Institutions for data governance: Building trust through collective action

Main messages

1. The institutions required to govern data fill four main functions: strategic planning; developing rules and standards; compliance and enforcement; and generating the learning and evidence needed to gain insights and address emerging challenges.

2. Nongovernmental institutions and mechanisms such as data intermediaries can help governments and other actors safely share and use data to capture greater value, while promoting equitable access to data and the value they create.

3. Public institutions must have sufficient resources, adequate autonomy, and technical capacity, including data literacy, to fulfill their mandates efficiently. Political champions in positions of power are critical to leading data management reforms that create incentives and a culture of data use, dissemination, and transparency.

4. A multistakeholder, purpose-driven approach to data management and governance can help institutions keep pace with an ever-evolving data ecosystem and enhance their legitimacy, transparency, and accountability.

How can institutions help govern data for development?

As described in part I of this Report, capturing greater value from data requires sharing and using more data. This chapter describes how institutions can help facilitate the secure flow of data, while ensuring their confidentiality and protection in alignment with principles of the social contract for data.

Formed by state and nonstate institutions, *a data governance ecosystem*[1] provides structure and incentives for the trusted creation, storage, processing, sharing, use, and destruction of data throughout their life cycle. It does so by means of implementation of policies, laws, platforms,[2] systems, and standards. Three building blocks contribute to an effective and inclusive data governance ecosystem: the data governance functions carried out by institutions and actors; the role fulfilled by data intermediaries; and the performance-enhancing features of institutions.

Data governance functions include developing overarching data strategies and policies; elaborating legal frameworks and guidance on how rules should apply and be enforced if violated; undertaking arbitration in case of conflict; and maintaining monitoring, evaluation, and constant feedback loops to promote engagement, learning, and improvements.

These functions are performed by data governance institutions, whose roles and relations are specific to the context. This chapter highlights patterns in institutional mandates in the public sector and in the roles of nongovernmental institutions and actors across countries. Examples are provided of commonly used institutions, while recognizing that both the actual and optimal allocation of data governance functions across institutions will vary, depending on local conditions (see box 8.1).

Box 8.1 Uruguay's whole-of-government approach to data governance

Implementation of data governance reforms across the whole of government is complex. Some countries have opted to first build the foundational hard and soft infrastructure. This Report interprets soft infrastructure broadly to include software platforms (sometimes called data and information management systems[a]) supported by technical interoperability standards, data integration methods, and people accountable for the functioning of these systems. Siloed approaches, bespoke technical architecture, and disparate database taxonomies are often indicative of outdated soft infrastructure, preventing data from being used more widely.

Because of the disparate nature of existing platforms and the complex web of data management architecture, the initial stages of soft infrastructure reforms usually focus on digitizing, classifying, and sharing data within the public sector. The first step in the process should be identifying the data to which the government has access, how these data are classified (open, restricted, or personal), and who produces or uses the data, along with other information such as limitations and provenance. Desirable platforms and standards enable secure data flows across a wide variety of institutions and actors. This foundation of modern data infrastructure (both soft and hard) is meant to ensure that, for example, data produced in one ministry in the public sector can be easily shared with other ministries or users so that programs and policies are informed by multiple sources of data. More generally, well-designed, user-centric data infrastructure will encourage the repurposing and reuse of data, thereby increasing the value of data otherwise trapped in siloed infrastructure.

Along with infrastructure, countries must invest in the "analog complements," including adopting enabling legislation and regulations and institutionalizing governance arrangements to ensure the sustainability of reform efforts.[b]

One example of an institution-focused approach to data-driven digital transformation is that taken by Uruguay. Its Agency for Electronic Government and Information and Knowledge Society (Agesic), launched in 2007, has driven the country's successful e-government reforms. Because of its proximity to the Office of the President, Agesic has benefited from the high-level strategic leadership required to drive the country's digital agenda in a multistakeholder manner. A central factor in the success of Uruguay's digital transformation has been the integration of a well-developed domestic information and communication technology (ICT) industry that provides access to quality platforms and services with local technical knowledge to inform design and implementation efforts and avoid reliance on infrastructure built by the public sector.[c] The country's interoperability platform, the Integrated Government Architecture,

(Box continues next page)

Box 8.1 Uruguay's whole-of-government approach to data governance *(continued)*

and its supporting Enterprise Architecture Framework (TOGAF), are the technical foundation on which a robust data governance framework has been built.

Uruguay's Digital Transformation Agenda 2020 exemplifies how countries can take a whole-of-government and multistakeholder approach to guaranteeing that the various layers of the data governance ecosystem (platforms, systems, policies, laws, standards, and institutions) are designed and implemented in a coordinated, inclusive manner to enable better use of data for decision-making and user-centric service delivery.[d]

a. World Bank (2016).
b. OECD (2019a).
c. Porrúa (2013).
d. Agesic (2019).

After de jure governance arrangements are in place, actors may still not have strong incentives to create, share, and use data productively.[3] They may find these actions too costly, or they may try to free ride on the efforts of others.[4] Incentives to hoard data in siloes may arise from perceptions that control of data is tantamount to power over government decision-making. Other challenges to data sharing may be linked to autonomy or capacity constraints.

Data intermediaries and a user-centric design of digital platforms can lower the costs of sharing data, thereby reducing incentives for free riding. They also can support inclusion in data use by increasing the usability of information for nontechnical experts. This chapter explores how these new types of institutions and mechanisms facilitate data sharing and reuse between diverse actors and increase access to otherwise siloed datasets.

Free riding of data can occur in both the private and public sectors.[5] This chapter discusses three *features of institutions* that could improve incentives for collecting, sharing, and using data: (1) the technical capacity, including sound data literacy, to discharge their functions effectively; (2) a culture of performance and rewards and incentives for staff that support a transition to data-driven government; and (3) the institutional accountability and independence that help establish public trust in the integrity of institutions, particularly those tasked with rule making and compliance, which may otherwise be vulnerable to undue political or commercial influence.

Adopting an inclusive, multistakeholder approach to data governance can help ensure that the right challenges around data use are identified and addressed, keeping in mind the diverse needs of end users, including traditionally marginalized groups. Moreover, collaboration by a wide range of stakeholders from the private sector, academia, civil society, and international organizations can help governments strengthen the social contract around data by enhancing perceptions of procedural fairness and legitimacy. Finally, coordination among institutions in the public sector and nongovernmental stakeholders can avoid data and process duplication and facilitate secure data sharing, leading to gains in efficiency. Transparency and opportunities for scrutiny and accountability can be built into decision-making processes to increase their legitimacy.

The final section of this chapter uses the maturity model introduced in chapter 1 to illustrate how countries can best develop a solid institutional foundation to support their data governance ecosystem.

Data management across the data life cycle

The data life cycle starts when a government, private sector firm, civil society organization (CSO), nongovernmental organization (NGO), or academic institution (including think tanks and researchers) collect data (see figure 1.2 in chapter 1). These data are then validated, stored, and processed, and then possibly shared with others. After using the data, the actor may archive them or destroy them. If the data are retained, they can be reused. The life cycle begins again when data are reused, potentially for a completely new purpose. Engaging in outcome-oriented and user-centric data management at each step of the data life cycle can promote greater value creation from data (for examples, see table 8.1).

Some data management decisions lower the costs of data sharing across actors, thereby facilitating reuse. For example, as data are being processed they should be coded using standardized units or

Table 8.1 Data management decisions along the data life cycle

Stage of life cycle	Area in which data management is needed
Create/receive	• Determine lawful use (such as obtaining consent for data collection and sharing). • Collect identifications that allow data to be merged with other datasets.
Process	• Standardize units and categories (such as industry classifications). • Use data formats that are widely compatible and accessible. • Validate the quality (accuracy), relevance, and integrity of data.
Store	• Encrypt data; use secure servers; back up and archive data.
Transfer/share	• Verify whether consent allows for data to be shared. • Deidentify data, if appropriate.[a] • Sign confidentiality agreements for use of identified data. • Publish data via bulk downloads or APIs.
Analyze and use	• Ensure reproducibility; publish code or algorithms. • Do not publish identifiable data. • Visualize and communicate insights from data.
Archive and preserve	• Classify and catalog data systematically so they can be found easily. • Include data dictionaries and notes on how data were created. • Maintain access to data and their security and integrity over time.
Destroy or reuse	• Keep records of destruction processes. • Verify that consent for use is still valid.

Source: WDR 2021 team.

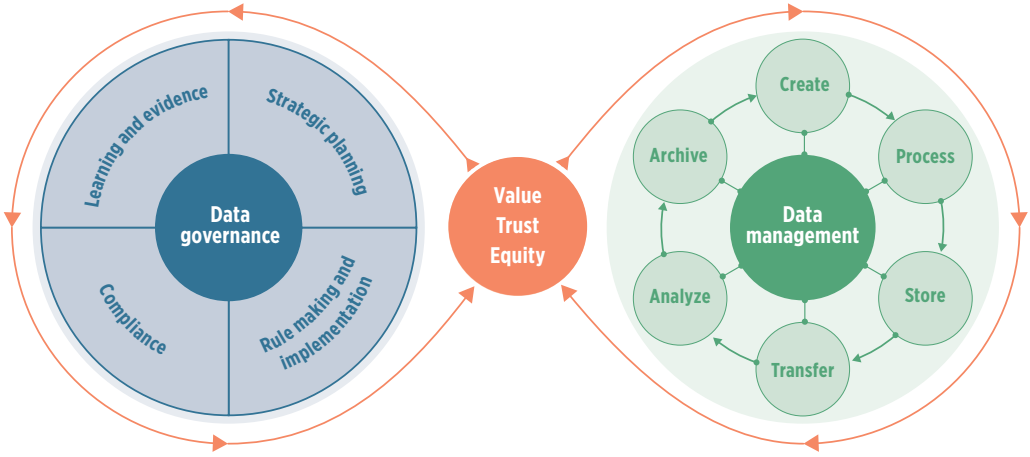
Note: APIs = application programming interfaces.

a. See Elliot et al. (2016); Polonetsky, Tene, and Finch (2016).

categories, such as common industry classifications, and converted to a format widely compatible with various types of software. Adopting common classifications and formats requires an upfront investment, but it will allow actors to share and combine data more easily. In Mexico, states and local municipalities collect and share data via the central government's open data network, Red México Abierto, in accordance with centralized data quality standards.[6]

The decisions at every stage of the data life cycle will vary, depending on the type of data and their proximity to features of public goods.[7] To guide and structure decisions, data management needs to rely on a data governance framework. In a mature data system, data governance and data management work together to create value from data use in a manner consistent with the values of the social contract (figure 8.1). The data governance framework can

Figure 8.1 Data governance and data management, working seamlessly together in support of the social contract



Source: WDR 2021 team.

Note: The data management life cycle at right appears in figure 1.2 in chapter 1.

stipulate rules about the use and reuse of data, including consent, and also set standards for processing and classifying data. Together, clearly defined data management standards and a robust data governance framework can help users better harness the value from data in a safe and equitable manner.

Data governance functions

Traditionally, scholars studying how data governance frameworks can improve data management have concentrated on private sector firms.[8] However, recognition is growing that data governance frameworks are also needed to guide countries' public sectors and multilateral organizations seeking to enhance the value of data to improve lives.[9] Box 8.2 illustrates why such a framework is important to the functioning of a data economy—and how intricate it can be—using the example of digital IDs.

This chapter draws on the literature and experiences of public sector management worldwide and the body of work on corporate data governance to

Box 8.2 The importance and complexity of data governance institutions: The example of digital identification (ID) systems

Verifying identity attributes or authenticating an identity—particularly using an official trusted source—can be an essential step in determining whether a person is who he or she claims to be and is authorized to apply for or receive the requested service or benefit. The application of digital identity verification and authentication mechanisms in conjunction with trusted and inclusive ID systems can increase access to services, reduce fraud and administrative costs, and create opportunities for innovation, such as through the automation, integration, and remote delivery of services. However, these mechanisms also process sensitive data, sometimes including biometric data, and therefore must be subject to strong governance and accountability frameworks.

An ID system's purpose—how personal data will be used—is typically set by law or regulation. These rules govern the system's design and operation, as well as the technical specifications, standards, and procedures to be adopted to ensure that the system delivers the level of assurance needed for identification and verification. These rules also protect security and personal data and mitigate risks of surveillance and discrimination.[a] Such rules may limit the collection and use of personal data to the minimum necessary to achieve the specific processing purpose, or require deidentification or encryption. The rules may state as well that certain data—such as biographical data and biometric data—should be processed separately to prevent any attempt to assemble complete profiles of individuals.[b] Whether data localization requirements will apply to the data will depend on the risks, opportunities, and costs involved, and whether third-party databases, processors, or cloud providers can provide assurances about security and data protection requirements.

Administrative rules aimed at mitigating risks of human error and misuse of personal data may require that identification and authentication functions be separated in the system or that administrators be authorized with the "least privilege" powers necessary to perform their delegated functions.[c] If the system outsources critical functions to others, such as enrollment agents, registrars, or credential providers, these parties may be subject to certification and obligations. Third parties using the system, such as hospitals, banks, universities, and public agencies, must be subject to rules on the basis by which they can access the ID system, standards on the form of data they exchange, and controls on how they can use the data they handle. Rules will govern how such interactions must be logged to create records of an individual's activities and relationships with numerous bodies.

Other institutions and actors may also be involved. For example, an independent digital identification agency may be responsible for managing the system. A civil registration agency may need to interoperate with it. A data protection authority (DPA) may exercise general oversight to ensure implementation of the appropriate governance principles[d] and compliance with the law. A foundational ID system may be considered critical infrastructure, requiring monitoring by the DPA, a Computer Security Incident Response Team (CSIRT), or other body responsible for cybersecurity. If the ID system is part of a regional mutual recognition arrangement[e]—such as the European Union's electronic IDentification, Authentication and trust Services (eIDAS) framework[f]—interoperability and use of common standards with foreign agencies that issue IDs and credentials may be required.

a. Cavoukian (2011).
b. Danezis et al. (2014).
c. For example, the Unique Identification Authority of India (UIDAI) operates clearance levels for accessing the Aadhaar identification database. See UIDAI, Aadhaar (dashboard), https://uidai.gov.in/.
d. The development of data strategy, policy, and regulations should be informed by a principles-based approach (Floridi and Taddeo 2016).
e. The African Union (AU), Economic Community of West African States (ECOWAS), East African Community (EAC), and Association of Southeast Asian Nations (ASEAN) are considering introducing mutual recognition of identification credentials across borders.
f. EC (2020); EU (2014).

Figure 8.2 Functions of data governance

Source: WDR 2021 team.

take a broad view of data governance. Its functions are divided into four thematic clusters: strategic planning; rule making and implementation; compliance; and learning and evidence to provide insights and improve policy making (figure 8.2). Within each thematic cluster are several functions.[10] The next major section maps the governance functions described here to specific institutions and actors both inside and outside government.

Strategic planning

Developing strategies and establishing institutional arrangements. The overall objective of data institutions and governance frameworks is to safely realize greater social value from data. Finding the appropriate balance between encouraging greater use of data while maintaining safeguards against misuse is ultimately the role played by each country's social contract for data. Achieving this balance in practice requires that institutions and actors work together to transform the general principles[11] of the social contract into strategies, policies, and integrated data systems (chapter 9). This transformation must go beyond protecting personal data to include strategies for responsible and ethical data use (chapter 6). This step is particularly warranted because of the rapidly changing data landscape and incentives to collect vast amounts of data, creating opportunities for data use and misuse (chapter 3). At the country level, the first step is to develop a national data strategy in line with the country's priorities (chapter 9). To facilitate implementation, strategies should be devolved into action plans with clear targets.[12] Strategies should also include identifying institutional arrangements and mapping governance functions to existing or new institutions.

