Global Data Governance Mapping Project
Year Two Report
Background and Guidelines

July, 2022

By Adam Zable, Thomas Struett, and Susan Ariel Aaronson

Year 2 Report

Global Data Governance Mapping Project

Background and Guidelines

This document is designed for two purposes: to provide additional detail on the metric attributes and indicators and to help other researchers gain clarity on how we made decisions on what data to include and/or exclude.. We include details on definitions, the rationale for attributes and indicators, and our notes on what evidence we counted and what we didn't count and why.

We built the metric on primary source evidence provided by governments online. In some cases, we also used secondary sources. We used online translation tools to help us better understand such evidence when it is not available in English or Spanish. The method we used to translate government documents is detailed at the end of this report.

Figure 1 The Six Attributes
Strategic: The government has a vision or plan for different types of data in the economy and polity.
Regulatory: The government constructs a legal regime around data's types and/or uses.
Responsible: The government thinks about the ethical, trust, and human rights implications of data use and re-use.
Structural: The government alters institutional structures in response to data-driven transformation.
Participatory: The government informs its constituents about its activities and asks for public comment, with the intention of incorporating their feedback.
International: The government joins with other first-movers in shared international efforts to establish data governance rules and norms.

Attribute 1: Strategic

Definition:

> Government officials draft and disseminate a vision or plan for data's role in the economy, polity, and society. These strategies also often delineate the responsibilities of those collecting, using, and sharing data. Strategies allow policymakers to manage complexity, take advantage of opportunities and advance actions in the face of uncertainty.[1]

Indicator 1a National Data Strategy

Definition:

> A strategy designed to increase the provision, use, and re-use of various types of data in adherence with national norms and laws. Most such plans cover data as a commercial asset, and some strategies address data as a public good. These strategies often discuss how data governance relates to emerging technologies such as AI, how data governance may build trust, and how the country can use data to prosper over time.[2]

Rationale:

> According to the OECD, governments use these national strategies to focus attention and resources at a national level, describe how societal entities can work together to benefit from data, and to put forward a vision on how to manage change as well as risks that may arise for individuals and the nation as a whole when national entities use data to innovate or to solve societal questions.[3]

Guidelines for Inclusion:

> The strategy must:

---

[1] John Bryson,, Lauren Hamilton Edwards and David M. Van Slyke. 2018. "Getting strategic about strategic planning research." *Public Management Review* 20 (3): 317–339. doi:10.1080/14719037.2017.12851

[2] Susan Ariel Aaronson "A Future Built on Data: Data Strategies, Competitive Advantage and Trust," CIGI Paper 266, June 9, https://www.cigionline.org/publications/a-future-built-on-data-data-strategies-competitive-advantage-and-trust/

[3] OECD, "Data governance: Enhancing access to and sharing of data." December 10. 2021, www.oecd.org/sti/ieconomy/enhanced-data-access.htm.

- focus on several different types of data (as opposed to strategies that focus only on one type of data, such as statistical data, as in Tanzania's National Data Roadmap for Sustainable Development, or personal data, as in Albania's Strategy for the Right to Information and Personal Data Protection 2018-2020).
- have an explicit focus on data governance, as opposed to digital infrastructure, data centers, or digitization.
- be written by national government officials, as opposed to those written by officials at the city or regional level, such as the Dubai Data Strategy.

1b Public administration data strategy

Definition:

A strategy that delineates how the government will collect, share, protect and control data funded, collected, and controlled by governmental entities.[4]

Rationale:

Governments use these strategies to build trust with their public and show they will simultaneously protect personal data as they fund, collect, and store government data.

Guidelines for Inclusion:

The strategy must be comprehensive in scope, meaning binding the national government as a whole, not exclusively related to any specific agency, sector, or data type such as open data.

