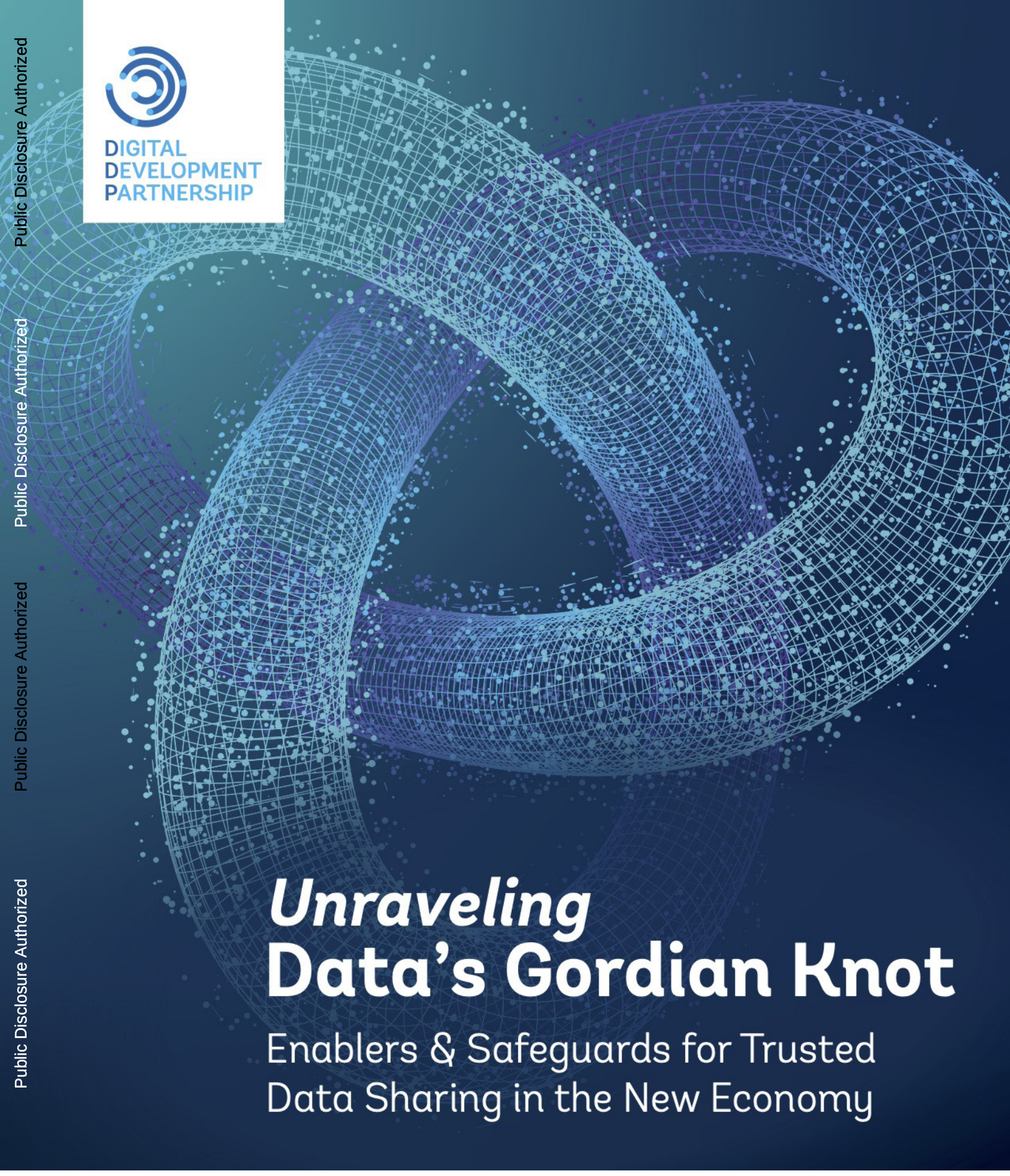
DIGITAL DEVELOPMENT PARTNERSHIP



Unraveling Data's Gordian Knot

Enablers & Safeguards for Trusted Data Sharing in the New Economy

WORLD BANK GROUP

WITH SUPPORT FROM:

Google GSMA Microsoft

CONTENTS

FOREWORD

As countries around the world battle the COVID-19 pandemic, the importance of sharing and using data effectively has never been more apparent. Data collection and analysis tools for diagnostics, detection, and prediction are of critical importance to respond intelligently to this crisis and prevent more lives from being lost. An effective response requires data to be shared between institutions, across sectors, and beyond national borders. Because data is critical to understanding, anticipating, and responding to the crisis, new approaches to share data are being tried, some which may have concerning consequences for individual data protection. It is an extraordinary moment where the use of personal data for helping society may potentially come into conflict with data protection norms.

This report, *Unraveling Data's Gordian Knot*, could not be more pertinent to the fight against COVID-19. In it we find that unlocking data for reuse need not be at odds with individual rights. Rather, data sharing has the promise to uphold data protections and even enhance individual agency and trust. With the right enabling environment, data can be freed for use by governments, businesses, and individuals while ensuring people's agency and rights are central.

For people, and particularly for traditionally disadvantaged groups, leveraging one's data to access a service—using, for instance, a credit score, a land rights certificate, or medical history—without the burden of bureaucracy or corruption can be profoundly empowering. It can mean the difference between receiving health treatment in time or not. Or receiving a fairly priced loan or not. Demonstrating eligibility for social services or not. Perhaps more than the direct services themselves, it gives individuals who too often have been disenfranchised or oppressed, an intangible asset that helps them prove who they are and better their lives.

As the World Bank continues to invest in digital infrastructure, digital public platforms, and the enabling environment that supports such infrastructure, it is critical that we also focus on the enablers and safeguards for robust data ecosystems that allow data to be harnessed by governments, firms, civil society, and individuals. Analytical pieces such as this report and the upcoming World Development Report are important frameworks that can help operationalize how to support countries around the world leverage data as an essential tool for development and ensure all people are able to actively participate in and benefit from the new data-driven economy.

Dr. Boutheina Guermazi
Director, Digital Development, The World Bank

ACKNOWLEDGMENTS

This World Bank report was drafted under the leadership of Vyjayanti Desai and was authored by Jonathan Dolan, Kay McGowan, and Priya Vora of Future State, together with a cross GP team of the World Bank, including Adele Barzelay, Prasanna Lal Das, David Satola, Sharada Srinivasan, and Vyjayanti Desai. The drafting team also comprised James Freymuth of the Bill and Melinda Gates Foundation and Elizabeth Renieris. The report was written with information from country case studies as of July 2020.

At the decision meeting, chaired by Boutheina Guermazi (Digital Development Director), Vivien Foster (World Bank), Kai Kaiser (World Bank), Rory Macmillan (Macmillan Keck), James Neumann (World Bank), and Michael Pisa (Center for Global Development), served as peer reviewers.

The team would also like to express their gratitude to all those who provided insights and gave their time to provide guidance and support at various stages of the project, including:

- Jose Clastornik, Laura Rodrigues, Laura Amado, Gonzalo Sosa Barreto, Susana Dornel, Drudeisha Madhub, Rajnish Hawabhay, Jonathan Mendoza, Jesús Javier Sánchez García, Kellie Tan, Joseph Lee, Daniel Lim, Venkatesh Hariharan, Tanuj Bhojwani, Hannes Astok, Heiko Vainsalu, Uuno Vallner, Katrin Nyman Metcalf, Anette Forsindal, Dianne Hubbard, Jamie Leach, and Andrew Stott who participated in interviews or served as expert external reviewers of the report.

- Other World Bank Group staff who offered periodic inputs into the report itself and facilitated introductions to government officials and other experts who contributed to this report including Julian Najles, Jonathan Marskell, Anat Lewin, Malarvizhi Veerappan, Audrey Ariss, Veronica Silva, Fredesvinda Fatima Montes, Tiago Carneiro Peixoto, Herini-aina Mikaela Andrianasy, and Lesly Goh.

EXECUTIVE SUMMARY

DATA-DRIVEN DEVELOPMENT: A DIGITAL GORDIAN KNOT

Data is more abundant than ever before and is increasing in unprecedented ways, creating new industries and reshaping existing ones. In low- and middle-income countries—increased access to digital technologies, more time online, and increased ways to use digital products and services—are combining to dramatically expand the amount of data produced by individuals. Governments around the world are seeking to leverage data to accelerate economic growth, improve the efficiency and transparency of government, and tackle persistent socioeconomic development challenges. The opportunities of data-driven development are compelling and examples of positive outcomes abound.

The use of data has the potential to underpin these new levers for development. However, it could also limit competition and innovation by consolidating decision-making power among a limited number of powerful actors. Use of data could exacerbate exclusion and inequality by undermining trust in critical institutions through data breaches and government surveillance and targeted disinformation campaigns, and reinforcing biases through opaque algorithms.

Over the years, some have suggested that unlocking data in order to create value is at odds with the goal of protecting people from abuses and misuses of data. Yet, adopting a robust policy, legal, and technical regime of safeguards can support value creation from data by enabling individuals to benefit from clearer rights and greater agency over their data, while also increasing the transparency and accountability in how data is used. Emerging technological and governance solutions can further support these objectives and rebalance power asymmetries in favor of people and small and medium enterprises. The effective implementation of existing data protection regimes and adoption of innovations in data governance enable trusted data usage and sharing, thereby helping address the alleged tension between data protection and data flows.

The report finds that the ability of data to be a force for positive development is dependent upon how the value and control of data are distributed across the data life cycle and getting that distribution right requires new modalities for trusted sharing of data.

FOCUS ON TRUSTED DATA SHARING

This report asserts that creating a data sharing environment in which transactions between data providers and data users are trusted requires enabling the right mix of laws and policies, institutional arrangements, and technical architecture, as well as an informed and engaged civil society. In other words, getting the right "enablers" and "safeguards" in place for data sharing is of central importance to realizing the development potential of data, ensuring that the opportunities offered by data accrue across diverse stakeholder groups, and securing certain rights of individuals in relation to their data.

> The aim of this report is to highlight emerging practices and interesting features of countries' current approaches to establishing these safeguards and enablers of data sharing.

The report draws extensively from seven country case studies (India, Estonia, Singapore, Chile, Mauritius, Uruguay, and Mexico), as well as two sector-specific spotlights on data sharing in Open Banking (highlighting the experiences in the United Kingdom and Australia) and in health data sharing (highlighting the current response to the COVID-19 pandemic) where efforts have been made to establish such enablers and safeguards. In selecting these countries and sectors, the report makes some normative assumptions about what is needed, but then takes an iterative approach to test and refine this assertion by examining the experiences of the countries included in the case studies and, ultimately, propose a framework for a trusted data sharing ecosystem.

Through this iterative process, it is apparent that an increasing number of countries are adopting a rights-based approach to data protection. Under this approach, in addition to regulatory duties applying to organizations enforceable by a regulator, individuals have legal rights that they can enforce directly against those organizations through a private right of action. It is also clear that government action to expand the value of data to individuals and entrepreneurs manifest most visibly in jurisdictions that have adopted effective data protection regimes in an attempt to shift some of the burden for data protection and security to service providers. However, this approach is primarily a legal solution that does not necessarily create the other conditions (e.g., strong and responsive institutions, informed and engaged civil society) which enable individuals, entrepreneurs, or society to benefit fully from the rich data histories generated online. It is also apparent that this legal and regulatory approach to building a trusted data sharing ecosystem by protecting the rights of individuals is insufficient on its own and validates the need for complementary investments. The countries profiled in this report have taken varied approaches to doing so. Nevertheless, there are a number of common characteristics in place to maximize the value of data as a tool to achieve development outcomes. These characteristics together expand who can derive value from data and ensure individuals' rights are preserved even as data is shared more extensively. They can be organized around five main pillars and provide a framework for governments seeking to support trusted data sharing:

Pillar	Purpose	Practices and Features
Policies, laws, and regulations	To clearly define rights and obligations over data, including the rights of people to determine when and how personal data is collected, shared, and used	1. Clear and enforceable rights-based approach to data protection policies and laws 2. Investment in a whole-of-government approach to implementing data governance in order to reconcile instances where there are competing policy priorities across government agencies 3. Iterative and adaptive approach to data policy making in order to continuously calibrate and refine the relationship between sharing data and keeping it safe and secure

Pillar	Purpose	Practices and Features
Robust and resourced institutions	Enabling institutions responsible for developing and implementing strategies, policies, laws, regulations, standards, and guidelines to enable effective data collection, processing, and use. Safeguarding institutions to monitor and oversee progress, enforce rules while also offering citizens responsive and effective redress	1. Strong coordinating bodies within government that can harmonize approaches to data protection and data sharing 2. Specific steps to engender trust in institutions and to establish appropriate capabilities within institutions, including, supervisory and oversight functions and clear redressal systems for individuals

Pillar	Purpose	Practices and Features
Trusted technical architecture	To standardize data sharing within government and regulated institutions while giving people more controls and transparency into data flows	1. Investments in technology platforms that break down data silos and facilitate the exchange of data in ways that create accountability (e.g., Singapore's digital watermarks for tracing the originator of documents) and transparency (e.g., Estonia's State portal that gives individuals granular insights into who is sharing their data and for what purposes). 2. Iterative and adaptive approach to introducing and continuously improving technical architecture to expand capabilities for the user and to strengthen data protection

Pillar	Purpose	Practices and Features
Capabilities within and in support of government	To analyze and make use of data	1. Investments in reorganizing and strengthening the human resources of government agencies in order to harmonize approaches to data governance and to ensure the proper capabilities to establish and implement effective data governance strategies. Such efforts include programs to cross-train policy makers and technologists and to embed technical expertise across traditional government ministries 2. Strategic collaboration between governments and private firms or civil society to share data in ways that are both secure and more broadly accessible

Pillar	Purpose	Practices and Features
Active civil society and informed populace	To use data effectively and keep governments and companies accountable	1. Well-resourced and sustained national programs to provide digital skills training 2. Multistakeholder processes to develop open data policies and other strategic planning related to data protection and data sharing

Ultimately, when designed and implemented well, these pillars—and the practices and features that help build them—can support an ecosystem in which data sharing and data protection become mutually reinforcing. While there is no one-size-fits-all approach to promoting trusted data sharing, governments can draw from the experiences profiled in this report and tailor these practices to fit their specific development objectives.

INTRODUCTION

Today there are more than 4 billion internet users globally, an increase of approximately 1 billion since 2015, and global smartphone penetration has increased by more than 40 percent in that same time as the cost of devices and data plans have dropped.[1] And yet, this growth is only part of the digital transformation happening today. According to Cisco's latest Visual Networking Index, there will be 3.5 networked devices per capita globally by 2021[2] and some estimates suggest that connected devices could grow to 125 billion by 2030—an annual average growth rate of 12 percent.[3]

As the World Bank's 2018 *Data-Driven Development* report noted, "even traditional industries, such as oil, automobile manufacture and financial services, are becoming data driven. We are undoubtedly experiencing a data revolution in which our ability to generate, process, and utilize information has been magnified many times over by the machines that we increasingly rely upon."[4]

Data is more abundant than ever before and is increasing exponentially. The frequently cited 2016 IBM report, "10 Key Marketing Trends For 2017," noted that 90 percent of all data had been generated in 2015 and 2016 alone, and recent estimates suggest more data was created in 2017 than in all previous years combined. These trends will only accelerate globally and low- and middle-income countries will become an increasingly substantial part of this growth.

Importantly, some of the regions where internet usage has lagged historically are now seeing some of the fastest growth rates. Africa, for instance, has recently enjoyed 20 percent year-on-year growth in internet usage[5] driven by the rapid expansion of mobile internet and, along with the Middle East, it is expected to see the fastest growth in mobile broadband usage over the next five years.[6] Internet users in low and middle income countries now outnumber internet users in developed markets by more than two to one, and the difference is growing. It has been estimated that low- and middle-income countries will contribute approximately 900 million new internet users between 2018 and 2022, compared with approximately 80 million from developed markets that are already highly connected. In other words, if these projections hold, more than 90 percent of all new internet users will come from low- and middle-income countries.[7]

The expanding population of internet users, however, is only part of the data abundance story. Internet users in low- and middle-income countries are spending more time online each day and diversifying the ways in which they are using the internet. Consumers in these markets, for instance, are increasingly using the internet for commercial purposes. E-retail revenues in the biggest emerging markets rose to $800 billion in 2017, a figure that represents 15 percent of all retail revenues in those markets. By 2022, it is expected that almost half of all low and middle income retail spending will reflect some type of digital

1 Howell, Jenalea. "Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says (2017, October 24, 2017). https://news.ihsmarkit.com/prviewer/release_only/slug/number-connected-iot-devices-will-surge-125-billion-2030-ihs-markit-says. Accessed March 2020.

2 Cisco Visual Networking Index (VNI): Forecast and Methodology, 2016–2021. (Updated 2017, September 15), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html#_Toc484813970. Accessed March 2020.

3 Howell, Jenalea. "Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says (2017, October 24, 2017), https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says. Accessed March 2020.

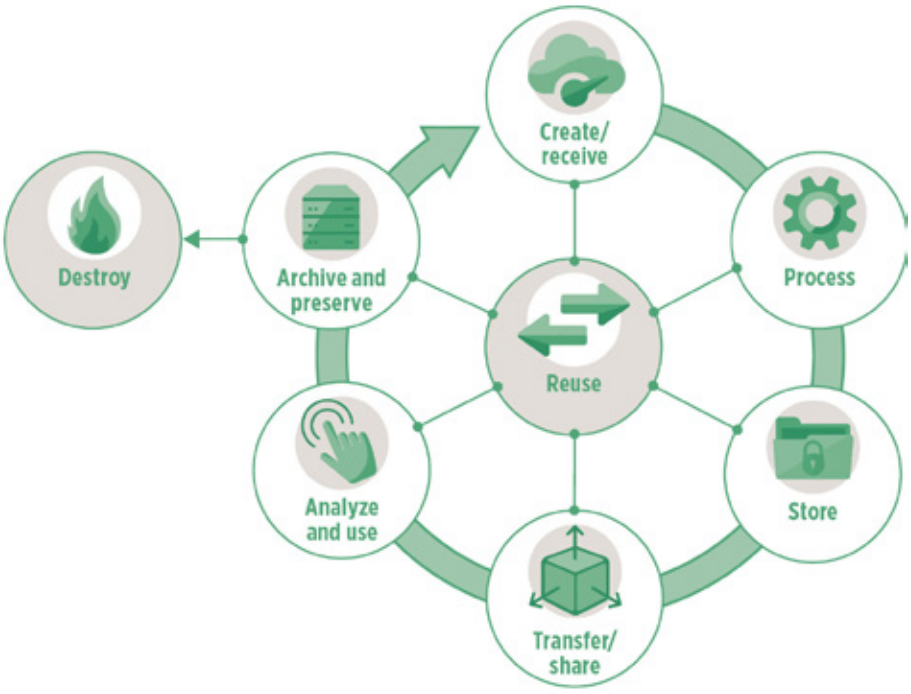
4 World Bank. "Data-Driven Development" blog, https://www.worldbank.org/en/topic/digitaldevelopment/publication/data-driven-development. Accessed March 2020.

5 Ericsson, "Ericsson Mobility Report, November 2019."

6 Shapshak, Toby. "Africa Is Fastest Growing Region For 5G Mobile Broadband Uptake, Says Ericsson." Forbes, https://www.forbes.com/sites/tobyshapshak/2019/11/28/africa-is-fastest-growing-region-for-5g-mobile-broadband-uptake-says-ericsson/#7ad53c111c25. Accessed May 2020.

7 Jain, Nimisha; Walters, Jeff; Bharadwaj, Aparna; Niavas, Stefano; Azevedo, Daniel; and Sanghi, Kanika. "Digital Consumers, Emerging Markets, and the $4 Trillion Future." BCG, https://www.bcg.com/publications/2018/digital-consumers-emerging-markets-4-trillion-dollar-future.aspx. Accessed March 2020.

Figure 1: The Data Life Cycle



Source: WDR 2021 team.

influence.[8] And, in 2018, three of the top five app download markets were emerging economies—with India increasing app downloads by 170 percent from the previous year and Indonesia increasing by 60 percent over the same period.[9]

Together, these factors in low- and middle-income countries—increased access, increased time online, and increased uses—are combining to dramatically expand the amount of data produced by individuals. As data rapidly becomes more abundant, low- and middle-income countries are becoming more focused on realizing its full potential through three main channels: (1) driving economic growth through trade and private sector and entrepreneurial activity, (2) creating more efficient, accountable, and transparent government, and (3) empowering people.

The following sections of this report examine these development motivations in more detail with a specific focus on how data sharing helps underpin each. Data has the potential to underpin these new levers for development. However, it could also limit competition and innovation by consolidating decision-making power among a limited number of powerful actors. Use of data could also exacerbate exclusion and inequality by undermining trust in critical institutions through data breaches and government surveillance, targeted disinformation campaigns, and reinforcing biases through opaque algorithms.

> Ultimately, the ability of data to be a force for positive development is dependent upon how the value and control of data are distributed across the data life cycle.

8 Jain, Nimisha; Walters, Jeff; Bharadwaj, Aparna; Niavas, Stefano; Azevedo, Daniel; and Sanghi, Kanika. "Digital Consumers, Emerging Markets, and the $4 Trillion Future." BCG, https://www.bcg.com/publications/2018/digital-consumers-emerging-markets-4-trillion-dollar-future.aspx. Accessed March 2020.

9 Sydow, Lexi. "Growth and Expansion Through Mobile in 2019: Mature and Emerging Markets." App Annie, https://www.appannie.com/en/insights/market-data/mobile-2019-mature-and-emerging-markets/. Accessed April 2020.

A FOCUS ON DATA SHARING

Because of its nonrivalrous nature, data can be shared for the benefit of stakeholders across the private sector, government, and individuals. Repeated reuse can help harness the full potential of data to extract a wide range of insights. At the same time, however, greater sharing of data can increase the risks of misuse. Creating a data sharing environment in which transactions between data providers and data users are trusted requires the right mix of laws and policies, institutional arrangements, and technical architecture.

In other words, getting the right "enablers" and "safeguards" in place for data sharing is of central importance to realizing the development potential of data and ensuring that the benefit of data accrues across diverse stakeholder groups.

Without adequate safeguards, data providers may be concerned about potential abuses, ranging from weak security of data transactions to the opaque collection and sale of personal data by third-party data brokers. At the same time, without adequate enablers—including transparency, interoperability, and data portability—it may become prohibitively difficult to transfer data among different providers in an agile and seamless manner.[10]

OECD'S DEFINITIONS OF DATA SHARING

The Organisation for Economic Co-operation and Development (OECD) 2019 report, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, provides a useful reference in this respect, offering detailed data sharing definitions and the relationship between the primary categorizations of data. At a minimum, for the purposes of this report, it is worth noting the OECD's definitions of data sharing and the relationship between public, private, and personal data.

Definitions for Data Sharing

"Data sharing" refers to the provision of data by the data holder, on a voluntary, passive, or mandatory basis. Certain types of data sharing agreements may be based on commercial or noncommercial contractual agreements (e.g., data philanthropy); other data sharing may be mandated by policy or law, such as Open Data or Access to Information, or data required for service delivery or identification. Voluntary data sharing is assumed to be based on common interests between the entities agreeing to share their data, including the interest and expectation that data holders can become data users and vice versa, but power asymmetries (e.g., between firms, or between governments and individuals) and other political economy dynamics may affect the expectation of reciprocity among stakeholders engaged in data sharing agreements.

"Enhanced access and sharing" refers to mechanisms and approaches aimed at maximizing the social and economic benefits from the wider and more effective use of data, while, at the same time, addressing related risks and challenges. The term does not cover cases where governments access private sector data either for law enforcement and national security purposes or for granting regulatory approval (e.g., for the marketing of pharmaceutical or agricultural chemical products).

10 Language from World Bank 2021 WDR draft.

Domains of Data: Understanding Public, Private, Personal, and Open Data

The creation or collection, processing and use of personal and nonpersonal data by public or private sector actors give rise to a number of typologies and governance domains.

The *personal versus nonpersonal data* domain, which relates to the identifiability of the data. Personal data can be volunteered, observed, or inferred (WEF 2011). Recent technologies and analytical techniques, such as those based on Artificial Intelligence (AI) or Internet of Things (IOT), are creating new categories of "mixed" data that erodes the binary distinction between personal and nonpersonal data.

The *public versus. private sector* domain, which relates to the entity or actor (government or private sector) which controls the relevant data. Public sector and private sector data are controlled by governments and firms respectively. Both types of data may be proprietary, but may be permitted for reuse or sharing under specified terms. Access and control rights over data may be determined by governments and firms: in the public sector, these are often specified through data classification policies, depending on their sensitivity. In the private sector, data may be protected via intellectual property rights, and licensed to specified users.

Openly available vs. restricted data, which relates to the manner in which proprietary data sets are made available for use and reuse by public or private sector entities, often through data sharing agreements or licenses. At one end of the spectrum, data may be completely restricted on proprietary, security, or sensitivity grounds. Proprietary data is typically protected by IPRs (including copyright and trade secrets) or by other access and control rights (provided by contract and legal requirements, e.g., cybercrime law), reflecting the fact that there is typically an economic interest to control or limit access to such data. On the other side of the spectrum, public and private sector data can be made openly available (through licenses and publication in specific formats and on a user-facing platform) for free access, use, and reuse according to the terms of a sharing friendly license. In between, access to data sets can be restricted by data sharing agreements, along terms agreed by the parties.

These domains are overlapping and dynamic, and the underlying type of data does not necessarily determine how they might be treated legally or governed across the data life cycle. It is more accurate and helpful to determine how such data are used or processed. For example, restricted "public sector" and "personal data" (e.g., a household survey or education data aggregated and shared) might end up being treated as "private sector" and "nonpersonal" data when de-identified and integrated into an application developed by a private sector company. Similarly, proprietary company data collected by IOT sensors might become "public sector" and "open" data if shared with a local government under a Public Private Partnership (PPP) and published (after being de-identified) on their open data platform.

Source: OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en.

The aim of this report is to highlight emerging practices and interesting features of countries' current approaches to establishing these safeguards and enablers of data sharing.

While there is no single authoritative typology of data, there are various approaches to classifying data, with significant overlap among them. The intent of this report is not to develop a new or singular typology of data nor does it attempt, given the significant overlap between types of data, to create definitive boundaries around which data are part of this analysis and which are not. Rather, this report attempts to convey the opportunity for a data ecosystem that broadly creates trusted data sharing and specifying, where necessary, the type of data being addressed.

Complexities of data sharing—both in terms of type of data and the mechanics of how that data is shared—present policy makers in low- and middle-income countries with important strategic questions related to their national development strategies: How do national development objectives align with data protection and data sharing policies? What are the incentives of different actors to share data and how can the government promote trusted data sharing? How can data protection be achieved in environments of low human, institutional, or technological capacity? What are the most effective levers for creating systems of trusted data flow within and across borders?

RATIONALE AND CONTEXT FOR THE REPORT

RATIONALE FOR THE REPORT AND THE TRUSTED DATA SHARING OPPORTUNITY

A 2019 survey of digital policy makers conducted in collaboration with Oxford University's Pathways to Prosperity revealed that "Data Sharing and Interoperability" and "Privacy and Data Protection" are increasingly among the top policy priorities of emerging market policy makers. In the survey of over 100 emerging market policy makers and their advisers, one-third of all respondents identified one of these two issues as their top priority, followed by "Telecommunications Infrastructure" (25 percent) and "Jobs and Skills" (24 percent).

We mention here two broad trends that are shaping the answers to these strategic questions:

Trend #1: A growing recognition of data as a valuable factor of production and powerful lever of influence.

Decision-makers at all levels—from governments to business to individuals—increasingly recognize the value of data as a factor of production and as a tool to be leveraged for better decision-making and greater influence. The UN Sustainable Development Goals (SDG)[11] depend on the effective exploitation of data across numerous sectors.

The nature of data, the uses for which it may be deployed, and the challenges to which these give rise, now make data governance a vital dimension of economic development policy. For example, Japan placed data governance squarely on the international agenda for the 2019 G20 summit.[12] As recognized in the World Bank's 2018 *Data-Driven Development report,*[13] stakeholders are increasingly seeking to establish access to and rights over data.

When establishing governance regimes over data, countries can draw from experiences of governing other resources but there are no exact parallels. Unlike other factors of production, data is, in theory, abundant, reusable, nonrivalrous, and typically created by the interaction of at least two parties.

With such a resource, the value of data is driven less by natural scarcity and more by scarcity and restrictions imposed through rights and obligations, whether imposed by legislatures, regulators, contracts or other sources of law such as tort liability. Determining who can access and process data, as well as when, is critically important to determining how and to whom the benefits of data-driven insights accrue and are distributed in an economy.

For example, property right limits on data that is the lawful intellectual property of a firm that has developed the data as a form of copyright pose restrictions on others using it. This is particularly so with proprietary commercial data, which may often be mixed with personal data. Contractual obligations between organizations, public and private, that impose restrictions and responsibilities on use of data that is shared-further refine the productive use to which it may be put. Regulatory requirements imposed by cyber security and data protection laws in general, or sectors of particular importance such as health and finance, restrict further what can be done with data. Rights of individuals to access personal data held about them, have errors corrected, have data ported to other entities (including formatting requirements) shape the economic opportunity further. Prohibitions on outputs that perpetuate or effect bias among different

11 WDI: Sustainable Development Goals, World Bank Group, https://datatopics.worldbank.org/sdgs/sdg-goals-targets.html (last visited Dec. 27, 2019).

12 Resolved: Japan Could Lead Global Efforts on Data Governance, Center for Strategic & International Studies, (Jun. 27, 2019), https://www.csis.org/analysis/resolved-japan-could-lead-global-efforts-data-governance.

13 World Bank. 2019. "Information and Communications for Development 2018: Data-Driven Development."

population groups affect how artificial intelligence may be used for commercial and public administrative decision-making.

The business models of some of the world's most valuable companies are now predicated on collecting vast amounts of data about individuals, their behaviors and preferences, resulting in a wider industry of data collection and trade through third party data brokers. Firms whose business models increasingly rely on data insights not only include technology companies but also mobile network operators, banks and other actors from traditional industries. By design, commercial service providers not only offer products but capture data usage which can be used to target ads, improve the platform's services, or profit from selling insights. In turn, many consumer products are offered free of charge or heavily discounted. Despite this immediate value to consumers, there are concerns among policymakers, activists, rights advocates and others that such data-reliant business models can erode trust, expose personal data to potential compromise, threaten competition, stifle innovation, and constrain distribution of the economic value of data.

There are emerging examples of private firms exploring ways to pool or transfer data securely between technology platforms. This includes Microsoft's Open Data Initiative, Google's Private Join and Compute, and a consortium of technology companies introducing the Data Transfer Project.

Of course, private sector actors are not the only entities seeking to leverage data. While governments have always sought ways to benefit from the value of data — for instance, China's emerging Social Credit System[14] or the United States' use of mobile phone data for immigration and border enforcement[15] – nothing has put governments' interest in harnessing data into sharper focus than the COVID-19 Pandemic. These efforts, some of which are addressed later in this report, include contact tracing efforts (e.g., using cellphone call data records or CDRs), to ramping up public health data surveillance and more recently, verifying vaccination status (e.g. vaccine certificates) and immunity.

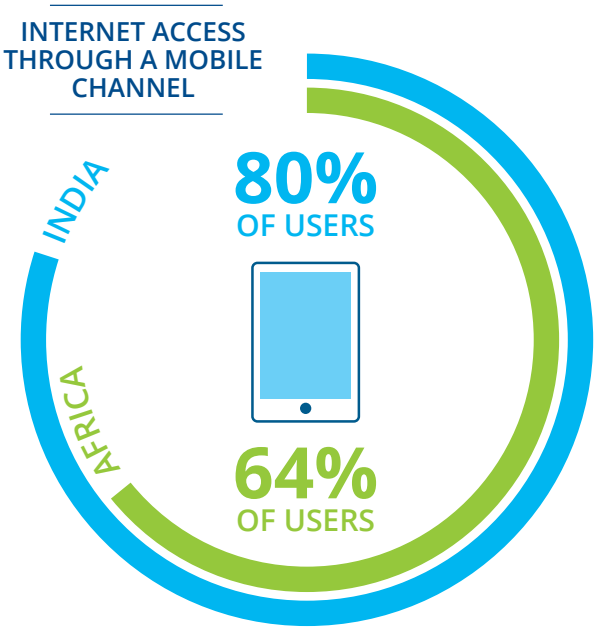
The COVID-19 pandemic has also shown that the risks of allowing control over these data and their benefits to concentrate in the hands of a powerful few is present in many countries. Data inequities arising from these concentrations of power are exacerbated by phenomena such as (1) data deficits—instances where data is relatively scarce—emerging in economies or communities that have low purchasing power leading to disparities in the data-driven services that can be tailored to meet their needs, (2) weak institutions that are not well equipped to keep up with rapid changes in technology related to an increasing dependence on data, or (3) the inability of otherwise competent regulators to effectively address the imbalances resulting from the lack of regulatory reach – given that the jurisdictional home of many of the Big Tech and Big Data firms are in developed countries. The resulting regulatory lacunae is particularly prevalent in lower- or middle-income countries where governments and private service providers have limited bargaining power thus directly affecting their ability to establish guardrails between infrastructure and application layers in order to foster a local innovation ecosystem.

Additionally, consumers in developing countries are structurally more vulnerable to data capture and over-consent as they often have fewer choices in services, must provide consent to receive certain benefits, or because of a lack of awareness or digital skills. Free services that collect vast amounts of data on usage

14 Creemers, Rogier, China's Social Credit System: An Evolving Practice of Control (May 9, 2018). Available at SSRN: https://ssrn.com/abstract=3175792 or http://dx.doi.org/10.2139/ssrn.3175792

15 The New York Times Editorial Board. "The Government Uses 'Near Perfect Surveillance' Data on Americans". *The New York Times*, February 7, 2020, https://www.nytimes.com/2020/02/07/opinion/dhs-cell-phone-tracking.html. Accessed April 2020.

patterns are particularly prevalent in low-income communities, where the risks of data sharing are less well known. Additionally, the convenience of a mobile device, coupled with the cost of computers and scarcity of reliable power, has led to people accessing the internet through a mobile device than through a desktop. In India, 80 percent of users access the internet through a mobile channel. In Africa, where internet usage is lower, 64 percent of users rely on a mobile device for internet access. The mobile revolution has led to a user interface dominated by applications ("apps"). Apps such as Alibaba, WhatsApp, and Facebook have become portals through which a user can access a variety of services generating further data for the parent company. Many of these apps collect and transmit data without user knowledge even when not in use.



Perhaps most importantly, low- and middle-income countries are seeing faster digitization than economic advancement. In the words of Nandan Nilekani, individuals in developing countries are becoming data-rich before they become economically enriched.[16] It is therefore a critical moment in time to explore ways of converting this data wealth into a lever of development.

There are numerous examples of positive development outcomes underpinned by data sharing including examples from the countries profiled in this report (see annexed case studies). Two ways in which governments in particular are commonly seeking to leverage data as a factor of production are:

First, to drive economic growth through trade and private sector and entrepreneurial activity:

Some governments are developing data policies to establish consistency with trade partners and facilitate e-commerce and digital businesses. Other governments seek to create more opportunities for entrepreneurs to leverage data to design products and services for consumers. Of the countries profiled in depth later in this report, a number of examples emerge where efforts to create a trusted data sharing ecosystem have helped increase economic activity and more inclusive growth:

1. Mauritius has contributed to its strong economic growth by, among other things, establishing itself as a regional leader in the financial services industry and a gateway to doing business in the sector throughout Africa. This leadership role has been possible because the country has put into place both a strong data protection regime in line with international practices and because of its efforts around Open Data policies. Together, these elements have enabled the country to effectively support financial sector regulatory sandboxes

16 Nilekani, Nandan. https://blogs.worldbank.org/voices/giving-people-control-over-their-data-can-transform-development.

and underpin institutions like the Mauritius Africa FinTech Hub, which provides an ecosystem where entrepreneurs, corporations, governments, tech experts, investors, financial service providers, and researchers can collaborate to build financial services products for the African market.

2. In India, business-to-business company ShopX is processing half a million transactions daily via its digital platform, which connects fast-moving consumer goods (FMCGs) companies and traders to small retailers throughout the country. The platform enables suppliers and retailers to use data on consumer behavior and preferences to improve sales and to facilitate the entry of lower-income Indians into the digital economy.
3. Morocco's data protection Law n° 09-08 (February 2009) closely mirrors the EU's 95/46/EC Directive (the precursor to the European Union's General Data Protection Regulation (GDPR)), and was intended to enable convergence with EU law to incentivize foreign direct investment (FDI) and leverage Morocco's competitivity in data offshoring and outsourcing and its geographic proximity to European markets. Morocco's request for an adequacy recognition from the European Commission in 2009 is still pending, but the country became a signatory to Convention 108 (the sixth country in Africa to accede) in May 2019. Since 2018, the Moroccan data protection authority (CNDP) has collaborated with the Council of Europe under the Neighbourhood Partnership 2018–2021 to work towards progressively revising the 2009 law and aligning it to GDPR, while considering local specifications, to maintain its competitiveness.

Second, to create more efficient, accountable, and transparent government:

Similarly, the availability of data, paired with the ability to harness data for decision-making by government, enables (1) better-informed policies, (2) more efficiency and efficacy of public service delivery, and (3) more inclusive and participatory government. A number of governments profiled in this report have prioritized creating a transparent and secure way for the government to share data in order to achieve these goals. For example:

1. In Chile, the integrated social information system (RIS)—which comprises the Social Registry of Households and the Intended Public Beneficiaries registry—contains data shared by 43 state agencies at all levels of government, covering nearly 75 percent of Chile's population. This intersectoral database determines eligibility for about 80 social protection programs and collects self-reported data, administrative data, and geographic data from different sources.
2. In Andhra Pradesh, a state in India with 50 million people, the government can access and analyze detailed statewide reporting data, in real time and across thousands of delivery points, to monitor the provision of rations to poor beneficiaries. They can detect transaction failures almost immediately and facilitate rapid follow-up and remediation.[17]

Trend #2: A growing convergence globally, including in middle- and low-income countries, around legal frameworks for personal data protection.

This trend has been driven both by efforts to align with GDPR for the purposes of trade and by increased pressure on policy makers by citizens who have started to demand more protections for their data and more transparency in light of high-profile data breaches and a growing awareness of data misuse. For example, countries like Mauritius (see annexed case study) have actively sought to update their data protection laws to attract foreign investment from

17 Gelb, Alan, Mukherjee, Anit and Navis, and Kyle Navis. "Citizens and States: How Can Digital ID and Payments Improve State Capacity and Effectiveness?" Center for Global Development, March 31, 2020.

businesses working with European countries, creating a legal regime that enables safe and secure data transfer. On increased awareness and demand by individuals for more protection, a recent CGAP study of the financial services sector found that consumers care about the privacy and protection of their data and are willing to pay more and wait longer for a loan product with strong data privacy and protection. In Nairobi, 64 percent of 220 customers surveyed chose a loan with a 10 percent fee and strong data privacy rather than a loan at half that rate. In Bangalore, results were similar: 66 percent of 197 customers chose the loan with strong privacy at a 10 percent rate versus one at 9 percent.[18]

Governments of many low- and middle-income countries are currently developing laws and policies to respond to these trends questions, defining both how data is protected and how data can be shared securely. UNCTAD's most recent data finds that 132 out of 194 member countries have some legislation in place to address privacy and data security.[19] Outside the EU, Asia and Africa are experiencing the most rapid change in data privacy laws, but significant developments continue in Latin America and the Caribbean as well.

