

Governing Data for Development: Trends, Challenges, and Opportunities

Michael Pisa, Pam Dixon, Benno Ndulu, and Ugonma Nwankwo

Abstract

Governments that can successfully harness the world's ongoing digital transformation and the data it produces can make better informed policy decisions and target their resources more effectively. To achieve this goal, they must establish clear rules about how data can be used across its lifecycle. Until recently, the development community has paid more attention to supporting government use of digital tools and data than on how governments can manage data responsibly. This is now changing in line with a broader shift in societal views about the risks of data misuse. To better understand how governments can use data to support economic development and inclusive growth while protecting citizens and communities against harm, we interviewed over 40 data policy experts from government, civil society, the private sector, development organizations, and the data privacy community over summer 2020. This paper synthesizes the views we heard into key themes and explores some of the questions and challenges that a policy and research agenda aimed at supporting effective government data use should consider.

Center for Global Development
2055 L Street NW
Fifth Floor
Washington DC 20036
202-416-4000
www.cgdev.org

This work is made available under the terms of the Creative Commons Attribution-NonCommercial 4.0 license.

Governing Data for Development: Trends, Challenges, and Opportunities

Michael Pisa
Center for Global Development

Pam Dixon
World Privacy Forum

Benno Ndulu
University of Dar-es-Salaam; Former Governor, Central Bank of Tanzania

Ugonma Nwankwo
Center for Global Development

The Center for Global Development is grateful for contributions from the Hewlett Foundation in support of this work.

Michael Pisa, Pam Dixon, Benno Ndulu, and Ugonma Nwankwo, 2020. "Governing Data for Development: Trends, Challenges, and Opportunities." CGD Policy Paper 190. Washington, DC: Center for Global Development. <https://www.cgdev.org/publication/governing-data-development-trends-challenges-and-opportunities>

Center for Global Development
2055 L Street NW
Washington, DC 20036

202.416.4000
(f) 202.416.4050

www.cgdev.org

The Center for Global Development works to reduce global poverty and improve lives through innovative economic research that drives better policy and practice by the world's top decision makers. Use and dissemination of this Policy Paper is encouraged; however, reproduced copies may not be used for commercial purposes. Further usage is permitted under the terms of the Creative Commons License.

The views expressed in CGD Policy Papers are those of the authors and should not be attributed to the board of directors, funders of the Center for Global Development, or the authors' respective organizations.

Contents

Governing Data for Development Working Group	1
Introduction	2
Theme 1: The need to break down silos.....	13
Theme 2: Promoting data governance as an enabler rather than hindrance	15
Theme 3: Equitably distributing the value of data insights by “closing the loop”	17
Theme 4: The benefits, hazards, and hurdles of data collaboration	21
Theme 5: Establishing effective data protection frameworks.....	25
Theme 6: The need for greater global and regional coordination.....	33
Theme 7: Developing the skills needed to govern data	35
Theme 8: The impact of COVID-19	37
Conclusion: Areas for future research	40
Appendix 1: Complete list of interviews	42
Appendix 2: Selected interview quotes	44

Governing Data for Development Working Group

This scoping paper is a preliminary input for a research program led by the Center for Global Development, with funding from the Hewlett Foundation, that seeks to better understand how governments can use data to support innovation and economic development while protecting citizens and communities against harm. The project is guided by a working group composed of the following experts:

Co-Chairs

Pam Dixon, Founder and Executive Director, World Privacy Forum

Benno Ndulu, Professor of Development Economics, University of Dar-es-Salaam;
Former Governor, Central Bank of Tanzania

Working Group Members

Adedeji Adeniran, Director of Education and Governance Research/Senior Research Fellow, Centre for the Studies of African Economies

Shaida Badiee, Founder and Managing Director, Open Data Watch

Donatien Beguy, Population Scientist and Data Expert, UN-Habitat

Stephen Chacha, Co-Founder and Executive Director, Tanzania Data Lab

Somsak Chunharas, President of National Health Foundation in Thailand

Vyjayanti Desai, Program Manager, Identification for Development

Teki Akuetteh Falconer, Founder & Executive Director, Africa Digital Rights' Hub

Drudeisha Madhub, Data Protection Commissioner, Data Protection Office, Mauritius

David Medine, Consultant, Consultative Group to Assist the Poor

Santosh Misra, CEO, Tamil Nadu e-Governance Agency and Commissioner of e-Governance, Government of Tamil Nadu, India

Tom Orrell, Managing Director, DataReady

Olasupo Oyedepo, co-founder and Director, African Alliance of Digital Health Networks

Michael Pisa, Policy Fellow, Center for Global Development

Isaac Rutenberg, Director, Center for Intellectual Property and Information Technology Law

Omar Seidu, Head, Demographic Statistics and Coordinator of Data for SDGs, Ghana Statistical Services

Rachel Sibande, Program Director, Data for Development, Digital Impact Alliance

The authors would like to thank all the individuals who agreed to be interviewed for this project, whose names are listed in Appendix 1. While we are grateful for insights provided by interviewees and working group members, any mistakes made in this paper belong to the authors.

Introduction

Governments that can successfully harness the world's ongoing digital transformation and the resulting proliferation of new datasets, data types, and data ecosystems can make better informed policy decisions and target their resources more efficiently and effectively. To achieve this goal, they must establish clear rules about how data is collected, analyzed, used, and shared in a way that protects citizens from abuse while supporting innovation, development, and inclusive growth.

The COVID-19 pandemic has highlighted the importance of governments having the ability to systematically access accurate and timely information and, in many countries, accelerated the shift towards a digital-first approach due to the need to expand the reach of the social safety net while providing services at a distance.¹ It has also highlighted the disadvantage faced by those unable to access the internet — a “digital divide” that closely mirrors existing inequalities.² Finally, the pandemic has brought to the forefront difficult questions about the limits that should be placed on governments and private companies that seek to use potentially sensitive data to monitor the spread of disease and target public health efforts.

In all these ways, the COVID-19 pandemic has held up a mirror to a world in which countries and communities are advancing unevenly on a path of digitalization while grappling with fundamental questions about how governments can best use data to achieve their policy aims and how the value of data should be distributed throughout society.

Although countries are digitalizing at vastly different speeds, the trend towards greater reliance on digital tools and data is unidirectional. In many countries, national governments are the primary catalyst of this transformation through their increasing use of digital systems (including mobile applications, digital payments, and digital ID) to deliver services and provide social support.³ These systems generate massive amounts of data and rely on the integration of multiple databases to enable a more coherent social support response but also raise privacy concerns because of how they link information about individuals across different services.⁴

At the same time, there is growing interest among government officials to draw insights from data that is more granular and produced at a higher frequency than traditional official statistics, including administrative data, which government agencies generate through the operation of public services and, increasingly, data collected by the private sector. While integrating data from private and public sources can help governments fill knowledge gaps

¹ Gelb, Alan and Anit Mukherjee. Digital Technology in Social Assistance Transfers for COVID-19 Relief: Lessons from Selected Cases. September 2020.

² For data on the digital divide see the International Telecommunications Union's ITU Facts and Figures (2019).

³ Gelb, Alan, Anit Mukherjee, and Kyle Navis. Citizens and States: How Can Digital ID and Payments Improve State Capacity and Effectiveness? March 2020.

⁴ Clark, Julia and Conrad Daly (World Bank). Digital ID and the Data Protection Challenge: Practitioner's Note. October 2019.

that official statistics alone cannot address, it also raises novel ethical, legal, and regulatory concerns for policymakers to contend with.⁵

The purpose of this paper

This scoping and synthesis paper serves as a preliminary input for a research program led by the Center for Global Development and guided by a working group of experts from government, civil society, the development community, and the data privacy community that seeks to better understand how governments can use data to support innovation and economic development while protecting citizens and communities against harm.

As a first step in this process, we interviewed more than 40 people working to support public sector data use, including experts from government, civil society, the private sector, and academia.

We asked these experts for their views on what types of capacities, resources, legal frameworks, and institutional mechanisms countries should have in place to use data responsibly and effectively; the opportunities and risks created by greater public sector use of data created by the private sector; and whether the digital policy response to the COVID-19 pandemic has changed how they think about these issues.

In this paper, we present the views shared with us as faithfully as possible, while organizing them into a set of key themes raised. We also include a selection of quotes arranged by theme in the appendix. Before turning to these themes, we briefly set out the context for this work and note the limitations of our research.

Data governance becomes political

In recent years, mounting concerns about the global expansion of artificial intelligence (AI) and machine learning surveillance and awareness of how predictive analytics can lead to discrimination through poor or purposeful design have rekindled an old debate about how much governments and businesses should know — or can predict — about their citizens and customers.⁶ This has in turn led to greater emphasis on the importance of countries having rules in place to govern how data is used across its lifecycle as well as mechanisms for redress in case of harm.

The concept of data governance, which has existed since at least the 1960s when companies began to adopt data processing systems, is generally used to describe the practices and

⁵ Humpherson, Ed. [Joining Up Data for Better Statistics](#). September 2018.

⁶ These debates are not new. For example, see discussions about the privacy implications of the U.S. social security system in the 1930s in Sarah Igo's [The Known Citizen: A History of Privacy in Modern America](#) (2018). On the dangers of predictive analytics see comments of the Electronic Privacy Information Center (EPIC) to the U.S. Office of Science and Technology Policy: [Request for Information: Big data and the future of privacy](#) (2014). For evidence on shifting public attitudes on the use of data, see the [CIGI-Ipsos Global Survey on Internet Security and Trust](#) (2019) and EPIC's webpage on [Public Opinion on Privacy](#).

systems used by private corporations to manage data as an asset.^{7,8} Recently, however, the term has been extended to refer to the laws and policies governments enact to govern the use of data in society.⁹ For the purpose of this paper, we use the term to refer to the comprehensive set of rules, policies, and procedures that guide how organizations manage, use, and share data internally and across data ecosystems — and note that the term “organizations” extends to both governments as a whole and individual public agencies.¹⁰

Most data governance activities are highly technical. For example, the DAMA-DMBOK, a key reference book on the topic, puts data governance at the center of ten different data management activities, including integration and interoperability, storage and operations, and modeling and design.¹¹ But because these activities collectively determine how organizations use and share data, including potentially sensitive data, data governance has become politically salient, with most debate centering on issues related to data privacy.

Over the last decade, the adoption of data protection and privacy laws has accelerated dramatically. Since 2010, 64 countries have enacted new data privacy laws, bringing the total number of countries with such laws up to 144.¹² Most of the countries that enacted these laws in the last decade are low and middle-income countries (LMICs). Even in countries with well-established data protection and privacy regimes, however, the gap between having laws on the books and implementing them effectively is vast and the Data Protection Authorities (DPAs) responsible for overseeing these efforts are often under-resourced, according to several data privacy experts we spoke to.

⁷ For example, 14 of the first 15 website results generated by a Google search for “data governance” on October 15, 2020 focused solely on the concept’s application to the private sector.

⁸ Magnitude Marketing. [A Brief History of Data Governance](#). June 2010.

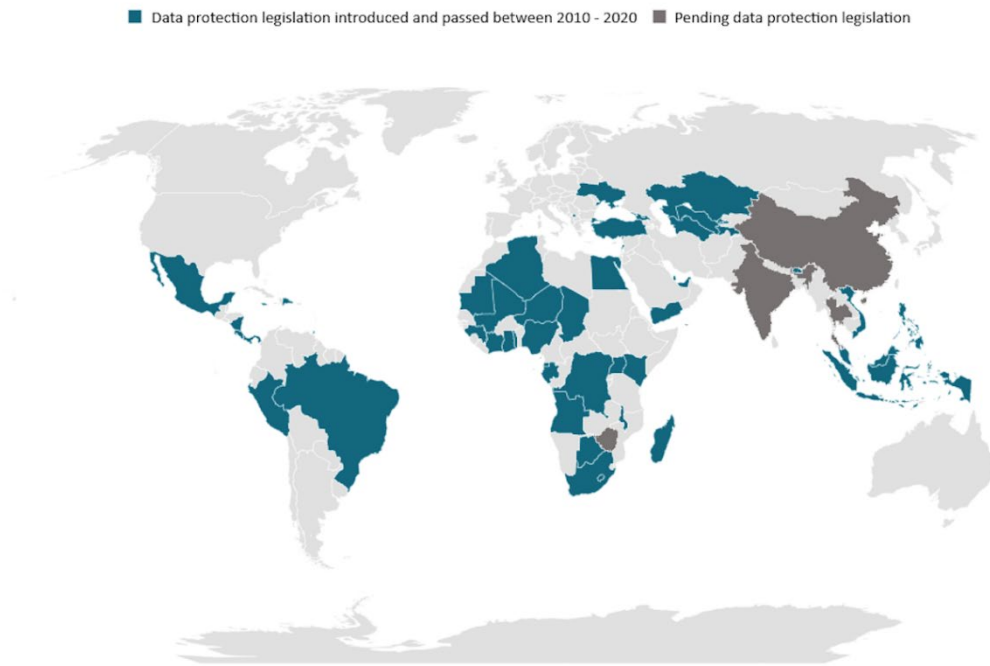
⁹ See for example, Foreign Policy’s [Global Data Governance Part One: Emerging Data Governance Practices](#) (2020).

¹⁰ This definition draws on insights from the literature on data and information governance that extends from information management in industrial contexts (e.g., Deming’s [Profound System of Knowledge](#)) to management of particular types of systems (e.g., Ostrom’s [Governance of the Commons](#)) and specific types of data (for management of big data, see Soares’ [Big Data Governance: An emerging imperative](#)).

¹¹ For the full list, see page 36 of the [DAMA-DMBOK Data Management Body of Knowledge](#) book or the following image [The DAMA Wheel](#).

¹² Greenleaf, Graham and Bertil Cottier. [2020 Ends a Decade of 62 New Data Privacy Laws](#). May 2020.

Figure 1. Recent adoption of data privacy laws driven by low- and lower-middle income countries¹³



Note: Data from Greenleaf's [Global Tables of Data Privacy Laws and Bills \(6th Ed January 2019\)](#) and Greenleaf and Cottier's [2020 Ends a Decade of 62 New Data Privacy Laws](#). Additional research conducted by World Privacy Forum (2020).

Embedding accountability and transparency into public data systems

A consistent message heard from the experts we interviewed for this paper was that governments cannot fully reap the benefits that digital tools and data integration offer without creating and maintaining public trust — with the caveat that some governments may seek to forego the need to build trust by using data and digital tools to exert more control over their citizens.

To build and maintain this trust, governments must embed accountability and transparency in public data systems and create clear and enforceable rules to protect citizens' rights that fit the technological, legal, and cultural context of their country. Achieving these aims will require sustained and flexible effort, given the rapidly changing nature of digital technology, as well as a new set of skills, roles, and institutions and the resources necessary to support their development.

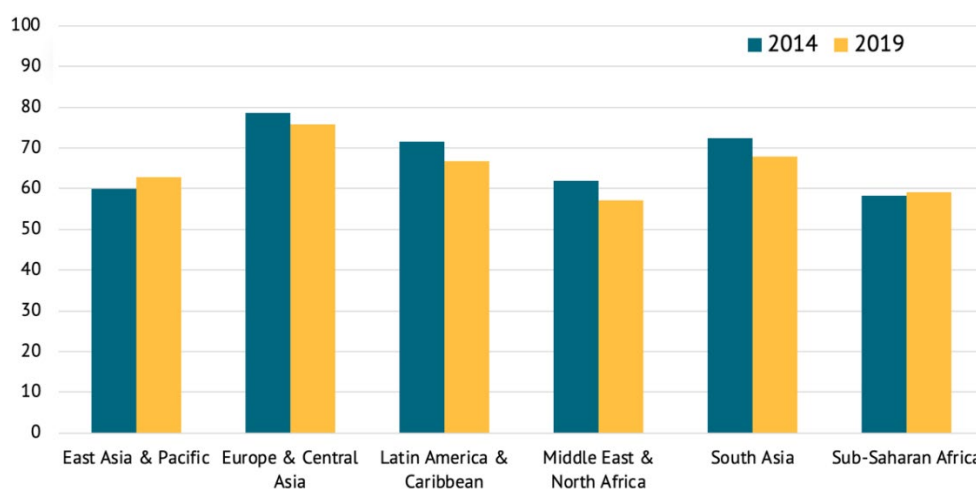
This task is demanding for the most digitally advanced countries and even more so for lower-income countries where resources are more limited, technical expertise is scarcer, and

¹³ Figure 1 was updated after publication to add countries that have pending legislation and to remove countries that passed laws before 2010, due to some ambiguities in the data.

rates of internet use are much lower.¹⁴ A 2014 paper by the Center for Global Development and the African Population and Health Research Center ([Delivering on the Data Revolution in Sub-Saharan Africa](#)) found that many sub-Saharan African countries lacked foundational “data building blocks” and often did not collect “data that are intrinsically important to the calculation of almost any major economic or social welfare indicators,” including “data on births and deaths; growth and poverty; taxes and trade; sickness, schooling, and safety; and land and the environment.”¹⁵ More recent work by the World Bank and OECD suggests that public data systems in other regions also rest on weak foundations and that progress to strengthen them has been slow and uneven over the last ten years.^{16,17}

Governments that wish to integrate data from external sources but start from a weak foundation face difficult questions about what reforms to prioritize and where to direct scarce resources as they seek to modernize. Most of the experts we spoke to believed that governments should first prioritize strengthening the collection of basic datasets before shifting focus to integrating data collected externally.¹⁸

Figure 2. Statistical capacity regional averages



Source: [World Bank Statistical Capacity Indicator Dashboard](#)

¹⁴ While over 80 percent of people in the United States and Europe have internet access, only 19 percent in sub-Saharan Africa and 20 percent in South Asia have access. From the World Bank’s open data portal see [Individuals Using the Internet \(% of Population\)](#) for more information.