Rule making and implementation

Legislating and regulating. Laws and regulations are the critical safeguards and enablers needed to standardize and organize data throughout the data life cycle. They stipulate how sharing, pooling, or granting of access will be carried out, including limits on certain uses of data to promote trust (see the detailed discussion in chapter 6). Rule-making functions include creating new public sector data governance institutions whose mandate, criteria for appointing managers, and funding arrangements are stipulated by regulation or decree.

Setting standards. Systems should be designed around recognized harmonized formats and protocols for data production, storage, transfer, access, protection, and security, thereby supporting interoperability, increasing data quality, and improving the usability and integrity of data.

Providing clarification and guidance. Institutions can reduce barriers to compliance with laws and regulations (say because of lack of information about obligations) by providing stakeholders with clear, practical, easily accessible, and user-friendly guidance.[13] The more complex the data and the actors involved, the greater may be the need to clarify and guide participants to ensure a shared understanding of how the data are governed.

Compliance

Enforcing. Enforcement is the day-to-day work of ensuring compliance with laws and regulations, standards, and norms.

Auditing. Enforcement is supplemented with regular and occasional audits to identify areas of noncompliance that may require remedies or improvements in the rules.

Arbitrating. When rules do not answer all the questions, arbitration may be helpful. For example, if there is doubt about whether the combination or association of certain data renders the data sensitive (such as by revealing religion), a decision may be required on whether the data processing falls within the scope of the data protection law.

Remedying. Faults in compliance require remedies to correct or compensate for any breaches or damage

from the use of data. For example, if data have been obtained or manipulated without authority, thereby breaching data protection or security requirements, it may be necessary to notify the data subjects or cancel an identity credential.

Learning and evidence

Backward-looking monitoring and evaluation (M&E). M&E can serve at least two purposes. First, it can help supervisors track the performance of their own staff and organizations, allowing them to make better management decisions.[14] Second, M&E can assess how a program or policy delivers on identified objectives. Disseminating M&E frameworks and results in user-friendly formats can foster accountability and promote trust in data governance institutions.

Forward-looking learning and risk management. Complex areas of data governance can benefit from horizon scanning and scenario planning, as well as from anticipatory governance.[15] These tools and approaches can be used to identify and respond to emerging or unforeseen issues before they become acute societal challenges and to inform planning and policy-making activities. For example, the growing use of artificial intelligence (AI) and big data technologies in some sectors (such as the utilities market) or for emergency uses (such as contact tracing during the COVID-19 pandemic) may require policy makers to adapt existing data governance regimes before any misuse of that data occurs.

Innovation. Both M&E and risk management can be helpful in responding to the rapid technological changes reshaping the possibilities and risks in how data management systems are designed and used. In response to the rapidly changing environment, institutions can play an important role in facilitating timely assessments of what works in the newly evolving data environment and offer guidance on how to quickly adapt to change and promote knowledge sharing. Institutions can also play an important role in rolling out lessons and capacity building both within the nation and internationally. Once a new approach has been shown to succeed in one region, country, or locality, existing mechanisms should enable it to be tested in others, especially those with limited internal resources.

Mapping data governance functions to illustrative institutions

The governance functions described in the preceding section may be performed by *entities within government*, at the center of government, and at the technical level. They also may fall to sector-specific agencies, the judiciary, independent regulators and watchdogs, or subnational government bodies.[16]

These functions may be performed as well by *nongovernmental institutions*, including individual citizens; CSOs; NGOs; the private sector (such as industry associations and standard setting organizations); the news media; academic institutions, think tanks, or researchers; and bilateral and multilateral organizations.[17]

Nongovernmental institutions and actors play an important role in performing or informing data governance functions. Deliberation and consensus building between these actors promote trust and responsive policy making, thereby strengthening the social contract on data (see discussion later in this chapter). These processes have become more important over the last 20 years.[18] Nongovernmental institutions can also impose checks on governments in states with weak or limited formal institutions where elite capture may impede data governance and hinder outcomes in the public interest.[19]

Table 8.2 maps institutions and actors to the governance functions they typically perform, according to the most prominent function of each institution. This mapping does not imply that certain institutions do not also perform other functions that may fall in other thematic clusters. The institutions and actors discussed here are not meant to be prescriptive or exhaustive. Rather, they illustrate how these functions and processes can be performed in different contexts.

The institutional arrangements adopted should consider preferences about the data at issue, the existing structure of the public sector and society, technical capacity, and available technologies. Institutions that perform well in certain contexts may fail in others. As the 2002 *World Development Report* on building institutions for markets stated, "Much of the important work in building institutions lies in modifying those that already exist to complement better other institutions and in recognizing what not to build."[20]

Strategic planning institutions

Government entities. Many countries—especially higher-income countries—have taken a *centralized approach* by adopting a national data governance entity that provides strategic direction, makes policy decisions, and sets institutional arrangements. Countries either establish a separate data governance agency or opt for a dedicated data governance unit embedded in an existing institution. Fifty-three percent of high-income countries have a data governance entity in place, compared with only 18 percent of upper-middle-income

Table 8.2 Candidate institutions and actors to perform or inform data governance functions

Thematic clusters and functions	Indicative institutions and actors
Strategic planning • Developing strategies and policies in line with the social contract for data • Establishing institutional arrangements	*Data governance arrangement* • Centralized approach: data governance agency/unit embedded in an existing institution (such as NSO, digital economy ministry) • Decentralized approach: data governance units and responsibilities embedded across government • CSOs • Universities • Research institutions
Rule making and implementation • Legislating/regulating • Setting standards • Providing clarification and guidance	*National legislature and sector-specific regulators* • Telecom regulator • Banking and financial securities market regulator • Industry associations • CSOs • Institutional Review Boards *International institutions* • Sector-specific SSOs • International organizations (World Bank, IMF, UN, WTO)
Compliance • Enforcing • Auditing • Arbitrating • Remedying	*Watchdog and umpire* • Data protection authority • Access to information agency • Antitrust authority • Consumer protection agency • Audit body • Courts • Ombudsperson • CSIRT
Learning and evidence • Engaging in backward-looking monitoring and evaluation • Engaging in forward-looking learning and risk management	*Knowledge community* • M&E unit within entity or independent M&E body • CSOs and NGOs, multilateral development institutions, international development banks • Academic institutions • Think tanks, policy institutes, research institutions • News media • Training bodies • Professional associations

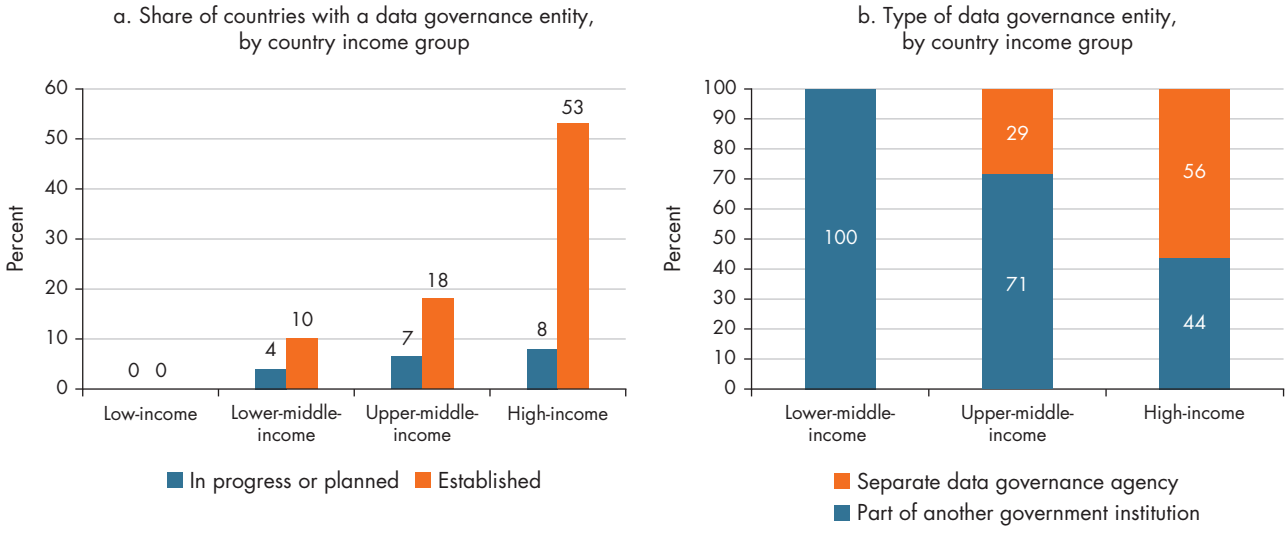
Source: WDR 2021 team, based on a functional approach to governance and public sector management.

Note: CSIRT = Computer Security Incident Response Team; CSO = civil society organization; IMF = International Monetary Fund; M&E = monitoring and evaluation; NGO = nongovernmental organization; NSO = national statistical office; SSO = standard setting organization; UN = United Nations; WTO = World Trade Organization.

countries and 10 percent of lower-middle-income countries (figure 8.3, panel a).[21] To date, no low-income country has established a data governance entity. For the most part, countries that do not have a data governance entity also do not have a stand-alone national data strategy in place. Only 3 percent of low-income countries have such a strategy, compared with 6 percent of lower-middle-income countries, 18 percent of upper-middle-income countries, and 52 percent of high-income countries (see chapter 9 for a discussion of development of a national data system in support of a national data strategy).[22]

Lower-middle-income countries and upper-middle-income countries are more likely to embed the strategic planning function in an existing government institution (figure 8.3, panel b). One reason for doing so is that creating stand-alone institutions can be costly and inefficient, requiring sufficient resources and technical capacities to be productive.[23] Embedding new functions in existing institutions

Figure 8.3 No low-income and few lower-middle-income countries have a separate data governance entity; most embed them in another government institution



Source: WDR 2021 team calculations, based on World Bank, DGSS (Digital Government/GovTech Systems and Services) (dataset), https://datacatalog.worldbank.org/dataset/digital-governmentgovtech-systems-and-services-dgss-dataset. Data at http://bit.do/WDR2021-Fig-8_3.

Note: Panel a: data are for 198 economies. Data governance entities include both separate agencies and units that are part of another institution. Panel b: data are for 58 countries. Data are only for countries that have a data governance entity established or in process. Low-income countries are not included in the figure because none has a data governance entity.

or creating an interinstitutional body such as a data governance council may give governments greater flexibility in the early stages of establishing a data governance framework. This approach also enables governments to draw on expertise from relevant institutions and, by incorporating more stakeholders in the process, to increase the inclusivity of strategy setting and policy design.

In Jordan, the strategic planning function is assigned to an existing government institution. The Policies and Strategies Directorate of the Ministry of Digital Economy and Entrepreneurship (former Ministry of Information and Communications Technology) is responsible for developing relevant strategies and policies. The directorate has drafted the country's Digital Transformation Strategy for Government Services (2019–22), as well as technical policies related to various elements of data governance, including the government's policies on data classification and cybersecurity. Similarly, the government of Thailand assigned the strategic planning function to previously existing agencies by fully replacing its Ministry of Information and Communication Technology with the Ministry of Digital Economy and Society in 2016. Several agencies responsible for cross-cutting data and digital technology functions were consolidated under this new centralized structure.[24]

Brazil is one of the few upper-middle-income countries with a separate data governance entity. Established in 2019, the Central Data Governance Committee is tasked with steering Brazil's transition to a data-driven public sector by promoting data sharing among federal agencies and integrating citizens' information in a single platform (the Citizen Base Register).[25] The committee was created as a separate entity by presidential decree to ensure high-level collaboration and coordination of data governance activities.

Other countries have followed a more *decentralized approach*, whereby a network of ministries, departments, and agencies share responsibilities for implementing data governance functions. For example, national statistical offices (NSOs) often serve as the focal point for development of National Strategies for the Development of Statistics (NSDSs), a component of a country's data strategies (see chapters 2 and 9).[26]

The entity responsible for strategic planning must be placed at the highest level in government, where it can exercise the appropriate leverage. In some countries, this location is at the center of government, such as the Prime Minister's Office or President's Office, in coordination with the NSO.

Nongovernmental institutions. Institutions outside of government, including *civil society actors, academic institutions, think tanks, and nongovernmental research*

institutions, also play a key role in developing strategies and policies.[27] Some initiatives are almost entirely driven by civil society, such as in the open data space. For example, nongovernmental actors established the Open Definition in 2012, standards for open data licensing in 2013, and the Open Data Charter in 2015.[28] Civil society actors can also add value by advising on how strategies and policies can build on and be responsive to local dynamics and address problems in a manner suited to the local context.

Strategic planning functions may also be performed by international or regional organizations. In 2018 the Association of Southeast Asian Nations (ASEAN) adopted the ASEAN Framework on Digital Data Governance, which guides members seeking to strengthen and coordinate their policy and regulatory regimes and institutional arrangements for data governance and to achieve interoperable data governance systems. The framework is aimed at bolstering the region's digital economy and enhancing cross-border data flows in a manner consistent with the data regulatory thresholds of partners. Similarly, the African Union's Digital Transformation Strategy for Africa (2020–30) is aimed at increasing data interoperability (to spur greater use of data and transform the digital economy) and improving standards for data protection.[29]

Rule making, standard setting, and implementing institutions

Rule making and implementation functions are performed across the three branches of government. *National legislatures* typically make laws, while executive bodies develop implementing regulations. Enforcement of legal frameworks is undertaken by independent regulators (such as data protection authorities) and the judiciary. Nongovernmental actors could support enforcement by means of monitoring, advocacy, advice, and legal aid. In addition, *sector-specific regulators*—such as telecommunications, banking, and financial securities market regulators—could support sectoral rule making. For example, a banking sector regulator could require banks to submit credit information to credit reference bureaus, which, in turn, could increase access to finance for those who may not be able to obtain bank credit in the absence of credit reference bureaus.[30] Similarly, securities markets regulators could compel listed companies to disclose financial data to assist investors in their decision-making and thus improve the allocation of resources across the economy (see chapter 6).

Sector-specific standard setting organizations, such as the Extractive Industries Transparency Initiative (EITI), the Open Government Partnership (OGP), and the United Nations' International Telecommunication Union (ITU), establish common sets of principles, rules, and procedures that help support interoperability and portability of data within a sector. Transaction costs then fall and the prospects rise for productive data flows between data suppliers, data intermediaries, and data users.

Private sector industry participants also have an important role to play in setting standards because they can facilitate market access, increase efficiency, reduce costs, and manage labor and environmental standards to achieve responsible productivity.[31] Although private standards are voluntary, they may become de facto industry norms if they are widely adopted. They can be especially appropriate when informed by public sentiments; industry actors may be moved by pressure related to ethical behavior, fair labor practices, their environmental footprint, and more. Voluntary industry standards can also potentially avoid the rigid qualities of government standard setting.[32] For example, *industry associations* develop standards and provide guidance at the industry level. The foremost example is the International Organization for Standardization (ISO),[33] an independent global organization with a membership of 165 national standards bodies composed of domain experts who develop market relevant standards based on an international consensus. On the other hand, market asymmetries may lead to a lack of inclusivity in the development of standards, with dominant companies having a first-mover advantage to determine industry specifications (see chapter 6).

Institutional Review Boards (IRBs) monitor research involving human subjects, including impact evaluations and other M&E efforts. They have the power to approve, require modifications in (to secure approval), or disapprove research. IRBs are mostly found in high-income countries and are not yet a critical data governance institution in low-income countries. Yet their reviews have an important role in ensuring responsible data use in research and protecting the rights and welfare of human research subjects, including those from low- and middle-income countries.