1c Artificial Intelligence strategy

Definition:

AI strategies outline a national vision for how a nation can build and/or maintain its ability to create and utilize AI for commercial as well as societal use. They often provide guidance to government agencies, often discuss investments in AI research and development, and talk about the role of government in developing standards and the rule of law for this emerging technology. [5]

[4] See as example US Federal Data Strategy, Action Plan 2021, October 2021, https://www.ai.gov/strategy-documents/#US_NATIONAL_AI_STRATEGY_DOCUMENTS

[5] Samar Fatima, Kevin C. Desouza, James S. Denford, Gregory S. Dawson, "What explains government's interest in artificial intelligence? A signaling theory approach," Economic Analysis and Policy, Volume 71,

Rationale:

AI can provide many benefits to society, but it also can produce considerable risks to employment, incomes, and human autonomy. AI raises human rights, equity and ethical considerations -National AI strategies delineate how nations plan to balance these benefits and risks. They also delineate how the nation plans to govern the mix of various types of data (public, personal, and proprietary data) used for AI.[6]

Guidelines for Inclusion:

Canada was the first country to produce an AI strategy in 2017 and it serves as a good example. [7]

1d Strategy For Data in Emerging Digital Ecosystems

Definition:

A strategy that outlines how a nation can utilize various data-driven technologies for economic and societal benefit. The strategy emphasizes the importance of data governance to the achievement of this goal. We also include strategies for other data-driven technologies. Often, these strategies focus on creating a digital economy or digital ecosystem rather than focusing solely on one type of data-driven sector..[8] We include a variety of plans including smart cities or territories, advanced manufacturing or 4th Industrial Revolution, and digital economy or society.

Rationale:

Policymakers use these strategies to encourage innovation and economic progress, taking advantage of new technologies to address societal challenges, and laying out a vision for how they intend to succeed in emerging digital environments going forward in the 21st century. Officials want to show how they will use, protect, and create value from data and new data-driven technologies to

2021, Pages 238-254, (https://www.sciencedirect.com/science/article/pii/S0313592621000667)

[6] OECD, Policy Note, An overview of national AI strategies and policies, 2021, https://goingdigital.oecd.org/data/notes/No14_ToolkitNote_AIStrategies.pdf

[7] https://www.investcanada.ca/programs-incentives/pan-canadian-ai-strategy

[8] Certain exceptions exist, such as France's National Strategy for the Cloud, which covers data governance more directly than the vast majority of other cloud strategies, which act more as implementation guidelines for public agencies rather than vision statements.

achieve both societal and commercial goals. They also want to reassure their citizens that they will do so without favoring one segment of society and while building trust and the rule of law to new technologies.

Guidelines for Inclusion:

The strategy must discuss the use, protection, and creation of value from data within the context of emerging digital ecosystems. Policymakers discuss the role of data as an input in such a document. .

Attribute 2: Regulatory

Definition:

The government constructs a legal and regulatory regime around various types of data. Specifically, policymakers enact rules regarding the collection, use, and reuse of data for data subjects, data controllers, and/or data users. Regimes related to data may include aws and/or executive orders, directives, decrees, regulations, administrative codes, proclamations, etc., so long as it is mandatory, binding, and enforceable.

Rationale:

Policymakers neact laws/regulations on data to provide clarity on what individuals and groups of individuals can do with various types of data. These regimes protect our general safety, and ensure our rights as citizens against abuses by other people, by organizations, and by the government itself.

Guidelines for Inclusion:

In this attribute, we include only binding acts of state, which includes laws but can also include executive orders, directives, decrees, regulations, administrative codes, proclamations, etc., so long as it is mandatory, binding, and enforceable. We are interested in comprehensive, general laws rather than sector-specific. If a law has passed but is not yet in force, we count it.

2a Law for the protection of personal data

Definition:

Laws that delineate how private and often public entities are required to treat personal information when these entities collect, store, utilize and monetize personal data.