¹⁵ CGD Data for African Development Working Group. [Delivering on the Data Revolution in Sub-Saharan Africa](#). July 2014.

¹⁶ World Bank. [Statistical Capacity Indicator Dashboard](#). Data scores last released in 2019.

¹⁷ OECD. [Key trends in development co-operation for national data and statistical systems](#). August 2020.

¹⁸ Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization, echoed this sentiment at the October 19, 2020 opening session of the UN World Data Forum by calling on countries to improve civil registration and vital statistics “build a strong foundation for data systems around the world.” See his opening session speech [here](#).

The development community's role

The development community — which we define broadly to include practitioners in international development institutions, bilateral development agencies, and smaller development organizations as well as government officials focused on supporting socioeconomic development — has spent considerable energy and resources helping governments expand connectivity, implement digital services, and improve the collection and analysis of data over the last twenty years. The focus on data collection has been even greater since 2015 when the United Nations recognized the need for “quality, accessible, timely and reliable disaggregated data” to achieve and monitor progress towards the Sustainable Development Goals (SDGs).^{19,20} More recently, many development organizations have championed public-private data partnerships as a way to improve government access to data insights.²¹

While the need to use data responsibly has been part of the “data for development” conversation since at least the early 2010s, most development organizations, with some notable exceptions, have given much more attention to supporting the use of digital tools than they have to how countries can govern the use of data and data ecosystems.²² This is now changing, however, in line with the broader shift in societal views about the risks of data misuse. Recent signs of this shift include:

- The World Bank’s decision to dedicate several chapters of its upcoming World Development Report (“Data for Better Lives”) to data governance issues and the commitment made in 2019 by the World Bank’s International Development Association (IDA) to support a new initiative on “Data for Policy” aimed at supporting the development of national statistical systems (NSS).^{23,24,25}
- The United Nations Development Group (UNDG)’s issuance of guidance on data privacy, data protection, and data ethics for using big data to achieve the 2030 Agenda for Sustainable Development.²⁶

¹⁹ United Nations. Transforming Our World: The 2030 Agenda for Sustainable Development. September 2015.

²⁰ For additional information, also see the UN’s A World That Counts: Mobilising The Data Revolution for Sustainable Development (2014).

²¹ For examples, see Theme 4.

²² Since the early 2010s, the responsible use of data has been part of the “data for development” conversation. Examples include the UN’s emphasis on privacy in their publication A World That Counts: Mobilising The Data Revolution for Sustainable Development (2014) and UN Global Pulse’s Big Data for Development: Challenges & Opportunities (2012) report. Responsible data use is also discussed through the World Bank’s focus on “analog complements” to the digital economy in its World Development Report: Digital Dividends (2016). Development organizations that have been ahead of their peers in addressing the need for development and aid organizations to use data responsibly include Development Gateway (see, in particular Increasing the Impact of Results Data (2016)), UN Global Pulse, and DataReady.

²³ World Bank. IDA 2019: Special Theme: Governance and Institutions. May 2019.

²⁴ World Bank. Evolution in the data ecosystem – an idea that’s got legs. April 2020.

²⁵ World Bank. World Development Report 2021: Data for Better Lives. May 2020.

²⁶ UNDG. Data Privacy, Ethics and Protection Guidance on on Big Data for Achievement of the 2030 Agenda. November 2017.

- The African Union and the Internet Society’s launch of the 2018 “Personal Data Protection Guidelines for Africa” to facilitate implementation of the Union’s Convention on Cyber Security and Personal Data Protection established in 2014.²⁷
- The call by the Committee for the Coordination of Statistical Activities for a Global Data Convention “for the safe and ethical use of data that establishes a social contract that strikes a balance between full use of data for development and wellbeing and the protection of security, privacy, and human rights, and between commercial use and public good.”²⁸

A challenging external environment

Countries that seek to establish systems that support using data in a fair, transparent, and accountable manner face several challenges outside of their control due to the structure of the global digital economy and geopolitical realities.

The most important of these is the dominance of the world’s largest tech firms and their outsized role in collecting, storing, and processing data to create detailed profiles of their users by tracking online activity, location, and social graphs and using this information to target advertisements.²⁹ Despite growing pushback within civil society against the “track and target” business model and ongoing efforts by the European Union to curb some of these activities, the situation is unlikely to change unless the United States and China, home to the world’s largest digital companies, take steps to rein in these practices on their own.³⁰

The limited control that most LMICs have over big tech companies that operate within their borders has led to growing concerns about sovereignty and increasing interest in data localization laws that require firms that collect data about a country’s citizens to store or process that data within the same jurisdiction. In the past, governments have justified such laws on the grounds that they enhance cybersecurity and data protection but more recently have cited economic competitiveness concerns.³¹ There is little evidence, however, that data localization laws further either aim.^{32,33}

Interest in imperfect solutions like data localization persists because global debates about data governance are still in a nascent stage, have focused largely on issues related to cross-

²⁷ African Union & Internet Society. Personal Data Protection Guidelines for Africa. May 2018.

²⁸ CCSA. Call for a Global Data Convention. October 2020.

²⁹ Pisa, Michael and John Polcari. Governing Big Tech’s Pursuit of the “Next Billion Users”. February 2019.

³⁰ For an example of civil society views on big tech, see Amnesty International’s Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights (2019). For more information on EU efforts see the Financial Times’ EU targets Big Tech with ‘hit list’ facing tougher rules (2020).

³¹ For example, see language on the benefits of data localization for building an AI sector in India in or the development of AI in the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

³² Bauer, Matthias, Martina F. Ferracane and Erik van der Marelthions. Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization. May 2016.

³³ Bhat, Ashi and Suneeth Katarki. India: The Debate – Data Localization And Its Efficacy. September 2018.

border data transfers, and solely reflect the priorities of wealthy countries.³⁴ Despite efforts to create institutional mechanisms to support global coordination on data policy where LMICs can voice their concerns, little traction has been made.³⁵

As a result, the data policy landscape remains fragmented with the world's most powerful economies taking different approaches, including the United States with its patchwork of sector-specific laws and regulations; the EU, with its more comprehensive approach based on the General Data Protection Regulation (GDPR); and China, which has implemented a GDPR-like framework for the commercial sector but whose government uses digital tools to support surveillance and stifle dissent. The lack of global consensus on how countries should govern data, particularly in regard to data privacy and protection, makes it harder for individual countries to determine the right path.

Research limitations

Before turning to the themes that came up most frequently in our interviews, we note the limits of both our aims and research approach:

- First, no two national data systems are identical and local context always matters. This raises a challenge for any project that seeks to examine these issues in a cross-country manner. Although we focus mainly on LMICs, which face greater resource constraints, more limited access to data expertise, and less digital connectivity, and rely more on external support for their national statistical systems, many of the challenges discussed in this paper are experienced by countries regardless of their level of income or digital development.
- Second, although we seek to highlight relevant research and initiatives whenever possible, this document is neither a systematic literature review nor a comprehensive summary of issues related to using data for development. Because our goal is to faithfully reflect the conversations we had, we limit our analysis to topics our interviewees raised most frequently, at the cost of touching lightly on other important topics like gender and data and the role of open data. The one area mentioned frequently by interviewees that we do not examine in depth is the shortage of funding needed to bring national statistical systems up to the level needed to meet and monitor the SDGs. We chose to omit discussion of this topic because it has been covered well in recent work by the OECD (“Key trends in

³⁴ See for example the G-20's Initiative on “Data Free Flow with Trust” discussed in ITIF's [Principles and Policies for “Data Free Flow With Trust”](#) (2019) and WEF's [Data Free Flow with Trust \(DFFT\): Paths towards Free and Trusted Data Flows](#) (2020).

³⁵ Recent efforts to advance ideas to support global cooperation on data and digital policy include the UN Secretary-General's [High-level Panel on Digital Cooperation](#) (2020), and [Pathways for Prosperity's Digital Diplomacy](#) (2020).

development co-operation for national data and statistical systems”) and PARIS21 (“Financing Challenges for Developing Statistical Systems”).^{36,37}

- Finally, to allow interviewees to speak with greater candor, we gave them the option of speaking off-the-record. For that reason, some of the views expressed to us and presented in this paper are not directly attributed to the speaker.

What we heard

Throughout the course of our interviews, the following eight themes came up most frequently.

Theme 1: The need to break down silos

Interviewees from both the data privacy and economic development communities lamented the lack of sustained engagement between the two groups and the way in which data privacy and economic development are often framed as opposing forces. Instead, most experts emphasized the synergies that could be gained through greater cooperation between the two fields. From a development perspective, the case for stronger cooperation is straightforward since lack of trust in digital ecosystems and the regulatory uncertainty caused by poor implementation of data privacy laws can impede economic growth and development. Ongoing shifts in both communities have created an opening for greater convergence and collaboration at the national, regional, and global levels. Multilateral organizations, including the IMF, United Nations, and World Bank can play a role in supporting collaboration at the global level by investing resources, lending expertise, and being open to engaging more with data privacy experts.

Theme 2: Promoting data governance as an enabler rather than a hindrance

Efforts to promote good data governance will be ineffective if they are solely donor-driven rather than aligned with government priorities. This is especially the case if national policymakers see data governance reforms as creating bureaucratic hurdles that impede useful innovation or divert resources from more immediate priorities. Development organizations can help convince government officials of the importance of good data governance by demonstrating: (1) how clear rules and reliable information can help policymakers achieve their objectives by facilitating data access, analysis, sharing, and appropriate re-use in a safe, transparent, and sustainable manner; (2) how those rules can be implemented at reasonable cost, both in terms of government resources and compliance burden; and (3) how universal principles of data governance can be applied and implemented in a manner that is tailored to local realities and proportional to risks.

³⁶ Lange, Simon. OECD. Key trends in development co-operation for national data and statistical systems. August 2020.

³⁷ Calleja, Rachael and Andrew Rogerson. PARIS21. Financing Challenges for Developing Statistical Systems: A Review of Financing Options. January 2019.

Theme 3: Equitably distributing the value of data by “closing the loop”

In many development projects the value of data — defined in terms of actionable insights that can be used to improve services and policy — does not flow back to the individuals, communities, and organizations who initially provide the data that underpins those projects. Instead, the data value chain effectively remains an open loop in which insights remain unshared with local communities from which the data was derived. Sharing analytical insights back to the communities where data is first collected can help government use data more effectively by strengthening the incentive to provide accurate data, helping communities develop the data skills, and creating a critically important feedback loop. Interviewees suggested a range of top-down and bottom-up solutions to achieve these goals. Some experts also suggested that companies should be required to return some of the monetary value produced from using data back to the countries and communities where it is collected.

Theme 4: The benefits, hazards, and hurdles of data collaboration

There is broad agreement within the statistics community that, although conventional statistical methods will continue to play an important role, they are too time-consuming, costly, and burdensome to satisfy the demand for higher frequency and more granular data alone. Transforming national statistical systems to make better use of existing and secondary data is a large and expensive effort that requires staff at national statistical offices (NSOs) to take on new responsibilities, develop new skills, and collaborate with outside actors. Public-private data partnerships can provide value but also raise risks and legal hurdles that governments must develop new expertise to manage. Legal uncertainty about how to comply with existing regulations was cited as the biggest barrier to such partnerships.

Theme 5: Establishing effective data protection frameworks

The last ten years has seen a rapid acceleration in the adoption of data protection frameworks by LMICs. One key driver of this trend is the EU’s enactment of the GDPR in 2016, since which it has become the de facto global standard for data protection and privacy rules. Many of the experts we interviewed, however, argued that the GDPR is a poor fit for lower income countries because of its complexity. This complexity helps explain the large gap between data protection “laws on the books” and the way in which those laws are implemented “on the ground” in most countries. Weak implementation in turn contributes to regulatory uncertainty, which experts cited as a major hurdle to forming successful data partnerships. Today, several LMICs are charting a new course by modifying their approach to data protection to meet domestic needs and priorities, while accounting for the impact of data privacy laws on inclusive economic growth, and in some cases extending beyond GDPR.

Theme 6: The need for regional and global solutions

Global agreement on a single set of data privacy principles essentially exists today in the form of the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

and *Convention 108+*.³⁸ But agreement on actual implementation guidance that provides the necessary protection while being flexible enough so countries can apply the principles in a manner consistent with their needs, priorities, and capacities is lacking. Achieving such agreement would require greater coordination at both the global and regional levels among data protection authorities and governments. Currently, global and regional institutional arrangements to bring together data protection officials as a unified body remain underdeveloped and there is a need not only for greater institutionalization at the global level but also pathways for LMICs to have greater voice in discussions around global data protection standards and implementation. There is also a need for meaningful multilateral engagement between data protection authorities and organizations focused on supporting economic growth and better social outcomes, including the international financial institutions and sectoral multilaterals such as the World Health Organization.

Theme 7: Developing the skills needed to govern data

Working on the legal aspects of data governance requires a unique combination of skills and expertise. The significant gap between the demand and supply of people with this expertise both within government and the private sector presents a major barrier to using data for development in most countries. Given the depth and specificity of the technical and legal knowledge that working on the multiple dimensions of data ecosystems requires, capacity-building efforts will need to be long-term engagements. Experts suggested several models and emphasized that donors will have an important role to play. They also debated the degree to which governments should rely on external actors to provide this expertise in the medium-term.

Theme 8: The impact of COVID-19

Interviewees believed that the policy response to COVID-19 pandemic has changed how society thinks about the use of data and digital tools in at least three ways: First, by accelerating the shift towards a digital-first approach in many countries. Second, by pushing governments to rely more on the private sector for information to monitor spread of the disease. And third, by heightening public awareness about the need for data privacy by making them more aware of the degree to which their data can be used to track their movements and behavior.

Based on these themes, in the conclusion, we offer several suggestions for a research and action agenda.

³⁸ See the OECD's [Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#) (last updated in 2013) and the Council of Europe's [Convention 108+](#).

Theme 1: The need to break down silos

Interviewees from both the data privacy and economic development communities lamented the lack of sustained engagement between the two camps and the way in which data privacy and economic development are often framed as opposing forces.³⁹ The general view was that this lack of collaboration has real costs that will grow over time unless steps are taken to bridge the two communities. While the relationship between development organizations and privacy regulators has been largely one of avoidance or even antipathy in the past, several shifts are occurring that may change this.

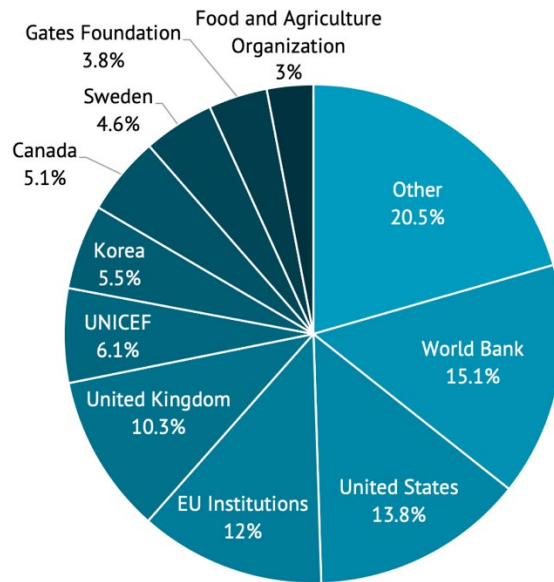
From a development perspective, the case for stronger cooperation between the two communities of practice is straightforward: While most countries have data protection and privacy laws in place, these laws are often poorly enforced, if at all. As awareness of the risks of data misuse increases and as the need to establish and preserve trust in digital tools and data becomes clearer, governments will find themselves under increasing pressure to reduce the risk of harm. Lack of trust in digital ecosystems and regulatory uncertainty caused by poor implementation of data laws can both impede economic growth and development and addressing these barriers will become more critical as economies become increasingly digitized.

