KHAZANAH
RESEARCH
INSTITUTE

DISCUSSION PAPER 3/21 | 15 APRIL 2021

Open Government Data in Malaysia: Landscape, Challenges and Aspirations

Ashraf Shaharudin

Khazanah Research Institute

The **KRI Discussion Papers** are a series of research documents by the author(s) discussing and examining pressing and emerging issues. They are stand-alone products published to stimulate discussion and contribute to public discourse. In that respect, readers are encouraged to submit their comments directly to the authors.

The views and opinions expressed are those of the author and may not necessarily represent the official views of KRI. All errors remain the authors' own.

DISCUSSION PAPER 3/21 | 15 APRIL 2021

Open Government Data in Malaysia: Landscape, Challenges and Aspirations

This discussion paper was prepared by Ashraf Shaharudin from the Khazanah Research Institute (KRI). The author is grateful for the valuable comments from Kuang Keng Kuek Ser from the DataN, Khairil Yusof from the Sinar Project, Dr Lim Chee Han and Chee Yoke Ling from the Third World Network (TWN), Dr Sonny Zulhuda from the International Islamic University Malaysia (IIUM), Sri Murniati from the Institute for Democracy and Economic Affairs (IDEAS) and researchers from the KRI: Adam Manaf Mohamed Firouz, Gregory Ho Wai Son, Muhammad Nazhan Kamaruzuki, Dr Rachel Gong and Shao Loong Yin. Special thanks to the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), particularly Dr Fazidah Abu Bakar, Zuraidah Abdul Rahman and Zulkfli Ahmad for helping the author to understand better the landscape and challenges of open government data in Malaysia. Opinions and mistakes belong to the author.

Authors' email address: **Ashraf.Shaharudin@KRInstitute.org / ashrafshaharudin@gmail.com (after 6 Dec 2021)**

Information on Khazanah Research Institute publications and digital products can be found at **www.KRInstitute.org**.

DISCUSSION PAPER 3/21 | 15 APRIL 2021

Open Government Data in Malaysia: Landscape, Challenges and Aspirations

Ashraf Shaharudin

This is the third paper in the open government data series, as part of the Networked Nation project that looks into digital issues in Malaysia. The first paper, Open Government Data: Principles, Benefits and Evaluations, provides a general overview of the open government data. The second paper, Open Government Data for Academic Research, provides insights on the perception of researchers on open government data in Malaysia.

Summary

- **It is time for Malaysia to enact a Right to Information (RTI) law.** Except for the Official Secrets Act 1972 that provides broad and decentralised authority to individual government bodies to share government data and implies circumspection in data sharing, Malaysia does not have any other overarching law for government data.
- **Malaysia should consider a data privacy law that includes government data.** Protecting privacy does not work against open government data but *for* open government data. Beyond having privacy laws, government agencies need a comprehensive framework for assessing and mitigating data privacy and security risks.
- **Data management of different government agencies has to be streamlined.** Although the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) has been leading the open government data agenda, the agency has minimal power to direct and enforce the agenda.
- **The government should increase investment in digital infrastructure and human capital across all agencies.** Many government agencies indicate that they have a small ICT team. Meanwhile, MAMPU has limited capacity to reach out to and support every agency.
- **Supporting inclusive and meaningful use of open government data is as important as publishing data.** Expanding data skills training and embedding data literacy in school syllabi could help improve data skills to encourage meaningful use of open government data. In addition, the government should nurture and foster collaboration with data intermediaries among non-profits (e.g. researchers, civil society organisations etc.) to generate more public value from data.

Table of Contents

1. Introduction

During the United Nations 2020 World Data Forum in October, the global data community reaffirmed the urgency to develop "more timely, high-quality, disaggregated, [and] geospatially enabled data, that is relevant, well-documented, interoperable and open by default while respecting the right to privacy" [1]. The forum emphasised the need for information transparency that is especially crucial during this pandemic when public anxiety is heightened, and misinformation is rife. Limited information leaves room for assumptions and false rumours, fuelling further misinformation that could undermine public health responses[2].

While recognising efforts that the Malaysian government has made in communicating Covid-19 information to the public as well as the unprecedented nature of this crisis, there is admittedly still much room for improvement in government data sharing[3]. Because of the far-reaching impacts of this crisis, not only is Covid-19 data important but also socioeconomic data such as employment, education, digital access, food security and housing[4]. Complete, granular and timely data is instrumental for the government to devise strategic interventions, for researchers to contribute to giving timely policy advice, for civil society groups to channel their resources where needed, and for the public to be informed of the situation.

Based on global assessments carried out before the pandemic, Malaysia's *open government data* level is behind Indonesia, the Philippines, Singapore, and many other developing countries[5]. Open government data is a concept that encompasses the best practices for government data-sharing, appropriate for a digital age, to generate the maximum possible value from the data. In theory, open government data is defined as government data that are free from legal and technical constraints to be used by anyone at anytime from anywhere. It fulfils several criteria: completeness, granularity, timeliness, accessibility, machine-processability and non-proprietorship[6]. Government data is any information that is collected by the government either through direct responses such as census and survey or through remote observation enabled by technology such as satellite imagery and sensors[7].

With the need for government data transparency escalated by the Covid-19 crisis and building on my previous discussion paper on the principles, benefits and evaluations of open government data, this paper unpacks the existing government data ecosystem and the challenges in implementing open government data in Malaysia.

---

[1] UN (2020)
[2] WHO (2020)
[3] Ashraf (2020c)
[4] Ashraf (2020c; 2020a)
[5] Ashraf (2020b)
[6] Refer to Ashraf (2020b) for further discussion on the principles of open government data
[7] Loosely following the definition taken by World Bank (2020). It is worth clarifying that this paper uses data and information interchangeably for reasons discussed in a previous paper Ashraf (2020b).

2. Government data ecosystem in Malaysia

Data ecosystem, in this paper, refers to the governance, infrastructure, and practice of data collection, storage, sharing, disposal and use. It is necessary to understand the existing government data ecosystem in Malaysia to identify the likely barriers as well as opportunities in implementing open government data in the country.

2.1. Laws related to government information

Official Secrets Act 1972

Except for the **Official Secrets Act 1972**, Malaysia does not have any other overarching law for government data. The Act defines "official secret" as[8]

> *any document specified in the Schedule and any information and material relating thereto and* ***includes any other official document, information and material*** *as may be classified as "Top Secret", "Secret", "Confidential" or "Restricted", as the case may be, by a Minister, the Menteri Besar or Chief Minister of a State or such public officer appointed under section 2B*

The Schedule includes[9]

> *Cabinet documents, records of decisions and deliberations including those of Cabinet committees; State Executive Council documents, records of decisions and deliberations including those of State Executive Council committees; Documents concerning national security, defence and international relations.*

The Official Secrets Act provides broad and decentralised authority to individual government bodies to declare information as restricted, confidential, or secret[10]. As opposed to a Right to Information (RTI) law[11]—which Malaysia currently does not have at the federal level—that sets openness as the normative approach towards government information sharing, the Official Secrets Act implies circumspection. It is therefore logical for public servants to practice restraint in releasing government data when confronted with legal uncertainty[12], especially when there is no competing or superseding law that compels disclosure.

[8] Section 2 of the Official Secrets Act 1972 (Act 88) (incorporating all amendments up to 1 January 2006)
[9] Section 2A of the Official Secrets Act 1972 (Act 88) (incorporating all amendments up to 1 January 2006)
[10] World Bank (2017a)
[11] Also referred to by different names in different jurisdictions such as Freedom of Information (FOI) law and Public Information Disclosure law
[12] World Bank (2017a)

Statistics Act 1965

Meanwhile, the **Statistics Act 1965** deals with the role of the Department of Statistics (DOS) and the Chief Statistician. According to the Act, the functions of DOS are[13]

> *… to collect and interpret statistics for the purpose of furnishing information required in the formation or carrying out of Government policy in any field or otherwise required for Government purposes or for meeting the needs of trade, commerce, industry or agriculture (including forestry, fishing and hunting).*

and

> *… where they consider it in the public interest [to] have power to communicate statistics collected by them or their interpretation of statistics so collected not only to the Government department or person for whom the information was collected but also to other authorities or persons to whom the information or interpretation may be useful.*

The Statistics Act confers broad authority to DOS to "collect and interpret" data related to any field necessary for public policy. However, the Act does not provide DOS with the mandate to manage or direct the national statistical system[14]. Hence, individual agencies[15] can and do collect their own data, administered by their own governance structure with devolved data sharing authority protected under the Official Secrets Act.

In September 2020, the Malaysian government announced its plan to revise the Statistics Act to strengthen the role of DOS to "develop a systematic mechanism for coordination, reach and cooperation in data sharing"[16]. The Minister in the Prime Minister's Department admitted that government data is presently scattered across different databases held by various agencies. Therefore, the plan is to streamline data coordination between government agencies.

A reform to the Statistics Act is much welcome. However, one question remains. How is the decision to share government data to stakeholders outside the government made? Under the current Statistics Act, DOS has the power to share data with anyone outside the government "where they consider it in the public interest". This essentially means that the Chief Statistician has broad discretion to determine what data can be shared with the public. If the proposed coordination of government data management that empowers DOS comes to pass, depending on the form of the coordination and in the absence of laws that compel government data disclosure, it may imply granting substantial and concentrated power to an individual to decide what government data can be shared.

---

[13] Section 2 of the Statistics Act 1965 (Act 415) (Revised 1989)
[14] World Bank (2017b)
[15] In this paper, 'agencies' refers to government ministries, agencies, and states government offices.
[16] Nur Hanani (2020)

Personal Data Protection Act 2010

With regard to personal data, Malaysia is the first country in Southeast Asia[17] to enact a **Personal Data Protection Act (PDPA) in 2010**. This Act refers to "personal data" as[18]

> *… any information in respect of commercial transactions …*
>
> *that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010;*

However, this Act does not apply to[19]

> *(1) … the Federal Government and State Governments. [and]*
>
> *(2) … any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.*

The Office of the Personal Data Protection Commissioner, under the Ministry of Communications and Multimedia (KKMM), published the Personal Data Protection Standard 2015 that serves as a guideline in the implementation of the PDPA. It comprises of security standard, retention standard and data integrity standard[20].

Aside from the PDPA and professional regulations such as the Malaysian Medical Council (MMC)'s Code of Professional Conduct, there is no other law that protects data privacy in Malaysia. The non-applicability of the federal and state governments under the PDPA means the privacy of government data is not protected by any law. Although the common law principle of privacy breach may still apply to government data, the absence of a written law covering government data has to be looked into, especially with the increasing amount of digital data collected by governments. Further discussion on this is in Section 5.3.

[17] World Bank (2017b)
[18] Section 4 of the Personal Data Protection Act 2010 (Act 709)
[19] Section 3 of the Personal Data Protection Act 2010 (Act 709)
[20] Personal Data Protection Standard 2015, Personal Data Protection Commissioner Malaysia

2.2. Overview of policy on open government data in Malaysia

Eleventh Malaysia Plan 2016 – 2020

The **11th Malaysia Plan** seeks to enhance service delivery with citizens at the centre. One of the strategies outlined is to leverage data by "proliferating open data among agencies, encouraging cross-agency data sharing, and leveraging big data analytics (BDA)". In this respect, the plan aims to strengthen the role of the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), an agency under the Prime Minister's department, to spearhead the modernisation of the public sector[21].

The Malaysian Administrative Modernisation & Management Planning Unit (MAMPU)

As the agency responsible for open government data initiative in Malaysia, MAMPU manages the Malaysia Open Data Portal (data.gov.my), a one-stop portal for government data in Malaysia[22]. In 2015, the agency distributed a **General Circular: Public Sector Open Data Implementation** to all federal and state government agencies as well as local authorities to guide the implementation of open government data. MAMPU defines open data as "data that can be used freely, can be shared and reused by citizens, government and private agencies for any purposes"[23]. Three goals of open government data were articulated in the circular:

- To improve the transparency of government service delivery through accurate, fast, and relevant data sharing.
- To increase the productivity of the country's digital economy through new industries or innovations with the involvement of the people and the business community.
- To put Malaysia on par with other countries in digital government initiatives.

Under the **Public Sector Information and Communication Technology (ICT) Strategic Plan 2016 – 2020**, MAMPU underlines a data-driven government as one of the plan's cores[24]. The plan outlines five programmes under two strategies related to government data (Table 1).