Rationale:

There is no digital economy if individuals cannot trust that their personal data is protected by those that collect and utilize it. Firms and governments that don't protect such data can lose trust, market share and even their ability to participate in a particular market.[9] For this reason, most nations have enacted privacy and personal data protection laws.[10]

Guidelines for Inclusion:

Some countries such as Singapore that covers the government and private sector personal data protection rules.[11] But many governments have separate laws and some governments only cover the government or the private sector. We only count those governments that have established a data protection regime that covers the government as well as the private sector's use of data. Hence, we do not count China's Personal Information Protection Law[12] because it does not apply to the government. We also do not count US laws such as the United States' 1974 Privacy Act[13] because it does not apply to the private sector (it also does not operate under a modern definition of digital data).Canada's Privacy Act[14] covers the public sector only, and its private sector equivalent, the Personal Information Protection and Electronic Documents Act[15] (pending reform) only covers data collected *in the course of business transactions*. Thus, we do not count it.

Secondly, we only count laws applying to all sectors, rather than those directed at specific sectors, such as the US Health Insurance Portability and Accountability Act of 1996 (HIPAA).[16] In some cases, the nation has separate 'comprehensive'

---

[9] https://www.bloomberg.com/news/articles/2022-07-01/tiktok-says-some-china-based-employees-can-access-us-user-data

[10] UNCTAD reports that 137 or 71% of the world's 194 nations have adopted such laws. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[11] Public Sector (Governance) Act 2018 and Personal Data Protection Act (PDPA)

[12] https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/

[13] https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974,of%20records%20by%20federal%20agencies.

[14] https://laws-lois.justice.gc.ca/eng/acts/P-21/FullText.html#h-397260

[15] https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html

[16] https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge

laws for the public and private sectors; and in these cases (Singapore, for examplee count both as oaffirmatively.

2b Open data law for the proactive release of government information

Definition:

Laws that require governmental bodies to make the bulk of public sector data freely available, easy to use, distribute and reuse, subject to limited exceptions, in a proactive manner rather than at the request of citizens.

Individuals and companies can use and reuse this data. These laws include exceptions such for public policy purposes such as to protect national security or privacy.[17] Under right to information laws, citizens must request specific types of information and the government in turn reacts and responds. However, proactive disclosure laws require policymakers to release the bulk of public information without an individual or groups requesting such disclosure. These governments treat data as a public good-open, usable and reusable.[18]

Rationale:

Policymakers now understand that data funded, collected, and held by the government is a public good. When government data is made accessible and re-usable, it can enable individuals, private firms and civil society groups, as well as governments themselves to innovate and collaborate in new ways.Moreover, the OECD reports that by making their datasets available, public institutions become more transparent and accountable to citizens. Finally, by encouraging the use, reuse and free distribution of datasets, governments promote business creation and innovative, citizen-centric services.[19]

For our purposes, a law is considered to mandate open data i,[20] but not Open data puts the onus on the government to proactively and transparently release information. If a law dictates a regime wherein citizens have unrestricted *access* to government datasets, it would thus not count unless there is a mandate for the government to actively publish data, subject to certain exceptions. Although some governments find it more efficacious or cost-effective to handle open data in

[17] https://opendatatoolkit.worldbank.org/en/essentials.html; ;and
[18] https://opendatapolicyhub.sunlightfoundation.com/guidelines/01-proactive-release/; and ttps://www.oecd.org/gov/digital-government/open-government-data.htm
[19] https://www.oecd.org/gov/digital-government/open-government-data.htm
[20] Especially if the datasets identified for transparency have to do with finances, statistics, projects or budgets of public authorities. SAYS WHO?> source

policies, strategies, portals, or action plans, only regulatory action ensures accountability. Open data policies are thus not counted.
necessarily explicitly for purposes of re-use. It is the proactive publication of data held by the government for a wide variety of types of information, generally in an open/reusable format that allows for its re-use by citizens. Open data puts the onus on the government to proactively and transparently release information. If a law dictates a regime wherein citizens have unrestricted *access* to government datasets, it would thus not count unless there is a mandate for the government to actively publish data, subject to certain exceptions. Although some governments find it more efficacious or cost-effective to handle open data in policies, strategies, portals, or action plans, only regulatory action ensures accountability. Open data policies are thus not counted.

2c Freedom of Information Act

Definition:

Laws designed to ensure that upon request, citizens can access government documents.