International financial institutions (IFIs) dedicated to supporting economic development, particularly the World Bank, already play a large role in setting digital policy priorities in the countries they work with by influencing the institutional reforms they pursue, the laws they enact, and the organizations they establish data partnerships with (Figure 3 from the OECD provides a breakdown of financial support for data and statistics by provider).⁴⁰ But these organizations have not systematically engaged on issues related to data privacy and protection until recently.

³⁹ For more on the relationship between data privacy and innovation see IFIP's [Privacy as Enabler of Innovation](#) (2020) and the NBER's [Privacy and Innovation](#) (2011).

⁴⁰ Lange, Simon [OECD]. [Key trends in development co-operation for national data and statistical systems](#). August 2020.

Figure 3. Financial support for data and statistics by provider, 2016 - 2018



Source: [Key Trends in Development Co-operation for National Data and Statistical Systems. OECD Development Policy Paper. August 2020 No. 31](#)

Despite the late start, the IFIs are likely to play an increasingly important role going forward, as they establish data protection and privacy standards for client countries to meet. For example, the World Bank is now developing a set of minimum data privacy standards that it will eventually require countries to adopt or maintain before funding digital- and data-related projects.

This is not without controversy. Some interviewees noted instances in which IFI staff worked with governments on projects that raise data privacy concerns that they did not engage with relevant regulatory authorities to address. Others expressed concern that governments would become increasingly reliant on outside experts to provide the skills needed to meet externally imposed standards. Most interviewees, however, supported having donors use their influence to promote better data protection and privacy practices *if* they also take on the responsibility of helping governments build the requisite skills to meet these standards and coordinate their activities with the relevant data protection regulators.

Just as some of the data rights experts we interviewed wanted development organizations to pay more attention to data protection and privacy, several of the development practitioners we spoke to believed that DPAs are too often unwilling to account for the effect of regulation on economic outcomes and care more about levying punitive measures than helping organizations better understand how to comply with laws.

While the DPA officials we interviewed recognized that this perception exists, they noted a shift towards greater pragmatism and highlighted how some leading DPAs have begun to stress the importance of creating and implementing data privacy laws that support the

development of the digital economy.⁴¹ There is also increasing awareness among DPAs in high-income countries of the need to support LMICs in implementing their own data privacy laws as a way to encourage harmonization in support of a more global digital economy. For example, the European Commission has stated that privacy issues will be “on the top of the agenda” of the EU- Africa Digital Partnership.^{42,43}

Finding the middle ground where experts from both the development and data privacy communities can constructively engage is crucial to creating a digital economy that is inclusive, fair, trustworthy, and supportive of innovation. Ongoing shifts in both communities have created an opening for greater convergence and collaboration, which needs to happen at the national, regional, and international levels. We discuss opportunities for greater regional and international collaboration further in Theme 6.

Theme 2: Promoting data governance as an enabler rather than hindrance

The experts we spoke to uniformly welcomed the development community’s increasing interest in promoting good data governance. But many also voiced concerns that efforts in this area would be ineffective if they are solely donor-driven rather than aligned with government priorities. This is especially the case if national policymakers see data governance reforms as creating bureaucratic hurdles that impede useful innovation or require resources to be diverted from more immediate priorities, like health, education, job creation, and maintaining a social safety net.

While aid providers in the humanitarian sector have long recognized the importance of data privacy and ethical data use in their work with vulnerable populations, most development organizations (including the multilateral development banks, bilateral aid organizations, and large foundations) have only recently started to prioritize these issues publicly.⁴⁴ Several experts lamented that some major donors still do not conduct appropriate due diligence around possible harms when investing in digital projects nor require their grantees to conduct data protection and privacy impact assessments.

Despite these criticisms, there was widespread recognition among interviewees that large development organizations, particularly the World Bank, already play a determinative role in setting digital policy priorities in partner countries and most experts believed that donors can

⁴¹ For example, the Global Privacy Assembly’s [2019-2021 Strategic Plan](#) states that “The GPA will develop a clearer and broader narrative for a longer-term and more coherent approach to issues around the data protection aspects of regulation of the digital economy, including through closer engagement with relevant multilateral and international bodies.”

⁴² European Commission. [Towards a EU-Africa Digital Partnership](#). December 2017.

⁴³ Similarly, the UK Information Commissioner’s Office (ICO) aims to “develop stronger links with data protection authorities in Commonwealth countries via our leadership of the Common Thread Network. This will support and build capacity with other data protection authorities, increasing opportunities for international collaboration, particularly with emerging or fast-developing economies.”

⁴⁴ Key humanitarian documents on responsible include UN OCHA’s [Data Responsibility Guidelines](#) (2019) and the ICRC’s [Handbook on data protection in humanitarian action](#) (2020).

and should do more to promote transparent and accountable data use by providing advice, technical expertise, capacity-building services, and analytical frameworks that policymakers can draw on.

The need for greater country ownership

At the same time, many interviewees were torn between a desire to have donors play a more active role in promoting responsible data practices and a desire to give national policymakers greater say in designing programs financed by foreign aid, consistent with the tenet that country ownership leads to better and more sustainable outcomes.⁴⁵

Several experts drew attention to the *Principles for Digital Development* and its emphasis on “designing with the user” as providing a useful guide for development practitioners working on digital projects but noted that many of the organizations who have endorsed the Principles apply them inconsistently, with one expert noting that donor funding for digital policy is “not at all based on government priorities.”⁴⁶

If policymakers enact data governance reforms solely in response to external pressure without believing in their value, they are less likely to carry them out effectively or provide authority to the institutions created to implement them. Experts warned that this could hinder innovation by creating more regulatory uncertainty than had previously existed while failing to guard against unethical data uses.

For policymakers to see value in data governance, they must first see data as an asset whose maintenance is worth investing in — a view they are more likely to hold if they rely on data as an input to their own decision-making. As one expert mentioned, “once policymakers see the power of good-quality data and become used to thinking about decisions in a certain way, it becomes addictive and can set up a virtuous cycle.” Contrarily, “if they are not using data as an asset,” requiring policymakers to pay attention to data governance is “just forcing them to do something they don’t value in the first place.”⁴⁷

Beyond raising awareness of the risks of data misuse, the development community can help convince policymakers of the importance of responsible data use by demonstrating (at least) three things: First, how clear rules and reliable data protection mechanisms can help policymakers achieve their objectives by facilitating data access, sharing, and re-use in a safe, transparent, and sustainable manner. Second, how those rules can be implemented at

⁴⁵ Savedoff, William. What Is “Country Ownership”? A Formal Exploration of the Aid Relationship. October 2019.

⁴⁶ The Principles for Digital Development are a “set of living guidance intended to help practitioners succeed in applying digital technologies to development programs” designed and endorsed by the world’s largest development organizations, including The Bill and Melinda Gates Foundation, the Swedish International Development Agency (SIDA), the UN’s Children’s Fund (UNICEF), UN Development Program (UNDP), the World Bank, and the U.S. Agency for International Development (USAID), and the World Health Organization (WHO).

⁴⁷ Deepa Karthykeyan. Co-founder & Director, Athena Infonomics. Interview. June 16, 2020

reasonable cost, both in terms of government resources and compliance burden. And third, how universal principles of data protection and privacy can be applied in a manner that is tailored to local realities and proportional to risks.

Demonstrating all three will require developing better evidence on the costs and benefits of different approaches to governing data use. It will also require designing systems that align with the technical, institutional, and funding capacity countries possess and outlining a sequence of reforms that governments can follow to establish them. The wide variation in national data ecosystems argues for using a maturity model approach to assess government readiness to enact a graduated series of reforms that require increasing levels of sophistication. The World Bank will propose a such an approach in its upcoming World Development Report, which will be published in early 2021.⁴⁸

Theme 3: Equitably distributing the value of data insights by “closing the loop”

Because the digital divide closely mirrors existing inequalities, there is a significant risk that already disadvantaged groups will fall further behind unless steps are taken to ensure that the benefits of digitalization are fairly distributed across the whole of society. Over the last ten years, the development community has sought to do this, focusing on three areas: (1) increasing access to the internet and digital tools; (2) strengthening government data collection so that everyone is counted; and (3) promoting greater access to public data to strengthen government accountability and transparency.⁴⁹

Despite this work, a consistent theme in our interviews was that in many development projects the value of data—defined in terms of actionable insights that can be used to improve services and policy — does not flow back to the individuals, communities, and organizations who initially provide the underlying data. Instead, the data value chain effectively remains an open loop in which insights remain unshared with local communities.⁵⁰ While a handful of interviewees argued that the monetized value of data should be shared back with communities when it is used for commercial purposes, most experts focused on the importance of sharing insights generated.

For example, one expert who works for a data intermediary in the health sector observed that “there is a lot of work being done with data that has little value for the local environment. When people want to analyze data, it is often not done in country because the resources and skills aren’t there. The agenda is often not in the interest of the country and

⁴⁸ World Bank. *World Development Report 2021: Data for Better Lives*. May 2020.

⁴⁹ The UN report *A World That Counts: Mobilising The Data Revolution for Sustainable Development* (2014) highlights the need to improve data collection in lower-income countries to meet and monitor the SDGs and spearheaded a work program carried forward today by organizations like the *Global Partnership for Sustainable Development Data (GPSDD)*, *Data2x*, *Open Data Watch*, *PARIS21* and *SDSN TReNDS* and initiatives like *Data4Now*.

⁵⁰ Development Gateway highlighted the same problem, which it likened to a “broken link” in *Increasing the Impact of Results Data* (2018).

external actors harness the true value of what is produced. I would be hard-pressed to identify analysis of routine health data done out of country that had in-country benefits, in terms of policy change or usable insights.”⁵¹ This observation is consistent with interviewees’ experiences across different sectors and with different types of organizations.

A similar dynamic takes hold when donors choose to work outside of national data systems. As one expert who has overseen data projects in several LMICs noted: “there is a significant challenge with donors going into countries to implement programs and conducting their own ‘extractive data’ exercises without engaging with national statistical systems. The risk is that countries won’t develop the ability to make use of data produced in their own borders and this will push development towards a de facto paternalistic relationship — and weaken country ownership — because only donors will have the capacity to make use of the data.”⁵² Another expert noted that governments must often jump over legal hurdles to get access to data collected by international organizations within their own borders, and that NSOs often lack the legal expertise to negotiate for this access.

The open loop problem is not limited to cases involving foreign actors. Several interviewees working to strengthen data use by local communities noted their frustration that most NSOs and government agencies focus much more on collecting data than on exploring how data insights might be used by local communities and rarely engaged with community leaders to determine what insights would be most valuable. Others noted that NSOs are often unwilling to consider using new external data sources because of an overriding interest in controlling the quality of data used.

Solutions for closing the loop: Top-down, bottom-up, and meeting in the middle

Sharing analytical insights back to the communities where data is first collected can strengthen a government’s ability to use data effectively in several ways. First, people who receive value back from the data they provide have a greater incentive to ensure that information is accurate. Second, having access to data insights can help individuals and communities develop the skills needed to use this information as a guide to their decisions. Third, sharing insights back to communities supports the creation of feedback loops, which can help policymakers monitor the effectiveness of their policies on an ongoing basis and correct course as needed.⁵³

Interviewees suggested a range of solutions to achieve this goal and noted that progress would require both top-down and bottom-up efforts.

⁵¹ Grégoire Lurton. Data Science Lead, Bluesquare. Interview. June 9, 2020.

⁵² Agnieszka Rawa. Managing Director, Millennium Challenge Corporation. Interview. July 24, 2020.

⁵³ For more on the potential role of feedback loops in development see USAID’s [A guide to Digital Feedback Loops](#) (2019).

Top-down solutions

Development projects rarely share data insights back to local communities because project developers have little incentive to do so. Changing this will require a shift in perspective and prioritization at high levels of government and development organizations towards a model of engagement that seeks to empower citizens not only as producers of data but also as effective *users* of data.⁵⁴

As a first step, development organizations and government agencies should include clear ex-ante commitments in contracts for data-driven projects about how insights generated from analyzing data provided by local communities will be shared with them in a *usable* format that meets local needs.⁵⁵ For example, in Nigeria, the Logistics and Health Program Management Information Portal (LHPMIP) Project provided insights drawn from data collected across the country about the supply of HIV/AIDS treatments in the form of large printouts with charts and graphs posted at local health facilities.⁵⁶

Bottom-up solutions

Bottom-up solutions focus on increasing participation at the local level to identify the problems that communities most want to solve, and support more active engagement in collecting the data needed to address them.⁵⁷ The Open Institute in Nairobi, Kenya provides a powerful example of this model. The organization works directly with local communities to help them collect and visualize data pertaining to issues they want solve and then helps them engage with governments using the datasets they have created as a tool to push for policy reform and better service delivery.

While participatory models have strong appeal, there are questions about how easily they can be scaled, given the time and resources required. As one expert noted, the perceived value of data is mostly about automation and scale, but greater participation usually frustrates achieving both.⁵⁸ Ultimately, governments need to weigh the tradeoffs between data-driven projects that can be rolled out quickly and at scale versus those that rest on greater community engagement that are more aligned with the priorities of local communities.

⁵⁴ For related work see on empowering data users see the Pathways for Prosperity Commission's [Personal data empowerment: restoring power to the people in a digital age](#) (2018).

⁵⁵ Some organizations already follow this model. For example, during its project design phase, [Development Gateway](#) outlines a data management protocol focused on “getting as much data back into the hands of their government partners as possible, within regulatory constraints.” Josh Powell, CEO, Development Gateway. Interview. July 23, 2020.

⁵⁶ Olasupo Oyedepo, co-founder and Director, African Alliance of Digital Health Networks. Interview. June 9, 2020.

⁵⁷ For more on community-led problem identification see the GovLab and Bertelsmann Foundation's report: [People-led Innovation: Toward a Methodology for Solving Urban Problems in the 21st Century](#) (2018).

⁵⁸ Sean McDonald, co-Founder, Digital Public. Interview. July 27, 2020.

Meeting in the middle: The potential role of citizen-generated data

Developing scalable and sustainable models for greater local participation in creating and using public data requires greater collaboration between national governments, subnational governments, and local communities. One approach to such collaboration cited by several interviewees is for governments to make greater use of citizen-generated data, i.e., “data that people or their organizations produce to directly monitor, demand or drive change on issues that affect them” that is often produced “through crowdsourcing mechanisms or citizen reporting initiatives, often organized and managed by civil society groups.”^{59,60,61}

Citizen-generated data could help governments fill gaps in data collection more efficiently than traditional statistical methods in situations where there is a lack of trust between citizens and the government (e.g., FLOAT Beijing), or when an issue is not receiving enough attention from major institutions (e.g., HarassMap), or when crowdsourcing information is cost-effective (e.g., the United States Environmental Protection Agency (EPA) relies on citizens to monitor and assess water quality in their communities).⁶²

For government officials to become comfortable using citizen-generated data, they must first be willing to accept certain tradeoffs, including have less control over how data is collected, its quality and accuracy, and in certain cases, if it was collected with consent. Several interviewees noted that NSO staff may be reluctant to use “messier” citizen-generated data even if the datasets produced are highly relevant. But there are ways for governments to work with citizens to mitigate these risks.⁶³ For example, the EPA “provides a series of toolkits, quality assurance protocols, trainings, and engagement channels for volunteers” to promote better data quality.

Another hurdle cited by experts is the disparity in data skills available at national, subnational, and local levels, and the apparent unwillingness of many national governments to share data down to lower levels of government. If governments choose to integrate citizen-generated data into their data strategy, they will need to engage more closely with local governments and address this skills gap.

Despite these challenges, several countries are moving forward with integrating citizen-generated data into their broader statistical work. For example, in Ghana, the NSO (Ghana Statistical Services) has developed a mobile-based app that citizens can use to report incidents affecting their local community including trash and illegal dumping sites, which will

⁵⁹ Wilson, Christopher and Zara Rahman. [Citizen-generated Data and Governments: Towards a collaborative model](#). October 2015.

⁶⁰ Inter-American Development Bank. Interview. July 29, 2020.

⁶¹ Omar Seidu. Head, Demographic Statistics & Coordinator of Data for SDGs, Ghana Statistical Services. Interview. June 19, 2020.

⁶² See [Float Beijing](#), [HarassMap](#), and [OpenStreetMap](#) for examples of citizen-generated data projects.

