parties and the innovation and competition benefits?

III. Roundtable 3 – AI and AI Ethics in the Context of COVID-19 and Beyond

On 15 December 2020, CIPL and CCSG hosted the final joint roundtable in this series on "AI and AI Ethics in the Context of COVID-19 and Beyond". This virtual roundtable gathered stakeholders to discuss the instrumental role that AI is playing in responding to COVID-19 and how its development as a tool for social impact will accelerate as a result of the pandemic. The roundtable also focused on important ethical questions that stakeholders have faced in deploying AI solutions and the steps they have taken to appropriately address these concerns while ensuring society reaps the full potential of AI.

Representatives from the Singapore PDPC, the UK ICO, Seoul National University School of Law, The University of Hong Kong, Facebook, Crypto, Telefonica and Mastercard, and a former legislative councilor from the Legislative Council of Hong Kong participated in the roundtable.

COVID-19 has accelerated digital transformation and AI has been seen as a major tool and technology that has enabled us to process huge amounts of data to help us fight the pandemic and facilitate some return to work and a safe environment and community for individuals. AI is a technology that promises a lot, but there are also challenges. The question is not how do we balance the benefits and challenges, but rather how can we ensure as much deployment of AI as possible in a responsible and trustworthy way to improve our lives.

The realization that AI is a useful technology is here to stay and virtually every company is investing in AI. Every government is ensuring that AI innovation is part of their industry policy and economic growth and recovery plans post-COVID so it will be imperative to deliver accountable AI in the coming years ahead.

The sections below outline the key issues, solutions and takeaways from this roundtable:

A. Developing Accountable AI Frameworks

- Over the past two years, regulators and leading organizations have been thinking deeply about how to create accountable and ethical frameworks around AI and how to address difficult issues ranging from bias and non-discrimination to redress and ensuring a human-in-the-loop where appropriate, etc.

- The Singapore PDPC has been working on an AI governance framework since 2019 and through conversations and partnerships with industry, it released the second edition of the framework in January 2020.[17] This framework crystallizes the PDPC's thoughts on how to apply an accountability approach to the design, application and use of AI.

- In releasing this framework, the PDPC acknowledged that for the framework to be useful, it needed to go beyond concepts and provide concrete guidance and so it developed an implementation and self-assessment guide for organizations[18] that takes the concepts outlined in the framework and breaks them down into relevant questions, guidance and controls.

- In addition to the framework and self-assessment guide, the PDPC also released two compendiums of use cases.[19] The two compendiums illustrate the entire framework through 30 examples.

- Most recently, in collaboration with the Lee Kuan Yew Centre for Innovative Cities, Singapore University of Technology and Design and the Infocomm Media Development Authority, the PDPC released Singapore's Guide to Job Redesign in the Age of AI.[20] This is a companion to the AI governance framework and sets out a human centric approach to the implementation of AI from an employer/employee perspective.

- Moving forward, the PDPC will continue an open approach to working with industry to fine tune and release revisions of these instruments and explore other practical tools as well as a voluntary certification-based framework for good data governance and AI ethics.

---

[17] Model Artificial Intelligence Governance Framework, Singapore PDPC, 2nd Edition, January 2020, available at http://go.gov.sg/ai-gov-mf-2.

[18] Companion to the Model AI Governance Framework, Implementation and Self-Assessment Guide for Organizations, Singapore IMDA and PDPC in collaboration with the World Economic Forum Centre for the Fourth Industrial Revolution available at https://go.gov.sg/isago.

[19] Compendium of Use Cases: Practical Illustrations of the Model AI Governance Framework, Singapore PDPC, available at https://go.gov.sg/ai-gov-use-cases; Volume 2 Compendium of Use Cases: Practical Illustrations of the Model AI Governance Framework, Singapore PDPC, available at https://go.gov.sg/ai-gov-use-cases-2.

[20] A Guide to Job Redesign in the Age of AI, available at https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework.

- Similarly, the UK ICO, in collaboration with the Alan Turing institute has published a guide on Explaining Decisions with AI.[21] The ICO also published a guide on Data Protection and AI,[22] which acts as the foundation for the ICO's thinking around AI. The ICO has seen organizations begin to apply this guidance and it is also testing it through its regulatory sandbox initiative.

    - The ICO created this guidance to (1) develop a methodology for the ICO's auditing and investigation teams to audit and assess the deployed use of AI systems in organizations and (2) share its thinking externally and consult on the development of the guide in order to publish something that all organizations can read, make sense of and implement.