International organizations, academic institutions, and CSOs can also help transform the principles of the social contract into actionable guidelines for ethical data use. For example, they can help data science professionals and practitioners create ethical codes of conduct that are specific to their organization or stakeholder community. In 2017 the United Nations Sustainable Development Group—a consortium of 36 United Nations (UN) agencies, departments, and

programs—convened to develop a set of ethical guiding principles to protect data privacy and to use big data in development and humanitarian contexts.[34] Likewise, the NGO DataEthics.eu, a collaborative effort across academia and civil society, has developed a series of data ethics principles designed using a European legal and value-based framework for voluntary adaptation and use by European Union (EU) data providers, data intermediaries, and data users.

Institutions that enforce compliance

Compliance can be enforced internally—that is, by parties governed or affected by the rules at issue—or externally by a third party. It can also be enforced informally[35] through peer pressure or shaming or formally through official investigations, rulings, and sanctions.

Informal institutional arrangements rely on commitment-based and opt-in approaches whereby parties are not obliged to undertake specific actions. For example, the United Nations Fundamental Principles of Official Statistics guide national statistical systems that self-govern according to these principles.[36]

Institutions with internal enforcement mechanisms can be effective because they typically feature a recognized system of incentives and penalties to encourage desired behaviors. For example, EITI and OGP have sanctioned or expelled member countries when it was determined that these countries did not adhere to articulated standards.[37] Both institutions sanctioned Azerbaijan (EITI in 2015 and OGP in 2016), and EITI delisted Equatorial Guinea and São Tomé and Príncipe in 2010 for insufficient progress against agreed-on deadlines. In the latter two countries, this delisting catalyzed the expected action.[38]

Public pressure can also be brought to bear by NGOs that assess the quality of data governance and monitor compliance with standards through public indexes or scorecards. An example is the Global Data Barometer, which assesses the quality and scope of countries' data governance, availability of key datasets, and capacity for responsible data use.[39]

Transnational institutional arrangements have a formal constitutional setup, such as Articles of Agreement, that obliges members to abide by specific standards or rules. They typically stipulate internal compliance requirements and articulate what sanctions apply to noncompliance. Censure is a typical enforcement mechanism. An example of a transnational institution is the International Monetary Fund (IMF). In 2011 it found Argentina to be in breach of its obligations under the IMF's Articles of Agreement because it was providing inaccurate consumer price index and gross domestic product data. After reforms by Argentina's NSO to address the methodological and data quality issues in question, the IMF lifted the censure on the country in 2016.

At the national level, *data protection authorities (DPAs)* oversee and enforce compliance with data protection legislation by investigating data breaches and issuing monetary penalties, enforcement notices, or other punitive measures when an organization is found to have breached its data processing obligations.[40]

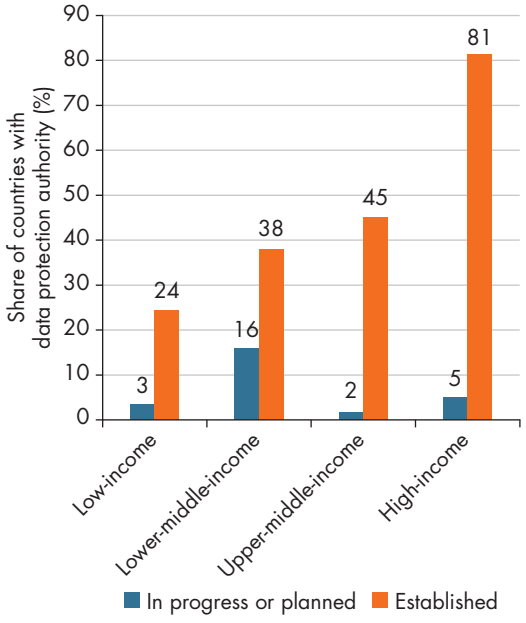
Some DPAs have adopted a more principle-based approach to compliance by encouraging data processing organizations to embed accountability practices into their operations. For example, Singapore's data protection commission, Infocomm Media Development Authority (IMDA), has adopted an enforcement framework that rewards good accountability practices such as adopting data protection by design and encouraging the use of data protection impact assessments through capacity building, change management, and organizational restructuring.[41] This approach can be helpful in instances in which existing data protection laws do not yet require such practices, in parallel to strengthening the legal framework. Other DPAs, such as the French National Commission for Informatics and Liberties (CNIL), provide incentives for compliance by developing certification schemes for data protection officers in order to standardize competencies within this compliance role.[42]

The presence of a DPA increases with country income level (figure 8.4). Although 81 percent of high-income countries have a DPA, only 45 percent of upper-middle-income countries, 38 percent of lower-middle-income countries, and 24 percent of low-income countries have such an authority.

In certain contexts, an existing institution, such as an *access to information agency* or related *ICT agency*, may be tasked with compliance responsibilities. For example, Argentina's DPA falls under the country's Agency of Access to Public Information—a 2018 presidential decree modified the then-newly adopted Access to Information Law.

An *antitrust authority* may find certain data practices anticompetitive (see chapter 7). It may break up an existing organization or its datasets when the organization has accumulated levels of control that give it an unacceptable level of market power. For example, a decision by Germany's Federal Cartel Office (Bundeskartellamt) prevented efforts by Facebook to combine data from Facebook, Instagram, and programming interfaces integrated into websites producing social plug-ins.[43] Antitrust authorities are

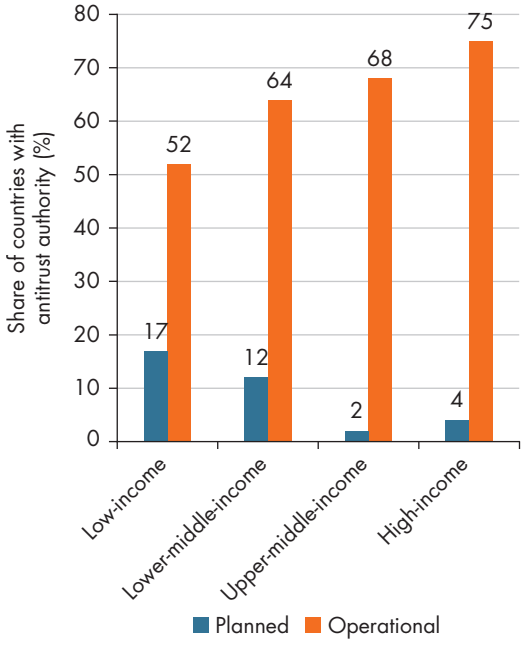
Figure 8.4 The lower the country income level, the fewer are the countries with data protection authorities



Source: WDR 2021 team calculations, based on World Bank, DGSS (Digital Government/GovTech Systems and Services) (dataset), https://datacatalog.worldbank.org/dataset/digital-governmentgovtech-systems-and-services-dgss-dataset. Data at http://bit.do/WDR2021-Fig-8_4.

Note: Data are for 198 economies.

Figure 8.5 More than half of countries across all income groups have antitrust authorities



Source: WDR 2021 team calculations, based on data from World Bank. Data at http://bit.do/WDR2021-Fig-8_5.

Note: Data are for 218 economies.

operational in more than half of countries across all income groups (figure 8.5).

Formal independent audits—or the possibility of one—can also be an effective mechanism to hold institutions to account and drive performance improvements. Audits are typically performed by an *audit body*, whether an independent Supreme Audit Institution, a committee (such as a parliamentary Public Accounts Committee), or a specialized subnational department (such as a city audit office).[44]

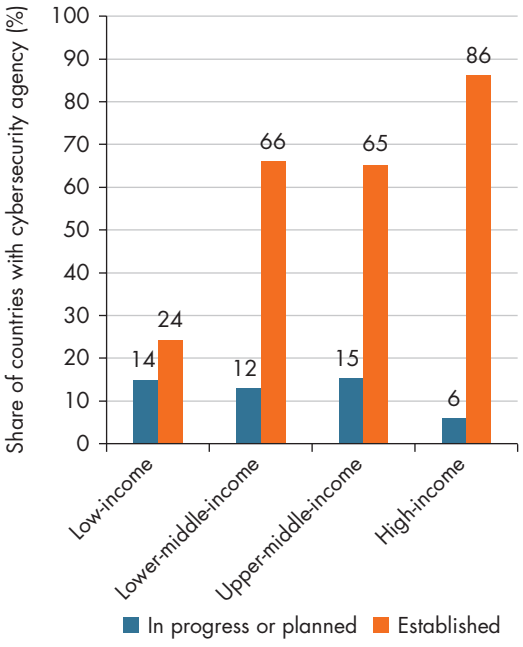
Likewise, *courts* provide a venue for independent redress and enforcement, and they can also facilitate informal settlement. A centralized or decentralized *ombudsperson* may be able to collect complaints and provide redress for grievances. In some countries, data protection legislation explicitly provides for grievance redress.[45] In countries with no such legislation or where existing legislation makes no such provision, service providers may set up specific grievance redress mechanisms to collect and address complaints internally.

Oversight is also needed to minimize risks to data platforms, data systems, and data per se. A *Computer Security Incident Response Team* (CSIRT) is a designated team of information security experts. It protects data management architecture and detects and resolves any computer, network, or cybersecurity incidents, such as data breaches and denial of service attacks.[46] CSIRTs and related institutions are also typically responsible for running public awareness campaigns aimed at data intermediaries and users to help ensure adherence to data security protocols. Cybersecurity agencies are relatively widespread in middle- and high-income countries, but are present in only 24 percent of low-income countries (figure 8.6).[47]

Institutions that promote learning and evidence-based policy making

M&E functions, as well as anticipatory governance, can be embedded in dedicated units in ministries and agencies involved in data management and governance functions. Some countries may have a *national-level M&E agency*, such as the US Government Accountability Office (GAO), which is responsible for auditing and evaluating US federal government activities. Other countries may locate their *M&E unit within an executive office* responsible for tracking strategic key performance indicators.

Figure 8.6 Only about one-quarter of low-income countries have cybersecurity agencies



Source: WDR 2021 team calculations, based on World Bank, DGSS (Digital Government/GovTech Systems and Services) (dataset), https://datacatalog.worldbank.org/dataset/digital-governmentgovtech-systems-and-services-dgss-dataset. Data at http://bit.do/WDR2021-Fig-8_6.

Note: Data are for 198 economies.

Outside of government, *CSOs, specialty NGOs, universities, think tanks, research organizations, the news media, and even individual citizens* play an important M&E role. Nongovernmental monitoring of issues of public concern can be useful in assessing government performance, as well as signaling accountability failures, such as corruption or inefficiencies or gaps in public service delivery. For example, during the COVID-19 pandemic Johns Hopkins University in the United States recognized and filled a gap by creating and launching a transparent, reliable data collection mechanism and dashboard for tracking virus cases globally. The mechanism was then used by policy makers and the public worldwide to better understand the spread of the virus and come up with ways to combat it. Such nongovernmental, independent actors can provide convenient and consistent access to accurate data and reduce data governance and management inefficiencies, while offering a host of actionable perspectives and advice. For example, the Data Governance Network is India's first policy-oriented research network on data governance, bringing together several leading think tanks. It was founded to inform policy making.[48] In 2017 the UK's British Academy and Royal Society published a series of reports entitled "Data Management and Use: Governance in the 21st Century," based on consultations with stakeholders from civil society, the private sector, and academia.[49] Nongovernmental institutions can also help generate learning and evidence on potential opportunities and harms when developing social contracts on data in different contexts. Some institutions are devoted to understanding the ethical implications of new methodologies and uses of data.[50] Others focus on sharing knowledge and acting as a catalyst for learning.[51]

To undertake learning and evidence activities, government institutions and other actors must rely on a workforce with the appropriate skills, which requires, in turn, more *public or private institutions specializing in skills development and certification* (see chapter 4). This need grows more pressing as data governance and management become increasingly sophisticated and the number and range of technicians and skills required increase.

Data intermediation and collaboration

Another way to enable better data use, reuse, and sharing is through data intermediation. An entity (data intermediary) or simply a contractual arrangement facilitates the collection, validation, and aggregation of data from data contributors and makes data understandable, usable, and accessible to data users.[52] Data intermediaries can facilitate data sharing in a trusted, more efficient manner between government institutions or between government and nongovernment actors as part of the broader national data system (table 8.3).

Data intermediaries (sometimes called infomediaries) can be important enablers in low- and middle-income economies that may have gaps in their data management frameworks or weak enforcement. Where the potential of otherwise siloed data would remain unrealized,[53] they can mediate data flows between data producers and individuals or communities for research and evidence-based policy making,[54] or they can provide public sector institutions with feedback.[55] Grassroots-based data intermediaries could also help individuals better understand and enforce their rights over their personal data. Other intermediaries create commercial opportunities through data markets.

Data intermediation in the private sector. Exclusively commercial, for-profit data intermediaries are relatively commonplace, functioning primarily as data

Table 8.3 Snapshot of common data intermediary structures

Purposes	Objectives	Types	Examples
Create commercial value and data markets.	Transform raw data into more consumable information.	Data aggregators, data brokers	Acxiom, Experian
Exchange data to solve public problems through collaborative structures.	Increase incentives for competitors to share and combine data resources for common use within sectors.	Data pools	Global Data Synchronization Network (GDSN)
	Create and manage shared and interoperable data assets and computing infrastructure for research.	Data commons, data clubs	The Open Commons Consortium (OCC), UK Biobank
	Contribute data in exchange for collective benefits.	Data cooperatives	LunaDNA (community-owned platform for health research)
Enable trusted sharing and use of sensitive data through enhanced accountability mechanisms.	Facilitate sharing of sensitive data and provide collective bargaining power to individuals.	Data trusts	Platform Info Exchange, UK (Mozilla Data Futures Lab pilot)

Source: WDR 2021 team.

aggregators. These intermediaries collect raw, disaggregated data that are difficult to work with, systematize and sometimes analyze them, and then repackage them for sale to others. Many commercially driven data aggregators are familiar features of society, including credit reference bureaus. More broadly, data brokers scrape public records and buy or license private data to build profiles of individuals that can be sold for a profit—often for marketing purposes, risk mitigation (including for identification verification and fraud detection), and people search pages.[56] Some 4,000 data brokers operate worldwide in an industry valued at US$250 billion.[57]

Data markets are passive digital platforms through which data owners can offer their datasets for sale. When structured well, data markets can enable crowdsourcing of data (including from data subjects), support interoperability, create a central point of discoverability, and enforce minimum data quality standards.[58] Rising concerns about the use (and abuse) of personal data by profit-driven data intermediaries—particularly given the rise in locational data and the ultimate anonymity of data, as well as data subjects' lack of control—have increased public scrutiny and led to new rules on their operations (box 8.3).

Data intermediation for public or common goods. New types of intermediaries oriented toward public or common goods are emerging. Data collaboratives facilitate and promote data sharing between diverse actors by ensuring compliance with minimum data protection and security rules, as well as quality standards and rules to make data interoperable.

Data collaboratives can involve a diverse array of actors—such as government institutions, private companies, research institutions, or CSOs—that come together to exchange data with a view toward solving public problems.[59] Data sharing arrangements[60] could, but need not, involve the creation of a separate entity tasked with managing data, including ensuring safe and ethical usage.