The foundations of data protection are rooted in the deep history of individual rights and rule of law. As early as 1948, the Universal Declaration of Human Rights (UDHR) provided a right to protection of the law against arbitrary interference with one's privacy, family, home, or correspondence. Similar rights were codified in subsequent international instruments, including the International Covenant on Civil and Political Rights (ICCPR) in 1966 and the European Convention on Human Rights in 1950, as well as national constitutions and other legal instruments. Through such legal instruments, governments have afforded people certain rights to privacy, free personality development, personal identity, and physical security, among other guarantees, which form the underpinnings of modern data protection schemes.

Among the earliest attempts to apply these foundations to data stored in computer systems, or databases, was a legislative proposal by the U.S. Department of Health, Education and Welfare (HEW) in 1973, which resulted in the adoption of the Fair Information Practices Principles (FIPPS). In 1980, expanding on FIPPS, the Organisation for Economic Co-operation and Development (OECD) issued its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." These were the first internationally agreed upon data privacy principles. While not mandatory, the OECD guidelines outlined a set of eight principles to guide the protection against human rights abuses by member states, such as the abuse or unauthorized use of an individual's personal data. These principles are: (a) collection limitation; (b) data quality; (c) purpose specification; (d) use limitation; (e) security safeguards; (f) openness; (g) individual participation; and (h) accountability.

The first legally binding international instrument to address data protection followed shortly thereafter in 1981 with the Council of Europe's (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data or "Convention 108" as it's more commonly known. Convention 108 has wide reach as it is open for signature by any country, whether CoE member or not, and has influenced the development of data governance frameworks around the world including, most notably, Europe's most modern data protection law—the General Data Protection Regulation (GDPR) (EU) 2016/679, which was adopted in 2016 and entered into full force in 2018.

18 Fernandez Vidal, Maria and David Medine. 2019. "Is Data Privacy Good for Business?" Focus Note. Washington, DC.: CGAP, https://www.cgap.org/sites/default/files/publications/2019_12_Focus_Note_Is_Data_Privacy_Good_for_Business.pdf. Accessed April 2020.

19 United Nations Conference on Trade and Development. "Data Protection and Privacy Legislation Worldwide," https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. Accessed July 1, 2020.

Like its predecessor, the European Data Protection Directive 95/46/EC of 1995 (the "Directive"), the GDPR sets out principles for processing personal data, data subject rights, obligations of data controllers and processors, and outlines penalties for failures to comply, among other things. As such, it is known as a "comprehensive" data protection law.

While data protection has existed as long as data has ever been managed by organizations seeking to use it for gain, the introduction of GDPR has been an important accelerator of the rights-based legal approach to data protection, establishing various specific rights and obligations of different actors in a data transaction. Unlike its predecessor, the Directive, which required member compliance but was an indirect mechanism for implementation (as it required transposition into national law and resulted in variations across the various EU Member States), the GDPR as a regulation took direct effect across the EU and was designed to harmonizes data protection across all Member States to ensure even application of the law. This also facilitates the free flow of movement of data across European borders, a core objective of the GDPR.

The impact of GDPR has been significant and goes well beyond the geographic boundaries of the European Union. Through its extraterritorial scope, companies and entities around the world are required to comply with the GDPR's requirements in order to do business in Europe or engage with European data subjects. Governments around the world have looked to GDPR. The impact of GDPR has been significant and goes well beyond the geographic boundaries of the European Union. Through its extraterritorial scope, companies and entities around the world are required to comply with the GDPR's requirements in order to do business in Europe or engage with European data subjects. Governments around the world have looked to GDPR to inform their own rules around data protection and responsibilities of data processors. This broad influence has also inspired the CoE recently to modernize Convention 108 to align more closely with the GDPR (known as "108+"). Indeed today, the GDPR is often the benchmark against which other personal data governance models are compared.

Additionally, the convergence around a rights-based approach to data protection has motivated an increasing number of countries to seek an approach to data governance that directly empowers individuals and tackles persistent social and economic inequities. People have long been seen as beneficiaries of good data usage practices on the part of government and the private sector but, by enabling people with more direct control over the data they generate, the nascent efforts in these countries seek to (a) ensure data is used in accordance with the specific preferences of each person no matter how those preferences may change over time, and (b) more directly available to individuals to use in order to express preferences and access life-enhancing commercial and public services.

For people, and particularly for traditionally disadvantaged groups, the notion of having access to one's data—such as a credit score or land rights certificate or medical history—and the ability to share that data in a trusted environment can be profoundly empowering. In Rwanda, for instance, personal data histories such as transaction records and consumer behavior are now helping people demonstrate their creditworthiness and gain access to loans to start or grow businesses.

KEY FEATURES OF THE GDPR THAT SUPPORT TRUSTED DATA SHARING

A general exposition about the many features of the GDPR is beyond the scope of this Report. This Sidebar focuses on some of its key features that support "trust" in data sharing. The GDPR is one of the more recent expressions of these features - many of which are also found in other laws and approaches to data protection, as well as GDPR's predecessor instrument, the '95 Directive.

Amongst its many features, following are some key aspects of GDPR that serve as the pillars of trusted data sharing:

1. *Agency*. GDPR facilitates data sharing by giving individual data subjects rights and agency over their personal data. These rights limit the ability of third parties to collect, process, or sell personal data without consent of the data subject. A key aspect of this agency is the ability of data subjects to have to agree to "automatic processing" (referring to AI systems) of their data. Another is data portability, that facilitates and encourages the sharing of personal data across data controller organizations.

2. *Transparency*. Both the rights of data subjects and the obligations of data controllers and data processors create transparency in how individuals' data is used and processed, contributing to the overall trust ecosystem.

3. *Accountability*. Just as importantly, GDPR establishes mechanisms for redress in the event of interference with these rights. These rights include the right to information about data collected, its intended purpose(s) for processing, and other information; rights of access, rectification, the restriction of processing, and erasure, for example.

The GDPR provides broad exemptions for personal data that are "processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes." This enables a variety of data sharing and open data-style projects and research, particular public sector uses of data that might improve service delivery, urban planning, scientific or medical research, and a variety of other ends.

The countries profiled in the report provide further illustration of how a trusted data sharing ecosystem underpinned by effective data protection cannot only improve delivery of services to people as beneficiaries but also equip them with new capabilities that contribute to individual empowerment:

1. In India, easy access to trusted digital records such as school degrees and transcripts—paired with the ability to share that information in a verifiable and transparent way—enables people to prove their readiness for jobs. Not only does this offer the opportunity for employment among people who otherwise have few proof points of their skill level, it minimizes corruption through the issue of false certificates

2. In Uruguay, the commitment to Open Government, paired with civil society efforts to connect government data sets, resulted in the A Tu Servicio platform, that enabled citizens to make more informed decisions when selecting their health care providers. The program has introduced greater patient choice into Uruguay's health care sector, enabling citizens to navigate through a range of options and has helped improve the quality of data—e.g., errors were discovered by users, providers, and the Health Ministry itself—and helped to lower prices for consumers by creating more competition among providers.[20]

ADDRESSING THE RISKS OF DATA SHARING

As the examples above illustrate, the benefits of data compound when data is "unlocked" and shared beyond the original data holder. When insights from one data set are combined with another, the outcome can be transformational. Insights generated through data have been powerful drivers of growth and innovation. The diverse national responses to the COVID-19 pandemic have served to illuminate both the varied ways in which governments access citizen data and the systems in place to unlock it for public benefit. The early observations and interesting features and challenges emerging from these responses, especially in China, are examined more closely in the case study on health data sharing included as an annex to this report.

Yet, as compelling as it may be to broaden access to data, there are challenges and risks to data sharing. In addition to the broad concerns described early of misuse and consolidation of influence that can characterize the data economy, there are a number of other specific challenges which are, in many instances, more acute in low- and middle-income countries.

These face risk of security breaches due to the high costs of security relative to economic resources, inadequate administrative systems and lack of expertise to manage such risk. Furthermore, the uptake of the digital economy depends on achieving and sustaining widespread trust in and legitimacy of access to and use of personal data by governmental agencies and service providers. The relevance of such legitimacy was illustrated in recent court cases suspending aspects of important national data-driven

20 Sangokoya, David, Clare, Ali, Verhulst, Stefaan and Young, Andrew. "URUGUAY'S A TU SERVICIO: EMPOWERING CITIZENS TO MAKE DATA-DRIVEN DECISIONS ON HEALTH CARE." GovLab, January 2016.

development initiatives (in this case, national digital identification systems) in India,[21] Jamaica,[22] and Kenya[23] for want of effective data governance protections for privacy.

Weaker digital literacy and awareness of risk of treatment of personal data and weak consumer protections leave individuals potentially even more exposed to the asymmetry of knowledge and bargaining power when dealing with large organizations processing data. These asymmetries are exacerbated where accumulation of data gathered through direct sharing from individuals or through market intermediaries enables firms to build effective monopoly power and exclude rivals.

Competition concerns may also arise from increasing use of algorithms for business pricing and other strategies, including by facilitating the implementing, monitoring, and policing of cartels, or reducing competition through industrywide adoption of predictable reactions to changing market conditions.[24] Lack of deep expertise in such complex matters leaves low- and middle-income countries vulnerable to risk of exploitation by savvy companies.

Algorithms trained on data from past experience may also reflect and perpetuate the biases embedded in historical differences among ethnic, religious, or gender groups—differences that are very significant in many low- and middle-income countries. Thinner and less reliable data sets may result in poor training data for machine learning systems, resulting in less robust decision-making (whether automated or derived from data analytics), with inadequate systems for recourse for individuals.

Perhaps the most important consideration when evaluating data sharing strategies is the strength of safeguards in place to address such risks and challenges. Without safeguards, data sharing can exacerbate infringements on data protection and privacy rights which, at best, undermine public trust and, at worst, strengthen authoritarian regimes and exacerbate discrimination. The next section examines how a number of countries, as well as the health and financial sectors, are working to strengthen those safeguards while cultivating rich data sharing environments.

21 Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012, 1 (Sup. Ct. India Aug. 24, 2017).

22 Robinson v. Att'y Gen. of Jamaica [2019] JMFC Full 04 (Sup. Ct. Jamaica Apr. 12, 2019), available at https://supremecourt.gov.jm/content/robinson-julian-v-attorney-general-jamaica.

23 Nubian Rights et al. v. Attorney General of Kenya (High Ct. Kenya Apr. 1, 2019), available at http://kenyalaw.org/caselaw/cases/view/172447/.

24 Stucke, M.E. and Ezrahi, A. (2016) Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy, Harvard University Press.

INNOVATIVE MODELS FOR DATA MANAGEMENT AT-A-GLANCE

While the case studies included in this report focus on what governments are doing and can do to create an environment for data sharing, it is important to acknowledge that data sharing arrangements need not be designed and overseen by governments. In fact, widespread data sharing exists already through private agreements. Bilateral data sharing contracts are the dominant form of data sharing. This can be, for example, when an internet service company shared insights about user preferences for the purposes of targeted advertising.

Some arrangements have been criticized for the opaque nature of these private contracts, particularly where the data being shared through these contracts is collected and used in ways that data subjects might not have anticipated or wanted. Tracking the rights, consents, and restrictions applicable to data that has been collected and transferred through potentially several intermediaries is complex and often not done. Due diligence by organizations as the provenance of data they acquire may not be as diligent as it should be. The result is a data environment in which vast amounts of data are transferred without careful attention to the privacy of data subjects, and sometimes without necessary security.

New models are emerging that generate and share opportunity from data sharing while managing, mitigating, and allocating risk transparently with accountability. These are secured under a robust framework of legal rights and obligations (some by law, some negotiated by contract, some by standards given the force of contract) according to the various roles involved.

Data collaboratives are entities which govern the sharing of data between entities and, sometimes, individuals based on pre-established rules. Highly functioning data collaboratives will specify:

- Scope: purpose for the data collaborative to exist
- Data assets: types of data to be shared, standards for describing data
- Participants: rights and responsibilities of data requesters and data holders admitted into the data collaborative
- Risk management: security protocols, liability, jurisdiction in which the collaborative is operating
- Access: mechanisms for data to be shared, permissions, and usage rules
- Retention: where data is stored, how frequently it is updated, and duration of the agreement
- Individual rights: the extent to which individuals have control or transparency into how and when data is shared

With these characteristics in place, there are a number of forms that a data collaborative can take. New York University's GovLab has started an extensive catalogue of data collaboratives and has identified a few key models, including (1) data pooling, (2) research partnerships, and (3) trusted intermediaries.

One example of a research partnership data collaborative highlighted by the GovLab is 23andMe Patient-Centric Research Portal, which can be used for medical studies initiated by partner institutions,

like the Mount Sinai Asthma Health and Stanford Medicine's MyHeart Counts projects to access 23andMe research services using a new ResearchKit app, through which customers can choose to share data. Customers of 23andMe's services can also choose to participate in other surveys to aid medical research, and provide data to 23andMe's industry, academic, and nonprofit partners.

An example of a trusted intermediary model includes Beeline Crowd Sourced Bus Service, launched by Singapore's GovTech and the Land Transport Authority (LTA) with a number of private and nongovernmental organizations lending support, Beeline acts as a matching service between people using the Beeline app and the city's private bus services. Beeline collects consolidated bus transportation and user data collected via their app, which can then represent "community demand." In doing so Beeline crowdsources transportation insights directly from passengers using the service. These "user suggested routes" are created when there is enough demand for a particular route. Beeline attempts to close the gap between commuters' needs and the services offered by private bus companies by providing a feedback mechanism within the app. The service has also led to the creation of GrabShuttle in 2017, a fixed-route shuttle service that allows users to track the buses in real time.

And, finally, BBVA's "Measuring People's Economic Resilience To Natural Disasters" collaborative is an example of data pooling: In partnership with UN Global Pulse, BBVA's Data and Analytics team analyzed financial data prior to, during, and after Hurricane Odile hit Baja California Sur in 2014. Using anonymized data on sale payments and ATM cash withdrawals, the partners measured the resilience of communities following a natural disaster. The researchers found economic recovery time was 2 to 40 days depending on location. They also found income levels and gender differences play a role in recovery time.

Data trusts are a form of data collaborative with an inbuilt accountability mechanism based in Trust Law that imposes a fiduciary duty on a third party trustee legally responsible for implementing the purpose and policies under the agreed trust framework. Importantly, data holders placing data into a data trust no longer control the data. It is instead being held by the third-party that manages the access and usage of the data in service of the stated legal purpose and beneficiary. The beneficiary can be specific (an individual or a set of users, for example) or broad (the general public, for example). Beneficiaries have the legal right to challenge the third-party's performance and seek redress.

UK BioBank is an example of a data trust. It aims to improve the prevention, diagnosis, and treatment of a wide range of serious and life-threatening illnesses by following the health and well-being of 500,000 volunteer participants and provides health information, which does not identify them, to approved researchers in the UK and overseas from both academia and industry.

Personal data stores are a technical tool whereby individuals can store and permission access to personal data. Some personal data stores permission data to be used by developers to create new applications whereas other PDSs permission data for use by academics, brands, and nonprofits. Personal data stores compete on the basis of helping individuals understand their data assets and make use of them through new analysis or profit generation. Digi.me is an example of a personal data store that permissions data to be used by developers to build apps.

METHODOLOGY AND PURPOSE

The following section examines how different countries are approaching data governance in order to realize these benefits and mitigate the risks, drawing on seven country-specific experiences (India, Estonia, Singapore, Mauritius, Chile, Uruguay, and Mexico) as well as the experiences of governing open banking in the financial sector (drawing extensively from the experiences of the United Kingdom and Australia) and health data sharing (drawing from a range of government responses to the COVID-19 pandemic). In analyzing these experiences, the paper surfaces emerging practices and interesting features of trusted data sharing from across the world which are intended to inform other governments as they develop their own data governance posture.

The report has been developed through interviews with current and former government policy makers from the countries profiled in the case studies and draws upon a 2019 survey of more than 100 emerging market policy makers and their advisors conducted in collaboration with Oxford University's Pathways for Prosperity Commission. Additional inputs come from a wide range of World Bank staff and partners, as well as extensive secondary sources.

While the report benefits from significant inputs from each of these contributors, it is important to acknowledge that the case study methodology used to anchor the report does create certain parameters for the analysis, namely:

1. Normative approach to country selection: The countries profiled in the case studies for this report were selected based on a number of criteria that would offer diversity in geography, size, and primary motivations for investing in trusted data sharing. However, all of the countries had one thing in common: they acknowledge that data sharing and data protection need not be at odds, and they have each taken intentional steps to create a virtuous cycle between the two. Additionally, in an attempt to outline a more complete framework, the report intentionally sought to profile countries that have taken steps to support trusted data sharing that go beyond policies and regulations. Together these selection criteria necessarily ruled out certain countries and focused the report's attention on countries that are both taking a rights-based approach to data protection and investing in institutions, technical architecture, and capacity building to support trusted data sharing.

2. Iterative approach to learning about each country: The countries profiled each have their own priorities and own experiences in supporting a trusted data sharing ecosystem. This makes detailed direct comparisons more challenging (e.g., those governments that have prioritized data sharing as a means to improving government efficiency compared with supporting trade). However, the iterative approach to analyzing each country—through interviews with policy makers and secondary research—elicited the emerging practices and interesting features that policy makers in the respective countries identified as most important for trusted data sharing.

3. A focus on *"success"* stories: The practices and features examined in this report remain nascent in most countries and, as such, evidence of development impact remains scarce. The intent of this report is to frame the opportunities for governments to foster a trusted data sharing environment. With this in mind, the authors made the intentional decision to focus on illustrative "success" stories and used extensive consultations with World Bank staff, other global data experts, and numerous policy makers to identify countries that are widely perceived to be on a successful path towards a trusted data sharing environment. While the extensive consultative process provided a high degree of confidence in the successes of the countries profiled, it also highlighted two challenges of this methodology: (1) without strong counterfactual

examples (i.e., profiling countries that have struggled to create a trusted data environment or have succeeded by means other than the five pillars), the report cannot assert more definitively that each of the five pillars is required for success nor can it make conclusions about the relationships between the five pillars, and (2) the lack of an existing monitoring and evaluation (M&E) framework leaves the definition of "success" somewhat subjective, and makes tracking progress towards a trusted data sharing environment difficult for any country.

This report is meant to stand alone as a focused look at trusted data sharing and provide a resource for governments grappling with the associated strategic questions. It will also serve as an input into the World Bank's 2021 World Development Report, which will explore a wider range of data governance issues including, but not limited to, cybersecurity, tax policy, access to data infrastructure such as cloud services and internet exchange points, and the economic value of data.

INSIGHTS FROM CASE STUDIES

The case studies (annexed) examine instances in several countries and sectors in which the government has taken intentional steps to consider the relationship between data protection and data sharing—in some cases, it has been part of a broad vision for national digital transformation and in others as part of a response to global trade aspirations.

In the end, despite these varied reasons, each country profiled has taken an active role in promoting trusted data sharing. In all cases, policy makers have identified specific value propositions for data sharing and have taken bold actions toward creating enablers and safeguards in data sharing arrangements.

Examining the contours of a trusted data sharing ecosystem that begin to emerge from the country case studies helps to validate the initial assertion of this paper, that policies and laws, dedicated institutions, and secure technology architecture are interdependent and mutually reinforcing.

Ultimately, the experiences of the countries profiled point to a number of specific characteristics that, together, help maximize the value of data as a tool for development outcomes. These both expand who can derive value from data and help preserve individuals' rights even as data is shared more extensively. These characteristics can be organized around five main pillars:

1. *Laws and regulations that clearly define the rights and obligations over data, including the rights of people to determine when and how personal data is collected, shared, and used.* In the countries profiled in this report, this has been achieved both through a clear and enforceable rights-based approach to data protection policies and laws, as well as through an iterative and adaptive approach to data policy making in order to continuously calibrate and refine the relationship between sharing data and keeping it safe and secure.

2. *Robust and resourced institutions capable of enforcing the rules while also offering citizens responsive and effective redress.* In the countries profiled in this report, this has been achieved both by identifying strong coordinating bodies within government that can harmonize approaches to data protection and data sharing, as well as investing in a whole-of-government approach to implementing data governance, which can help reconcile instances where there are competing policy priorities across government agencies. Furthermore, governments have sought to take specific steps to engender trust in institutions and to establish appropriate capabilities within institutions including supervisory and oversight functions and clear redressal systems for individuals.

3. *Trusted technical architecture to standardize data sharing within government and regulated institutions while giving individuals more control and transparency into data flows that use their data*. In the countries profiled in this report, this has been achieved by investments in technology platforms that break down data silos and facilitate the exchange of data in ways that create accountability (e.g., Singapore's digital watermarks for tracing the originator of documents) and transparency (e.g., Estonia's State portal that gives individuals granular insights into who is sharing their data and for what purposes). Like data policy making, creating trusted technical architecture requires an iterative and adaptive approach to expand capabilities for the user and to strengthen data protection.

4. *Capabilities inside and alongside government to analyze and make use of data.* In the countries profiled in this report, this has been achieved through investments in reorganizing and strengthening the human resources of government agencies in order to harmonize approaches to data governance and to ensure the proper capabilities to establish and implement effective data governance strategies. Such efforts have included, in some instances, programs to cross-train policy makers

and technologists and, in other instances, effort to embed technical expertise across traditional government ministries. This has also been achieved through strategic collaboration between governments and private firms or civil society (e.g., Uruguay's A Tu Servicio initiative) to share data in ways that are both secure and more broadly accessible.

5. *Active and participatory civil society and informed populace who can keep governments and companies accountable*. In the countries profiled in the report, this has been achieved both through well-resourced and sustained national programs to provide digital literacy training and through multi stakeholder processes to develop open data policies and other strategic planning related to data protection and data sharing.

Through the intentional steps each of the countries profiled has taken to unify the goals and the implementation of data protection and data sharing, they have emerged as regional and global leaders in the use of data for development, and have collectively helped to illuminate the enablers and safeguards necessary for trusted data sharing.

The descriptions in the following section are not intended to provide a comprehensive review of all aspects of each country's data protection and data sharing approaches. Rather, they are meant to emphasize areas of each country's approach that may be illustrative to other countries grappling with how to create the enablers and safeguards necessary for creating the five pillars for trusted data sharing.

ENABLERS AND SAFEGUARDS FOR TRUSTED DATA SHARING

Pillar 1: Policy and regulatory environment that defines *and* enacts rights over data

1.1 Laws and regulations

Laws and regulations are the foundations of data rights and, within that, how data can be shared. Among the countries evaluated, there is a convergence around legal attributes fostering trust in data sharing, namely:

- Laws related to data protection are supported by fundamental rights enshrined in a national constitution or similarly high-level legal instrument, which provides a stronger basis for defending and asserting them, including in face of changes in leadership or political climates.
- Laws related to data protection have limited exceptions and avoid broad carve outs for categories of data, certain uses of data, and certain actors (such as the public sector).
- The laws are based on a clear set of core data protection principles such as transparency, fairness, data minimization, purpose limitation, storage limitation, and accountability, among others.
- The laws clearly articulate a broad array of individual rights in respect of personal data, as well as clear mechanisms for exercising those rights.
- The laws clearly articulate the obligations of entities who collect, store, and otherwise process personal data, as well as rules for how those entities engage third parties in furtherance of those processing activities.
- The laws establish clear accountability mechanisms for entities who collect, store, or otherwise process personal data.

- There are clear enforcement mechanisms to protect and defend individual rights, including penalties sufficient to deter noncompliance by entities who collect, store, or otherwise process personal data.
- There is a readily identifiable entity in charge of supervision and enforcement, with convenient modes of accessibility to the public.
- There are clear rules for cross-border transfers of personal data, including a supervisory mechanism for those transfers and local redress in the event of breaches or abuses of data transferred.
- Laws related to data sharing, including open data rules, focus on enhanced transparency with respect to the flows of data, authorization and access mechanisms, and accountability.
- Laws related to data sharing, including open data rules, aim to realize the benefits of data sharing while also protecting individual rights.
- Laws that enable access and use of data, including open data policies or laws, access to information legislation, and mechanisms to support the interoperability of information systems, and datasets to enable portability and reuse of data. Mechanisms can include clear data classification policies, unified standards for data taxonomies and machine-readable formats, establishing access through bulk download and APIs, and ensuring that the appropriate licenses are in place to support reuse of data (e.g., Creative Common licenses or OdBL).
- In cases where emergency legislation is passed to enable data collection, processing, and use of data in exceptional circumstances (e.g. the COVID-19 pandemic), it is essential that these laws be subject to robust procedural safeguards to limit their scope and ensure they are not misused. These include ensuring proving that these laws are lawful, necessary, and proportionate to meet government's intended objectives to justify their adoption. They must also include strict sunset clauses and renewal requirements, as well as provide for independent judicial review and redress, to reassess efficacy, necessity and safety over time.

1.2 Coordinated and iterative policy environment

Several of the countries instituted a whole-of-government approach to ensure the legislative requirements are effectively implemented. Such a whole-of-government approach is essential given the cross-cutting nature of data and the myriad interests and issues involved. ICT ministries and telecommunications regulators play a formative role in setting a country's telecommunications agenda, but the relevance of data is far more expansive, involving every sector of a country's economy and, as a result, involving departments across government.

Additionally, the fast-moving nature of technological advancement makes iteration in digital policy making essential. While many countries commonly have in place three- or five-year national digital strategies, a trusted data ecosystem requires additional iteration in policy making and support for more agile institutions. This is, in part, because many models for trusted data sharing are only just now emerging and there are opportunities for regular learning and continuous improvements, but also because the relationship between data sharing and data protection is not a specific end-state but rather a dynamic relationship that requires regular recalibration. Countries profiled in this report have looked to iterate in different ways—some through regulatory sandboxes, others through processes for continual technological improvements, and others through flexible institutions.

The following examples offer ways in which five countries have approached iterative whole-of-government data governance:

1. *Uruguay:* By recognizing the challenges of coordination and by aiming to reduce institutional fragmentation, the Uruguayan government has expanded the mandate of Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC) to better coordinate implementation of data protection, access to information, cybersecurity,

and open government initiatives across national government agencies, as well as with local government. These provide clear and consistent processes and help harmonize goals. In its initial phases, AGESIC's biggest challenge was interagency coordination. Originally, it was set up to create the necessary infrastructure for digital transformation and considered a producer of technical knowledge and policy but did not have a mandate to drive implementation of e-government initiatives, relying instead on other ministries and agencies to implement e-governance programs. Many of these other government agencies were wary of the costs of introducing new technologies, were sensitive to the new processes entailed, and had limited human capacity to execute new initiatives. In addition, a lack of interoperable databases and platforms made it difficult for the ministries and agencies to collaborate and develop standardized e-government services. In July 2015, the government issued a decree which required "putting central government procedures and services, and those of other public entities, online." The decree entrusted AGESIC in the "directing, organizing, structuring, executing, and monitoring the initiative," thereby empowering it to issue relevant technical standards and regulations.

2. *Mexico:* A National Digital Strategy Office was created under the Office of the President to coordinate the Digital Strategy, which addresses five key elements necessary for the country to maximize the development potential of data: infrastructure, digital skills, interoperability of government data, the legal and regulatory environment, and open data.

3. *Chile:* Chile's social information system was housed under the Ministry of Planning, which has since then become the Ministry of Social Development and Family. This provides key benefits. In particular, the institution housing the integrated registry has the capacity to coordinate and sign data use agreements across sectors and in the central and subnational governments. While the registry is centralized and operates as a virtual social registry, tasks such as data collection are completed by local municipalities.

4. *Singapore:* The creation of the Smart Nation and Digital Government Group (SNDGG)—which is well-resourced and has a strong mandate—has helped ease intragovernmental data sharing by allowing a strong government coordinating body to focus on developing shared digital infrastructure (e.g., data transfer platforms), enforcing common standards (e.g., for data security), and ensuring interoperability of applications. Specific government agencies remain domain experts in front-line data collection and in management and use of specific databases. Furthermore, Singapore's experience across the Smart Nation implementation, open banking initiatives, and both Public and Private Sector Data Security efforts, policy changes must be complemented with the appropriate organizational structures and technical infrastructure to achieve the changes that the government hoped to see.

5. *United Kingdom (Experiences from Open Banking):* In the United Kingdom, a single standard setting body provided regulatory certainty for open banking and helped drive private sector investment and adoption in comparison to the roll out of PSD2 in the rest of Europe.

Pillar 2: Robust and resourced institutions capable of enforcing the rules while also offering citizens responsive and effective redress

There are a number of institutional functions that need to be established in order to ensure trust in data sharing processes including government units with clear mandates and aligned incentives, appropriate capabilities, supervisory and oversight functions, and clear redressal system for individuals. Building

government capacity in these areas requires investment in people and institutions. The following provide two examples of countries that have invested in the necessary institutional capabilities to support trusted data sharing:

1. *Estonia:* The citizen portal enables transparency into data access and data use including time and date stamping of data access, who is requesting the data and why. Additionally, Estonia has a long history of specific steps to building trusted institutions. The leaders of Estonia's digital transformation prioritized building trust in new forms of communication between government and citizens. For example, the government's decision to use e-mail communications—which was emerging as a legitimate means of communications at the time—as a key building block of a trusted digital society—helped to "slowly take down the institutional barriers impeding communications to be as easy and relaxed as possible. As a result, 'people trust digital interactions because we intentionally built digital nonformal forms of communication which people are used to employing, and that is something which contributes to making the social components of trust."

2. *Chile:* Given that the RIS registry is centralized but data collection is carried out locally and in a distributed manner, intensive coordination among all relevant stakeholders is necessary to seek their buy-in, and formalizing relationships between them within the government has become essential for successful implementation. The mechanism that the Ministry of Social Development and Family currently utilizes to formalize these relationships is one of interinstitutional data sharing arrangements. These agreements, signed between public sector agencies and the ministry, determine the nature of data shared as well as protocols around when the data is updated within the registry. This enshrines protection for individuals' data as well—in negotiating interinstitutional agreements, agencies delineate sensitive noncritical data from other data that can be shared with ease, enabling better public service delivery while protecting rights.

Pillar 3: Technical architecture to standardize data sharing within government while giving people more controls and transparency into data flows

The underlying hardware and software are critically important to ensuring data flows in accordance with the law. In addition to establishing the policy environment and institutional capabilities in place to maximize the value of data, tools, and protocols that make the exchange of data and the user experience intuitive and safe are key. As the case studies reveal in further detail, these types of technology investments range from interoperable databases that are accessible to and used across government agencies for sharing data, e-services portals that allows citizens to access government services, and individual data portals that allow people to aggregate, store, and share data, and inclusive digital platforms such as digital identification that ensure all people are participants in the digital economy, but if designed with key elements in mind, can enable data sharing and data security.

The following provide four examples of countries that have invested in technology platforms to enable trusted data in various ways:

1. *India:* DigiLocker is a platform for the issuance and verification of electronic documents, thus eliminating the use of physical documents. A public version of services like DropBox, DigiLocker account users get a dedicated cloud storage space linked to their Aadhaar ID number. The Digital Locker Technology Framework establishes standards and tools for users to gain access to and manage their data. This platform, paired with the technology layers of Data Empowerment and Protection Architecture (DEPA),

allows individuals to have more control of their data and share it in a more transparent and trusted way.

2. *Estonia:* Data access permissions are included in X-Road, the country's data exchange layer, to effectively automate compliance with data sharing policies. Furthermore, the transparency by design features of X-Road enable citizens to understand when and why their data is being accessed, creating a key data protection safeguard by not only providing individuals' insights into the movement and use of their data, as well as mechanisms for recourse in the case of errors or misuse.
3. *Singapore:* Singapore's Vault.Gov.SG provides a platform for civil service officers to explore a catalogue of widely-used government data sets and download sample data sets to understand the data better. Once a civil service officer has found the necessary data, they can submit a request to the appropriate authority for review. Review of the request takes no more than seven working days and if approved, data is digitally watermarked and encrypted with project and officer IDs before dissemination, deterring leaks and providing clear traceability. The civil service officer can then upload the data into Singapore Government's central analytics platform, Analytics.gov, which has commonly used analytics tools, and incorporates all the requisite data security controls and measures. Analytics.gov also allows data scientists to share code with other public sector data users to accelerate the deployment of data and AI models.
4. *Mexico:* InteroperaMX, modeled after Estonian's X-Road, allows public institutions to share reliable and trustworthy data, with clear identification of the source and certification of the information. As in Estonia, InteroperaMX supports efficient delivery of public services, including through a once-only policy whereby citizens only have to provide personal data to a single, appropriate government agency and then that data is shared through a set of defined permissions.

Pillar 4: Capabilities inside and alongside government to analyze and make use of data

Data can only be utilized within government for smarter, agile policy making when there are the systems and human capacity to analyze data and, importantly, respond to data insights. This requires new incentives to attract new talent and upskill existing workforces in data analysis skills and disruptive technologies, and a significant change management effort to create an atmosphere of data-informed operations. Singapore and Mauritius respectively offer examples of governments to have made intentional efforts to build these capabilities.

1. *Singapore:* To draw more interest and provide a more compelling offering to highly-sought after data talent, compensation packages were revamped to ensure market competitiveness with the global tech sector. The government actively marketed Singapore as a hub for international talent and made a variety of overtures to try to repatriate Singaporeans working in data overseas. To better retain those talents, HR policies have been restructured which included the creation of specialist career pathways that recognized highly skilled individual contributors and enabling data and digital tech specialists to gain exposure and broaden their experience through job rotations across government. Programs have also been set up to facilitate employee exchanges with the private sector providing for industry professionals to share their experience with government teams and government employees to gain experience in private companies. Additionally, to best utilize this rebuilt bench of data skills, a variety of efforts have been made to better integrate traditional policy and operations knowledge and skill sets with the technical skills these new talents offer.
2. *Mauritius:* Following best practice guidance for successful open data implementation, the National Open Data Policy created a Central Open Data

Team (CODT), which reports to the Chief Technical Officer of the Ministry of Technology, Communication, and Innovation (MoTCI). The CODT is responsible for steering Open Data work across government ministries and departments, including establishing and reviewing standards for Open Data and setting up and administering the National Open Data Portal. The CODT is also responsible for setting the standards for Privacy Compliance Assessments to be carried out at the level of Ministries and Departments prior to the release of data sets as Open Data. Importantly, in addition to the centralized team, each ministry was compelled by the National Open Data Policy to create an Open Data team to support the CODT. These ministry-level teams are expected to have at a minimum a permanent secretary, a program manager, a systems analyst, and a statistician—a team drawn from different government agencies and embedded into each ministry. The creation of the ministry-level teams builds upon existing practice within the Government of Mauritius to have embedded statisticians from the National Statistics Office in each ministry.

Pillar 5: Active and participatory civil society and informed populace who can effectively use data and keep governments and companies accountable

5.1 Investing in the digital literacy of people to enable active and informed participation

Even in a policy environment with strong protections for individuals' data, people must also have the requisite skills and awareness to actively and responsibly engage in the data ecosystem. A number of countries profiled in the report have invested in sustained efforts to have an informed population, ranging from how to access and use digital technologies, to ways to stay safe online, and behave in ethical and effective ways on digital platforms. These efforts enable individuals to both understand their ability to access and share their data, as well as protect themselves against misuses. Estonia, Singapore, and Uruguay are other examples of specific digital literacy investments that have helped underpin a trusted data sharing environment:

1. *Estonia:* In 1996, the government launched the "Tiger Leap" initiative, which continued massive investments in internet connectivity and introduced computer skills in all secondary schools starting at the age of seven to ensure future generations would be digitally literate. Another initiative, Look@World, done in partnership with banks and telecoms provided computer training to 10 percent of the adult population who represented the least digitally literate segments of society, including blue-collar workers and retired individuals. Programs in digital literacy continue even today with efforts like Targalt Internetis which promotes internet safety and awareness of data rights. In looking to Estonia as a model, it is critical to acknowledge both the specific and sustained efforts to build trust in public institutions and the institutional investments that were made to build a highly digitally literate populous.

2. *Singapore:* The country introduced its Digital Readiness Blueprint to ensure all Singaporeans can access technology to enhance their lives. The government established a digital readiness working group, with participants from the public, private, and civil society, tasked with ensuring access to inclusive digital infrastructure, building digital literacy, and driving participation in digital communities and usage of technology. The blueprint outlines recommendations around improving cyber security and data awareness skills, providing access to basic digital enablers, and driving interaction with data-driven technologies which are key to maximizing the benefits and containing the risks of data.

3. *Uruguay:* Uruguay has not only prioritized digital skills acquisition as a foundational element of

an inclusive digital government but has been a leader in normalizing the concept of the digital citizen—i.e., a set of skills that enables citizens to access, retrieve, understand, evaluate and use, to create as well as to share information and media in all formats, using several tools, in a critical, ethical, and effective way to participate and engage in personal, professional, and social activities.

5.2 Equipping individuals with means for protecting and controlling their data

The rights-based approach introduced above confers on individuals specific and extensive rights related to personal data. The following is not intended to catalogue again each of these rights in detail, but rather highlight emerging practices and interesting features identified through the case studies that enable individuals to avail themselves of those rights. These examples highlight that enablers of trusted data sharing must go beyond the legal framework. In particular, two areas related to rights and capabilities emerged through the case studies: redressal mechanisms and models for consent.

The ability for consumers to seek redressal when their data rights have been violated is essential to maintaining trust in an ecosystem of data sharing. Consumers should have access to independent redressal mechanisms that allow them to correct problems quickly and efficiently. Similarly, most individual consent frameworks are generally a one-size-fits-all model, i.e., as a consumer you have little to no ability to exert preferences. However, new policies, institutional practices and technologies are emerging that have the potential to change this paradigm—creating the possibility of more tailored consent frameworks where consumers can determine the scope, time limit, and revocability of consent to use their personal data. Examples of these new types of individual controls and capabilities over personal data include:

1. *India:* India has introduced new, regulated entities that have a responsibility to help translate individual consent preferences into how their data is shared and processed. With the creation of this new class of regulated entities, called "account aggregators" in the financial sector where the model is first being rolled out, Reserve Bank of India is spearheading a new means of establishing trust in the data economy by separating consent collection from data processing. While many countries have established DPAs to serve as grievance and redressal mechanisms, India is unique in having created a new class of licensed institutions with the competitive incentive to serve and inform individuals. These entities ensure people can make informed decisions about data sharing and, because the regulated entities do not have access to the underlying data, they compete on the basis of developing customer-facing trusted services.

2. *Mauritius:* Institutional innovations like the DPA of Mauritius are intended to create efficient methods for complaints by individuals of data misuse and redressal of misuse. Importantly, the DPA has strengthened consumer trust, by improving the level of data protection of relevant products and services, while also enhancing data subjects' rights, thereby providing individuals greater control over their personal data.

5.3 Civil society engagement

To strengthen trust in a data sharing environment, individuals' interests must be represented by a robust civil society that can advocate on behalf of the interests of people and societies, hold governments accountable, and safeguard against government overreach—particularly in light of the common carve-outs in laws for government access and use of personal data. In the last four years, for instance, the Government of Jordan has led notable efforts to implement reforms to promote the use of Open Government Data (OGD).