⁶³ GPSDD, Open Knowledge International, and Public Data Lab. [Choosing and engaging with citizen generated data](#). 2019.

allow local governments to collect information at a high frequency and level of granularity to design policies and target services.⁶⁴

Theme 4: The benefits, hazards, and hurdles of data collaboration

Governing effectively requires access to accurate and timely information. Traditionally, governments have relied on official statistics produced by public agencies to guide their policymaking decisions. But the world's ongoing digital transformation has resulted in a proliferation of new data sources, many of which provide data at a higher frequency and level of granularity than traditional statistical methods can match. Policymakers increasingly want their national statistical systems to generate insights at the same level of frequency, precision, and speed.

There is broad agreement within the statistics community that, although conventional statistical methods like censuses and surveys will continue to play an important role, they are “too time-consuming, costly, and burdensome” to satisfy this demand alone.⁶⁵ As noted in the *Cape Town Global Action Plan for Sustainable Development Data* adopted in 2017, “national statistical systems face the urgent need to adapt and develop in order to meet the widening, increasing and evolving needs of data users, including for the full implementation of the 2030 Agenda for Sustainable Development.”⁶⁶

In most countries, NSOs play the primary role in organizing data collection, setting statistical standards across government, implementing statistical methods, and publishing the results.⁶⁷ While other government ministries may be responsible for producing statistics on specific topics, it is the NSO that “often acts as the central clearing house, bringing together the work of other statistical offices.”⁶⁸

To meet the demand for more relevant, timely, and granular data, NSOs increasingly seek to integrate secondary data (i.e. data that is not primarily collected for statistical purposes) into their work.⁶⁹ For example, data from telecommunications companies about individuals' movements was an important data source for COVID-19-related work. Transforming national statistical systems to make better use of secondary data is a large, expensive, and

⁶⁴ Omar Seidu. Head, Demographic Statistics & Coordinator of Data for SDGs, Ghana Statistical Services. Interview. June 19, 2020.

⁶⁵ OECD. *The role of national statistical systems in the data revolution*. 2017.

⁶⁶ [United Nations. Cape Town Global Action Plan for Sustainable Development Data](#). March 2017.

⁶⁷ Open Data Watch. *Open Data Inventory*. n.d.

⁶⁸ *Ibid.*, n.d.

⁶⁹ “Secondary data can be defined as any data holdings containing information which were not primarily collected for statistical purposes. Thus, secondary data includes everything from national and local administrative or public-sector data (e.g. tax, social security, or education records, public registers and smart meter utility data, to name a few), private and commercial data (e.g. credit rating, utilities data or store loyalty card information) and big and GIS data (e.g. credit/debit card purchase transactions, mobile phone CDR, satellite imagery, or ASI ship identification records).” Steve MacFeely. [In search of the data revolution: Has the official statistics paradigm shifted?](#) July 2020.

highly technical effort that requires NSO staff to take on new responsibilities and develop new skills. It also requires extensive collaboration with other government agencies and non-governmental organizations including academic institutions, research organizations, and in some cases, private sector companies.⁷⁰

Administrative data

Administrative data has historically been the most important source of secondary data for governments, which government agencies generate through the operation of public services.⁷¹ Sources of administrative data useful for supporting and monitoring progress towards the SDGs include birth and death registries, health records, migration registers, and tax records. Because these data are collected through day-to-day business operations, they are often more cost-effective to collect than relying on censuses and surveys and can also be more accurate, detailed and have better coverage.⁷²

Making effective use of administrative data depends on the ability to merge data across different systems without losing meaning.⁷³ But achieving interoperability across different ministries and levels of government is a difficult challenge even for well-resourced governments. While some of the hurdles to interoperability are legal and political, involving a lack of trust between agencies or a desire to silo data for political advantage, others are technical, including inconsistent database design, tagging, and coding.⁷⁴

Data collected by the private sector

Much of the development community's interest in using secondary data has shifted to data collected by the private sector, which governments can use to fill knowledge gaps that official statistics and administrative data alone cannot address, increasing the speed and precision with which they can respond to changing realities and citizen needs.

In recent years, a growing number of development organizations have promoted data collaborations between the public and private sector as a way for policymakers to access

⁷⁰ Organizations like [PARIS21](#), [UNSD](#), [GPSDD](#), and [Open Data Watch](#) are working with governments to help countries strengthen and modernize their NSOs and the broader national statistical systems in which they operate, including a number of organizations dedicated to supporting this process in lower income countries.

⁷¹ In [Latin America and the Caribbean-Africa Peer Exchange on Administrative Data](#) (2019), GPSDD defines administrative data as including “data collected for legal compliance or for service delivery, data documenting government decisions, and data generated to support planning, implementation, and monitoring progress.”

⁷² Rivas, Lisbeth and Joe Crowley. IMF. [Using Administrative Data to Enhance Policymaking in Developing Countries: Tax Data and the National Accounts](#). August 2018.

⁷³ This definition of interoperability comes from Liz Steele and Tom Orrell in their publication: [The frontiers of data interoperability for sustainable development](#) (2017) and is cited by Luis González Morales and Tom Orrell in GPSDD's [Interoperability: A practitioner's guide to joining-up data in the development sector](#) (2018).

⁷⁴ For a broad summary of the challenges of sharing administrative data across government see GPSDD's [Latin America and the Caribbean-Africa Peer Exchange on Administrative Data](#) (2019). For an overview of the technical hurdles to interoperability see GPSDD's [Interoperability: A practitioner's guide to joining-up data in the development sector](#) (2018).

information and insights that most governments are unable to produce on their own.⁷⁵ The World Bank, which has championed several initiatives that involve public-private data collaborations including Development Data Partnership and Data4Now, has argued that “harnessing the full development potential of data entails repeated reuse of data,” including “data originally collected for commercial purposes for public policy (and reuse of public intent data by firms).”⁷⁶

Governments are also increasingly turning to private companies and non-profit organizations that offer data integration, management, analysis, and visualization services.⁷⁷ These organizations can provide technical skills that would otherwise be unavailable to resource-constrained governments and often function as de facto data brokers, connecting actors in the national statistical systems with secondary data providers.

While most interviewees believed that public-private data partnerships can provide value to governments and their citizens — and several were directly involved in supporting them— there was also broad agreement that these collaborations raise risks that have not been given the attention they deserve.⁷⁸ These include lack of transparency and controls on how companies might seek to use merged data for commercial gain and how integrating data from public and private sources can make it easier for governments to surveil citizens.⁷⁹ The latter risk is particularly important since most national data privacy laws exempt government activities related to national security, law enforcement, and preventing threats to public safety.

Other interviewees pointed to broader concerns raised by the intertwining of interests between governments and large tech companies that may make it more difficult for countries to hold these companies accountable.

Several interviewees also argued that development organizations needs to do a better job monitoring and evaluating how data collaborations are used to further the public good.⁸⁰ This includes being more transparent about the purpose for which data is being shared, the

⁷⁵ Recent initiatives that support public-private data collaborations include the [Development Data Partnership](#) led by the Inter-American Development Bank, International Monetary Fund, and World Bank; the [Data For Now](#) Initiative led by the Global Partnership for Sustainable Development Data, the World Bank, the United Nations Statistics Division, and SDSN TReNDS; and ongoing work by organizations like [GovLab](#) and [UN Global Pulse](#).

⁷⁶ Note that we are combining two separate quotes from pages 6 and 12 of the World Bank’s [2021 World Development Report Data for Better Lives Concept Note](#) Concept Note.

⁷⁷ Examples include companies like [BlueSquare](#) and [Zenysis](#), and non-profits like [Flowminder](#).

⁷⁸ The World Economic Forum’s [Data Collaboration for the Common Good: Enabling Trust and Innovation Through Public-Private Partnerships](#) (2019) distinguishes between four types of risks raised by data collaboration: commercial risks, regulatory risks, security risks, and privacy and ethical risks.

⁷⁹ Regarding the former, “the social license of public sector data use may not extend to private sector use. Empirical research consistently suggests public discomfort with the use of health data for commercial gain, or with commercial (for-profit) companies accessing their health data.” Angela Ballantyne. [Big Data and Public-Private Partnerships in Healthcare and Research](#). September 2019.

⁸⁰ For more on M&E for digital and data-related projects see: [Development Gateway. Understanding Data Use: Building M&E Systems that Empower Users](#). August 2018. And Digital Principles. [Monitoring & Evaluating Technologies in Social Change Projects](#). n.d.

controls put in place to limit use beyond this purpose, the risks of using certain types of potentially sensitive data, and the extent to which approaches like anonymization and aggregation might help mitigate these risks — and evaluating the safety and value of a project based on these criteria.

Finally, several experts expressed concern that the asymmetry in resources and expertise between large tech companies and LMIC governments raises the risk that data sharing arrangements will be negotiated in the favor of the former and fail to include reasonable protections against data re-use beyond the originally intended purpose of data sharing.

Hurdles to successful collaboration

Despite growing interest in public-private data partnerships, “persistent barriers are holding back public-private data sharing at scale.”⁸¹ A recent collaborative learning exercise led by the Global Partnership on Sustainable Development Data (GPSDD) identified four key barriers to public-private data sharing:

- Lack of common standards limit interoperability and quality of insights
- Weak legal and regulatory frameworks contribute to a lack of trust
- Low capacity on the data holder and data user sides limits the scope for analysis and an understanding of what is possible and limits transparent communication with the public around management of privacy and security
- Misaligned incentives and a limited body of evidence on the value of data prevents partners from agreeing on business models based on shared value

In our interviews, the most frequently cited barrier to establishing a successful data partnership was the need to comply with legal requirements related to data protection and privacy — and understanding what those requirements are. As one expert noted, “dealing with legal issues is Step 0.1 when setting up a data sharing partnership.”⁸²

The organizations we spoke to took different approaches to assess and manage the legal risks involved with sharing data in specific contexts. Some created their own assessment tools or relied on pre-existing templates like the GDPR’s data protection impact assessment.^{83, 84} Others, like UN Global Pulse, have gone a step farther by providing public access to the tools they have created, including a Risk, Harms, and Benefits Assessment Tool and a Due Diligence Tool.⁸⁵ Relatedly, the Contracts for Data Collaboration initiative

⁸¹ Global Partnership for Sustainable Development Data. [Unlocking Privately Held Data for Public Good](#). Final Report. July 2020.

⁸² Tracey Li. Data Scientist and Project Manager, Flowminder. Interview. July 7, 2020.

⁸³ [EU GDPR Data Protection Impact Assessment](#). N.d.

⁸⁴ For example, before formalizing data sharing agreements for projects aimed that public sector of use telecom data, the Digital Impact Alliance applies its own risk assessment template, data governance, and security plans. Organizations that Digital Impact Alliance. [Responsible Use of Network Data: Ensuring responsible, widespread access and use of network data for SDG decision-making](#). N.d.

⁸⁵ [UN Global Pulse: Risks, Harms, and Benefits Assessment Tool](#), [UN Global Pulse: Due Diligence Tool](#)

provides an analytical framework and an online library of legal clauses to assist parties seeking to establish data sharing arrangements.⁸⁶

Despite the availability of these tools, several experts lamented what they saw as a lack of available guidance and noted that they had taken part in projects in which data sharing agreements were drafted on an ad hoc basis and without appropriate due diligence. While this disconnect may be due to a simple lack of awareness of the tools that exist, a more basic problem may be that much of the existing guidance pertains to ensuring ethical and responsible data sharing, while organizations on the ground demand more guidance on the related but distinct legal aspects of data sharing, which must often be tailored to national frameworks.

Interviewees suggested several ways to address these challenges including having DPAs play a more active role in public-private data collaborations. We discuss this option and other ways to support compliance with data protection and privacy laws in the next section.

Theme 5: Establishing effective data protection frameworks

As human activity becomes increasingly digitized, the need to have rules in place to govern how data is used throughout its lifecycle and across different data systems becomes more important. The challenge facing governments is how to establish rules that protect citizens from harm while still allowing for useful innovation.

Modern approaches to data protection can be traced back almost a half century with the establishment of the *Fair Information Practices* in the United States in 1973 and the subsequent codification of and expansion on those principles by the OECD in the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* published in 1980.⁸⁷ The years that followed were characterized by slow and steady diffusion and development of national frameworks for data protection, mostly in wealthier countries, based and building on these principles.

Over the last two decades, however, and particularly in the last ten years, the number of countries that have adopted data protection legislation has significantly increased. Since 2010, 64 countries, the vast majority of which are LMICs, have enacted new data privacy laws, bringing the total number of countries with such laws in place up to 146.⁸⁸

⁸⁶ The [Contracts for Data Collaboration](#) is a partnership between NYU's GovLab, SDSN Trends, University of Washington, and World Economic Forum.

⁸⁷ The *Fair Information Practices* formed the early basis for European and US privacy law and underly most global privacy laws today. Dixon, Pam. [A Brief Introduction to Fair Information Practices](#). December 2007.

⁸⁸ Greenleaf, Graham and Bertil Cottier. [2020 Ends a Decade of 62 New Data Privacy Laws](#). January 2020.

Table 1. Countries that enacted new data privacy laws between 2010 - 2020

Region	Number of countries with data privacy laws and bills	Countries that introduced and passed data privacy legislation between 2010 – 2020
Africa	23	Algeria (2018), Angola (2011), Botswana (2018), Chad (2015), Congo-Brazzaville (Republic of Congo) (2019), Côte d'Ivoire (2013), Egypt (2020), Equatorial Guinea (2016), Gabon (2011), Ghana (2012), Guinea (Conakry) (2016), Kenya (2019), Lesotho (2011), Madagascar (2015), Malawi (2016), Mali (2013), Mauritania (2016), Niger (2017), Nigeria (2019), São Tomé and Príncipe (2016), South Africa (2013), Togo (2019), Uganda (2019)
Caribbean	13	Antigua & Barbuda (2013), Aruba (2011), Barbados (2019), Bermuda (2016), BES Islands (2010), Cayman Islands (2017), Curaçao (2010), Dominican (2013), Jamaica (2020), Saint Kitts & Nevis (2018), St. Lucia (2011), St. Maarten (2010), Trinidad and Tobago (2011)
Latin America	7	Brazil (2018), Costa Rica (2011), Mexico (2010), Nicaragua (2012), Panama (2018), Philippines (2012), Peru (2011)
Middle East	6	Abu Dhabi (2015), Bahrain (2018), Lebanon (2018), Qatar (2016), Yemen (2012), United Arab Emirates [sectoral, various incl, 2012, 2016]
Asia	5	Bhutan (2017), Indonesia (2016), Malaysia (2010), Singapore (2012), Vietnam (2010), [China (2016) - cybersecurity, partial only], [India - ITA, partial only], [Enforcement of Thailand's PDPA postponed until May 2021].
Central Asia	4	Kazakhstan (2013), Tajikistan (2018), Turkmenistan (2017), Uzbekistan (2019)
Europe	5	Faroe Islands (2010), Georgia (2012), Kosovo (2010), Turkey (2016), Ukraine (2011)

Data from Greenleaf's [Global Tables of Data Privacy Laws and Bills \(6th Ed January 2019\)](#) and Greenleaf and Cottier's [2020 Ends a Decade of 62 New Data Privacy Laws](#). Additional research conducted by World Privacy Forum (2020). Note: Two significant privacy bills which have been introduced but not passed are India's Personal Data Protection Act (Tabled in Parliament December, 2019), and Zimbabwe's Cybersecurity and Data Protection Bill 2019 (Gazetted March 2020).

Several factors have driven the rapid increase in new data protection and privacy laws in LMICs in recent years, including: the catalytic effect of the EU GDPR; growing awareness of the risks of data misuse and the desire to create an enabling framework for responsible innovation; and the need to meet donor standards on data protection and privacy.

The GDPR, which was enacted in 2016 and implemented in 2018, altered the global data protection landscape by providing a more rigorous model for protecting the privacy of individual data than had previously existed through mechanisms that strengthened individual control over how data is used and made data controllers more accountable. The GDPR also explicitly incorporated the *Privacy By Design Principles*, which seek to ensure “that personal

data are automatically protected in any given IT system or business practice” by default.^{89,90} The GDPR helped catalyze the global expansion of data protection frameworks through its extraterritorial applicability discussed further in Box 1.

Box 1. The GDPR’s extraterritorial impact

One of the most controversial elements about the GDPR is the extraterritorial scope of its approach to determining the privacy and security of data transfers to third countries, which requires the European Commission to determine whether non-EU countries “provide a level of protection for personal data which is comparable to those of EU law” as the basis for transferring data. Taken a step further, jurisdictions can further pursue a formal “adequacy decision.”⁹¹ If a country is deemed adequate by the EU, its ease of digital trade and digital economy opportunities are better than jurisdictions without this designation. This has led to a push to achieve adequate compliance with the GDPR by governments outside of the EU, who want to ensure that their domestic companies are not competitively disadvantaged.