Some data collaboratives function primarily to increase participants' access to data in order to solve collective action issues and use insights from analyzing aggregated, nonrivalrous data. *Data pools* are usually contract-based mechanisms in the private sector that create a centralized repository of data. Participants can obtain, maintain, and exchange information in a standard format.[61] The Global Data Synchronization Network (GDSN),[62] an internet-based, interconnected network of interoperable data pools, facilitates product-related data sharing across companies in sectors such as retail, health care, and transport and logistics. In the private sector, data pools create unique opportunities for market insight, gains in efficiency, and innovation because of their tailored analytical function, although they also present competition risks (see chapters 6 and 7).[63] In the public sector, data pools can be used to safeguard centralized data stores. Mauritius has built trusted digital data repositories using unique digital identities, federated authentication, and a set of key digital services that can be embedded in wider public or private sector applications when data sharing is required.[64]

Data commons and data clubs, broadly inspired by data pools, may help entities or people create, curate, maintain, and analyze shared data assets to create an evolving, interoperable resource for the research

Box 8.3 Increased scrutiny of and constraints on private data intermediaries

Although for-profit data intermediaries have historically operated with little public awareness of their practices or even existence, society's growing unease with the private collection and sale of personal data, often without the consent of data subjects, has led to greater regulatory scrutiny in recent years.[a] The vast amount of locational data being collected by companies via smartphone apps and then repackaged for sale to advertisers, financial institutions, geospatial analysis companies, and real estate investment firms, among many others, raises additional concerns about the ultimate anonymity of data.[b] Locational data become especially valuable when they are combined with a mobile advertising ID, which allows advertisers and other businesses to integrate activity across apps.

The United States issued a high-level government report in 2014 recommending federal legislation that would subject data brokers to heightened governance rules around data security, transparency, and the degree of control held by data subjects.[c] Although no federal legislation has been passed, the state governments of California and Vermont have adopted laws requiring data brokers that collect and sell information about the residents of these states to register annually with the state government. Neither state has gone so far as to give data subjects the right to opt out of data collection and trading (although the Vermont law does require detailed disclosure of such procedures), nor has either required data brokers to disclose what data they collect and to whom they are selling data.[d] Both states require data brokers to abide by certain minimum data security standards.

In Europe, Privacy International, a European civil society organization (CSO), filed complaints in 2018 with the data protection agencies of France, Ireland, and the United Kingdom alleging that seven data brokers, credit bureaus, and ad-tech companies were violating individuals' privacy rights under the European Union's General Data Protection Regulation (GDPR).[e] The complaints claim that the companies in question build intricate, potentially inaccurate profiles of peoples' lives based in part on derived, inferred, and predicted data used as personal data, inconsistent with protections provided under the GDPR's Data Protection Principles. CSOs and governments are likely to increase their scrutiny with the spread of data broker activity, particularly if governments are perceived as failing to respond to citizens' concerns through stronger regulation and enforcement.

a. Ram and Murgia (2019).
b. Thompson and Warzel (2019).
c. FTC (2014).
d. For California, see Assembly Bill No. 1202, An Act to Add Title 1.81.48 (Commencing with Section 1798.99.80) to Part 4 of Division 3 of the Civil Code, Relating to Privacy (*Legislative Counsel's Digest*, October 14, 2019). See also Attorney General's Office, California Department of Justice, "Data Broker Registry," Sacramento, https://oag.ca.gov/data-brokers. For Vermont, see Vermont Office of the Attorney General (2018). See also Vermont Secretary of State, "Data Brokers," Montpelier, https://sos.vermont.gov/corporations/other-services/data-brokers/.
e. PI (2018).

community.[65] The Open Commons Consortium (OCC), a US nonprofit, operates data commons and cloud computing infrastructure to support research related to scientific, environmental, medical, and health care issues.[66] Since 2009, the OCC has managed the Open Science Data Cloud (OSDC), a membership-based, multipetabyte science cloud that colocates scientific data with cloud-based computing, high-performance data transport services, and common analytical tools. UK Biobank aggregates the health data of more than 500,000 individuals from the United Kingdom and makes it available to any "bona fide researcher" in the world.[67] Making public intent data available in a similar manner across government, and between government and the private sector and civil society, can promote evaluation and learning activities around existing public policy and service delivery, especially where the technical capacity to run the required statistical analyses is lacking.

Somewhat similarly, *data cooperatives* usually involve individuals who choose to contribute their personal data (while retaining ownership) in exchange for collective social and personal benefits, such as research using larger common data that would otherwise be siloed or inaccessible.[68] The objectives are generally nonmonetary. For example, patients with specific health conditions might contribute their health records to a cooperative that makes them available for medical research. LunaDNA is a community-owned platform for health research that anyone can join, share their health data, and in exchange receive ownership shares in the organization.[69]

Data intermediaries with built-in accountability mechanisms can facilitate sharing of sensitive data, including between the public and private sectors.[70] The role of these intermediaries can be played by individuals or legal structures that are positioned between data contributors and users and provide independent third-party stewardship of data.[71] In the context of public-private partnerships, they may be more effective if they are located outside government. But they can also be governed by public institutions tasked with safeguarding and facilitating data sharing across government. For example, India's 2020 "Report by the Committee of Experts on Non-Personal Data Governance Framework" identifies the Ministry of Health and Family Welfare as the appropriate trustee for data on diabetes among Indian citizens.[72]

Certain forms of these intermediaries are emerging in some jurisdictions, to support the protection of transactions involving personal data. In India, pursuant to draft legislation similar to the European Union's General Data Protection Regulation, third-party consent managers ensure that individuals are consenting to every instance of data sharing rather than "preauthorizing" data processing and sharing at the point of collection. The Reserve Bank of India has already introduced these standards across the entire financial sector. A data trust, a unique type of accountability-based data intermediary, is based on the legal structure of a "trust," and as such imposes a fiduciary duty on trustees.[73] Trustees are legally required to steward data with impartiality, prudence, transparency, and undivided loyalty toward the trust's beneficiaries, and in accordance with the trust's internal rules of governance.[74] Depending on the context, additional rules governing data access and use, as well as internal liability mechanisms for data breaches or misuse, can be tailored accordingly through contractual agreement. One of the alleged benefits of data trusts is that they offer individuals and groups a means of restoring "bottom-up" control over personal data: individuals can pool the legal rights they have over their personal data within the framework of the trust and negotiate with larger data "controllers" from there.[75]

Data trusts may be particularly useful in managing personal health data in the context of COVID-19 contact tracing in which deidentified data on test results can be shared (with data protection safeguards) and used to alert other individuals if they are at risk of infection.[76] Data trusts can also support the responsible collection and reuse of sensitive health data to support academic research or public health monitoring. Data trusts are still largely theoretical constructs. However, examples are beginning to be piloted,[77] given growing interest in such mechanisms to promote accountability and rebalance collective bargaining powers between data providers and users. In countries with an enabling legal system, data trusts can create unique opportunities in low-capacity contexts, and especially in countries with weak data protection legislation and enforcement. Certain countries and organizations have taken a broader definition of data trusts (which creates an accountability role without necessarily imposing a strict fiduciary duty) to pilot their effectiveness in practice. Such structures have been explored for use in the fight against illegal wildlife poaching in lower-middle-income countries by the UK government. WILDLABS is a community working to discover and implement technology-enabled solutions to conservation challenges, and the Open Data Institute (ODI), a London-based nonprofit organization, is creating more open and trustworthy data ecosystems. These arrangements are a low-cost, secure means for the conservation community to collect and share data, while overcoming shortcomings in local laws and enforcement, as well as limited resources.[78] Data trusts or other contractual data sharing structures can also facilitate cross-border data transfers, especially where international data sharing agreements do not exist. The Microsoft Intelligent Network for Eyecare (MINE), a collaboration between Microsoft India and India's L V Prasad Eye Institute, facilitates the transfer of patient data from a diverse range of countries to the United States, where participating research institutes then use advanced analytics and machine learning to inform the development of strategies to prevent avoidable blindness and scale delivery of eye care services worldwide.[79]

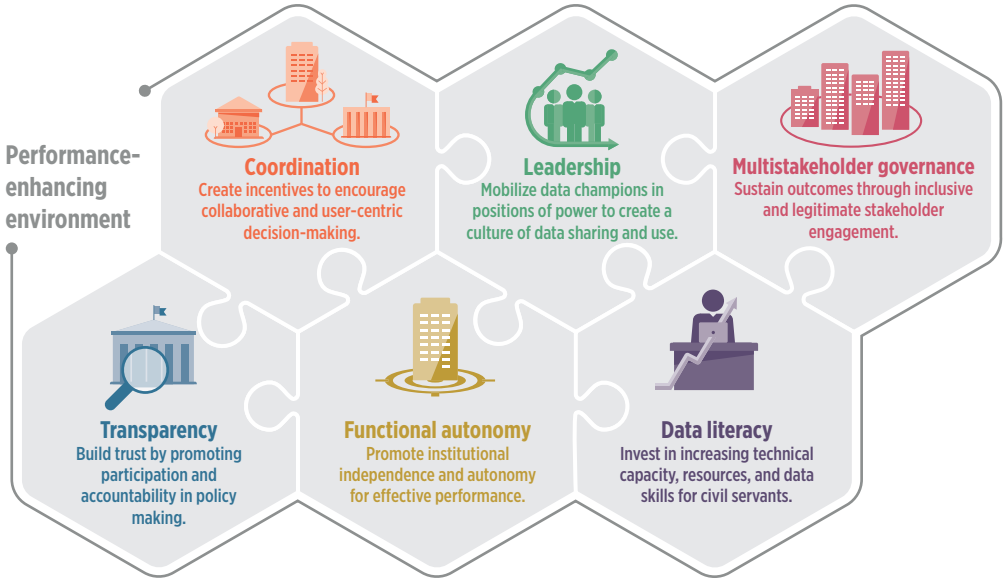
Making data governance institutions effective

No matter the country context, institutions can only carry out their roles effectively if their staff are capable of and willing to use good data to undertake their core operations, inform policies, and deliver services (figure 8.7). Countries that have made great strides in improving data governance implementation across the whole of government have typically benefited from the leadership of a strong political champion of the importance of data.

Increasing technical capacity, resources, and data literacy for civil servants

The cognitive challenges posed by data are unlike those of most other commodities in terms of

Figure 8.7 Features of well-functioning institutions for effective data governance



Source: WDR 2021 team.

understanding the scale and complexities of (potential) use. Governing data thus requires a strong technical capacity and investments in human capital development for those who collect, process, analyze, and use data to support evidence-based policy making, core government operations, and service delivery.[80] Investing in technical capacity is also essential when regulating data-driven businesses (see chapter 7). The public sector will need resources to meet the increasing demand for data analytics and information technology (IT) skills (see chapters 4 and 5), especially with the shift to digital government.

Data literacy, which refers to an individual's capacity to "read, work with, analyze, and argue with data," is particularly weak in government institutions in low- and middle-income countries.[81] Skilled staff may be concentrated in ministries of finance or planning, as well as in entities responsible for the production and quality of statistics, such as NSOs. Strict salary scales and wage caps within most public sector entities affect their ability to compete with the private sector in recruiting specialized staff.

Building data literacy requires investing in training to develop a range of technical competencies in data collection, management, and interpretation across the data life cycle, including data protection and security.[82] Training also should empower civil servants to examine data for inaccuracy and bias and to contextualize data, including through effective visualization and communication techniques.[83] These tasks require cooperation between data specialists (such as data officers and IT staff) and technical staff in sectoral or cross-cutting entities.

Public sector training institutions may have the requisite organizational role and resources to support the development of specialized training courses.[84] Where local resources are lacking, or to further bolster domestic capacity, international nonprofit institutions could provide up-to-date, standardized training programs in collaboration with entities that traditionally train civil servants. These programs could be specific to certain areas or sectors, such as the multijurisdictional training and certification on data protection of the International Association of Privacy Professionals (IAPP) or the Open Data Institute's training to support open government data. Other organizations provide more tailored training to meet user needs, such as that by the GovLab Academy[85] or Apolitical.[86] Certification schemes can help support compliance by harmonizing training requirements.

Institutions should also ensure that human resources and staffing needs are planned for and managed through national capabilities plans or other instruments. Institutional mandates and staff terms of reference should be redefined to incorporate data governance functions and prescribe standardized guidelines for handling data properly.

Chapter 9 discusses how, beyond the public sector, governments should invest in programs to build data literacy within the broader population to reduce

the digital divide and empower people to use data to improve their lives.

Creating a culture of performance that supports a data-driven public sector

Even when institutions have the necessary technical infrastructure and de jure frameworks, shifting policy makers away from traditional and often siloed decision-making toward data-driven and coordinated policy design and implementation depends on creating the right incentives. These incentives are a combination of institutional management practices and cultural norms that are especially relevant to low- and middle-income countries, where reform efforts are often stymied by "implementation gaps" resulting from behavioral and political economy constraints. Research conducted in Ghana finds that innovation in public agencies with fixed hierarchies may partly constrain innovation by impeding the acceptance of ideas from subordinate civil servants.[87] At the organizational level, institutional fragmentation, the large transaction costs of information sharing, and budgetary allocations can create incentives to restrict access to data or keep data siloed.[88]

Investments in change management and other techniques are essential to increasing the buy-in to and impact of data governance reforms.[89] These tools should be deployed within a strategy of change management that is adapted to the organizational culture of an institution[90] and broader political economy considerations.[91]

Mobilizing "data smart" political champions who view data as foundational. Strong political champions or a political culture that appreciates and understands the value of data are critical to ensuring the effectiveness of change management reforms. Countries at the forefront of leveraging greater value from data through better data governance frequently have strong advocates of the value of data in positions of power. Estonia, with its decades-long history of leadership by data advocates, has invested in improving the data science skills of the general public.[92] As a result, it is the first country to allow online voting in its general elections, and essentially all public services are available online.

Adopting a collaborative leadership approach to decision-making. Collaborative leadership is a central feature of effective change management. Leaders seek a diversity of opinions and ideas among teammates in building strategies and solving problems.[93] Governments can benefit from collaborating with the relevant entities across the public sector and with nongovernmental stakeholders such as civil society and private sector organizations to identify challenges and prioritize key drivers of change.[94] In Tunisia, the government's decision to adopt a collaborative leadership approach to drafting its latest open data decree was an important shift from its previously unsuccessful efforts that had resulted in siloed and fragmented initiatives and limited results. By convening more than 50 officials from across the Tunisian public administration and several CSOs, the government was able to gather diverse views on the best-fit options to include in the decree.[95] This collaborative process was led by a unit in the Prime Minister's Office, thereby endowing the effort with high-level support and ownership.[96]

Deploying effective communication and dissemination strategies to increase actual and perceived transparency and promote trust in the process. In environments characterized by low levels of trust, effective collaboration may have to begin by addressing underlying conflicts. Such a process can generate creative solutions and important trade-offs.[97] Perceived increases in transparency and accountability, including diverse representation in stakeholder groups, are key to fostering trust.[98] Communication is also essential to support enforcement of rules in novel situations. For example, during the COVID-19 pandemic guidance from the European Commission and the European Data Protection Board[99] helped national data protection authorities, governments, businesses, and civil society stakeholders understand how to build interoperable data sharing efforts and technologies (such as privacy-preserving contact tracing applications) for health monitoring and policy making while complying with the GDPR.[100]

Creating incentives and reward mechanisms that encourage innovation and coordinated decision-making in the public sector.[101] Salaries and bonuses can be effective incentives or rewards, but in low-capacity environments where funds are restricted, awarding prizes or other monetary incentives can incentivize collaboration and performance in the public sector.[102] In Morocco, since 2015 the Ministry of Economy, Finance and Administrative Reform has awarded the annual e-mtiaz prize to support competition between public sector entities and service providers in adopting innovative tools and services that improve the quality of public service delivery through e-administration, including the development and use of e-services.[103]

A data-driven culture can also be supported through "hackathon" initiatives and competitions in which data users are encouraged to collaborate for a short period of time on a project. In 2019 the Tunisian Court of Accounts organized a "Hack 4 Transparency"

event to support objectives that included collecting, processing, exchanging, mining, and analyzing public financial data; improving communication with external stakeholders; and improving transparency, accountability, and participation in the use of public funds. The winners of the five regional hackathons and the subsequent national final received cash prizes offered by the private sector.[104]

Promoting institutional independence and autonomy for better performance

De facto autonomy—defined as the actual scope of independent decision-making powers and influence over (and protection from) other institutions in the governance system[105]—is critical to institutional performance and successful implementation of policies or legal frameworks.