Rationale:

Citizens have a right to request and then to access information held by their government unless it must be kept secret for reasons of public morals, public health, or national security. According to the Open Government Partnership, the right to access government-held information is a critical component of democracy and a foundational pillar of open government. Access to information inherently improves government transparency which can enable the public to participate meaningfully in official decision-making and to hold government actors accountable for their decisions. [21]

Guidelines for Inclusion:

2d Right to be protected from automated decision-making

Definition:

[21] https://www.hhs.gov/foia/index.html for the US;
https://www.opengovpartnership.org/policy-area/right-to-information/

Laws designed to provide individuals with a legal right not to be subject to a decision based solely on automated means and/or to be profiled by such systems.

Some governments provide individuals with a new right–the right **not to be subject to a decision based solely on automated means o rto be profilled by such systems. Many but not all of these laws are .** Automated decision making means a decision is solely by automated means without any human involvement). Some laws also forbid profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.[22]

Rationale:

Automated decisions are those made by algorithms, without human involvement, that affect people in the real world. Decisions made by algorithmic processes can have human rights spillover effects, for example a bank refusing a loan to a data subject based on an abstruse algorithm in a computer program. But these decisions are often carried out by proprietary algorithms that transform personal data into trade secrets of the companies who control them. Trade secrets are meant to protect business confidential, or proprietary, data, the valuable know-how and business information that is undisclosed and intended to remain confidential. Trade secrets are protected from scrutiny by trade secrets laws and international agreements, making them difficult to regulate in terms of how they are managed, as personal or public sector data can be. Rather than looking for regulations on the use of proprietary data directly, one way to assess regulatory action in this area is to look at laws on the *use* of that data via its application as automated decisions. Having a legal right to be protected from automated decision-making means that companies, authorities and other entities cannot make decisions about individuals using only technology with no human intervention. This indicator thus serves two functions: to assess indirectly the regulation of private-sector-controlled data, and as an indication that the government is thinking about the negative side effects of data-driven technological change on the polity.

Guidelines for Inclusion:

[22] For the UK, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/; and for EU, https://gdpr-info.eu/art-22-gdpr/

For our purposes, not only do laws which grant citizens a measure of legal protection against fully automated decision making (such as in China) count, but also laws which grant citizens a measure of legal protection against any kind of decisions, which are the result of fully automated *processing* of personal data. It can take the form of a right to object, complain, be informed, or merely to be 'safeguarded', from such decisions (for the latter see Ukraine's Law on Protection of Personal Data).

2e Right to data portability

Definition:

Some laws provide individuals with the legal right to receive one's personal data from a data controller and have it transferred to other controllers in a structured, machine-readable format.

Rationale:

Data portability is an important signal that the government recognizes the value of greater access rights to data, and has taken steps to legislate in light of that recognition.

Guidelines for Inclusion:

Attribute 3: Responsible

Definition:

The government issues frameworks and guidance that delineate both the government's responsibility to act and how other societal actors should act in regards to the ethical, trust, and human rights implications of data use and re-use.

Rationale:

In order to govern data comprehensively and democratically, governments should think deeply about the spillover effects of data-driven change and the implications of such change, in terms of trust, equity, and human rights, on the polity. In so doing, the state acknowledges its responsibilities towards its citizens.

Guidelines for Inclusion:

3a Digital charter[23]

[23] https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights/

Definition:

A grant of authority or rights from the government that delineates a set of principles designed to build trust and signal users that their human rights will be protected as they go online.

Rationale:

It is a signal to citizens that the government is thinking about how emerging technologies may affect human rights and trust and what the state owes to its citizens when it comes to data governance. It emphasizes the rights of the citizen when it comes to control, trust, and transparency.

Guidelines for Inclusion:

Can be expressed as a bill, charter, or policy paper on digital rights of the citizens vis-a-vis the state; a set of principles or a mechanism for accountability for the same. Keywords may include responsible and ethical data use, citizen-centricity, and increasing control, trust, and transparency.

3b Public sector data ethics framework

Definition:

Framework or guidelines for public servants to deal with data ethically and responsibly in the course of their work.

