CGD BRIEF
AUGUST 2021

Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development

Roundtable Summary

Compiled by Michael Pisa and Ugonma Nwankwo

INTRODUCTION

The rapid increase in the number of countries that have enacted data privacy regimes over the last decade promises greater protection of personal data for a growing share of the world's inhabitants. But meaningful questions remain about the effectiveness of these regimes in practice, alongside concerns that poor implementation of data privacy laws could weaken the protection provided and stifle innovation that supports economic growth and development. These risks are greatest in low- and middle-income countries (LMICs) since de facto global standards for data protection were primarily designed by rich countries to meet their own needs.

Over the summer and fall of 2021, the Center for Global Development is hosting a series of private roundtable discussions to explore the relationship between data governance and economic development. The first roundtable was held May 20, 2021 and explored whether existing data protection and privacy frameworks fit the needs and priorities of resource-constrained countries and, if not, what the consequences are, and how to address them.

This document summarizes key takeaways from the meeting, including the remarks of three keynote speakers and themes raised in a discussion among 30 experts, who are listed in the Appendix. The roundtable was moderated by Pam Dixon, founder and executive director of the World Privacy Forum, and co-chair of the working group for CGD's Governing Data for Development project. Because this report summarizes the discussion faithfully, additional context is provided only when it is necessary to help readers understand the points raised.

KEY TAKEAWAYS

Through the course of the roundtable, a handful of key themes emerged from the dialogue. These themes are summarized below.

Countries need to find their own approach

- The European Union's General Data Protection Regulation (GDPR) has played a dominant role in shaping global data privacy and protection norms. Participants expect the GDPR to continue to play

This brief is based on a roundtable hosted by CGD as part of the Governing Data for Development project, which explores how governments can use data to support innovation, development, and inclusive growth while protecting citizens and communities against harm. The views expressed here are those of the participants and do not necessarily represent the views of CGD staff. For other briefs in the series, as well as more on the project, visit cgdev.org/governing-data.

this role but argued that countries need to develop their own approach to regulating the use of personal data, in line with local priorities, needs, and capacities.

- Despite broad agreement on the principles that underlie the GDPR, participants expressed concerns about how difficult the framework is to implement, particularly for governments facing significant resource constraints.

Data protection authorities should prioritize their activities according to risk and value

- Most data protection authorities (DPAs) in low- and middle-income countries face funding constraints and struggle to attract employees with the necessary expertise. Some also lack autonomy from other government agencies.

- Participants urged DPAs operating under these conditions to design regulations they can effectively implement under resource constraints and prioritize their activities according to the risk and value created by using data in certain sectors and activities.

Stronger regional coordination will improve data privacy and protection

- Greater regional coordination between DPAs would make it easier for them to share and learn about best practices; strengthen their ability to enforce laws and influence Big Tech companies; and facilitate regulatory harmonization across countries, thereby lowering the cost of doing business across borders.

- Participants highlighted the importance of taking a bottom-up approach to regional harmonization that involved DPAs at the outset.

Effective data privacy requires digital literacy

- Low levels of digital literacy in both the general population and among policymakers present a major hurdle to implementing data privacy laws effectively. Informed consent is essentially meaningless in situations where data subjects lack a basic understanding of how their data is collected and used.

- DPAs and civil society organizations can play a critical role in in raising public awareness about digital rights. Recent initiatives such as the Africa Data Leadership Initiative (ADLI) seek to strengthen digital literacy among policymakers.

KEYNOTE REMARKS

The roundtable opened with three keynote presentations. The following are summaries of the remarks made by Teki Akuetteh Falconer (founder and executive director, Africa Digital Rights' Hub and former executive director, Data Protection Commission of Ghana), Thelma Quaye (head of Digital Infrastructure and Capacity Building, Smart Africa), and Suyash Rai (fellow, Carnegie India).

Summary of Remarks by Teki Akuetteh Falconer, Africa Digital Rights' Hub

Broadly speaking, there are three approaches to data protection and privacy that countries can use as a model: (1) the EU approach, which establishes a comprehensive privacy framework based on individual rights; (2) the US approach, where most privacy laws pertain to specific sectors and states are increasingly pursuing their own frameworks; and (3) the China approach, which combines elements of both the US and EU approach with significant exemptions on how the government may access and use personal data.