Table 1: Strategic core 2 (data-driven government) in the Public Sector ICT Strategic Plan 2016 – 2020

Strategy	Objective	Programme
Utilisation of government data	Optimising the use and realising the value of public sector data	Expansion of the public sector open data initiative
		Acceleration of public sector big data initiative
		Government service delivery transformation with data analytics
Managing and coordinating public sector data	Managing public sector data efficiently and holistically	Development of public sector data governance
		Development of data sharing and management hub

Source: MAMPU (2016)

[21] EPU (2015)

[22] MAMPU (n.d.). Open government data is not only published in the Malaysia Open Data Portal (data.gov.my). Many ministries and agencies publish data in their own website, and some have their own open data portal such as eStatistik of the Department of Statistics.

[23] Prime Minister's Department (2015)

[24] MAMPU (2016)

There is an obvious hurdle in implementing strategies outlined in the Public Sector ICT Strategic Plan. While MAMPU can initiate efforts to coordinate government data management and encourage data sharing, it does not have a legal mandate to enforce those efforts. As discussed in the previous sub-section, individual agencies have broad autonomy in their data management.

The Department of Statistics Malaysia (DOS)

The **Department of Statistics Malaysia (DOS) Transformation Plan 2015 – 2020** expresses the department's commitment to improving accessibility to its data[25]. DOS has bilateral memoranda of understanding (MOU) with at least 12 universities for data sharing[26]. As previously mentioned, although DOS is the national statistical agency, the department's authority including its open data policy is limited to the data it collects.

The Ministry of Communications and Multimedia (KKMM)

The Ministry of Communications and Multimedia (KKMM) identified open data as one of the key areas in the **Communications and Multimedia Blueprint 2018 – 2025**[27]. On the surface, KKMM's open data agenda focuses on data from the private sector. However, while the blueprint listed programmes specifically for data from the private sector, it also suggests "strengthen[ing] the quality and coverage of open *government* data by reinforcing policy guidelines on open data performance"[28]. It is unclear how open data initiatives by MAMPU and KKMM fit together.

The Ministry of Science, Technology and Innovation (MOSTI)

The **National Policy on Science, Technology and Innovation 2021 – 2030** under the Ministry of Science, Technology and Innovation (MOSTI) also highlights open data as one of its strategies[29]. The focus of this policy is research data. In 2019, MOSTI (previously known as the Ministry of Energy, Science, Technology, Environment and Climate Change) established the **Malaysia Open Science Platform (MOSP)** to advance open science by formulating policy, nurturing capacity building, and developing infrastructure[30]. However, one aspect that is perhaps overlooked by MOSTI is access to government data for research[31].

The National Archives of Malaysia

There is no noteworthy initiative to digitise non-digital data. Nevertheless, under the **National Archives of Malaysia Strategic Plan 2016 – 2020**, the agency plans to digitise archival materials. The goal is, however, to enhance the conservation and preservation of archival

---

[25] DOSM (2015)
[26] World Bank (2017b)
[27] KKMM (2018)
[28] KKMM (2018)
[29] MOSTI (2021a)
[30] MOSP (2020)
[31] Ashraf (2020d) discusses the value of government data for research and issues faced by academic researchers in accessing government data

materials[32]. There is no mention of increasing access to archives as part of the objective of the effort. Besides, digitised archival materials are not in a machine-processable format[33]. The National Archives of Malaysia is currently under the purview of the Ministry of Tourism, Arts and Culture Malaysia[34].

Training for public servants

The Public Service Department (JPA) and the National Institute of Public Administration (INTAN) started to institutionalise **digital government training** for public servants in 2016. Six new areas of training have been introduced: (i) strategic digital management, (ii) big data service management, (iii) digital government management, (iv) infrastructure management, (v) security and privacy management, and (vi) quality and regulation. Inclusive of eight information and communication technology (ICT) areas introduced previously, there are now 14 areas of training related to ICT competency[35]. This training, however, is only for public servants managing ICT (Grade F in the public service classification)[36]. In the Malaysia Digital Economy Blueprint launched in February 2021, the government announced plans to expand digital training for public servants across all grades and schemes[37].

2.3. Open government data governance

Since government data management in Malaysia is decentralised with every agency having the authority to decide what data can be shared, open government data governance is also decentralised (Figure 1).

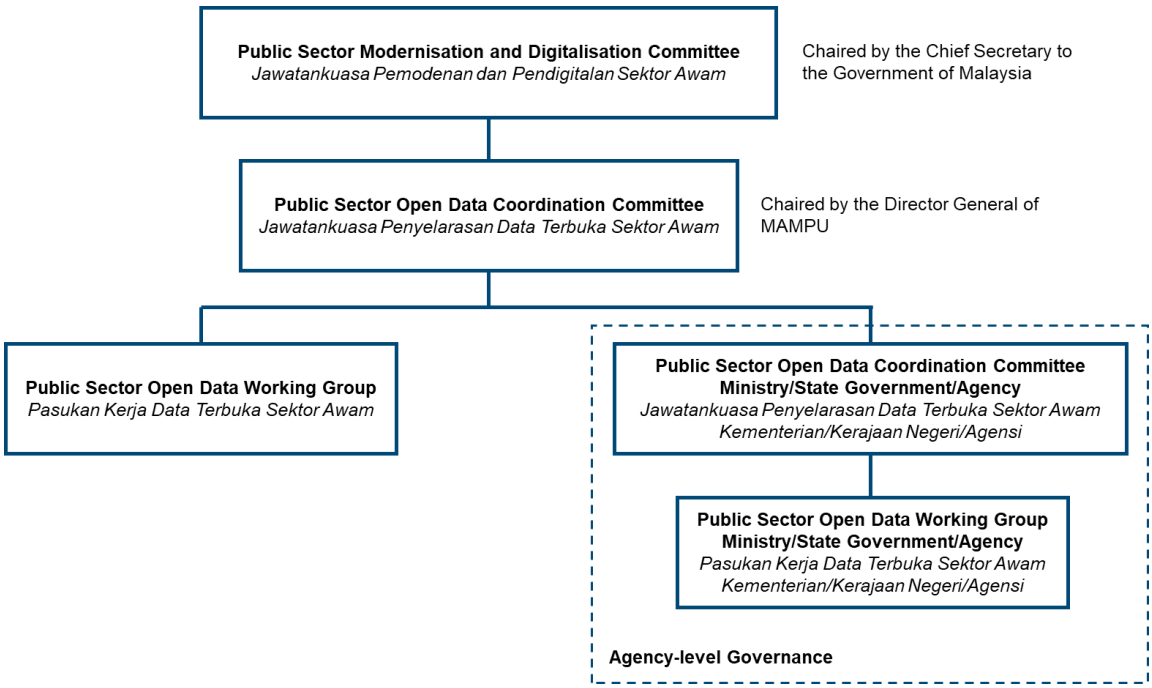
At the central government level, the highest committee responsible over the open government data initiative is the **Public Sector Modernisation and Digitalisation Committee**, chaired by the Chief Secretary to the Government of Malaysia. Under said committee there is the **Public Sector Open Data Coordination Committee**, chaired by the Director General of MAMPU. In general, the Coordination Committee only carries out strategic planning and policy advisory roles with no enforcement mandate. MAMPU has a Public Sector Open Data Working Group under the committee. This group mainly handles the Public Sector Open Data Platform, identifies potential datasets to be made open and provides advisory services to government agencies.

Every ministry and government agency has its own Public Sector Open Data Coordination Committee chaired by its respective Chief Information Officer or Chief Technology Officer **and its own Public Sector Open Data Working Group**. The Coordination Committee devises an open data strategy for the organisation and approves datasets that can be made open based on the recommendation from the working group. In most ministries and agencies, the Public Sector

[32] ANM (2016b)
[33] Personal communication with MAMPU in January 2021
[34] For comparison, the National Archives of the UK is a non-ministerial department, the National Archives of Singapore is under the Ministry of Communications and Information, the National Archives of Australia is a federal agency, and the Archives New Zealand is under the Department of Internal Affairs.
[35] JPA and INTAN (2016)
[36] Personal communication with MAMPU in January 2021
[37] EPU (2021)

Open Data Coordination Committee comprises the same members as the ICT Development Committee (*Jawatankuasa Pemandu ICT*)[38]. Detailed functions of the committees and working groups mentioned are presented in Table 2.

Figure 1: Open government data structural organisation in Malaysia



Source: Prime Minister's Department (2015) and personal communication with MAMPU in January 2021

Table 2: Functions of open government data governance committees

Committee	Functions
Public Sector Open Data Coordination Committee at the central government level	• Determines the direction and strategy of public sector open data. • Monitors the implementation of public sector open data. • Monitors the level of public sector open data use. • Plays an advisory role in discussing current policies and issues related to public sector open data.
Public Sector Open Data Working Group at the central government level	• Prepares and implements public sector open data implementation plan. • Provides a secure open data platform. • Provides mechanisms and procedures for the publication of open data by agencies in the Public Sector Open Data Portal. • Reviews and identifies potential data sets. • Provides advisory services to agencies concerning the implementation of open data.
Public Sector Open Data Coordination Committee at the ministry/ state government/ agency level	• Formulates strategies and plans for the implementation of open data at the ministry/office of the state secretary/agency level. • Establishes a working group to perform open data tasks/activities. • Approves datasets to be made open. • Monitors the level of open data use. • Ensures policy requirements and targets are complied with and achieved.

[38] Prime Minister's Department (2015) and personal communication with MAMPU in January 2021

Public Sector Open Data Working Group at the ministry/ state government/ agency level	• Reviews and identify datasets to be made open. • Obtains the approval for datasets to be made open. • Prepares and publishes metadata. • Ensures that the approved open datasets are uploaded to the agency's website and DTSA Portal. • Reviews the level of open data use.

Source: Prime Minister's Department (2015)

It is worth mentioning at this point that DOS has a cadre system where statisticians from the department are deployed to ministries and agencies to provide technical assistance in the collection, analysis, interpretation, and dissemination of data. The number of statisticians placed in a ministry or an agency ranges from one to 24 people, depending on the statistical needs of each organisation[39]. Although these statisticians may not be directly responsible for the open government data initiative in each agency, they are likely part of the Open Data Working Group at the agency level[40].

Apart from DOS, the National Archives of Malaysia has also placed officers in every ministry since 2013 to conduct work related to public sector record management[41]. Public sector records include letters, memos, emails, reports, and proposals[42]. Some information in these records may be of public interest too such as public procurement information.

3. Supply-side challenges of open government data

Supply-side challenges refer to the challenges faced by government agencies in supplying open government data. These challenges can be grouped into three inter-related broad categories: policy, infrastructure and human resource, and culture.

3.1. Overarching policy

The biggest supply-side challenge in implementing open government data is the absence of an overarching and clear policy framework. With the Official Secrets Act according every agency the prerogative to decide what data can be shared, and with no law compelling disclosure, open government data initiatives rely largely on each agency's leadership. Implementing open government data is likely the lowest priority when there are other duties and issues deemed more important and urgent by an agency.

Moreover, the current process of releasing data is not very simple as it has to be recommended by the Public Sector Open Data Working Group and approved by the Public Sector Open Data Coordination Committee at the agency level, which is often the same committee that has to handle other ICT matters. Internal data management regulations are not always consistent, for example, repeated requests for the same or similar data do not usually lead to by-default approval[43].

[39] World Bank (2017b)
[40] Personal communication with MAMPU in January 2021
[41] ANM (2016b)
[42] ANM (2016a)
[43] World Bank (2017a)

MAMPU, through the Public Sector Open Data Coordination Committee at the central government level, can only encourage and facilitate government agencies to implement open government data. It does not have an overriding power to dictate the individual agency's open data policy. For example, on a case-by-case basis, DOS provides access to its microdata, but such access is subject to several constraints such as only a third of the indicators or the sample requested by data users being released[44]. MAMPU has no say on this policy.

Many matters that are important to ensure successful and safe implementation of the open data initiative such as data privacy and security are regulated at the agency level[45]. Agencies also determine fees for their data[46]. Depending on their financial autonomy, the revenues collected are either (partially) kept by the agencies or transferred to the Consolidated Fund controlled by the Ministry of Finance[47].

Integration of databases held by different agencies is still sparse[48]. For example, databases maintained by the Ministry of Human Resources and the Ministry of Home Affairs do not necessarily coincide[49]. Inter-agency data sharing is decided on a case-by-case basis with senior managerial approval necessary for most cases[50]. Even data inventories that catalogue what data an agency holds are not accessible by other agencies except with management authorisation on a case-by-case basis[51]. The same issue happens between federal agencies and state agencies[52].

Currently, there is no mechanism to assess the implementation of open government data even though the Public Sector Open Data Coordination Committee at both the central and agency level is supposed to monitor its progress[53]. This is not a unique problem; lack of monitoring and evaluation is noted as a common issue in the implementation of government ICT initiatives[54].