Rationale:

Policymakers issue such frameworks in the hopes that such guidance will improve decision-making and increase trust. For our purposes it is an indicator that the government is taking seriously the need to establish accountable processes for the management of data.

Guidelines for Inclusion:

Guidance must include overarching principles and also specific ways to apply these principles in routine work. Keywords may include equity, diversity of perspectives, and/or bias and risk considerations.

3c Responsible AI Initiatives

Definition:

A set of principles and/or a framework issued by a government body that outlines how officials can promote and utilize artificial intelligence in an ethical, accountable, and human rights respecting manner. Also includes algorithmic

accountability policy initiatives, including a broad array of frameworks, principles, laws, and reports.

Rationale:

Maintaining a human-centric framework is crucial for the effective and safe utilization of artificial intelligence and other advanced algorithms. To prepare society for the introduction of AI, many countries have started publishing frameworks or guidelines for principles-based design, development, deployment, and operation of AI by stakeholders throughout society in both the public and private sectors. A number of nations have also begun trying to tackle the problem of a lack of oversight over these systems, by introducing principles, handbooks, and publishing other documents that act to add a level of accountability to the use of algorithmic systems.

Guidelines for Inclusion:

The document must:

- Be issued by the national government as opposed to regional
- Be towards society as a whole rather than specific sectors, as in the case of, for example, Spain's Requirements for Audits of Treatments that include AI
- Include something tangible on which the government intends to act; examples include Sweden's trust model for AI, Brazil's AI procurement guidelines and pilots, the Netherlands' audit framework, and Canada's Directive on Automated Decision Making which requires ministers using automated decision systems to perform an algorithmic impact assessment. This is as opposed to, for example, the Nigerian Communications Commission's Ethical and Societal Impact of Artificial Intelligence, which describes the current state of affairs and gives recommendations for policymakers to develop guidelines.

For more information, see: Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights- based Approaches to Principles for AI, The global landscape of AI ethics guidelines, Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications, and Algorithmic accountability in the public sector

3d Trust framework for digital identity management

Definition:

Framework or guidelines that establish rules for providing digital identity services, to ensure that people's information is safe and secure and to ensure that such systems are built on trust and human rights protection.

Rationale:

Online trust is the foundation of the digital economy. Digital identities are created as people use the Internet and produce information about themselves; they are the information collected and used online which represents the offline user. In order to be confident in their use of digital technologies, people must be able to have confidence that the personal data that describes them and their online activity is managed responsibly. Governments, in turn, must be able to protect people from online threats such as fraud, data loss, and digital exclusion in order to reap the full benefits that digital identities could bring. To build confidence, some countries have started issuing frameworks or guidelines on how organizations that create and use identity services should behave. A trust framework for digital identity may include standards for processes and practices, terms of accreditation for identity services, the scope and purpose of the identity system, roles and duties of actors involved, rules and regulations for the processing of identity information, and the responsible governing bodies.

Guidelines for Inclusion:

The document can be the result of a public-private partnership, but it must be evident that the government was involved in an official capacity.

3e Guidelines for non-governmental data sharing

Definition:

Guidance or toolbox created by a government as to how nongovernmental entities can share data in different contexts.

Sets out the legal, technical, and practical aspects to be taken into account as organizations think about and undertake the transfer and sharing of data.

Rationale:

Data exhibits numerous characteristics that call for it being considered a public infrastructural good and thus governed through commons-based governance structures. Mechanisms that increase data sharing or access rights to datasets, or

lay out how data can be bought and sold, are therefore aspects of a responsible approach to data governance.

Guidelines for Inclusion:

Guidelines must:

- Be targeted at nongovernmental private entities including business, but not individuals (this also includes the case of the UAE, whose Smart Data Principles apply mostly to governmental actors, but also to "Private Sector Entities exchanging data with government bodies or re-using government data."[24])
- Set out the legal, technical, and practical aspects, rather than only one of those.
- Be guidelines, meaning documents meant to be binding but which lack the force of law.

Search terms: guidelines on trusted private sector data sharing and use, contracts

Attribute 4: Structural

Definition:

The government alters institutional structures in response to data-driven transformation.