Within institutions, performance depends on staff having sufficient autonomy to make informed, innovative decisions.[106] Independence may also be important to ensure the integrity of the data processed by an institution. Identification agencies that process personal data, including potentially sensitive data, about the population and the various services and benefits they receive should be able to resist undue access to this data by those who might misuse it. Similarly, NSOs that produce reliable, objective data for public policy making and administration must not be swayed by political interests that may wish to downplay, distort, or conceal inconvenient statistics. Beyond incentivizing performance, institutional independence and autonomy can strengthen accountability mechanisms in the data ecosystem. Performance reporting and audits are more trustworthy when they are conducted by impartial institutions.

An institution may operate with significant de facto (actual) independence regardless of its de jure (formal) status.[107] Nonetheless, public sector institutions often require de jure independence so they can undertake the activities falling within their mandate. The need for institutional independence is critical when both government and nongovernment entities are regulated within the same framework and competitive neutrality is required. It is also critical when decisions can have a significant impact on interests and actual and perceived impartiality in the execution of governance functions is needed.[108] Entities playing a rule-making or compliance function, such as DPAs, regulators, audit institutions, and courts or independent ombudspersons, need to be formally independent in order to effectively oversee compliance of other entities and to provide an impartial venue for redress and remedy.

Formal independence has legal, financial, and administrative dimensions. Legislation can define roles and responsibilities and establish formal protections. It may be necessary to establish a legally autonomous institution with formally delegated authority, especially for regulators, oversight institutions, and NSOs.[109]

Financial independence relies on institutional funding free from day-to-day political or private influence. Such independence can be supported by putting in place the appropriate procedures for proposing and approving budgets. In Ethiopia, the Philippines, and Rwanda, NSOs are authorized to formulate their own budgets flexibly, based on the demands made on them through national development plans and other routine activities in the statistical system, such as periodic censuses. Providing funding on a multiyear basis rather than every year can increase stability and protect institutions from short-term political change. Institutions may also be able to raise funds directly through licensing fees, enforcement penalties, and administrative charges.[110]

Administratively, key positions may be politicized by the executive or be vulnerable to state capture and corruption. Independence may be enhanced by establishing precise, transparent criteria for selecting and appointing qualified leaders. Candidates should be required to disclose conflicts of interest.[111]

Achieving better coordination across institutions for better data governance

Coordinating for better data governance. Coordination across institutions helps prevent siloed or uneven application of data governance functions based on opportunities and capacity. Coordination can ensure that data governance processes, such as technical standards, rules and means of audit, remedies in case of noncompliance, and M&E frameworks, are consistently applied and, where relevant, can identify emerging areas for action. Useful outputs could include guidance notes or technical manuals that provide detailed instructions on how to harmonize knowledge and implementation efforts across institutions.

Successful coordination depends at the outset on clearly allocating and delineating the roles and responsibilities of data governance institutions. Institutions or individuals tasked with coordination should then create robust processes to guide and govern their interactions and track their efficacy. Coordinating entities should also be sufficiently empowered by high-level leadership to effectively undertake this role. The structure and formality of coordination mechanisms will vary. Some countries have chosen

to designate a central coordinating institution or individual located within the executive. In Albania, the Albanian National Agency for Information Society is under the direct supervision of the Prime Minister's Office. France has taken a similar vertical approach. The chief data officer (*administrateur général des données*) works directly under the authority of the prime minister. Centralizing coordination responsibilities and oversight in this way facilitates a strong hierarchy with direct supervision entities that review, revise, and approve plans and initiatives from subordinates and oversee their implementation.[112]

In other contexts, horizontal coordination mechanisms may involve networks of "peers" at the same functional or hierarchical level.[113] These types of coordination are often carried out by interagency committees or working groups. In the United States, 24 government agencies are required to designate an employee (civil servant) who is not a political appointee as their chief data officer. The officer is charged with convening and coordinating agency data governance and interagency coordination.[114] Chief data officers coordinate with one another through the Chief Data Officers Council. They also coordinate with other government councils that conduct data-related activities.[115]

Because of the cross-cutting nature of data governance and the scale of the challenge, stakeholders would benefit from a range of coordination mechanisms to leverage their relative strengths and reinforce one another. Centralized coordination can reduce transaction costs, compared with the more horizontal approaches to coordination, although consolidating too much power in a single entity can heighten the risk of mismanagement and abuse.

Coordinating for better data use. Ministries and government agencies collect, manage, and use data, whether in the form of tax returns, the outcomes of social or business programs, research, fuel consumption statistics, health data, immigration flows, geospatial maps, land management results, or crop inventories. However, data management platforms across ministries are often limited and lack unified interoperability standards, leading to duplication in data production and IT procurement. These issues may be compounded by a broader culture of rivalries and lack of collaboration within the public sector. As a result, data generated in the public sector may be consigned to data wastelands, captured in siloed repositories and platforms. Adherence to established norms and standards and efficient use of shared digital platforms to integrate and share data can improve government efficiency and public service delivery through administrative simplification and shared services.

Ensuring the transparency and accountability of public sector institutions

To encourage the transparency and accountability of data governance institutions, policy makers should offer opportunities for scrutiny and input. Public consultation and inputs on the design of policies and laws and regulations can support transparency and stakeholder engagement.[116] Institutions should be required to publish and review their objectives and performance indicators during regular planning cycles. Peer-to-peer scrutiny can be enhanced through formal processes or technical working groups, depending on the institutional culture and needs.[117]

In addition to regular review procedures, institutions could open their records and reports for review. In some cases, audit by independent third parties, including NGOs, using international standards and benchmarks with a view toward identifying areas of underperformance or noncompliance, may incentivize institutional accountability. The transparency of such processes is enhanced if the results of the audit are shared with the public through either publications or public hearings. Public knowledge and review of the performance of institutions are critical to building and maintaining confidence and trust in data governance institutions. Civil society's role in supporting trusted data use and reuse is also reflected in newer forms of community-led data governance and oversight mechanisms. For example, the UK's Connected Health Cities project in Manchester convenes a "citizens' jury" to hear expert evidence before approving an approach for the project.[118]

When institutions prioritize datasets for publication on an open data platform, stakeholder input in the process can ensure that priorities are based on user demand rather than on government preferences or judgment alone. Greater transparency and collaboration could increase the use of open data by nongovernmental actors, which, in turn, could increase research and advocacy opportunities, as well as innovation and private sector development.

Sustainable outcomes through inclusive multistakeholder governance

As the digital economy has expanded globally, an increasingly complex, geographically diverse group of stakeholders has become active in the data ecosystem. However, traditional concepts of governance

based on national sovereignty or strict multilateralism do not take into account these dynamics. A multistakeholder approach to data governance is better equipped to govern the complex data ecosystem in a transparent, inclusive, and distributed way, which reflects the interests of all key stakeholders. This approach is aligned conceptually with the successful application of multistakeholder processes designed to govern the internet.[119] And it is an essential component of the "trust framework" that strengthens the social contract around data use. It will be especially important as data governance shifts toward international harmonization of policies, rules, and standards.

"Multistakeholderism" is an approach to data governance, not an end in itself. It is intended to facilitate better, more sustainable outcomes by enabling all stakeholders to undertake their roles in a coordinated manner.[120] These outcomes include ensuring more robust and flexible data governance frameworks that respond to the pace of technological change[121] and improving the transparency and legitimacy of and buy-in to the process (see box 8.4).[122] More broadly, this approach can contribute to achieving a more equitable distribution of the value of data, as well as protection from any harm arising from data misuse.[123] More equitable distribution emerges when traditionally excluded groups—including lower-middle-income countries, small and medium enterprises (SMEs), CSOs, and indigenous peoples—are able to participate and benefit from the technical expertise in these forums (see spotlight 8.2).

A continuum of multistakeholder arrangements.[124] Although some areas of data governance (such as setting standards for interoperability) may accommodate or even require a more deliberative, consensus-based approach dominated by technical experts, the development of policies and laws and regulations will inevitably involve some form of top-down, final decision-making by a government agency or a regulator (such as developing mechanisms to ensure data security, which may need to be centralized).[125] In such cases, nongovernmental actors may play more of a nonbinding consultative role, providing inputs in the policy-making or rule-making process.[126] These actors will have an important role to play in developing "soft law" mechanisms (chapter 6), research, training, and advocacy.

Leading successful examples of multistakeholder initiatives that develop technical standards for internet (and increasingly data) governance include the World Wide Web Consortium (W3C) and Internet Corporation for Assigned Names and Numbers (ICANN). Although they differ in structure, both organizations are constituent-driven, developing their governance processes and outputs using a bottom-up, participative approach. Meaningful participation of civil society and other nongovernmental groups is assured through their inclusion in formal decision-making structures.[127]

Like stakeholder roles, the type of forum designed to host multistakeholder governance processes should be purpose-driven. Concerns about restricting access to commercially sensitive or confidential data and processes may at times limit participation to members. Other issues, particularly those of societal importance such as the use of facial recognition in the public sector, may require unrestricted forums for debate.[128]

For all its advantages, the multistakeholder approach poses various challenges. Self-regulation frameworks, including voluntary codes of conduct, developed through multistakeholder processes are effective only if strong domestic enforcement mechanisms are in place.[129] Even for a consensus-based and stakeholder-driven rule-making process, weak enforcement and outcomes may reduce stakeholder buy-in. In addition, legitimacy and buy-in may suffer if the process is merely consultative rather than using stakeholders' inputs to shape outcomes. Meaningful participation of underrepresented or marginalized groups can be difficult, particularly for new market entrants such as start-ups or SMEs, smaller CSOs and NGOs, or indigenous peoples.[130] Barriers to effective multistakeholder participation can also be found in international data governance arenas. Lower-middle-income countries may find it difficult to participate as co-designers or "standard setters" and find themselves limited to being "standard-takers" (see chapter 7).[131]

Finally, stakeholders need to guard against use of the multistakeholder approach by government and others to legitimize top-down decision-making that leads to an accumulation of power. Where accountability mechanisms are lacking, the multistakerholder approach can be misused to exclude other parties (whether in the public or private sector or civil society).[132] Designing inclusive forums and accountable processes and earmarking resources to enable the participation of traditionally underrepresented stakeholders will be key to the success of such processes. Creating bottom-up approaches to data governance designed around multistakeholder engagement can help realign power asymmetries and improve contestability in the current social contract on data (see box 8.4).

Box 8.4 Building multistakeholder data governance into smart city initiatives through "digital democracy"

Smart cities combine sensors and other technologies with physical infrastructure and services to enhance the lives of their residents.[a] Investments usually target sectors and services such as transportation, utilities, and law enforcement. Meanwhile, public-private partnerships are often used to leverage the technical and innovation capability of the private sector by outsourcing infrastructure and data management.[b] Because these initiatives involve the continual collection of personal or nonpersonal data from embedded sensors,[c] governance structures are needed to ensure that the data collected from citizens are used responsibly for public intent rather than commercial use and that residents retain control over their data. The need for robust data governance in this area will become more acute as the uptake of smart cities increases against a backdrop of growing urbanization worldwide.[d]

More inclusive decision-making about data collection and use is being facilitated by bottom-up models of collaboration. Barcelona was one of the first cities to leverage the analytical opportunities of the Internet of Things (IoT) and combine datasets to improve evidence-based policy making and service delivery. And it was one of the pilots for the European Union's DECODE initiative. DECODE is exploring how to build data-centric digital economies in which data generated and gathered by individuals, the IoT, and sensor networks are made available for collective use, while making sure that individuals retain control over their data and their personal data are safeguarded.[e] Barcelona's City Council partnered with the city's digital democracy platform to publish data collected by sensors and other means on the Decidim platform[f] to promote transparency and accountability in decision-making.

In Belgium, Ghent has developed a collective governance model. In its "City of People," citizens can create online profiles on the platform Mijn Ghent (My Ghent), which they can use to access public services such as libraries and child care.[g]

Such digital democracy platforms have been replicated in lower- and middle-income countries. For example, Morocco's Fikra e-participation platform collects citizen feedback and generates community-driven ideas to improve public service delivery.[h]

a. Maddox (2015).
b. Copenhagen has created a public-private partnership with Hitachi to assess how to monetize datasets. Abu Dhabi has partnered with a Swiss telemedicine company to improve health care. And Singapore's Smart-Nation initiative is relying on a network of start-ups to provide the government with technology and data-driven services. See MGI (2019).
c. Scassa and Vilain (2019).
d. According to Cisco Systems, more than 60 percent of the world's population will live in cities by 2050. See Mitchell et al. (2013).
e. See DECODE, "Giving People Ownership of Their Personal Data," Barcelona, https://decodeproject.eu/.
f. See "Construïm la Barcelona que volem!" decidim.barcelona, Barcelona, https://www.decidim.barcelona/.
g. Tannam (2018).
h. See e-Government Program, Kingdom of Morocco, "e-Participation Platform: FIKRA," http://www.egov.ma/en/e-participation-platform-fikra.

Assessing the institutional foundation through the lens of a maturity model

Recommendations for improving the institutional foundations of data governance at the national level can be tailored to a country's current level of institutional development. Based on the maturity model introduced in chapter 1, recommendations for assessing and improving institutions are presented in the sections that follow.

Establishing fundamentals

Any gaps and weak links in a country's institutional arrangement for data governance will be revealed by first taking stock. In many countries, especially lower-income ones, infrastructure, data collection and processing, and technical capabilities in the public sector are generally uneven. At best, certain "islands of excellence" may be using data effectively for decision-making or service delivery on an ad hoc basis, but without a clear strategic orientation or executive-level leadership of the data governance agenda. As a result, duplication of data is common, interoperability infrastructures are lacking, and the institutions needed to ensure the security, integrity, quality, and protection of data are minimal.

Countries should begin by establishing a baseline for assessing the capabilities of the existing institutions to facilitate the secure generation and flow of data among all data producers and users (recognizing that many actors are both producers and users of data). This analysis should be purpose-driven, with a view toward understanding the activities already

taking place—either inside or outside of government—that may be development opportunities, along with the risks. The analysis should distinguish between the stated function of institutions and what they actually deliver. As one example, the African Union Commission's Malabo Convention supported the harmonization of the regional policy and legal framework for cybersecurity and data protection across Africa,[133] but institutions working in support of the convention have often come up short, in part because of the underrepresentation of local DPAs to enforce agreements of the convention.[134]

This stocktaking should examine institutional relationships as they interact with the private sector and civil society. It would then serve as a springboard to developing institutional arrangements that promote the production and flow of data between these actors. These institutions and initiatives can provide market participants with the confidence in and certainty about the rules of the game, reduce risk, and increase capacity and the incentives for firms to use data for economically and socially productive purposes.

Initiating data flows

Once it is clear how well the existing institutions are promoting the secure production and flow of data, work can begin to fill in gaps and strengthen their capabilities. Not all gaps have to be filled by public institutions. Domestic or international academic institutions, CSOs, international organizations, and research institutions could help fill capacity gaps in government. Depending on the local context, a government agency or unit (new or existing) could be given responsibility for establishing a strategic plan to promote greater use of data to improve public policy, the efficiency of the private sector, and the informational awareness of the population—all within the agreed-on parameters of the social contract for data. This entity should have sufficient leverage across the public sector agencies that govern or manage data and should reside at the center of government under high-level executive leadership.

Institutions should coordinate the development of standards to ensure data quality and data integration capabilities across government. This effort would include developing an integrated data management architecture for public intent data that curates, maintains, and facilitates secure data sharing and reuse across government. Data trusts or other contract-based mechanisms could continue to play an important role in promoting access to private intent data in areas in which public institutions, rules, and enforcement remain weak and fail to address the concerns of data owners and data subjects. At the same time, institutional arrangements should be developed to encourage and enforce compliance with rules established to promote the dissemination and safe use of data.