The EU adequacy process, which began with the original EU Data Protection Directive (EU 95/46), which was adopted in 1995, and continued with the GDPR, has long been criticized for its opacity. Several interviewees expressed frustration that, in their view, the European Commission has not provided clear guidance on the basis of their adequacy decisions and highlighted that no LMIC countries in Africa or Asia have received an adequacy decision.⁹² They also expressed concern that a lack of adequacy could handicap smaller economies, as they will be less able to engage in digitally linked trade with the EU and may receive less investment as a result.

Today, the GDPR is the baseline to which all other countries’ data protection framework are compared and every framework enacted in recent years reflects its influence.⁹³ Ultimately though the GDPR is a European law designed to deal with European challenges from a European perspective. While the experts we spoke to recognized its importance in providing a rigorous model for achieving data privacy, they also noted that the framework is challenging for governments to implement due to its complexity and high degree of

⁸⁹ European Data Protection Supervisor. [Preliminary Opinion on privacy by design](#). May 2018.

⁹⁰ Privacy by Design evolved from early attempts to incorporate fair information practice principles directly into the design and operation of information and communications technologies (See [Privacy by Design: Origins, meaning, and prospects for assuring privacy and trust in the information era](#) (2011)). Today, Privacy by Design is a methodology for proactively embedding privacy into IT, business practices, and networked infrastructures. The measures are designed to anticipate and prevent privacy invasive events before they occur.

⁹¹ European Parliament and Council of the European Union. [GDPR Third Countries](#). April 2016.

⁹² To date the EC has only recognized a handful of countries as providing adequate protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. Adequacy talks are ongoing with South Korea. Notably, the US had an adequacy “workaround” in the EU-US Safe Harbor, which was deemed not acceptable in a series of famous court decisions generally known as Schrems I and II. For more information see [Adequacy Decisions](#).

⁹³ Greenleaf, Graham and Bertil Cotter. [2020 Ends a Decade of 62 New Data Privacy Laws](#). January 2020.

prescriptiveness, and cautioned that it was a poor fit for LMICs without significant modification.⁹⁴

A consistent theme in our interviews was that even when data protection laws exist “on the books,” they may not be translated into “law on the ground,” with the effect that protections for individuals and groups may remain weak. The gap between written law and effective implementation exists even in the EU, where Member States are struggling to implement and enforce the GDPR, despite having had roughly 25 years of practice implementing a similar framework under the Data Protection Directive, which contains many of the same provisions as the GDPR.⁹⁵

For most LMICs, the challenge of translating new data privacy laws into action is far greater. Interviewees emphasized three related barriers to effective implementation: the complexity of existing data privacy frameworks, the lack of the legal skills and knowledge needed to comply with data privacy laws across government, and a shortage of funding for DPAs.

Why data privacy is seen as a barrier

Poor implementation of existing data privacy laws or the absence of such laws can impede the use of data to improve development outcomes. Each of the development practitioners we spoke to had been directly or indirectly involved in projects that had either failed to start, been derailed, or were significantly slowed by concerns related to data protection and privacy. The reasons for these outcomes varied across projects:

Regulatory uncertainty: Several experts noted that government officials in countries with newly established data protection laws often do not know how to comply with new regulations and therefore may refuse to consider engaging in projects that involve data sharing, even when those projects seem to comply with existing laws.⁹⁶ More generally, experts said that uncertainty about how to act in accordance with existing data protection laws, or how to act in their absence, was a major impediment to developing successful data sharing projects — and that this uncertainty extends to both government officials and their development partners.

Lack of technical tools and skills: In addition to a lack of regulatory clarity, experts also noted a lack of understanding about how to implement technical solutions that could mitigate the risks of sharing potentially sensitive data. For example, one expert noted that assessments conducted in one sub-Saharan African country revealed that the NSO had steered away from data sharing projects, even when it was technically feasible to significantly

⁹⁴ For example, GDPR requires proof of compliance (Articles 6 and 7). Many times, this will require technological proof of compliance, such as keeping digital logs of individual consent, or mapping and meta-tagging microdata which requires extensive data mapping. Many LMIC digital start-ups are likely to find this type of compliance a challenging, if not insurmountable, obstacle.

⁹⁵ European Commission. [Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation](#). June 2020.

⁹⁶ Josh Powell. CEO, Development Gateway. Interview. July 23, 2020.

limit the privacy risks involved, because NSO officials lacked training on how to anonymize data.

Lack of a data protection framework: Others noted how the absence of national data privacy laws can derail projects and investments as donor organizations have become increasingly unwilling to support data projects in countries that lack these protections.⁹⁷ One interviewee countered this by arguing that having a data protection framework in place is a poor predictor of whether governments will engage in data sharing partnerships and whether those partnerships will be successful, and that these outcomes depend more on how “progressive” regulators are and how clear their practical guidance is.

Unwillingness to engage with Data Protection Authorities: Several interviewees who were responsible for managing data sharing projects noted their reluctance to engage with DPAs for assistance, even when they had questions about how to comply with regulations because they were skeptical that a DPA could provide timely assistance and reluctant to risk slowing down their projects. Several other interviewees, however, reported that the DPAs they engaged with played a helpful role in clarifying how to comply with new regulations.

The path forward

The challenges facing governments in establishing and implementing data privacy frameworks that provide necessary protections while supporting innovation require comprehensive and system-wide solutions. Interviewees said that progress is most needed in the following areas:

Putting global standards in local context: Choosing simplicity over complexity

Governments with resource and capacity constraints must find ways to implement data privacy laws efficiently and effectively. For that reason, some experts suggested that governments should shift away from treating GDPR as the basis of their laws towards other frameworks that are less prescriptive, like the Council of Europe’s *Convention 108+*.⁹⁸ These experts noted that *Convention 108+*, which is the only legally binding multilateral instrument on the protection of privacy and personal data, retains high standards on protecting human rights while allowing governments greater flexibility in implementation.

One obvious challenge is that many countries have already enacted complex data privacy frameworks influenced by the GDPR and they are unlikely to change their approach in the absence of a major shift in the global discourse on data privacy, which puts more pressure on regulators to translate existing laws in a manner that allows them to be effectively carried out.

One way governments can do this is by translating legislative principles into concrete codes of practice (or “codes of conduct”) that specify how data protection and privacy frameworks

⁹⁷ The World Bank’s [Nigeria Digital Identification for Development Project](#) (2020) is a recent example.

⁹⁸ Council of Europe. [Convention 108+ website](#). N.D.

can be operationalized in specific settings and contexts — a process that the GDPR spells out in detail in Article 40 and that many GDPR-influenced policy frameworks include a provision for.^{99,100} Such codes typically focus on one sector or industry and are developed in collaboration between relevant stakeholders and the regulator, usually the DPA, which is given the authority to enforce them. Each of the DPA officials emphasized the importance of such codes in allowing governments to translate "law on the books" to "law on the ground" in a practical manner tailored to local context.

A strong, active, and pragmatic DPA

Having a strong and active DPA that takes into account the effect of data privacy laws on innovation, enforces laws in a proportional manner, and can provide clear guidance on how to comply with existing laws is the best way to achieve the regulatory clarity that organizations seek. But achieving these aims requires both sufficient staffing and funding.

Although cross-country data on how DPAs are funded is unavailable, there was broad agreement among interviewees that the vast majority of DPAs in LMICs are insufficiently funded. This lack of resources makes it harder for them to carry out enforcement, develop guidance, build awareness, and attract staff with the appropriate skills, each of which is necessary for successful implementation of privacy laws. Several interviewees also emphasized the importance for DPAs to have real enforcement power, without which both government agencies and private companies are more likely to ignore them.

Finally, several experts noted that DPAs should seek to cultivate a reputation for being pragmatic, solution-oriented, and eager to assist others in using data legally and responsibly. If they instead implement data protection laws in a punitive manner, organizations are more likely to try to avoid engaging with DPAs when possible.

LMICs charting new path on data protection and privacy

Today, several LMICs are charting new paths in data protection and privacy law by modifying their approaches to meet domestic priorities and, in some cases, extending protections beyond those offered by the GDPR. For example, Kenya's Data Protection Act of 2019 contains many elements of the GDPR but makes several adaptations.¹⁰¹ Notably, the definition of "data processor" under the Kenya law includes "public authority, agency, or other body," which is broader than the GDPR's definition. The affirmative inclusion of public agencies, combined with a requirement for organizations to conduct risk assessments for activities that have the potential to create high risk to the rights and freedoms of data subjects, suggests that the government of Kenya will be required to conduct data protection

⁹⁹ European Parliament and Council of the European Union. [Article 40 GDPR: Codes of Conduct](#). April 2016.

¹⁰⁰ In addition to codes of conduct, voluntary consensus standards (VCS) are another important multi-stakeholder standard that have received more attention in recent years. VCS can be used by jurisdictions that lack GDPR-like provisions for creating codes of conduct if a formal government entity has ownership of the process and can enforce the final standards. For more on VCS, see U.S. Office of Management and Budget. [Federal Register: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities](#). February 1998.

¹⁰¹ [Kenya Data Protection Act](#). November 2019.

impact assessments on its own programs, which is something that the GDPR does not require of EU member states.

The way data privacy jurisprudence evolved in Kenya is also instructive, as it reflects the influence of civil society organizations, like the Nubian Rights Forum, whose legal challenge of Kenya’s public digital ID program (Huduma Namba) likely contributed to a fast-tracking of the data protection bill.¹⁰²

India’s draft Personal Data Protection Bill — which builds off a landmark decision by the Indian Supreme Court in 2017 that established data privacy as a fundamental right and a white paper drafted by a committee of experts led by former Supreme Court justice B.N. Srikrishna — advances the debate on national approaches to data governance by introducing several novel measures.¹⁰³ The Bill is also explicit about the relationship between data governance and economic growth, noting in its introduction that “it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion.”¹⁰⁴

Although the Personal Data Protection Bill mirrors some aspects of the GDPR — for example, it establishes an independent data protection authority and certain privacy rights — it deviates in several important ways, including:

- **Broader definitions of personal and sensitive personal data:** The draft Bill defines “personal data” as data “about or relating to a natural person who is directly or indirectly identifiable” but, unlike the GDPR, does not take into account the “reasonable likelihood” that an individual will be identifiable.¹⁰⁵
- **Criminalizing the reidentification of personal data:** The Bill makes it a criminal offense punishable by up to three years imprisonment for anyone to knowingly or intentionally re-identify personal data that has been de-identified by a data fiduciary or a data processor.
- **Data localization:** Unlike the GDPR, which eschews explicit data localization measures, India’s draft Bill states that all “critical personal data” must be stored and processed only in India, while all “sensitive personal data” must be stored in the country but can be processed outside subject to certain conditions.

India’s draft bill has come under criticism from different angles. Some critics have argued that the Bill will undermine economic growth due to its limitations on data processing,

¹⁰² Ikagai Law. [Kenya’s Huduma Namba: Ambition Fraught with Risk](#). April 2020.

¹⁰³ India. [The Personal Data Protection Bill](#). December 2019.

¹⁰⁴ [Justice K.S.Puttaswamy\(Retd\) vs Union Of India Judgement](#). September 2018 (decision made in August 2017). [White Paper of the Committee of Experts on a Data Protection Framework for India](#). December 2017.

¹⁰⁵ Covington & Burling LLP. [India Introduces Updated Draft of Personal Data Protection Bill](#). February 2020.

perceived high compliance burden, and data localization requirements.¹⁰⁶ Others have complained that the Bill grants too much power to the state because of “numerous vaguely defined exemptions on data regulation” that could enable greater state surveillance.¹⁰⁷

Despite these criticisms, the passage of the Personal Data Protection Bill, which is expected to occur (perhaps with modifications) in 2021, will have global consequences. Unlike most LMICs, India’s economy and population is large enough to give the country leverage over the world’s biggest tech firms, which are more likely to modify their business practices to comply with India’s law than they would be for smaller countries. In addition, other governments will pay close attention to how India’s approach works in practice to see if it provides a good model for data protection and privacy in a fast-growing and fast-digitalizing economy.

Other countries are also taking steps to develop new approaches to data protection and privacy, at least on paper. For example, Togo’s Data Protection Law passed in 2019 stipulates that any merging (“interconnection”) of data must not violate human rights or privacy and sets out requirements for data controllers to obtain authorization for merging data.¹⁰⁸

Whether these laws are effective in practice and how they affect economic outcomes will depend largely on how they are implemented. This makes it important for DPAs to understand the economic implications of their actions and raises the value of guidance that can support flexible and effective implementation.

Box 2. Regarding the use of consent as a primary method of effectuating data protection

Several experts argued that modern data protection frameworks, including the GDPR, are fundamentally flawed in their reliance on individual consent (though it is worth emphasizing that consent is one of six lawful bases upon which data can be processed under the Regulation). One critic asserted that many of the GDPR’s protections fall away once consent is granted, which puts an unreasonable burden on individuals, particularly those with limited digital literacy. Others argued that overreliance on individual consent creates a “missing the forest for the trees” problem by failing to address the potential for group harms that can arise from profiling and machine learning.¹⁰⁹

¹⁰⁶ Burman, Anirudh. Will India’s Proposed Data Protection Law Protect Privacy and Promote Growth? March 2020.

¹⁰⁷ Basu, Arindrajat and Justin Sherman. Key Global Takeaways From India’s Revised Personal Data Protection Bill. January 2020.

¹⁰⁸ See Articles 33 and 34. Togo. Data Protection Law (in French). October 2019. For more on Togo’s law, see Dixon, Pam Africa’s Rising Leadership in Privacy

¹⁰⁹ Similar arguments are made in Group Privacy: New Challenges of Data Technologies (2017) and The Data Delusion (2018). However, other critics, especially in wealthy countries, strongly criticize the GDPR for stifling AI innovation due to its prohibitive language regarding automated profiling.

Today, there is growing interest in data governance approaches that rely less on consent mechanisms. In its 2020 paper “Making Data Work for the Poor” the Consultative Group to Assist the Poor (CGAP) suggests two models for ensuring that data is only used for legitimate purposes and in a manner that serves individuals’ interests: the first, would require organizations to pass a “legitimate purposes test,” and the second would require them to abide by a fiduciary duty requirement.¹¹⁰

While these ideas have not been comprehensively adopted, the GDPR includes legitimate interest as one of the six lawful bases for processing data (Article 6(1)(f)), as do many of the GDPR-inspired legal frameworks.¹¹¹ And India's draft Personal Data Protection Bill also invokes the concept of fiduciary duty.

Theme 6: The need for greater global and regional coordination

Global or regional agreement on a single set of data privacy principles essentially exists today in the form of both the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the Council of Europe’s *Convention 108+*, which are well-established and widely approved.¹¹² However, broad agreement on how these principles should be implemented is lacking. Many countries stand to benefit from guidance on how these principles can be applied in a way that is effective and flexible enough for resource-constrained governments to tailor to their needs.

Achieving agreement on such guidelines will require greater coordination at the global level.¹¹³ But global and regional institutional arrangements to bring together data protection officials are underdeveloped compared to those in other fields where cross-border spillovers are more pronounced, including finance and health. For example, there is no equivalent of an institution like the Financial Stability Board, which promotes coordination among national financial authorities and international standard-setting bodies, or the World Health Organization, which coordinates multiple country-level data flows.

In the past few years, however, some of the world’s leading DPAs have taken steps to transform an active global community of DPAs into a model that more closely resembles a multilateral institution in composition and governance. The most significant development was the remaking of the International Conference of Data Protection and Privacy Commissioners (founded in 1979) from an annual conference into a year-round organization

¹¹⁰ Medine, David and Gayatri Murthy. *Making Data Work for the Poor*. January 2020.

¹¹¹ A good discussion of how legitimate interests and lawful basis for processing interact in the GDPR may be found at the UK Information Commissioner's Office Guidance on this interaction, see [What is the 'legitimate interests' basis?](#)

¹¹² See the OECD’s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (last updated in 2013) and the Council of Europe’s *Convention 108+*.

¹¹³ Looking at technology governance more broadly, the Pathways for Prosperity Commission proposed “key principles for a cooperative digital world” in its report *Digital Diplomacy – Technology Governance for developing countries* (2020), including a bottom up approach starting with regional or like-minded cooperation.

called the Global Privacy Assembly (GPA) in 2019. The GPA is now crafting guidance on privacy policy, including in response to COVID-19, and its 2019-2021 strategy aims to enhance the organization's role and voice in wider digital policy, including by promoting an “evolution towards global policy, standards and models.”¹¹⁴

To achieve this goal, the GPA will need to develop closer ties with other international bodies (e.g., the G-20, multilateral development banks, the IMF, and many UN agencies), whose work increasingly involves issues related to the digital economy and the use of data by both the private and public sectors. Developing such ties would increase the GPA's stature and, more importantly, support greater collaboration between the economic development and data protection and privacy communities of practice.