This process has gone beyond the technical and legal aspects of reform by publicly consulting with civil society, academia, and civil servants throughout the public sector. This approach in opening public sector data sparked a wider national discussion around open data and introduced newly-proposed reforms on government's data classification and the right to access information, while opening the door for the exploration of new data-driven local technological innovation and economic growth. These efforts at instilling good governance norms and practices into the policy process have been one of the drivers of change for a broader reform of Jordan's public administration. Public entities that were typically perceived as cautious of releasing data have since embraced a more open approach to publishing open data sets. Capacity-building activities piloted by the Minister of Digital Economy and Entrepreneurship (MoDEE) have contributed to standardizing data classification schemes within the public sector and have resulted in 35 public entities releasing over 200 datasets in the second half of 2019. These figures are expected to increase significantly as these change management and capacity building efforts are institutionalized, and a further 70 entities are expected to participate this year.

The following highlight four examples of civil society engagement that has prompted government action or held government accountable in the cases profiled in this report:

1. *Australia (Experiences from Open Banking):* The legislation and implementation of the Consumer Data Right has been notably supported heavily by consultation with the general public and specifically with relevant private sector firms. The most important precedents to the CDR, the Productivity Commission Report on Data Availability and Use and the Treasury Review into open banking in Australia, were both the result of open consultations and open comment periods. The Consumer Data Right legislation underwent two rounds of consultation and two rounds of open Privacy Impact Assessments while the Australian Competition and Consumer Commission (ACCC) rules frameworks and accreditation processes for the Consumer Data Right have gone through public drafting and consultation processes.

2. *Uruguay:* Each iteration of the Digital Agenda for Uruguay (ADU) has been a product of a multistakeholder process with representatives from government, academia, the private sector, and civil society organizations. Importantly, the implementation and monitoring of the ADU is carried out by the National Council for the Information Society which includes representatives from all sectors. This approach has led to high degrees of public trust. The current 2016–2020 ADU continues to emphasize the importance of the trust ecosystem in order "to promote full participation in the information society," including an effort to expand the use of secure digital identity mechanisms for authentication purposes.

3. *Mexico:* Mexico views their open data systems as strategic infrastructure for the country's development. The infrastructure (open data portal, datasets, etc.) was built based on a citizen consultation through the one-stop government portal, Gob.mx/participa. In this consultation, more than two thousand participants from civil society, private sector, and citizens participated to prioritize and propose the data they considered central to public concerns and helpful in identifying solutions to the country's development challenges.

4. *Health Data Sharing (Experiences from COVID-19 Response):* As the COVID-19 pandemic has highlighted, data protections are relaxed in times of crisis which can amplify both how governing bodies intend to govern data and the extent to which civil society has the ability to meaningfully engage on these complex issues.

THE CHALLENGES OF IMPLEMENTATION

Governments are increasingly aware that the policies and practices for data protection and data sharing must be complementary. In Singapore, for instance, government officials acknowledged in consultations for this report that the increased focus on data protection and improved data security in recent years did not constrain the data sharing environment, but rather supported increased integration and sharing of data for better delivery of public services. Several data incidents uncovered in recent years highlighted the need to review the government's information security policies and practices, and strengthen the data security regime against current and future threats. To do so, the Prime Minister convened the Public Sector Data Security Review Committee (PSDSRC) to conduct a comprehensive review and inspection of ICT systems and make recommendations to address existing gaps, and build a strong data security regime that enables trusted flows of data by protecting data and detecting and responding to incidents.[25] Similarly, in Uruguay, the decision to consolidate within AGESIC the authorities for data protection, public sector data interoperability, and open government is recognized as a key part of the country's successful digital transformation. In both instances, the connection between these two led to increased confidence in the ability to share data securely.

It is important to note that in documenting the experiences of each country and sector profiled above, this paper emphasizes promising approaches to both enablers and safeguards for sharing data. Many countries are seeking to align with the growing convergence around a rights-based approach to data protection, driven by both commercial and geopolitical forces. Each country profiled continues to evolve and address challenges in its approaches to data sharing. As such, this paper intentionally focuses on those promising features—not out of ignorance of the persistent challenges with which every country still grapples (e.g., government override of rights in the name of national interest), but rather in the hope that these promising features might serve as an example to other countries.

It is also important to note that the starting point for every country varies significantly—some, like Estonia, have designed their approach to trusted data sharing in a near-greenfield environment, while others have had to revisit and amend existing policies to align with national development strategies or in the face of data breaches. Further, it is important to emphasize that the pace and sequence of change for each country differs. While the alignment of laws, institutions, architecture, and human capacity is desirable, the case studies suggest that it may not always be possible to expect alignment of these factors simultaneously. The legislative process often lags behind technological developments and political priorities. Additionally, given the concentration of power in the data economy mentioned early in this report, methodical multistakeholder consultations that include active engagement from civil society and represent the interests of people are critical in this process.

Furthermore, while this report intentionally chose to profile countries that that have rejected the notion that data sharing and data protection are necessarily in tension with one another and, in doing so, is able to identify the contours of a trusted data sharing environment, the framework proposed above is only a starting point. Implementing each of the five pillars is challenging on a number of levels—not least of which are the complexities of power dynamics, vested interests, varied risk appetite within bureaucracy, and

25 Dolan, Jonathan. Notes from meeting with Singapore's GovTech team, January 9, 2020.

mismatched incentives for different stakeholders. While the report does not attempt to tackle these issues of political economy directly, it is important to acknowledge they play a formative role in how data is shared and with whom—just as they would for distribution of any asset.

For all of these reasons, it is impossible to prescribe the particulars of a top-down trusted data sharing strategy. In the end, however, the countries assessed for this report—despite having markedly different data governance journeys—reveal the need for two things to help drive implementation and overcome these challenges:

1. Sustained, high-level political will: In Uruguay, many initiatives that have emerged from the national digital plan are intentionally designed as joint efforts between AGESIC, the country's centralized authority for the information society, and other government agencies and line ministries. AGESIC is under the Office of the President, and even as administrations have changed, presidents have reiterated their support for AGESIC and have defended the importance of data as a tool for serving the country's citizens. Chile's MINSEGPRES is yet another case in point, serving as a line ministry that coordinates the digital agenda between legislative and administrative arms of the government.
2. Links to specific use cases: Like other cross-sectoral development efforts, trusted data sharing solutions not only require political leadership but also specific use cases to mobilize stakeholders. In introducing its Consumer Data Right (CDR), the Australian government acknowledged this point, outlining key use cases for the data that would be made more widely accessible in the scheme and outlined its vision for the customer journey. Interestingly, initial use cases appear to have important implications for how and whether individuals participate in data sharing. Open Banking Standards, for instance, are facilitating data sharing in the financial sectors with the goal of stimulating competition and enhancing money laundering controls. In countries with Open Banking, FinTechs and challenger banks, for example, can more easily gain access to transaction histories in order to compete on loan products.

CONCLUSION

As low- and middle-income countries experience unprecedented growth in data, governments are grappling with how to leverage data for development. In particular, three main development motivations are emerging:

1. Driving economic growth through trade and private sector and entrepreneurial activity

2. Creating more efficient, accountable, and transparent government

3. Empowering people

However, in the absence of an intentional approach to maximizing the value of data, the competing policy priorities of different government agencies can make it difficult to harmonize data protection in a manner that enables the sharing of data to expand its value. Furthermore, the extent to which governments prioritize these distinct opportunities within their national development strategies has important implications for how data governance policies and laws, institutions, and technical architecture are designed and implemented. For instance, among the country case studies highlighted, data interoperability platforms are a common investment in more efficient government but, depending on a country's emphasis on transparency or individual empowerment, may or may not be paired with a portal where citizens can follow how and why their personal data is being accessed and shared.

Similarly, even as many governments converge around a rights-based approach to governing personal data, the steps countries are taking to ensure citizens are actively engaged in and understand how their data is generating value varies. In some instances, governments have focused with aligning with international norms for data protection in order to catalyze trade, while others have taken a more proactive approach to equipping individuals with new rights and capabilities: India's DEPA enables citizens to create consent profiles for how their data is used, Estonia's State portal allows citizens to manage how their data is shared at a granular level (e.g., which doctors can request which aspects of their health data), and Uruguay has invested heavily in creating digital citizens who have "skills that enables (them) to access, retrieve, understand, evaluate and use, to create as well as to share in a critical, ethical, and effective way."

Despite the markedly different motivations and relative prioritization of development objectives, the experiences of the countries profiled in this report make it clear that data sharing is a lynchpin for extending the value of data beyond big tech firms—whether the goal is to enable individuals to exercise more control and derive more benefit from their data, or to enable entrepreneurs to leverage data to innovate or to break down government data silos to provide more efficient and effective government services. However, regardless of which of these goals most motivates data sharing, the case studies suggest that data sharing policies, laws, and mechanisms can be designed and implemented in ways that do not jeopardize individual rights or erode social norms through data breaches, targeted disinformation campaigns, and other abuses.

In other words, data protection and data sharing can be complementary—instead of competing—elements in a country's approach to governing data, thereby supporting a trusted ecosystem in which data is shared more extensively, specifically because it can be done securely and in ways that provide clear protections for individuals. Fortunately, through the deliberate actions of an increasing number of governments, the contours of this complementary approach are starting to emerge.

AREAS FOR FURTHER RESEARCH AND LEARNING

Although there is an emerging picture of what governments can do to foster a trusted data sharing environment, most countries globally—including many of those profiled in this report—are in the early stages of their data governance journey and must continue to adapt to a rapidly evolving landscape. Countries are grappling not only with technological advances but also with changes in consumer behavior and consumer expectations with respect to how their data is shared and who derives value from it.

Given this evolving context, a number of areas will require ongoing research and testing before the impact of current efforts are fully understood and before specific best practices for trusted data sharing can be asserted with greater certainty. Among others, the most notable areas include:

1. *Creating metrics for tracking progress towards a trusted data sharing environment:* As described in the methodology section, the lack of clear metrics for assessing investments in the five pillars is a key limitation in defining success and evaluating progress towards a trusted data sharing environment. Creating such a monitoring and evaluation framework will deepen the understanding of the relationship between the five pillars, help identify if there are gaps in the framework proposed in this report, and further illuminate for governments the path to maximizing the value of data for their development objectives while also cultivating trust in the data ecosystem.

2. *How models for consent evolve or are replaced by other data protection mechanisms:* As described above, India's emerging efforts to decouple consent collection from the data request represent an important innovation in protecting personal data and equipping individuals with greater agency over their data, and other countries are starting to recognize the need for a person or institution charged with safeguarding the interests of people in their interactions with technology platforms. This could result in other "fiduciary" models or the creation of learned intermediaries tasked with representing or advising consumers. In addition to government efforts, there are a number of private sector-led initiatives, including Inrupt, Digi.me, and The Data Transfer Project that are seeking to reimagine how consumers consent to share their personal data—even in environments where national standards for data sharing are not yet in place. As governments and companies experiment with different models and as these efforts mature, there will be important opportunities to learn about the challenges and opportunities of different approaches and better understand how each align with national development objectives.

3. *How costs and benefits of data governance should be weighed:* Some of the policy dilemmas in designing a data protection framework revolve around the opportunity costs of introducing stronger data protection measures. While many data protection measures are intended to equip the individual, some involve greater costs than others. The costs to a given organization (public, private, or civil society) of accommodating timely data subject access requests and data portability, for instance, might be weighed against the intended benefits of correcting the quality of data held or improved citizen/consumer choice. When is transparency enough to impose a quality discipline, as opposed to a more onerous portability requirement? Do the lessons differ between situations where the key purpose of sharing is to equip individual consumers to make market choices (e.g., competition in financial services) and situations where the sharing is intended to enable generation of insights for policy decisions by governments? Such questions may

be driven by market policy considerations, such as lowering barriers to switching providers, but these are typically very context specific both in terms of the time and manner of their introduction and the effort and cost to be effective (one of the UK and Australian lessons has been that open banking is very specific to the type of data and APIs that are involved). Further research would be helpful to understand the costs of remedies and assess when the anticipated benefits of sharing would justify the remedies introduced.

4. *How the principles and practices that are starting to emerge apply to rapidly emerging technologies:* As a number of the cases studies in this report demonstrate, data sharing when designed and implemented well can give transparency into who accesses data and why, thereby reinforcing data protection and increasing trust. However, as the current response to the COVID-19 pandemic has highlighted, there is another layer of transparency needed in terms of how algorithms and machine learning technologies use data to affect decision-making. How can policies adequately ensure the opportunities of this data can serve public and private players? How can governments handle a future in which personal and nonpersonal data are increasingly mixed? How can governments put in place responsibilities over algorithmic decisions?

5. *The medium- to long-term impact of data sharing requirements on business:* While there has been a convergence around a rights-based approach to data, driven in part by the enactment of GDPR, it remains too early to project its full impact on business. This area of investigation will have to consider the incentives of the private sector to collect and share data. What data sharing is beneficial and what is not? When to require and when to prohibit data sharing? What means of data sharing are most effective, for instance requiring interoperability, data portability, or full access to datasets? On what basis should obligations apply, for instance, applicable to all organizations collecting and processing data or only certain ones for the purpose of achieving particular economic and social goals, or for the purpose of enabling greater competition?

6. *How consumer demand will evolve in response to the data sharing models that are emerging today:* GDPR has helped catalyze some convergence around a rights-based approach to data governance. A number of the countries profiled in the report are experimenting with models for equipping citizens with new rights and capabilities to manage their own data. At this time, the extent to which individuals will want to manage their personal data and the capabilities they will need to do so in an informed and responsible way are still not yet fully understood. The extent to which individuals will want direct control over their data versus simply wanting more transparency in how their data is being used will remain an important area for investigation as data sharing models expand and evolve. Answering these questions will require not only understanding individuals' preferences and capabilities but also understanding how different data sharing models create new forms of risks.

7. *The nature of trust in data protection:* The CGAP study (mentioned in the report) that found Kenyans and Bangladeshis ready to face inconvenience or pay more for stronger data protection argues that data protection is good business. Further research would be helpful to understand better what it is that data subjects are valuing when they are offered a system geared towards greater trust. How much are they concerned about data security and personal financial risk (e.g., of the individual facing fraud from identity theft or lower credit reference rating) as opposed to privacy concerns (e.g., about autonomy and liberty)? The answers to these questions may be culturally contingent, but if so, it would be useful to policy makers to understand this as it can help them choose where to put their attention and the regulatory burden.

ANNEX: CASE STUDIES

INDIA: DATA SHARING TO EMPOWER INDIVIDUALS

BACKGROUND

The Republic of India is the world's most populous democracy, covering most of Asia's southwestern landmass. With more than 1.3 billion people across 28 states and eight territories, India's scale and diversity rival those of continents rather than most other countries. While the constitution recognizes 22 official languages, in fact nearly 20,000 languages and dialects are used throughout India. The people of India are socially and culturally varied, and contend with significant inequality. Despite impressive gains in economic growth in recent years, some 114 million Indians still live in severe poverty,[26] and less than four percent of the population had income high enough to be subject to tax in 2019.[27]

Despite these complexities, digital uptake has accelerated rapidly in recent years. India is a large and fast-growing digital market, with over 1.2 billion mobile phone connections and 560 million internet subscribers in 2018, second only to China. Competitive offerings by telecommunications firms have turbocharged internet subscriptions and data consumption, which quadrupled in both 2017 and 2018 and is helping bridge the country's digital divide; internet infrastructure and subscriptions in India's lower-income states are growing faster than in higher-income states. Based on current trends, the number of internet users is projected to increase by about 40 percent to 800 million and the number of smartphones to double to 700 million by 2023.[28] Demographically, some 65 percent of the population is below the age of 35, and 100 million Indians are expected to enter the workforce over the next decade.[29]

To address the aspirations of India's increasingly connected, youthful population and the imperative to expand economic opportunity, over the past decade the government has made major investments in digital infrastructure and related enablers, which are reshaping government service delivery and fueling commercial innovation. This common technology framework, known as the "India Stack" because of the ways in which the various solutions can be combined for a multitude of uses by entrepreneurs and

26 UNDP. "Human Development Reports: Population in severe multidimensional poverty (%), http://hdr.undp.org/en/indicators/101006. Accessed March 2020.

27 Economic Times Online. "Two crore Indians file returns but pay zero income tax," https://bit.ly/2x2LvFN. Accessed March 2020.

28 Kaka, Noshir; Madgavkar, Anu; Kshirsagar, Alok; Gupta, Rajat; Manyika, James; Bahl, Kushe; and Gupta, Shishir. "Digital India: Technology to transform a connected nation," McKinsey Global Institute, March 27, 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation#. Accessed March 2020.

29 Census of India 2011. Accessed March 2020.

governments alike, is rapidly changing India's data landscape and prompting the Government of India to consider how data produced by Indians can be leveraged to empower people, advance socioeconomic objectives, and fuel the domestic innovation economy.

THE INDIA STACK

The various platforms or "layers" of the India Stack were created over time to address long-standing gaps in the basic systems that enable broad-based participation in the formal economy. These gaps, which overwhelmingly impact the poor, women, and minorities, left some 400 million adults and other marginalized populations outside of the formal economy and often beyond the reach of key government assistance programs. In 2008, only one in 25 people in India had formal identification and only about a quarter of the adult population had a bank account. The extreme financial exclusion coupled with inefficiencies in India's vast network of welfare programs meant that progress was slow and uneven. This wasn't due to neglect; progress was slow despite decades of government-led efforts to raise living standards among the poor. In the early 2000s, an acute federal budget challenge sharpened focus on the fact that public assistance expenditures were outpacing government revenue growth. The GoI's federal and state-level social protection programs accounted for more than one-sixth of the government's annual budget, and as such, the well-documented "leakages" in the multilayered supply chain of the social safety net became an obvious target for reform. At the heart of the problem was the inability to ensure benefits, whether subsidized commodities or cash transfers, made it into the hands of eligible recipients without diversion, loss, or duplication.

Given the scale and scope of the interrelated problems of financial exclusion and massive inefficiencies in the welfare system, in 2009 India began to create digital infrastructure to close gaps in identity systems and the banking sector. This infrastructure, the India Stack, is a set of loosely coupled technologies and protocols, bolstered by policies, regulations, and/or laws, as relevant. Each API or standard may have its own "owner" within the GoI or public trust entities, and its own distinct licensing nuances. Importantly, all components of the Stack are based on two foundational design principles: (1) creating digital platforms as public goods so both government and private sector participants are able to develop technological innovations; and (2) incorporating data privacy and security in the design of digital public goods.

Because of the shared design principles, each layer contributes to lowering the costs of transactions on both the supply side and the demand side by eliminating paper documents, enabling remote transactions, reducing the use and thus cost of cash handling, and simplifying compliance with government regulations. This effect is expanding the addressable market, making it easier and less expensive to deliver public and private services to lower-income Indians. It also creates efficiencies across the broader economy and systems of public administration.

Understanding the two most mature layers of the India Stack—identity and payments—is central to understanding India's emerging approach to data sharing, known as the Data Empowerment and Protection Architecture. Because the identity and payments layers are currently enabling more than 800 million transactions per month, Indians across income segments and small businesses, once "invisible" are now generating rich data histories online.

AADHAAR: FOUNDATIONAL DIGITAL IDENTITY

In 2009, a new government agency, the Unique Identity Authority of India (UIDAI), was tasked with creating a population registry that could serve government needs including more efficient benefits distribution. UIDAI designed a nationwide population registry scheme that assigns a unique, randomly-generated twelve-digit number to every individual. The system collects minimal personal and demographic data (name, gender, date of birth, and address), as well as biometric data (fingerprints, iris scan, and a facial photo). Linking an email address and/or mobile telephone number to one's profile is optional.

Aadhaar, or "foundation" in many Indian languages, is a foundational rather than functional identity management system in that the biometric profiles are used only to confirm identity and authenticate transactions. Aadhaar participation does not confer any specific rights or privileges such as citizenship, eligibility to vote, permission to drive, etc. Other, domain-specific identities such as India's tax ID—the Permanent Account Number (PAN)—use Aadhaar to deduplicate its registries.

A verifiable identity is the bedrock of a modern economy in large measure because it enables participation in the formal economy by ensuring financial institutions and other regulated enterprises comply with national and global standards to mitigate illicit finance. In 2012, the Reserve Bank of India authorized Aadhaar identities to fulfill KYC[30] requirements via the e-KYC component of the India Stack. Digitalizing the manual KYC process allows banks and other companies to handle the process paper-free, drastically reducing the costs of onboarding new customers while complying with anti-money-laundering regulations. e-KYC also enabled the GoI to begin transferring welfare benefits and targeted subsidies directly to bank accounts. The impact of e-KYC has been substantial. According to one estimate, banks that use e-KYC lower their compliance costs for new accounts from about US$ 13 to less than US$ 1.[31] As of the end of 2019, an average of three million Aadhaar-based e-KYC requests were processed daily.

In the years since it was introduced, Aadhaar has been deeply embraced by the private sector and many government agencies. As of 2019, 95percent of adults in India were enrolled and reported using the system at least once per month. In 2018 the Supreme Court ruled that private entities cannot refuse to provide services to someone for lack of Aadhaar enrollment. The high court further held that children cannot be denied education for lack of Aadhaar.[32] Despite these rulings, a 2019 survey found that some 65 percent of people mistakenly believe that providing Aadhaar is mandatory by law for opening bank accounts, obtaining SIM cards, and even school enrollment. In fact, Aadhaar is only legally required in order to receive public benefits distributed through federal and state welfare programs. This linkage to subsidies and social protection programs, combined with the cost savings and efficiency gains for accessing commercial services, makes Aadhaar participation effectively (if not legally) mandatory for individuals and businesses to function in India.[33]

UPI: INTEROPERABLE DIGITAL PAYMENTS

The Unified Payments Interface (UPI) is a real time, fully interoperable retail payment system developed by the National Payments Corporation of India (NPCI) and deployed in 2016. UPI is the layer of the

30 Know-Your-Customer ("KYC") is the process of verifying identity and assessing if the customer is suitable for a business relationship. Before opening a financial account, banks are required to conduct a KYC check for regulatory compliance requirements, to prevent fraud, money laundering, and terrorist financing. In India, KYC also is required for activating a mobile phone connection.

31 https://www.livemint.com/Industry/0S81b1kQmceoP1OAaligcK/Is-the-banking-system-overlooking-key-challenges-in-its-rush.html

32 Gelb, Alan, Mukherjee, Anit and Navis, Kyle Navis. "What India's Supreme Court Ruling on Aadhaar Means for the Future," Center for Global Development, September 26, 2018.

33 State of Aadhaar Initiative, https://stateofaadhaar.in/index.php. Accessed March 2020.

India Stack that enables seamless money transfers between accounts, regardless of the type of financial provider. UPI creates a single interface between all bank accounts, effectively granting everyone with a smartphone access to the payment system and allowing financial transactions to take place instantly, on demand, and in fiat money inside the formal financial system. NPCI, a not-for-profit utility capitalized by 56 banks and closely regulated by the Reserve Bank of India, oversees and maintains UPI.

UPI has made payments simpler by removing the need to enter lengthy bank account numbers and IFS codes. To make a UPI payment, the user has to know only the recipient's virtual payment address (VPA), or use QR codes. The VPA is a simple combination of username and bank name that looks similar to abc@xyzbank. UPI is a modern, mobile-first system that does away with the need for physical cards. In a country like India, with its low literacy levels, this kind of simplicity is essential for financial inclusion.

As of late 2019, the two most mature layers of the India Stack—identity and payments—are being used for more than 800 million transactions per month each. These transactions, combined with growing usage of commercial tech applications, are enabling millions of Indians, many of them still poor, to generate rich data histories about themselves. The opportunity to translate this emerging "data wealth" into meaningful benefits for individuals and SMEs inspired the design of the India Stack's newest layer, which enables consent-based data sharing. This effort, called the Data Empowerment and Protection Architecture, is discussed below.

In parallel with the growth of the India Stack, the government promoted inter- and intra- government data sharing to facilitate e-government services. The Union Cabinet passed the National Data Sharing and Accessibility Policy in 2012, requiring the Government of India to make all nonsensitive data be available in machine and human readable forms. To facilitate this, the Ministry of Electronics and Information Technology (MEITy) has taken a number of steps to introduce efficiencies in government sharing of data, including a Policy on Open Application Program Interfaces (APIs) which prompted all arms of government to publish APIs and adhere to the same API standards, the DigiLocker platform for the issuance and verification of electronic documents, and the India Enterprise Architecture Framework (IndEA Framework) which aims to create a consistent model for Enterprise Architectures across the national, regional, and local governments and their agencies in order to provide more integrated e-government services.[34]

KEY FEATURES OF DATA GOVERNANCE

LEGAL DECISIONS AND LEGISLATIVE ACTION

It is important to note that the first layer of the India Stack, the Aadhaar identity system was introduced *before* a legal and regulatory framework was enacted. This led to intense debate and culminated in legal challenges to the constitutionality of the system that went all the way up to the Indian Supreme Court. Concerns of government overreach led in 2012 to a raft of lawsuits challenging the legality of Aadhaar on a number of grounds. Most notably that the collection of biometric data violates civil rights and that the Aadhaar Act of 2016 did not provide adequate statutory basis for the identity system. Eventually these challenges reached the Indian Supreme Court, which, in separate rulings in 2017 and 2018, found that privacy is a fundamental right for citizens protected under the country's constitution; that Aadhaar system's collection of biometric data does not violate the constitution; and placed limits on the GoI's ability to mandate Aadhaar. The Court found that while the government

34 Government of India, Ministry of Electronics and Information Technology (MEITYy). "IndEA Framework," https://www.meity.gov.in/writereaddata/files/IndEA_Framework_1.0.pdf. Accessed Nov. 3, 2020.

could embed Aadhaar in welfare schemes, it could not mandate private sector use or require citizens to use their Aadhaar number to open a bank account, get a phone connection, or in school admission. It also determined that an Aadhaar holder's data cannot be disclosed on the grounds of national security.

While these court rulings defined fundamental rights and limitations on Aadhaar related to data protection, the broader legal environment for data governance remained woefully outdated. The prevailing Information Technology Act of 2000 provided norms for data collection and usage but no guidelines for data storage, user consent, or general processing requirements. To address these gaps, a commission led by retired Supreme Court Justice BN Srikrishna produced a report and framework for data protection, which formed the basis for the draft Personal Data Protection Bill (PDPB) pending before parliament. The draft legislation grants Indians many of the same rights over data as GDPR does for EU citizens. The bill, if passed, will give individuals the right to access and port personal data. It would also place the responsibility on data holders to be accountable to people regardless of consent obtained. In other words, data holders must put in place structures that will minimize harm to individuals, even inadvertent harm, when processing personal data no matter what consent was granted by the user. While the PDPB does promise to codify this rights-based approach as an umbrella standard for data collection and processing, there are concerns that exemptions granted to the government for data collection and use in the national interest (Section 35 of the draft PDPB) are too broad and risk undermining citizens' right to privacy.

DATA EMPOWERMENT AND PROTECTION ARCHITECTURE

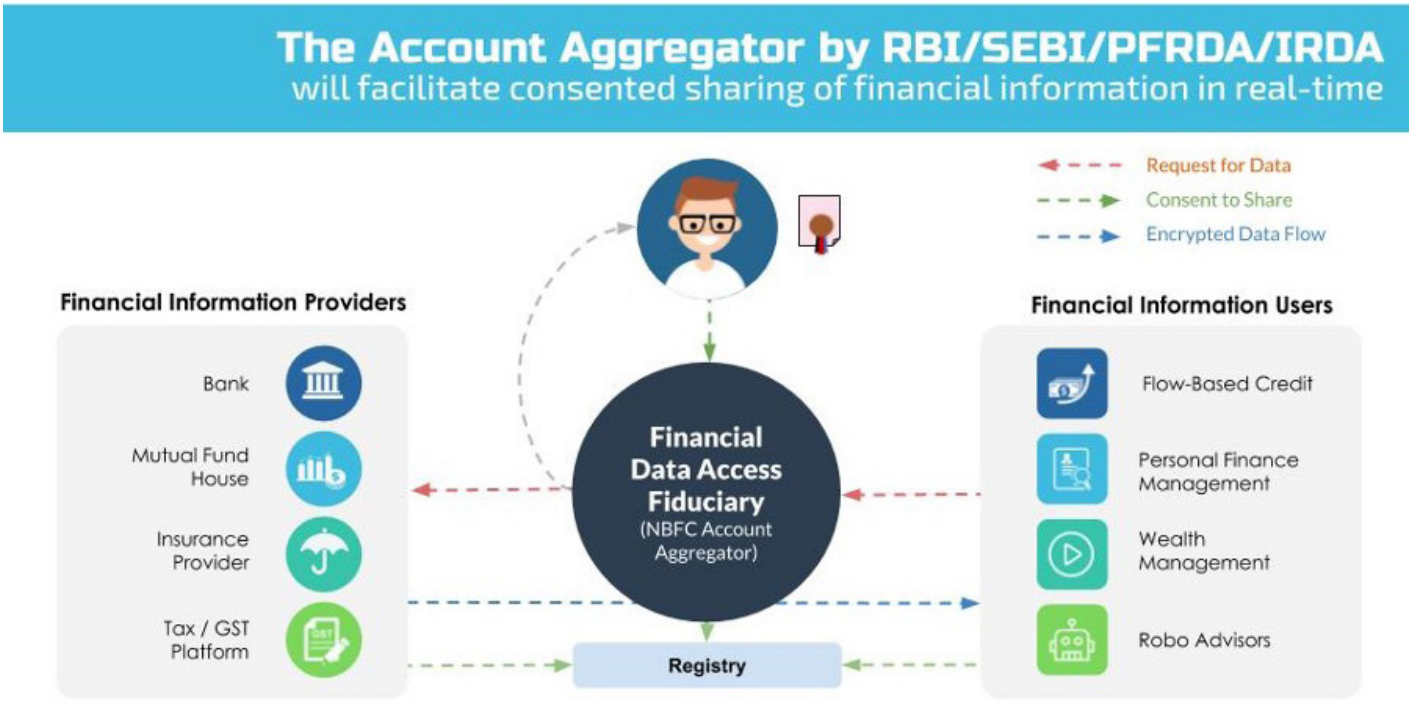
In parallel to this legislative action, MEITy and Reserve Bank of India (RBI) have introduced efforts to operationalize the right of citizens to access and control some of the data they generate online. The aspiration, as described in the Srikrishna Report, is to enable Indians to access and use their data for their own benefit, and to ensure that data can be made available for innovation beyond the platform on which it is produced. DEPA, some argue, can enable Indians to translate their "data wealth" into improved socioeconomic opportunities.

At the broadest level, MEITy has introduced national guidelines to standardize consent for data sharing so as to ensure individuals are consenting to every instance of data sharing rather than "pre-authorizing" data processing/sharing at the point of collection. The standardized consent artefact requires each transaction specify the parties involved, data to be shared, purpose of data sharing, and time-stamped signatures. By standardizing consent in this manner, it becomes possible to audit data flows to ensure users' authorization matches the subsequent data transfer.

The Reserve Bank of India became the first to introduce these standards across the entire financial sector with the issuance of the Account Aggregator Master Directive in 2016, which was updated in 2019 with technical specifications.[35] RBI is adopting DEPA in order to foster competition in the heavily concentrated banking sector and to fuel the innovation needed to deepen financial inclusion by "unlocking" data from silos held by dominant private and public sector providers. With the creation of this new class of regulated entities, called "account aggregators," RBI is spearheading a new means of establishing "trust" in the data economy by separating consent collection from data processing. In other words, account aggregators effectively serve as "data fiduciaries" that request and verify consent from individuals.

35 Reserved Bank of India Notifications, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598&Mode=0. Accessed March 2020.

Figure 2: Account Aggregator Model



Source: Sahamati. "Account Aggregator Frequently Asked Questions," https://sahamati.org.in/faq/. Accessed March 2020.

According to the newly formed industry association for account aggregators, Sahamati (meaning consent, in Hindi), no financial information of the user can be retrieved, shared, or transferred without the explicit (and digital) consent of the user. Thus account aggregators act as a "data-blind" conduit between entities requesting the data and the providers of the data, and do not process the data. The data that flows through an account aggregator is encrypted and can be processed only by the entity for whom the data is intended. This structure limits the business case of the account aggregators to fairly intermediating consent, which will operate on a utility model of charging transaction fees.[36] In addition, account aggregators do not and cannot store data, thus mitigating the potential for leakage and misuse. Importantly, this model also prevents the data holder from knowing the identity of the data requestor.

To encourage participation by financial providers in emerging DEPA solutions, the Goods and Services Tax Network (GSTN), under the supervision of the Ministry of Finance, is making available all goods and services tax (GST) data available through the established consent mechanisms. Access to this vast data repository of consumer and business data is expected to drive integration with the shared consent framework across the financial services sector. As of February 2020, RBI had issued three account aggregator licenses in full, four in principle, and anticipates an ecosystem of more than one dozen fully licensed aggregators by the end of the year.[37]

To bolster the data empowerment strategy, two institutional innovations have been developed to ensure that data sharing conforms to the consent provided and protects privacy. These include the forthcoming

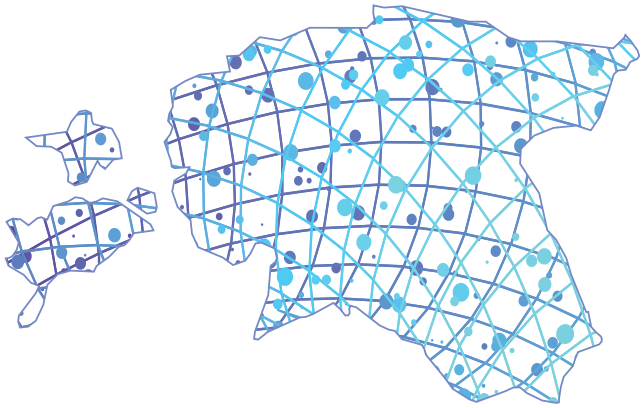
36 The consumer technically bears the cost of the account aggregators. However, it is expected that consumers in India will likely receive a voucher from the financial information user that is redeemable at any account aggregator. In this arrangement, the consumers have the freedom to choose their account aggregator and costs are borne by the data requestor.

37 Sahamati. "Account Aggregators in India," https://sahamati.org.in/account-aggregators-in-india/. Accessed March 2020.

Data Protection Authority described in the draft PDPB. While the exact role and resources for the DPA are still being finalized, it is expected to be a mediator of complaints from individuals who believe their data rights have been violated. In parallel, Sahamati is working with market players in the financial sector to establish norms for data exchange given the government has only specified requirements for consent collection. Sahamati also serves as a forum for adjudicating disagreements when a data request is not fully met.[38]

Ultimately, the goal of the DEPA framework is to establish a governance model for transactional data that balances the rights of individuals with those of the state. The policy and regulatory efforts are complemented by technical efforts to craft systems that safeguard privacy while unlocking data to empower individuals and small businesses. This effort is still in process and there is a vibrant public debate about how personal data should be treated by the law. However, the emerging approach appears to be two-fold:
(1) establish individual rights related to personal data, while also asserting rights for the state, and
(2) put in policy technology standards and protocols that enable consumers to actively assert the rights they are afforded by law.

38 Sahamati. "Sahamati—Collective of the Account Aggregator Ecosystem," https://sahamati.org.in/. Accessed March 2020.



ESTONIA: DATA SHARING FOR GOVERNMENT EFFICIENCY AND TRANSPARENCY

BACKGROUND

Estonia is a small, Northern European country of 1.3 million people nestled along the Baltic Sea. Following the restoration of the country's independence from the Soviet Union in 1991, the country quickly set about creating a parliamentary democracy and shifting toward market capitalism. Two early priorities were to conduct a comprehensive review of its citizenry and to establish an independent currency. To achieve both objectives simultaneously, the government established a system whereby citizens could self-register in a national database and, in doing so, exchange Russian rubles for Estonian kroner. This effort allowed the country to start afresh with a clean, digitized registry of its citizenry. Unbeknownst to the policy makers at the time, it was an important foundation for efficiently introducing a digital identity solution a decade later.

Estonia had been home to leading Soviet technical and scientific universities including the Tallinn Polytechnic University and Tartu State University. Several scientists, engineers, and academics were at the center of the (peaceful) independence movement and then moved into government upon sovereignty in 1991. This meant that Estonia had a number of key leaders who had been using the internet and its precursors, and recognized the potential of digital technologies even then. Their instinct to use technology to "leapfrog," combined with the regulatory flexibility the newly independent country had in the run up to accession to the European Union, manifested in several ways in the first decade of independence:

1. Massive investment in internet connectivity: Immediately following independence, the government privatized the national telecommunications monopoly and invested in fiber optic cables to connect the academic centers in Tallinn and Tartu. By the end of the 1990s, all schools in Estonia were connected to the internet.

2. Focus on digital skills: In 1996, the government launched the "Tiger Leap" initiative, which continued massive investments in internet connectivity and introduced computer skills in all secondary schools starting at the age of seven to ensure future generations would be digitally literate. Another initiative, Look@World, done in partnership with banks and telecoms provided computer training to 10 percent of the adult population who represented the least digitally literate segments of society. including blue-collar workers and retired individuals. Programs in digital literacy continue even today with efforts like Targalt Internetis which promotes internet safety and awareness of data rights.

3. Digitizing core registries to serve as the foundation of a modern government and economy. In addition to the first population registry, which later led to

the national digital identity system, the government created national land and business registries. To ensure all Estonians could identify themselves in order to access government services online, the government initially allowed people to use bank credentials. Once ready, however, the government launched a new digital identity solution in 2002. ID numbers of people are not kept secret—the idea is that because there is a secure digital ID and secure systems, knowing someone's number won't allow you to do anything with that information (unlike a social security number in the US, for example). The ID card looks like a normal ID card, but contains on the chip two digital certificates, one for identity authentication and the other for digital signature. Rollout started in 2002 and was complete in 2012.

Thus, although the average Estonian was still relatively poor and less than 10 percent of households owned a computer in 1999,[39] by 2016 approximately 90 percent of the population had become active users of the internet.

Importantly, in 1999-2000 the government undertook a pilot to connect three separate administrative databases without using a costly central solution. The experiment tested the security and efficacy of using the public internet to send queries to different databases, each originally built using different technologies. By 2001, Estonia was ready to roll-out a fully scaled X-Road system for data exchange across government systems. As described in more detail below, X-Road allows government agencies to develop their own ICT systems and policies but also ensures interoperability between them—a critical innovation that has enabled significant efficiency gains for the public sector and resulted in improved government services for citizens.

It is important to note, however, that investments in the X-Road technology alone did not enable the successful implementation of a government data sharing regime that enables better delivery of public services. In fact, Estonia has a number of other specific characteristics that were critical to successfully deploying X-Road and implementing a successful data sharing regime, most notably:

- *A high degree of trust in public institutions, reinforced by the use of digital technologies.* After the fall of the Soviet Union, the leaders of Estonia's digital transformation prioritized building trust in new forms of communication between government and citizens. One of those leaders, Linnar Viik, cites the government's decision to use email communications—which was emerging as a legitimate means of communications at the time—as a key building block of a trusted digital society. As he describes, that decision helped to *"slowly take down the institutional barriers impeding communications to be as easy and relaxed as possible. As a result, 'people trust digital interactions because we intentionally built digital non-formal forms of communication which people are used to employing, and that is something which contributes to making the social components of trust"*[40]

These types of early investment in building trust in public institutions have been maintained and strengthened by the government's efforts to provide a high degree of transparency in its use of data and provision of services.