    - The guide on Data Protection and AI covers 4 key chapters – (1) governance and accountability; (2) lawfulness, fairness and transparency; (3) security and data minimization; and (4) the broader impact on rights.

- In 2021, the ICO released the alpha version of an AI risk toolkit[23] which is intended to assist practitioners identify and mitigate risks to data protection that AI systems which process personal information create or exacerbate. The toolkit is open for public consultation.

B. Regulating AI

- There has been much debate around AI regulation with some countries currently exploring legislative options.[24] CIPL has promoted a layered approach to AI which encompasses (i) principle based rules and standards, (ii) accountability of organizations and (iii) regulators that are innovative and ready to interpret requirements in light of new AI applications and to create safe spaces to test new AI applications through regulatory sandboxes and policy prototyping initiatives.

- According to the ICO, ethics is the gap between the laws we have and the laws we need. We have a choice when dealing with that gap – we can wait for legislators and parliamentarians to develop the laws and respond to that or industry can proactively work on the gaps.

---

[21] Explaining Decisions Made with AI, UK ICO and the Alan Turing Institute, May 2020, available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/.

[22] Guidance on AI and Data Protection, UK ICO, July 2020, available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/.

[23] UK Information Commissioner's Office, AI and Data Protection Risk Mitigation and Management Toolkit (alpha version), released 15 March 2021 for public consultation, available at https://ico.org.uk/media/about-the-ico/consultations/2619422/ai-and-data-protection-risk-mitigation-and-management-toolkit.xlsx.

[24] For example, in April 2021, the European Commission released its proposal for a Regulation on a European approach for Artificial Intelligence, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75788.

- Moreover, the ICO notes that existing laws have the flexibility to deal with many issues that AI presents (e.g. in the early stages of the pandemic the ICO produced design guidelines for developers working on contact tracing apps so that they could interpret the requirements of the GDPR and innovate within that framework). However, that is not to say that there aren't new and emerging issues that we should be thinking about collectively and how we want to deal with them.

- The Singapore PDPC notes that apart from changing the law, we need to put in place measures that support innovation. This is where we go beyond just data protection law itself and look at where regulators can provide clarity and certainty on specific issues. In this regard, regulatory sandboxes and policy prototyping create a win-win situation. Through these initiatives, regulators can learn as much from industry as industry benefits from the conversation with the regulator, and together they can craft a clearer path ahead, especially in fast evolving areas.

- Many organizations using the AI and ethics frameworks mentioned in the previous section are already at a relatively mature stage when it comes to privacy and data but many SMEs innovating in this space don't even have the basics in place. Standards can help with this (e.g. ISO 27701 or the NIST Privacy Framework) but these don't account for important ethics questions. This is where policy prototyping can be invaluable and where startups can embed privacy requirements into their innovations as they go along rather than tagging them on after the fact.

- It is important to recognize that AI does not just impact the data privacy space but is a horizontal technology that crops up in a whole host of other regulatory areas. It is critical that we achieve consistency between different AI frameworks and guidance across the ecosystem. For example, in Singapore, there is a fair amount of consistency between the PDPC's AI governance framework and the Monetary Authority of Singapore's Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence.[25] In addition, the Securities and Exchange Board of India has implemented reporting obligations for AI and Machine Learning applications and systems that are offered and used by market intermediaries.[26]

- Following the 2008 financial crisis, there was much discussion around ethics in the banking space. Organizations are able to look at some of these principles and translate them into the AI space.

[25] Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, Monetary Authority of Singapore, November 2018 (updated February 2019), available at https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/FEAT-Principles-Updated-7-Feb-19.pdf.

[26] Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Mutual Funds, May 2019, available at https://www.sebi.gov.in/legal/circulars/may-2019/reporting-for-artificial-intelligence-ai-and-machine-learning-ml-applications-and-systems-offered-and-used-by-mutual-funds_42932.html.

- Given that AI is a horizontal technology, stakeholders must question whether any form of regulation is better placed on a sectoral level.

C. Trust and Equality with AI

- Adoption of AI depends not only on the technology itself but also on broader, social and cultural contexts and it is important for the public to be able to trust and benefit from the technology.

- In the context of the pandemic, public trust affected the uptake of contact tracing apps. Some estimate you need around 80% of mobile users to install contact tracing apps to be effective, but lingering concerns about government surveillance and leakage of information might have hindered adoption in many countries. There have also been heated debates about technology protocols for contact tracing – i.e. whether such apps should be centralized or de-centralized and privacy is central to this debate.