Signs of a maturing system will include adequate technical capacity, sufficient resources, clear roles and responsibilities, and a high level of data literacy. Extensive training—for both civil servants and citizens—to overcome digital literacy barriers and enable data management and use will also be part of the maturation process.[135] To engender trust and increase their transparency and accountability, institutions should also be required to publish annual plans and reports on their activities. Furthermore, certain institutions, such as regulators, NSOs, and data protection authorities, must be protected from undue political and commercial influences.

Optimizing the system

To maximize the value of data, institutions need to support a whole-of-government approach to the management of data. Capacity-building and communication efforts should be directed at training civil servants to use data for results, including better decision-making, performance monitoring, and service delivery. To strengthen a data-driven culture in the public sector, reward mechanisms such as prizes and performance-related pay can incentivize civil servants to pursue innovations and engage in collaborative decision-making. With sufficient investments in data institutions and the technical skills of civil servants, critical processes and service delivery channels can become automated and interconnected.

Establishing processes for data quality assurance, data integration, and data synchronization should be integral parts of data management at this stage. Institutions should similarly fully integrate stakeholder feedback mechanisms into data flows, thereby helping to increase the transparency and quality of processes. Ministries and agencies should share data via common platforms subject to robust data protection safeguards, which limit consolidated access to and control over large volumes of personal data.

Finally, institutions should be regularly monitored[136] and evaluated, with the results informing adjustments in resources and policies. Both should be adapted to cope with disruptive technologies and services as data generation (and use) continues to grow in both volume and variety.

To meet the challenges from cross-border data transfers associated with safeguarding and enabling

the use of both personal and nonpersonal data, institutions should coordinate at the regional or international level.[137] Such global efforts toward data governance should be recognized and promoted[138] and should enable convergence in the development of high-level principles to guide the design and implementation of national-level data governance frameworks (see spotlight 8.1).[139] These efforts should protect the interests of poorer nations in international negotiations on data issues in which they may have a limited voice.

No one-size-fits-all approach can be prescribed for every context. The maturity model is dynamic, and institutions will need to continually learn and improve to move to the next level. This approach can be applied equally to countries with low maturity and low resources and those with high maturity and high resources.

Notes

1. Harrison, Pardo, and Cook (2012).
2. One class of platforms is software infrastructure, which can include civil registration and vital statistics systems, digital identification systems, population registries, sectoral information management systems, data catalogs, data architecture (one of the pillars of enterprise architecture), Government Service Bus, interoperability frameworks, data lakes and warehouses, webservices and application programming interfaces, eTrust services, cybersecurity solutions, and privacy-enhancing technologies. These platforms are essential components of soft infrastructure.
3. Aghion and Tirole (1997).
4. Bergstrom, Blume, and Varian (1986).
5. Arraiz et al. (2019); Brown et al. (2019).
6. Government of Mexico, Datos Abiertos de México (database), https://www.datos.gob.mx/.
7. See Shapiro and Varian (1998).
8. See Abraham, Schneider, and vom Brocke (2019) for a review of this literature.
9. ASEAN (2012); OECD (2019b).
10. Many of the data governance functions included here coincide with those proposed by the British Academy and the Royal Society (2017b). Their report "Data Management and Use: Governance in the 21st Century" distills three groups of essential data governance functions: (1) anticipate, monitor, and evaluate; (2) build practices and set standards; and (3) clarify, enforce, and remedy. The report also argues for a single body to act as steward of the data governance landscape.
11. Principles—such as certainty, transparency, accountability, nondiscrimination, fairness, inclusiveness, openness, necessity, proportionality, and security—need to be developed to link data management practices to positive uses and behaviors to improve lives (see chapter 6). They also help identify practical steps for a data strategy along the data life cycle and ensure that data are valued as a strategic asset. An example is the US Federal Data Strategy. See Office of Management and Budget, "Federal Data Strategy: Leveraging Data as a Strategic Asset," Washington, DC, https://strategy.data.gov/.
12. The targets also include intermediate milestones and measurable key performance indicators (KPIs) to support monitoring and evaluation activities.
13. OECD (2018).
14. Brown et al. (2019).
15. Quay (2010).
16. Blair (2011).
17. Cheruiyot, Baack, and Ferrer-Conill (2019); Deloitte (2012); Garcia (2007); Gopal Jayal (2007); Grandvoinnet, Aslam, and Raha (2015); Hanna (2012); Hjalmarsson, Johansson, and Rudmark (2015); Malena (2004); Paul (2011); Peruzzotti and Smulovitz (2006).
18. Carson and Hartz-Karp (2005); He (2011).
19. Kpundeh (2000); World Bank (2017).
20. World Bank (2002, 4).
21. The DGSS data on which figure 8.3 is based were collected by visiting government, CSO, and other relevant websites. Most governments have a substantial web presence, and information on data governance is visible on their websites. However, the data do not capture institutions without a web presence. See World Bank, DGSS (Digital Government/GovTech Systems and Services) (dataset), https://datacatalog.worldbank.org/dataset/digital-governmentgovtech-systems-and-services-dgss-dataset.
22. These statistics are based on Data Governance System and Services (DGSS) data for 198 economies. See World Bank, DGSS (Digital Government/GovTech Systems and Services) (dataset), https://datacatalog.worldbank.org/dataset/digital-governmentgovtech-systems-and-services-dgss-dataset.
23. Bertelli et al. (2020).
24. The national statistics office of Thailand, the Electronic Transactions Development Agency, and CAT Telecom Public Company Limited (a state-owned enterprise that runs the country's international telecommunications infrastructure), among other agencies, were consolidated under the Ministry of Digital Economy and Society.
25. SGD (2020).
26. PARIS21 (2017).
27. See, for example, Fölscher and Gay (2012); Sjoberg, Mellon, and Peixoto (2017).
28. Wilson (2019).
29. African Union (2020).
30. Martínez Pería and Singh (2014).
31. Gunningham and Rees (1997); Gupta and Lad (1983).
32. Gunningham and Rees (1997); Gupta and Lad (1983).
33. See the website of the International Organization for Standardization, https://www.iso.org/about-us.html.
34. UNSDG (2017).
35. Informal or internal mechanisms may be especially effective if combined to provide multiple avenues for incentivizing compliance. This is one of the strengths of a multistakeholder approach to data governance.
36. United Nations (2014).

37. Turianskyi et al. (2018).
38. This delistment was accompanied by an invitation to return to EITI when implementation obstacles had been removed (which as of this writing has occurred).
39. See Latin American Open Data Initiative (Iniciativa Latinoamericana de Datos Abiertos), GDB (Global Data Barometer) (dashboard), https://globaldatabarometer.org/.
40. The Moroccan Data Protection Law of 2009 provides for fines of up to DH 300,000, depending on the severity of the violations. In certain cases, prison sentences can be issued for between three months and two years (Kettani 2017).
41. Kin (2020).
42. See Commission Nationale de l'Informatique et des Libertés, "What You Should Know about Our Standard on Data Protection Training Programmes," https://www.cnil.fr/en/what-you-should-know-about-our-standard-data-protection-training-programmes.
43. Bundeskartellamt (2019). A plug-in is a piece of add-on software that helps make the base software do what it does not normally do by itself. Plug-ins (also known as extensions or add-ons) are downloaded and installed to make the software being used more feature-rich (O'Neill 2020).
44. Richardson, Hendrickson, and Boussina (2018).
45. Gauri (2011).
46. A CSIRT is known, among other designations, as a Computer Emergency Response Team (CERT); Incident Response Team (IRT); Computer Security Incident Response Capability or Center (CSIRC); Computer Incident Response Capability or Center (CIRC); Computer Incident Response Team (CIRT); Incident Handling Team (IHT); Incident Response Center or Incident Response Capability (IRC); Security Emergency Response Team (SERT); or Security Incident Response Team (SIRT).
47. See chapter 6 for data on cybersecurity legislation collected through the Global Data Regulation Survey.
48. See Data Governance Network, IDFC Institute, Research (document and data repository), Mumbai, India, https://datagovernance.org/research.
49. British Academy and Royal Society (2017a).
50. Examples are the Centre for Data Ethics and Innovation in the United Kingdom; the Ethics of AI Lab at the University of Toronto in Canada; and the Ethics and Governance of Artificial Intelligence Initiative at the Massachusetts Institute of Technology and Harvard University in the United States.
51. Examples are the Global Partnership for Sustainable Development Data and the World Data Forum.
52. O'Donnell and Keller (2020).
53. Wylie and McDonald (2018).
54. Hill, Stein, and Williams (2020).
55. Shkabatur (2012).
56. FTC (2014).
57. WebFX Team (2020).
58. Deichmann et al. (2016).
59. See Governance Lab, Tandon School of Engineering, New York University, "Data Collaboratives," Brooklyn, NY, https://datacollaboratives.org/.
60. Bernholz (2016).
61. Rodian (2018).
62. GS1, "How GDSN Works," Ewing Township, NJ, https://www.gs1.org/services/gdsn/how-gdsn-works.
63. Lundqvist (2018).
64. World Bank (2021).
65. Grossman (2019); Grossman et al. (2016); Hardinges and Tennison (2020).
66. See the Open Commons Consortium website, https://www.occ-data.org/.
67. See the UK Biobank website, https://www.ukbiobank.ac.uk/learn-more-about-uk-biobank.
68. Pentland and Hardjono (2020).
69. See the LunaDNA website, https://www.lunadna.com/about/.
70. Wylie and McDonald (2018).
71. Bernholz (2016); Hardinges (2018).
72. MeitY (2020).
73. Delacroix and Lawrence (2019).
74. Hardinges (2020).
75. Delacroix and Lawrence (2019); ODI (2019).
76. Bengio (2020).
77. Platform Info Exchange is a UK-based nonprofit trade union for rideshare drivers such as Uber. The organization helps these "gig workers" access, analyze, and inform decisions using the personal data collected about them while they are working, through class action data requests. This work is designed to create a worker-led data trust downstream. Platform Info Exchange is funding this pilot through a fellowship received in January 2021 by Mozilla's Data Futures Lab. See https://foundation.mozilla.org/en/blog/announcing-3-new-awards-to-fuel-better-data-stewardship/.
78. WiredGov (2019).
79. Microsoft News Center India (2016).
80. OECD (2019b).
81. Bhargava and D'Ignazio (2015).
82. Skills should be developed to support the collection or acquisition of data (purpose-driven data collection), the management and curation of data (managing the data life cycle and promoting interoperability), and the analysis, visualization, and other uses of data across their life cycle.
83. Egle and Zahuranec (2020); OECD (1997).
84. OECD (1997).
85. See Governance Lab, Tandon School of Engineering, New York University, "Solving Public Problems with Data," Brooklyn, NY, http://sppd.thegovlab.org/.
86. Apolitical has a number of resources and courses on using data better in the public sector. See the Apolitical website, https://apolitical.co/home.
87. Williams and Yecalo-Tecle (2020).
88. Brown et al. (2019).
89. Management Concepts (2016).
90. Campbell and Sandino (2019).
91. See, for example, Nauheimer (2015); UNDP (2006).
92. *Economist* (2013).
93. Ibarra and Hansen (2011).
94. CL4D (2016).
95. See Open Government Partnership program, "A Workshop for Representatives of Public Structures on the

Open Data Order Project," Tunis, Tunisia, http://www.ogptunisie.gov.tn/?p=226.

96. These efforts were supported closely by the World Bank as part of technical assistance under the Moussanada Multi-Donor Trust Fund.
97. Weiss and Hughes (2005).
98. Carr and Walton (2014). Social accountability committees can be a helpful vehicle to promote legitimacy and impact through multistakeholder decision-making (World Bank 2020).
99. For example, see EDPB (2020).
100. eHealth Network (2020); EU (2020).
101. Mazzucato (2018).
102. Camera, Casari, and Bigoni (2013).
103. Recent applications or services that have won awards include the geoportal for the Urban Agency of Errachidia-Midelt, the e-upgrade for Royal Air Maroc (the national airline), and the online portal for the Moroccan pension fund (Caisse Marocaine des Retraites). See Ministry of Economy, Finance, and Administrative Reform, "Prix National de l'Administration Electronique e-mtiaz," Rabat, Morocco, https://www.mmsp.gov.ma/fr/decline.aspx?m=4&r=218.
104. The hackathon was supported by the World Bank through the Moussanada Multi-Donor Trust Fund. In addition to the main competition, teams that did not proceed to the final still had an opportunity to present their solutions to the Court of Accounts for the following challenges: decentralization and local governance; citizen participation in the audit process; and simplification of, disclosure of, and follow-up on audit recommendations.
105. Bach (2016).
106. For a useful definition of autonomy in the public sector, see the autonomy index developed by Rasul, Rogger, and Williams (2018). It captures "the extent to which bureaucrats of all levels are empowered to make meaningful contributions into policy formulation and implementation processes, and the flexibility with [which] bureaucrats can use their discretion in responding to project peculiarities and introducing innovations" (Rasul, Rogger, and Williams 2018, 3).
107. Gilardi and Maggetti (2011); World Bank (2017).
108. OECD (2012).
109. OECD (2017).
110. Blackman and Srivastava (2011).
111. OECD (2017).
112. Peters (2018).
113. Peters (2018).
114. See the Foundations for Evidence-Based Policymaking Act of 2018, Pub L. No. 115–435, 132 STAT. 5529 (2019), which applies to 24 agencies identified in the Chief Financial Officers Act of 1990 (CFO Act) in 31 U.S.C. §901(b). For more information, see DOJ (2020).
115. See OMB (2020).
116. Johns and Saltane (2016).
117. Arizti et al. (2020).
118. NHSA (2020).
119. WGIG (2005).
120. DeNardis and Raymond (2013).
121. Effective multistakeholder approaches to policy design and implementation can increase the responsiveness of government, compared with the traditional top-down approaches or rule making that tend to lag behind the pace of technological change and may become obsolete by the time the legislative process is completed and regulations are adopted.
122. Multistakeholder approaches can also increase buy-in among stakeholders, so long as they are adequately represented, their interests are considered, and their preferences are reflected (to the extent possible) in policy setting, design, and implementation.
123. In bringing divergent interest groups together, multistakeholder approaches to data governance can balance differing priorities to broker agreement on the systems to be adopted for the use, reuse, and sharing of data for development. For example, the multistakeholder approach can facilitate convergence on (1) the principles, norms, and standards for data collection and use; (2) the tools and mechanisms (technical, legal, and procedural) to enable responsible and trustworthy data use and sharing; and (3) the types of institutions or functions required to effectively implement these principles, norms, standards, tools, and mechanisms. For example, stakeholders may differ in their views of data minimization (that is, acquiring only the data necessary to achieve the limited and disclosed purpose for which those data are necessary); protecting data; or creating or identifying the institutions tasked with extracting the maximum public value from data.
124. Strickling and Hill (2017).
125. Dutton (2015).
126. WGIG (2005).
127. At ICANN, civil society is represented in the at-large mechanisms for participation in decision-making; in management and address registries; and in the Internet Architecture Board. It also participates in the selection of board members. Business representatives participate in their own business constituency group. More broadly, ICANN supports transparent and inclusive decision-making by providing unrestricted access to its meetings and encourages public debate through public forums, including representation from low- and middle-income countries. See WGIG (2005).
128. Dutton (2015); Strickling and Hill (2017).
129. Rubinstein (2018).
130. Strickling and Hill (2017).
131. WGIG (2005).
132. For example, a study by Maurer and Morgus (2014) found that two-thirds of the countries that favored intergovernmental (multilateral) control over the internet regulate political, social, or religious content on the internet within their borders, constraining freedom of expression. The study analyzed state voting records at the ITU's World Conference on International Telecommunications (WCIT) in Dubai, Saudi Arabia, in 2012.
133. African Union (2014).
134. Information communicated during the World Bank and German Federal Ministry of Economic

Cooperation and Development's Online Consultation, "Data for Better Lives: Enablers and Safeguards," June 9–10, 2020.