- *The ability of a small number of public and private sector leaders to coalesce into an agile network that shares a vision of digital transformation and was able to cultivate quick and lasting political support.* This network enabled many of the policies and practices that have led to a successful X-Road implementation to take root without a centralized office for digital transformation, unlike many other countries that have created a restrictive, privacy-protecting data sharing environment. Instead Estonia

39 Krull, Andre. "ICT Infrastructure and E-readiness Assessment Report: Estonia" Praxis, 2003.

40 E-Estonia. "The cornerstone of e-governance is trust" May 2018, https://e-estonia.com/cornerstone-governance-trust/. Accessed March 2020.

developed a number of design principles that were reinforced by strong public-private networks and movement by members of these informal networks between sectors. These principles included the once-only policy that enables citizens and businesses to provide information to the government only one time and the focus on secure interoperability of decentralized databases.[41]

KEY FEATURES OF DATA GOVERNANCE

The proof-of-concept for decentralized data sharing launched Estonia's holistic approach to data exchange within government and among people. This is achieved through a coherent set of technologies, regulations and laws, and institutional responsibilities that enforce and support the policy goals of control over personal data.

CREATING THE POLICY AND REGULATORY ENVIRONMENT FOR DATA SHARING

Data governance in Estonia is based on core constitutional rights and provisions in a selection of relevant legislation, which applies to data regardless of its form. It is a conscious choice not to create specific legislation for digital data or for e-governance, in order not to create parallel systems. Article 26 of the Estonian constitution provides that "everyone is entitled to the inviolability of his or her private and family life" and prevents state interference absent specific circumstances enumerated by law.[42] This constitutional right, in part, forms the foundation for Estonia's Personal Data Protection Act (PDPA), which entered into force on January 15, 2019. The PDPA covers the elements of the GDPR that are left for national law. The Personal Data Protection Act Implementation Act entered into force on March 15, 2019, to implement the PDPA, which is now in force in Estonia.

The Estonian data protection authority, known as the Data Protection Inspectorate (DPI), fulfills the duties of an independent data protection authority as required by the GDPR and represents Estonia on the European Data Protection Board. The DPI sits within the Ministry of Justice but acts independently with the right to monitor the application of data protection in all public and private contexts, including governmental data processing. It issues guidelines, handles complaints from citizens and issues legally binding decisions.[43]

The GDPR is directly applicable and thus binding law.. The specific elements of the GDPR relevant for Estonia are that, as set out in recital 151 of GDPR, the Estonian legal system does not include administrative fines, so in Estonia fines are imposed by the supervisory authority in the framework of a misdemeanor procedure instead. PDPA does not mandate the appointment of data protection officers, and the age of consent is 13 under the PDPA (which can be from 13 up to 16 under the GDPR).

Relatedly, the PDPA can be viewed in relation to the Estonian Penal Code, which treats some data-related offenses as criminal offenses. For example, the unauthorized disclosure of personal data obtained in the course of professional activities by law enforcement and the unauthorized granting of access to such personal data are both misdemeanors under the law. More severe offenses, including the illegal disclosure of sensitive personal data are crimes subject to imprisonment. In an effort to provide more protections, the PDPA Implementation Act tightened the restrictions on public access to criminal records.

---

41 Kattel, R. and Mergel, I. (2018). Estonia's digital transformation: Mission mystique and the hiding hand. UCL Institute for Innovation and Public Purpose Working Paper Series (IIPP WP 2018-09). https://www.ucl.ac.uk/bartlett/public-purpose/publications/2018/sep/estonias-digital-transformation-mission-mystique-and-hiding-hand. Accessed January 2020.

42 Constitute Project. "Estonia's Constitution of 1992 with Amendments through 2015," https://www.constituteproject.org/constitution/Estonia_2015.pdf?lang=en. Accessed January 2020.

43 Jackson, Eric. "The right mix: how Estonia ensures privacy and access to e-services in the digital age." Estonian World, January 13, 2015, http://estonianworld.com/security/right-mix-estonia-ensures-privacy-access-e-services-digital-age/. Accessed January 2020.

In addition to these domestic enforcement mechanisms, Estonia is also a party to the Council of Europe's Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data, the first binding international law concerning individuals' rights to the protection of their personal data. Importantly, Estonia has also signed the Amending Protocol to modernize Convention 108 (known as "108+"), which imposes new and heightened obligations on data processing and transborder data flows. This could make Estonia's legal protections stronger than GDPR-only jurisdictions in the long run, thereby further enabling data sharing with partners outside the EU.

Perhaps just as important as the laws themselves is the way in which Estonians embrace their right to privacy. After decades of oppression and first-hand experience in violations from occupying forces, Estonians have maintained the right to privacy as a core topic throughout policy decisions related to economic stability.[44]

In practice this right to privacy requires the government to take measures to (1) protect the security of data on its citizens while also (2) offering means by which people have control over their data and transparency into government use of data.[45]

CREATING A TECHNICAL ARCHITECTURE FOR DATA SHARING

Part of facilitating data subject rights in Estonia are technology-enabled solutions that make public sector-held data more accessible. In particular, X-Road—the data exchange solution that safely offers citizens access to personal data and visibility into government use—creates a data sharing environment that is trusted and value-creating. X-Road builds upon the pilot effort to link decentralized databases. It allows linked public and private databases and information systems to automatically share information.

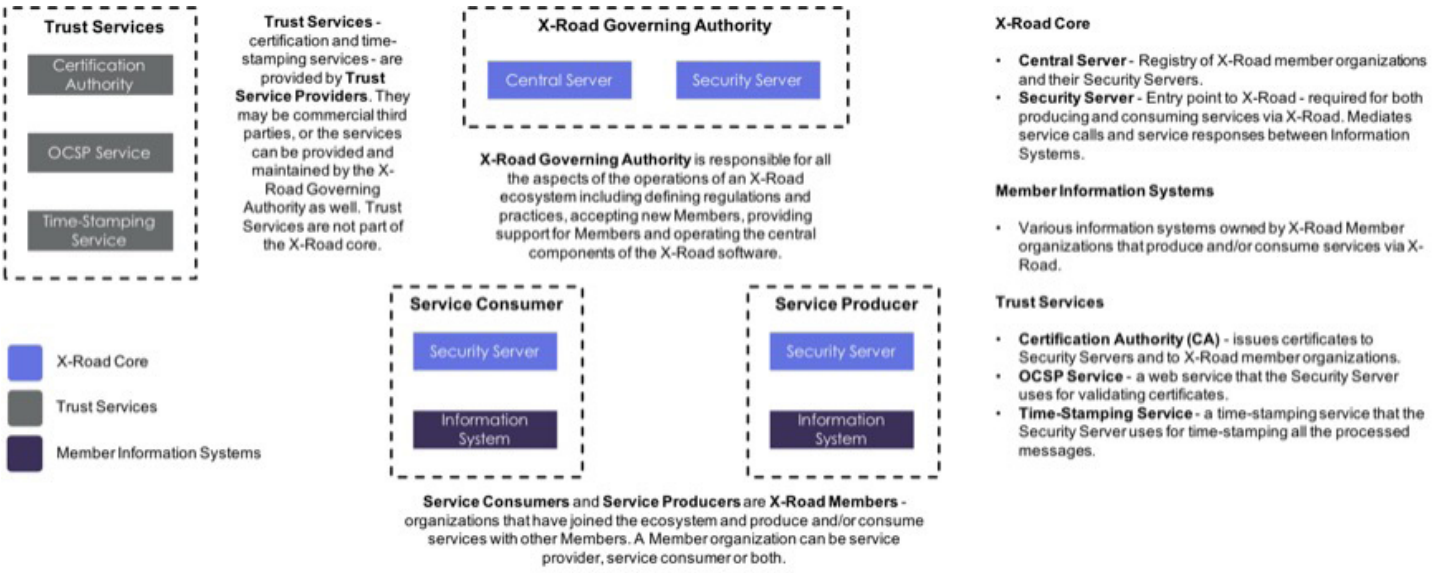
X-Road is an open source data exchange layer solution that enables organizations to exchange information over the Internet. X-Road is a centrally managed distributed data exchange layer between information systems that provides a standardized and secure way to produce and consume services and a common set of protocols and security mechanisms that allow members' information systems to recognize each other. Importantly, each government ministry or agency maintains its own database of information but common reference metadata ensures that the federated databases can exchange data, reducing the ability for one entity to hoard data and eliminating the possibility that one entity has entire control over citizens' data.

In this way, X-Road cultivates confidentiality, integrity and interoperability between data exchange parties.

44 Priisalu, J., and Ottis, R. Personal control of privacy and data: Estonian experience. Health Technol. 7, 441–451, June 15, 2017. https://doi.org/10.1007/s12553-017-0195-1.

45 Kivimaki, Petteri. "X-Road as a Platform to Exchange MyData," August 31, 2018. Nordic Institute for Interoperability Solutions, https://www.niis.org/blog/2019/10/30/x-road-as-a-platform-to-exchange-mydata. Accessed March 2020.

Figure 3: X-Road Data Exchange Layer Roles and Components



Source: Kivimaki, Petteri. "X-Road as a Platform to Exchange MyData," August 31, 2018. Nordic Institute for Interoperability Solutions, https://www.niis.org/blog/2019/10/30/x-road-as-a-platform-to-exchange-mydata. Accessed March 2020.

X-Road is released under the MIT license and is available free of charge for any individual or organization. Nordic Institute for Interoperability Solutions (NIIS) is responsible for the development of the X-Road core and managing the community of interested persons and experts. Technical and implementation support is provided by the private ICT companies. X-Road implements a set of common features to support and facilitate data exchange. X-Road provides the following features out of the box:

- information system identity management
- message routing
- access rights management
- organization level authentication
- machine level authentication
- transportation layer encryption
- time-stamping
- digital signature of messages
- tamper proof logging
- error handling

The identity of each organization and technical entry point (Security Server) is verified using PKI certificates that are issued by a trusted Certification Authority (CA) when an organization joins an X-Road ecosystem. The identities are maintained centrally, but all the data is exchanged directly between a consumer and provider. Message routing is based on organization and service level identifiers that are mapped to physical network locations of the services by X-Road. All the evidence regarding the data exchange is stored locally by the data exchange parties, and no third parties have access to the data. Time-stamping and digital signature together guarantee nonrepudiation of the data sent via X-Road.[46]

It is important to note that X-Road did not come about using a new technology but, rather, existing technologies were adapted to facilitate data sharing across many government systems. In fact, since its launch in 2001 there have been six major versions[47] of X-Road released, indicating an ongoing effort to

46 Kivimaki, Petteri. "X-Road as a Platform to Exchange MyData," August 31, 2018. Nordic Institute for Interoperability Solutions, https://www.niis.org/blog/2019/10/30/x-road-as-a-platform-to-exchange-mydata. Accessed March 2020.

47 NORDIC INSTITUTE FOR INTEROPERABILITY SOLUTIONS. "X-Road History," https://x-road.global/xroad-history. Accessed March 2020.

refine and adapt as the needs have changed, adding, for example, security features and a web management interface.

X-Road functions well because the rules of data sharing and use are established in law, software code, and practice without removing essential responsibilities from data controllers. Specifically,

- "Once-only" data capture. A Databases Act was adopted in March 1997 to regulate the creation and maintenance of digital databases and create a state register of databases. The Act was repealed in 2006, with core principles now in the Public Information Act, as part of the strategy to avoid specialized e-governance legislation. By authorizing the central government, the Estonian Information System Authority specifically, to oversee the creation of all new databases, the government is assured that information is captured only once. From the perspective of businesses and citizens, it means they only have to supply government agencies and participating businesses their information once. X-Road-enabled data interoperability coupled with the digital ID card enables personal data to be securely and accurately pre-populated in advance of need provided that there is a legal basis for the use of data, so that *"Instead of having to "prepare" a loan application, applicants have their data—income, debt, savings—pulled from elsewhere in the system. There's nothing to fill out in doctors' waiting rooms, because physicians can access their patients' medical histories."*[48]

- Data permissions. To ensure appropriate government access of personal data, strict permissions have been established for accessing X-Road data. To achieve this, permissions of data access and use are enshrined in code.[49] Each institution as data controller determines what information is available and who has access to it. Looking at an individual's data without a reason is a criminal offense.[50] A number of key principles govern the system of data permission:

  - *Confidentiality principle*—only authorized institutions has access to data. Each institution will authorize officials from institutions or organizations with a data usage agreement to have access to the data in the databases or exchanged via X-Road.
  - *Autonomy principle*—X-Road member itself defines which data services it wishes to provide and to whom to grant the access rights of the service usage.
  - *Integrity principle*—X-Road also ensures that data exchanged by the means of data service reach relevant members without leaks and as a whole (without deviations and with evidential value). Deviation of data between members can be identified.

- Data transparency. Citizens and residents can access nearly all of their own data online through the State Portal (www.eesti.ee) or other specialized portals (e.g., Patient Portal). There are over 2,600 services integrated through X-road, more than 1,200 connected organizations, public registries, and databases and ca. 52,000 organizations as indirect users of X-tee services. Estonians can log in to the portal, using their identity cards or other eID tools to view all personal data and correct mistakes.[51] Furthermore, X-road enables data owners to determine what information is available and which organizations have access to it. X-Road ecosystem has two-level authorization. Authorization

48 Heller, Nathan. "Estonia, the Digital Republic." *The New Yorker* 18 & 25 December 2017. Digital.

49 European Union: European Regional Development Fund. "Security Server User Guide" https://x-tee.ee/docs/live/xroad/ug-ss_x-road_6_security_server_user_guide.html. Accessed March 2020.

50 Heller. "Estonia, the Digital Republic."

51 Herlihy, Peter. (2013, October 31). 'Government as a data model': what I learned in Estonia [blog post], https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/. Accessed January 2020.

of organization has been realized by core X-Road tools, authorization of end-users is the responsibility of front end systems. For example, an individual can make a particular medical file accessible to some of his or her doctors while keeping it private from others, if desired. Additionally, each time an authority figure like a police officer or doctor or government official looks at an individual's secure data online, it is recorded and visible to the person concerned.

- Data security: Estonia became the first country to develop a solution on the principles shared with blockchain at the national level. X-Road uses cryptographic chaining technology, where each institution can make decisions based on data in a private ledger. X-Road ensures that no data could be changed or manipulated by anyone and that authenticity of data can be verified.[52] X-Road facilitates more than 1.5 billion transactions per year (as of 2019), none of which have a supporting traditional paper trail. The ability to deploy strong cryptographic algorithms or similar technologies to increase verifiability of data has contributed significantly to overall trust in the system.

- Data availability: Estonia has also taken steps to create backup systems for added security, creating a "data embassy" in Luxembourg in 2017 that follows the same international laws as physical embassies.[53] This innovation is only possible because of legislative amendments that enable cloud-based data storage in the government cloud. The Estonia Government Cloud is developed in accordance with the national IT Security Standard (ISKE), to ensure the compliance with safety and quality requirements, including, for instance, the handling of sensitive personal data with confidentiality and integrity. The cloud-based data storage solution enables the creation of e-embassies.[54]

X-Road's distributed nature has made it far less costly and more secure than other e-government data exchange systems around the world. The entire X-Road data exchange system—including maintenance, salaries, and investments—is roughly $3 million per year, exponentially less than what some other countries spend for lower quality e-government platforms.

Ultimately, Estonia's model for data sharing has cultivated two key aspects of agency—trust and control. The successful provision of e-government services has been built upon citizens' trust in the government's intent and ability to keep their information secure. With online tax declaration and medical services reaching near universal adoption in Estonia, it is clear that the steps the government has taken—technically (X-Road), legislatively (Personal Data Protection Act), and behaviorally (transparency in instances of security breaches)—has helped build that trust. While each of these factors have contributed significantly to the environment of trust that Estonia enjoys today, they have not developed in an entirely planned or linear way. Laws and technical solutions were developed step by step.

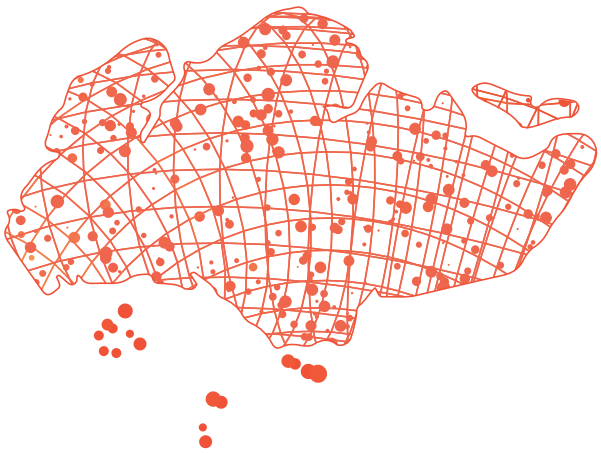
X-Road includes tools against inside misuse of data by officials. All queries of officials are logged. Organizations, and, in some cases even citizens can check queries of officials. If an official has misused the data, they will be punished or fired.

The transparency created by the State Portal and the ability of individuals to see how their data is being used and access, correct, and manage it virtually has helped reinforce—rather than create—the trust environment.

52 E-Estonia. "Security and Safety," https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/. Accessed January 2020.

53 E-Estonia. "Data Embassy," https://e-estonia.com/solutions/e-governance/data-embassy/. Accessed January 2020.

54 E-Estonia. "E-Governance: Government Cloud," https://e-estonia.com/solutions/e-governance/government-cloud/. Accessed January 2020.



SINGAPORE: DATA SHARING FOR ECONOMIC GROWTH AND INDIVIDUAL EMPOWERMENT

BACKGROUND

Singapore is a small island nation with a reputation for pro-business adaptive regulation and a historical emphasis on trade and the financial sector. In 2014, Singapore introduced its Smart Nation initiative, a digital transformation effort that has been thoroughly planned and driven by the government. This initiative has reinforced the country's position as a regional leader in digital transformation[55] and established Singapore as a global data hub. At the time of its launch, the Smart Nation Initiative was seen as the next in a series of "successful whole-of-nation transformations in response to digital disruption." It built upon the National Computerization push in the 1980s and early-1990s and Intelligent Island and Intelligent Nation initiatives that developed the country's information and telecommunications (ICT) industry starting in the mid-1990s.[56] The Smart Nation Initiative set forth a vision for improvements to internet access and mobile connectivity, e-government services, and IT training to modernize Singapore with a central focus on how data could enable an innovation ecosystem and modernize the delivery of public services.

The initial strategy, led by the Smart Nation Programme Office in the Prime Minister's Office, helped surface meaningful opportunities for this phase of the country's digital transformation, but met significant headwinds in implementation, leading Prime Minister Lee Hsien Loong to acknowledge in 2017 that "for all our pushing, we are not really going as fast as we ought to."[57] The Smart Nation Programme Office identified challenges in its efforts to implement the initiative. Most notably, it found that the high-level aspirations underpinning the initiative were not well-connected to specific opportunities and use cases. Instead, an iterative process of identifying needs from bottom up and setting requirements and standards from the top down would be more effective. With that finding in mind, an updated strategy was published in 2018, envisioning "a Singapore where people will be more empowered to live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all."[58]

The Smart Nation Initiative is now organized around three foundational strategy documents and identifies three key enablers that cut across the country's vision of the digital future (see figure below).

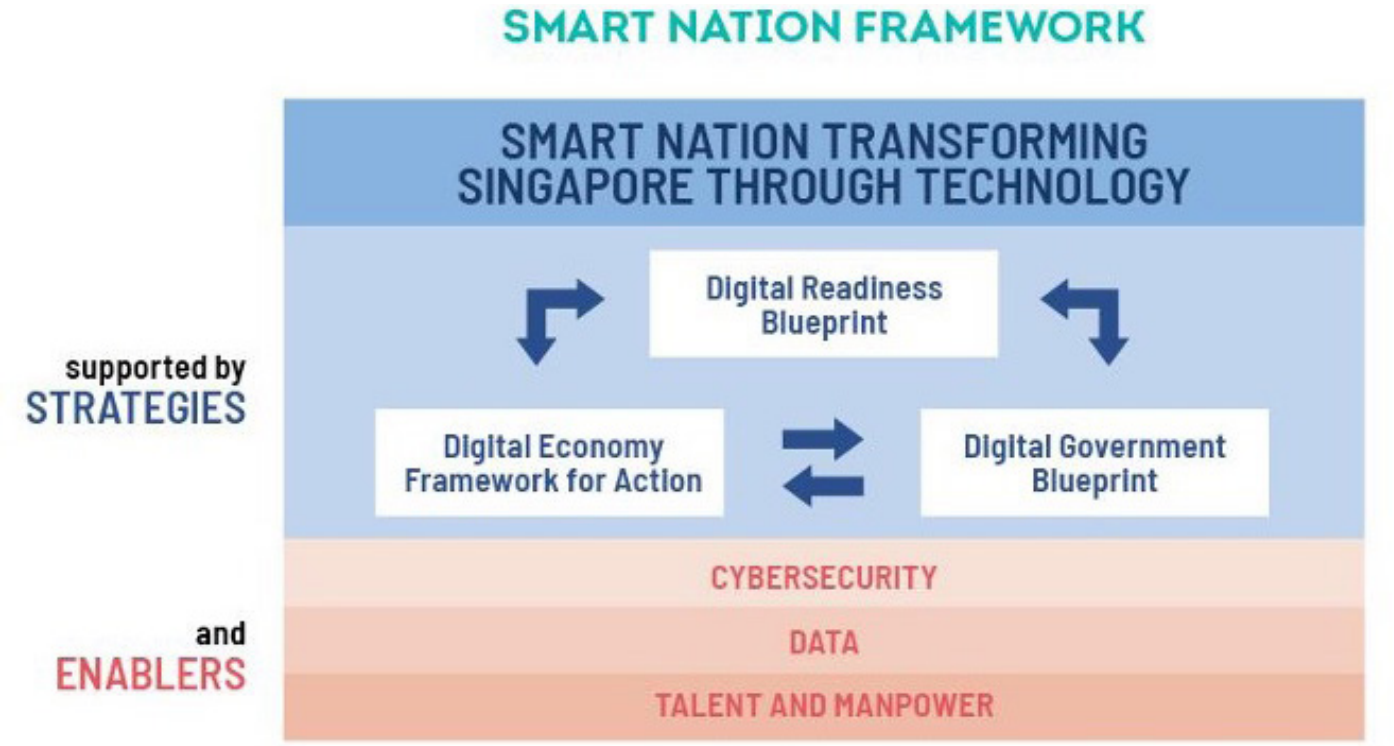
55 The Economist Intelligence Unit. "Singapore," January 2017, http://connectedfuture.economist.com/wp-content/uploads/2016/11/Connecting-Capabilities_SINGAPORE_v6.pdf. Accessed, March 2020.

56 Tan, Belinda and Yimin, Zhou. "Technology and the City: Foundation for the a Smart Nation." Centre for Liveable Cities Singapore, Urban Systems Studies, 2018, https://www.clc.gov.sg/docs/default-source/urban-systems-studies/uss-technology-and-the-city.pdf. Accessed December 2019.

57 The Straight Times. "PM maps out way ahead for S'pore in tech, trade and trust between people," February 28, 2017, https://www.straitstimes.com/opinion/pm-maps-out-way-ahead-for-spore-in-tech-trade-and-trust-between-people. Accessed December 2019.

58 Smart Nation Singapore website, https://www.smartnation.sg/docs/default-source/default-document-library/smart-nation-strategy_nov2018.pdf. Accessed December 2019.

Figure 4: Smart Nation Framework



Source: Civil Service College Singapore (A Singapore Government Agency Website), https://www.csc.gov.sg/articles/digital-government-smart-nation-pursuing-singapore's-tech-imperative. Accessed December 2019.

1. The Digital Economy Framework for Action outlines a plan to make Singapore a leading digital economy that will attract foreign investments and provide opportunities for Singaporeans. Published by the Infocomm Media Development Authority (IMDA) in May 2018 with strategic priorities around accelerating digitization of existing industry sectors, improving the competitiveness of Singapore's digital ecosystem, preparing the economy for digital disruption, and transforming the InfoComm Media sector itself to be a leader for other industries.[59] The plan highlights "Policy, Regulations, and Standards" and "Physical and Digital Infrastructure" as key enablers for such a transformation.[60]

2. The Digital Government Blueprint articulates the vision for making Singapore's government "digital to the core." This entails utilizing connectivity, data, and computing to enable citizens, businesses, and public officers. The digital government plan includes a five-year roadmap, which outlines how the government should use digital technologies when serving the public, including a National Digital Identity (NDI) system for Singapore businesses and residents. This system will facilitate secure and effective digital communication between the private sector and the government. The blueprint also emphasizes the importance of data sharing and management in creating an effective e-government.[61] The six strategies in place to build

59 INFOCOMM Media Development Authority (A Singapore Government Agency Website), https://www.imda.gov.sg/infocomm-media-landscape/SGDigital/Digital-Economy-Framework-for-Action. Accessed December 2019.

60 Along with Talent and Research and Innovation. Ibid

61 Smart Nation Singapore. "Digital Government Blueprint (Summary): A Singapore Government that is Digital to the Core, and Serves with Heart," https://www.tech.gov.sg/files/digital-transformation/dgb_summary_june2018.pdf. Accessed December 2019.

a digital government, "building common digital and data platforms," "operating reliable, resilient and secure systems" and "strengthening integration between policy, operation and technology"—all speak to the critical nature of appropriately using and safeguarding data to improve government service delivery and rectify major implementation issues of the initial Smart Nation Vision.[62]

3. The Digital Readiness Blueprint was created to ensure all Singaporeans can access technology to enhance their lives, every day. The government established a digital readiness working group, with participants from the public, private, and civil society, tasked with ensuring access to inclusive digital infrastructure, building digital literacy, and driving participation in digital communities and usage of technology.[63] The blueprint outlines recommendations around improving cybersecurity and data awareness skills, providing access to basic digital enablers, and driving interaction with data-driven technologies which are key to maximizing the benefits and containing the risks of data.[64]

REIMAGING GOVERNMENT FOR THE DIGITAL FUTURE

To help realize the Smart Nation vision, the Government of Singapore has invested deeply in its own capabilities, retraining and reskilling its employee base to meet the demands of a data economy, and hiring many software engineers, data scientists, product managers, and others with the necessary skills to ensure it does not fall behind the private sector. The government has also restructured in a number of ways since the launch of the Smart Nation including, most notably with respect to data governance. The government:

- Brought together separate agencies in the converging media and infocommunications sectors to provide a single, leading interface on digital and data to the private sector.[65] The new entity, IMDA, was launched in August 2016 and tasked with the responsibilities of cultivating the digital economy and ensuring public engagement in it, responsibilities that would later be reflected in the Digital Economy Framework for Action and Digital Readiness Blueprint, respectively.[66] IMDA included an industry group to plan and execute private sector development efforts around data and digital topics, the Personal Data Protection Commission charged with administering and enforcing Singapore's comprehensive Personal Data Protection Act, and a community outreach and engagement team to provide local content and educate the public on the use of technology.

- Elevated the authority of the Government Technology Agency (GovTech), empowering it to build deep ICT and engineering expertise to transform

62 Along with "Integrating services around citizen and business needs," "Raising our digital capabilities," and "cocreating with citizens and business, and facilitating adoption of technology" which are important enablers and outcomes of good data governance. See: https://www.tech.gov.sg/media/technews/6-things-you-need-to-know-about-the-digital-government-blueprint?utm_medium=recommender_1&utm_source=aHR0cHM6Ly93d3cudGVjaC5nb3Yuc2cvZGlnaXRhbC1nb3Zlcm5tZW50LWJsdWVwcmludC8=&utm_content=aHR0cHM6Ly93d3cudGVjaC5nb3Yuc2cvbWVkaWEvdGVjaG5ld3MvNi10aGluZ3MteW91LW5lZWQtdG8ta25vdy1hYm91dC10aGUtZGlnaXRhbC1nb3Zlcm5tZW50LWJsdWVwcmludA==.

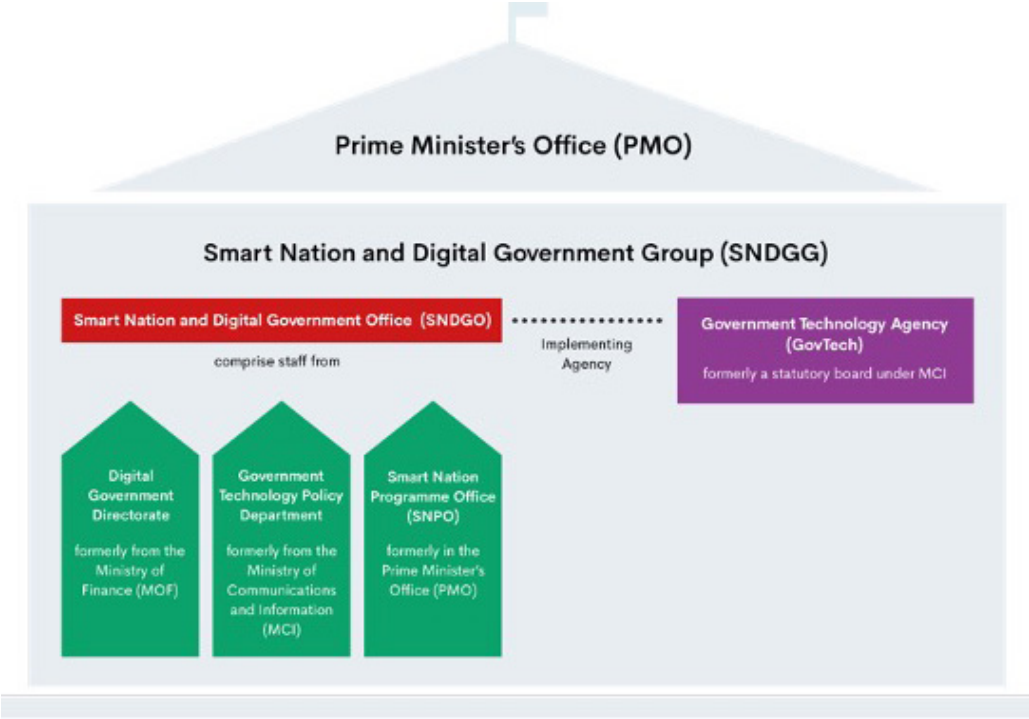
63 Civil Service College Singapore (A Singapore Government Agency Website), https://www.csc.gov.sg/articles/readying-singapore-to-be-a-digital-society. Accessed December 2019.

64 Ministry of Communications and Information. "Digital Readiness Blueprint" https://www.mci.gov.sg/-/media/mcicorp/doc/mci_blueprint-report_final.ashx. Accessed December 2019.

65 INFOCOMM Media Development Authority (A Singapore Government Agency Website), https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2016/imda-to-empower-businesses-workers-and-communities-to-seize-opportunities-in-a-digital-future. Accessed December 2019.

66 INFOCOMM Media Development Authority (A Singapore Government Agency Website), https://www.imda.gov.sg/-/media/Imda/Files/About/Media-Releases/2016/Annex-A--About-IMDA.PDF. Accessed December 2019.

Figure 5: GovTech Singapore



Source: GovTech Singapore (A Singapore Government Agency Website). "Our Role," https://www.tech.gov.sg/who-we-are/our-role/. Accessed December 2020.

government.[67] The 1,800 strong group of data scientists, technologists, and engineers is tasked with efforts across application development, government digital infrastructure, data science, geospatial data, sensor technology, and cybersecurity.[68] This restructuring also served to clarify responsibilities in government on cross-cutting topics such as data protection and technology adoption while elevating the importance of data talent and providing a central group able to drive implementation of whole-of-government and national level data projects.

- Created only a few months after the initial restructuring, the Smart Nation and Digital Government Group (SNDGG), a new guiding body to marry the planning and policy skills needed to tackle such projects with the necessary implementation expertise.[69]

Ultimately, these institutional reforms enabled SNDGG—which is well-resourced and has a strong mandate—to focus on providing shared digital infrastructure (e.g., data transfer platforms), enforce common standards (e.g., for data security), and ensure interoperability of applications. Concurrently, specific government agencies remain domain experts in

67 Ministry of Communications and Information. "Launch of the Government Technology Agency: SPEECH BY DR YAACOB IBRAHIM, MINISTER FOR COMMUNICATIONS & INFORMATION," October 7, 2016, https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2016/10/launch-of-the-government-technology-agency?=page&page=15. Accessed December 2019.

68 Tham, Irene. "GovTech launched to lead digital transformation in public sector," The Strait Times, October 7, 2016, https://www.straitstimes.com/tech/govtech-launched-to-lead-digital-transformation-in-public-sector. Accessed December 2019.

69 GovTech Singapore (A Singapore Government Agency Website). "Formation of the Smart Nation and Digital Government Group in the Prime Minister's office," March 20, 2017, https://www.tech.gov.sg/media/media-releases/formation-of-the-smart-nation-and-digital-government-group-in-the-prime-minister-office. Accessed December 2019.

front-line data collection and in management and use of specific databases. Ultimately, SNDGG has helped ease intragovernmental data sharing.

With these institutional changes in place, the Singapore Government turned its attention to the individuals and processes within those agencies and ministries, identifying the need to rebuild government data talent, ensure better communication between technical experts and policy makers, and improve the way the government delivers development projects.
To draw more interest and provide a more compelling offering to highly-sought after data talent, compensation packages were revamped to provide salaries more comparable to the private sector.[70] The government actively marketed Singapore as a hub for international talent and rolled out a series of initiatives to attract Singaporeans working in data overseas. To retain these talents, HR policies have been restructured to allow employees with data and digital skills to more easily switch between ministries and agencies, broadening their exposure and ensuring talent isn't siloed in the SNDGG.[71] Programs have also been set up to facilitate employee exchanges with the private sector, providing for industry professionals to share their experience with government teams and government employees to gain experience in private companies.[72] Additionally, to best utilize this rebuilt bench of data skills, a variety of efforts have been made to better integrate traditional policy and operations knowledge and skill sets with the technical skills these new talents offer. At the management level, new leadership positions have also been created to ensure technical expertise is included in senior conversations about data and digital transformation. Ministries are now staffed by Chief Data Officers and Chief Information Security Officers, often in addition to CIOs and Chief Digital Strategy Officers.[73] Within organizations, individuals are given opportunities and encouraged to cross-train data skills while projects are often assigned to cross-functional cross-agency teams, or at least have other domains represented in planning and testing sessions.[74] Matrixed teams, a digital experimentation unit, and other principles of "Agile Development" have also been adopted to facilitate the government's "policy-ops-tech integration" goal, leading to more iterative project planning and changes to how budgets are allocated and progress measured.

These shifts in processes, culture, and ways of working have had a profound effect on the SNDGG and other ministries. GovTech, for instance, has been able to expand its number of data scientists and software engineers from approximately 400 to 600 in the last few years.[75]

KEY FEATURES OF DATA SHARING

The updated 2018 Smart Nation strategy recognized data as "a key resource in Smart Nation" and "a key foundation" with value across the public and private sectors and of central importance to achieving the Smart Nation vision. The strategy outlined the need to develop "the systems, process, and capabilities to maximize the value of data" across its life cycle and the aspiration to "be a global hub for data, akin to [their] world class airport and seaport." To achieve this foundational goal, the strategy tasked the government in leading the way, shifting government data strategy to ensure an "Integrated Data Management Framework, including reviewing legislation, implementing

70 Khern, Ng Chee. "Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative," Issue 21 Ethos: A Publication of Civil Service College Singapore, July 2019, pg. 15.
71 Khern, Ng Chee. "Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative," Issue 21 Ethos: A Publication of Civil Service College Singapore, July 2019, pg. 15.
72 Khern, Ng Chee. "Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative," Issue 21 Ethos: A Publication of Civil Service College Singapore, July 2019, pg. 15.
73 Khern, Ng Chee. "Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative," Issue 21 Ethos: A Publication of Civil Service College Singapore, July 2019, pg. 15.
74 Khern, Ng Chee. "Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative," Issue 21 Ethos: A Publication of Civil Service College Singapore, July 2019, pg. 15.
75 Freymuth, James. Interview notes. 2019.

policy and building capabilities and shared services" to reduce the time necessary to source, clean, verify, and use data, improve integration of data to build fit-for-purpose datasets and ensure ease of access "to data and analytics capabilities for policy analysis, operations, service delivery, and private sector facilitation." In opening remarks at the 7th Personal Data Protection Seminar in July 2019, Mr S Iswaran, Minister for Communications and Information of Singapore, reinforced this vision for data, highlighting the need for evolving the country's data governance in accordance with a changing data landscape—that building a strong digital economy requires both "strengthening data protection capabilities and growing trusted data flows."[76] This belief, that increased data flow and better data protection will build a strong digital economy, is foundational to Singapore's approach to data sharing.

CREATING THE POLICY AND REGULATORY ENVIRONMENT FOR DATA SHARING

In line with its historical approach to regulation, Singapore has taken an open and iterative approach to regulating data, choosing to err on the side of minimizing regulatory intervention as new technologies and markets develop, while closely monitoring that development, as well as global experiences to understand when additional action may be necessary. They advocate for learning through participation, opening sandboxes in a variety of different sectors, to encourage collaboration with the private sector and setting aside large sums for the investment in domestic firms exploring new technologies or use cases.

Despite this restrained approach to nascent markets, Singapore has also been a strong advocate for the adoption of technology, once it is convinced of its viability, by both the private sector and government. It has published a large number of detailed strategic plans to transform industries, government functions, and parts of society. It has made large investments to incentivize adoption from funding technology development to driving awareness of applicable capabilities to shaping the necessary enabling environment. The country's leadership in implementing open banking has been illustrative of this approach (see Spotlight on page X for further details on how Singapore's commitment to trusted data flows has helped drive open banking).

Despite this pro-innovation and iterative approach to regulating the innovation sector, Singapore has increasingly recognized the need to take a more explicit position on legal protections for data as a lever for creating a more trusted system. In other words, the evolution of the policy and regulatory environment has evolved over the last few years to have an increased focus on data protection and data security as a means to increase accountability, including specific efforts to build confidence in the sharing of data. This evolution started with the introduction of the Personal Data Protection Act of 2012 (PDPA).

Prior to enacting PDPA, Singapore did not have an overarching data protection law. Rather, the collection, use, disclosure, and security of personal data were regulated to a lesser degree by a patchwork of laws including sector-specific data protection frameworks, such as the Banking Act in respect of the financial sector, which continue to operate alongside the PDPA.[77] The PDPA was implemented in three phases:

1. In January 2013, setting out the scope and interpretation of the Act, and establishing the Personal Data Protection Commission (PDPC) and Data Protection Advisory Committee (DPAC).

76 Ministry of Communications and Information. "Opening Remarks by Mr. S. Iswaran, Minister for Communications and Information, at the 7th Personal Data Protection Seminar," July 17, 2019, https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/7/opening-remarks-by-mr-s-iswaran-at-7th-personal-data-protection-seminar-on-17-july-2019. Access 2019.

77 The PDPA sets a baseline standard for personal data protection across the private sector, alongside existing laws and regulations. This general data protection framework does not affect any right or obligation under existing laws, and that in the event of any inconsistency, the provisions of other preexisting laws will prevail. For example, the banking secrecy laws under the Banking Act govern customer information obtained by a bank, and the Telecom Competition Code governs end-user service information obtained by a telecommunications licensee.

2. In July 2014, the Act's main data protection provisions came into effect, setting out the obligations of organizations with respect to the collection, use, disclosure, access to, correction, and protection of personal data.

3. Finally, the Personal Data Protection Regulations (the Regulations) were also enacted in 2014 to supplement the PDPA in respect of the requirements for transfers of personal data out of Singapore, procedures related to requests for access to or correction of personal data, and rules for exercising rights in relation to disclosure of personal data of deceased individuals.[78]

International best practices on data protection were incorporated into the formulation of the PDPA and the Regulations. Upon its enactment, the then-Minister of Information, Communications, and the Arts referenced influential data protection frameworks in jurisdictions such as Canada and the European Union, as well as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework.