Rationale:

In response to the shifting needs of a digital society, governments should evolve new bureaucratic structures to accommodate new responsibilities and activities. Governments create or adapt existing institutional structures to protect personal data, take advantage of data as an asset, share data, and innovate on ways to extract additional value from data.

Guidelines for Inclusion:

[24] https://u.ae/-/media/guidelines/UAE-Smart-Data-Standards-EN--Part-1.ashx

4a Data protection body

Definition:

An institutional structure accountable for the governance and protection of personal data in society. This structure is typically established by the country's personal data law and is responsible for enforcing it.

Rationale:

Guidelines for Inclusion:

4b Open data portal

Definition:

An online government platform which enables users to access collections of government data that have been opened for public re-use.

Rationale:

Government open data portals may be constructed in response to requirements of freedom of information laws or open data laws.

Guidelines for Inclusion:

Open data portal must include a broader swathe of data than only statistics and budgets.

4c Open data Coordinating body

Definition:

Institutionalized body or oversight committee responsible for coordinating the opening of governmental data sets to the public.

Rationale:

Having a coordinating body for G2C data indicates that a government is taking seriously the need to adapt structurally to data-driven change.

Guidelines for Inclusion:

The body must have a role, explicitly mentioned in a website or document found online, in coordinating the release of government open data. This does not necessarily include, for example, the operator of the country's open data portal, the

task force behind an open data strategy, the civil society dialogue mechanism required under the Open Government Partnership, Federal ministries of communications technologies or similar high-level ICT authorities.

4d Public sector data governance body

Definition:

Institutionalized body responsible for coordinating public sector data assets to extract or exploit the value of data in the public sector. Often responsible for supporting data sharing among governmental entities; managing digital identity programs and/or base registry programs.

Rationale:

Having a data governance body indicates that a government is taking seriously the need to adapt structurally to data-driven change.

Guidelines for Inclusion:

The body must have a role, explicitly mentioned in a website or document found online, in coordinating public sector data assets. This does not necessarily include, for example, data departments of individual ministries, unless it is a ministry with remit over digital issues (and even departments such as statistical, evidence-based decision making, digital transformation, digital economy, or ICT do not necessarily count unless they deal explicitly with data governance or coordinating data sharing in the public sector). It may be the same organization responsible for open data, but in the description of its duties/mandate it must include G2G as well as the G2C of 4c. Although it is preferable if they are directly governmental, advisory bodies commissioned and/or chaired by governmental authorities also count.

Attribute 5: Participatory

Definition:

The government informs its constituents about its activities and asks for public comment, with the intention of incorporating their feedback.

Rationale:

Participatory data governance occurs when governments allow different constituents to contribute to the discussion, and are transparent and accountable about their activities to the public. The policy feedback loop, whereby

policymakers seek feedback on how the public sees their efforts and then work to incorporate this feedback into future efforts, is a key part of democratic governance in general. But it is perhaps even more important in data governance, where, to be able to extract the most value possible from data while protecting people from harm, and to be able to keep up with the rapid pace of change, including outside perspectives is crucial.

Guidelines for Inclusion:

5a Public consultation on data

Definition:

Government has formally asked for public comment on data-related legislation, strategies, or policies.

Rationale:

We were unable to ascertain the final (and most important) phase of the feedback loop, wherein policies are actually changed based on public feedback. We therefore include indicators that help identify nations that are acting on the first two phases, i.e. consulting the public and acknowledging their responses.

Guidelines for Inclusion:

This indicator looks at whether the country has consulted with the public regarding how it governs data. We include any open calls to allow the public to provide feedback on government policy making regarding data, including both personal and public data. Public consultations can include asking the public to email an agency with feedback about a specific policy, holding in person events to allow the public to provide feedback, or using a government-run portal to ask for feedback on a draft policy. We acknowledge the broad scope of what we define as public consultation and that more effective public consultations can empower citizens.[25] In order to limit our results to those relevant to the data-driven economy, we include only consultations initiated since January 1, 2016. Civil society organizations that frequently report on public consultation efforts, such as IAPP and Access Now, were consulted in addition to official government sources. For EU member states for whom no such consultation could be found, the EU consultation was used as this is an area where member states often turn to the European Commission (citation needed)

[25] See fhttps://iap2.org.au/wp-content/uploads/2020/01/2018_IAP2_Spectrum.pdf We thank Jeni Tennison for the valuable discussion on this indicator.