135. Bruhn, Lara Ibarra, and McKenzie (2014); Bruhn et al. (2016); Frisancho (2020); Lührmann, Serra-Garcia, and Winter (2018).
136. For example, the CSO Privacy International tracks extraordinary measures adopted by governments, international organizations, and technology companies in response to COVID-19 to ensure these measures do not lead to data exploitation and violate human rights. See Privacy International, "Tracking the Global Response to COVID-19," London, https://privacyinternational.org/examples/tracking-global-response-covid-19.
137. OECD (2013).
138. According to a survey conducted by the Pathways to Prosperity Commission in 2019, policy makers in lower-income countries emphasized that the areas in which "global efforts" were most needed were taxation; cybercrime and cybersecurity; privacy and data protection; market competition; intellectual property; and data sharing and interoperability. Within these priority areas, international cooperation and coordination were considered the most needed to support the development of regulatory and technical standards. International regulatory cooperation in these six areas can have positive externalities, including improving regulatory predictability, reducing compliance burdens and the risks of regulatory arbitrage, and potentially encouraging investment flows. See Pathways for Prosperity Commission (2019).
139. Carter and Yayboke (2019).

References

Abraham, Rene, Johannes Schneider, and Jan vom Brocke. 2019. "Data Governance: A Conceptual Framework, Structured Review, and Research Agenda." *International Journal of Information Management* 49 (December): 424–38.

African Union. 2014. "African Union Convention on Cyber Security and Personal Data Protection." Document EX.CL/846(XXV), June 27, 2014 (adopted), African Union, Addis Ababa, Ethiopia. https://www.opennetafrica.org/?wpfb_dl=4.

African Union. 2020. "The Digital Transformation Strategy for Africa (2020–2030)." African Union, Addis Ababa, Ethiopia. https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.

Agesic (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, Agency for Electronic Government and Information and Knowledge Society, Uruguay). 2019. "Agenda Uruguay Digital 2020: Transforming with Equity." Agesic, Office of the President of the Republic, Montevideo, Uruguay.

Aghion, Philippe, and Jean Tirole. 1997. "Formal and Real Authority in Organizations." *Journal of Political Economy* 105 (1): 1–29.

Arizti, Pedro, Daniel J. Boyce, Natalia Manuilova, Carlos Sabatino, Roby Senderowitsch, and Ermal Vila. 2020. *Building Effective, Accountable, and Inclusive Institutions in Europe and Central Asia: Lessons from the Region*. With contributions of William Gallagher and Patricia Rogers. Washington, DC: World Bank.

Arraiz, Irani, Miriam Bruhn, Benjamin N. Roth, Claudia Ruiz Ortega, and Rodolfo Mario Stucchi. 2019. "Free Riding in Loan Approvals: Evidence from SME Lending in Peru." Policy Research Working Paper 9072, World Bank, Washington, DC.

ASEAN (Association of Southeast Asian Nations). 2012. "Framework on Digital Data Science." Document endorsed at 12th ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), Cebu, the Philippines, November 15–16, 2012. https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf.

Bach, Tobias. 2016. "Administrative Autonomy of Public Organizations." In *Global Encyclopedia of Public Administration, Public Policy, and Governance*, edited by Ali Farazmand, 171–79. Cham, Switzerland: Springer.

Bengio, Yoshua. 2020. "Peer-to-Peer AI-Tracing of COVID-19." *Yoshua Bengio* (blog), March 23, 2020. https://yoshuabengio.org/2020/03/23/peer-to-peer-ai-tracing-of-covid-19/.

Bergstrom, Theodore, Lawrence Blume, and Hal Varian. 1986. "On the Private Provision of Public Goods." *Journal of Public Economics* 29 (1): 25–49.

Bernholz, Lucy. 2016. "Workshop Summary: Trusted Data Intermediaries." Stanford Center on Philanthropy and Civil Society, Stanford University, Stanford, CA. https://pacscenter.stanford.edu/wp-content/uploads/2018/05/TDI-Workshop-Summary.pdf.

Bertelli, Anthony M., Mai Hassan, Dan Honig, Daniel Rogger, and Martin J. Williams. 2020. "An Agenda for the Study of Public Administration in Developing Countries." *Governance* 33 (4): 735–48.

Bhargava, Rahul, and Catherine D'Ignazio. 2015. "Designing Tools and Activities for Data Literacy Learners." Paper presented at Workshop on Data Literacy, Web Science 2015 Conference, Oxford, UK, June 30, 2015.

Blackman, Colin, and Lara Srivastava, eds. 2011. *Telecommunications Regulation Handbook*. Washington, DC: World Bank, InfoDev, and International Telecommunication Union.

Blair, Harry. 2011. "Gaining State Support for Social Accountability." In *Accountability through Public Opinion: From Inertia to Public Action*, edited by Sina Odugbemi and Taeku Lee, 37–51. Washington, DC: World Bank. https://elibrary.worldbank.org/doi/10.1596/9780821385050_CH04.

British Academy and Royal Society. 2017a. "Data Governance: Public Engagement Review." British Academy and Royal Society, London. https://royalsociety.org/-/media/policy/projects/data-governance/data-governance-public-engagement-review.pdf.

British Academy and Royal Society. 2017b. "Data Management and Use: Governance in the 21st Century; A Joint Report by the British Academy and the Royal Society." British Academy and Royal Society, London. https://royalsociety.org/topics-policy/projects/data-governance/.

Brown, Walter, Daniel Rogger, Ella Spencer, and Martin Williams. 2019. "Information and Innovation in the Public Sector." IGC Growth Brief 019, International

Growth Center, London. https://www.theigc.org/wp-content/uploads/2019/10/Brown-et-al-2019-Growth-Brief_Web.pdf.

Bruhn, Miriam, Luciana de Souza Leão, Arianna Legovini, Rogelio Marchetti, and Bilal Zia. 2016. "The Impact of High School Financial Education: Evidence from a Large-Scale Evaluation in Brazil." *American Economic Journal: Applied Economics* 8 (4): 256–95.

Bruhn, Miriam, Gabriel Lara Ibarra, and David McKenzie. 2014. "The Minimal Impact of a Large-Scale Financial Education Program in Mexico City." *Journal of Development Economics* 108 (May): 184–89.

Bundeskartellamt. 2019. "Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources." *News*, February 7, 2019, Bundeskartellamt, Bonn, Germany. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

Camera, Gabriele, Marco Casari, and Maria Bigoni. 2013. "Money and Trust among Strangers." *PNAS, Proceedings of the National Academy of Sciences* 110 (37): 14889–93.

Campbell, Dennis, and Tatiana Sandino. 2019. "Sustaining Corporate Culture in a Growing Organization." Harvard Business School Technical Note 119–109, Harvard Business School, Boston, MA.

Carr, Priyanka B., and Gregory M. Walton. 2014. "Cues of Working Together Fuel Intrinsic Motivation." *Journal of Experimental Social Psychology* 53 (July): 169–84.

Carson, Lyn, and Janette Hartz-Karp. 2005. "Adapting and Combining Deliberative Designs: Juries, Polls, and Forums." In *The Deliberative Democracy Handbook: Strategies for Effective Civic Engagement in the Twenty-First Century*, edited by John Gastil and Peter Levine, 120–38. San Francisco: Jossey-Bass.

Carter, William A., and Erol Yayboke. 2019. "Data Governance Principles for the Global Digital Economy." Report, Center for Strategic and International Studies, Washington, DC. https://www.csis.org/analysis/data-governance-principles-global-digital-economy.

Cavoukian, Ann. 2011. "PbD, Privacy by Design, the 7 Foundational Principles: Implementation and Mapping of Fair Information Practices." Information and Privacy Commissioner of Ontario, Toronto. https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/.

Cheruiyot, David, Stefan Baack, and Raul Ferrer-Conill. 2019. "Data Journalism beyond Legacy Media: The Case of African and European Civic Technology Organizations." *Digital Journalism* 7 (9): 1215–29.

CL4D (Collaborative Leadership for Development). 2016. "CL4D Portfolio of Unblocking Project Implementation Challenges and Accelerating Progress." World Bank, Washington, DC. https://www.leadfordev.org/Data/gpl4d/files/field/documents/cl4d_portfolio_brochuresoftcopyversion.pdf.

Danezis, George, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, and Stefan Schiffner. 2014. "Privacy and Data Protection by Design." European Union Agency for Network and Information Security, Heraklion, Greece. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

Deichmann, Johannes, Kersten Heineke, Thomas Reinbacher, and Dominik Wee. 2016. "Creating a Successful Internet of Things Data Marketplace." *Our Insights* (blog), October 7, 2016, McKinsey and Company, New York. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/creating-a-successful-internet-of-things-data-marketplace.

Delacroix, Sylvie, and Neil D. Lawrence. 2019. "Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance." *International Data Privacy Law* 9 (4): 236–52.

Deloitte. 2012. "Open Growth: Stimulating Demand for Open Data in the UK." Briefing note, Deloitte Analytics, London. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/deloitte-analytics/open-growth.pdf.

DeNardis, Laura, and Mark Raymond. 2013. "Thinking Clearly about Multistakeholder Internet Governance." Paper presented at GigaNet, the Eighth Annual Global Internet Governance Academic Network Symposium, Bali, Indonesia, October 21, 2013.

DOJ (Department of Justice, United States). 2020. "Roles and Responsibilities under the Foundations for Evidence-Based Policymaking Act." Open Government. https://www.justice.gov/open/roles-and-responsibilities-under-foundations-evidence-based-policymaking-act.

Dutton, William H. 2015. "Multistakeholder Internet Governance?" Background paper, *World Development Report 2016: Digital Dividends*, World Bank, Washington, DC.

EC (European Commission). 2020. "Trust Services and Electronic Identification (eID)." *Shaping Europe's Digital Future: Policy*. https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification.

Economist. 2013. "How Did Estonia Become a Leader in Technology?" *The Economist Explains*, July 31, 2013. https://www.economist.com/the-economist-explains/2013/07/30/how-did-estonia-become-a-leader-in-technology.

EDPB (European Data Protection Board). 2020. "Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak." *Guidelines*, EDPB, Brussels. https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_en.

Egle, Danuta, and Andrew J. Zahuranec. 2020. "How to Build the Data Skills Toolkit Public Employees Need." *Data Stewards* (blog), June 24, 2020. https://medium.com/data-stewards-network/how-to-build-the-data-skills-toolkit-public-employees-need-6af3af43e627.

eHealth Network. 2020. "Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19: Common EU Toolbox for Member States." Version 1.0, eHealth Network, Brussels. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

Elliot, Mark James, Elaine Mackey, Kieron O'Hara, and Caroline Tudor. 2016. *The Anonymisation Decision-Making Framework*. Manchester, UK: UKAN Publications.

EU (European Union). 2014. "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC." *Official Journal of the*

European Union L 257/73. https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf.

EU (European Union). 2020. "Communication from the Commission: Guidance on Apps Supporting the Fight against COVID 19 Pandemic in Relation to Data Protection." *Official Journal of the European Union* C 124 I/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN.

Floridi, Luciano, and Mariarosaria Taddeo. 2016. "What Is Data Ethics?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical, and Engineering Sciences* 374 (2083): 20160360. https://doi.org/10.1098/rsta.2016.0360.

Fölscher, Alta, and Emilie Gay. 2012. "Fiscal Transparency and Participation in Africa: A Status Report." Collaborative Africa Budget Reform Initiative, National Treasury, Pretoria, South Africa.

Frisancho, Verónica C. 2020. "The Impact of School-Based Financial Education on High School Students and Their Teachers: Experimental Evidence from Peru." IDB Working Paper IDP-WP-871, Inter-American Development Bank, Washington, DC.

FTC (Federal Trade Commission, United States). 2014. *Data Brokers: A Call for Transparency and Accountability*. Washington, DC: FTC. https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

Garcia, Helen R. 2007. "Perspectives on Communication and Social Accountability: A Qualitative Survey of World Bank Practitioners." Paper presented at World Bank's Communication for Governance and Accountability Program Workshop, "Generating Genuine Demand with Social Accountability Mechanisms," World Bank Office, Paris, November 1–2, 2007.

Gauri, Varun. 2011. "Redressing Grievances and Complaints Regarding Basic Service Delivery." Policy Research Working Paper 5699, World Bank, Washington, DC.

Gilardi, Fabrizio, and Martino Maggetti. 2011. "The Independence of Regulatory Authorities." In *Handbook on the Politics of Regulation*, edited by David Levi-Faur, 201–14. Cheltenham, UK: Edward Elgar Publishing.

Gopal Jayal, Niraja. 2007. "New Directions in Theorising Social Accountability?" *IDS Bulletin* 38 (6): 105–10.

Grandvoinnet, Helene, Ghazia Aslam, and Shomikho Raha. 2015. *Opening the Black Box: The Contextual Drivers of Social Accountability*. New Frontiers of Social Policy Series. Washington, DC: World Bank.

Grossman, Robert L. 2019. "Data Lakes, Clouds, and Commons: A Review of Platforms for Analyzing and Sharing Genomic Data." *Trends in Genetics* 35 (3): 223–34.

Grossman, Robert L., Allison Heath, Mark Murphy, Maria Patterson, and Walt Wells. 2016. "A Case for Data Commons: Toward Data Science as a Service." *Computing in Science and Engineering* 18 (5): 10–20.

Gunningham, Neil, and Joseph Rees. 1997. "Industry Self-Regulation: An Institutional Perspective." *Law and Policy* 19 (4): 363–414.

Gupta, Anil K., and Lawrence J. Lad. 1983. "Industry Self-Regulation: An Economic, Organizational, and Political Analysis." *Academy of Management Review* 8 (3): 416–25.

Hanna, Nagy K. 2012. "Open Development: ICT for Governance in Africa." World Bank, Washington, DC.

Hardinges, Jack. 2018. "Defining a 'Data Trust.'" *Knowledge and Opinion* (blog), October 19, 2018, Open Data Institute, London. https://theodi.org/article/defining-a-data-trust/.

Hardinges, Jack. 2020. "Data Trusts in 2020." *Knowledge and Opinion* (blog), March 17, 2020, Open Data Institute, London. https://theodi.org/article/data-trusts-in-2020/.

Hardinges, Jack, and Jeni Tennison. 2020. "What Do We Mean by Data Institutions?" *Knowledge and Opinion* (blog), February 10, 2020, Open Data Institute, London. https://theodi.org/article/what-do-we-mean-by-data-institutions/.

Harrison, Teresa M., Theresa A. Pardo, and Meghan Cook. 2012. "Creating Open Government Ecosystems: A Research and Development Agenda." *Future Internet* 4 (4): 900–28.

He, Baogang. 2011. "Deliberation and Institutional Mechanisms for Shaping Public Opinion." In *Accountability through Public Opinion: From Inertia to Public Action*, edited by Sina Odugbemi and Taeku Lee, 203–14. Washington, DC: World Bank. https://elibrary.worldbank.org/doi/10.1596/9780821385050_CH14.

Hill, Ryan, Carolyn Stein, and Heidi Williams. 2020. "Internalizing Externalities: Designing Effective Data Policies." *AEA Papers and Proceedings* 110 (May): 49–54. https://doi.org/10.1257/pandp.20201060.