3.2. Infrastructure and human capital

Implementing open government data involves mobilising digital infrastructure and human resources that in most governments are already scarce[55]. It involves more work having to deal with legacy systems such as data format that requires modification[56]. In Malaysia, many agencies

[44] World Bank (2017a)
[45] World Bank (2017a)
[46] World Bank (2017a) and personal communication with MAMPU in January 2021
[47] For example, according to the Companies Commission of Malaysia Act 2001, "the Commission shall pay to the Federal Consolidated Fund an amount not exceeding thirty per cent out of the current annual surplus of the Commission at such time". Hence, some portion of the revenue collected through data fees are kept by the Companies Commission. Source: Government of Malaysia (2018)
[48] World Bank (2017a)
[49] World Bank (2017b)
[50] World Bank (2017a)
[51] World Bank (2017a) and personal communication with MAMPU in January 2021
[52] World Bank (2017b)
[53] Personal communication with MAMPU in January 2021
[54] Sudirman and Yusof (2017)
[55] Barry and Bannister (2014); Ruijer and Meijer (2020); Martin (2014)
[56] Barry and Bannister (2014) and personal communication with MAMPU in January 2021

indicate that they have a small ICT team[57]. Meanwhile, MAMPU also has limited capacity to reach out to and support every government agency, with less than five management and professional level staff responsible for the open data initiative[58].

The quality of open government data varies widely across agencies, which, aside from reflecting the priority of the agency and its organisational culture, partly indicates differences in data infrastructure and human capital across agencies. However, there is no systematic competency framework to track and measure ICT skill levels among public servants[59]. It is not known whether there is a framework to assess the adequacy of digital infrastructure across agencies. Without a systematic assessment of the current status and actual needs of digital infrastructure and human capital across agencies, it is uncertain how resources are allocated appropriately to each agency to achieve the government's ICT aspirations.

3.3. Public sector awareness and culture

There is low intrinsic motivation among Malaysian public servants to implement open government data[60]. This is not surprising as there is no overarching policy that institutionalises open government data as an essential public service as opposed to merely being a nice-to-have public offering. It is likely that some public servants view making data open an additional burden imposed by MAMPU[61]. Some think that data published by the government is enough, given that it is not widely used by the public[62].

There is also the fear of misinterpretation, manipulation, and misuse of government data among public servants[63]. Some are also concerned that foreign parties may appropriate a bigger advantage over local stakeholders as the result of open government data[64]. These concerns are not trivial. They need to be properly addressed to ensure not only buy-in from public servants but also inclusive and safe use of government data.

4. Demand-side challenges of open government data

Demand-side challenges are challenges faced by data users in accessing and using government data. These challenges can be the result of shortcomings of data users or data providers.

---

[57] World Bank (2017a)
[58] Mustapa, Hamid, and Nasaruddin (2019) and personal communication with MAMPU in January 2021
[59] World Bank (2017a)
[60] World Bank (2017a)
[61] Based on general sentiment I assessed during Malaysia Open Data User Group forum in December 2020, which was attended by representatives from government agencies
[62] World Bank (2017a) and based on observations gathered during a Malaysia Open Data User Group forum in December 2020
[63] World Bank (2017a)
[64] World Bank (2017a)

4.1. Latent demand for data

Latent demand refers to the "demand for a product or service that a consumer cannot satisfy because they do not have enough money, because the product or service is not available, or because they do not know that it is available"[65]. Latent demand is a major demand issue when it comes to government data. An argument that there is low demand for government data, hence there is no necessity to publish a lot of data, is rather untenable when the supply of the right data, i.e. data that is useful and needed, is not accessible or when potential data users do not know what data they can demand.

In Malaysia, civil society groups and researchers noted that granular, complete, timely and old data is not accessible[66] and some data is not free[67]. Moreover, a lot of data published on agency websites is not in an open format, for example in PDF instead of a machine-processable format. Besides, most government agencies do not publish data inventories[68], making it difficult for the public to know what data they can request if it is not publicly available.

The process of requesting publicly unavailable data from government agencies is not clear. Many external stakeholders consider requesting data an unpredictable and inefficient process[69]. Many agencies do not publish the standard procedure for data requests on their website.

Although there is a lot of data published in the data.gov.my portal, a high proportion of the portal's users perceive the portal as 'not useful', relative to other open data platforms[70]. Limited user-friendliness of the open data portal presents a hindrance to effective government data use even when data is made available online[71].

4.2. Digital skills

Coursera, a popular massive open online course (MOOC) provider, conducts benchmark assessments of skills proficiency around the world called the Global Skills Index (GSI)[72]. In its latest and second edition published in 2020, the index evaluated 60 countries in 11 fields of study in business, technology, and data science. The GSI is not necessarily representative of a country because it only reflects Coursera learners. That said, the findings are still insightful as Coursera learners are mostly those who want to learn a new skill or enhance their skills by their own initiative.

---

[65] Cambridge English Dictionary (n.d.)
[66] Ashraf (2020d); World Bank (2017a)
[67] World Bank (2017a)
[68] World Bank (2017a) and personal communication with MAMPU in January 2021
[69] World Bank (2017a)
[70] Ashraf (2020d)
[71] Ruijer and Meijer (2020); Meijer, Conradie, and Choenni (2014)
[72] Coursera (2020). The GSI adopts proficiency measurements based on a machine learning method called the Glicko algorithm to assess how proficient each learner is in each competency and how challenging each assessment is.

Domains of skills that are relevant for this paper are technology and data science. Skills in the technology domain include computer networking, databases, human-computer interaction, operating systems, security engineering, and software engineering. Skills in the data science domain include data management, data visualization, machine learning, mathematics, statistical programming, and statistics.

In the technology domain, Malaysia ranked 49 out of 60 countries and is behind the Philippines, Thailand, Singapore, Indonesia, and Vietnam. In the data science domain, Malaysia ranked 43 and is behind Thailand, the Philippines, and Singapore. As mentioned, the GSI is not representative of the entire population but the fact that Malaysia is behind many countries including neighbouring and other developing countries is a call for action. In the context of open government data, users without the right skills will not be able to utilise government data for meaningful change. In a broader context, the lack of technology and data skills may become a hindrance for Malaysia to develop high-value industries and catch up with global technological advancement.

5. The way forward for Malaysia

Based on global experience, some open development policies—that include open data, open innovation, open science, crowdsourcing, etc.—are short-lived, under-resourced, and poorly implemented[73], frustrating the goals they are supposed to achieve. Therefore, for Malaysia to fully reap the benefits of open government data while also managing its potential downsides, the country needs a cohesive policy and a sustained commitment to said policy. As with other techno-social innovations, transformative impacts from open government data do not occur overnight[74]. As it stands, open government data is still a novel concept that needs time and effort before breaking through into the mainstream.

Open government data is not an end in itself. The ultimate goal of the open government data agenda is to improve the well-being of the people through economic development, good governance, and knowledge creation enabled by access to data[75]. Policymakers also need to be cognizant of potential negative impacts that result from opening up data. Without the right policy, the impacts of open government data will not necessarily be equal across society. Open access to data may reinforce existing power asymmetries and inequalities. It is necessary to locate open government data policy within a bigger techno-social context and multi-layer governance.

At the global level, the governance of 'knowledge commons'[76] is often embedded in trade agreements such as intellectual property regulations[77]. At the national level, meaningful and inclusive use of open government data is a function of internet infrastructure, digital literacy, laws around censorship and freedom of expression, surveillance and privacy concerns, and various other aspects of culture, socioeconomics, and politics[78]. At the local level, state governments or

[73] Mansell (2020)
[74] Martin (2014)
[75] Ashraf (2020b)
[76] Data is a 'knowledge common' once it is openly accessible
[77] Mansell (2020)
[78] Mansell (2020)

municipal authorities may drive open government data through a bottom-up approach without relying on the federal government[79] or they may create obstacles to the agenda by refusing to share local-level data.

This section highlights some important considerations in shaping an inclusive and meaningful open government data policy. The discussion in this section focuses primarily on national-level policy and is by no means comprehensive. That said, some issues discussed in this section are relevant not only for open government data but also the larger agenda of digital government and digital transformation.

5.1. Right to Information law in the digital age

This sub-section begins by establishing the normative view of the Right to Information as a fundamental human right and a core component of democratic participation. It then discusses how a Right to Information (RTI) law can play a role in the successful implementation of open government data although the two embody different approaches to government data sharing.

The basis for the Right to Information (RTI)

Article 19 of the Universal Declaration of Human Rights (1948) states that

> *everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and* ***to seek, receive and impart information and ideas*** *through any media and regardless of frontiers*

Likewise, item 23 of the ASEAN Human Rights Declaration (2012) that Malaysia adopted states that

> *every person has the right to freedom of opinion and expression, including freedom to hold opinions without interference and* ***to seek, receive and impart information****, whether orally, in writing or through any other medium of that person's choice*

His Royal Highness Sultan Azlan Shah, the ninth Yang di-Pertuan Agong of Malaysia and the former Lord President of the Federal Court noted that[80]

> *though the Federal Constitution does not expressly provide that all persons have the "right to know",* ***the fundamental right of expression as embodied in Article 10(1)(a) will be meaningless if the public do not have the necessary information*** *on which they can express their views*

and that

[79] Keng (2018)
[80] Sultan Azlan Shah (2004)

> *it should not be overlooked that* ***the right to know and the right to free expression are as basic and important as any other fundamental right*** *enshrined in the Federal Constitution*

On the role of governments with regard to data they collect, the African Commission on Human and Peoples' Rights provided a concise articulation that says[81]

> *public bodies hold information not for themselves but* ***as custodians of the public good*** *and everyone has a right to access this information, subject only to clearly defined rules established by law*

In the same vein, Sultan Azlan Shah noted that[82]

> *… the responsibility of the executive (which is usually made up of elected representatives) is to administer the country on the people's behalf. The executive possesses no other power except that which has been given to them by the people themselves. Therefore in the exercise of these powers,* ***the executive should ensure that they do not clothe themselves with excessive powers which in turn may be invoked by them to curb the rights provided for by the Constitution***

The Right to Information is also a core component for democratic participation. In the case of Union of India v. Association for Democratic Reforms, the Supreme Court of India held that[83]

> *one-sided information, disinformation, misinformation and non-information all equally create an* ***uninformed citizenry which makes democracy a farce***

In the Malaysian context, Sultan Azlan Shah noted that[84]

> *the three branches of the Government—the legislature, the executive and the judiciary—should ensure that the means of obtaining information is made available to the people, so that* ***they can play a meaningful role in the participation of an open Government***