African governments that want to enact a data protection law should start by asking themselves what they want the law to achieve and what "mischief" they are trying to cure. The answers to these questions will guide whether they should adopt one model over another (or aspects of each). Regardless of which model policymakers adopt, they need to tailor their choices to the local and cultural context.

The key issue is not whether countries have the "right" laws or the "right" institutions in place. Rather, it is whether they have the resources needed to effectively implement existing laws. The severe resource constraints that DPAs in Africa generally face makes it difficult to carry out their duties and enforce laws.

Today, most African countries lack the resources needed to effectively roll-out a GDPR-like framework.

But a sectoral approach would raise its own challenges, such as creating regulatory gaps between sectors that lead to uneven application of data privacy rules, and the need to pass multiple pieces of legislation. Ultimately, African policymakers will need to develop a data protection and privacy framework that works well for the region and considers the various challenges, including ways to implement such frameworks within resource-constrained environments.

Summary of remarks by Thelma Quaye, Smart Africa

Smart Africa is a pan-African organization with a commitment from heads of state to drive the adoption of digital and mobile technologies in Africa, including by uniting the continent's fragmented digital markets into a single digital market. To support this aim, Smart Africa created a Data Protection and Privacy Working Group to foster greater regulatory harmonization across these issues.

Current models of data protection and privacy are not fit for purpose in Africa.

The need for greater regional harmonization. Although roughly 30 African countries have data protection frameworks in place—most of which are heavily influenced by the GDPR—greater harmonization would make it easier for companies to operate across countries in the region and strengthen enforcement.

The need for greater regional harmonization is well illustrated by recent developments where we see technology companies offering different privileges to users in certain jurisdictions over those in Africa despite having similar data protection laws. This reflects weak enforcement of data protection laws in Africa and the reality that, on their own, most African countries have minimal power to influence the behavior of Big Tech companies. If African countries present a united front on data policy, like EU Member States, they would have greater power to influence and change the behavior of these companies.

Supporting cross-border data flows. Out of the 30 countries in Africa that have data protection laws, only two have policies that support the free flow of data, while the rest have "very bureaucratic" processes in place for determining when data can flow across borders. Barriers to cross-border data flows raise the cost of doing business in Africa. For example, the telecommunications company MTN Africa could provide services more efficiently if it could share data across the region more easily. Smart Africa has established the Africa Data Leadership Initiative, a peer learning platform, to build expertise and promote open data sharing.

Insufficiently resourced DPAs. Several factors hamper the ability of African DPAs to perform their duties:

- Many DPAs are not given a clear mandate to conduct necessary enforcement actions.
- DPA staff often lack the technical expertise needed to carry out laws effectively.
- There is a widespread lack of operational resources.
- Many DPAs lack autonomy from the executive branch, which prevents them from taking independent actions needed to enforce laws.

Summary of remarks by Suyash Rai, Carnegie India

Carnegie India is researching how to build effective DPAs in resource-constrained countries and have used their findings to advise the Indian government on its approach to developing the proposed Privacy and Data Protection Bill (PDP). These remarks focus on how India's PDP has evolved and early findings from the research.

The main drivers behind India's effort to enact a comprehensive data protection framework are:

1. The 2017 Indian Supreme Court ruling on privacy, which stemmed from debates on the Aadhaar biometric ID system, established privacy as a fundamental right, and directed the government to establish a data protection framework.
2. The growing importance of data to India's economy, along with the need to maintain confidence in the ability of Indian data processing companies to process data related to foreign nationals—an aim that could be supported by achieving GDPR adequacy.

While there are several key differences, the PDP is broadly modeled after the GDPR and like the GDPR, the draft law is comprehensive and far-reaching. Because India does not currently have data privacy laws in place, the country will "go from 0 to 100 in one step." Given the large leap involved, the law could do more harm than good, depending on how a newly created DPA implements the law.

To help prepare the Indian government for this transition, Carnegie India's research has focused on two questions related to how the PDP should be implemented in the early stages: (1) How can the DPA get off to a good start? and (2) How should the DPA manage its workload?

Start Strong. We have advocated for the Indian government to establish a DPA through an executive order even before the PDP is passed so the institution can build rudimentary capacity before it is burdened with implementing the full law. We are researching the rollout strategies used by other DPAs to determine the capacities and financial resources needed, as well as the processes that can support independence, accountability, and transparency. We are also considering the degree to which other government agencies (e.g., financial and telecommunications regulators), and even industry groups and academic institutions, could help carry out some of the responsibilities set by the DPA.