There is a need not only for greater institutionalization at the global level, but also pathways for LMICs to have a greater voice in discussions on global standards. One way to ensure this is for the GPA to collaborate more closely with regional data privacy networks and other regional bodies with broader remits such as the African Union and ensure those bodies are represented at key meetings.

Unlike global bodies, which bring to together countries with very different characteristics, regional bodies draw their strength from convening countries that are more similar and therefore more likely to face comparable challenges. Regional coordination is particularly important for LMICs because on their own they lack the economic heft needed to influence global debates on data governance and the behavior of large tech firms. Regional bodies can also play an important role in pooling expertise and supporting peer learning efforts.

Although a number of regional data protection and privacy networks exist, organizations and initiatives dedicated to supporting regional learning and advancing policy related to broader data governance issues in LMICs are just beginning to take shape.¹¹⁵ Most of these initiatives focus on Africa, including the Africa Digital Rights' Hub, which promotes research and advocacy on digital rights; the Africa Data Leadership Initiative, “a peer network designed for and by African policymakers, consumer rights advocates, and private sector stakeholders to ensure the data economy drives equitable growth and social progress across the continent”; the Centre for Intellectual Property and Information Technology Law based at Strathmore University in Nairobi, Kenya, which conducts research and training on digital policy issues; and ID4Africa, which has convened DPAs and digital identity

¹¹⁴ Global Privacy Assembly. *Strategic Plan 2019-2021*. October 2019.

¹¹⁵ Data privacy networks that include LMIC members include regional organizations like the African Data Protection Network and the Asia Pacific Privacy Authorities (APPA) Forum, and linguistic and cultural networks like the Ibero-American Network of Data Protection (RIPD), which includes Spain, Portugal, Brazil, and the Spanish-speaking countries in the Americas, and the Association francophone des autorites de protection des donnees personnelles (AFAPDP), which is a group of francophone DPAs. The Common Thread Network is a network of DPAs in Commonwealth countries.

authorities in a series of public events aimed at bridging gaps between the two communities.¹¹⁶

In South Asia, most digital policy research has focused on India, including work by the Data Governance Network at the IDFC Institute.¹¹⁷ One organization with a more regional policy is LIRNEasia, which describes its mission as “catalyzing policy change through research to improve people’s lives in the emerging Asia Pacific by facilitating their use of hard and soft infrastructures through the use of knowledge, information and technology.”¹¹⁸ In addition, the Association of Southeast Asian Nations (ASEAN) has created a Data Protection and Privacy Forum and a framework on digital data governance to “strengthen the governance of digital data in ASEAN with a view to promoting the growth of trade and flow of data within and among ASEAN Member States in the digital economy.”¹¹⁹

In Latin America, regional initiatives on data governance are less developed, despite a long history of civil society engagement on digital rights issues.¹²⁰ Centro Latam Digital (The Center for Digital Policy in Latin America), a think-tank focused on digital policy issues in Latin America, including data privacy and cybersecurity, was established in 2018.¹²¹ In addition, the Inter-American Development Bank (IDB) is increasing its focus on the topic, including through its *Social Digital* program, which focuses on how digital tools can support better delivery of social services, and its work through its Modernization of the State program, which supports digital transformation of the public sector.¹²²

Theme 7: Developing the skills needed to govern data

In many countries, there is a large gap between the demand and supply of individuals with the knowledge and skills required to govern the use of data. To date, most of the development community’s work to build data capacity has focused on building basic digital literacy, programming, and statistical skills. However, there is a growing need for expertise on the legal and technical aspects of data use.¹²³

Government agencies that want to use data from or share data with third parties must have the ability to negotiate complex contracts that prevent data from being re-used for unintended purposes and to monitor these contracts to hold other parties accountable.

¹¹⁶ For more information, see [Africa Digital Rights Hub](#), [Africa Data Leadership Initiative](#), [Centre for Intellectual Property and Information Technology Law](#), and [ID4Africa](#).

¹¹⁷ [Data Governance Network](#)

¹¹⁸ [LIRNEasia](#)

¹¹⁹ [ASEAN Data Protection and Privacy Forum](#). [ASEAN Framework on Digital Data Governance](#). December 2018.

¹²⁰ Rodriguez, Katitza and Renata Avila-Pinto. Electronic Frontier Foundation. [Privacy Rights Activism in Latin America](#). September 2012.

¹²¹ [Centro Latam Digital](#)

¹²² [IDB Social Digital](#). [IDB Modernization of the State](#).

¹²³ See PARIS21’s [Capacity Building 4.0](#) for an overview of the core competencies required by modern NSOs. Also see the UN Global Working Group on Big Data for Official Statistics’ [Competency Framework for Big Data Acquisition and Processing](#) (2020).

Having this ability is particularly important when dealing with large tech firms, who can bring greater resources and knowledge to bear in negotiations. If agencies lack confidence in their ability to negotiate contracts that are enforceable, equitable, and comply with existing regulation, they are more likely to turn down data sharing projects, even if those projects are ethically designed, legally compliant, and may produce valuable insights.

To a surprising degree, interviewees noted that lack of legal data expertise often extends to the third-party data providers and intermediaries that LMIC governments work with. Staff at several of these organizations said that they struggle to find legal experts who can advise them on how to translate domestic law (and often the GDPR) into the local context in which they operate. One interviewee complained that development organizations spend too much time trying to “crowdsource” expertise on legal data matters from within the development community and argued that it is more effective to bring in “real privacy experts,” preferably on a pro bono basis when possible.¹²⁴

Working on the legal aspects of data governance requires a unique combination of skills and expertise, including an understanding of data protection laws and practices; data systems; and privacy risks raised by data use and how to mitigate them.¹²⁵ Government officials that oversee data projects would also ideally have an ability to understand and manage the value of data as an asset and pose relevant questions that can be answered with data.^{126,127} For this reason, there is growing interest in the official statistics community in creating a new profession and community of practice around the idea of “data stewards” to support collaborative data efforts.¹²⁸

Because this skillset requires knowledge in several technical areas, it will take significant time and investment to develop. Most interviewees believed that governments should prioritize developing this expertise for the reasons described above. But several argued that LMICs should address more urgent digital capacity needs – including the need to develop basic data skills (e.g., numeracy and simple programming, data analysis, and data visualization skills) -- before seeking to build legal data expertise. Without this fundamental skill base, they argued the domestic digital economy would not thrive, resulting in limited demand for those with narrower data governance skills.¹²⁹

¹²⁴ Tracey Li. Data Scientist and Project Manager, Flowminder. Interview. July 7, 2020.

¹²⁵ These competencies align with the role of “data privacy officer” or “data protection officer” (as referred to by the GDPR), which is growing in importance and demand. According to the [International Association of Privacy Professionals \(IAPP\)](#), which oversees the Certified Information Privacy Professionals credential, there are now more than 50,000 privacy professionals in the world (up from only 14,000 in 2014), see [50K members: A landmark for the IAPP and global privacy](#).

¹²⁶ Stefaan Verhulst. co-Founder, The GovLab. Interview. July 20, 2020.

¹²⁷ For more on soft skills needed to effectively manage data for public good, see [NYU and GovLab’s Data Stewardship project](#).

¹²⁸ GovLab. [Wanted: Data Stewards. \(Re-\)Defining the Roles and Responsibilities of Data Stewards for an Age of Data Collaboration](#). March 2020. See also: UN World Data Forum Webinar. [Data stewardship: A solution for official statistics' predicament?](#) March 2020.

¹²⁹ Donatien Beguy. Population Scientist and Data Expert, UN-Habitat. Interview. July 8, 2020.

Regardless of the approach taken, there was broad agreement that most LMICs would need to continue relying on donors and data intermediaries for legal data expertise for the foreseeable future. There was also agreement that donors can help build legal data expertise among their partners by making capacity-building a more explicit priority of the data partnerships they support. This would involve setting clear goals about the knowledge that would be shared through a project and investing in training modalities to provide deeper expertise. It would also require donors to commit to sharing project data back with their government partners whenever it is legally allowable.

Given the depth and specificity of the technical knowledge required, capacity-building efforts will need to be long-term engagements. Several interviewees suggested having governments and donors collaborate with major national academic institutions, government training institutions, or regional coordinating bodies to develop self-sustaining centers of excellence, where training programs can be institutionalized and replicated, and where a cadre of experts can be developed. The shared regional Cybersecurity Resource Centers that CGAP is pursuing in several regions offers a possible model for this type of approach.¹³⁰

Theme 8: The impact of COVID-19

The COVID-19 pandemic and the digital policy response to it has changed how society thinks about the use of data and digital tools by accelerating the global trend of digitalization, highlighting fissures and deficiencies in public data systems that preexisted the crisis, and drawing attention to how greater reliance on digital tools can threaten privacy.

The opportunities and risks of accelerating digitalization

The importance of physical distancing during the pandemic has accelerated the shift towards a digital-first approach by governments. As one interviewee noted, whereas before the crisis having the ability to provide digital services was a “want” for governments, today it is a “need.”¹³¹

Recent research by Gelb and Mukherjee highlights how governments have used digital systems — including digital ID, mobile communications, and digital payments, alongside data integration across social registers and other databases — to expand the size and reach of the social safety net, while providing services at arms-length. They find that countries that had foundational digital platforms for digital ID and payments in place before the crisis began, were better able to rapidly deploy social assistance than countries without those capabilities.

¹³⁰ For additional information see CGAP’s [Regional Centers Can Help Low-Income Countries Build Cyber Resilience](#) (2020).

¹³¹ Arturo Munte Kunigami. IDB. Interview. July 29, 2020.

As governments rely more on digital technology to provide services, it becomes imperative to ensure that all citizens can access services online (usually on mobile devices).¹³² In addition, as governments seek to develop a more coherent and efficient social protection response by integrating **beneficiary databases**, they must grapple with the threats to personal privacy this creates.¹³³ These challenges are even more acute when they involve the use of centralized digital ID systems that link individual identities to multiple services, such as health care, financial services, and education. Several interviewees noted concerns about the data privacy and protection risks associated with using centralized databases and the growing interest in decentralized models.

NSOs struggle to meet the demand for more and better information

Throughout the pandemic, governments have sought information at a higher frequency and level of granularity than traditional statistical approaches can provide to monitor the spread of COVID-19, understand the economic impact of distancing requirements, and inform their policies. This has forced NSOs to engage with and rely on other agencies and private sector companies to a much greater degree than before the crisis.

Some NSOs have combined official statistics with administrative data about the number of health facilities and health workers in different regions to assess local capacity in handling COVID-19 outbreaks.^{134,135} Others, like the Ghana Statistical Services, have filled data gaps by using telephone surveys to gather household data on the impact of pandemic (e.g., are pregnant women receiving antenatal care? are routine vaccinations being missed?) that go beyond what the Ministry of Health is collecting.

More often, however, interviewees stressed that the pandemic has exposed the challenges of sharing data without preexisting data sharing agreements, noting that the NSOs they worked with were often unable to access administrative records from other agencies due to data privacy concerns. While some countries have used executive orders to enable data sharing across government agencies for the purpose of responding to COVID-19 as a way to move forward, in others, NSOs have been sidelined from discussions at the highest levels of government about using data to combat the pandemic.¹³⁶

¹³² See the work of [Alliance for Affordable Internet](#) and [World Wide Web Foundation](#) in making the internet increasingly accessible and affordable for everyone.

¹³³ Gelb, Alan and Anit Mukherjee. [Digital Technology to Scale Up COVID-19 Social Assistance: What Have We Learned?](#) September 2020.

¹³⁴ UN DESA. [Use of administrative data sources under COVID-19](#). April 2020.

¹³⁵ Raftree, Linda. [Use of Administrative Data for the COVID-19 Response](#). June 2020.

¹³⁶ For example, in Colombia, a presidential decree allowed the statistical office access administrative records and census records to combat COVID-19. See Multidimensional Poverty Peer Network. [Using the MPI as a tool for crafting government responses to the Covid-19 pandemic](#) (2020).

New digital tools and tensions with privacy

Although interest in public-private data partnerships had been increasing before COVID-19, the degree to which governments have sought to use data collected by the private sector to combat the pandemic marks an important shift.

Early in the crisis, companies like Google, Facebook, Apple, mobile network operators, and others responded to the demand for high-frequency information to track human mobility patterns and the spread of disease symptoms by sharing data or insights produced through use of their digital devices and applications.¹³⁷ At the same time, governments increasingly turned to specialized companies who drew on data from various sources to analyze, monitor, and visualize mobility patterns, the spread of disease, and the health system response.¹³⁸

These collaborative efforts have created value for governments unable to produce the same information on their own. Several interviewees, however, expressed concern over instances in which public officials have used the urgency of the crisis to sidestep existing rules and best practices, including the need to conduct due diligence before sharing data with outside actors.

Interviewees held differing views on how the pandemic would shape public attitudes about how much governments should know about their citizens. But most believed that the crisis made the issue more immediate and real to people, in part due to early debates around the use of contact-tracing apps, which made them more aware of the degree to which their data could be used to track their movements and behavior. One interviewee noted that the pandemic had brought data privacy concerns “from the fringes to the mainstream.”¹³⁹

While most interviewees believed that heightened public awareness of these issues would make governments more accountable and force them to take additional steps to create and maintain public trust in digital tools and public data use, this optimism was tempered by two realities: First, governments who have lower levels of concern about civil liberties will invariably be drawn to use digital tools for surveillance. Second, the pandemic’s economic impact has reduced the fiscal resources governments can direct towards supporting better data governance.

¹³⁷ For examples of tech-based initiatives that companies have undertaken during the pandemic see: [Using mobile big data to help inform the fight against COVID-19 in the Democratic Republic of Congo](#) and [Addressing COVID-19 through Public-Private Data Partnerships -Where Do We Put New Testing Facilities?](#) and [Apple and Google’s COVID-19 tracking system will make its full US debut in new Virginia app](#).

¹³⁸ This includes companies like [Cuebiq](#) and [Dalberg Data Insights](#) which use telecom data to understand human mobility trends, and others like [Bluesquare](#) and [Zenisys](#) which help governments analyze, monitor, and visualize the spread of disease and health system response. See also [COVID-19 outbreak response, a dataset to assess mobility changes in Italy following national lockdown](#) (2020) and [Mobility Flows Analysis](#) (2020).

¹³⁹ Marelize Gorgens. Senior Monitoring and Evaluation Specialist, World Bank Group. Interview. July 23, 2020.

Conclusion: Areas for future research

Although the eight themes discussed above cover a broad set of issues, each of them speaks to how governments can use data effectively and responsibly. Achieving this goal requires not only a new set of skills, roles, institutions, and resources, but also greater coordination at the global, regional, and national levels between different communities of practice and an openness by those communities to share lessons and learn from one another.

Given the breadth of the issues involved, deciding where to prioritize reforms and target resources at each of these levels will be challenging. We believe that research in the following areas, which flow directly from our interviews, will help policymakers prioritize their efforts and better understand the policy options available to them.

Learning what drove successful data partnerships in response to COVID-19

The COVID-19 pandemic and the policy response to the crisis represent a shock to national statistical systems that researchers can use to identify how effective past capacity-building and institutional development efforts have been in preparing national statistical systems for using secondary data. A research program that examines how different countries fared in using data to respond to the crisis and the reasons for that variation, including whether different capacity-building and institutional development programs were helpful in preparing for this challenge, would be valuable, particularly as the effectiveness of such training programs is often difficult to measure.¹⁴⁰

Bringing greater transparency and evaluation to public-private data partnerships

Given the increasing importance of public-private data partnerships, it is important to ensure that these efforts support inclusive development, which requires a better understanding of how to manage the differing incentives of the private and public sectors within such collaborations. To date, much of the effort spent on evaluating data partnerships has focused on cataloging successful use cases. While this can help highlight the value of merging data from public and private sources, a more rigorous approach to monitoring and evaluating (M&E) data collaborative projects is needed. And while a handful of organizations have developed M&E for data-intensive projects that assess the risks of using certain types of data and ways to mitigate that risk, it is clear from our interviews that more work is needed to promote broader take-up of these practices, including by national governments.

¹⁴⁰ Cite Paris 21 and OECD.