Hjalmarsson, Anders, Niklas Johansson, and Daniel Rudmark. 2015. "Mind the Gap: Exploring Stakeholders' Value with Open Data Assessment." In *Proceedings of the 48th Annual Hawaii International Conference on System Sciences, HICSS 2015*, edited by Tung X. Bui and Ralph H. Sprague, Jr., 1314–23. Los Alamitos, CA: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/HICSS.2015.160.

Ibarra, Herminia, and Morten T. Hansen. 2011. "Are You a Collaborative Leader?" *Harvard Business Review* 89 (7–8): 68–74.

Johns, Melissa, and Valentina Saltane. 2016. "Citizen Engagement in Rulemaking: Evidence on Regulatory Practices in 185 Countries." Policy Research Working Paper 7840, World Bank, Washington, DC.

Kettani, Mehdi. 2017. "Régime Juridique de la Protection des Données Personnelles." Client Brief, DLA Piper, New York.

Kin, Yeong Zee. 2020. "Enabling Data Innovation through Accountability: Singapore's Approach." Paper presented at seminar organized in Singapore by the Office of the Chief Economist, Middle East and North Africa Region, World Bank, April 7, 2020.

Kpundeh, Sahr J. 2000. "Corruption and Corruption Control in Africa." Paper prepared for Gulbenkian Foundation workshop, "Democracy and Development in Africa," Lisbon, June 23–24, 2000. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.595.4791&rep=rep1&type=pdf.

Lührmann, Melanie, Marta Serra-Garcia, and Joachim Winter. 2018. "The Impact of Financial Education on Adolescents' Intertemporal Choices." *American Economic Journal: Economic Policy* 10 (3): 309–32.

Lundqvist, Björn. 2018. "Data Collaboration, Pooling, and Hoarding under Competition Law." Stockholm Faculty of Law Research Paper 61, Stockholm University, Stockholm.

Maddox, Teena. 2015. "The World's Smartest Cities: What IoT and Smart Governments Will Mean for You." *TechRepublic*, November 10, 2015. https://www.techrepublic.com/article/smart-cities/.

Malena, Carmen. 2004. "Social Accountability: An Introduction to the Concept and Emerging Practice." With Reiner Forster and Janmejay Singh. Social Development Paper: Participation and Civic Engagement, World Bank. Washington, DC.

Management Concepts. 2016. "Successful Change Management Practices in the Public Sector: How Governmental Agencies Implement Organizational Change Management." Management Concepts, Tysons Corner, VA.

Martínez Pería, María Soledad, and Sandeep Singh. 2014. "The Impact of Credit Information Sharing Reforms on Firm Financing." Policy Research Working Paper 7013, World Bank, Washington, DC.

Maurer, Tim, and Robert Morgus. 2014. "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate." Internet Governance Paper 7, Center for International Governance Innovation, Waterloo, Ontario, Canada.

Mazzucato, Mariana. 2018. "Mission-Oriented Research and Innovation in the European Union: A Problem-Solving Approach to Fuel Innovation-Led Growth." European Commission, Brussels. https://ec.europa.eu/info/sites/info/files/mazzucato_report_2018.pdf.

MeitY (Ministry of Electronics and Information Technology). 2020. "Report by the Committee of Experts on Non-Personal Data Governance Framework." Report 111972/2020/CL&ES, MeitY, New Delhi. https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/08/mygov_159453381955063671.pdf.

MGI (McKinsey Global Institute). 2019. "How Can the Private and Public Sectors Work Together to Create Smart Cities?" McKinsey, New York.

Microsoft News Center India. 2016. "Microsoft, L V Prasad Eye Institute, and Global Experts Collaborate to Launch Microsoft Intelligent Network for Eyecare." *Microsoft Stories India*, December 19, 2016. https://news.microsoft.com/en-in/microsoft-l-v-prasad-eye-institute-and-global-experts-collaborate-to-launch-microsoft-intelligent-network-for-eyecare/.

Mitchell, Shane, Nicola Villa, Martin Stewart-Weeks, and Anne Lange. 2013. "The Internet of Everything for Cities: Connecting People, Process, Data, and Things to Improve the 'Livability' of Cities and Communities." Point of View, Cisco Systems, San Jose, CA. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/everything-for-cities.pdf.

Nauheimer, Holger. 2015. *The Change Management Toolbook: A Collection of Tools, Methods, and Strategies*. Stellenbosch, South Africa: ChangeWright Consulting.

NHSA (Northern Health Science Alliance). 2020. "Connected Health Cities: Impact Summary 2016–2020." NHSA, Manchester, UK. https://www.thenhsa.co.uk/app/uploads/2020/03/Connected-Health-Cities-Impact-Report-Summary.pdf.

ODI (Open Data Institute). 2019. "Huge Appetite for Data Trusts, According to New ODI Research." *Knowledge and Opinion* (blog), April 15, 2019, Open Data Institute, London. https://theodi.org/article/huge-appetite-for-data-trusts-according-to-new-odi-research/.

O'Donnell, Fionntán, and Jared Robert Keller. 2020. "Building Trust in Alternative Data Ecosystems." *Knowledge and Opinion* (blog), April 16, 2020, Open Data Institute, London. https://theodi.org/article/building-trust-in-alternative-data-ecosystems/.

OECD (Organisation for Economic Co-operation and Development). 1997. "Public Service Training in OECD Countries." SIGMA Paper 16, OECD, Paris. https://doi.org/10.1787/5kml619ljzzn-en.

OECD (Organisation for Economic Co-operation and Development). 2012. "Recommendation of the Council on Regulatory Policy and Governance." Council on Regulatory Policy and Governance, OECD, Paris. https://www.oecd.org/governance/regulatory-policy/49990817.pdf.

OECD (Organisation for Economic Co-operation and Development). 2013. *The OECD Privacy Framework*. Paris: OECD. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD (Organisation for Economic Co-operation and Development). 2017. "Creating a Culture of Independence: Practical Guidance against Undue Influence." OECD, Paris. https://www.oecd.org/gov/creating-a-culture-of-independence-9789264274198-en.htm.

OECD (Organisation for Economic Co-operation and Development). 2018. "OECD Regulatory Enforcement and Inspections Toolkit." OECD, Paris. https://doi.org/10.1787/9789264303959-en.

OECD (Organisation for Economic Co-operation and Development). 2019a. *Digital Government Review of Argentina: Accelerating the Digitalisation of the Public Sector*. OECD Digital Government Studies Series. Paris: OECD. https://www.oecd-ilibrary.org/governance/digital-government-review-of-argentina_354732cc-en.

OECD (Organisation for Economic Co-operation and Development). 2019b. *The Path to Becoming a Data-Driven Public Sector*. OECD Digital Government Studies Series, November 28. Paris: OECD. https://doi.org/10.1787/059814a7-en.

OMB (Office of Management and Budget). 2020. "Federal Chief Data Officers Council Holds Inaugural Meeting." OMB, Washington, DC. https://strategy.data.gov/news/2020/01/31/federal-chief-data-officers-council-holds-inaugural-meeting/.

O'Neill, Mark. 2020. "What Is a Plugin?" *Technology Trends* (blog). January 7, 2020 (updated). https://smallbiztrends.com/2014/07/what-is-a-plugin.html.

PARIS21 (Partnership in Statistics for Development in the 21st Century). 2017. "National Strategies for the Development of Statistics." PARIS21 Consortium, Paris. https://paris21.org/national-strategy-development-statistics-nsds.

Pathways for Prosperity Commission. 2019. "Digital Diplomacy: Technology Governance for Developing Countries." Pathways for Prosperity Commission, Oxford, UK. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-10/Digital-Diplomacy.pdf.

Paul, Samuel. 2011. "Stimulating Activism through Champions of Change." In *Accountability through Public Opinion:*

From Inertia to Public Action, edited by Sina Odugbemi and Taeku Lee, 347–57. Washington, DC: World Bank. https://doi.org/10.1596/9780821385050_CH23.

Pentland, Alex, and Thomas Hardjono. 2020. "Data Cooperatives." In *Building the New Economy: Data as Capital*, edited by Alex Pentland, Alexander Lipton, and Thomas Hardjono, chap. 2. Cambridge, MA: MIT Press. Published ahead of print, April 30, 2020. https://wip.mitpress.mit.edu/pub/pnxgvubq/release/2.

Peruzzotti, Enrique, and Catalina Smulovitz, eds. 2006. *Enforcing the Rule of Law: Social Accountability in the New Latin American Democracies*. Pitt Latin American Studies Series. Pittsburgh: University of Pittsburgh Press.

Peters, B. Guy. 2018. "The Challenge of Policy Coordination." *Policy Design and Practice* 1 (1): 1–11.

PI (Privacy International). 2018. "Why We've Filed Complaints against Companies That Most People Have Never Heard of, and What Needs to Happen Next." *Advocacy*, November 8, 2018, PI, London. http://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what.

Polonetsky, Jules, Omer Tene, and Kelsey Finch. 2016. "Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification." *Santa Clara Law Review* 56 (3): 593–629.

Porrúa, Miguel A. 2013. "E-Government in Latin America: A Review of the Success in Colombia, Uruguay, and Panama." In *The Global Information Technology Report 2013: Growth and Jobs in a Hyperconnected World*, edited by Beñat Bilbao-Osorio, Soumitra Dutta, and Bruno Lanvin, 127–36. Insight Report. Geneva: World Economic Forum. http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf.

Quay, Ray. 2010. "Anticipatory Governance: A Tool for Climate Change Adaptation." *Journal of the American Planning Association* 76 (4): 496–511. https://doi.org/10.1080/01944363.2010.508428.

Ram, Aliya, and Madhumita Murgia. 2019. "Data Brokers: Regulators Try to Rein In the 'Privacy Deathstars.'" *Financial Times*, January 7, 2019. https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521.

Rasul, Imran, Daniel Rogger, and Martin J. Williams. 2018. "Management of Bureaucrats and Public Service Delivery: Evidence from the Nigerian Civil Service." Policy Research Working Paper 8595, World Bank, Washington, DC.

Richardson, Harriet, Steve Hendrickson, and Houman Boussina. 2018. "ERP Planning: Information Technology and Data Governance." Audit Report (rev.), Office of the City Auditor, Palo Alto, CA. https://www.cityofpaloalto.org/civicax/filebank/documents/66250.

Rodian, Justine. 2018. "Master Data Management Definitions: The Complete A-Z of MDM." *Master Data Management* (blog), April 19, 2018. https://blog.stibosystems.com/the-complete-a-z-of-master-data-management.

Rubinstein, Ira S. 2018. "The Future of Self-Regulation Is Co-Regulation." In *The Cambridge Handbook of Consumer Privacy*, edited by Evan Selinger, Jules Polonetsky, and Omer Tene, 503–23. Cambridge Law Handbooks Series. Cambridge, UK: Cambridge University Press.

Scassa, Teresa, and Merlynda Vilain. 2019. "Governing Smart Data in the Public Interest: Lessons from Ontario's Smart Metering Entity." CIGI Paper 221, Center for International Governance Innovation, Waterloo, Ontario, Canada. https://www.cigionline.org/publications/governing-smart-data-public-interest-lessons-ontarios-smart-metering-entity.

SGD (Digital Government Secretariat, Brazil). 2020. "Central Data Governance Committee." *Digital Government*, June 22, 2020, SGD, Brasília. https://www.gov.br/governodigital/pt-br/governanca-de-dados/comite-central-de-governanca-de-dados.

Shapiro, Carl, and Hal R. Varian. 1998. *Information Rules: A Strategic Guide to the Network Economy*. Brighton, MA: Harvard Business Review Press.

Shkabatur, Jennifer. 2012. "Check My School: A Case Study on Citizens' Monitoring of the Education Sector in the Philippines." World Bank Institute, Washington, DC.

Sjoberg, Fredrik M., Jonathan Mellon, and Tiago Peixoto. 2017. "The Effect of Bureaucratic Responsiveness on Citizen Participation." *Public Administration Review* 77 (3): 340–51.

Strickling, Lawrence E., and Jonah Force Hill. 2017. "Multi-Stakeholder Internet Governance: Successes and Opportunities." *Journal of Cyber Policy* 2 (3): 296–317.

Tannam, Ellen. 2018. "How Can Smart Cities Make Data a Public Good before Time Runs Out?" *Silicon Republic*, July 26, 2018. https://www.siliconrepublic.com/enterprise/decode-nesta-smart-cities.

Thompson, Stuart A., and Charlie Warzel. 2019. "Twelve Million Phones, One Dataset, Zero Privacy." *New York Times*, December 19, 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

Turianskyi, Yarik, Terence Corrigan, Matebe Chisiza, and Alex Benkesnstein. 2018. "Multi-Stakeholder Initiatives: What Have We Learned? An Overview and Literature Review." United States Agency for International Development, Washington, DC. https://www.saiia.org.za/wp-content/uploads/2018/08/2018-MSI-overview-literature-review.pdf.

UNDP (United Nations Development Programme). 2006. "Institutional Reform and Change Management: Managing Change in Public Sector Organisations." Conference Paper 5, UNDP, New York.

United Nations. 2014. "Resolution Adopted by the General Assembly on 29 January 2014: Fundamental Principles of Official Statistics." Document A/RES/68/261, United Nations, New York. https://unstats.un.org/unsd/dnss/gp/FP-New-E.pdf.

UNSDG (United Nations Sustainable Development Group). 2017. "Data Privacy, Ethics, and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda." UNSDG, New York. https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.

Vermont Office of the Attorney General. 2018. "Guidance on Vermont's Act 171 of 2018: Data Broker Regulation." Office of the Attorney General, Montpelier, VT. https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf.

WebFX Team. 2020. "What Are Data Brokers, and What Is Your Data Worth? [Infographic]." *Internet* (blog). March 16, 2020. https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/.

Weiss, Jeff, and Jonathan Hughes. 2005. "Want Collaboration? Accept and Actively Manage Conflict." *Harvard Business Review* 83 (3): 92–101.

WGIG (Working Group on Internet Governance, United Nations). 2005. "Background Report." Château de Bossey, Bogis-Bossey, Switzerland. https://www.itu.int/net/wsis/wgig/docs/wgig-background-report.pdf.

Williams, Martin J., and Liah Yecalo-Tecle. 2020. "Innovation, Voice, and Hierarchy in the Public Sector: Evidence from Ghana's Civil Service." *Governance* 33 (4): 789–807.

Wilson, Christopher. 2019. "Civil Society." In *The State of Open Data: Histories and Horizons*, edited by Tim Davies, Stephen B. Walker, Mor Rubinstein, and Fernando Perini, 355–66. Ottawa, Canada: International Development Research Center; Cape Town, South Africa: African Minds.

WiredGov. 2019. "Digital Revolution to Use the Power of Data to Combat Illegal Wildlife Trade and Reduce Food Waste." Press release, January 31, 2019, WiredGov, Stockport, UK. https://www.wired-gov.net/wg/news.nsf/articles/Digital+revolution+to+use+the+power+of+data+to+combat+illegal+wildlife+trade+and+reduce+food+waste+01022019081000?open.

World Bank. 2002. *World Development Report 2002: Building Institutions for Markets*. Washington, DC: World Bank; New York: Oxford University Press.

World Bank. 2016. *World Development Report 2016: Digital Dividends*. Washington, DC: World Bank.

World Bank. 2017. *World Development Report 2017: Governance and the Law*. Washington, DC: World Bank.

World Bank. 2020. *Enhancing Government Effectiveness and Transparency: The Fight against Corruption*. Global Report (revised October 3). Washington, DC: World Bank.

World Bank. 2021. *Unraveling Data's Gordian Knot: Enablers and Safeguards for Trusted Data Sharing in the New Economy*. Washington, DC: World Bank.

Wylie, Bianca, and Sean McDonald. 2018. "What Is a Data Trust?" *Big Data, Platform Governance* (blog). October 9, 2018. https://www.cigionline.org/articles/what-data-trust.