The PDPA is administered and enforced by the PDPC and established the Data Protection Advisory Committee (DPAC), which advises the PDPC on matters relating to the review and administration of the personal data protection framework, such as key policy and enforcement issues. Currently, the DPAC is headed by the Senior Advisory/Director General of International Affairs of IMDA.

The PDPC may initiate an investigation to determine whether an organization is compliant with the PDPA, upon receipt of a complaint or on its own motion. In deciding whether to commence an investigation the PDPC considers a variety of factors, including whether the organization may have failed to comply with all or a significant part of its obligations under the PDPA, whether the organization's conduct indicates a systemic failure to comply with the PDPA, the number of individuals who are or may be affected by the conduct, and public interest considerations. The PDPC is also empowered to review complaints in relation to individuals' access and correction requests.

The PDPC may enter into cooperation agreements with foreign data protection authorities for data protection matters such as cross-border cooperation, including information exchange, or to assist the enforcement or administration of data protection laws.

Scope of Law

The PDPA covers all forms of "personal data," electronic or nonelectronic. "Personal data" is broadly defined as data about an individual who can be identified from that data, or from that data and other information the organization has or is likely to have access to. While the PDPA does not distinguish between the types and sensitivities of personal data, the PDPC has imposed more stringent guidelines with respect to National Registration Identity Card (NRIC) numbers and other national identification numbers.[79] In general, organizations may not collect, use, or disclose NRIC numbers and other national identification numbers unless such collection, use, or disclosure is required by law (or an exception under the PDPA applies), or necessary to accurately establish or verify the identity of the individual to a high degree of fidelity.

The PDPA applies to all organizations in Singapore, regardless of size or scale that collect, use or disclose

78 The PDPA and the Regulations were also accompanied by a set of related regulations, including the Personal Data Protection (Composition of Offences) Regulations 2013, Personal Data Protection (Enforcement) Regulations 2014, and Personal Data Protection (Appeal) Regulations 2015. The PDPC has issued substantial guidance to clarify the Act's interpretation, including sector-specific guidelines for telecommunications, healthcare, and education, among other sectors.

79 See PDPC, ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR NRIC AND OTHER NATIONAL IDENTIFICATION NUMBERS (31 August 2018), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf.

personal data in Singapore, regardless of whether they are formed or recognized under Singapore law or whether they are resident or have an office or place of business in Singapore. An "organization" is broadly defined as any individual, company, association or body of persons, corporate or unincorporated, and whether or not formed or recognized under the law of Singapore, or resident or having an office or place of business in Singapore. Notably, the PDPA does not apply to

- individuals acting in a personal or domestic capacity, employees acting in the course of their employment, and public agencies or organizations acting on behalf of a public agency in relation to the collection, use, or disclosure of personal data.

- "Data intermediaries" are also exempt from most of the PDPA's provisions and only have to comply with the rules relating to the protection and retention of personal data. A "data intermediary" is an organization that processes personal data on behalf of another organization, the principal organization, pursuant to a written contract (similar to a "data processor" under the GDPR). They are only required to make reasonable security arrangements to protect personal data in their possession in order to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks, and to anonymize or cease retaining personal data as soon as it is reasonable to assume that retention no longer serves the purposes for which the data was collected or is no longer necessary for legal or business purposes. A data intermediary that surpasses the processing required by their contract would no longer be deemed an intermediary and would be subject to the full reach of the PDPA.[80]

The PDPA specifically requires that organizations designate one or more individuals to act as data protection officer(s) (DPO)[81] and to make their business contact information known to the public. DPOs are responsible for ensuring an organization complies with the provisions of the PDPA, although the designation of a DPO does not relieve an organization of its obligations and liabilities in the event of noncompliance. Although there are no strict requirements to apply a data protection-by-design approach or carry out impact assessments, DPOs are encouraged to conduct regular data protection impact assessments (DPIAs) to assess and address organization-specific risks.

Public Sector Data

Public agencies in Singapore are not governed by the PDPA, but under the Public Sector (Governance) Act and the Government's Instruction Manual. The need for two different legislations governing data management in the public and private sectors arises because the public has different expectations of the services provided by the government and the private sector. The public expects the government to deliver services in an integrated manner across agencies, but they do not expect this of the private sector. For example, citizens would expect the Ministry of Education to obtain personal data of children at the compulsory school age from the Immigration and Checkpoints Authority to ensure that they are enrolled in a primary school. A citizen would not expect a tuition center to know what other tuition centers his child is enrolled in.

Public officers who are involved in data incidents are held accountable in the following ways:

1. They may be liable to fines up to $5,000 and/or up to 2 years' imprisonment for the following acts prescribed in the PSGA:
   a. Reckless or intentional disclosure of data without authorization.
   b. Improper use of data for a gain.
   c. Reckless or intentional attempt to reidentify anonymized data.

80 This is akin to a data processor exceeding the scope of its authority becoming a de facto controller per the GDPR.
81 See Section 11(3), PDPA.

2. Disciplinary measures set out in the Public Service (Disciplinary Proceedings) and administrative measures set out in the Public Service Division's accountability frameworks. These measures include:
   a. Counselling, warnings, or reprimands;
   b. Stoppage of increment, fines, adjustments in bonus payments;
   c. Redeployment, reduction in rank, retirement, dismissal.

Last March, following several high-profile breaches involving government entities, the government acknowledged the need to review the government's information security policies and practices, and strengthen the data security regime against current and future threats, particularly as the government was driving more pervasive sharing and use of data to improve service delivery and policy making.

As a result, Singapore's Prime Minister announced the appointment of a Public Sector Data Security Review Committee (the Committee) to review data security practices in the public sector.[82] Led by then-Deputy Prime Minister and Coordinating Minister for National Security, the Committee included private sector experts in data security and technology, as well as ministers from Singapore's Smart Nation initiative. The Committee was also tasked with reviewing the role of vendors and third parties engaged by the government and recommending technical measures, processes, and capabilities to improve the protection of citizens' data and the government's incident response capabilities. In November, following a comprehensive inspection of 336 systems in 94 agencies, the Committee made five recommendations:

1. Enhanced measures to protect data and prevent its compromise, including data minimization and storage limitation measures, the use of digital watermarking and other forensic techniques to monitor data flows, and the use of password protection and encryption;

2. Enhanced measures to detect and respond to data incidents, including by establishing a central point of contact for the public to report government data incidents, designating the Government Data Office to monitor and analyze security incidents, and implementing a standard process for incident postmortems;

3. Enhanced data security-related competency and training, including clarification of roles for managing data security and building a culture conducive to reporting incidents;

4. Increased accountability for data protection, including the introduction of organizational KPIs for data security and amending the PDPA to cover vendors and nonpublic officers who mishandle personal data; and

5. Introduce and strengthen organizational and governance structures to build a resilient public sector data security regime that can meet future needs, including the appointment of the Digital Government Executive Committee, chaired by the Permanent Secretary of SNDGG, to oversee public sector data security and the establishment of a new Capability Centre in GovTech to deepen the government's expertise in data protection technologies.

The Government accepted these recommendations and promised their implementation in 80 percent of systems by the end of 2021 and full implementation by 2023. For now, government agencies remain exempt from the PDPA.

82 Prime Minister's Office (A Singapore Government Agency Website). "Appointment of Public Sector Data Security Review Committee" March 31, 2019, https://www.pmo.gov.sg/Newsroom/Appointment-of-Public-Sector-Data-Security-Review-Committee. Accessed February 2020.

Lawful Bases for Processing

The PDPA provides for consent as the primary basis for collecting, using, and disclosing personal data, For consent to be valid, the individual must be informed of the purposes for which his or her personal data will be collected, used, or disclosed, and such purposes must be what a reasonable person would consider appropriate in a given context. Fresh consent is required to use personal data for a different purpose than the one for which consent was obtained. Consent may not be conditioned on the provision of a product or service (beyond what is necessary to provide the product or service). Where false or misleading information is provided, or deceptive or misleading practices are used, consent is not valid. Consent may be implied where an individual voluntarily provides personal data to an organization for a particular purpose and it is reasonable that the individual would do so in that circumstance.

There are many exceptions to the requirement to obtain consent under the PDPA, including where the collection of personal data is necessary for any purpose that is clearly in the interest of the individual and consent cannot be obtained, the personal data is publicly available, the disclosure is necessary for any investigation or for the provision of legal services, the personal data is collected by an individual's employer for employment purposes, and for law enforcement purposes. Two new bases for processing without consent are under review. Per the "notification of purpose" basis, an organization could process personal data without consent, where its collection, use, or disclosure is not expected to have any adverse impact on the individual.[83] Per the "legitimate interests" basis, organizations could process personal data without consent where economic, social, security, or other benefits to the public outweigh any adverse impact to the individual, and reliance on this basis is disclosed.

Other Laws

Various other general and sector-specific legislation in Singapore sets out specific data protection rules, including the Banking Act (on the disclosure of customer information by a bank or its officers), the Computer Misuse Act (on computer system hackers and other similar forms of unauthorized access or modification to computer systems), the Cybersecurity Act (establishing a legal framework for the oversight and maintenance of national cybersecurity in Singapore), the Private Hospitals and Medical Clinics Act (relating to the confidentiality of information held by private hospitals and other licensed health care establishments), and the Telecommunications Act (safeguarding end-user service information).

The Monetary Authority of Singapore (MAS) is empowered under the Monetary Authority of Singapore Act and other sectoral legislation to issue data protection-related rules for the financial sector. Examples include the Notices and Guidelines on Technology Risk Management, Notices and Guidelines on Prevention of Money Laundering and Countering the Financing of Terrorism (AML/CFT), and Guidelines on Outsourcing.

Accountability

Accountability is a fundamental principle of the PDPA, which requires organizations to ensure and demonstrate responsibility for personal data which it has collected or obtained for processing, or which it has control over. The PDPC notes that organizations today operate in an increasingly connected and competitive digital economy where individuals' online and real-world activities generate a large and growing amount of data. As such, a box-checking approach towards the handling of personal data is increasingly impractical and the PDPC undertook a pivot towards an accountability approach to managing personal data that will help organizations strengthen public trust, enhance business competitiveness, and provide

83 Organizations that wish to rely on this basis must provide the individual with appropriate notification of the purpose of the collection, use, or disclosure of the personal data, and information about how the individual may opt out, where applicable. Also, organizations must conduct a risk and impact assessment, such as a data protection impact assessment, as an accountability measure to identify and mitigate any risks when seeking to rely on the 'notification of purpose' basis.

greater assurance for customers. Singapore's shift towards accountability is already underway. In the first stage, the PDPC has introduced accountability tools such as guides to data protection by design ("DPbD"), Data Protection Impact Assessment ("DPIA") and Data Protection Management Programme ("DPMP"). As part of the second stage, in January 2019, the IMDA launched the Data Protection Trustmark (DPTM) scheme as a badge of recognition for organizations that demonstrate accountability in meeting data protection standards. This voluntary certification scheme for enterprises incorporates elements of the PDPA, international benchmarks (e.g., APEC CBPR/PRP) and other best practices, and aims to help organizations increase their competitive advantage, build consumer trust, and demonstrate sound and accountable data protection practices. Organizations may apply to IMDA for approval to participate in the DPTM certification scheme, and an independent assessment body will assess whether its data protection policies are aligned with the DPTM's requirements The DPTM certification is valid for three years and organizations may apply for recertification at least six months before the date of expiry. In the third stage, PDPC is reviewing the PDPA to reflect this shift towards an accountability approach.

Updates and Trends

The PDPA has been under review since 2017 through a series of public consultations led by the PDPC, with the latest being the public consultation on the Personal Data Protection (Amendment) Bill published in May 2020. The proposed amendments to the PDPA underscore Singapore's shift towards an accountability-based approach to data protection, to strengthen public trust, enhance business competitiveness and provide greater organizational accountability and assurance to consumers. Key areas of proposed amendments include (i) strengthening organizational accountability through the introduction of a mandatory data breach notification requirement; (ii) enhancing the PDPA's framework for the collection, use, and disclosure of personal data, to enable wider use of personal data for legitimate interests and business improvement purposes; (iii) providing greater consumer autonomy through the introduction of a data portability obligation to facilitate data flows to support innovation that benefits consumers; and (iv) strengthening the effectiveness of PDPC's enforcement powers. The amendment of the PDPA will complete Singapore's strategic shift to an accountability approach to personal data protection. These amendments were read and passed by the Parliament on October 5, 2020.

Other than changes in regulation, Singapore also promotes adoption of good data governance and accountability practices through the Trusted Data Sharing Framework to give businesses a common frame of reference when exploring data sharing partnerships. The framework guides businesses to share consumer data in a trusted and transparent way to reduce abuse and misuse. As for organizations who have specific use cases in mind and wish to explore and pilot innovative data uses with their data partners, they can also use the Data Regulatory Sandbox to consult PDPC. This helps to reduce business uncertainty in compliance to current and planned policies while informing regulators of how businesses are using data of consumers.

As a practical example of how the Trusted Data Sharing Framework and Regulatory Sandbox can be applied, Singapore's Infocomm Media Development Authority (IMDA), Personal Data Protection Commission (PDPC) facilitated data sharing between public and private sectors to build innovative data-driven solutions focused on bettering health outcomes and financial well-being, that can address the UN Sustainable Development Goals. The learnings from this data sharing collaboration was also published in the form of a Practical Guidance, allowing the wider industry to understand that data sharing can take place within a trusted governance framework and in accordance with the relevant regulations.

CREATING A TECHNICAL ARCHITECTURE FOR DATA SHARING

The technical architecture that Singapore has created for data sharing unsurprisingly mirrors its Smart Nation Framework, with specific investments made in platforms that enable data sharing for government efficiency, individual participation or engagement, and to cultivate a vibrant digital economy:

1. *Infrastructure for Government Efficiencies:* SNDGG's shift to more "Agile" modular product development has imposed new requirements and opened up more opportunities for common data infrastructure. The Government Tech Stack was created to provide agencies with key building blocks to incorporate into digital services to reduce development effort and time-to-market while easing maintenance and interoperability.[84] As Digital government "means recognizing that data is a strategic asset that underpins digital transformation, and purposefully organizing the business model of government around data," data is a fundamental piece of the Stack necessary to power digital services.[85] This ambitious goal required the government to build a coherent data architecture based on its Integrated Data Management Framework (IDMF), which included data infrastructure and new organizational constructs to support and scale data sharing.

   The Vault.Gov.SG platform is one key piece of data infrastructure that enables the Government to manage data effectively across the data life cycle stages. The Vault.Gov.SG platform, a collaboration between the Government Data Office and the Open Government Products team,[86] provides a platform for civil service officers to explore a catalogue of commonly-used government data sets, review the metadata and data dictionary, and download sample data sets (based on synthetic representative data). Once a civil service officer has found the necessary data, they can then submit a request to the appropriate authority for review. Officer requests require sign-off from their Agency's Chief Data Officer that the data is necessary for the stated purpose. The request is submitted to the appropriate authority and reviewed within seven working days. If approved, data is digitally watermarked and encrypted with project and officer IDs, before distribution to the officer, deterring leaks and providing clear traceability.

   Vault.Gov.SG is the result of an entrepreneurial effort by a team of Open Government Products engineers and the Government Data Office. Kicked off in 2018, the team endeavored to provide a proof-of-concept that data sharing between agencies could be done in days instead of months. Vault .Gov.SG was officially launched in November 2019. Officers who obtained data from Vault.Gov.SG could also make use of Analytics.gov, the Singapore Government's central analytics platform with significant processing power and commonly-used analytics tools, to analyze the data and develop models. Analytics.gov, also allows data scientists to share code with other public sector data users to accelerate the development of analytics and AI models.

   The Government Data Architecture is one of the initiatives under the Core Operations Development Environment and eXchange (CODEX), launched by Prime Minister Lee Hsien Loong in 2018.[87] CODEX provides a central set of reusable digital services

84 Khern, Ng Chee. "Digital Government, Smart Nation: PURSUING SINGAPORE'S TECH IMPERATIVE," Issue 21 Ethos: A Publication of Civil Service College Singapore, July 2019, pg. 15.

85 Mao, Daniel Lim Yew. "Bringing Data into the Heart of Digital Government" Civil Service College Singapore (A Singapore Government Agency Website), July 30, 2019, https://www.csc.gov.sg/articles/bring-data-in-the-heart-of-digital-government. Accessed December 2019.

86 Mao, Daniel Lim Yew. "Bringing Data into the Heart of Digital Government" Civil Service College Singapore (A Singapore Government Agency Website), July 30, 2019, https://www.csc.gov.sg/articles/bring-data-in-the-heart-of-digital-government. Accessed December 2019.

87 GovTech Singapore. "Engineering Digital Government, MakingLives Better," Annual Report 2018/19, https://www.tech.gov.sg/files/media/corporate-publications/FY2019/GovTech-AR-2019-Main-min.pdf. Accessed January 2020.

across the Government Technology Stack to shift public agencies from siloed or outsourced development approaches. CODEX comprises hosting platforms and micro services supported by a data layer to help agencies reduce development time and expense and ensure a common data platform across agency applications.

2. *Infrastructure for equipping people with new capabilities:* One of the Strategic Nation Projects identified in the Smart Nation vision update was the National Digital Identity project. The National Digital Identity project, focused on building the necessary infrastructure to ensure that individuals and organizations can interact digitally with both the public and private sector, has trusted data sharing at its core.[88] The project encompasses efforts to build trusted digital data repositories, unique digital identities, federated authentication, and a set of key digital services that can be embedded in wider public or private sector applications.[89] In conjunction with e-payments, these layers mirror elements of the India Stack.

The trusted data layer of the Government Tech Stack is served by MyInfo, a personal data and consent manager. MyInfo was initially built to serve a "tell-us-once" use case for government e-forms, allowing users to automatically populate certain fields while processing government transactions.[90] The platform was then successfully piloted with the banking sector to provide high fidelity government data to streamline the account or loan application process, with average application times decreasing up to 80 percent and approval rates increasing up to 15 percent due to improved data quality.[91] It has since been integrated into "almost 200 private sector and more than 150 government digital services."[92] The MyInfo Business platform is piloting the same consent and data management capabilities to accelerate digital transactions for the private sector[93] and has onboarded over 220,000 SMEs as of February 2019.[94] The MyInfo platforms are enabled by the SingPass and CorpPass identity applications. SingPass, which was initially released in 2003, provided access to a secure online portal to transact with government agencies.[95] It has been more recently complemented with SingPass Mobile,[96] a new password-less mobile application which had 420,000 users in its first ten months,[97]

88 Smart Nation Singapore, https://www.smartnation.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi. Accessed December 2019.

89 NDI {API} (A Singapore Government Agency Website), https://www.ndi-api.gov.sg/library. Accessed December 2019.

90 GovTech Singapore (A Singapore Government Agency Website). "MyInfo," https://www.tech.gov.sg/products-and-services/my-info/. Accessed December 2019.

91 GovTech Singapore (A Singapore Government Agency Website). "Businesses can tap on MyInfo to offer faster transactions for citizens," November 10, 2017, https://www.tech.gov.sg/media/media-releases/businesses-can-tap-on-myinfo. Accessed December 2019.

92 Lee, Kendrick. "GovTech's 'tell-us-once' platform eliminates tedious form-filling for citizens," National University of Singapore: Institute of Systems Science, https://www.iss.nus.edu.sg/community/newsroom/news-detail/2019/08/05/govtech-s-tell-us-once-platform-eliminates-tedious-form-filling-for-citizens. Accessed December 2019.

93 Smart Nation Singapore, https://www.smartnation.sg/docs/default-source/press-release-materials/media-factsheet---myinfo-business.pdf. Access December 2019.

94 Smart Nation Singapore, https://www.smartnation.sg/docs/default-source/press-release-materials/infographic---serving-citizens-and-businesses-better-through-technology.pdf. Accessed December 2019..

95 Smart Nation Singapore, https://www.smartnation.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi. Accessed December 2019.

96 GovTech Singapore (A Singapore Government Agency Website). "5 National Projects For 1 Smart Nation," August 7, 2018, https://www.tech.gov.sg/media/technews/5-national-projects-for-1-smart-nation?utm_medium=recommender_4&utm_source=aHR0cHM6Ly93d3cudGVjaC5nb3Yuc2cvbWVkaWEvdGVjaG5ld3MvZ2l2aW5nLWV2ZXJ5LWNpdGl6ZW4tYS11bmlxdWUtZGlnaXRhbC1pZGVudGl0eS1uZGk=&utm_content=aHR0cHM6Ly93d3cudGVjaC5nb3Yuc2cvbWVkaWEvdGVjaG5ld3MvNS1uYXRpb25hbC1wcm9qZWN0cy1mb3ItMS1zbWFydC1uYXRpb24=. Accessed December 2019.

97 GovTech Singapore. "Engineering Digital Government, MakingLives Better," Annual Report 2018/19, https://www.tech.gov.sg/files/media/corporate-publications/FY2019/GovTech-AR-2019-Main-min.pdf. Accessed January 2020.

and CorpPass, a private sector equivalent with 350,000 business switched over,[98] to use advanced authentication technologies to provide digital identity for residents and businesses.[99] Together, SingPass and MyInfo or their business equivalents, allow for an entirely digital onboarding process by providing proof of identity and verified government data to meet KYC or other compliance requirements.[100] The National Digital Identity API Portal provides application developers and partners access to the technical specifications to integrate these digital services into their applications and offers supporting tools and environments to ease experimentation and development.[101] The future of the National Digital Identity project focuses on building a federated authentication ecosystem with a number of private sector Authentication Service Providers working alongside the government within a common trust framework and across a variety of authentication forms (including QR code and facial recognition),[102] providing additional enabling digital services like digital signing and private sector consent collection, and encouraging the adoption of the project APIs to reimagine digital user journeys.[103]

Together, a trusted interface for digital government service interactions and standardized data architecture across government enable another of the Smart Nation Strategic National Projects, the Moments of Life initiative. The Moments of Life mobile application "integrates and provides relevant information and services to citizens based on their needs at key moments of their lives."[104] Using government data from various ministries and a trusted digital identity, citizens are able to register significant life events with relevant agencies (for instance, registering a newborn at birth while seamlessly applying for government child benefits and a library card for the young one) or access personalized government services (such as researching and registering interest in preschools or accessing retiree programs and benefits).[105]

3. *Infrastructure for open banking*: The first step in creating open banking infrastructure was publishing an API playbook with guidelines for API usage in the financial sector, both collaborative efforts by MAS and ABS.[106] The nearly 500 page playbook provides a comprehensive framework for API selection, implementation, usage, interpretation, and governance with data, security, and API standards, and a list of recommended APIs that "set the gold standard for regulatory advice on the topic in Asia."[107] The playbook covers nearly all the topics of similar "open banking" legislation but with its lack of specificity and focus on commercial use cases indicates MAS reluctance to guide the market's development. While the playbook espouses the value of adoption and the wisdom of standardization, even going

98 GovTech Singapore. "Engineering Digital Government, MakingLives Better," Annual Report 2018/19, https://www.tech.gov.sg/files/media/corporate-publications/FY2019/GovTech-AR-2019-Main-min.pdf. Accessed January 2020.

99 Smart Nation Singapore, https://www.smartnation.sg/what-is-smart-nation/initiatives/Startups-and-Businesses/corppass. Accessed December 2019.

100 NDI {API} (A Singapore Government Agency Website), https://www.ndi-api.gov.sg/library/trusted-data. Accessed December 2019.

101 NDI {API} (A Singapore Government Agency Website), https://www.ndi-api.gov.sg/about. Accessed December 2019.

102 NDI {API} (A Singapore Government Agency Website), https://www.ndi-api.gov.sg/library/trusted-access, Accessed December 2019.

103 NDI {API} (A Singapore Government Agency Website), https://www.ndi-api.gov.sg/library/trusted-services, Accessed December 2019.

104 Smart Nation Singapore, https://www.smartnation.sg/what-is-smart-nation/initiatives/moments-of-life/faq. Accessed December 2019.

105 Smart Nation Singapore, https://www.smartnation.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/moments-of-life-initiative. December 2019.

106 Monetary Authority of Singapore. "Singapore's FinTech Journey—Where We Are, What Is Next"—Speech by Mr. Ravi Menon, Managing Director, Monetary Authority of Singapore, at Singapore FinTech Festival—FinTech Conference," November 16, 2016, https://www.mas.gov.sg/news/speeches/2016/singapore-fintech-journey. Accessed December 2019.

107 Rothwell, Graham. "THE BRAVE NEW WORLD OF OPEN BANKING IN APAC: SINGAPORE," Accenture, September 27, 2018, https://bankingblog.accenture.com/brave-new-world-open-banking-apac-singapore?lang=en_US.

so far as to note a number of relevant standards, the playbook does not suggest a specific standard, much less mandate adoption or prescribe a standard.[108]

This movement into infrastructure was continued in 2017, when MAS launched the Financial Industry API Register to serve as an updated and universal landing site for Open APIs and developer sites available across the financial services industry.[109] The register provides access to both transaction APIs that provide sensitive client data and require authentication, as well as information APIs that contain nonsensitive data like product offerings or ATM locations with lower authentication thresholds. The register currently provides access to over 500 APIs available from 5 banks with DBS bank leading the way with more than 200 APIs and partnerships with more than 50 entities. Interestingly, it also includes access to MAS's own developer APIs which provides access to MAS monthly statistics bulletin APIs,[110] as the organization has invested in building its digital expertise and expanded available APIs from 12 at start to over 40 today.[111]

The next infrastructure project was intended to take some of the same principles of the Financial Industry API register across borders. MAS, along with the World Bank's International Finance Corporation, and the ASEAN Bankers Association, launched the ASEAN Financial Innovation Network and its API Exchange Platform (APIX) in 2018 to allow Financial Institutions and FinTechs to discover one another in a neutral marketplace, design collaborative experiments to test digital solutions in a shared sandbox, and deploy those solutions rapidly.[112] The marketplace platform is cloud-based and cross-border in keeping with its goal of providing a space for financial service providers across South East Asia to innovate and collaborate. The platform, which includes structured methods for integration and defines relevant standards, plans to support an array of solutions for use cases such as customer onboarding, credit scoring, payments, and compliance.[113] The platform, also, includes discussion boards and messaging to encourage a learning community among participants with safeguards to ensure information around product offerings or problems from FinTechs or financial institutions are not unknowingly shared with competitors.

For FinTechs, participation in the program is not geographically limited, opening up a variety of potential markets to providers across the globe as long as their applications are accessible by API and the APIs are continuously supported to enable active experimentation.[114] APIX actively monitors API performance to ensure compliance but is encouraging FinTech adoption with cloud service provider credits along with access to the sales opportunities and testing tools the platform provides.[115]

108 Monetary Authority of Singapore. "Financial Industry API Register," https://www.mas.gov.sg/development/fintech/financial-industry-api-register. Accessed December 2019.

109 Monetary Authority of Singapore. "Financial Industry API Register," https://www.mas.gov.sg/development/fintech/financial-industry-api-register. Accessed December 2019.

110 Monetary Authority of Singapore. https://secure.mas.gov.sg/api/Search.aspx. Accessed December 2019.

111 Monetary Authority of Singapore. "MAS Launches First Set of Data APIs," November 11, 2016, https://www.mas.gov.sg/news/media-releases/2016/mas-launches-first-set-of-data-apis. Accessed December 2019.

112 Monetary Authority of Singapore. "API Exchange (APIX)," https://www.mas.gov.sg/development/fintech/api-exchange. Accessed December 2019.

113 FinTech News Singapore. "ASEAN Financial Innovation Network: An Industry Fintech Sandbox to Drive Innovation and Inclusion" November 17, 2017, https://fintechnews.sg/14574/fintech/asean-financial-innovation-network-support-financial-services-innovation-inclusion/.

114 APIX. "APIX Open Innovation Platform & Sandbox," November 15, 2018, https://apixplatform.com/static/apix-news/batch55.html. Accessed December 2019.

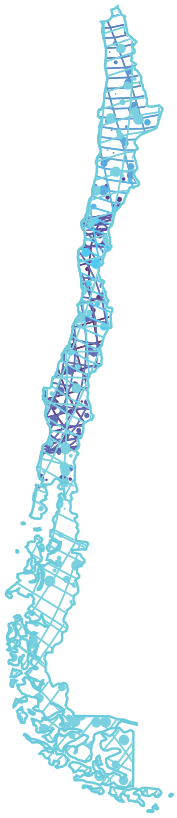
115 APIX. "About Us," https://apixplatform.com/static/about/. Accessed December 2019.

The AFIN Exchange furthers MAS's goal of catalyzing new business opportunities for its domestic data-driven financial technology providers and is in keeping with its wider efforts to standardize data governance policy within the region. While the core idea is similar to the register and sandbox MAS has set up domestically, the standardization of integration and authentication are important evolutions in bringing the solution closer to equivalent implementations from the UK and other countries who have set standards across the data sharing journey and mandated compliance.

Going forward, there is hope that the new data portability provisions as part of the Personal Data Protection Commission's review of the Personal Data Protection Act may widen Singapore's open banking aperture. Indeed, MAS has very recently indicated that they will be implementing a data aggregation portal in 2020 in line with what was proposed by the PDPC and Competition and Consumer Commission of Singapore discussion paper on Data Portability as part of the open banking program.[116] The portal would allow consumers to aggregate financial data from a wider set of sources, including investment managers, insurers, and banks, and share that information with traditional financial services providers and FinTechs.[117] While details on how this will be instituted are not yet clear, it has the potential to set a de facto standard for data sharing in open banking in a way that MAS avoided until now. Consumer protection gaps are still a risk to the continued success of open banking implementation, as recent government data breach incidents, in particular, have shown, but are the focus of many other policy, education, and enforcement initiatives across the Smart Nation Vision.

116 Lee, Jamie. "Consumers to be able to aggregate and share financial data next year," *The Business Times*, October 25, 2019, https://www.businesstimes.com.sg/banking-finance/consumers-to-be-able-to-aggregate-and-share-financial-data-next-year. Cited Discussion Paper available: https://www.cccs.gov.sg/resources/publications/occasional-research-papers/pdpc-cccs-data-portability

117 Lee, Jamie. "Singapore digs deep to bring true financial liberalisation," *The Business Times*, November 11, 2019, https://www.businesstimes.com.sg/hub/sff-x-switch-2019/singapore-digs-deep-to-bring-true-financial-liberalisation. Accessed December 2019



CHILE: DATA SHARING FOR GOVERNMENT EFFICIENCY

BACKGROUND

Chile has taken a comprehensive approach to social protection focused on several dimensions of risk that arise from poverty, starting in the 1980s. Economic reforms under the government in the 1970s impacted the most vulnerable—between 1973 and 1980, the number of state-controlled companies fell from 300 to 24, with big cuts to budgets for infrastructure, housing, education, and social security.[118] This led to high rates of poverty, with nearly 17 percent of the population classified as indigent by 1987. The government's response to these changes was the introduction of a social protection regime, which has expanded over the decades and now supports citizens in times of unemployment, ill health, old age, disability, extreme poverty, and other vulnerable conditions.

After Chile's transition to a democracy, the government built on and expanded efforts to ensure social protection in the face of high inequality. Through a 2004 law, Chile established the *Chile Solidario* initiative, which combined a system of distributed public benefits to the extreme poor with active psychosocial support through social worker intermediation and outreach. *Chile Solidario* relied on accurate data for identifying and reaching those in need. However, it was preceded by a fragmented safety net: a mapping exercise undertaken in 2002 found 142 programs with poverty reduction objectives being run by 33 different agencies. This reflected a system that undermined government effectiveness. Consolidating these efforts was key, and the government created an integrated social information system (SIIS) mandated by law under *Chile Solidario*, to link these several public databases that collected citizens' data. To link several

118 Davies, Richard (2020). *Why is inequality booming in Chile? Blame the Chicago Boys.* Retrieved 10 November 2020, from https://www.theguardian.com/commentisfree/2019/nov/13/why-is-inequality-booming-in-chile-blame-the-chicago-boys.

disparate databases managed by different public agencies, Chile used the national ID number—*Rol Unico Nacional*—alongside the *ClaveUnica*—a national Digital ID. This enables data gathered by different ministries to be linked together into a single large registry, which is then used for enhancing public service delivery.[119]

As of 2019, the integrated social information system (RIS)—which comprises the Social Registry of Households[120] and the Intended Public Beneficiaries registry—contains data shared by 43 state agencies at all levels of government, covering nearly 75 percent of Chile's population. This intersectoral database determines eligibility for about 80 social protection programs and collects self-reported data, administrative data, and geographic data from different sources.

Increased data sharing in Chile rests alongside a regime that enshrines protections for citizens' data. Chile was the first Latin American country to enact a data protection law in 1999; a 2018 amendment to that law enshrined data protection as a fundamental right alongside the right to privacy under Article 19 of the Chilean constitution. Civil courts enforce data-related disputes, although a current data protection bill in parliament seeks to establish an independent data protection agency.

Chile's experience with data protection and data sharing over the last two decades in Latin America have important lessons for data governance. Chile has implemented intersectoral data sharing through institutional arrangements between public sector agencies using a digital ID for interoperability. This provides key lessons for other countries who may not have the luxury of starting from scratch to implement a whole-of-government approach to data sharing. Chile also demonstrates the experience of a country with strong constitutional grounding and laws for personal data protection, but one that uses civil courts for enforcement, which may be burdensome for some to seek relief.

This case study is structured in three subsequent sections. The first section looks at the evolution of the integrated social household registry and its data sharing mechanism. The second section focuses on the legal and constitutional underpinnings of data protection in Chile, and the experience of using courts as enforcers. The third section abstracts lessons for data governance frameworks from Chile's experience.

KEY FEATURES OF DATA SHARING

ADVANCING INTERSECTORAL DATA SHARING BY LINKING SEVERAL PUBLIC DATABASES

Chile's experience with targeting social protection programs through an integrated approach to vulnerability preceded the rapid uptake of digital technologies across various government departments. As ministries across the government digitized their services as part of different national *Agenda Digital* strategies, data sharing across different ministries, especially to run the integrated social information system, became key. While deciding to set up the registry to aid *Chile Solidario*, the government chose to leverage existing data sources available within different ministries.

Chile's system of data collection has evolved over the years with increasing digitization of public services. The first Ficha CAS in the 1980s was administered through a paper-based system by enumerators at the local level and contained only self-reported data. Data collection was used primarily for program implementation at the municipal level, without the ability to aggregate data across territorial boundaries. CAS 2—an update to the first Ficha CAS that continued until

119 Galasso, E. (2015). Reflections on social protection and poverty alleviation from the long term impact of *Chile Solidario*. Retrieved 10 November 2020, from https://blogs.worldbank.org/developmenttalk/reflections-social-protection-and-poverty-alleviation-long-term-impact-chile-solidario.

120 Registry of Households: http://www.registrosocial.gob.cl/.

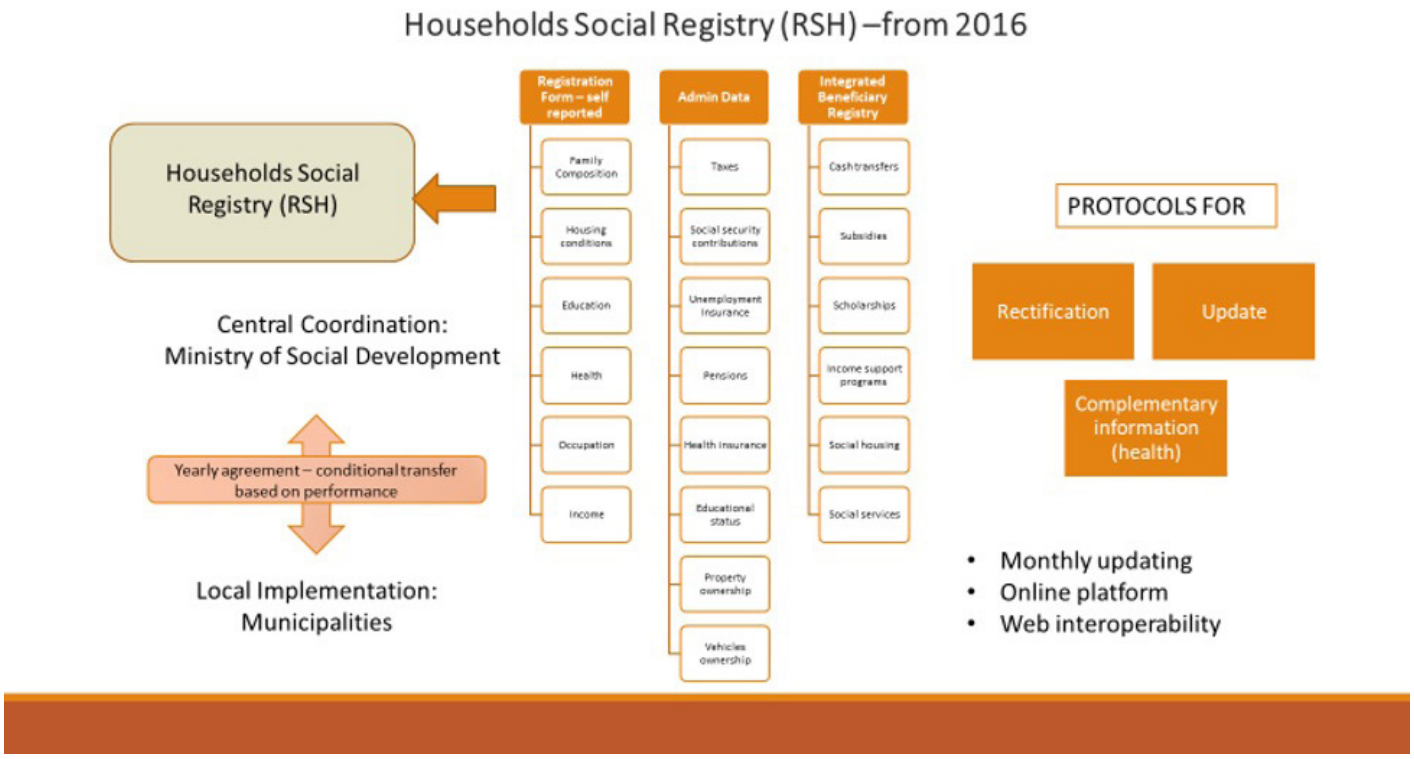
2006—contained self-reported data that was collected and digitized, with a basic mechanism for electronic data exchange manually. Municipalities collected and reported aggregate data from their data gathering efforts, under this model.

With increased political will for digitization through the early 2000s and 2010s, the systems that fed into the integrated social information system increased in both number and complexity. This enabled the government to integrate different data sets to identify vulnerable households better and refine their targeting of social protection programs for that purpose. The latest version of Integrated Social Information System is the result of several iterations by the Government of Chile, and integrates GIS data to provide granular, spatial maps of vulnerability for the purposes of targeting.

The comprehensive registry now has over 13 million entries, amounting to over three quarters of the population. Citizens can self-report information when applying for public services through local municipal offices to update their information on income, occupation, education, and family composition on the Registro de Social Hogares.

The current information interface is integrated and dynamic: citizens can apply for over 80 social programs, update their information, and access their information online or through local offices. Self-reported information includes housing, education, health, family composition, occupation, and income. Data drawn from other administrative systems include information on taxes, unemployment insurance, social security and pensions, health insurance, and asset ownership.