The government can also ease the transition period by notifying the law in stages, rather than all at once, to prevent the type of delays seen in South Africa, which took seven years to advance from the passage of its data protection law to putting the law into effect.

Prioritize Resources According to Risk. Because the DPA's capacity will be limited early in its tenure, the institution should use a risk-based approach to direct resources to areas where the risks are highest to prevent overload. To design its approach, the DPA can draw lessons from other policy areas where the risk-based approaches are used, including illicit finance and cybersecurity.

ROUNDTABLE DISCUSSION

The keynote remarks were followed by a moderated discussion focused on questions and issues raised by the opening speakers. The following are key themes that emerged from this discussion.

Countries need to find their own approach

The theme raised most frequently by participants was that countries need to develop their own approach to regulating the use of personal data, in line with local priorities, needs, and capacities. While there was broad recognition that the set of policy options available to LMICs will continue to be influenced by policies enacted by the European Union, United States, and China, most participants stated that a new approach that better meets the needs of countries with more limited resources is needed.

Because all participants agreed that the GDPR has played—and will continue to play—the dominant role in shaping global data governance norms, most of the discussion focused on ways the framework works well as a model for other countries to follow and ways it does not.

There was broad agreement on the principles that underlie the GDPR, but some participants noted that it was unrealistic to expect the Regulation—which draws on more than 30 years of European data privacy experience and jurisprudence to address *European* cultural priorities—to translate well to other countries without significant modification.

One participant emphasized that different societies place a different value on privacy relative to other values and social aims, and that countries should have the freedom to design legal frameworks in alignment with their preferences. Another argued that because of its focus on individual rather than social outcomes, the GDPR could hinder countries from using digital technologies to support economic development and transform their domestic economies. Several participants currently working with national governments to design a comprehensive data protection framework noted concerns raised by local tech companies that a faithful interpretation of the GDPR could hinder innovation, including in AI, putting them at a competitive disadvantage with firms in other countries.

Other participants were more concerned with the difficulty of implementing the GDPR framework effectively. Most of the discussion focused on challenges faced by data protection authorities (DPAs), the institutions established by most modern comprehensive data privacy frameworks to carry out activities related to interpreting and enforcing privacy law, educating the public,

and monitoring compliance. Participants identified three areas where DPAs often face obstacles: (1) funding constraints, (2) difficulty attracting and retaining experts, and (3) lack of autonomy.

- *Funding Constraints.* Most DPAs are underfunded, with many struggling to cover basic operational costs. This undermines the ability of DPAs to carry out their most basic duties and attract employees with the necessary expertise.

- *Difficulty attracting and retaining experts.* As one participant noted, even when DPAs have adequate funding, they are often unable to pay enough to compete with the private sector for highly skilled employees because their compensation practices must align with other government agencies. The same participant noted that the inability of DPAs to attract top talent raised the importance of establishing data privacy frameworks that are simple to implement.

- *Lack of Autonomy.* Many DPAs lack independence from the executive branch or other government agencies—with some even being co-hosted within ministries of ICT or the telecommunications regulators. This lack of independence and autonomy undermines their ability to hold other government actors responsible for violating privacy laws. Participants agreed that DPAs cannot perform their duties effectively without autonomy.

While these obstacles would exist regardless of the type of data privacy framework a country pursues, several participants noted that the complexity and far-reaching nature of the GDPR made it particularly difficult to implement well under existing conditions.

The challenge of enforcement

Participants agreed that data protection laws are weakly enforced in most LMICs. When enforcement actions are taken, they are usually targeted at domestic firms, since most DPAs have a very limited ability to force Big Tech companies to comply with domestic laws. To illustrate this challenge, participants pointed to how WhatsApp handled recent updates to its terms of use. Commenters noted that the WhatsApp issue called attention to the company's longstanding policy of allowing commercial user data to be shared with parent company Facebook and used to target advertising updates. While the company originally announced that it would not force European users to agree to share personal information in compliance with the GDPR, the company did not extend this privilege to any African countries, even though many have similar privacy laws in place.[1]

Comprehensive frameworks still the more appealing option

Despite the challenges associated with implementing a comprehensive data privacy law, participants believed that most countries would struggle even more to implement a sectoral approach to privacy (like the one taken by the United States) since the latter requires legislatures to pass different laws for different sectors, each of which can take several years to draft and pass. The difficulty raised by having to pass multiple laws, coupled with differences in regulatory capacity across sectors, creates a risk that countries that take a sectoral approach could end up with major gaps in their data privacy coverage, with some sectors well-covered and others not at all.