5b Government Response to Consultation

Definition:

Government official or body has recorded public comment and directly responded to stakeholder inputs in an official document.

Rationale:

We seek to know if governments actually hear public comments and respond with public policy changes. We therefore include indicators that help identify nations that are acting on the first two phases, i.e. consulting the public and acknowledging their responses.

Guidelines for Inclusion:

The response must respond to specific points brought up in the consultation or lay out how the government intends to alter policy based on the responses. This does not include a summary of contributions to a consultation, nor a list of the feedback given, nor a general acknowledgement that feedback has been heard/incorporated, without responding to specific points.

Search terms: summary /response of/ to public comment/ opinion/ hearing/ consultation

5c Multistakeholder Advisory Body

Definition:

A formal, ongoing consultative body that advises and works with the government on data governance issues. Requires a diverse group of stakeholders as members, including from the public and/or civil society.

Rationale:

In addition to asking for input from the public at large, governments should consult outside experts from a wide range of backgrounds on data governance issues. Such a group may be described as a council, task force, advisory panel, or expert group, multi-stakeholder in nature (meaning civil society or civilian representatives are included), that provides opinions and recommendations to help government regulators better understand and strategize about data and emerging technologies. digital data.

Guidelines for Inclusion:

The body must:

- Include members from different sectors than only business and government or all outside business.
- be standing bodies rather than bodies created to fulfill a time-limited objective
- Be devoted to emerging tech or data governance directly, as opposed to addressing sectoral data issues from time to time.
- Make their members and/or backgrounds available online (Germany listed every member of their body but did not provide biographies, requiring us to search their bios to see if the body was truly multistakeholder).

Search terms: government advisory board/committee on digital data/artificial intelligence/data governance

Attribute 6: International

Definition:

The government joins with other first-movers in shared international efforts to establish data governance rules and norms.

Rationale:

While the other five attributes deal with how a nation governs data domestically, this attribute attempts to gauge a country's willingness and readiness to participate in international data governance efforts and to cooperate with other nations to do so. Elements of both binding rules and soft norms are considered, because the end goal for both is taken to be changing participants' domestic regimes and thus result in an interoperable international arena.

Guidelines for Inclusion:

Only groups and agreements which are open to all nations to join, are considered.

6a Convention 108+

Definition:

A binding convention (treaty) developed by the Council of Europe to protect personal data which was updated to accommodate digital technologies. It includes rules governing sensitive data such as genetic or biometric data. Each Party has to

adopt in its domestic law the measures necessary to give effect to the provisions of the Convention.

Rationale:

Convention 108 opened for signature on 28 January 1981 and was the first legally binding international instrument in the data protection field. It required parties to protect the human rights of all individuals when personal data is processed. Convention 108+ in contrast updates the treaty in order to address the challenges for privacy resulting from the use of new information and communication technologies; and to strengthen the convention's follow-up mechanism. We focus on ratification because it signals that the country has approved membership through democratic procedures and is ready to put the treaty into effect.

Guidelines for Inclusion:

6b Open Government Partnership

Definition:

Country is a member of the Open Government Partnership (OGP).

Rationale:

OGP is a voluntary international partnership that requires member states to advance open government principles and cooperate with citizens on issues of open government.

Guidelines for Inclusion:

Countries that are inactive or suspended are not counted.

6c OECD Artificial Intelligence Principles

Definition:

The OECD AI Principles are a set of voluntary principles designed to promote use of AI that is innovative and trustworthy and that respects human rights and democratic values. It was first adopted only by the 38 OECD members, but as of May 2022, some 60 countries say they adhere to these principles.