and that

> *an open Government must be* ***the hallmark of a truly democratic country***

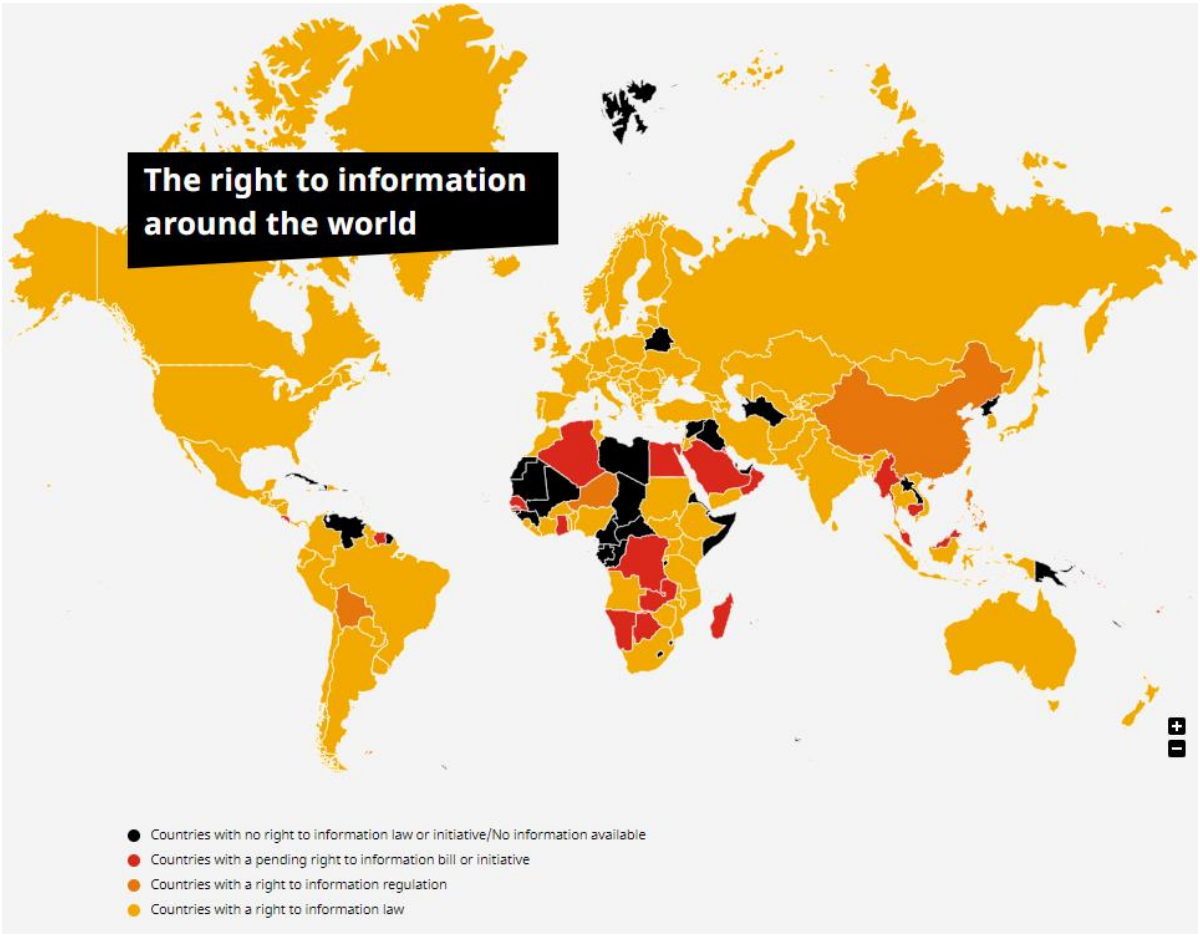
---

[81] African Commission on Human and Peoples' Rights (2002)
[82] Sultan Azlan Shah (2004)
[83] Supreme Court of India (2002)
[84] Sultan Azlan Shah (2004)

A Right to Information (RTI) law

A Right to Information (RTI) law, which is also referred to by different names such as Freedom of Information (FOI) law and Public Information Disclosure law, is a law that formalises the right of the people to access information held by public bodies. It typically provides clear processes and requirements for people to request information and for public bodies to respond to such requests.

Figure 2: The world's map of the Right to Information law



Source: Directly taken from https://www.article19.org/right-to-information-around-the-world/ (Accessed 26 January 2021)

As of 2019, 126 out of 193 United Nations member states and two non-member states have an RTI decree, whether in a form of a law or an actionable regulation[85]. Around 90% of the world's population and 96% of the population in the Asia Pacific live in a country with an RTI law or regulation[86]. In Southeast Asia, Thailand (since 1997), Indonesia (since 2008), Timor-Leste (since 2016), and Vietnam (since 2016) have an RTI law whereas the Philippines (since 2016) has an actionable RTI regulation[87]. Malaysia, unfortunately, is among the few countries that still do not have an RTI law or an actionable regulation at the national level. However, Malaysia does have a

[85] Open Society (2019); Global RTI Rating (n.d.)
[86] Article 19 (2018)
[87] Open Society (2019)

pending RTI law, with stakeholders' consultation started in 2018[88]. The law was expected to be tabled in the parliament mid-2020[89] but till today it has not happened. The states of Selangor and Penang already have state-level RTI laws. Figure 2 shows countries with an RTI law or regulation and countries with an RTI bill pending.

Harmonising Open Government Data and a Right to Information law

While the Right to Information laws typically operate through reactive disclosure of government information (i.e. on-demand disclosure), open government data calls for proactive disclosure of information. At the heart of open government data is **collaboration** as opposed to litigation[90]. Besides, in practice, RTI law is commonly used to obtain data related to the government's operations and accountability. On the other hand, open government data involves opening up a wider range of data held by the government including socioeconomic and environmental data[91].

Despite the different mechanism and approach to government data, open government data and RTI law are not in conflict; in fact, they complement each other. An RTI law is necessary to compel disclosure[92]. Although open government data upholds the principle of 'open by default', governments may be reluctant to disclose certain information. This is when an RTI law would come into the picture to demand disclosure and provide legal recourse. Therefore, a policy framework that blends the two can create a more effective system of government data-sharing that fosters collaboration as well as checks and balances.

Considering a federal RTI law for Malaysia has yet been tabled in the parliament, several issues are worth looking into to formulate an RTI law that is fitting for a digital age and consistent with open government data. The following discussion draws on some lessons from existing RTI laws around the world. References to the Penang Freedom of Information Enactment 2010 and the Freedom of Information (State of Selangor) Enactment 2011 are made simply because they are the only freedom of information (FOI) laws existing in Malaysia. Discussing their shortcomings does not necessarily imply that the laws are bad but serves to highlight where improvements could be made, not only for those state laws but more importantly for formulating a federal law.

First, a good RTI law is one that predicated on the 'open by default' principle. Although this principle is particularly emphasised in open government data, it is a principle that forms the basis for many RTI laws around the world. Therefore, it is not a new idea. Unfortunately, this principle is missing from the Penang and Selangor FOI laws. FOI law in these states has no overriding power over other laws, including the Official Secrets Act that confers broad discretions to government agencies to decide what data can be disclosed with limited judicial review. This limitation, to some

[88] Parliament of Malaysia (2019)
[89] Kannan and Babulal (2019)
[90] Noveck (2017)
[91] Noveck (2017)
[92] Noveck (2017)

extent, is likely because a state law has to operate under the overarching federal law. Both the Selangor and Penang FOI laws state that[93]

> *If the information sought to be accessed by any person is contained in a document disclosure of which is subject to any written law,* ***access to such information shall be subject to such written law****.*

On the contrary, many RTI laws around the world, for example, the Indian Right to Information Act 2005, the New Zealand's Official Information Act 1982, and the US Freedom of Information Act list specific grounds on which information is exempted from disclosure such as information that would likely cause harm to national security, national economy and international relations. Otherwise, all information should be accessible. Although the Indian Official Secrets Act (OSA) 1923 has an overriding effect on the country's RTI law, the Indian OSA is different than the Malaysian OSA, as the former only deals with espionage activities. In the absence of a clear exemption list coupled with a broadly defined 'official secret' in the OSA, the Penang and Selangor FOI laws have limited compelling force to counter the discretionary power of agencies.

As pointed out by Botterman et al. (2000), the exemption list in the US FOI law, and similarly in India's and New Zealand's laws, is not a mandatory closure list. Instead, it is a discretionary disclosure list where agencies can, following a reasonable judgement, decide to withhold information on the grounds listed. The Indian RTI law states that the exempted information can be disclosed "if public interest in disclosure outweighs the harm to the protected interests"[94]. For example, even if the information has potential to hurt national economic interest, it could be disclosed if the public interest in disclosure is bigger. The US FOI law requires agencies to "consider whether partial disclosure of information is possible whenever the agency determines that a full disclosure of a requested record is not possible" and "take reasonable steps necessary to segregate and release nonexempt information"[95].

It should be emphasised that the 'open by default' principle does not mean that all information should be disclosed. Some information should not be disclosed not only to protect the privacy of individuals or groups but for the sake of public interest such as to protect the sovereignty and security and the economic and diplomatic interests of the country. The 'open by default' principle instead calls for a 'harm test' in determining whether a piece of information can be disclosed[96], countering the presently common mindset of 'secret by default'.

Second, an RTI law of a digital age needs to embrace digital technology. The amendment to the United States FOI Act in 1996 expanded the definition of "record" to include information made available in electronic format. Additionally, the amendments required certain records to be released in electronic format and for agencies to provide electronic reading rooms for the public

[93] Section 5 of the Freedom of Information (State of Selangor) Enactment 2011 and Section 5 of the Penang Freedom of Information Enactment 2010

[94] Section 8 (2) of the Indian Right to Information Act 2005

[95] Paragraph (8)(A)(ii) subsection (a) of the FOIA Improvement Act of 2016

[96] Further deliberation is, of course, needed to determine how harm is measured

to access records[97]. More recently, on 14th of January 2019, the United States' Open, Public, Electronic and Necessary (OPEN) Government Data Act was enacted that mandates all non-sensitive government data be made available in machine-readable format under an open license[98]. The Indian RTI Act not only encourages information to be released in electronic format when possible, but, early in the Act, also emphasises computerisation of government records and that they are "connected through a network all over the country on different systems so that access to such records is facilitated"[99]. Likewise, the South African Promotion of Access to Information Act 2000 requires records that are "available or capable of being made available in computer readable form" to be released in that form[100].

On the contrary, even though the Penang and Selangor FOI laws are more recent than the US, Indian and South African RTI laws, nothing is said about releasing information in an electronic or digital format, let alone in a machine-readable format. In fact, they both imply analogue format as the standard manner for information access. Take the Selangor FOI law as an example; it says[101]

> *10. (1) Access to information may be in the following manner:*
>
> *(a) in the situation where the information is an article or thing from which sounds or visual images are capable of being reproduced,* ***an appointment may be made for the applicant to hear or view those sounds or visual images****; or*
>
> *(b) in the situation where the information are words in the form of record which are capable of being reproduced in the form of sound or words in the form of shorthand writing or in codified form,* ***the department may reproduce the information in the form of a written copy****.*
>
> *(2) Access to information may be given in the form or manner that is most practical to the department, subject to the form of the information itself.*

Although there is a provision in both Selangor and Penang FOI laws that gives access to information "in the form or manner that is most practical *to the department*"[102], it does not encourage information release in a digital format nor explicitly indicate a digital format as an option to access information. Moving forward, Malaysia should consider an RTI law that not only encourages information release in a digital format but also in a machine-processable format to harmonise the law with the open government data agenda.

In 2012, the US government launched FOIAonline, a website that helps users submit an information request, track the progress of the request in real-time and immediately access

---

[97] Botterman et al. (2000)
[98] Title II of the US Foundations for Evidence-Based Policymaking Act
[99] Section 4(1) of the Indian Right to Information Act 2005
[100] Section 29(2) of the South African Promotion of Access to Information Act 2000
[101] Section 10 of the Freedom of Information (State of Selangor) Enactment 2011
[102] Section 10(2) of the Freedom of Information (State of Selangor) Enactment 2011 and Section 10 (1) of the Penang Freedom of Information Enactment 2010

documents that have previously been released[103]. This is more efficient and transparent than having to "inform the applicant of the matter in writing" such as in the case of "information not in possession" in the Selangor FOI law[104].

Third, Malaysia should formulate an RTI law that requires proactive disclosure of certain information. This is in line with the spirit of open government data. The Indian RTI Act explicitly listed 17 information items that should be published automatically and updated every year including "the monthly remuneration received by each of [agency's] officers and employers", "the manner of execution of subsidy programmes", "particulars of recipients of concessions, permits or authorisations granted by it", and "such as other information as may be prescribed"[105]. The law also requires the publication of "all relevant facts while formulating important policies or announcing the decisions which affect public"[106], which is particularly relevant with regard to Covid-19 interventions. It is beyond the scope of this paper to examine how the proactive disclosure clause in the Act is translated into actual implementation in India and where lessons can be drawn for Malaysia. That said, having such a provision in the RTI law is a crucial first step.

Nevertheless, most of the items listed for proactive disclosure under the Indian RTI law relate to aspects of governance. To harmonise the RTI law with the participation objective of open government data, other types of data, such as socioeconomic and environmental data should also be considered for proactive disclosure. Under the South African RTI law, every public body is required to identify information that can be disclosed and updated voluntarily. Such information would be gazetted for automatic disclosure[107]. However, the South African law gives the liberty to the information officer of the public body and the minister in charge to determine such information. Meanwhile, the United States FOI Act requires automatic online publication of information that an agency "determines have become or are likely to become the subject of subsequent requests" or "that have been requested 3 or more times"[108].

Sinar Project, a Malaysian non-governmental organisation that advocates for open government data, has highlighted how due to limited data publicly available on certain topics such as crime, parliamentarians often repeatedly asked for the same data in parliament sittings. As Sinar Project pointed out, this should be a clear indicator of the importance of such data and should have led to proactive disclosure[109].