Figure 6: Household Social Registry



Source: Veronica Silva Villalobos, Social Protection and Jobs Global Practice, The World Bank Group

As of 2019, the system contains data from 43 public sector agencies and helps determine eligibility for 80 public programs. The registry pulls data from three different data sources—self-reported data by beneficiaries, administrative data from several ministries, as well as data from the integrated beneficiary registry that comprises details from different social protection programs run by the government. Overlaying GIS data in the current system allows targeting granularity. The information is updated monthly, on terms agreed to by the institutions sharing data. Monthly updating allows for agencies to accurately vet the administrative data under their purview and make it available for the purpose of benefits allocation. This ensures data accuracy. Salient features of the registry's functioning are described in the next section.

Leveraging different data sources requires a system of strong institutional arrangements and coordination between different actors. Chile's SIIS, the predecessor to the RIS, was housed under the Ministry of Planning, which has, over the years, transformed to become the Ministry of Social Development and Family. This provides key benefits.

First, the agency housing the integrated registry had the capacity for coordination and standardization across sectors involved in the central and subnational governments. While the registry is centralized and operates as a virtual social registry, tasks such as data collection are still completed by local municipalities. Therefore, intensive coordination among all relevant stakeholders to seek their buy-in, and formalizing relationships between them within the government became essential for successful implementation. The mechanism that the Ministry of Social Development and Family currently utilizes to formalize these relationships is one of interinstitutional data sharing arrangements. These agreements signed between public sector agencies and the Ministry of Social Development and Family determine the nature of data shared as well as protocols around when the data is updated. This enshrines protection for individuals' data as well—in negotiating interinstitutional agreements, agencies delineate sensitive noncritical data from other data that can be shared with ease, enabling better public service delivery while protecting rights.

Updating data within this intersectoral sharing mechanism is critical for effectiveness, as a system that bases determination of benefit eligibility on a static data set will face challenges in reaching those most in need—and those struggling due to seasonal or transitionary poverty. Indeed, this was amongst the most common criticisms under the Ficha CAS 1 and Ficha CAS 2 systems.[121] To overcome this, the registry updates every month with new data from systems that share their data, except for cases where interinstitutional arrangements dictate otherwise.

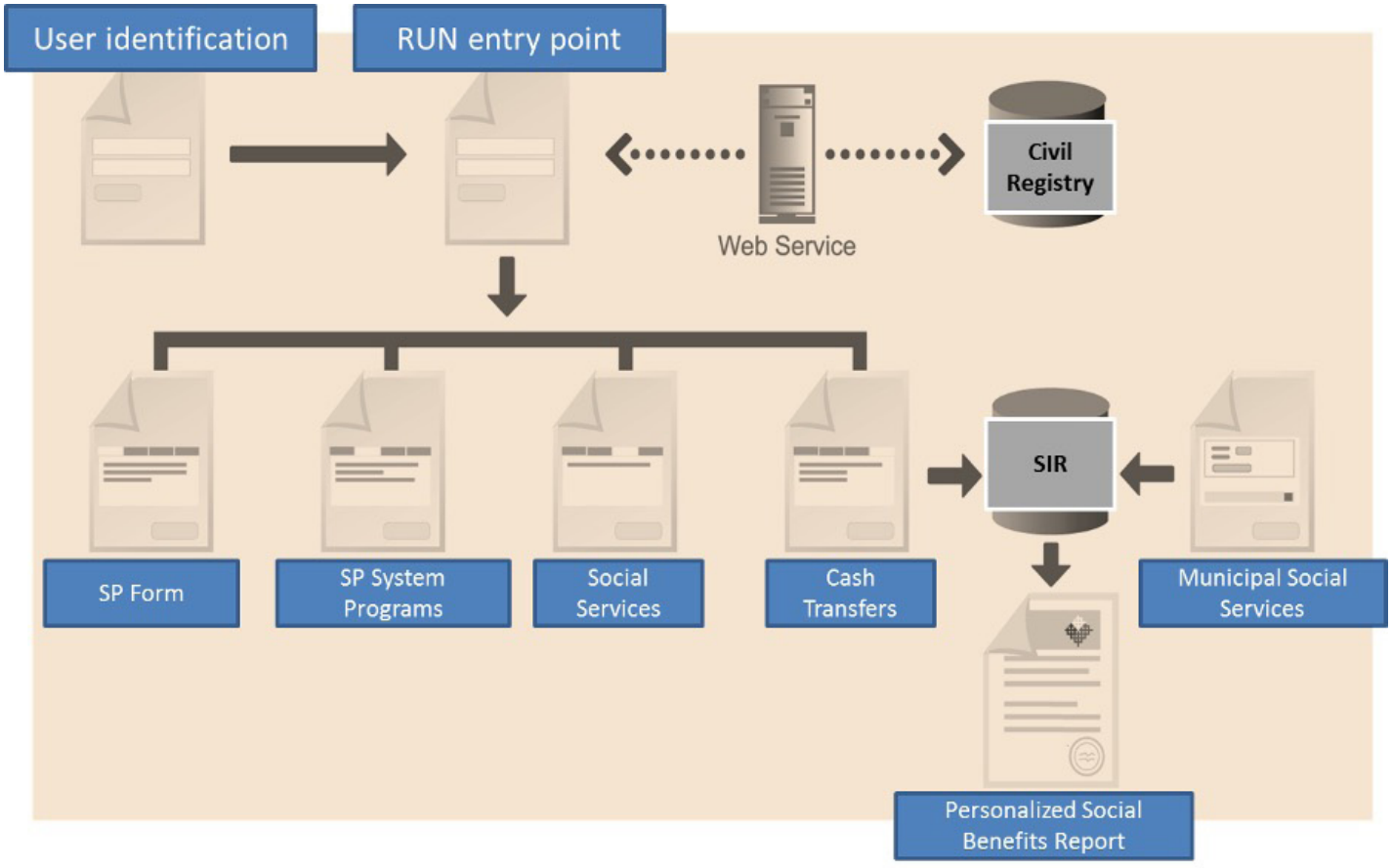
A key element of integrating data sets across different sources for the same individuals is the ability to link data on them across different databases. This requires a unique identification mechanism, which in Chile's case is administered by a separate agency within the Ministry of Justice and Human Rights within the government—the Civil Registry. The Civil Registry (*Servicio de Registro Civil e Identificación*) administers the registration of all citizens in Chile. The registry has long issued a physical card—*Cédula de Identidad*—to enable citizens to prove their identity to public and private institutions, and to vote. The physical card is complemented by a single national ID number, which serves as the *Rol Único Tributario* (RUT), a tax identification number, and the *Rol Único Nacional* (RUN), the number in the national civil register.

The current registry uses a software application developed in-house to link the various administrative databases held by different public sector agencies using the common *Rol Único Nacional* as a common identifier across different databases. The current

121 Carine Clert and Quentin Wodon (2001). The Targeting of Government Programs in Chile: A Quantitative and Qualitative Assessment. World Bank Policy Research Working Paper.

iteration of *ClaveÚnica* offers a straightforward web authentication model. Citizens are required to register for the *Cédula de Identidad* and request for an activation code that is mailed to them in order to activate their digital ID. They use this in conjunction with their *Rol Único Nacional* to create their digital identity on the government website. They then use that profile to activate their ability to receive services, including updating their self-reported information on the *Registro de Social Hogares*. A brief summary of the architecture of the current system and the interface with the Civil Registry is described below in the figure.

Figure 7: Summary of the Civil Registry System Architecture



Source: Veronica Silva Villalobos, Social Protection and Jobs, The World Bank Group

DATA PROTECTION

Data Protection as a Constitutional Right

Article 19 of the Chilean Constitution recognizes, protects, and guarantees the right to privacy of all people. Chile was the first Latin American country to pass a comprehensive data protection law in 1999. Chile's Law No. 19.628 applies to personal data, defined as identified or identifiable information that pertains to a natural person. This law also establishes responsibilities and limitations to the processing of personal data. Law No. 21.096 amended the constitution in 2018, establishing the protection of personal data as a constitutional right under article 19.4.

> Article 19.- The Constitution ensures to every person:
>
> 4° The respect and protection of private life and the honor of the person and his family, and furthermore, the protection of personal data. The treatment and protection of this data will be put into effect in the form and conditions determined by law.

The explicit inclusion of the right to data protection imposes affirmative duties on third parties regarding the treatment and protection of data, as opposed to the mere exclusionary right granted through the right to privacy already enshrined under Article 19 of the Constitution.

The current law in force is not based on any international instrument on privacy or data protection in force, such as the OECD guidelines, Directive 95/46/EC, EU General Data Protection Regulation, or the European Convention on Human Rights and Fundamental Freedoms.

THE PERSONAL DATA PROTECTION LAW (19.628/1999)[122]

Key features of the law are in line with current data protection principles enshrined in the GDPR, despite Chile's law being enacted in 1999. Key features of the law are highlighted below.

Scope

Data processing is broadly defined as any operation(s) or procedures, automated or not, that make it possible to collect, store, record, organize, prepare, select, extract, match, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use it in any form. The law covers both government entities as well as private sector providers under its ambit.

Finality Principle

The Chilean legal system abides by the finality principle, which states that the use of data cannot exceed the remit of the purposes for which it was collected. This is similar to the purpose limitation principle under the GDPR and other new and emerging data protection regulations. To comply with the law (19.628), all government bodies and agencies in Chile must register databases containing personal data with the Civil Registry and provide a legal basis for their existence, purpose, data types stored, and stakeholders implicated. The agencies are required to inform the Civil Registry and identification service of any changes to that information within 15 days. No private sector equivalent exists.

Protections for Sensitive Data

The law distinguishes between ordinary data and sensitive data. Sensitive data may only be processed with consent from the data subject or where the processing is necessary for a public purpose, such as the determination of health benefits. In addition to sensitive data under the personal data protection law, sector-specific laws apply to certain other kinds of personal data, as described in the following section.

122 The full draft text of the law is available in Spanish online: https://www.bcn.cl/leychile/navegar?idNorma=141599.

The law takes a functional approach to defining protections. There are no distinct duties for owners, controllers or processors; all provisions apply across them. Government agencies are limited by the remit of their legal authority. However, the law is not explicit on the regulation of private sector aggregation of sensitive and nonsensitive data.

Rights of Data Subjects

Under 19.628, people who provide their personal data enjoy: a right of modification, if the personal data is erroneous, inexact, equivocal, or incomplete; a right to block processing when the individual has voluntarily provided his or her personal data but no longer wants it to be processed; a right of cancellation or elimination of expired data; a right to access their data for free, and the right to oppose the use of their data for advertising, market research, or opinion polls.

Under the right to access, a data subject may make a request to an institution holding their data to provide their data, as well as information about how it was collected; the purpose for storing it; and the nature of its ongoing use.

Data subjects may not exercise their rights of modification under certain circumstances, such as when it would affect government supervisory functions, the confidentiality or secrecy established in legal or regulatory proceedings, or national security.

Damages

The law provides for monetary fines of up to 5,000 UTM[123] for improper processing of data. Judges adjudicate claims based on general tort and contract law principles and decide the amount of compensation based on the specific circumstances of the case. The fines can range between US$60 (50,000 Chilean Peso) and US$600 (500,000 Chilean Peso); they are at times higher, when financial data is under question. The law has not been tested by cases involving large data breaches.

There is an established redress procedure if the person responsible for the personal data registry or bank fails to respond to a request for access, modification, elimination or blocking of personal data within two business days, or refuses a request on grounds other than the security of the nation or the national interest.

SECTORAL LAWS

Beyond Law 19.628, Chile has sector-specific laws that relate to data protection. Financial data (personal financial information) is governed by Law 19.496 and imposes a five-year term limit for the communication of confidential information after the financial obligation has ended. Law 19.799 in relation to electronic signatures ensures the privacy of signatories. Personal data is required to be deleted or cancelled when there are no legal grounds for its storage or after data has expired.

Law N° 3/1978, the General Law of Banks, established the confidentiality of transactions that individuals conduct with and through banks. The law distinguishes transactions covered by secrecy, which in principle are subject to an absolute prohibition of disclosure, and transactions covered by reserve, which are subject to a significant limitation on the possibility of disclosing the transaction (a disclosure may only be made to persons that can demonstrate a legitimate interest and only if it cannot be foreseen that the knowledge of the disclosed facts may cause property damage to the customer).

Law 20.584/2012 regulates the rights and duties of individuals in the context of health care. It says that all information contained in patient files or documentations of medical treatments are sensitive data and establishes the obligation of health care professionals to maintain patient data confidential and to comply with the principle of purpose limitation. It also includes certain cases when such data can be delivered, partially or totally, to the data subject and to other individuals or entities.

123 UTM stands for "Unidad Tributaria Mensual," a monthly tax unit that is used generally for the payment of taxes, fines, or customs duty in Chile. The measure of this unit is constantly adjusted for inflation.

Law 20.285, Chile's Freedom of Information Law, allows for access to government-held information, which provides for a level of accountability.

Sensitive data Law 20.521/2011 amended Law 19.628 to prohibit credit risk predictions or assessments based on subjective data.

Law 20.575/2012 established the 'purpose principle' in the processing of personal data for commercial risk assessment for the credit granting process.

INSTITUTIONAL ARRANGEMENTS TO EFFECTIVELY ENACT DATA PROTECTION

Weaknesses in the current law include the lack of adequate supervisory mechanisms and lack of clarity on how it may apply to cover the electronic processing of information. To remedy these shortfalls, Chilean lawmakers have been working to reform the law for several years, proposing the creation of a personal data protection agency to ensure compliance with legal obligations.

As there is no special data protection authority in Chile, data protection is addressed by civil courts. Cases have not explicitly dealt with data loss in digital forms, although there was a case that held Santander Bank liable for disposing paper-based financial records in a landfill.[124] Electronic data breaches have not been considered in the relatively thin body of cases that have been considered under Law 19.628.

The National Congress of Chile is considering a new Data Protection Bill. This bill includes additional rights for data subjects, introduces provisions on consent and new obligations for data controllers, and amends the definitions of sensitive data to include biometric data. This bill seeks to align with Convention 108 and the GDPR.

The Data Protection Agency would be housed within the Chilean Transparency Council, the agency responsible for both data protection and freedom of information laws. The Transparency Council is the most experienced agency with respect to data protection and fully autonomous within the Chilean regulatory framework, which should help ensure competence, resourcing, and independence.

Chile is seeking an upgrade to its laws that will secure an adequacy determination from the EU.

Reforms will be, in large part, based on the 2017 Standards for Data Protection for the Ibero-American States from the Ibero-American Data Protection Network, an effort to harmonize data protection laws across Latin America. One core objective is "to make the flow of personal data between Ibero-American States and beyond their borders easier, in order to contribute to the economic and social growth of the region."

RECENT DEVELOPMENTS

Chile has initiated several efforts to capitalize on the potential of the digital economy. The Government's Digital Transformation Strategy (2018) has three objectives: to improve public services for citizens and businesses; to engage in evidence-based policy making; and to mainstream the digital transformation across government and the economy. Chile recently adopted a Presidential Instructive on the Digital Transformation of the Administration and the Development of a new Digital Transformation Strategy for the State through The Digital Transformation Law, Law 21.180 (November 11, 2019).[125] The law seeks to make 80 percent of government services available online by 2021; 100 percent by 2023. Further, Law 21.180 establishes digital government services as default, with paper-based transactions only available when the

124 State of Privacy Chile (2019). Privacy International. Retrieved from https://privacyinternational.org/node/28#dataprotection.

125 OECD (2019), Digital Government in Chile—A Strategy to Enable Digital Transformation, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/f77157e4-en.

lack of digital access and skills justifies it. The law revises the legal and regulatory framework for digital government to accelerate digital integration and intragovernmental interoperability.

Chile's recent Digital Transformation strategy identifies the digital identity among its six lines of action. This has been bolstered by Presidential Instructions in 2019 that create a roadmap for more than 300 central government agencies to adopt the *ClaveUnica* as their sole authentication mechanism. At present, *ClaveUnica* is used primarily for browser-based web authentication and functional IDs are still used by some public sector agencies. The policy and strategy-setting function to enable full digitization and integration across the government has been given to a specialized body—MINSEGPRES—*Ministerio Secretaria General de la Presidencia*. This line ministry is in charge of relationships with Congress and the process of discussing and approving bills. The Ministry as a team works on this agenda, and the MINSEGPRES has played a leading role in championing data sharing within the highest levels of government since the 1980s and helped galvanize political will amongst all participating ministries. Operational coordination for this effort is led by the Civil Registry, which will work with other ministries to integrate the digital ID to simplify e-government procedures to improve public service delivery.

Complete integration of the *ClaveUnica* is also expected to allow citizens to carry data wallets, where they will be able to view an audit trail of organizations that have collected and used their data and in what capacity. At this moment, data on user experience of these wallets is unavailable as they have yet to be implemented.

Internationally, through its participation in the Digital Economy Partnership Agreement (DEPA) with Singapore and New Zealand, Chile seeks to promote digital trade through e-invoicing, cross-border data flows, AI, and digital ID. Chile has also taken steps to prohibit data localization requirements that impede cross-border data flows. These efforts have attracted private sector investment—Google, for instance, recently expanded its data center in Chile.

MAURITIUS: DATA SHARING FOR ECONOMIC GROWTH

BACKGROUND

The economic transformation of Mauritius—an island nation of fewer than 1.5 million—from a monocrop-based economy with negative growth only a few decades ago to one of the fastest growing economies in Africa has been attributed to good macroeconomic policy, strong public and private institutions and productive interactions between them, and emphasis on trade-led development.[126] Between 1970 and 2009, Mauritius averaged five percent growth in real GDP and diversified to become a strong, dynamic economy.[127]

Over the last decade Mauritius has continued its economic success story, maintaining strong average growth rates and emerging as Africa's most mature digital market.[128] The information and telecommunications (ICT) sector has emerged as a third main pillar of the modern Mauritian economy—along with tourism and the financial sector—and now accounts for approximately six percent of GDP growth and employs 25,000 people.[129]

The growth of the ICT sector has been anchored by a National Strategic Plan since 1998 and renewed every three to five years, providing significant policy guidance to drive the development of the country's knowledge economy and to respond to the rapid changes in the technology sector. This helped drive the country's digital transformation in a number of ways:

- Massive investment in internet connectivity: Mauritius Telecom has invested more than Rs 5 billion (approx. US$75m) to roll out fiber across the island and, in 2018, became only the sixth country in the world with 100% Fiber to the Home (FTTH),[130] enabling individuals to benefit from broadband speeds of up to 100 Mbit/s at some of the most affordable rates in Africa.[131]

126 https://siteresources.worldbank.org/AFRICAEXT/Resources/Mauritius_success.pdf, p.3.

127 African Center for Economic Transformation. "Mauritius Transformation Profile" http://africantransformation.org/2014/02/07/mauritius/. Accessed December 2019.

128 BuddeComm Telecomms Maturity Index. January 3, 2019, https://www.budde.com.au/Research/Global-Telecoms-Maturity-Index-Top-20-Countries. Accessed December 2019.

129 Economic Development Board of Mauritius, https://www.edbmauritius.org/node/19. Accessed December 2019.

130 ITU News. "The digital transformation of Mauritius: Q+A with Minister Sawmynaden," August 29, 2019, https://news.itu.int/the-digital-transformation-of-mauritius-qa-with-minister-sawmynaden/. Accessed December 2019.

131 Alliance for Affordable Internet. "Affordability Report: Regional Snapshot—Africa," https://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2019/12/AR2019_Africa-Regional_Screen_AW.pdf. Accessed January 2020.

- Invested extensively in building the digital capabilities of its people: Starting in 2006, the National Computer Board (NCB) began to implement a universal ICT Education Program, making training available to all Mauritians to learn how to use the internet and through which the internationally recognized Computing Core Certification was offered. This broad-based training was meant to build a more inclusive e-government and ensure citizens could avail themselves of the rapidly expanding offering of tech-enabled public services. Additionally, in 2014 the government set up the ICT Academy to build its own ICT talent pool. The Academy is set up as a public-private partnership in which the government covers 45 percent of the cost. The Academy offers internationally recognized industry-led ICT certification courses such as those provided by multinational ICT companies such as Microsoft, Oracle, CISCO, and SAP across a wide range of ICT industry needs including cybersecurity, software development, and so on.[132]

- Innovation Ecosystem: The country has invested in creating an innovation ecosystem, particularly in the financial services sector, where Mauritius has positioned itself to be the gateway to the African market. To effectively support innovation in the financial sector, the government has supported regulatory sandboxes and institutions like the Mauritius Africa FinTech Hub, which provides a ecosystem where entrepreneurs, corporations, governments, tech experts, investors, financial service providers, and researchers can collaborate to build financial services products for the African market.

As it has digitized its economy, Mauritius has also been a regional leader in developing the policies, institutions, and architecture for facilitating the exchange of data between government ministries and between the government and business. This effort has been shaped predominantly by an effort to digitize government services, drive trade, and create a strong innovation ecosystem for businesses and entrepreneurs. Importantly, the Government of Mauritius has enhanced the National Strategic Plan with a number of pieces of legislation that have enabled the country to foster a competitive and trusted digital ecosystem, making Mauritius an attractive market for ICT investments and tech-enabled business process outsourcing (BPO) and increasing the country's participation in digital trade.

These complementary—but not fully unified—policy and legislative efforts have included specific steps to expand the value of data in ways that align with the country's economic growth strategy while also ensuring data protection and privacy. Most notably, these efforts include:

1. *Adoption of its Data Protection Act 2017 (DPA 2017)*, which made Mauritius the first country in the southern hemisphere to update its data protection legal regime to come into compliance with the General Data Protection Regulation (GDPR);

2. *Implementation of InfoHighway*, a government data exchange layer that customized and adapted Estonia's X-Road model for Mauritius and helped connect basic registries—supported through an MoU with Estonia's eGovernance Academy (eGA);

3. *Adoption of the National Open Data Policy in 2017* and the subsequent creation of Open Data Mauritius, a portal that houses and provides links to government data sets.

132 Oolun, Krishna; Ramgolam, Suraj; and Dorasami, Vasenden. "The Making of a Digital Nation: Toward i-Mauritius," World Economic Forum, The Global Information Technology Report 2012, http://www3.weforum.org/docs/GITR/2012/GITR_Chapter2.2_2012.pdf. Accessed December 2019.

KEY FEATURES OF DATA SHARING

CREATING THE POLICY AND REGULATORY ENVIRONMENT FOR DATA SHARING

The Digital Government Transformation Strategy 2018–2022 provides directions to accelerate public sector digitization to enhance operational effectiveness and efficiency.[133] The Strategy notes "how critical it is to use and reuse data to support the work of Government, to optimize, transform, and create better government services and to achieve large-scale business optimization that improves effectiveness." The Strategy lays out twelve key principles for achieving the country's digital transformation goals, including three which specifically address how data is governed: (1) Reiterating the country's commitment to its Open Data Policy, (2) Emphasizing data-driven decision-making and policy formulation, and (3) Establishing the "Once-Only Policy" for Mauritius, which mandates, "Capture data only once from citizens and stakeholders and reuse the data (e.g., copy of IDs, proof of address, birth/marriage/death certificate) if it is already available within government."

Open Data

Building upon a World Bank-supported Open Data Readiness assessment conducted in 2015, the Mauritian Cabinet approved the National Open Data Policy in 2017, which established an "Open by Default" position for all government data except when dealing with personal data or data with a national security dimension. More specifically, the policy outlined the instances when the National Open Data Policy provides exception to the "open" classification:

- They contain any personal or sensitive information as per the Data Protection Act;
- they are classified as confidential under the Government Security Instructions;
- they have a public safety or national security dimension;
- they are covered by third party-rights; and
- they are reworked by the ministries and departments, to produce value-added services for specific customers.

The Open Data Policy is intended to "create value out of the release of government data sets" and is considered a "bedrock" for innovation, which is seen as a key driver of the country's future economy.[134] At the time of approval, the Government of Mauritius had identified 25 data sets that would be available immediately. This number has since grown to over 250 with more than a quarter of those being updated within the last year.

The national policy also stipulated that all data sets would be governed by The Creative Commons Attribution 4.0 International licence which allows users of Open Data to use, reuse, and redistribute the data provided that appropriate Attribution clauses are included in the data sets by the users. The Creative Commons Attribution 4.0 International licence ensures that the supplier of data continues to hold copyright on the data while allowing the users to use, reuse, and redistribute the data freely or even commercially.[135]

Data Protection

Mauritius adopted its first comprehensive data protection with a 2004 Data Protection Act which came into force in February 2009. In the same year, Mauritius adopted Data Protection Regulations which

133 Government of Mauritius, Central Informatics Bureau. "Digital Government Transformation Strategy 2018–2022" http://cib.govmu.org/English/Pages/digitalgovernment.aspx. Access December 2019.

134 Dolan, Jonathan. Notes from interview with Data Protection Commissioner of Mauritius, February 26, 2020.

135 Ministry of Information Technology, Communication, and Innovation, http://mtci.govmu.org/English/Documents/2017/Communique/Press%20Communique/Mauritius%20Open%20Data%20Policy%20May%202017.pdf. Accessed December 2019.

supplemented the DPA 2004 by creating the rules, processes, and fees for registering as a data controller and created the Data Protection Office, under the aegis of the Prime Minister's Office, led by the Data Protection Commissioner, who is responsible for enforcement. Much of the data protection-related case law[136] based on the earlier 2004 Act was specifically concerned with the protection of personal data in connection with identity-related information such as fingerprints and other biometrics in connection with Mauritius' National Identity Card Act, Act 60 of 1985.[137]

In June of 2016, Mauritius became the second non-European state to ratify the Council of Europe's Convention 108 (and its additional protocol on supervisory authorities and transborder data flows).[138] The 2017 Data Protection Act (DPA), which repealed the 2004 Act, was specifically designed to update the national law and align it with international standards. When the DPA was enacted in 2017, in a clear example of the "Brussels effect," Mauritius' Data Protection Commissioner expressly acknowledged that the DPA was drafted to be "in line with" the GDPR[139] and reflected in the rationale of the bill in the National Assembly. The DPA 2017 governs privacy rights of individuals in relation to requirements of collection, processing, storage, transfer, and handling of personal data and special categories of personal data that warrant heightened protections, where "personal data" is broadly defined to mean "any information relating to a data subject." The regulation is seeking to strike a balance between the interests of businesses, the Government of Mauritius, and the fundamental right to privacy of individuals.

The regulation applies to the processing of personal data that is wholly or partly performed by automated means by organizations that are (a) established in Mauritius and (b) organizations not established in Mauritius but using equipment in Mauritius to process personal data (other than for the purpose of transit through Mauritius). Notably, it does not apply to "the exchange of information between ministries, government departments, and public sector agencies."[140]

The DPA 2017 is a sector neutral law and applies to all categories of industries. There are four main roles stipulated by the DPA 2017 in relation to data.

- *Data subject:* an identified or identifiable individual
- *Controller:* a person or public body which, alone or jointly with others, determines the purposes and means of processing personal data and has decision-making power with respect to the processing; one or more parties may be joint controllers if they determine the purposes and means of processing together
- *Processor:* person or public body that processes personal data on behalf of the controller

Implementation of the DPA 2017 has brought numerous benefits to Mauritius. By increasing accountability of controllers, the DPA 2017 has helped controllers implement better processes, having better organizations, and achieving better productivity. It also introduced steeper penalties, with some offenses actually subject to penalty of up to five years imprisonment.

136 See, e.g., Madhewoo M. v. The State of Mauritius & anor 2013 SCJ 401; see also Madhewoo M. v. The State of Mauritius & anor [2016] UKPC 30.

137 See http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/N/Page%201/NATIONAL%20IDENTITY%20CARD%20ACT,%20No%2060%20of%201985.pdf. Accessed February 2020.

138 https://www.coe.int/en/web/portal/-/mauritius-joins-the-data-protection-convention-convention-108-.

139 See An Overview of the Data Protection Act, DPO of Mauritius, http://dataprotection.govmu.org. Accessed February 2020.

140 See Art. 3(4)(a), DPA.

It has also strengthened individuals' trust, by enabling the latter to gain confidence in the level of data protection of relevant products and services. In addition by enhancing data subjects' rights, the DPA 2017 has provided individuals greater control over their personal data. Moreover, it has improved the digital legal landscape to respond to the new EU requirements for adequacy, thereby attracting foreign investors. And finally, the DPA 2017 has helped to minimize data breaches.[141]

Section 3(4)(a) of the Data Protection Act 2017 (DPA) exempts the exchange of information between ministries, government departments and public sector agencies from the Act where such exchange is required on a need-to-know basis, providing wide latitude for intergovernmental and interagency data sharing. In addition, the Electronic Transactions Act has been amended to allow a public sector agency (such as a ministry, government department, local authority, or a statutory body) to share information, through its electronic system, with a private sector institution.

CREATING A TECHNICAL ARCHITECTURE FOR DATA SHARING

Mauritius and the Indian Ocean Commission (intergovernmental organization composed of Comoros, Madagascar, Mauritius, Réunion, and Seychelles) signed an MoU with Estonia's e-Governance Academy to implement the national data exchange layer and on developing digital identity, basic registries, and databases.

In Mauritius, where the platform is known as InfoHighway, the principal objective is not only to provide a secure and scalable platform offering e-government services by the Government of Mauritius but also a robust service platform to facilitate the consumption of published data among government agencies and private entities to improve operational efficiency in public administration and business operations. InfoHighway therefore aims to fulfill the following main objectives:

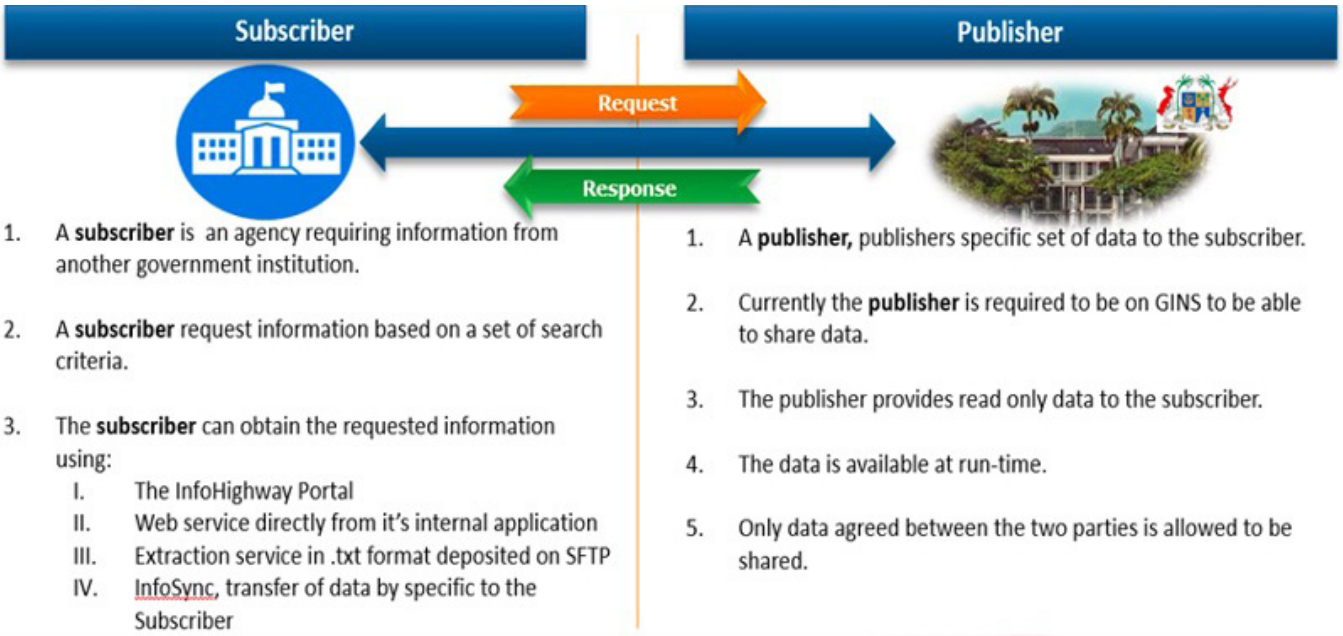
- Provide Government of Mauritius with a single platform offering scalable e-services;
- Provide a robust service platform to facilitate the consumption of published data among government agencies and private entities to improve operation efficiency;
- Improve the turnaround availability time of updated and useful data for government agencies and private institutions for their business needs, all in a secure environment; and
- Establish links to other ministries/epartments and institutions.

InfoHighway is administered by the Ministry of Technology, Communication, and Innovation. The DPO is a member of the InfoHighway High-Level Management Team, which considers requests from agencies wishing to exchange data through the platform.

InfoHighway uses a "Publish and Subscribe Model" for intragovernmental data sharing, whereby the agency sharing data is the "Publisher" and the one requesting the data is the "Subscriber."

141 Dolan, Jonathan. Notes from interview with Data Protection Commissioner of Mauritius, February 26, 2020.

Figure 8: InfoHighway Subscribe-Publish Model



Source: The Ministry of Technology, Communication and Innovation. "InfoHighway Website," https://ih.govmu.org/. Accessed March 2020.

Government officials view the application and governance structure of InfoHighway to be a key contributor to cultivating trust in the data sharing system. Broadly, this includes four main steps:

1. Prospective subscribers and publishers fill in an application form to join the InfoHighway. At the time of application, the expected purpose for participating in the data sharing system are identified.

2. Submit the filled form to the MoTCI.

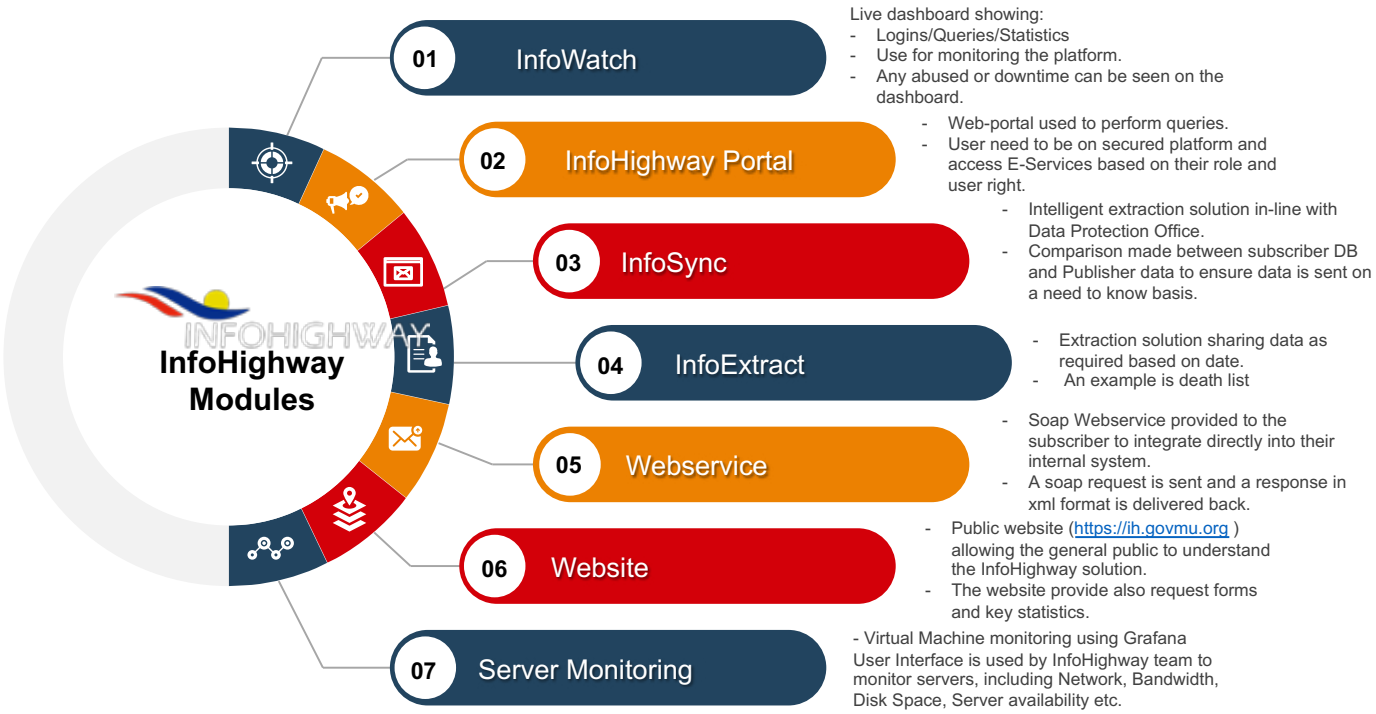
3. The form is then considered by the High Level Management Team tasked with operationalizing the InfoHighway. The committee consists of representatives of the Ministry of Finance, Economic Planning and Development, Attorney General's Office, Data Protection Office, Economic Development Board, Civil Status Division, Central Informatics Bureau, IT Security Unit, and the National Computer Board). Examination of the request to share data is carried out to ensure compliance with the Electronic Transactions Act, Data Protection Act, Civil Status Act, Business Registration Act, and other legislations, and the justification for the data sharing.

4. Approvals is then granted or refused on the basis of the examination.[142]

In addition to the mechanics of the application and review processes, it is also important to understand that the technical design of InfoHighway technically is several modules operating together in a secure environment.

142 Dolan, Jonathan. Notes from Interview with CTO's office. April 27, 2020.

Figure 9: InfoHighway Modules



InfoSync, for example, is the module of InfoHighway that ensures synchronization of data happens across government agencies—connecting, for instance, social security data with marriage license data. This module has two key features that help build trust. First, it reinforces data protection policies by ensuring only those governments that "need to know" have access to the relevant data for a specific transaction. Second, it helps minimize how much data any one government agency must hold in order to provide services, thereby reducing potential vulnerabilities. InfoWatch, another key module for building trust in the data sharing ecosystem, supports the dashboard which is used to monitor data flows and increase transparency into how data is being shared.

Currently InfoHighway is only used for intragovernmental data sharing and allows for visibility into the nature of the data request and the size of the data being shared but only the parties to the data exchange are able to see the content of the data. The government is currently finalizing plans—which may go into effect as early as this year—to open up InfoHighway to private firms as well and, at the moment, the expectation is that they will have to log the type of content they are sharing to give the government some visibility into the data flowing through InfoHighway. There are additional plans being made to give individuals new capabilities to view and manage how their data is flowing over InfoHighway, though the timeline for this is still being determined.[143]

143 Dolan, Jonathan. Interview with CTO's Office. April 27, 2020.

BUILDING THE INSTITUTIONAL CAPABILITIES FOR DATA SHARING

Following best practice guidance for successful open data implementation, the National Open Data Policy created a Central Open Data Team (CODT), which reports to the Chief Technical Officer of the Ministry of Technology, Communication, and Innovation (MoTCI). The CODT is responsible for steering Open Data work across government ministries and departments, including establishing and reviewing standards for Open Data and setting up and administering the National Open Data Portal. The CODT is also responsible for setting the standards for Privacy Compliance Assessments to be carried out at the level of ministries and departments prior to the release of data sets as Open Data.

Importantly, in addition to the centralized team, each ministry was compelled by the National Open Data Policy to create an Open Data team to support the CODT. These ministry-level teams are expected to have at a minimum a permanent secretary, a program manager, a systems analyst, and a statistician—a team drawn from different government agencies and embedded into each ministry. The creation of the ministry-level teams build upon existing practice within the Government of Mauritius to have embedded statisticians from the National Statistics Office in each ministry.

In addition to these government constructs, the local private sector emerged as an important force in shaping the country's data sharing efforts. Local entrepreneurs and business associations became vocal advocates in the push for creating the policy and have sustained efforts to hold the government accountable. This push from the private sector on the demand side is apparent in the language of the Open Data policy documents. In making the case for the country's Open Data policy, the government identifies (1) Economic Advantages and (2) Accountability and Transparency as the main policy drivers.