Data protection authorities should prioritize their activities according to risk and value

Participants unanimously agreed that policymakers must consider the GDPR as the starting point when considering their own approach to data privacy but emphasized that they should seek to modify the framework into something that meets local needs and reflects local realities, including resource and capacity constraints.[2] At the same time, several participants emphasized that any approach to data protection a government chooses to take should remain rooted in a rights-based framework that protects citizens against data misuse.

Countries that have already established a data privacy regime consistent with GDPR are unlikely to make major reforms to that regime in the near term, so any modifications would need to take place through regulatory changes. DPAs will need to craft regulations they can execute effectively. Participants discussed several ways

1 The Irish Times, "WhatsApp says European users do not have to share data with Facebook," January 7, 2021.

2 See Rohan Samarajiva's "Best form of data protection is what is workable in a particular country," May 2020.

DPAs can strengthen implementation and enforcement in the face of significant resource constraints:

Using a risk-based approach to prioritize activities. Especially at the outset, DPAs are unlikely to have the resources and expertise needed to carry out their duties across all areas where personal data is used. Echoing the comments made by Suyash Rai, several participants argued that DPAs should direct resources in a phased manner according to the risks posed and value produced by data use in certain sectors, organizations, and activities, with the aim of increasing coverage as their capacity matures. While one participant noted that DPAs do this type of prioritization in practice, she noted that guidance on how to approach prioritization more systemically would be helpful.

Debating whether registering data controllers and processors should be a priority. There was an extended debate on the priority new DPAs should give to enforcing legal requirements that call for registering data controllers and data processors, a key part of many omnibus privacy statutes. Several participants argued that registration requirements can easily overwhelm new DPAs because of the sheer scale of the effort involved, which risks drawing limited resources away from monitoring compliance and enforcing the law. One participant argued that because registering an entity may not lead them to use data more responsibly, new DPAs are better off focusing on the main concern: how to protect data.

Other participants believed that DPAs *should* focus on registering entities early in their tenure because doing so provides them with a better understanding of the actors in the local ecosystem and the kind of information they use—information that ultimately helps DPAs monitor compliance. These participants noted that DPAs could reduce the registration burden by requiring only "significant" data processors and data controllers to register and by ensuring that online registration platforms are easy to use.

Doing more with less. Beyond risk-based prioritization, participants suggested several ways DPAs can be effective in the face of significant resource constraints:

- *Automate and outsource responsibilities.* One participant suggested that DPAs could ease some of their administrative burdens by relying more on regulatory technology (RegTech) solutions to automate how privacy complaints are handled. DPAs could also outsource some of the complaint-handling process to the private sector using a model similar to the one used by the U.S. Federal Trade Commission to enforce the Fair Credit Reporting Act (in which customers lodge complaints with private credit bureaus and the government only steps in when disputes are unresolved).

- *Name and Shame.* Most DPAs lack the leverage needed to take on the world's biggest tech companies. But participants believed they can increase their influence by being strategic about the cases they pursue and how they publicize their efforts. Several participants suggested that DPAs should create a public registry of companies that violate data regulations, noting that the reputational cost for companies would likely be greater than the monetary penalties they could issue.

Stronger regional coordination will improve data privacy and protection

There was unanimous agreement that strengthening coordination across DPAs, particularly at the regional level, is crucial to improving the implementation of data privacy laws in LMICs. Such coordination would benefit DPAs in three ways: first, by making it easier for them to share and learn about best practices; second, by strengthening their ability to influence Big Tech companies; and third, by facilitating regulatory harmonization across countries.

In discussing how coordination could strengthen enforcement, the WhatsApp "terms of use" controversy again served as a reference point. One participant believed that African countries were not extended the same terms as European ones because, unlike EU member states, they "did not speak with one voice." Another participant noted that at least four Latin American DPAs sent separate public requests to WhatsApp to stop the terms of use update until its effect could be studied. While the DPAs were aware their ability to stop WhatsApp's policy change was limited, the collective effect of their actions created greater pressure on the company and showed that the DPAs were paying attention to the issue.

By making it easier to share best practices, stronger coordination among DPAs would also make it easier for DPAs to align their practices, which would lower compliance costs for companies that operate across borders. One participant highlighted recent conversations with African telecommunications providers, who noted the high cost of developing bespoke compliance programs for each country they operated in and argued that harmonizing data privacy regulations in the region would lead to greater investment in digital technology.