Ideally, the government should also employ a "release-to-one-release-to-all" policy by publishing data requested through RTI law in the public domain (not only directly to the applicant) to avoid dealing with repeated requests from different applicants, which divert government resources unnecessarily[110]. Furthermore, under the Selangor FOI law, agencies are not required to entertain

---

[103] Altman et al. (2015)
[104] Section 11 of the Freedom of Information (State of Selangor) Enactment 2011
[105] Section 4(1) of the Indian Right to Information Act 2005
[106] Section 4(1) of the Indian Right to Information Act 2005
[107] Section 15 of the South African Promotion of Access to Information Act 2000
[108] Paragraph (2)(D) subsection (a) of the FOIA Improvement Act of 2016
[109] Sinar Project (n.d.; n.d.b)
[110] Noveck (2017)

an application "from the same person which has been complied with within the previous six months"[111]. Adopting a "release-to-one-release-to-all" policy may help reduce vexatious requests.

It is worth discussing fees for RTI requests. Adopting the "release-to-one-release-to-all" policy would imply that agencies are not able to collect fees from subsequent disclosures of information. It is, therefore, important to be clear on the purpose of imposing fees for RTI requests. Unlike the Selangor and Penang FOI laws, many global RTI laws clearly outline how fees should be regulated. Generally, according to these laws, the fees are imposed merely to recuperate the cost of providing access to information. The Indian RTI Act states that information should be "available free or at such cost of the medium or the print cost price"[112] and "no such fee shall be charged from the persons who are of below poverty line"[113]. The South African law states that the fee should be reasonable for "the cost of making a copy of a record" and "the time reasonably required to search for the record and prepare"[114]. The US FOI Act differentiates fees imposed on information requests for commercial, educational and media, and other purposes[115]. The Act also states information disclosure in the public interest should be done at no charge or reduced fees[116]. In a nutshell, agencies should not be concerned about the loss of revenue from proactive disclosure as government information is not supposed to be monetised in the first place.

Taking all the three recommendations together, Malaysia should consider an RTI law at the federal level that embodies the principle of 'open by default' and one that has an overriding effect over other government information laws. Malaysia should also consider formulating an RTI law that combines the proactive disclosure approach of the Indian, South African, and the US laws by (i) explicitly listing types of information that should be automatically available, (ii) requesting every public body to determine the information that should be regularly and automatically disclosed (to be governed by a gazette), and (iii) imposing automatic public disclosure for information that has been requested either through an RTI request or in parliament. All information released whether through RTI requests or proactive disclosure should be made available in a machine-processable format whenever possible (but not as the sole format, as options should be given to accommodate those with no digital access) and be publicly accessible.

5.2. Streamlining government data policy

Governments have two main duties concerning government data: to protect the privacy and the security of the data and to realise public value from the use of the data[117]. These duties are essentially embodied in open government data. The ultimate goal of open government data is to maximise the potential value from data. But the agenda can only be supported by the public if

[111] Section 12 of the Freedom of Information (State of Selangor) Enactment 2011. A similar provision but with no stipulated timeframe can be found in the Penang FOI law.
[112] Section 4 (4) of the Indian Right to Information Act 2005
[113] Section 7 (5) of the Indian Right to Information Act 2005
[114] Section 22 (7) of the South African Promotion of Access to Information Act 2000
[115] Paragraph (4)(A)(ii) subsection (a) of the FOIA Improvement Act of 2016
[116] Paragraph (4)(A)(iii) subsection (a) of the FOIA Improvement Act of 2016
[117] Dawes (1996)

they trust that their privacy and security will not be compromised as the result of the government collecting and sharing data related to them.

To carry out these two duties well, data management of different government agencies has to be streamlined. For example, to devise a sound policy to improve the health of the population, the government might want to understand the factors that lead to poor health choices, such as the affordability of a nutritious diet, inaccessibility of public parks, lack of education and awareness, or time poverty that leads people to opt for fast foods. To fully understand the issue, analyses of data from various sources, not limited to health data, are required. Hence, data integration is needed. However, increasing data integration may increase the risk of reidentification of personal information. Data privacy and security risks need to be addressed holistically. Open government data, therefore, cannot be an afterthought with each government agency working in a silo with no or limited overarching policy.

Institutionalised commitment

As discussed in Section 2.1, one of the major stumbling blocks in implementing open government data in Malaysia is the absence of a clear legal framework to institutionalise providing access to government data as one of the core services of the government. In 2015, MAMPU distributed a general circular to all agencies on the implementation of open government data. This circular is a good starting point to familiarise agencies with the concept of open government data, but it has weak enforcement power. In this regard, it is time for Malaysia to enact an **RTI law** that is fit for a digital age and that embodies the principles of open government data (as discussed in the previous sub-section).

Malaysia should seal its commitment to open government data by adopting **international partnerships and declarations**. Notably, Malaysia is not a member of the Open Government Partnership (OGP) or the Open Data Charter (ODC). Through the OGP, participating countries work with civil society organisations to co-create two-year open government action plans with concrete commitments to be implemented. Among Southeast Asian countries, Indonesia and the Philippines are members of the OGP. Meanwhile, the ODC adopters pledge their commitment to publishing timely and comprehensive, accessible and usable, comparable and interoperable government data open by default, for improved governance and citizen engagement and for inclusive development and innovation. In Southeast Asia, the Philippines is the only ODC adopter.

Clear and agile governance framework[118]

Malaysia should consider introducing a cross-agency **Chief Data Steward** role to lead the open government data agenda with key functions include carrying out (i) partnerships and community engagement such as with researchers and civil society groups; (ii) internal coordination and

[118] While this paper proposes an open government data governance structure, it does not go into detail how the existing structure in Malaysia would be adjusted into the proposed structure (e.g. who should be appointed as the Chief Data Steward, how does MAMPU and DOS fit into the proposed structure, etc.) as that is something that the government has to study and deliberate further

agencies engagement; (iii) data audit and ethics, value and risk assessment; (iv) dissemination and communication of data; and (v) data collaboratives including with the private sector[119].

The Chief Data Steward shall be supported by at least **two permanent groups** of public servants that perhaps form a department to oversee the open government data agenda. The first group is a **stakeholders' engagement group** that mainly carries out engagement with governmental and non-governmental stakeholders and public communication of government data. This group provides recommendations on the social aspect of open government data policy. The second group is a **digital service group** comprised of experts who oversee the technical aspects of open government data such as data privacy and security protection, data standards, data platforms, and data analytics. This group provides recommendations on the technical aspect of open government data[120]. These two groups shall play both operational and developmental roles in the open government data agenda.

The Chief Data Steward role is not a completely novel idea. New Zealand has a Government Chief Data Steward (GCDS). While the role of the Chief Statistician is an agency-specific role (similar to Malaysia, the Chief Statistician leads DOS), the role of GCDS is an across-government role. The stated duties of the GCDS include to co-develop a Data Stewardship framework to enable agencies to manage data as a strategic asset; lead the government's commitment to accelerate the release of open data including the implementation of the International Open Data Charter; and develop data governance across the system through evolving approaches to data ethics and Māori data governance[121].

Along with these two permanent groups that support the Chief Data Steward, the government could consider forming a **Government Data Consultative Council** comprised of governmental and non-governmental stakeholders representing various government agencies and various segments of society[122]. The role of the Council would be providing recommendations to the government on matters related to the collection, management, publication and use of government data. The main goal of this council is to serve as a platform in ensuring that the open government data policy is inclusive (a subject that will be discussed further in Section 5.4) and responsive to fast-changing technological advances[123]. The premise underlying the establishment of this council is that the public, apart from the government as the data custodian, should have a say on how data about them is collected, used and shared.

Concerns and barriers identified by public servants in implementing open government data need to be addressed rather than dismissed[124]. Some of the concerns are legitimate such as how

---

[119] Inspired by Verhulst et al. (2020) with modifications

[120] Inspired by Government of Ontario (2015) with modifications

[121] New Zealand Government (2021)

[122] Inspired by Young et al. (2020) with modifications. The idea of a consultative council is not alien in Malaysia. The National Wages Consultative Council (established by Act 732) and the National Youth Consultative Council (established by Act 668) are examples of consultative councils established by law. There are also consultative councils created through Cabinet's endorsement such as the Consultative Council on Foreign Policy and the now-dissolved Consultative Council for People's Harmony.

[123] Verhulst and Young (2016)

[124] Barry and Bannister (2014)

opening up data may impact the country's standing in international negotiations[125]. The considerable work that needs to be put in by public servants and the learning process that needs to take place have to be taken into account in planning the development path of the open government data agenda[126]. The uneven levels of institutional maturity and technical capacity of different agencies to carry out open government data have to be recognised[127]. In this regard, differentiated milestones with specific action plans customised for and negotiated with agencies according to their capacity should be considered.

A clear governance framework also includes proper **decision-making and documentation protocols** to guide and record key decision points impacting data collection, processing, analysis and sharing[128]. This is to ensure accountability of decisions and to identify pain points where improvements could be made. In addition, agencies should also create a mechanism to track data requests and details on how decisions on the data are made to avoid arbitrary denial[129].

Open government data could be an entry point to strengthen coordination between agencies by facilitating data sharing. **Inter-agency data sharing** avoids redundancy in data handling that could lead to improving productivity and reducing the operating cost of agencies[130]. As the first step to foster inter-agency data sharing, agencies should publish their data inventories and make them accessible by at least other government agencies. It is also a good first step for agencies to identify data that can be published publicly.

Digital infrastructure and skills

Digital infrastructure and skills across all agencies ought to be improved by increasing investment in technology, reskilling existing public servants and hiring a high-skilled workforce with competence in data management and digital technology. One of the initiatives that the Malaysia Open Science Platform (MOSP) has started is providing data stewardship training to existing librarians in public universities to equip them with the skills to manage digital raw research data on the open science platform. MOSP targets to train 200 data stewards by July 2021[131]. This initiative could be an inspiration for the government to carry out a **reskilling initiative** for existing public servants.

Implementation of open government data involves several technical aspects beyond putting data on a website. Apart from ensuring that the privacy and security of the data are protected (a subject that will be discussed further in Section 5.3), to facilitate data integration, data should be **interoperable**. Interoperability is the ability to seamlessly "transfer and render useful data and other information across systems, application or components"[132]. To give an example, because of interoperability, we do not have to worry about signalling standards or transoceanic cables when

[125] Personal communication with MAMPU in January 2021
[126] Martin (2014)
[127] World Bank (2020)
[128] Verhulst et al. (2020)
[129] World Bank (2017a)
[130] Dawes (1996)
[131] Personal communication with MOSP in October 2020
[132] Gasser (2015)

making international calls[133]. Interoperability requires hardware and systems that are connected and data that can understand each other. It is not enough for interconnected systems to pass bits from one system to another if the data cannot 'talk' to each other[134]. In 2003, MAMPU produced the Malaysian Government Interoperability Framework (MyGIF), which was then supplemented by the Malaysian Government Interoperability Framework for Open Source Software (MyGIFOSS) released in 2006. Moving forward, the government should consider whether the framework requires revision or update and devise a strategy to ensure the implementation of the framework by all agencies.

To rapidly expand open government data, innovations to make the process of publishing data easy for public servants should be developed. This includes **automating** the process of inventorying, annotating and classifying data[135]. The government should also think of ways to integrate data sourced from traditional means such as surveys and census with **data sourced from 'non-traditional' ways** such as satellite and environmental sensors data. This could allow for greater refinement in policies as well as quick estimates for time-sensitive interventions[136]. However, apart from technical considerations, this sort of integration also requires ethical considerations.

With regard to infrastructure for open government data, some areas that the government could look into further include **procurement policies** to ensure future purchases of information technology (IT) systems support open data and a **strategy to transition all IT systems** in all agencies to comply with open data standards[137].

Monitoring, evaluation and review

Any policy relies on proper monitoring, evaluation and review to achieve its goals. As pointed out, currently there is no mechanism to evaluate the implementation of open government data by agencies. There is a risk of "open washing", a scenario whereby governments only publish data that is easy and uncontroversial simply to appear to be implementing open government data[138]. Therefore, to ensure an open government data policy achieves its intended goals, **assessment metrics**[139] should include not only quantitative aspects such as the number of datasets published, but also qualitative elements[140] such as engagement with external stakeholders, human capital development, documentation of decision provenance, and data privacy and security protection.

In the spirit of transparency that open government data represents, **annual reports on the progress** made by each agency against the previous year's commitments and priorities and goals for the upcoming year should be made publicly available for the legislature and the public to

[133] Gasser (2015)
[134] Gasser (2015)
[135] Janssen, Charalabidis, and Zuiderwijk (2012); Noveck (2017)
[136] World Bank (2020)
[137] Inspired by Government of Ontario (2015)
[138] Mansell (2020; Noveck (2017)
[139] Government of Ontario (2015)
[140] World Bank (2017a)

review[141]. As Helen Margetts from the Oxford Internet Institute puts, to "turn open data into better government", "we need more data about open data"[142].