Examining new models of data protection and privacy through the lens of economic development

Although data protection and privacy laws are just one element of countries' broader data governance frameworks, they tend to receive the most attention because they touch on politically sensitive issues. Today, an increasing number of countries are modifying their approach to data protection and privacy to meet their domestic needs and priorities, including supporting economic growth and innovation. This includes both legal reforms and efforts to design codes of conduct that fit local contexts. Although the effect of these changes may not be well known for years, research aimed at understanding how these reforms work in practice would help policymakers better understand the available policy options available.

Exploring models for greater cooperation between the data privacy and development communities

Researchers can support greater collaboration between the development and data privacy communities at the national, regional, and global levels by examining approaches used in other fields to bring experts with different professional backgrounds together to share knowledge and develop mutually-agreeable policy norms and guidance. A work agenda on this topic could also seek to create engagement opportunities between the two groups and facilitate dialogue by surfacing areas of misunderstanding and opportunities for coordinated action.

Over the next year, CGD's *Governing Data for Development* working group will focus its efforts in three related areas. First, we will examine the approaches governments can take to increase transparency, accountability, and trust in public use of potentially sensitive data and how different approaches might affect their ability to meet broader socioeconomic goals. Second, we will review emerging best practices among LMIC governments that are tailoring data protection and privacy laws and regulations to their own needs, priorities, and capacities. Third, we will seek to bring together experts from the development and data privacy communities of practice to work towards a shared understanding of the reforms, institutions, resources, and capacity-building efforts needed to support good data governance by national governments. As part of this effort, we will also promote the development of institutional arrangements that provide a pathway for policymakers, experts, and civil society advocates from LMICs to contribute to global debates on standards, principles, and guidance related to data protection and privacy.

Appendix 1: Complete list of interviews

Adedeji Adeniran, Director of Education and Governance Research/Senior Research Fellow, Centre for the Studies of African Economies

Joseph Atick, Executive Director, ID4Africa

Shaida Badiee, Founder and Managing Director, Open Data Watch

Krista Baptista, Senior Director, Center for Digital Acceleration, DAI Global

Komal Bazaz-Smith, Digital Connectivity & Cybersecurity Partnership Project Director, Digital Frontiers, DAI Global

Donatien Beguy, Population Scientist and Data Expert, UN-Habitat

Mojca Cargo, Senior Manager, Public Sector Engagement, GSMA

Stephen Chacha, Co-Founder and Executive Director, Tanzania Data Lab

Somsak Chunharas, President, National Health Foundation in Thailand

Vyjayanti Desai, Program Manager, Identification for Development

Jonathan Dolan, Research Lead, Future State

Teki Akuetteh Falconer, Founder & Executive Director, Africa Digital Rights' Hub

Joaquín Jaime González Casanova Fernández, Director General, National Institute for Transparency, Access to Information and Personal Data Protection

Amanda Glassman, Executive Vice President, Senior Fellow, and CEO of CGD Europe, Center for Global Development

Marelize Gorgens, Senior Monitoring and Evaluation Specialist, World Bank Group

Priya Vora, CEO, Future State

Johannes Jutting, Executive Head, PARIS21

Al Kags, Founder, Open Institute

Deepa Karthykeyan, co-Founder and Director, Athena Infonomics

Paige Kirby, Senior Policy Advisor, Development Gateway

Arturo Munte Kunigami, Modernization of the State Senior Specialist, Inter-American Development Bank

Tracey Li, Data Scientist and Project Manager, Flowminder

Grégoire Lurton, Data Science Lead, Bluesquare

Drudeisha Madhub, Data Protection Commissioner, Data Protection Office, Mauritius

Sean McDonald, co-Founder, Digital Public

Kathleen McGowan, co-Founder, Future State

David Medine, Consultant, Consultative Group to Assist the Poor

Jose Antonio Mejia, Modernization of the State Lead Specialist, Inter-American Development Bank

Claire Melamed, CEO, Global Partnership for Sustainable Development Data

Santosh Misra, CEO, Tamil Nadu e-Governance Agency and Commissioner of e-Governance, Government of Tamil Nadu, India

Jade Nester, Director, Consumer Policy, GSMA

Galia Nurko, Digital Specialist, Center for Digital Acceleration, DAI Global

Victor Ohuruogu, Senior Africa Regional Manager, Global Partnership for Sustainable Development Data

Tom Orrell, Managing Director, DataReady

Olasupo Oyedepo, co-founder and Director, African Alliance of Digital Health Networks

Josh Powell, CEO, Development Gateway

Agnieszka Rawa, Managing Director, Millennium Challenge Corporation- President's Emergency Plan for AIDS Relief Partnership (MCC-PEPFAR) Partnership

Isaac Rutenberg, Director, Center for Intellectual Property and Information Technology Law

Julia Schmidt, Policy Analyst, Statistics and Data Directorate, PARIS21/OECD

Omar Seidu, Head, Demographic Statistics and Coordinator of Data for SDGs, Ghana Statistical Services

Florencia Serale, Data Consultant and Co-chair, Open Data Charter's Implementation Working Group

Rachel Sibande, Program Director, Data for Development, Digital Impact Alliance

Jenna Slotin, Senior Director of Policy, Global Partnership for Sustainable Development Data

Ramiz Uddin, Head of Results Management and Data, a2i Programme, Bangladesh

Stefaan Verhulst, co-Founder, The GovLab

Jeanine Vos, Head of SDG Accelerator, GSMA

Steve Wood, Deputy Commissioner (Executive Director, Regulatory Strategy), Information Commissioner's Office (ICO), UK and Chair of the OECD Working Party on Data Governance & Privacy

Appendix 2: Selected interview quotes

Theme 1: The imperative of breaking down siloes

“Historically, data has been a fragmented space that needed to be consolidated. Groups focusing on data issues used to be able to operate in their individual siloes, but now, in light of the COVID-19 pandemic, their work is often overlapping, for example, data protection and open data. NSOs have been largely absent from these discussions, but they have a lot of legitimacy and can be instrumental in carrying out some of these discussions to consolidate these varying groups.”

- *Arturo Muenta Kunigami, Inter-American Development Bank*

“The work the GPA has done so far has been to try to develop a better mechanism for civil society to interact with it. We’ve now set up a standing stakeholder panel for engagement and the Executive Committee is going to decide on who will sit on the panel in due course. We will have representatives from civil society, from businesses, from academia, and I think that will give more of a voice for the GPA to hear what those groups think are important.”

- *Steve Wood, Information Commissioner's Office*

“This notion that statistical agencies are the only custodians of all data is dead and outdated. Yes, they have census infrastructure, which is important, but that is only one part of the story. Every ministry today plays a role in collecting large amounts of information.”

- *Deepa Karthykeyan, Athena Infonomics*

“Over 300 data collaborative initiatives have emerged in the context of COVID. It’s great to have 300 plus initiatives, but it would be even better if there was coordination among them to minimize duplication. At the moment, there is no sole coordinator. There is lots of energy to do something, but there is also a lot of fragmentation.”

- *Stefaan Verbulst, The GovLab*

“I’m a big fan of community-based identification of questions because if answered they could deal with problems communities have. I also care about identifying metrics that communities care about that can then be leveraged by data. How differently people will act when they have access to data is never contemplated. It’s always about analyzing because they have access to data, not necessarily because they understand the problem. The participatory model of problem definition should become the standard.”

- *Stefaan Verbulst, The GovLab*

“A privacy ombudsman could look at different decision-making tools, and/or they could advise consumers about data uses. They would not be people who just look at algorithms, but they also

look at the practices of companies, the internet of things device practices, and advise consumers when to stay away from specific products with problematic data practices. The privacy representative does not have to be a single person. It can also be a private, government or NGO, entity.”

- *David Medine, Consultant to CGAP*

“Interoperability remains a huge challenge across ministries and levels of government. Everyone has their own database and each department has its own particular way of creating a dataset. Realizing this challenge, we launched a program called the State Family Database to streamline and harmonize the interoperability issues and to resolve the data disparity that exists across the departments. Essentially, we are trying to harmonize and synchronize all the federated databases.”

- *Santosh Misra, Tamil Nadu e-Governance Agency*

“We realize that our ability as a country to build our data systems does not only depend on data produced by the national statistics office. It also depends on line ministries and data produced by civil society and other players in the system. We conducted an assessment last year to check the quality of data produced across these areas and we realized that there are quality challenges, especially for the data coming from civil society. So we designed a project to work with civil society, academia, the private sector, and the line ministries to co-create a data quality assurance framework. We expect by the end of this year, to have a framework for Ghana that guides all those in the data ecosystem on how to produce quality data.”

- *Omar Seidu, Ghana Statistical Service*

“On the development side, the conversation around privacy has not been fulsome, but on the privacy side there has been almost no conversation around development and that is an error. It is important for these stakeholders to come together.”

- *Joaquín Jaime González Casanova Fernández,
National Institute for Transparency, Access to Information and Personal Data Protection*

Theme 2: Promoting data governance as an enabler rather than a hindrance

“To bridge the gap between data protection laws on the books and their implementation on the ground, we need to make it clear that on the one hand yes, these regulations or policies are in place to prevent harm, but on the other hand they are meant to prevent harm within the broader context of wanting to facilitate data, sharing data access, and data use to proactively address issues.”

- *Joshua Powell, Development Gateway*

“The operators are held to very different standards than a range of other actors across the mobile ecosystem, particularly in countries where there is no general data protection law. We have been pushing for the development of a smart general data protection regulation that is horizontal, tech neutral, and has an independent regulatory body.”

- *Jade Nester, GSMA*

“We enforce the responsible use of data among those who have access to the datasets by ensuring that whatever data goes into our data portal has the right approval of the data owners. We do not store or publish personalized data sets. All our data is highly disaggregated and anonymized. We also work with the data producer for them to give consent. If datasets can be used by the public then they can be downloaded, if not, people can only use it in the portal. Unfortunately, there are limitations due to the lack of data protection in Tanzania, especially as it relates to using private sector data. Having guardrails and clear guidance on data protection would be helpful in moving forward.”

- *Stephen Chacha, Tanzania Data Lab*

Theme 3: Equitably distributing the value of data insights by “closing the loop”

“There is a lot of work being done with data that has little value for the local environment. When people want to analyze data, it is often not done in country because the resources and skills aren’t there. The agenda is often not in the interest of the country and external actors harness the true value of what is produced. I would be hard-pressed to identify analysis of routine health data done out of country that had in-country benefits, in terms of policy change or usable insights. Bluesquare is currently working to establish a stronger connection between health information systems and data analysts through data sharing agreements in which results will be fed back through the platforms used, so that they can be integrated in the tools used by decision makers in the country.”

- *Grégoire Lurton, Bluesquare*

“There is a significant challenge with donors going into countries to implement programs and conducting their own ‘extractive data’ exercises without engaging with national statistical systems. The risk is that countries won’t develop the ability to make use of data produced in their own borders, and this will push development towards a de facto paternalistic relationship -- and weaken ‘country ownership’ -- because only donors will have the capacity to make use of the data.”

- *Agnieszka Rawa, Millennium Challenge Corporation*

“For donors, it’s increasingly important that their ministerial counterparts, their implementation partners, and the beneficiaries of their investments, have the tools to engage with data, and come to the decision-making table with data. Data is power but only if you know how to use it.”

- *Agnieszka Rawa, Millennium Challenge Corporation*

“When data is produced, during an emergency (e.g pandemic), through external partners’ support, such datasets are often hosted outside of the country. This creates certain hurdles for people in that country to access the datasets. Capacity to effectively negotiate data partnerships and access is a major challenge.”

- *Anonymous*

“Minimal effort is often put into effectively disseminating data gathered because a lot of countries often don't have adequate capacity to analyze and visualize large datasets, in a very timely manner. So data is collected and it can take several months to derive value from it for the average user.”

- *Anonymous*

“Sometimes NSOs see themselves as custodians of data in a country but there is not much effort to open themselves up to scrutiny or provide access. It's like they are more interested in generating data rather than seeing whether the data they generate is useful.”

- *Donatien Beguy, UN Habitat*

“Data value is not equitably distributed back down the chain. This is not because of any malicious intent; rather, it’s often not important to project developers or planners. I worked on a project where we collected HIV/AIDS supply chain data across the country using mobile phones. Using this data, we printed out A3 size color printouts of charts and graphs displaying health data, for example, the total number of women who were accessing HIV treatment at a specific facility. These printouts were displayed inside health facilities. These charts were discussed with patients and staff in the facilities. Because of this feedback loop, we observed that the quality and timeliness of the data improved because the data was used by both the health facility staff and the patients. Unfortunately, the deliberate planning and inclusion of feedback loops is still not commonplace.”

- *Olasupo Oyedepo, African Alliance of Digital Health Networks*

“The perceived value of data is mostly about automation and scale, and participation is something that fundamentally frustrates that. People talk about doing things for good or for people or for the public, but the design nomenclature has moved significantly beyond that and most of the best practices design with. So, those kinds of systems inherently frustrate scale without thinking about devolution architectures.”

- *Sean McDonald, Digital Public*

“In Thailand, major hospitals often field requests from companies developing AI to access their big data. But I worry that there will not be equitable sharing of the value and insights created from these partnerships. Moreover, Thailand requires clinical trials to be registered. But, many of the clinical trials are conducted by multilaterals. So, those trials are registered and stored in

other countries, and the dataset from Thailand is available in other countries, but is not necessarily always available to the people of Thailand.”

- *Somsak Chumbaras, National Health Foundation (Thailand)*

“How data is used and how people are compensated matters a lot for accuracy. People collect data more accurately when it will be used.”

- *Amanda Glassman, Center for Global Development*

“We have to be wary about who the audiences are for these platforms. The UN, for instance, has a whole host of open data platforms, but the reality is that only a small proportion of the world’s population will really be able to utilize that data. This brings to light the issue of data equity and open access to data. Open data still benefits those who are best positioned to leverage that data, monetize that open data to take advantage of standards, and take advantage of platforms. There are inherent inequities in the current systems and models. Open data is great, but we have to recognize not everyone has access to this open data. So only a limited number of people can utilize the data.”

- *Tom Orrell, DataReady*

“There are also capacity and intent issues. There is limited/no intent to empower data producers to be data consumers. To generate good data those demanding the data need to understand the correlation between data quality and who is generating them and what their incentives are and be equipped to frame policies and tools that create a virtuous cycle on data collection and use.”

- *Deepa Karthykeyan, Athena Infonomics*

Theme 4: The benefits, hazards, and hurdles of data collaboration

“There is a lot of the attention around engaging with the private sector and using private sector data. My concern here is the failure to understand that the private sector has very distinct incentives from public sector. Not thinking critically about those incentives and how those incentives may not align with good practice and data privacy and ethics could be a big blind spot.”

- *Paige Kirby, Development Gateway*

“The Kenyan government engages foreign companies and those foreign companies sometimes have the upper hand in dealing with data. We have seen several instances where the government has not benefited as much as it should have from data-intensive collaborations.”

- *Isaac Rutenberg, Center for Intellectual Property and Information Technology Law*

“There is not enough guidance on how to structure data-sharing agreements. Bluesquare is relying on a blend of guidelines from GDPR and clinical research standards. For many intermediaries, templates for formal data sharing agreements would be most useful. In many

situations, Bluesquare is a data broker between the national system and other organizations that want to use the data. So there is an urgency for us to frame our data sharing work through more formal agreements.”

- *Grégoire Lurton, Bluesquare*

“There are a range of foundational issues missing to accelerate data collaboration in a systematic way. Most existing collaborations are one-offs that are also unsustainable. There are also questions around how to establish and maintain collaborations that are responsible.”

- *Stefaan Verbulst, The GovLab*

“Integrating newer forms of data has proven difficult because the access question has not been solved. There are still issues around legality, competition, and compliance that even the most advanced NSOs are struggling to overcome.”

- *Johannes Jütting, PARIS21*

“If you are not talking about the role of governments as data owners and generators and folks who govern data, then you are not talking about the problem at all. While the private sector and players like Facebook and Google generate large amounts of data and are important and wield power, the government must drive the conversation because they are designed to deliver welfare.”

- *Deepa Karthykeyan, Athena Infonomics*

“We were approached by a mobile network operator saying they had data sets from their mobile networks they felt could contribute to managing COVID. Unfortunately, no one knew how to go about this collaboration as there were several limitations.”

- *Stephen Chacha, Tanzania Data Lab*

“During the COVID pandemic, we provided data to the academic sector to aid in predictions. But, we also needed data from the telcos. This was very challenging because there weren’t any [data sharing] safeguards in place. So, when working with the telcos to help in the fight against COVID, we requested that they use their own internal standards on which to provide information.”