Rationale:

"The OECD AI Principles promote use of AI that is innovative and trustworthy and that respects human rights and democratic values. Adopted in May 2019, they set standards for AI that are practical and flexible enough to stand the test of

time."[26] Adhering to the OECD AI Principles indicates a willingness to work cooperatively on trustworthy, human rights- and democracy-enhancing AI.

Guidelines for Inclusion:

6d Trade agreements with binding provisions on cross-border data flows

Definition:

Trade agreement with binding provisions governing cross border data flows. Under such provision, the signatories must allow the free flow of data for covered persons across borders with legitimate exceptions to achieve essential domestic policy purposes such as protecting public health.

Rationale:

If a country has signed a trade agreement with binding provisions governing cross border data flows (with longstanding exceptions as delineated under the General Agreement on Tariffs and Trade and the General Agreement on Trade in Services), that is perhaps the clearest indication that the government is attempting to establish international data governance rules. Non-binding agreements are not included because their language is aspirational; since a government has the free decision to participate in a trade agreement or not, if a country joins a non-binding agreement they are doing so because they have made the choice to not bind themselves to meaningful action. Includes disputable and non-disputable provisions/agreements.

Guidelines for Inclusion:

Language in the text must say that exceptions must be for legitimate reasons and applied in a nondiscriminatory and least-trade-restrictive manner. Most recent agreements are not only binding but disputable. One recent agreement, RCEP, states that these provisions are not disputable.

6e Budapest Convention

Definition:

[26] https://oecd.ai/en/ai-principles

The convention developed by the Council of Europe is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.

Rationale:

We do not consider cyber security data governance for the purposes of this metric, as cyber security is primarily concerned with protecting networks and digital infrastructure. Attempts to include cybersecurity in attribute 1, as a cybersecurity strategy, and in 4, as a cybersecurity body, thus ultimately went nowhere, as the evidence found was usually only incidentally concerned with the data that runs over these networks. Notwithstanding the above, we consider the international aspects of cybersecurity somewhat different, which is why we include cyber security here in attribute 6, in the Budapest Convention.

We do this for two reasons:

1. A nation willing to cooperate on issues of cybercrime indicates a broader interest in transnational data governance.
2. Cybersecurity policy typically differs nation to nation. For such a policy to be effective, however, it must be given the teeth of law, which is where cyber crime laws come in. Since cyber crime knows no borders, for such a law to be effective it must "extend beyond dealing with criminal activity within a subnational or national jurisdiction and become a tool to maximize cross-border cooperation… It also demands practical collaboration, usually achieved through mutual legal assistance treaties (MLATs)."[27] Therefore, we argue that cybersecurity is most relevant for data governance in its aspects that deal with international cooperation. The Budapest Convention is the main international legal instrument that includes MLAT processes.

Guidelines for Inclusion:

Country must be a party that has signed and ratified convention, per https://www.coe.int/en/web/cybercrime/the-budapest-convention

[27] https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000_Ch06.pdf page 193

Document Translation Strategy

Steps:

1. Use Google Translate to convert the indicator name or keywords into the language of the target nation.
2. Search for that result, in both the national language and English, on both a public search engine and in the internal website of the responsible Ministry.
    a. Use Google's advanced search features to narrow the scope of the search. For example, if searching for a document from Poland, add 'site:.pl' or even 'site:.gov.pl' after the search terms.
3. Translate the search results, using for example Google Chrome's built-in right-click menu option and the chrome Google Translate extension to automatically translate the results page.
4. For PDF results that do not translate using those tools, open the 'cached' version from the search dropdown menu next to each link on the search engine, and use chrome's translate tools on it there.
5. If there is no cached option, or a better translation or for the document is needed or to maintain its layout, use the online document translator found at https://www.onlinedoctranslator.com/en/. Upload the document and choose the language, and it keeps the layout.
6. If the document is too long or big, the website prompts you to use a different online tool to extract pages to shorten it (it only allows up to 100 pages at a time or 10mb), and then you can reupload it to onlinedoctranslator.
7. Scanned documents are currently unreliable to translate.