- The pandemic resulted in moving more services to digital infrastructure and AI is really going to reinforce this trend. It is worrying as to whether this is going to make social and economic inequality even worse. For example, AI might increase productivity and make the supply chain more efficient but, at the same time, we need to ensure protection of workers and those with less bargaining power. Moreover, with the increasing use of algorithms in decision-making and the provision of services, the pressing issue is about avoiding biases in AI. We must ensure that we don't use AI to reinforce social injustices.

- Even if an AI developer has the best of intentions and makes an AI application transparent and explainable, and provides adequate oversight, the data used to train AI itself may be biased. One way to mitigate this problem may be to use curated data but oftentimes this is difficult to implement because datasets are simply too large.

- It is important to support and develop a strong and vibrant civil society to monitor the evolution of AI and ensure fairness and accountability.

- It is also important to recognize that AI itself can be used to build trust. For example, the pandemic has resulted in many increased instances of fraud and abuse by bad actors ranging from phishing scams, credentials harvesting and fund diversion to malware infections, hijacking of teleconference calls and ransomware attacks. AI can be deployed to identify and combat fraud at scale.

- In addition, the inclusion of a human in the loop may actually undermine trust in some AI applications. This may be the case, for example, in the context of using AI for recruitment purposes. If a human enters the selection process of candidates at some stages but leaves decisions solely to AI in others, that may undermine trust in the use of AI for the recruitment process as a whole.

D. Accountable AI Practices

- ***Ensure appropriate leadership*** – Implementing an AI framework and adopting good practices around organizational processes will amount to nothing if the organization does not engender a culture where AI accountability and the responsible development of AI is in the DNA of every single individual from leadership down to practitioners.

- ***Consider the impact on individuals and society*** – The ICO notes that when considering risk or an ethical issue and trying to judge the impact of AI on that issue, organizations should ask themselves this question: "What does this mean for the individual and society when we are considering what is best for them as per the laws that they are protected under". If proceeding with the processing is the right thing to do, then there is a huge amount of collaboration that can take place. If it doesn't feel like it is the right thing to do, then there are opportunities to work with regulators to try and address those issues before they manifest for the individual.

- ***Consider the impact on society of not using the data*** – Organizations should also ask themselves if it is ethical to not use data when assessing the impact of an AI application (e.g. the reticence risk). In South Korea, COVID-19 infection rates have remained low in comparison to the rest of the world. Would it have been unethical not to use AI and data to achieve this despite there being various privacy considerations and risks involved?

- ***Utilize different forms of impact assessments*** – In the AI context, many organizations are either proposing or working on new forms of risk and impact assessments, ranging from automated decision impact assessments (ADIA) to ethics and human rights impact assessments.

- ***Utilize data trusts*** – Data trusts are an interesting application of the fiduciary duty concept. There might be many different purposes for setting up data trusts – to look after user data, improve governance, separate processing from ownership of data, promote data sharing where different companies/institutions pool their data, unlock research and commercial value, or even mitigate non-compliance risks.

E. Policy Prototyping

- Policy prototyping programs are collaborative pilot projects that mobilize a coalition of public and private actors. Facebook has been very involved in these processes and has partnered with government institutions, other industry partners, academics and civil society to deploy them. They are co-regulatory exercises with all these different stakeholders involved.

- These programs are also regulatory innovation labs that enable the development and testing of a policy idea in the field of new and emerging technologies, including AI. The policy idea can be inspired by a law that is being discussed, a self-regulation instrument, a code of conduct, a set of industry guidelines, etc.

- Policy prototyping programs are also empirical programs that provide evidence-based policy input to policymakers either to improve existing governance frameworks or to inform new ones.

- The policy prototyping process typically involves selecting a group of participants (e.g. AI companies) and asking them to apply policy prototypes (co-created normative frameworks on certain AI topics, like explainability or fairness) to specific AI applications they have built and are deploying. Based on this application, the organization conducting the policy prototyping process can collect information about the participants' experience and test and evaluate the prototypes under real world conditions. These frameworks can be improved based on the lessons learned and ultimately inform the AI regulatory debate by delivering evidence based policy recommendations.

- Facebook is currently active in the policy prototyping space in the EU, LATAM and APAC. In APAC, the program is being conducted with Singapore's IMDA and PDPC, and it consists of testing the elements of explainability and transparency of the AI Governance Model Framework and the Self-Assessment Guide.

If you would like to discuss this paper or require additional information, please contact Sam Grogan at sgrogan@huntonak.com.