On the first point, the document notes, "The overriding priority of the government is the creation of high value jobs and wealth. The expansion of the circle of opportunities and economic space are the cornerstones of the intention of the government to engage into an Open Data Initiative. Open Data is the bedrock of innovation which will be the driving force of the Mauritian economy in the next decade."[144]

144 Ministry of Information Technology, Communication, and Innovation, http://mtci.govmu.org/English/Documents/2017/Communique/Press%20Communique/Mauritius%20Open%20Data%20Policy%20May%202017.pdf. Accessed December 2019.

URUGUAY: DATA SHARING FOR GOVERNMENT EFFICIENCY, TRANSPARENCY, AND INDIVIDUAL EMPOWERMENT

BACKGROUND

Uruguay is a high-income South American country with a population of approximately 3.5 million. The country has enjoyed a remarkable drop in the rate of families living below the poverty line, decreasing from 40 percent in 2004 to 6 percent in 2016.[145] Today, the country enjoys the lowest poverty rates and lowest corruption[146] of any country in Latin America.

In the early 2000s, only 10 percent of Uruguay's population had access to the internet, and broadband speeds were much lower than in developed countries. Yet, the government recognized the economic and social opportunities of digital technologies for its citizenry and devised a far-reaching plan to improve the country's mobile and internet infrastructure. As a small country, heavily dependent on exports of beef and agricultural goods, digital transformation represented an opportunity to dramatically remake its economy and modernize its engagement with everyday citizens through e-government services.[147]

Uruguay took the first steps toward improving digital connectivity in 2000 with the launch of the National Committee for Information Society. The committee drafted the Digital Agenda for Uruguay (ADU), a multistakeholder vision with representatives from government, academia, the private sector, and civil society organizations.[148] The council established concrete goals for the country's digital development and, to achieve these goals, the government of President Tabaré Vásquez in 2007 created the Agency for Electronic Government and Information Society (AGESIC) as the institutional home to drive the digital agenda.

AGESIC reports to the Office of the President and works with technical autonomy and in close collaboration across government agencies to offer improved digital services to the citizens of Uruguay, including leadership in data protection, access to information, cybersecurity, and digital government initiatives.

AGESIC's work has been guided by a series of national digital agendas, issued in 2008, 2010, 2015, and most recently in 2020. During this time, Uruguay has made

145 *The tip of the iceberg The Digital Govt Architecture of Uruguay* (slide deck from AGESIC).

146 Transparency International ranking.

147 Sabatino, Carlos. "Uruguay's Digital Development Policy," June 2017, Global Delivery Initiative, http://www.globaldeliveryinitiative.org/library/case-studies/uruguay%E2%80%99s-digital-development-policy.

148 Center for Public Impact: A BCG Foundation. "Digital Agenda in Uruguay," March 18, 2016, https://www.centreforpublicimpact.org/case-study/digital-agenda-uruguay/. Accessed April 2020.

tremendous strides in connecting its citizens to the internet and ensuring that people have the necessary digital skills to actively engage online. As of June 2019, 82 percent of homes were connected to broadband internet and the state-owned telecom provider, Antel, had reached 75 percent of homes with its fiber-to-the-home (FTTH) network and expected to have near-universal coverage by the end of 2020. Additionally, all of the country's public schools have high quality internet access, and it is the only country in the world that provides free laptops to all public and secondary school students.[149] The country has not only prioritized digital skills acquisition but has been a leader in the the concept of the digital citizen defined by UNESCO as a "set of skills that enables citizens to access, retrieve, understand, evaluate, and use, to create as well as to share information and media in all formats, using several tools, in a critical, ethical, and effective way to participate and engage in personal, professional, and social activities.[150]

Beyond creating the conditions for engaged digital citizens, Uruguay has developed its national digital agenda in a way that has cultivated public trust and enabled sustained political will even as administrations have changed.

1. *Cultivating trust*: As with the original ADU, the subsequent ADUs have been developed through a multistakeholder engagement process and all stakeholders remain engaged in the implementation and monitoring of the ADU through the National Council for the Information Society. This approach has led to high degrees of public trust. The current 2016–2020 ADU continues to emphasize the importance of the trust ecosystem in order "to promote full participation in the information society," including an effort to expand the use of secure digital identity mechanisms for authentication purposes.

2. *Sustained political will*: Many specific initiatives that have emerged from the ADU are joint efforts of AGESIC and other government agencies and line ministries. The National Plan for Digital Literacy, for instance, was designed and delivered through a collaboration between AGESIC and the National Telecommunications Administration (ANTEL), Ministry of Education and Culture (MEC), and National Bureau of Civil Service (ONSC).[151]

These conditions have enabled Uruguay to emerge, along with Mexico, as a regional leader in the use of technology to build a more efficient and responsive government, and as the building blocks for digital transformation—e.g., connectivity, digital skills—have solidified AGESIC's role within government has evolved and expanded. The first two iterations of the ADU were focused primarily on setting up the necessary infrastructure for digital transformation, establishing the enabling environment for ICTs to take root, and building human capacity. Starting in the 2011–2015 plan, the ADU started to shift its focus to delivery of direct services to people and this focus has been further emphasized in the current plan, including a commitment to have all government services online this year. This evolution has included placing an increased importance on the use of data to deliver benefits to people and society.

The use of data is now identified as an essential tool for the country's development in both the ADU and in the Digital Government Plan—two key documents that guide AGESIC's work.

149 Uruguay: Investment, Export, and Country Brand Promotion Agency. "URUGUAY: A TECHNOLOGICAL REVOLUTION IN A LITTLE MORE THAN A DECADE," December 2019, https://www.uruguayxxi.gub.uy/en/news/article/uruguay-una-revolucion-tecnologica-en-poco-mas-de-una-decada/. Accessed April 2020.

150 Clastornik, Jose. "The digital citizen is here—are governments ready?" Apolitical, August 4, 2019, https://apolitical.co/en/solution_article/the-digital-citizen-is-here-are-governments-ready. Accessed April 2020.

151 Center for Public Impact: A BCG Foundation. "Digital Agenda in Uruguay," March 18, 2016, https://www.centreforpublicimpact.org/case-study/digital-agenda-uruguay/. Accessed April 2020.

OPEN GOVERNMENT

Uruguay first established open government commitments in 2012, aligning with the goals set forth in the 2011–2015 ADU. Its adoption of open government has allowed Uruguay to lead the region in creating social value and informed government decision-making through the adoption of transparent processes and technological innovation.

A Tu Servicio—Open Government and Data Sharing in Action

Every February, Uruguayan citizens are given the opportunity to choose whether to change or stay with their existing health care provider. In the country's mixed public-private health care system, several factors come into play when making this decision: the location of the health provider, number of doctors and pediatricians available, hours open, etc. These decisions were difficult to make without easy access to this information. Initially, as part of the Government's Open Government efforts, the Ministry of Health published detailed spreadsheets on each health care provider. However, these spreadsheets were never downloaded more than 500 times in any given year.

Given the low uptake of the data, Datos Abiertos, Transparencia y Acceso a la Inform (DATA) Uruguay, an Uruguayan civil society organization focused on open data, independently attempted to create a user-friendly comparison tool, which started a dialogue between the organization and the Ministry. Ultimately, DATA Uruguay partnered with the Uruguayan Ministry of Health to create A Tu Servicio, a website providing easily digestible, searchable and visualized infographics based on open government health data and available to be used by the public.

The platform allows users to select their location and then to compare local health care providers based on a wide range of parameters and indicators, such as facility type, medical specialty, care goals, wait times, and patient rights. A Tu Servicio has introduced a new paradigm of patient choice into Uruguay's health care sector, enabling citizens not only to navigate through a range of options but also generating a healthy and informed debate on how more generally to improve the country's health care sector. Ultimately, the program resulted in an increase in users from 500 to around 75,000 downloads in 2016, resulting in 63,130 people actually changing health service providers during February 2016.

Beyond user growth, the project helped improve the quality of data—e.g., errors were discovered by users, providers, and the Ministry itself—and helped to lower prices for consumers. After its initial release in 2015 caught providers by surprise, several opted to decrease their prices in January 2016, knowing that the tool would allow for easy comparison and give them a competitive advantage.

The ability to share data in a trusted ecosystem, enabling programs like A Tu Servicio, is possible through a number of updates to the legal and regulatory environment, investment in a robust technical architecture for data sharing, and clear authority and consistent leadership from AGESIC.

KEY FEATURES OF DATA SHARING

CREATING THE POLICY AND REGULATORY ENVIRONMENT FOR DATA SHARING

Legal Foundations

Although Uruguay's constitution does not contain any express rights to data protection, Article 28 does provide that "The papers of private individuals, their correspondence, whether epistolary, telegraphic, or of any other nature, are inviolable, and they may never be searched, examined, or intercepted except in conformity with laws which may be enacted for reasons of public interest."

That said, Uruguay has a relatively long history of data protection. Data protection in Uruguay is governed under the "Data Protection Act" of 2008, Law No. 18,331 on Personal Data Protection,[152] the Habeas Data Act of 2008 (or Access to Information Law), and Decree No. 664/008 and Decree No. 414/009, which provide further clarifications and guidance on the Act. Decree No. 664/008 provides complementary provisions and guidance on the application of Law 18,331, while Decree No. 414/009 stipulates the requirements for registering databases.

The "Data Protection Act," which is very similar to the GDPR, outlines several principles for those collecting and processing personal data, including: the principle of legality, the principle of truthfulness and veracity, the purpose of limitation principle, the principle of prior consent, the principle of data security, the principle of confidentiality, and the principle of liability. Unlike GDPR, Uruguay's Data Protection Act also extends to "juridical persons" such as entities and corporations.[153]

In 2012, the European Commission formally approved Uruguay's status as a country providing "adequate protection" for personal data within the meaning of the European Data Protection Directive (Directive 95/46/EC), the predecessor to the GDPR. In 2013, Uruguay became the first non-European state to accede to the Council of Europe's Convention 108, further signaling its commitment to international data protection standards.

Uruguay is also a member of the Ibero-American Data Protection Network (RIPD for the Spanish acronym), which adopted the Standards for Data Protection for the Ibero-American States, a common data protection framework for the Ibero-American countries (the Spanish-speaking countries in North, Central, and South America, plus Portuguese-speaking Brazil). One of the aims of the RIPD is "to make the flow of personal data between Ibero-American States and beyond their borders easier, in order to contribute to the economic and social growth of the region,"[154] demonstrating how personal data protections can promote data sharing for economic development.

Data Protection Act

The Act defines "personal data" as "any kind of information related to a person or legal entity identified or identifiable," and "sensitive personal data" as "any kind of personal data evidencing: racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership, and any kind of information concerning health or sexual life."

The national DPA is the Unidad Reguladora de Control y Actos Personales (the "URCDP"). While there is no requirement that organizations appoint a data protection officer, an organization that owns or maintains a database containing information gathered or obtained through means, mechanisms, or sources located in Uruguay, must register that database with the URCDP.

152 See Ley 18331. https://www.impo.com.uy/bases/leyes/18331-2008.
153 See Art. 4(D), Data Protection Act 2008.
154 See https://iapp.org/media/pdf/resource_center/Ibero-Am_standards.pdf.

In order to collect data, an entity must obtain prior consent from the individual or entity whose information is being collected. Consent is not required in the case of personal data from public sources; obtained by public authorities in compliance with legal obligations; limited to domicile, telephone number, ID number, nationality, tax number, corporation name; necessary for the performance of a contract or the provision of a professional service; and obtained by individuals or corporations for their personal and exclusive use.

Personal data may only be processed for a legitimate reason, i.e., a lawful basis. Personal data may not be used for additional or secondary purposes different from the purposes for which the data was originally obtained. Once the purposes for processing personal data are achieved, personal data must be deleted.

Personal data can only be transferred to a third party for purposes directly related to the legitimate interests of the transferring party and the transferee and with the prior consent of the data subject. The data subject must be informed of the purpose of the transfer and the identity of the recipient. Evidence of such consent should be maintained, and the data subject may revoke that consent at any time. Prior consent of the data subject is not necessarily required when the personal data to be transferred is limited to the data subject's name, surname, identity card number, nationality, address, and date of birth. The transferor remains jointly and severally liable for the compliance of the recipient's obligations under the Act.

In general, the Act prohibits the transfer of personal data to countries or international entities which do not provide adequate levels of protection according to European standards. International transfers to "inadequate" countries or entities is allowed where the data subject consents to the transfer in writing, or when the guarantees of adequate protection levels arise from "contractual clauses" and "self-regulation systems" providing the same levels of protection as the laws of Uruguay. Intracompany transfers are permitted without authorization where an entity has registered a conduct of code with the URCDP (akin to binding corporate rules under the European framework).

Data processors must implement appropriate technical and organizational measures to guarantee the security and confidentiality of the personal data. These measures should be aimed at preventing the loss, falsification, and unauthorized treatment or access, as well as at detecting information that may have been lost, leaked, or accessed without authorization. In the event of a breach that could substantially affect the rights of the data subject, and/or the rights of any other agent or person involved, the data processor should notify affected persons.

The URCDP has broad investigatory and enforcement powers, including audit and inspection rights, and subpoena, search and seizure authority. The URCDP can impose penalties including warning, admonition, fines up to US$60,000, suspension of the database for five days, and closure of the database.

DATA ARCHITECTURE

Uruguay has a robust digital government architecture that facilitates the secure sharing of data including both a digital government services platform and single state portal for citizen access and a data exchange architecture that links federated records of people, enterprises, public services, and addresses available as metadata on the interoperability platform.[155]

The data exchange model is based on a combination of decentralized data management and centralized communication with the interoperability platform serving as a shared resource for all government and

155 Uruguay Digital. "Transforming with Equity 2020," https://uruguaydigital.uy/wps/wcm/connect/urudigital/44f1500c-6415-4e21-aa33-1e5210527d94/Download+Digital+Agenda+%28English+Version%29.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=44f1500c-6415-4e21-aa33-1e5210527d94. Accessed March 2020.

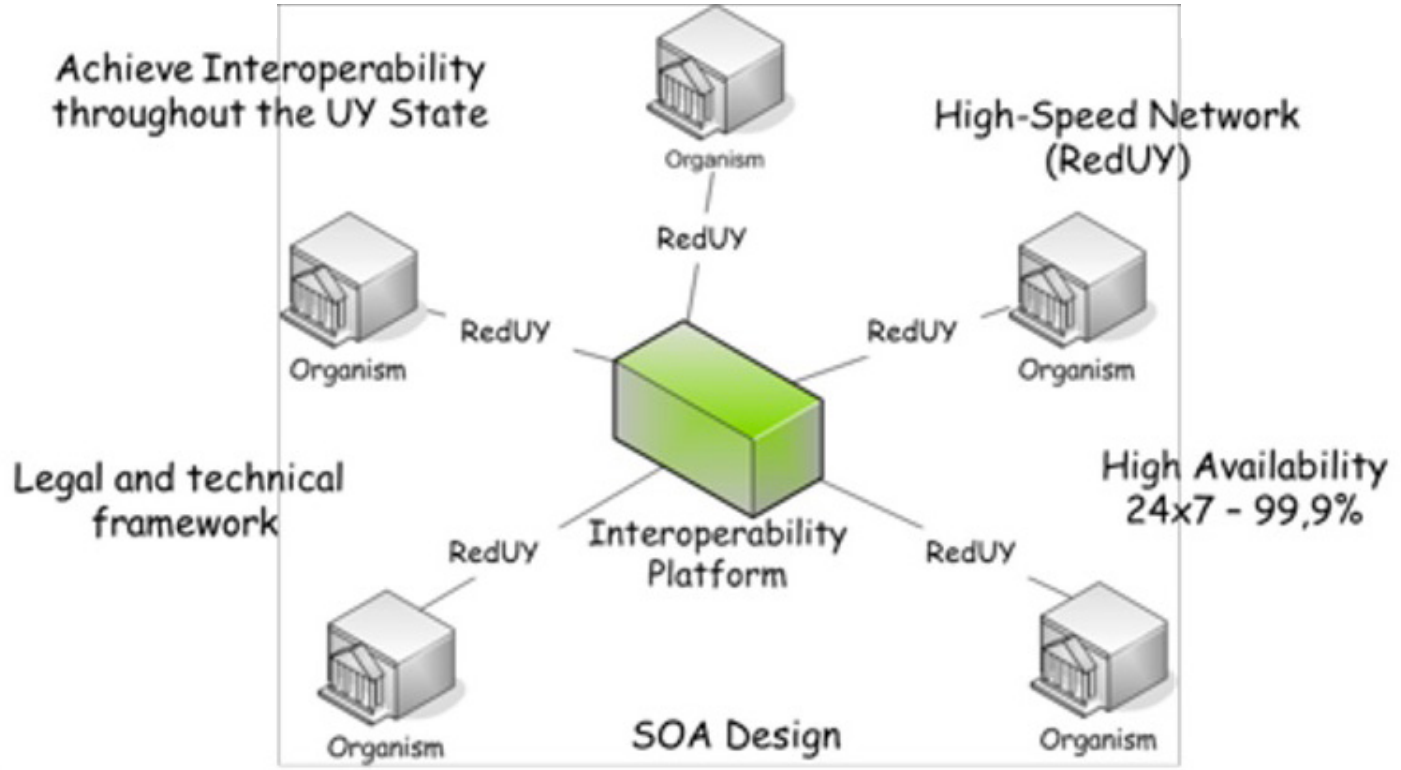
public agencies and establishes the standard for exchanging data between them. The interoperability platform is built on a secure private network.

The interoperability infrastructure was launched in 2008 but only began to be widely used in 2016 due to varied technology maturity across public agencies, the difficulty in breaking down silos generated by bureaucracy, and, importantly, the initial lack of trust between agencies in exchanging the information and in the whole-of-government approach.

Today, however, the platform exchanges over 10 million transactions per month with over 100 entities connected. It supports a wide range of critical government services initiatives. For example, each child born in Uruguay is registered with the Ministry of Public Health and, through the sharing of data, a civil identification number is immediately generated in the public registry.

The platform integrates systems across the state at the backend and is divided into two layers: an interoperability layer (semantic and technical) and a security layer. The semantic interoperability is solved by the metadata definition of common data objects. Those definitions are made in agreement with all agencies involved in the use of that information and published in the form of a data dictionary, an xml schema, and an uml object diagram. The technical interoperability is implemented with an Enterprise Service Bus (ESB) accompanied by a set of definitions based on open standards. This allows the simplification of data exchange and the ability of offering added value services on it.

Figure 10: Platform Overview



Source: Provided by AGESIC.

All exchanges over the platform are based on Web Services Soap1.1 and comply with WS-Basic Profile 1.1. Message delivery is implemented using WS-Addressing standard, which provides capacity of dynamic routing. The security layer covers physical security and logical security. SSL v3.0 (HTTPS) with mutual authentication is used for physical transport security. Logical security covers authentication and authorization of services. Open standards allow universal use of the platform, becoming independent from proprietary protocols and overcoming difficulties at the integration stage.

Legally the data sharing model requires that each exchange must be made between two entities—public or private—registered in the public records. To accomplish this, the government requires each exchange to be signed with a digital certificate that legally represents the entity. The entities authorized to access the platform are those that provide a public service. The platform allows access for the private sector only when the data concerned is owned by public entities that request the access under the same security conditions.

Importantly, the data exchange system is supported by whole-of-government architecture that defines a framework to standardize and optimize the building, evolution, and documentation of public organizations architectures (enterprise architectures), from the business processes to supporting infrastructure. The main goal is to establish a technical framework that includes standards, products, best practices, and recommendations in order to guide public organizations in the design of technical solutions in such a way that promotes interoperability. The whole-of-government architecture provides interoperability guidelines as well—establishing a framework for vertical sectors like e-health, public finance, and education. The interoperability guidelines align with the components of the interoperability platform and are based on a reference model for data architecture.

This model enables the government to work with different levels of data including: organizational and management data, private sector data, and citizen data. This ability to work across different types of data is essential to the country's whole-of-government approach.[156]

156 Technical description provided by AGESIC.

MEXICO: DATA SHARING FOR GOVERNMENT EFFICIENCY AND TRANSPARENCY

BACKGROUND

Mexico, an upper-middle-income country with a population of nearly 130 million people, has the second largest economy in Latin America after only Brazil and the fifteenth largest in the world. Over the last ten years, the country has experienced moderate but consistent economic growth, averaging just over two percent annually until 2019 when the economy contracted slightly. Despite this decade of reasonable economic stability, poverty and inequality have remained high with more than 43 percent of the population living in poverty and a Gini Index of almost 50.[157] Approximately three out of every five jobs remains in the informal economy, representing nearly a quarter of the country's economic output.[158]

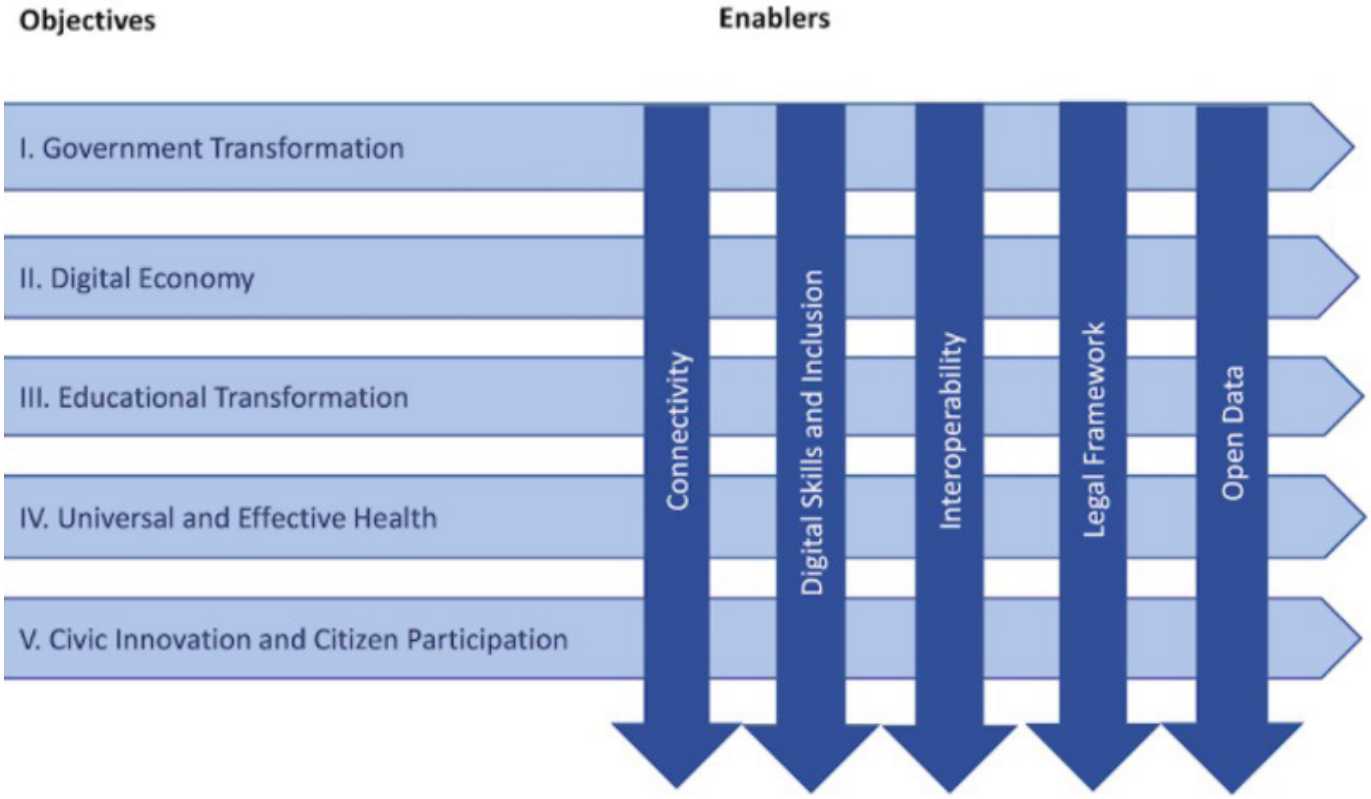
To tackle this persistent economic and social inequality, Mexico has invested heavily in digital transformation, particularly over the last eight years, and has emerged as a regional leader in leveraging information and communications technologies (ICT) to modernize government. While the use of ICTs to improve government services extends at least as far back as 2002, when the Presidential Agenda for Good Government included e-government as one of six pillars, the digital transformation of the public sector accelerated significantly in 2012.

Starting in 2012 and building on a decade of e-government experience, the government introduced a National Development Plan that acknowledged the importance of digitization and included the country's first National Digital Strategy which addressed both public sector digital transformation, as well as the building blocks needed for a more inclusive digital society including greater internet access and broad digital literacy. A National Digital Strategy Office was created under the Office of the President to coordinate the Digital Strategy.

157 IMF News. "Mexico's Economic Outlook in Five Charts," November 8, 2018, https://www.imf.org/en/News/Articles/2018/11/07/NA110818-Mexico-Economic-Outlook-in-5-Chart. Accessed May 2020.

158 Radu, Sintia. "Can Technology Solve Economic Disparity?" U.S. News, February 14, 2020, https://www.usnews.com/news/best-countries/articles/2020-02-14/technology-is-being-used-to-fight-economic-inequality-in-latin-america.

Figure 11: Framework for Mexican National Digital Strategy: Objectives and Enablers



Source: Government of Mexico, "National Digital Strategy," https://www.gob.mx/mexicodigital

To realize the goals of the Digital Strategy, the government successfully amended the Mexican constitution in 2013 to make universal internet access a right and ushered in a series of legal and institutional reforms governing the ICT sector, including the creation of an independent agency focused on ICT licensing and concessions, a commitment to build a nationwide fiber optic backbone network, and a commitment to install a shared public network— all of which designed to increase competition in the telecommunications market and reduce the country's digital divide.

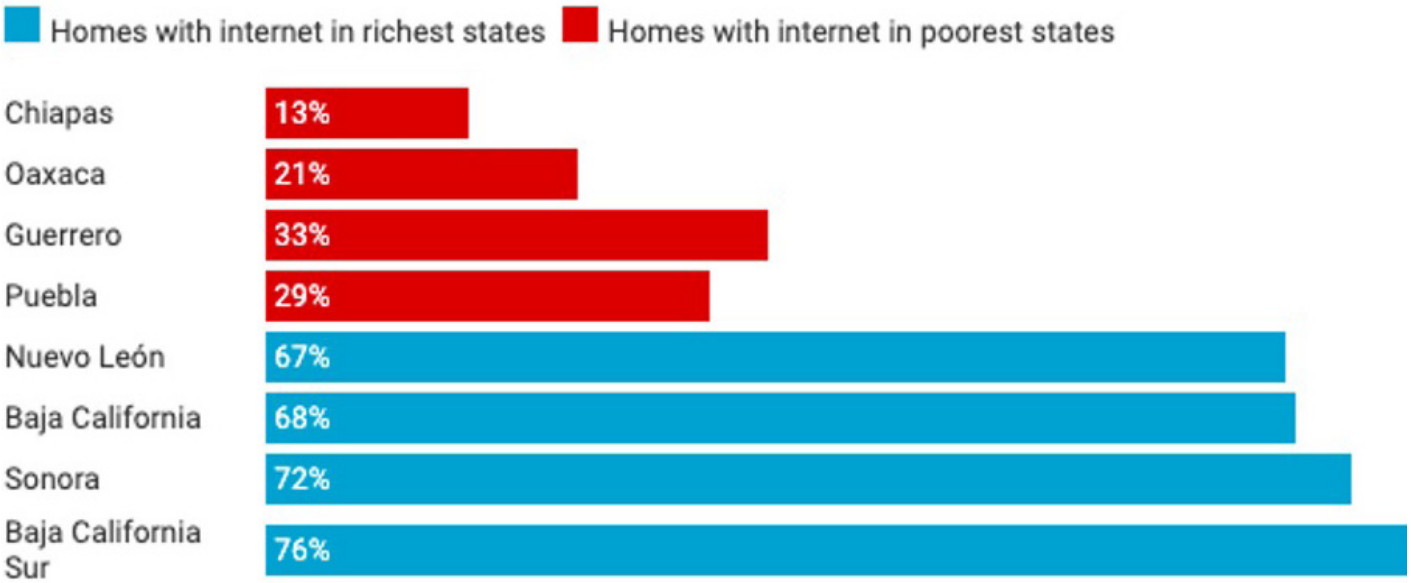
A study conducted shortly before the creation of the National Digital Strategy found that approximately seven out of ten people in the highest income bracket were Internet users, while only two out of ten people in the lowest income bracket used the internet, essentially reinforcing rather than reducing the social and economic disparities.[159]

The reforms introduced in 2013 have had remarkable success in expanding internet access, particularly the shared public network, which has become known as Red Compartida.

Red Compartida became the first large-scale, wholesale mobile network in the world and enabled the installation of a single network that can be shared by all operators, reducing their costs, particularly in regions that are otherwise commercially unattractive to install and deploy their own networks. Red

159 Montiel, Juan Manuel Mecinas. "THE DIGITAL DIVIDE IN MEXICO: A MIRROR OF POVERTY," Mexican Law Review, July–December 2016, https://www.sciencedirect.com/science/article/pii/S1870057816300464#fn0025.

Figure 12: Mexico's Digital Divide



Source: Barry, Jack J. "Mexicans have world-first constitutional right to government-provided internet," Apolitical, November 28, 2018, https://apolitical.co/en/solution_article/internet-poverty-connection-mexico.

Compartida is a US$7 billion privately funded project that is operated as a public-private partnership and is ultimately expected to cover more than 90 percent of the population in Mexico with the most advanced mobile broadband services. Ultimately, the PPP was signed in early 2017 and the project was awarded through an international-public-tender (IPT) process conducted through 2016. In supporting this model, the government not only aspired to extend internet access but viewed it as a key platform upon which digital government and other critical services from mobile banking to health and education services would grow.[160]

Catalyzed by the reforms that started in 2012–2013, Mexico has experienced significant and accelerating growth in the number of internet users in the country, growing from 44 percent in 2014 to over 70 percent in 2019 and continuing to expand.[161]

This growth in usage has been complemented by expanded government services, which have extended to the reach of public services and led to significant cost savings for the country.

As of 2018, 90 percent of government transactions can be initiated online and 75 percent can be completed digitally.[162] Furthermore, in addition to supporting more inclusive public services, Mexico has saved 1.6 percent of GDP between 2012 and 2017 by lowering

160 ITU, "Red Compartida," https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1514835212

161 Internet World Stats. "Internet Usage and Population in Central America," https://www.internetworldstats.com/stats12.htm

162 OECD (2020), *Digital Government in Mexico: Sustainable and Inclusive Transformation*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/6db24495-en.

the cost of government transactions for citizens and residents.[163] Mexico's experience is illustrative of how centralization of responsibility—in the National Digital Strategy office—can simplify and standardize digital government and strengthen the ability to share data safely and securely. The Digital Strategy office has defined three levels of standardization:

1. Level 1 defines the criteria for data capture,

2. Level 2 defines technical standards for the format of data downloads, and

3. Level 3 includes the web format, interoperability standards, and digital signature.

By February 2018, the Digital Strategy office had helped produce more than 5,400 standard information files, more than 600 standardized download formats, and 948 standardized online forms.[164]

As Mexico's digital government transformation has accelerated, the country has taken a number of additional steps to bolster citizen engagement and public trust in government, including a number of updates to personal data protection laws and investments in technologies and institutions to encourage secure sharing of data.

KEY FEATURES OF DATA SHARING

CREATING THE POLICY AND REGULATORY ENVIRONMENT FOR DATA SHARING

Key components of data governance in Mexico are the Constitution, the public sector data protection law, the private sector data protection law and corresponding regulations, and self-regulatory schemes.

The Constitution

Mexico's Constitution underpins its legal framework for data governance. The 1917 Constitution enshrined a fundamental right to privacy in Article 16. In 1977, the Constitution was amended to include a right to freedom of information.[165] In 2002, Congress passed the Federal Law of Transparency and Access to Public Government Information, which took effect in 2003.[166] The Law aimed to secure access to any public information and incorporate principles and standards for the protection of personal data. The federal law was followed by freedom of information legislation at the state level, which ultimately imposed different legal frameworks and institutional capacities on citizens and businesses, impeding transparency. In 2015, the Mexican Congress responded by enacting the General Act of Transparency and Access to Public Information[167] to enhance uniformity of access to information laws across Mexico's 33 separate jurisdictions.

---

163 Benjamin Roseth, Angela Reyes, Pedro Farias, Miguel Porrúa, Harold Villalba, Sebastián Acevedo, Norma Peña, Elsa Estevez, Sebastián Linares Lejarraga, and Pablo Filottrano. "Wait No More: Citizens, Red Tape, and Digital Government," Inter-American Development Bank, Jun 6, 2018, accessed through: https://books.google.com/books?id=u6x2DwAAQBAJ&pg=PA164&lpg=PA164&dq=digital+identity+mexico+and+interoperability&source=bl&ots=qPicy2oEHa&sig=ACfU3U2Tfn9_QA6NH7klVnw5MwNI2cD5_Q&hl=en&sa=X&ved=2ahUKEwimjf6Z9vboAhUTlXIEHa2HDeA4ChDoATADegQICRAv#v=onepage&q=mexico&f=false.

164 Benjamin Roseth, Angela Reyes, Pedro Farias, Miguel Porrúa, Harold Villalba, Sebastián Acevedo, Norma Peña, Elsa Estevez, Sebastián Linares Lejarraga, and Pablo Filottrano. "Wait No More: Citizens, Red Tape, and Digital Government," Inter-American Development Bank, Jun 6, 2018.

165 See Article 6, Mexican Constitution ("the right of information shall be guaranteed by the state").

166 In January 2014 Congress approved an amendment to the Constitution to create an autonomous entity to be in charge of enforcing the Private Data Protection Law and to take on the duties of the Federal Institute for Access to Information and Protection of Data ("IFAI"), which was originally created as a semiautonomous agency separate from the federal government. As a result of the new General Law for Transparency and Access to Public Governmental Information, which annulled the effect of the former Transparency Law – the IFAI's responsibilities are now handled by National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) as an autonomous entity. See https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210064/mexico.

167 INAI. "General Act of Transparency and Access to Public Information," March 12, 2016, http://www.law-democracy.org/live/wp-content/uploads/2012/08/Mexico-General-Act-of-Transparency-and-Access-to-Public-Information-compressed.pdf.

In 2009 Congress approved a crucial amendment to the Constitution to recognize the protection of personal data as a fundamental right. Article 16 of the Constitution amended to add an express right to data protection providing, in pertinent part, "All people have the right to enjoy protection on their personal data, and to access, correct, and cancel such data. All people have the right to oppose the disclosure of their data, according to the law. The law shall establish exceptions to the criteria that rule the handling of data, due to national security reasons, law and order, public security, public health, or protection of third-party's rights." This constitutional underpinning forms the basis for Mexico's data protection laws.

Public Sector General Data Protection Law

Mexico's domestic legal framework for data protection centers around two key laws—one for the public sector and one for the private sector. The more recent General Law on the Protection of Personal Data held by Obligated Parties (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados) ("GDPL"—the English acronym), which entered into force on 27 January, 2017, applies to any public authority, entity, body, or organism of the executive, legislative, and judicial powers of the government, autonomous entities, political parties, trusts, and public funds, at federal, state, and municipal levels.[168]

Private Sector Federal Data Protection Law

The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Proteccion de Datos Personales en Posesión de los Particulares) ("FDPL"), which entered into force on July 6, 2010,[169] covers companies and private individuals. While the FDPL is an omnibus data protection law that sets the principles and minimum standards that shall be followed by all private parties when processing any personal data, it also recognizes that standards for implementing data protection may vary depending on the industry or sector. As such, it may be supplemented by sectoral laws and self-imposed regulatory schemes focused on particular industry standards and requirements, to the extent that those standards and requirements comply with the data protection principles in the FDPL.[170]

The FDPL was followed by the Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (Reglamento de la Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares) (the "Regulations"), which entered into force on December 22, 2011[171] and set out to clarify the scope and obligations set out in the FDPL, and the Privacy Notice Guidelines (the "Guidelines"), which entered into force on April 18, 2013[172] and stipulated the requirements for privacy notices for data processing that any subject could do. In 2014, the Ministry of the Economy also issued the Parameters for Self-Regulation Regarding Personal Data,[173] setting out best practices, requirements, and eligibility parameters to be considered by the data protection authority for approval, supervision, and control of self-regulation schemes, and authorization and revocation of certifying entities as approved certifiers.

---

168 On 4 January, 2018 Congressman Ramón Villagómez Guerrero submitted a bill to modify the FDPL to standardize it with the GDPL, which has not yet been approved by Congress.

169 See Executive Branch—Ministry of the Interior Decree: https://iapp.org/media/pdf/knowledge_center/Mexico_Federal_Data_Protection_Act_July2010.pdf.

170 To date, the Mexican Official Standard NOM-004-SSA3-2012 for medical records is the only sector-specific legal framework.

171 See http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf.

172 Additional relevant materials include the Recommendations on Personal Data Security of November 30, 2010, the Parameters for Self-Regulation regarding personal data of May 30, 2014, and the General Law for the Protection of Personal Data in Possession of Obligated Subjects (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados), which entered into force on January 27, 2017.

173 See http://www.dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014.

Scope of the Private Sector Law (FDPL)

The FDPL applies to the processing of personal data by individuals and legal persons (i.e., corporations). "Processing"' includes the collection, use, communication, or storage of personal data by any means, and "personal data" means any information concerning an identified or identifiable individual. "Sensitive personal data" is personal data that, if misused, may lead to discrimination or pose serious risks to the data subject, including data that could reveal racial or ethnic origin; past or present health conditions; genetic information; religious, philosophical, or moral beliefs; union affiliation; political views; sexual orientation; fingerprints;[174] and geolocation, among other things. It is subject to heightened requirements.

The regulation of the Federal Law applies extraterritorially to all data processed when: (1) in a facility of the data controller located in Mexican territory; (2) by a data processor, regardless of location, processing data on behalf of a Mexican data controller; (3) where Mexican law applies by virtue of international law or the execution of a contract (regardless of the data controller's location); and (4) by any means located in Mexico, regardless of where the data controller is located, unless such means are for transit purposes only. Notably, the FDPL does not apply to the government, certain credit reporting agencies, or to personal, noncommercial processing.

Data controllers are bound by the core principles of legality, information, consent, notice, quality, purpose, loyalty, proportionality, and accountability.[175] This means personal data must be: collected and processed fairly and lawfully; for specific, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes; adequate, relevant, and not excessive in relation to the purposes for which it is collected or further processed Accurate and, if necessary, updated; erased or rectified; and kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed. Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data, as well as rights of access, rectification, cancellation, or objection ("ARCO rights").

To legally process personal data, data controllers must provide a comprehensive privacy notice providing: the identity and address of the data controller collecting the data; the purposes of the data processing; the options and means offered by the data controller to data subjects to limit the use or disclosure of their data; the means for exercising their ARCO rights; the data transfers to be made; the procedure and means by which the data controller will notify the data subjects of changes to the privacy notice; and identification of any sensitive personal data that will be processed.

Consent is required for all processing of personal data, except as otherwise provided by the law. Implicit, opt-out consent is generally permissible, while express, opt-in consent is required for processing financial data and express, opt-in, written consent is required for processing sensitive personal data. Consent is not required where the processing is: permitted by law; based on publicly available or de-identified data; pursuant to a legal relationship between the data subject and controller; undertaken in an emergency situation threatening an individual or their property; essential for medical attention, prevention, diagnosis, health care delivery, medical treatment, or health services management when the data subject is unable to give consent; subject to a duty of professional confidentiality; or pursuant to a resolution issued by a competent authority.