5.3. Data privacy and security protection

The right to privacy is protected under Article 12 of the Universal Declaration of Human Rights[143] and Article 17 of the International Covenant on Civil and Political Rights[144]. They state that

> *No one shall be subjected to **arbitrary interference with his privacy**, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

Open government data requires balancing the right to information and the right to privacy. Together with the two fundamental rights that need to be balanced, the agenda seeks to improve the well-being of the people through the use of data. Therefore, two moral duties need to be reconciled: fostering human rights and improving human welfare[145].

The potential harms due to the loss of privacy are wide-ranging including psychological harm, loss of insurability, loss of employability, market discrimination and political discrimination[146]. The loss of privacy may also weaken public trust in government data handling. They might be less inclined to contact government agencies if they are not confident that their data will remain confidential[147] or if they worry that their data will be misused by the government itself[148]. For example in the US, a survey by the National Domestic Violence Hotline found that of women who had experienced domestic violence, 60% did not report it due to privacy concerns[149].

Privacy is not merely about the presence of specific types of information in a dataset as harm can also be inflicted by the information that can be inferred from a dataset or when the dataset is linked to other datasets[150]. For example, privacy can be compromised if an individual is known to be a member of a subsample and all members of the subsample share the same characteristic[151]. Advances in AI make data privacy protection even more challenging[152].

---

[141] Inspired by Government of Ontario (2015)
[142] Margetts (2013)
[143] UN (1948)
[144] OHCHR (1976)
[145] Floridi (2014)
[146] Altman et al. (2015)
[147] Borgesius, Gray, and van Eechoud (2015)
[148] World Bank (2020)
[149] Green et al. (2017)
[150] Wood, O'Brien, and Gasser (2016)
[151] Altman et al. (2015)
[152] World Bank (2020)

Balancing the utility and privacy of open government data is not straightforward as releasing data inevitably carries data utility as well as privacy risks[153]. While many stakeholders in developing countries cite privacy considerations as the obstacle to open government data, these countries do not have strong privacy laws and frameworks, to begin with[154]. Two scenarios can be hypothesised from this condition: opening up government data without strong privacy laws and frameworks may cause harm that potentially results in a pushback on and a reversal of the open government data agenda, or privacy concerns would continue being an excuse for governments not to disclose data against the backdrop of weak privacy laws and frameworks. The solution to both these scenarios is to strengthen privacy laws and frameworks.

It is worth discussing data security briefly. Data security refers to the state of data that is safe from the threat of unauthorized action that may result in, for example, data privacy breaches, data tampering and data loss. Protecting data security is commonly included in privacy laws but the scope is limited to *personal* data. However, in many countries, there are laws on cybercrime. In Malaysia, it is the Computer Crimes Act 1997. It is worth noting that Malaysia is not a signatory of the Budapest Convention on Cybercrime, which is the only binding international instrument that provides guidelines for comprehensive national legislation on cybercrime and serves as a framework for international cooperation. It deals with various categories of cybercrime including computer-related fraud and violations of network security[155]. It was initiated by the Council of Europe but several non-European countries have ratified it including the US, Australia, Canada, the Philippines, and Sri Lanka.

Another equally important subject is security data, whether concerning military security, environmental security, economic security, civilian security etc. Although this subject is not discussed much in this paper, the way to think about this type of data is similar to how we should treat data privacy. Essentially, governments have to weigh the risks versus the public interests of disclosing certain data about security.

Data privacy and security law

Apart from the Personal Data Protection Act that currently does not cover data collected by the government, Malaysia does not have other data privacy laws. On the contrary, several countries around the world have a privacy law that extends to government data. The South African Protection of Personal Information Act 2000, the Indian Personal Data Protection Bill 2019, and the New Zealand's Privacy Act 2020 (replacing Privacy Act 1993) are some of the data privacy laws that apply to both governments and businesses. Some laws specifically protect the privacy of data held by government agencies such as the Canadian Privacy Act 1985.

It is time for Malaysia to consider a **data privacy law that covers government data**. Protecting privacy does not work against open government data but *for* open government data. Quoting the preamble of the South African Protection of Personal Information Act 2000,

[153] Green et al. (2017)
[154] Davies (2014)
[155] Council of Europe (n.d.)

> *… **the need for economic and social progress**, within the framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information*

Data privacy and security framework

Beyond having privacy laws, government agencies need a comprehensive framework for assessing and mitigating data privacy and security risks. Some considerations in thinking about the framework are discussed in the following[156].

First, shift from output assessment (e.g. "is the data safe?") **to process-oriented standards** (e.g. "have we assessed and acted upon risks at every stage of the data lifecycle?")[157]. The process-oriented framework calls for systematic evaluation of risks and mitigation measures that could be employed at every stage of the data lifecycle. For the purpose of an assessment framework, we can consider five stages of the data lifecycle[158]:

1. Collection: ingestion, acquisition, receipt or acceptance; includes the context of collection
2. Transformation: processing of the data prior to non-transient storage; includes structural transformations such as encryption and semantic transformations such as data reduction
3. Retention: non-transient storage by an entity; includes storage by a third party acting under the direction of the entity
4. Access/Release: access to data by a party not acting under the direction of the entity; includes access to transformation, subsets, aggregates and derivatives such as model results and visualizations
5. Post-release: Availability and operations on data (and subsets, etc.) that have been passed to third parties; includes any subsequent downstream access

At the collection stage, government agencies need to ask whether a particular piece of information needs to be collected in the first place. Even if the piece of information would never be made public, there is a privacy concern about government holding that information and potentially misusing it[159]. Some mechanisms for privacy protection in data collection are governments limiting the use of a particular data for a narrowly-defined specific purpose or setting up an independent privacy oversight board[160].

At the transformation and retention stages, standard protocols of private- and public-key encryption may prevent unauthorised actions. In addition, at the retention stage, other mitigation measures could include statutory breach reporting requirements and centralised databases that

---

[156] Considerations suggested here covers a wider base of privacy and security protection than the guidelines in the Personal Data Protection Standard prepared by the Personal Data Protection Commissioner Malaysia. This is mainly, but not entirely, because the Personal Data Protection Act pertains to commercial transactions data, not government data.

[157] Green et al. (2017)

[158] Following Altman et al. (2015)

[159] Green et al. (2017)

[160] Altman et al. (2015)

enable controlled queries across databases maintained by different agencies[161]. When necessary, retire data stored internally and remove data shared online when large privacy risks surface[162].

At the data release stage, some available technical tools are presented in Table 3. However, decisions on which tools should be used should consider privacy risks and data utility. To reiterate, data privacy protection should not disproportionately diminish the potential value from the use of the data.

Table 3: Technical tools to protect privacy at the release stage

Method	Description	Privacy impact	Utility impact
Removing fields	Deleting fields that contain sensitive information	Effectively removes the risks presented by those fields	Nullifies any utility made possible by the fields being removed
Aggregating data	Summarising data across the population and releasing those statistics	Effectively protects privacy as no raw data entries are released	It has severe negative impacts on utility as it does not allow for insights beyond the statistics presented
Generalising data	Reducing the precision of fields to make each entry less unique (e.g. district instead of sub-district)	The more that data is generalised, the more difficult it is to re-identify someone	Lower levels of generalisation provide more useful information than higher levels
k-anonymity	Generalising fields such that at least k individuals exhibit the same feature within those fields	The improvement in privacy protection increases as the level of generalisation (i.e. the value of k) increases	The negative impact on utility increases as the level of generalisation (i.e. the value of k) increases
Creating anonymous identifiers	Replacing attributes with randomly generated codes that have no underlying connection to the attributes	Creating anonymous IDs can help protect privacy but does not protect against re-identifications or inferences based on patterns of behaviour	It has minimal impacts on utility

Source: Green et al. (2017)

At the post-release stage, one mechanism of privacy protection is criminalising re-identification such as in the Indian Personal Data Protection Bill 2019 (that covers data held by government agencies). The law states that

> *(1) Any person who, knowingly or intentionally—*
>
> *(a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or*
>
> *(b) re-identifies and processes such personal data as mentioned in clause (a),*

[161] Altman et al. (2015)
[162] Green et al. (2017)

> *without the consent of such data fiduciary or data processor, then, such person shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both.*

Data use agreements can also include obligations to secure the data and liability for harm arising from the misuse of data[163]. Aside from protecting privacy, data use agreements can also mitigate the concerns of government agencies regarding the misrepresentation of their data[164]. For example, the UK Open Government License v1.0 requires users not to "mislead others or misrepresent the information or its sources"[165] and the French Open License states that "the reuse must not mislead third parties as to the contents of the information, its source and its date of last update"[166].

At every stage of the data lifecycle, it is vital to establish and maintain data inventory. Without full knowledge of what datasets exist at every stage of the lifecycle, it is unlikely that adequate data protection measures can be implemented[167].

Second, consider diverse and proportionate measures in deciding the most suitable measure to protect data privacy based on the characteristics and context of the data. This can be done by assessing three aspects: the range of threats to privacy; the vulnerabilities that exacerbate those threats; and the likelihood of disclosure of personal data given those threats and vulnerabilities[168]. The goal is to release as much data as possible without compromising privacy.

Privacy threats can be broadly categorised into three: deliberate acts, environmental threats such as natural disaster, and accidental threats such as accidentally granting access to a non-authorised person. Privacy vulnerabilities are factors that increase the likelihood of the threats to be realised including the characteristics of the data, the systems, and the related context[169]. While all data carries privacy threats and vulnerabilities, the likelihood of personal data disclosure might not necessarily be large.

Imposing restrictions on data access may be better than not disclosing the data at all when the restrictions can adequately address privacy risks[170]. For example, the US has a three-tier scheme for data access: public, restricted public, and non-public[171]. Public data is accessible to anyone without restriction. Restricted public data is only accessible by select researchers under certain

---

[163] Altman et al. (2015)
[164] Dulong de Rosnay and Janssen (2014)
[165] The National Archives (n.d.)
[166] Etalab (n.d.)
[167] Green et al. (2017)
[168] Modified from Altman et al. (2015). Altman et al. includes a fourth aspect, which is the likelihood, extent, and severity of harms inflicted as the result of personal data disclosure. However, in my opinion, the goal of privacy protection is to protect privacy. Whether harms would be inflicted and how severe would they be as the result of the loss of privacy are out of the question.
[169] Altman et al. (2015)
[170] Borgesius, Gray, and van Eechoud (2015)
[171] Altman et al. (2015)

conditions because the data contains sufficient granularity or linkages that make it possible to reidentify individuals. Non-public level data is only accessible within the government.

Third, implement documentation standards of privacy protection practices. The documentation should address privacy handling of datasets with common features as well as datasets with uncommon features[172]. This documentation should be publicly accessible when requested, to allow public and legislative scrutiny on privacy decisions. The government should also have internal periodic legal and technical review of privacy practices[173] as well as by third-party auditors[174] to ensure that those practices are adequate given that technologies and types of data continue to evolve.

5.4. Inclusive and meaningful use of government data

In promoting open government data, we should be careful not to project the techno-utopian ideal that suggests that given enough data, all problems are solvable[175]. The real value of data is derived from its use. Therefore, supporting the use of open government data is as important as publishing data[176]. On top of that, a digital initiative enabling open access does not necessarily produce equitable outcomes.

Inclusive data collection

Although discussions on open government data are often framed in the context of providing access to data, it is necessary to also pay attention to the data collection process to ensure the agenda results in equitable outcomes. If data about social and economically disadvantaged groups are either not collected, incomplete, inconsistent or unreliable, open government data may have little benefit to these groups. In fact, the agenda may be detrimental to them. While the subject of 'digital inequality' has shifted from merely digital access to meaningful use, both angles, broadly speaking, are based on active interaction with digital technology. Another angle that we should consider is passive interaction, in particular, passive data contributions. Because the data of digitally disenfranchised groups is not captured, they are considered 'digitally invisible'[177].

From a geographical perspective, there is evidence that shows places that are invisible in digital representations are also invisible in practice to many people[178]. In the context of open

---

[172] Borgesius, Gray, and van Eechoud (2015)
[173] Green et al. (2017)
[174] Altman et al. (2015)
[175] Noveck (2017)
[176] Janssen, Charalabidis, and Zuiderwijk (2012)
[177] This term was introduced by Longo et al. (2017) to the best of my knowledge. However, Longo et al. conceptualise "digitally invisible" groups as those who do not leave digital traces from the use of digital devices such as mobile phone and transaction cards. I extend the definition of the term to generally include groups who have limited digital data representing them regardless of how the data is collected. This include the type of data that is typically collected through traditional means such as surveys but if the data does not capture certain groups, and subsequently their data is not visible online, they can also be considered "digitally invisible".
[178] Graham and De Sabbata (2020)

government data, we cannot improve the well-being or consider the issues of a group of people if their data simply do not exist. Effectively, these people are invisible. Therefore, the first step to ensure that open government data results in equity is to ensure **inclusive data collection**.