- *Ramiz Uddin, Access to Information (a2i) of Bangladesh*

“COVID-19 brought to the forefront this issue of NSOs being caught between two different forces. First, they are being asked to make data available that they cannot make available. Second, NSOs are trying to access administrative records from other entities to make statistical use of them, but they are unable to use them because other agencies also claim the protection of privacy of that data. On one hand, you have NSOs trying to figure out how to

continue working, given that they can't be on the ground due to COVID, and on the other hand trying to figure out how to use data from other sources to continue being relevant.”

- *Jose Antonio Mejia, Inter-American Development Bank*

“MNOs are supporting governments in the COVID crisis for the specific purpose of the COVID-19 response, providing dashboards, insights and reports that are specifically relevant and useful for decision making in the country. This is why operators and the GSMA are very hesitant about granting generic access to datasets, because then you lose that clear purpose, access may no longer be time-bound, and it's harder to ensure accountability of that data. So, it has to be handled on a case by case basis to create a tailored solution that safeguards privacy end-to-end.”

- *Jeanine Vos, GSMA*

“Initially, people thought the pandemic would bring about change in data sharing, but by July we realized that it would be a lot more complicated. If the demand for data is not consistent, then we won't move past the data-sharing barriers we are observing. There is a disconnect. You have people saying they needed help and guidelines, and then you have organizations producing guidelines that aren't widely used.”

- *Jenna Slotin, Global Partnership for Sustainable Development Data*

“As a result of data quality not being the same across different agencies, we've discovered that only a reduced level of interoperability can be achieved because the data quality is making it difficult to harmonize across systems. Data quality is key to interoperability. I worry more about the interoperability of data than the interoperability of systems.”

- *Joseph Atick, ID4Africa*

Theme 5: Establishing effective data protection frameworks

“It is important to try to write data protection laws in a way so that they are self-enforcing as much as possible and use regulatory technology to automate dispute or complaint processes. Try to build a system that puts the least burden on a data protection authority so as to overcome regulatory capacity issues.”

- *David Medine, Consultant to CGAP*

“In some countries, comprehensive laws modeled on GDPR get put on the books and then virtually nothing happens. So, in these cases it may be better to start off with simple standards that companies and individuals can better understand and follow, and then build on these over time to more comprehensive laws.”

- *David Medine, Consultant to CGAP*

“The implementation strategy should look at leveraging industries, specific communities, to work with them in crafting guidance and frameworks that work well. For example, if a regulator

wants to craft guidelines in the health sector, they don't necessarily need to have expertise in the health field, rather they can work with people in the health space to create the guidelines. This collaborative approach will yield guidelines that work well for everyone."

- *Teki Akuetteh Falconer, Digital Rights Hub*

"The most important aspect in data protection is enforcement. Our data protection commission has the ability to prosecute people for breaches of the data protection act. This enables more people to consult the office prior to acting because of the fear that an organization or a ministry might be prosecuted for not respecting the data protection act in Mauritius."

- *Drudeisha Madhub, Data Protection Office, Mauritius*

"Our principals are good, but sometimes they are not able to adapt. This has proven to be the case during this pandemic. We must be flexible and provide ourselves with a margin of appreciation where we can decide to adapt and change principles to reflect what is happening on the ground. We need to be realistic."

- *Drudeisha Madhub, Data Protection Office, Mauritius*

"In the official statistics community, there is awareness of the importance of standards, privacy and risk assessments. However, in broader government services and in the development field, I'm observing that there is more hope and focus for blockchain and AI, the shiny stuff, and less focus and priority on the foundational technology."

- *Johannes Jütting, PARIS21*

"We have noticed that even in countries with a data protection act, there is a tendency for governments to pull back from sharing data at all rather than potentially violating that policy."

- *Paige Kirby, Development Gateway*

"Many Western standards are not always applicable in the global south. Yet, it remains attractive to adopt western standards because they are often considered the best practice. African countries are sometimes asked to dismantle their legacy deployments because it does not fit into a specific western standard, despite the fact that what they had been doing was working for them."

- *Olasupo Oyedepo, African Alliance of Digital Health Networks*

"Getting a legal framework in place is a priority. The challenge is that no one really specializes in this area in the development community or the official statistics community. And if this is not your specialty, there is a lot to learn."

- *Tracey Li, Flowminder*

“The idea that there should be stronger laws about data privacy and data usage is a given. But should they be as extensive and as comprehensive as GDPR? From the challenges that have been experienced by organizations following the introduction of GDPR, as well as seeing the barriers that GDPR raises, and seeing how it doesn't always have the effect it was intended to have, we see that GDPR is a good idea on paper, but implementing it remains a challenge.”

- Tracey Li, *Flowminder*

“We can't just take the European standards and apply them at large. Even the architects of the GDPR recognize that they need to make some adjustments to the law because they now see that there are aspects they were too strict on and aspects where they were not strict enough.”

- Marelize Gorgens, *World Bank*

“In creating the minimum standards, the bank is trying to find that line between being rigorous and being pragmatic. The bank recognizes that proportionality of risk is something they have to be mindful of in two ways: one, have to do that which is the fairest to most people, and two, have to ensure that vulnerable populations have special protections in place.”

- Marelize Gorgens, *World Bank*

“A maturity model is the best way of approaching this. It should be granular enough so everyone sees themselves in it. It would be useful to have groups that conduct assessments of where countries are in terms of maturity.”

- Shaida Badiee, *Open Data Watch*

“In the process of opening data, we address privacy issues. Our job is not difficult at the macro-data level because there's no personal information, but there are still privacy issues. We are now focusing on open data for surveys, census, and administrative data which goes into micro-data. Unfortunately, there are currently no global guidelines or procedures for access to micro-data. We realized ODW could not take action alone, so we reached out to the UN which has now set up an interagency expert group on microdata with a subgroup looking into how we can establish guidelines for microdata.”

- Shaida Badiee, *Open Data Watch*

“One of the challenges with data privacy and data standards is that there is plenty of focus work that needs to be done to create a framework at the national level. It often extends beyond the donor sector's scope, which is why it's important to have other sectors involved. There are also funding challenges. Data standards are often just viewed as a smaller activity that is part of a larger program, rather than being seen as a major problem and topic in its own right.”

- Krista Baptista, *DAI*

“The debate has focused too much on GDPR. This has forced us to focus on a very complicated set of rules that are geared toward a common market and are not necessarily geared

toward the protection of privacy and personal data as a human right. We need to figure out what it is that we are trying to protect and how we do it.”

- *Joaquín Jaime González Casanova Fernández,
National Institute for Transparency, Access to Information and Personal Data Protection*

“There's just so much attraction to the latest and greatest – such as AI - among donors and big development actors, and that's something that probably needs to be dialed back significantly if we want to effectively move forward in the responsible data use space.”

- *Josh Powell, Development Gateway*

“Regarding data sharing, there is a lot of “how to” guidance and a fair amount of technical guidance, but there is a gap in data governance guidance. There are many intermediaries whose business is built around technical guidance, but there are not many intermediaries on the governance side.”

- *Jenna Slotin, Global Partnership for Sustainable Development Data*

“If you ask the people in the official statistics community, they will tell you the NSOs have the mandate to do quality assurance and standards-setting across the sectors and ministries; but in practice, they are not well-funded to do this effectively. Coming from the health sector, I felt like a civil society check might be more important than the statistics bureau doing the quality assurance in a horizontal way. One of the ideas behind doing the data compact was precisely that it would set up the statistics bureau as the standard-setting quality assurance entity. The sectoral ministry or subnational governments would be charged with producing the data with certain periodicity and quality and the statistics department would be the checker on behalf of the ministry of finance or the presidency.”

- *Amanda Glassman, Center for Global Development*

Theme 6: The need for regional and global solutions

“There are no clear guidelines on which adequacy is given. This lack of clarity is where the challenge comes in. The problem with adequacy is that it gives a certain leverage within which to interact with Europe. For a continent like Africa, which is building its market base, it is very important, especially because we still trade with Europe. If African countries are interested in adequacy, it is important for them to push these things at the continental level where it is more likely to be successful, rather than it being left for individual countries such as Morocco or Mauritius, for example.”

- *Teki Akuetteh Falconer, Digital Rights Hub*

“The whole of government approach is what will determine whether something can succeed and move forward. This is where political commitment and somebody spearheading an effort across government can be the defining factor. This is a crucial element in any of these digital transformation efforts that we hope to see put in place.”

- *Vijayanti Desai, ID4D*

“The ICO has had an international strategy since 2017. Before this, we were mostly focused on the continent of Europe. We realized there was more the ICO needed to do in terms of regulatory cooperation between other data protection authorities. We recognized that data has no borders. Our international strategy links back to our regulatory role in the UK. The public in Britain wants to know that their data is safe no matter where it goes in the world. Promoting high standards of data protection globally benefits the ICO as a regulatory authority because it means we can work with other regulatory bodies to address the risks. No matter where you look globally, the same issues appear. The ICO currently chairs the Global Privacy Assembly. It used to be a regular annual meeting where resolutions were agreed to and best practices were shared, but we have transformed it into a year-round international organization because that is what is needed.”

- *Steve Wood, Information Commissioner's Office*

“We support some of the GDPR cross-border data flow elements, but we are a bit more open to innovative approaches. For example, we worked with ASEAN on their privacy framework, but we also developed a regulatory sandbox called Regulatory Pilot Space to try to enable cross border data flows and protect personal data in the region. This falls under the general ideals of the GDPR in that it's about accountability mechanisms, but it is not exactly like the GDPR.”

- *Jade Nester, GSMA*

“There is also an opportunity for organizations at the regional level or continental level to bring together sectoral players in this space. For example, a network of regulatory authorities that already exist in certain sectors to support peer learning. This enhances the credibility and value of work being done.”

- *Rachel Sibande, DLAL*

“We need to have an institutional approach to this rather than a problem and solution approach. We need to look at the regional level. We tend to look at this in terms of individual countries or the global level and make recommendations at those levels. But the reality is that the politics of this often play out at the regional level. So, I think if you're thinking about what sits between demand and supply, you need to think about institutions and you need to think about regional level institutions.”

- *Claire Melamed, Global Partnership for Sustainable Development Data*

“South-South Network is a great peer learning opportunity that is fostering cooperation amongst low income countries well-positioned to understand each other's challenges in public service delivery and share insights to solve them.”

- *Ramiz Uddin, Access to Information (a2i) of Bangladesh*

Theme 7: Developing the skills needed to govern data

“If you build capacity, it will not automatically mean you build leadership, trust, or accountability. However, you cannot build trust and accountability without doing capacity building alongside.”

- *Olasupo Oyedepo, African Alliance of Digital Health Networks*

“If you want to expand the mandates of governments to also think about data, if you want governments to start thinking about generating better quality data and also governing data where we are protecting rights, we need to start with investing in resources and people that are equipped to handle and to think about these issues. Governments need to invest in people of adequate seniority who can make a case for this consistently, not just a one-off thing that is something to check off as part of donor compliance. This is different than just hiring an external technical resource; rather, you are empowering someone within government to lead it.”

- *Deepa Karthykeyan, Athena Infonomics*

“In many national statistical systems, there is a lack of skills including nonconventional skills – such as management and negotiating the data - data sharing skills, legal skills and data ethics. Even if these skills exist in the organization, it remains very spread out and isolated within specific teams, rather than being institutionalized. When there is a weak foundational data system coupled with a weak legal system, we see problems. The UNSD Global Working Group on Big Data - to which PARIS21 is a participant - is developing a maturity matrix that is looking at the different capacities from legal to technical capacity, and also holistic and soft skills. Our goal is to develop a training guide that statistical offices can use to assess their capacity.

- *Julia Schmidt, PARIS21*

“Even if the conditions for building capacity are in place, there still needs to be a clear path for people working at NSOs. Sometimes you have people who are skilled, but do not see a career prospect with the NSO. Getting the skills and building the skills capacity is one thing but having a system that can absorb the skilled labor is another.”

- *Donatien Beguy, UN HABITAT*

“When you develop digital platforms, you need a digitally literate populations to leverage. For example, with EdTech, you have teachers that cannot even leverage the platforms. So, we need to focus on areas that will galvanize mass adoption. We need to include digital literacy into the curriculum from a very young age.”

- *Adedeji Adeniran, Center for Study of Economies of Africa*

“If communities have data and learn how to analyze and use the data, they can make the kind of arguments that need to be made for the government to act on their behalf.”

- *Al Kags, Open Institute*

“The goal is not to prescribe how individuals should decide or should engage on a digital platform or in their digital lives, but rather to enable people to be informed consumers who can determine if they’re comfortable with sharing certain information with a digital platform.”

- Galia Nurko, DAI

“One of the key priorities on our side is that at all points in our engagement with government, we stress the importance of data privacy and work to ensure the government understands the importance of data privacy before we even engage.”

- Mojca Cargo, GSMA

“Data science is the ability to take data and statistics knowledge, apply it to a sectoral problem, and then complementing it with some programming skills. This expertise is very hard to find in many of our MCC partner countries. What we find is people trained in data programming and statistics. But we need a continuum of data expertise that includes: simple numeracy, simple analytics [using excel sheets and visualizing data], sophisticated systems that are interoperable, then data science which can help with the more innovative solutions such as AI and machine learning.”

- Agnieszka Rawa, Millennium Challenge Corporation

“The problem with data is that the potential for misuse is very high. So, anyone dealing with data needs to have the capacity and the maturity to handle it. You need to have technical capacity otherwise a third-party will steal your nation’s data. You also need the capacity to understand that someone can harm you because of the data you hold. And, you need to have the capacity to understand how the data can be monetized.”

- Santosh Misra, Government of Tamil Nadu, India

“When it comes to the formulation of partnerships or when a design process is being undertaken there is always consideration for geographic, gender, racial, and ethnic balance — which is great. However, there is rarely consideration about whether data rights advocates and multilateral organizations are in the room. There needs to be a slightly broader interpretation of what it means to have data skills. I would argue that having an understanding of human rights is fundamentally a data skill. Having an understanding of governance processes is a data skill if you’re applying it to how data is governed.”

- Tom Orrell, DataReady

“Building capacity within governments takes time because we’re often going into countries where people have not done this before. You have to test their existing legal instruments to see if this is allowable. That’s a whole process. You have to develop data champions that have the political muscle to make this work. It takes a lot. And it requires working with a diverse range of partners. To align these actors requires strategy and in-country presence. We really appreciate

the technical implementing partners in the country. They play an important role in engaging with the government day-to-day.”

- Rachel Sibande, DIAL

Theme 8: The impact of COVID-19

“COVID has resulted in an increase in political will to get data protection and privacy right. The issue has gone from the fringes to the mainstream.”

- Marelize Gorgens, World Bank

“Before the rise of technology, Africans had experience in handling their corrupt governments. But technology has enhanced the power of corrupt governments who can take advantage of the personal data gathered during the COVID-19 health crisis and use it for surveillance or for purposes not related to the pandemic.”

- Al Kags, Open Institute

“Some governments took a very different approach to COVID, especially in relation to data. We have witnessed governments taking full control of the data being produced and publicized. The role of National Statistical Offices as custodians of data during COVID was almost nonexistent. COVID proved the level of fragmentation and lack of coordination in data ecosystems at country level especially when they are hit with crises.”

- Stephen Chacha, Tanzania Data Lab

“Data protection is very important for innovation. When people feel their privacy is not being protected, they will not generate data and they will remain offline. One of the challenges we are facing is people not giving the right information when they go for COVID testing – not even giving the right cell number. This indicates a distrust of how their data might be used.”

- Ramiz Uddin, Access to Information (a2i) of Bangladesh

“The presence of COVID has brought to the forefront the importance of digital - including having a digital response and knowing the potential risks and barriers of digital - and the importance of providing guidance for the operating units and bureaus across USAID on navigating this landscape.”

- Komal Bazaz-Smith, DAI

“Digital and privacy issues will have to be addressed more quickly than it otherwise would have been pre-COVID because organizations and governments realize that there are significant implications for how they imbue privacy and protection across all the different policies and legislation they develop.”

- Krista Baptista, DAI

“COVID-19 has shown us the relevance of administrative data. The inability of government agencies to share administrative data has been a limitation. Of course, we want to focus on new data sources, but the original big data are administrative records, and we need to take advantage of them. There is a need to improve their quality, but there is a bigger need to invest in using them for statistical purposes.”

- Jose Antonio Mejia, Inter-American Development Bank

“There has been plenty of discussion around infrastructure because COVID showed us that we need to go beyond transparency when opening data. The data we open has to be of good quality which means governments need to have good data infrastructure.”

- Florencia Serale, Inter-American Development Bank

“Progress was made following the Roundtable of African Data Protection Authorities. For example, people were reaching out to each other to realize the items discussed. Still COVID created a setback with agencies setting privacy aside. People are using the health crisis as a justification for shortcuts.”

- Joseph Atick, ID4Africa