Participants emphasized the importance of taking a bottom-up approach to aligning data policies across countries and involving DPAs from the outset. Participants expressed a concern that DPAs are often excluded from trade agreement negotiations that impinge on data protection practices.

Finally, one participant highlighted the tension between calls for greater regional harmonization and criticisms that some countries are simply "cutting and pasting" the GDPR into domestic law. He argued that, while a communal approach to regulatory harmonization may be ideal, having all countries in a region establish a GDPR-based data privacy framework would meet the same need.

Effective data governance requires digital literacy

Low levels of digital literacy in the general population and among policymakers present a major hurdle to effectively implementing data governance and privacy laws. Several participants argued that the concept of "informed consent," which serves as the primary legal basis for data processing in all major data privacy frameworks, including the GDPR, is meaningless in situations where data subjects do not have a basic understanding of how their data will be used—and that this description characterizes many transactions involving personal data. As an example, one participant highlighted a recent study of Kenyan banks' data privacy policies, which found that understanding them required a college education, despite only a small percent of Kenyans graduating from college.[3]

In addition to being digitally literate, an informed populace must also know their data rights and be able to question why data about them is being collected and how it will be used. Participants noted that DPAs should educate the public on these matters but said that they are often too resource-constrained to do so in practice. One participant highlighted the important role of civil society organizations (CSOs) in raising public awareness about digital rights.

While policymakers are generally more digitally literate than the general populace, several participants noted that many still do not understand how to design policies that unlock the value of data while protecting citizens' rights. Thelma Quaye highlighted the Africa Data Leadership Initiative (ADLI) jointly launched by the UN Economic Commission for Africa, Future State, and Smart Africa in 2020 to build African policymaker expertise in this area.[4]

NEXT STEPS

This event was the first in a series of private roundtables that the Center for Global Development is hosting to explore the relationship between data governance and economic development. Subsequent roundtables will explore the role of trade agreements in establishing digital policy norms, how global and regional institutions can support better data governance practices, and ways to increase the input of low- and middle income countries into debates on the design of global data governance standards.

The insights shared in the roundtable series will inform CGD's Governing Data for Development Working Group in drafting recommendations on steps policymakers can take at the regional and global levels to support the creation and implementation of data policies that work well for all countries. More information on the project, including a series of blogs and other roundtables summaries can be found here.

3 https://cipit.strathmore.edu/data-protection-in-the-kenyan-banking-sector/.

4 https://www.uneca.org/storys/eca-smart-africa-future-state-launch-africa-data-leadership-initiative.

ROUNDTABLE PARTICIPANTS

Abebe Shimeles, African Economic Research Consortium

Abu Bakar Bin Munir, University of Malaysia

Adedeji Adeniran, Centre for the Study of the Economies of Africa

Anir Chowdhury, Access to Information

Aretha Mare, Smart Africa

Ashnah Kalemera, Collaboration on International ICT Policy in East and Southern Africa

Bitange Ndemo, University of Nairobi

David Medine, Consultant

Deepa Karthykeyan, Athena Infonomics

Dianah Muchai, African Economic Research Consortium

Fabrizio Scrollini, Open Data Latin American Initiative

Fiorentina García Miramón, DataMexico

Helani Galpaya, LirneAsia

Isaac Rutenberg, The Centre for Intellectual Property and Information Technology Law

Jenna Slotin, GPSDD

JJ Disini, Disini Law Office

Luis Fernando Godoy Rueda, DataMexico

Martina Barbero, Global Partnership for Sustainable Development Data

Rachel Sibande, UN DIAL

Rohan Samarajiva, LirneAsia

Santosh Misra, Tamil Nadu e-Government

Shruti Viswanathan, Athena Infonomics

Sone Osakwe, Centre for the Study of the Economies of Africa

Stephen Chacha, Tanzania Data Lab

Suyash Rai, Carnegie India

Teki Akuetteh Falconer, Africa Digital Rights Hub

Thelma Quaye, Smart Africa

Victor Ndede, Amnesty Kenya

Wairagala Wakabi, Collaboration on International ICT Policy in East and Southern Africa

---

Center for Global Development
Ideas to Action: Independent research for global prosperity

WWW.CGDEV.ORG

MICHAEL PISA is a policy fellow at the Center for Global Development.

UGONMA NWANKWO is a research assistant at the Center for Global Development.