Equal use of data

To be able to use open government data meaningfully, one needs the ability to collect, treat, analyse and communicate data[179]. It might even be necessary to belong to a certain circle to know the availability of particular government data[180], especially if data published is not easily findable. As a result, open government data mostly attracts certain professionals such as lawyers, researchers, journalists, civic technologists, consultants, and executives in corporations. While some of these actors play pivotal roles in transforming data to generate public value, it is still necessary to increase the diversity of users of open government data to generate more inclusive public value[181].

Besides, from the perspective of the right to information, the unequal use of open government data may limit the dissemination of information to and about certain segments of society, leaving them uninformed about matters impacting them. For example, if most open government data users—especially data intermediaries who transform data into digestible information—live in urban areas and are largely concerned about urban matters, those who live in rural areas may have limited information about issues that are relevant to them.

The government could leverage the **Government Data Consultative Council** proposed in Section 5.2 to foster inclusivity in the open government data agenda by ensuring that permanent members of the council represent various segments of society including the indigenous people of Peninsular Malaysia and Sabah and Sarawak, people with disability, women, agricultural smallholders, and civil society organisations working with the underprivileged such as poor communities, migrant workers, and homeless people. Ideally, these representatives should advocate not only for the availability of data about groups they represent but also recommend policy to encourage the use of data by these groups or people who advocate for these groups. They could also bring to attention privacy issues impacting their community.

The government should develop educational programmes to increase data literacy targeting public servants, researchers, and civil society organisations. Aside from these targeted groups, the government should also consider integrating data literacy in the school curriculum[182]. With the growing demand for data skills, investment in data education is consonant with efforts to prepare our workforce for high-skill jobs.

[179] Wessels et al. (2017)
[180] Barrantes and Matos (2020)
[181] Verhulst et al. (2020)
[182] Drawing insights from financial literacy education, integrating financial literacy in school's syllabus has a more effective impact than targeted adult education. Source: World Bank (2020)

Public versus private value

While open government data reduces information asymmetries[183], it may lead to or reinforce asymmetries in power and opportunity[184] with privileged groups exploiting data for private value. We need to recognise that some proponents of open government data support the agenda because they see it as part of the deregulation agenda[185]. For example, the UK financial sector lobbyists use the open government data agenda to push for the release of vast amounts of weather data to grow the UK's weather derivatives market[186]. In the US, the bulk of FOI requests are from corporations who use data for their business interests instead of journalists or civil society organisations[187].

Beyond unequal use of government data to generate private value as opposed to public value, some use of government data by private companies has detrimental impacts to general public. In 2008, the UK's National Health Service decided to restrict access to data requested by the pharmaceutical industry due to concerns around "the potential for misinterpretation, misuse, and the identification of individual patients or prescribers". The pharmaceutical industry successfully lobbied for the reversal of the decision despite public concerns about their data being used to target, market and promote pharmaceutical drugs[188].

The role of policymakers is to devise a policy that strikes a balance between public value and private value generated through open government data. The goals of open government data policy have to be clearly stated with great emphasis on inclusiveness and public value. These goals should drive all decisions on the agenda. Among others, it requires policymakers to rethink copyright and intellectual property rights[189]. For example, the government could consider **waiving claims to intellectual property** for any product that is anchored by government data and ensure that government data is not transferred as intellectual property to a third party[190].

Data platform design

Another aspect that deserves considerable attention is the **design of data portals**. A user-friendly data portal has been identified as a factor that increases data use[191]. Besides, to ensure greater accessibility of government data for different audiences, the government should consider including data visualisation and analytics tools in data portals[192]. Information from raw data may not be accessible to people who are not familiar with handling data. Instead, data visualisations are more easily digestible. The government could also consider developing a lighter version of

[183] Ashraf (2020b)
[184] World Bank (2020)
[185] Bates (2014a)
[186] Bates (2014b; 2014a)
[187] Noveck (2017)
[188] Martin (2014)
[189] Seward (2020)
[190] Government of Ontario (2015). Further deliberation on this is, of course, needed.
[191] Wessels et al. (2017)
[192] Verhulst and Young (2016)

the data portal that may be appropriate for use in low-bandwidth areas[193] as well as a mobile-friendly version, especially for crucial data such as Covid-19 data.

Meaningful impact of open government data

If the public at large and even the public servants see no real value from open government data, they likely see no reason to support it. Over time, the promise of open government data would become less convincing. The government as well as other advocates of open government data should identify opportunities to **demonstrate its value**. For example, in the US, opening the entire corpus of data about food-borne illnesses allowed Chicago's Department of Innovation and Technology to build an algorithm that helped Chicago's Department of Public Health allocate its scarce resources for food safety violation's inspections[194]. This is an example of how open government data fosters inter-agency collaboration and realises value for public servants.

The government should integrate the open government data initiative with **other government initiatives** to secure its relevancy. For example, recently, the Ministry of Science, Technology and Innovation (MOSTI) launched the Malaysia Grand Challenge (MCG) that supports quality and high-impact research in ten priority areas including energy, education, smart cities and transportation, and environment and biodiversity[195]. Open government data could be one of the core components to support this initiative. In addition, each government agency could identify and support **niche areas** where open government data could be used to create innovations that are in line with the respective agency's strategic priorities.

The government should nurture and foster collaboration with **data intermediaries** among non-profits (e.g. researchers, civil society organisations etc.) who analyse or transform government data into digestible information for public dissemination or use the data for specific projects. This could empower non-profits to generate public value from government data, enhance the matching of the supply and demand of data[196], and create meaningful impact from the open government data agenda.

Feedback mechanism

As open government data is about collaboration, the agenda does not end with the government sharing information. The government needs to actively solicit **feedback**[197] not only with regard to the open government data policy but also other policy areas that the public advocate based on the data made publicly available. The discussion on the latter, however, is outside the scope of this paper.

One of the initiatives that the government could explore is to conduct **surveys** on the open government data initiatives to gather general snapshots of users' experience. Nevertheless, surveys tend to lack details and context. Therefore, the government should also conduct more

[193] Bezuidenhout et al. (2017)
[194] Spector (2016)
[195] MOSTI (2021b)
[196] Verhulst and Young (2016)
[197] Janssen, Charalabidis, and Zuiderwijk (2012)

deliberative methods to collect feedback[198] such as through the Government Data Consultative Council, focus group discussions, and public dialogues. Each government agency should also invite feedback on their respective initiative, particularly on their data portals.

6. Conclusion

The largest impediment to open government data in Malaysia is the lack of clarity in the legal framework concerning government data. Without legal clarity, public servants tend to err on the side of caution and choose not to disclose data. It is timely for Malaysia to enact an RTI law to promote transparency and collaboration. The law should be designed for a digital age and consistent with the open government data agenda, particularly by encouraging proactive disclosure of information.

Aside from the RTI law, Malaysia should also formulate privacy laws that extend to government data. With the proliferation of data collected by the government, especially with the Covid-19 pandemic, a privacy law strengthens public trust. Having such laws in place would compel government agencies to take data privacy and security protection more seriously. Beyond having laws, a comprehensive framework for assessing and mitigating data privacy and security risks need to be developed, taking into account risks at every stage of data lifecycle and proportionate measures to address those risks.

Apart from the legal framework, Malaysia should streamline the government data management system. Although MAMPU has been the lead agency in the open government data agenda, it has minimal power to direct and enforce the open government data agenda in all government agencies. Implementing open government data involves mobilising digital infrastructure and human resources that in most governments are already scarce. Therefore, the government should also increase investment in digital infrastructure and human capital across all agencies.

To encourage meaningful use of open government data, the government needs to expand data skills training and embed data literacy in school education. To increase the accessibility of government data, the design of data portals merits attention. The government should also engage with data intermediaries to translate open government data into meaningful impact in real life.

The advancement of digital technology brings forth a great volume and a wide range of data. Malaysia should accelerate the expansion of open government data to generate maximum possible value from government data, especially since this data is collected and managed using public funds. However, while we strive to realise the promise of good governance and improved well-being from open government data, we also have to look out for its potential threats. Therefore, strong and comprehensive government data policy is needed. The governance of open government data also has to be agile taking into considerations fast-evolving technological developments as well as how society interacts with technology.

[198] Young et al. (2020)

7. References

African Commission on Human and Peoples' Rights. 2002. "Declaration of Principles on Freedom of Expression in Africa." Declaration on Principles on Freedom of Expression in Africa. October 2002. http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html.

Altman, Micah, Alexandra Wood, David R O'Brien, Salil Vadhan, and Urs Gasser. 2015. "Towards a Modern Approach to Privacy-Aware Government Data Releases." *Berkeley Technology Law Journal* 30 (3): 1967–2072.

ANM. 2016a. "Panduan Pengurusan Rekod Sektor Awam." National Archives of Malaysia.

———. 2016b. "Pelan Strategik Arkib Negara Malaysia 2016-2020." National Archives of Malaysia. http://www.arkib.gov.my/web/guest/pelan-strategik-arkib-negara-malaysia-2016-2020.

Article 19. 2018. "Right to Know Day 2018: Progress on Information Access around the World." ARTICLE 19. September 27, 2018. https://www.article19.org/resources/right-to-know-day-2018-progress-on-information-access-around-the-world/.

Ashraf, Shaharudin. 2020a. "Covid-19: With Data, We Can Respond Better." http://www.krinstitute.org/Views-@-Covid-19-;_With_Data,_We_Can_Respond_Better.aspx.

———. 2020b. "Open Government Data: Principles, Benefits and Evaluations." Discussion Paper. Kuala Lumpur: Khazanah Research Institute. http://www.krinstitute.org/Discussion_Papers-@-Open_Government_Data-;_Principles,_Benefits_and_Evaluations.aspx.

———. 2020c. "Accelerating Malaysia's Open Government Data with COVID-19." University. *LSE Southeast Asia Blog* (blog). November 23, 2020. https://blogs.lse.ac.uk/seac/2020/11/23/accelerating-malaysias-open-government-data-with-covid-19/.

———. 2020d. "Open Government Data for Academic Research." Working Paper. Kuala Lumpur: Khazanah Research Institute. http://www.krinstitute.org/Working_Paper-@-Open_Government_Data_for_Academic_Research.aspx.

Barrantes, Roxana, and Paulo Matos. 2020. "Who Benefits from Open Models? The Role of ICT Access." In *Making Open Development Inclusive: Lessons from IDRC Research*, 219. MIT Press.

Barry, Emily, and Frank Bannister. 2014. "Barriers to Open Data Release: A View from the Top." *Information Polity* 19 (1,2): 129–52. https://doi.org/10.3233/IP-140327.

Bates, Jo. 2014a. "The Strategic Importance of Information Policy for the Contemporary Neoliberal State: The Case of Open Government Data in the United Kingdom." *Government Information Quarterly* 31 (3): 388–95. https://doi.org/10.1016/j.giq.2014.02.009.

———. 2014b. "The Progressive Ideals behind Open Government Data Are Being Used to Further Interests of the Neoliberal State." *Impact of Social Sciences - LSE* (blog). October 2, 2014. https://blogs.lse.ac.uk/impactofsocialsciences/2014/10/02/open-government-data-and-the-neoliberal-state/.

Bezuidenhout, Louise M., Sabina Leonelli, Ann H. Kelly, and Brian Rappert. 2017. "Beyond the Digital Divide: Towards a Situated Approach to Open Data." *Science and Public Policy* 44 (4): 464–75. https://doi.org/10.1093/scipol/scw036.

Borgesius, Frederik Zuiderveen, Jonathan Gray, and Mireille van Eechoud. 2015. "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework." *Berkeley Technology Law Journal* 30 (3): 2073–2131.

Botterman, Maarten, Tora Bikson, Sandy Bosman, Jonathan Cave, Erik Frinking, and Victor de Pous. 2000. "Public Information Provision in the Digital Age." RAND Europe.

Cambridge English Dictionary. n.d. "Latent Demand - Cambridge English Dictionary." n.d. https://dictionary.cambridge.org/dictionary/english/latent-demand.

Council of Europe. n.d. "Budapest Convention and Related Standards." Council of Europe - Cybercrime. n.d. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Coursera. 2020. "Coursera Global Skills Index 2020." Coursera. https://www.coursera.org/gsi.

Davies, Tim. 2014. "Open Data in Developing Countries: Emerging Insights from Phase 1." World Wide Web Foundation & ODDC.

Dawes, Sharon S. 1996. "Interagency Information Sharing: Expected Benefits, Manageable Risks." *Journal of Policy Analysis and Management* 15 (3): 377–94.

DOSM. 2015. "Department of Statistics Malaysia Transformation Plan 2015-2020." https://www.dosm.gov.my/v1/index.php?r=column/cone&menu_id=bWVOVWFVZDd4VlZqSS9lNVBaTkVzUT09.

Dulong de Rosnay, Melanie, and Katleen Janssen. 2014. "Legal and Institutional Challenges for Opening Data across Public Sectors: Towards Common Policy Solutions." *Journal of Theoretical and Applied Electronic Commerce Research* 9 (3): 1–14.

EPU. 2015. "Eleventh Malaysia Plan 2016-2020." Economic Planning Unit.

———. 2021. "Malaysia Digital Economy Blueprint." Policy Paper. Putrajaya: Economic Planning Unit, Prime Minister's Department. https://www.epu.gov.my/sites/default/files/2021-02/Malaysia-digital-economy-blueprint.pdf.

Etalab. n.d. "Licence Ouverte / Open Licence." Etalab's blog. n.d. https://www.etalab.gouv.fr/licence-ouverte-open-licence.

Floridi, Luciano. 2014. "Open Data, Data Protection, and Group Privacy." *Philosophy & Technology* 27 (1): 1–3. https://doi.org/10.1007/s13347-014-0157-8.

Gasser, Urs. 2015. "Interoperability in the Digital Ecosystem." *The Berkman Center for Internet & Society at Harvard University*, Research Publication, , no. 2015–13. https://dx.doi.org/10.2139/ssrn.2639210.

Global RTI Rating. n.d. "By Country: RTI Rating." Global Right to Information Rating. n.d. https://www.rti-rating.org/country-data/.

Government of Malaysia. 2018. "Companies Commission of Malaysia Act 2001 (Act 614)." https://www.ssm.com.my/Pages/Legal_Framework/Document/CCMA%20Act%20614_as%20at%201%20March%202018).pdf.

Government of Ontario. 2015. "Open by Default – A New Way Forward for Ontario." Government of Ontario. December 25, 2015. https://www.ontario.ca/page/open-default-new-way-forward-ontario#section-1.

Graham, Mark, and Stefano De Sabbata. 2020. "The Geographic Contours of Openness." In *Making Open Development Inclusive: Lessons from IDRC Research*. MIT Press.

Green, Ben Z., Gabe Cunningham, Ariel Ekblaw, Paul M. Kominers, Andrew Linzer, and Susan Patricia Crawford. 2017. "Open Data Privacy." *Berkman Klein Center for Internet & Society Research Publication*. https://dash.harvard.edu/handle/1/30340010.

Janssen, Marijn, Yannis Charalabidis, and Anneke Zuiderwijk. 2012. "Benefits, Adoption Barriers and Myths of Open Data and Open Government." *Information Systems Management* 29 (4): 258–68. https://doi.org/10.1080/10580530.2012.716740.

JPA, and INTAN. 2016. "Pembangunan Modal Insan Dalam Menyokong Era Kerajaan Digital."

Kannan, Hashini Kavishtri, and Veena Babulal. 2019. "Govt to Draft Freedom of Information Act to Replace Official Secrets Act." *NST Online*, July 18, 2019. https://www.nst.com.my/news/nation/2019/07/505404/govt-draft-freedom-information-act-replace-official-secrets-act.

Keng, Kuek Ser Kuang. 2018. "Open Data Should Be Part of Harapan's Freedom of Information Reform." *Malaysiakini*, August 29, 2018. https://www.malaysiakini.com/news/440851.

KKMM. 2018. "Communications & Multimedia Blueprint 2018 - 2025 - Digitise and Humanise." Ministry of Communications and Multimedia. https://www.kkmm.gov.my/images/171211_kkmm_blueprint2018_2025.pdf.

Longo, Justin, Evan Kuras, Holly Smith, David M. Hondula, and Erik Johnston. 2017. "Technology Use, Exposure to Natural Hazards, and Being Digitally Invisible: Implications for Policy Analytics." *Policy & Internet* 9 (1): 76–108. https://doi.org/10.1002/poi3.144.

MAMPU. 2016. "Pelan Strategik ICT Sektor Awam 2016-2020." MAMPU. https://www.mampu.gov.my/ms/penerbitan-mampu/send/2-buku/680-pelan-strategik-ict-sektor-awam-2016-2020-versi-bm-2.

———. n.d. "MyGOV - Open Government Data - Policy, Strategy and Governance - Open Data." The Malaysian Administrative Modernisation and Management Planning Unit. n.d. https://www.malaysia.gov.my/portal/content/30024.

Mansell, Robin. 2020. *Making Open Development Inclusive: Lessons from IDRC Research*. MIT Press.

Margetts, Helen. 2013. "How to Turn Open Data into Better Government." Media. The Guardian. October 22, 2013. http://www.theguardian.com/public-leaders-network/2013/oct/22/open-data-better-government.

Martin, Chris. 2014. "Barriers to the Open Government Data Agenda: Taking a Multi-Level Perspective." *Policy & Internet* 6 (3): 217–40. https://doi.org/10.1002/1944-2866.POI367.

Meijer, Ronald, Peter Conradie, and Sunil Choenni. 2014. "Reconciling Contradictions of Open Data Regarding Transparency, Privacy, Security and Trust." *Journal of Theoretical and Applied Electronic Commerce Research* 9 (3): 32–44.

MOSP. 2020. “What Is Malaysia Open Science Platform? – Malaysia Open Science Platform (MOSP).” Malaysia Open Science Platform. 2020. https://www.akademisains.gov.my/mosp/about/what-is-malaysia-open-science-platform/.

MOSTI. 2021a. “Dasar Sains, Teknologi dan Inovasi Negara 2021-2030.” Ministry of Science, Technology and Innovation. https://www.mosti.gov.my/web/dasar-halatuju/.

———. 2021b. *08.01.2021- MOSTI LANCAR MALAYSIA GRAND CHALLENGE (MGC) SEBAGAI PEMANGKIN NEGARA BERTEKNOLOGI TINGGI*. Youtube Video. MOSTI. https://www.youtube.com/watch?v=IK_kvC8U3QI.

Mustapa, Mimi Nurakmal, Suraya Hamid, and Fariza Hanum Md Nasaruddin. 2019. “Exploring the Issues of Open Government Data Implementation in Malaysian Public Sectors.” *International Journal on Advanced Science, Engineering and Information Technology* 9 (4): 1466–73.

New Zealand Government. 2021. “Government Chief Data Steward.” New Zealand Digital Government. 2021. https://www.digital.govt.nz/digital-government/leadership/government-functional-leads/government-chief-data-steward-gcds/.

Noveck, Beth Simone. 2017. “Rights-Based and Tech-Driven: Open Data, Freedom of Information, and the Future of Government Transparency.” *Yale Hum. Rts. & Dev. LJ* 19: 1.

Nur Hanani, Azman. 2020. “Statistics Act 1965 to Be Amended.” *The Malaysian Reserve*, October 21, 2020, sec. News. https://themalaysianreserve.com/2020/10/21/statistics-act-1965-to-be-amended/.

OHCHR. 1976. “International Covenant on Civil and Political Rights.” United Nations Human Rights. March 23, 1976. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

Open Society. 2019. “Countries with ATI Laws.” Right2Info.Org. May 2019. https://www.right2info.org/resources/publications/countries-with-ati-laws-1/view.

Parliament of Malaysia. 2019. “Penyata Rasmi Parlimen Dewan Rakyat, Parlimen Keempat Belas, Penggal Kedua, Mesyuarat Ketiga (7 November 2019).” https://www.parlimen.gov.my/files/hindex/pdf/DR-07112019.pdf#page=13&zoom=100&search=freedom%20of%20information.

Prime Minister’s Department. 2015. “Pekeliling Am Bil. 1 Tahun 2015 - Pelaksanaan Data Terbuka Sektor Awam.” Prime Minister’s Department.

Ruijer, Erna, and Albert Meijer. 2020. “Open Government Data as an Innovation Process: Lessons from a Living Lab Experiment.” *Public Performance & Management Review* 43 (3): 613–35.

Seward, Ruhiya Kristine. 2020. “Conclusion: Understanding the Inclusive Potential of Open Development.” In *Making Open Development Inclusive: Lessons from IDRC Research*. MIT Press.

Sinar Project. n.d. “Hidden Data in Parliamentary Documents.” Page. Sinar Project. n.d. https://sinarproject.org/open-parliament/notes/hidden-data-in-parliamentary-documents.

———. n.d. “Parliamentary Answers as Source for Data Demand and Government Oversight.” News Item. Sinar Project. n.d. https://sinarproject.org/open-parliament/updates/parliamentary-answers-as-source-for-data-demand-and-government-oversight.

Spector, Julian. 2016. “Chicago Is Using Data to Predict Food Safety Violations. So Why Aren’t Other Cities?” *Bloomberg.Com*, January 7, 2016. https://www.bloomberg.com/news/articles/2016-01-07/chicago-is-using-data-to-predict-food-safety-violations-why-aren-t-other-cities.

Sudirman, Suhaiza, and Zawiyah Mohammad Yusof. 2017. “Public Sector ICT Strategic Planning: Framework of Monitoring and Evaluating Process.” *Asia-Pacific J. Inf. Technol. Multimed.* 6 (1): 85–99.

Sultan Azlan Shah. 2004. *Constitutional Monarchy, Rule of Law, and Good Governance: Selected Essays and Speeches*. Edited by Visu Sinnadurai. Kuala Lumpur, Malaysia : Petaling Jaya, Selangor Darul Ehsan, Malaysia: Professional Law Books ; Thomson Sweet & Maxwell Asia.

Supreme Court of India. 2002. Union of India v. Association for Democratic Reforms and Another. Supreme Court of India.

The National Archives. n.d. “Open Government Licence.” Open Government License for Public Sector Information. n.d. http://www.nationalarchives.gov.uk/doc/open-government-licence/version/1/.

UN. 1948. “United Nations Universal Declaration of Human Rights.” December 10, 1948. https://www.un.org/en/universal-declaration-human-rights/.

———. 2020. “Global Data Community’s Response to Covid-19 — SDG Indicators.” United Nations. https://unstats.un.org/sdgs/hlg/Global-data-communitys-response-to-COVID-19/.

Verhulst, Stefaan, and Andrew Young. 2016. “Open Data Impact: When Demand and Supply Meet.” GovLab & Omidyar Network. http://odimpact.org/key-findings.html.

Verhulst, Stefaan, Andrew Young, Andrew Zahuranec, Susan Aaronson, Ania Calderon, and Matt Gee. 2020. “The Emergence of a Third Wave of Open Data.” The GovLab. https://opendatapolicylab.org/images/odpl/third-wave-of-opendata.pdf%20.

Wessels, Bridgette, Rachel Finn, Kush Wadhwa, and Thordis Sveinsdottir. 2017. *Open Data and the Knowledge Society*. Amsterdam University Press. https://doi.org/10.5117/9789462980181.

WHO. 2020. “Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation.” September 23, 2020. https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation.

Wood, Alexandra, David O’Brien, and Urs Gasser. 2016. “Privacy and Open Data.” *Berkman Klein Center Research Publication*, no. 2016–16.

World Bank. 2017a. “Open Data Readiness Assessment: Malaysia.” 115192. The World Bank. http://documents.worldbank.org/curated/en/529011495523087262/pdf/115192-WP-PUBLIC-MALAYSIA-DEVELOPMENT-EXPERIENCE-SERIES.pdf.

———. 2017b. “Malaysia Economic Monitor: Data for Development.” 116032. The World Bank. http://documents.worldbank.org/curated/en/993771497248234713/pdf/116032-REVISED-MEM-9-June-2017-FINAL-COPY-EDITED-96pgs-13-6-17.pdf.

———. 2020. “World Development Report 2021 Concept Note - Data for Better Lives.” World Bank. http://documents1.worldbank.org/curated/en/778921588767120094/pdf/World-Development-Report-2021-Data-for-Better-Lives-Concept-Note.pdf.

Young, Andrew, Stefaan Verhulst, Nadiya Safonova, and Andrew Zahuranec. 2020. “The Data Assembly: Responsible Data Re-Use Framework.” The GovLab & Henry Luce Foundation. https://thedataassembly.org/files/nyc-data-assembly-report.pdf.