174 Beyond "fingerprints," the concept of biometric data is not defined under the FDPL. However, nonbinding guidance issued by INAI defines that biometric data is "sensitive personal data."

175 As the FDPL was largely inspired by Directive 95/46/EC, these principles largely correspond to the European framework.

Data Security

All data controllers must establish and maintain physical, technical, and administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access, or processing, at least as stringent as the measures in place to manage their own information. The risk involved, potential consequences for the data subjects, sensitivity of the data, and technological development must be taken into account when establishing security measures.

Data controllers must promptly notify data subjects of any security breaches that materially affect the property or rights of the data subject, including information about the nature of the breach, the personal data compromised, recommended protective measures the data subject can take, corrective actions implemented by the controller, and the means by which to obtain more information regarding the breach.

Transfers of Data

While the general rule is that consent is needed from the data subject in order to execute data transfers, domestic or international transfers of personal data may be carried out without the consent of the data subject where the transfer is: pursuant to an applicable law or treaty; necessary for medical diagnosis or prevention, or health care delivery or management; made to a party under the common control of the data controller; necessary for the performance of a contract between the data controller and a third party in the interest of the data subject; necessary or legally required to safeguard public interest or for the administration of justice; necessary for the recognition, exercise, or defense of a right in a judicial proceeding; or necessary to maintain or comply with a legal obligation.

Data controllers may share or transfer data with data processors without informing or obtaining the consent of data subjects. However, processors may only process personal data according to the instructions of and for the purposes identified by the data controller, must implement adequate security measures to maintain the confidentiality of the personal data subject to processing, and must delete personal data after the legal relationship with the data controller ends or when instructed by the data controller, absent a legal requirement for the preservation of the personal data.

International data transfers do not need the approval of the INAI or any other regulator but must be evidenced by written agreement or any other document whereby the third party assumes the same data protection obligations undertaken by the data controller and the conditions for processing as consented to by the data subject as detailed in the corresponding privacy notice.

Supervision and Enforcement

While Mexican law does not require data controllers to register with a data protection authority or other regulator, controllers are required to designate a person or department to act as the Data Protection Officer for handling data subject requests and enhancing the protection of personal data within their organization.

The National Institute of Transparency for Access to Information and Personal Data Protection *(Instituto Nacional de Transparencia, Acceso a la Informacion y Proteccion de Datos Personales*) (INAI) is the country's data protection authority, while the Ministry of Economy (Secretaria de Economia) cooperate on specific elements as established by the FDPL. The INAI is responsible for the enforcement of individual rights, the resolution of disputes, verifications and audits, and sanctions. The Ministry of Economy is responsible for issuing industry guidelines, such as it did with the Guidelines for Binding Self-Regulation and the Guidelines for Privacy Notices, in collaboration with the INAI. A handful of other public agencies have some authority over secondary sectoral regulations.

Where data subjects cannot enforce their ARCO Rights via a data controller, they can seek recourse via INAI and ultimately the judiciary. INAI may perform verification procedures that include on-site inspections to verify data controller compliance. Violations of the law are subject to monetary sanctions in the range of 100 to 320,000 times the Mexico City minimum wage, and double that for violations involving sensitive personal data. Certain violations are subject to up to five years imprisonment, and double that for violations involving sensitive personal data.

FinTech Law

In March 2018, the Mexican Congress approved the *Ley para Regular las Instituciones de Tecnología Financiera* (the "FinTech Law"). The main objective of the FinTech Law is to regulate the providers of FinTech services such as crowdfunding platforms and e-money issuers, giving them legal recognition as "Financial Technology Institutions" (FTIs) authorized, regulated, and supervised by the local financial authorities as they receive, maintain, and manage resources from the public. Most importantly with respect to data sharing, Article 76 of the law sets the legal framework for mandatory data sharing information by financial entities and FTIs to third parties through standardized APIs, in line with internationally recognized Open Banking initiatives. Regulation 2/2020, issued by BANXICO on March 10, 2020, contains the provisions referred to in Article 76 and establishes the standards for the interoperability of APIs used by credit reporting agencies and financial switches, as well as for determining the technical information for such interoperability. The regulation deals with with the exchange of open and aggregated data, specifically regulating (1) requirements for the approval of APIs, (2) requirements for other regulated entities to gain access to the data, (3) minimum requirements for interconnection agreements, and (4) BANXICO's supervisory authorities, including the power to suspend the exchange of information and the minimum requirements of compliance remediation.[176]

Regional and International Legal Frameworks

Mexico is also party to a variety of international and regional legal frameworks on data protection. Mexico is a member of the Ibero-American Data Protection Network (RIPD), a network of 22 data protection authorities that promotes the development of a comprehensive data protection legislation and the introduction of data protection authorities throughout Latin America.

Mexico is also a member economy of the Asia-Pacific Economic Cooperation ("APEC") forum, which has published a framework to protect privacy within and beyond economies and to enable regional transfers of personal data to benefit consumers, businesses, and governments (the "APEC Privacy Framework"). The APEC Privacy Framework is designed to facilitate information sharing and forms the basis of the APEC Cross-Border Privacy Rules ("CBPR") system.

On June 12, 2018, Mexico became only the second Latin American country (after Uruguay) to accede to the Council of Europe's Convention 108 and its additional protocol on supervisory authorities and cross-border data flows, bringing its practices in closer alignment with emerging international best practices. While Mexico has not been recognized by the European Commission as a third country providing adequate data protection to facilitate personal data transfers to countries within the EU, it does participate in Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR), through which certified companies and governments work together to ensure that the movement of personal information across borders is protected in accordance with the standards prescribed by CBPR and can be enforced by the participating jurisdictions.[177]

176 GreenbergTraurig. "New Open Banking Regulation in Mexico," June 16, 2020, https://www.gtlaw.com/en/insights/2020/6/open-banking-en-mexico-nueva-regulacion. Accessed July 8, 2020.

177 Asia-Pacific Economic Cooperation. "What is the Cross-Border Privacy Rules System?" April 15, 2019, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System. Accessed July 8, 2020.

It is also important to flag the recent tripartite trade deal between the US, Mexico, and Canada included a new chapter on Digital Trade. The deal includes assurances that data can be transferred cross-border and that limits on where data can be stored and processed are minimized, to enhance data sharing and protect the global digital ecosystem.[178] In fact, it is the first US trade agreement or deal to include an express prohibition on local data storage requirements. Finally, the deal promotes "open access to government-generated public data, to enhance innovative use in commercial applications and services," which intends to encourage data sharing from the public to the private sector.

Creating a Technical Architecture for Data Sharing

Like other global leaders in digital government, Mexico has complemented its policy and legal environment for data sharing with investments in secure technical architecture.

Mexico has been a regional and global leader in open data—ranking fifth in the world on the OECD's OURData Index, which measures the availability, accessibility, and government support for reuse of public sector data.[179] The government has positioned open data in its national development plans as strategic infrastructure, along with more traditional infrastructure like roads and power plants, needed to support policies aimed at social and economic inclusion. Given this strategic positioning, the government has worked to identify a list of the most strategic, high-value data generated by the government and created the Open Data Infrastructure (IDMX) that catalogues the most valuable data sets from diverse government sectors.

The IDMX is embedded in the country's Open Data Policy Implementation Guide, and contains more than 600 data sets about anticorruption, human rights, economic development, climate change, and public services. This infrastructure was built based on a citizen consultation through the one-stop government portal, Gob.mx/participa. In this consultation, more than 2,000 participants from civil society, private sector, and citizens participated to prioritize and propose the data they considered central to public concerns and helpful in identifying solutions to the country's development challenges. The infrastructure is available through datos.gob.mx/idmx and the number of data sets is expected to increase over time.[180]

In addition to the Open Data portal for sharing government data publically, the government has also invested in InteroperMX, a data sharing and interoperability platform. InteroperaMX powers the government's one-stop digital government portal, Gob.mx, by facilitating secure data exchange between line ministries and government departments.

InteroperaMX, modeled after Estonian's X-Road, allows public institutions to share reliable and trustworthy data, with clear identification of the source and certification of the information. As in Estonia, InteroperaMX supports efficient delivery of public services, including through a once-only policy whereby citizens only have to provide personal data to a single, appropriate government agency, and then that data is shared through a set of defined permissions.

178 Office of the United States Trade Representative, "UNITED STATES–MEXICO–CANADA TRADE FACT SHEET Modernizing NAFTA into a 21st Century Trade Agreement" https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing.

179 OECD Stats. "Government at a Glance—2019 edition—Open Government Data," https://stats.oecd.org/index.aspx?queryid=94409.

180 ITU. "MX Open Data Infrastructure," https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1514323093.

INTEROPERAMX IN ACTION

Mexico has pointed to birth certificate management as a key use case of InteroperaMX and has used its successes to highlight the potential of the platform to catalyze further efficiency gains. A birth certificate is required as proof of identity for at least 45 percent of all public procedures and services at the federal level. In its analogue format, the birth certificate has represented considerable costs—both in terms of financial and time—to Mexican citizens, which has particularly disadvantaged low-income populations. The government of Mexico estimates that citizens invested MXN 2.2 billion in 2016 (approximately US$115.5 million), with the poorest 10 percent spending roughly 1.5 percent of their real annual income on birth certificate procedures, excluding the related costs of transportation, possible bribery, or time spent to complete the procedures. InteroperaMX now enables citizens to access their birth certificate online in just minutes though the interoperability of the national population registry and state-level databases where birth registration takes place. Additionally, birth certificates can then be used online to access over 150 other government services.

SPOTLIGHT ON OPEN BANKING: DATA SHARING FOR ECONOMIC GROWTH AND INDIVIDUAL EMPOWERMENT

BACKGROUND

WHAT IS OPEN BANKING AND ITS RELEVANCE TO DATA SHARING?

Open banking provides third-party financial service providers open access to consumer banking, transaction, and other financial data from banks and nonbank financial institutions through the use of application programming interfaces (APIs). Open banking is intended to drive innovation in the financial services industry by allowing the accounts to be connected and for data across institutions to be shared for use by consumers, financial institutions, and third-party service providers.

As the Consultative Group to Assists the Poor's research (CGAP) has highlighted, experiences in designing and implementing Open Banking initiatives are illustrative of the opportunities and challenges of creating a trusted data sharing ecosystem. As a recent piece pointed out, Open Banking's "new systems for data sharing and payments flexibility could spur innovation by unlocking access to consumer data now held within payment companies, banks, and other financial institutions. … Yet the very same structures that hold out such promise for inclusion and growth also introduce new dangers. Sharing customer information among multiple players heightens the risk of misuse of their data, leaving many millions vulnerable to being targeted with unsuitable offerings.[181]

These characteristics are heightened further in low- and middle-income countries where more open use of data can benefit low-income people entering the formal financial system and improve their ability to engage with the real economy. Conversely, of course, those same populations have fewer assets and are more likely to be functionally or financially illiterate and therefore may be particularly vulnerable to exploitation.[182]

For these reasons, it is valuable to understand how countries that have taken a leadership role in Open Banking have built systems that drive a virtuous cycle between data sharing and data protections for consumers. Open Banking is, in many respects, still in its infancy, but there are numerous examples of Open Banking emerging around the world, but this case study focuses on the emerging practices and interesting features of the implementations in the United Kingdom and Australia, given their relative maturity and availability of information.

181 Chen, Greg and Faz, Xavier. "Open Data and the Future of Banking." CGAP Leadership Essay Series, October 23, 2019, https://www.cgap.org/blog/open-data-and-future-banking. Access March 2020.

182 Chen, Greg and Faz, Xavier. "Open Data and the Future of Banking." CGAP Leadership Essay Series, October 23, 2019, https://www.cgap.org/blog/open-data-and-future-banking. Access March 2020.

Illustrative Country Experiences

UNITED KINGDOM

Open banking was implemented in the United Kingdom (UK) as part of the remedy to a competition review of the retail banking sector and executed based on the government's experience with Midata, a program that had been envisaged early in the 2010s to improve consumer welfare and choice. The effort aligned with government goals of supporting the growth of the UK financial technology sector and improving the competitiveness of the wider financial services industry in hopes of ensuring the future of London as a global financial hub and the UK as a net exporter of financial services. Coming out of the experience with Midata, the Enterprise and Regulatory Reform Act 2013 empowered the UK's new Competition and Markets Authority (CMA) to enforce the opening up of data which was also supported by efforts in the EU around data portability, specifically the data portability right (and data protections) included in the General Data Protection Regulation (GDPR) and expanded access to payment accounts provided for in the revised Payment Services Directive (PSD2).
While open banking is still in the midst of implementation, as is PSD2, the ecosystem of innovation surrounding the increased access to data open banking provides has seen early signs of success, with over 200 regulated providers as of January 2020, open banking-enabled services available to the majority of UK banking customers through existing mobile and desktop channels and over one million customers that have used an open banking-enabled application. The model has influenced many other regulators already and is notable for its funding and implementation model, consultative and open source standard setting process, regulator support for the start-up ecosystem, emphasis on consumer safeguards, and aspirations for expansion to other areas of finance and other sectors of the economy. PSD2 empowers account holders with the authority to share data, removing financial institutions' role as gatekeeper.[183]

To drive competition in retail banking in the United Kingdom, its Competition Markets Authority required the largest UK banks to open up and share their data. While it is still too early to assess the impact of these efforts, one recent study by the UK's Financial Conduct Authority found the move could usher in more competition and innovative business models, delivering better customer services such as cheaper payment solutions, budgeting and money management tools based on customer data, and the ability for customers to easily switch to new providers.[184]

AUSTRALIA

Australia was an early proponent of Open Data with its online data portal launched in 2009[185] and its Declaration of Open Government in 2010[186] and today ranks highly in the Global Open Data Index[187] and the Open Data Barometer.[188] Given the historical relationship and influence of the UK, the Australian Government

183 Brodsky, Laura and Oakes, Liz. "Data Sharing and Open Banking," McKinsey & Company, September 5, 2017, https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking. Accessed March 2020.

184 Chen, Greg and Faz, Xavier. "Open Data and the Future of Banking." CGAP Leadership Essay Series, October 23, 2019, https://www.cgap.org/blog/open-data-and-future-banking. Access March 2020.

185 Office of the Australian Information Commissioner. "Towards an Australian Government Information Policy," Issue Paper 1, https://www.oaic.gov.au/information-policy/issues-papers/issues-paper-1-towards-an-australian-government-information-policy/.

186 Original not available but archived copy available here: https://apo.org.au/sites/default/files/resource-files/2010/07/apo-nid62429-1076971.pdf.

187 Australia has a score of 79 percent with perfect or near perfect scores across Government Budget, National Statistics, Procurement, Administrative Boundaries, Draft Legislation, Air Quality, National Maps, Weather Forecasts, Company Registers, Election Results, and Locations, a 50 percent score for Water Quality, and a 0 percent score for Land Ownership and Government Spending. The Global Open Data Index 2016/2017 is an annual benchmark for publication of Open Government Data run by the Open Knowledge Network. Data categories are scored against the "Open Definition" that Open Data can be "freely used, modified, and shared by anyone for any purpose" but does not look at other aspects of data such as context, use, or impact. https://index.okfn.org/place/ https://opendefinition.org/.

188 The Open Data Barometer is produced by the World Wide Web Foundation with the support of Omidyar Network and takes steps to "uncover the true prevalence and impact of open data initiatives around the world." The 4th edition is based upon a peer reviewed expert survey, a government self-assessment, and secondary data from the WEF, WBG, UN, and Freedom House. https://opendatabarometer.org/?_year=2017&indicator=ODB

was closely monitoring the progress of GDPR, with special attention to its data portability right, and open banking in thinking about its own data governance strategy.

Like the UK, Australia suffers from competitive concentration and low switching in a variety of relevant industries including retail banking, energy, internet service, and mobile telephony. The Productivity Commission Inquiry Report on Data Availability and Use tasked with examining access to data and its use in Australia noted that Australia's data governance policy was falling behind many other countries globally and recommended both an update to data sharing and protection legislation alongside a comprehensive right for consumers to access and share their data.[189] These factors heavily influenced the government's commitment to enact a Consumer Data Right, intended to establish a cross-economy data portability provision that would be implemented sector by sector.

Australia's Consumer Data Right is interesting for its powerful rhetoric around consumer empowerment, specificity in data portability across a number of sectors, collaboration across functional and sector regulators, government involvement in standard setting, consultative process for guiding implementation, and phased implementation process.

In November 2017, the government announced that they would follow the recommendation of the Productivity Commission's Data Availability and Use Inquiry and earlier competitions reports and introduce a Consumer Data Right to give consumers greater access and control of their banking, energy, phone, and internet transactions.[190] Several competition-focused inquiries and reviews in Australia built momentum around data portability as a way to catalyze Australia's calcified industries and promote innovation, starting with the Competition Policy Review,[191] and Financial System Inquiry in 2015, which led to the Productivity Commission Inquiry,[192] and followed by the Independent Review to the Future Security of the National Electricity Market—Blueprint for the Future 2017[193] released at a similar time to the Productivity Commission report. Across each of these reports, regulators felt that increased access to data would enable better product comparison, easier switching decisions, and better advisory use cases which would increase consumer benefit, spur innovation, and improve competition which were echoed in the Productivity Commission report.

As a result of the Productivity Commission report, the Government initially announced it would introduce an open banking regime to Australia and a Treasury Review into open banking in Australia was commissioned in July 2017, to decide the most appropriate model.[194] The government sought a model "under which customers will have greater access to and control over their banking data" which would "increase price transparency and enable comparison services," "drive competition in financial services" and "deliver increased consumer choice and empower bank

189 Productivity Commission (Government of Australia. "Data Availability and Use—Inquiry Report," March 31, 2017, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf. Accessed December 2019.

190 Department of the Prime Minister and Cabinet (Government of Australia). "Australians to own their own banking, energy, phone and internet data," November 26, 2017, https://ministers.pmc.gov.au/taylor/2017/australians-own-their-own-banking-energy-phone-and-internet-data.

191 The Treasury (Government of Australia). "Competition Policy Review—Final Report," March 31, 2015, https://treasury.gov.au/publication/p2015-cpr-final-report.

192 The Treasury (Government of Australia). "Improving Australia's financial system Government response to the Financial System Inquiry," 2015, https://treasury.gov.au/sites/default/files/2019-03/Government_response_to_FSI_2015.pdf

193 Finkel, Alan, et al. "Independent Review into the Future Security of the National Electricity Market," June 2017, https://www.energy.gov.au/sites/default/files/independent-review-future-nem-blueprint-for-the-future-2017.pdf

194 The Treasury (Government of Australia). "Review into Open Banking in Australia," 2017–2018, https://treasury.gov.au/review/review-into-open-banking-in-australia

customers to seek out banking products that better suit their circumstances."[195]

The Australian government determined that the CDR will first apply to the banking sector, followed later by the energy sector, and telecommunications sectors. While CDR is intended to apply across sectors, the early implementation experiences in the financial sector are most illustrative for understanding how it can support a trusted data sharing ecosystem.

KEY FEATURES OF DATA SHARING

CREATING THE POLICY AND REGULATORY ENVIRONMENT FOR DATA SHARING

AUSTRALIA

Australia's introductory information on the CDR outlined important features of how it would function and be implemented. The CDR would allow access to data held by businesses about consumers and also the products available to them but be limited only to specific data sets and classes of data holders, setting the general scope of data, yet giving regulators room to make sector-specific decisions as to the merits of extending the right to different data sets and data holders.[196] Consumer scope was set wider than initially recommended by the Productivity Commission Report to include all individuals and businesses (rather than just SMBs), providing the right for those that might not be covered by other areas of Consumer Protection law. The introductory information limited data receiving participants to "accredited third parties," necessitating the creation of an accreditation process and suggesting tiers of accreditation based on data access and usage.[197]

The indication that data should be available "in a readily usable form and in a convenient and timely manner" set important foundations for the method of data transfer and the standards necessary to enable that transfer. The Consumer Data Right implementation is by four key principles:

- The Consumer Data Right should be consumer focused. It should be for the consumer, be about the consumer, and be seen from the consumer's perspective.
- The Consumer Data Right should encourage competition. It should seek to increase competition for products and services available to consumers so that consumers can make better choices.
- The Consumer Data Right should create opportunities. It should provide a framework from which new ideas and business can emerge and grow, establishing a vibrant and creative data sector that supports better services enhanced by personalized data.
- The Consumer Data Right should be efficient and fair. It should be implemented with security and privacy in mind, so that it is sustainable and fair, without being more complex or costly than needed.

The CDR introduction also outlined key use cases for the data that would be made more widely accessible in the scheme and outlined its vision for the customer journey, in keeping with the first principle for the CDR implementation. The introduction describes comparison tools for individuals and businesses to help better inform their financial services product selection and place them in a better position to switch products or negotiate better deals. The government also forecasted budgeting tools that aggregate financial information across sources and provide insights on spending habits or recommendations for reaching savings goals, improving the customer experience,

195 The Treasury (Government of Australia). "Review into Open Banking in Australia," 2017–2018, https://treasury.gov.au/review/review-into-open-banking-in-australia.

196 The Treasury (Government of Australia). "Consumer Data Right," May 9, 2018, https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf.

197 The Treasury (Government of Australia). "Consumer Data Right," May 9, 2018, https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf.

and convenience of using financial services. These use cases are intended to be enabled in a way that is both seamless, in that is not encumbered by the types of friction seen, for instance, in the Midata program, and makes it clear that consumers are sharing their data, with the option to specify specifically which data will be shared and for how long.

As articulated in the introductory document, the regime will differ from Open Data based on its consumer-initiated data transfers. Emphasis is placed on ensuring that consumers are well-equipped to consent to these transfers and understand what they are consenting to, prohibiting open-ended or implied consents. The government hopes that these will lead to greater consumer choice, convenience, and confidence and eventually a more customer-centric data sector, with providers competing based on their ability to develop products and services that meet individual consumer needs and deliver them in a way that maximizes value for consumers.

The CDR is distinguished from other data portability provisions by the structure of its process for enacting the right in new sectors, including its mechanisms for ensuring multiregulator input and allowing specificity in sector-specific rules. While GDPR includes a cross-sector data portability right, the necessary supporting policy and processes to implement that right in sectors beyond payments, where PSD2 and open banking have initiated this process, have not been enumerated.[198]

The implementation of the Consumer Data Right brings together an even wider set of regulators. Implementation is managed with a co-regulator model, with the ACCC, the Data Standards Body and the Office of the Australian Information Commission (OAIC), and the Department of the Treasury all playing specific roles.

- The Treasurer has final approval for ACCC rules, appoints the Data Standards body chair, and works with sector-specific regulators to coordinate implementation. The ACCC is the lead regulator with responsibility for sector-specific rulemaking including outlining the necessary functionality for the regime in each sector in consultation with the OAIC, the public, and sector-specific regulators, setting accreditation criteria and processes for data recipients, managing the accreditation register, and taking enforcement action in response to serious or systemic violations of the Consumer Data Right.[199]

- The OAIC "will work with the ACCC to inform consumers, data holders, and accredited data recipients about the scheme" and will also "be the primary complaints handler under the CDR scheme" with certain investigative and enforcement powers granted to the Australian Information Commissioner. [200] The OAIC will also provide privacy expertise, advising the ACCC on privacy impacts of its rules and supporting the standard setting process to ensure privacy protections.[201]

- The Data Standards Body is responsible for setting the necessary technical standards to enable the implementation of the Consumer Data Right.[202] These technical standards include those related to data transfer with an aim of ensuring adequate safety, convenience, and efficiency, those related to data description designed to create consistency,

198 Parliament of Austrlia. "Treasury Laws Amendment (Consumer Data Right) Bill 2019," August 2019, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6370.

199 The Treasury (Government of Australia). "Consumer Data Right Booklet," September 2019, https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf.

200 Office of the Australian Information Commissioner. "About the Consumer Data Right," https://www.oaic.gov.au/consumer-data-right/about-the-consumer-data-right/.

201 The Treasury (Government of Australia). "Consumer Data Right Booklet," September 2019, https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf.

202 The Treasury (Government of Australia). "Consumer Data Right," May 9, 2018, https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf.

integrity, accuracy, and clarity while reducing redundancy and documenting business processes, and those related to security purposes with protecting the system. The Data Standards Body works in a highly collaborative way with sector regulators, data holders, data recipients, industry solution providers, consumer advocates, and working group members to ensure standards are tailored to specific sectors where necessary but created with cross-sectoral linkages in mind.[203]

This co-regulator model sets out a workable structure for coordination between functional and sector regulators which allows for sector-specific customization while also ensuring some level of harmonization across the regime.

The cross-regulator model is further supported by regulator-specific budget allocations to encourage collaboration. The initial allocation of ~$45 million AUD over four years for open banking[204] has been supplemented with additional funds for testing and assurance[205] and a related allocation to the same regulatory entities to ensure adequate privacy safeguards. In all, the government will contribute ~$90 million AUD and 45 staff over 5 years towards the regulators implementing the Consumer Data Right.[206] The ACCC will receive the lion's share of the funding, receiving nearly $60 million through 2022–2023, while the OAIC and CSIRO nearly evenly split the remainder.[207] While this does include initial funding for the energy sector, this outlay seems predominantly for open banking meaning that implementations in other sectors may require additional funding.

While still in its early days of implementation in the financial sector, the CDR regime has the regulatory foundation and organizational processes in place to expand to a wider section of the economy unlike many of the other countries that have enacted data portability provisions.

The legislation and implementation of the Consumer Data Right has been notably supported heavily by consultation with the general public and specifically with relevant private sector firms. The most important precedents to the CDR, the Productivity Commission Report on Data Availability and Use[208] and the Treasury Review into open banking in Australia,[209] were both the result of open consultations and open comment periods. The Consumer Data Right legislation underwent two rounds of consultation and two rounds of open Privacy Impact Assessments[210] while the ACCC's rules frameworks[211] and accreditation processes[212] for the Consumer Data Right have gone through public drafting and consultation processes.

203 The Treasury (Government of Australia). "Consumer Data Right," May 9, 2018, https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf.

204 Brookes, Joesph, "New Consumer Data Right Funding Set To Fuel Open Banking," WHICH-50, May 10, 2018, https://which-50.com/new-consumer-data-right-funding-set-to-fuel-open-banking/. Accessed December 2019.

205 Pearce, Rohan. "MYEFO: Government funds work on Medicare payments, ATO resilience," ComputerWorld, December 15, 2019, https://www.computerworld.com/article/3490329/myefo-government-funds-work-on-medicare-payments-ato-resilience.html. Accessed December 2019.

206 The Treasury (Government of Australia). "Consumer Data Right," May 9, 2018, https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf.

207 Note: Unclear how the 45 Average Staff Levels (ASLs) are distributed across the regulators and whether that is captured in funding allocations.

208 Productivity Commission (Government of Australia. "Data Availability and Use—Inquiry Report," March 31, 2017, https://www.pc.gov.au/inquiries/completed/data-access/report. Accessed December 2019.

209 The Treasury (Government of Australia). "Review into Open Banking in Australia—Final Report," February 8, 2018, https://treasury.gov.au/consultation/c2018-t247313

210 The Treasury (Government of Australia). "Treasury Laws Amendment (Consumer Data Right) Bill 2018," August 4, 2018–September 7, 2018, http://treasury.gov.au/consultation/c2018-t316972/.

211 Australian Competition and Consumer Commission. "Consumer data right (CDR): ACCC consultation on Rules Framework," September 12, 2018, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-consultation-on-rules-framework.

212 Australian Competition and Consumer Commission. "Consumer data right (CDR): CDR draft accreditation guidelines," September 25, 2018, https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/cdr-draft-accreditation-guidelines.

UNITED KINGDOM

While the UK is seen as a leader in the field, it's particular form of open banking differs meaningfully from forms in other countries. open banking in the UK is mandated, although only for a narrow number of large institutions, and covers all payment enabled accounts for individuals and businesses. It does include a reciprocity provision, such that financial services firms who opt to receive data under the open banking regime must also share the same relevant data. Standards have been set by a government-empowered entity to provide for not only data sharing and security but also payment initiation and account portability. Open banking in the UK is focused on consumer consent-enabled account access and data transfers and the regulatory focus on ensuring a suitable customer experience has led to an expansion in the scope of the standards.

CREATING THE TECHNICAL ARCHITECTURE FOR DATA SHARING

AUSTRALIA

CDR is also instructive for the large role that the government is playing in standard setting. Through the co-regulator model, the Data Standards Body is charged with creating standards for how to share data within the CDR scope.[213] Data61 (the data arm of CSIRO, the Australian Government's research organization) has been appointed as the interim standards body and is working with the ACCC and the OAIC to design the necessary application programming interfaces to allow for consumers to access and share their data.[214]

Data 61 is a division of the Commonwealth Scientific and Industrial Research Organization, Australia's national science research agency, focused on leading the charge on digital research.[215] Data61 claims to be one of the world's largest digital research and development organizations, boasting "more than 1,000 data scientists and 300+ PhD students from 70 countries, combined with talent embedded in 30 partner universities" and a "global network of third parties such as academia, government, and business, also known as the D61+Network."[216] The Data Standards body is led by an Independent Chair, similar to the Trustee of the OBIE, who will provide direction for the standard setting effort, select members of advisory committees, and ultimately be accountable for standards decision-making.[217]

Data61 has created several iterations of the necessary banking and common API standards and posted them openly on GitHub. Given the more limited scope of Australian open banking (including only data access and transfer but not payment initiation), the technical API standards are somewhat less complicated but do include a number of common CDR APIs allowing for customer identification and endpoint status checks, banking-specific API's to access financial data sets, admin API's to track usage metrics, security standards for authentication and authorization, and data standards to set the schema for certain data types.[218] Standards development has been aided by an advisory group of various financial sector stakeholders and consumer advocates[219] and more granularly supported by working groups which have been open to anyone with interest and expertise.[220] While input from stakeholders has been widely solicited, the

213 The Treasury (Government of Australia). "Consumer Data Right," May 9, 2018, https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf.
214 The Treasury (Government of Australia). "Consumer Data Right," May 9, 2018, https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf.
215 CSIRO Data 61. "Our Values," https://data61.csiro.au/en/About.
216 CSIRO Data 61. "Our Work Culture," https://data61.csiro.au/.
217 The Treasury (Government of Australia). "Consumer Data Right," May 9, 2018, https://treasury.gov.au/sites/default/files/2019-03/t286983_consumer-data-right-booklet.pdf.
218 Consumer Data Standards. "Introduction," https://consumerdatastandardsaustralia.github.io/standards.
219 Consumer Data Standards. "Banking Advisory Committee," https://consumerdatastandards.org.au/about/advisory-committee/.
220 Consumer Data Standards, "Technical Working Group," https://consumerdatastandards.org.au/workinggroups/api-standards/.

government has played a central role in setting a wide variety of standards, especially in comparison to more commercially-driven open banking regimes, and has set a wide mandate as to who will need to comply with these technical standards.

In addition to these technical standards, based on learning from the UK experience, Data61, in its capacity as the Data Standards Body, has also set up a customer experience working group and published CX standards and guidelines.[221] The CX standards include data language, accessibility, consent, authentication, authorization, and consent withdrawal standards.[222] These standards have been "developed for the Australian context through extensive consumer research, industry consultation, and in collaboration with various government agencies" and supported by "an Advisory Committee, spanning representatives from the financial sector, FinTechs, consumer groups, and software vendors," illustrating its commitment to understanding user needs and building collaboratively.[223]

Given its role in standard setting within open banking encompassing both technical and customer experience standards, and ongoing general CDR standards work, the Australian government has delegated extensive responsibilities to the Data Standards Body in building infrastructure to enable the Consumer Data Right.

Implementation of the standards has been planned as an iterative process, allowing regulators and the public sector to learn from less complex and less sensitive pilots early on, in keeping with global best practice in open banking. Firstly, the regulation segments the relevant types of information into tranches and sets an implementation timeline for data of increasing sensitivity: on the first date, product report data about credit and debit cards, deposit accounts, and transaction accounts will be made available. Around six months later, banks will have to share consumer data about credit and debit cards, deposit accounts, and transaction accounts, and both consumer and product data about mortgage accounts. Another six months later, both product and consumer data for personal loan accounts, as well as transaction data across account types.[224] The first deadline, which although it has since been delayed on a couple of occasions, includes a pilot phase to experiment with the API's and ensure proper testing prior to going live at scale. This staging of data sets and capabilities by respective level of sensitivity and complexity for banks of varying sizes can be instructive to other countries planning similar implementations.

UNITED KINGDOM

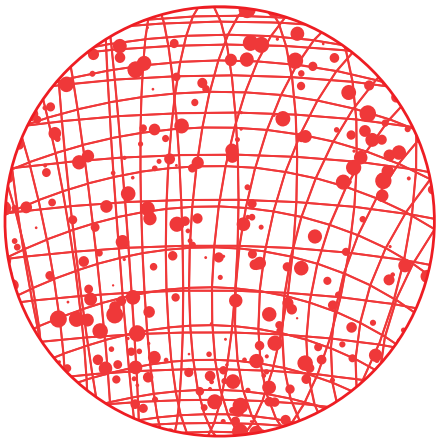
The Open Banking experience for consumers in the United Kingdom is enabled on both desktop and mobile application channels. Consumers interested in product or service offers from an existing bank or third party are redirected to the bank that currently provides their payment account. They authenticate themselves using their existing online banking credentials and then consent to share their data with the offer provider for a set amount of time. Access to their account and relevant data is then available to the service provider with unquestioned provenance in a machine readable format with no further intervention by the consumer necessary. Consumers can revoke this consent at any time, are prompted to renew it after the set time period expires, and have set channels by which to report suspicious account activity or other issues. The customer's bank would be in charge of ensuring the third party requesting data was licensed, authenticating the customer, capturing their consent, and providing access to the customer's data and account.

221 v1.2.0 available here: https://consumerdatastandards.org.au/wp-content/uploads/2020/01/CX-Standards-v1.2.0.pdf and here: https://consumerdatastandards.org.au/wp-content/uploads/2020/01/CX-Guidelines-v1.2.0-1.pdf.

222 Consumer Data Standards, "CX Standards," https://consumerdatastandards.org.au/cx-standards/.

223 Consumer Data Standards, "Consumer Experience Standards," https://consumerdatastandards.org.au/wp-content/uploads/2020/01/CX-Standards-v1.2.0.pdf

224 Australian Competition and Consumer Commission. "Consumer data right rules—data sharing obligations, phasing summary table," https://www.accc.gov.au/system/files/Proposed%20CDR%20rules%20-%20Phasing%20table.pdf.



SPOTLIGHT ON HEALTH SECTOR DATA SHARING: THE PROMISE AND PERILS OF DATA SHARING DURING COVID-19

The COVID-19 pandemic has brought into sharp focus the promise and perils of data sharing for disease surveillance and mitigation in countries across the world. The urgent need for reliable real-time information to simultaneously manage the outbreak, develop vaccines and treatments, and mitigate social and economic impacts of the pandemic have led to myriad digital applications and collaborations between data holders. Digital applications that require people to share sensitive personal data about their health status, location, and social interactions are proliferating around the world in response to COVID-19. Governments are collaborating with telecommunications service providers to track population movements at scale. New collaborations that combine different types of sensitive and nonsensitive data, as well as personal and nonpersonal data using machine learning tools to provide insights into the effects of the pandemic abound.

In countries with weak data protection frameworks, these advancements may pose a threat to privacy, hard-fought freedom, and civil liberties, and normalize unwarranted surveillance. This case study looks at three data sharing use cases and the data governance issues that they pose: (a) digital user applications for managing the pandemic, (b) Call Data Records (CDRs) to inform public policies on movement restrictions, and (c) data collaboratives for research collaborations.

USER APPLICATIONS

As the pandemic tests governments, economies, and health systems, data from individuals' use of digital devices has increasingly been used to monitor the spread of the disease, provide notification of potential exposure, and in some countries, help enforce restrictions of movement. Digital applications developed by governments, as well as private sector companies, have been used for symptom identification and case escalation, contact tracing, and exposure notification, as well as in some cases, containment enforcement. Several countries have used apps that integrate all three functions (such as the Aarogya Setu app in India), while others (e.g., South Korea) have opted for separate digital applications for each function.

PREVENTION AND SYMPTOM IDENTIFICATION

Mobile applications on smartphones, low-resource text-based, and Interactive Voice Response (IVR) systems on feature phones are being used for symptom identification and prevention in several countries. Some examples include:

- The NCOVI app, introduced by the government of Vietnam, that enables people to self-declare their health status.[225] In addition to providing

225 Dharmaraj, Samaya. "Vietnam Launches Health App to Manage COVID-19," OpenGov, March 10, 2020, https://www.opengovasia.com/vietnam-launches-health-app-to-manage-covid-19/.

information about their own health status, users are encouraged to report knowledge of suspected cases in their neighborhoods.

- The World Health Organization has launched a dedicated messaging bot in Arabic, English, French, Hindi, Italian, Spanish, and Portuguese along with WhatsApp and Facebook to keep people safe from coronavirus.

- South Korea requires all travelers to install the Self Diagnosis Mobile App on their phones and record their daily health status through the app for 14 days. Failure to comply triggers enforcement actions.[226]

CONTACT TRACING AND EXPOSURE NOTIFICATION

Mobile phone applications have been developed to track the movement of diagnosed cases in order to automatically alert people in their proximity that they may be at risk of infection. The intent of these applications is to augment conventional contact tracing techniques, which are highly labor intensive and carried out by public health authorities.

The technical specifications and implementation approaches of contact tracing solutions vary around the world.

- In Pakistan, the app relies on a cell phone tracking system based on call detail records (CDR) data, which uses the location of cell phone towers to identify the locations of users. The system identifies the locations visited by a known COVID-19 case over the prior 14 days, enabling authorities to notify the owners of phones that recently came into proximity of the infected person's phone that they should self-isolate.[227]

- In Israel, emergency regulation was invoked to allow for the temporary use of data collection systems operated by the country's intelligence service to combat security threats.[228]

- Singapore has deployed the Trace Together app—a voluntary app that uses Bluetooth technology to detect proximity to other users having this same app. When the app is downloaded, a random number is assigned to the user, and the data is stored on the phone itself in an encrypted manner. Singapore's Ministry of Health (MoH) is the only entity that can decrypt this data, and it can request the users to share it if the user is diagnosed with COVID-19.[229]

- Google and Apple have joined forces to launch exposure notification apps that work across the spectrum of Android and iOS powered phones. This application works on a decentralized model of data collection and exposure notification, with users controlling who can access their data.

As the use of contact tracing technology and applications rises, a heated debate on the nature of opt-in/opt-out clauses for these apps has emerged. In most cases, citizens can opt to temporarily share their location data to help with contct tracing. A study by epidemiologists at Oxford University estimated that more than half of the population in a given area would need to use the app that traces contacts and notifies users of exposure, combined with other tactics such

226 Park, Rosyn. "Govt Mandates Travelers From China To Download 'Self-Diagnosis' App," TBSeFM News, February 12, 2020, http://tbs.seoul.kr/eFm/newsView.do?typ_800=P&idx_800=2384604&seq_800=.

227 Jahangir, Ramasha. "Govt starts cell phone tracking to alert people at risk," The Dawn, March 24, 2020, https://www.dawn.com/news/1543301.

228 Chin, Monica. "Israel is using cell phone data to track the coronavirus," The Verge, March 17, 2020, https://www.theverge.com/2020/3/17/21183716/coronavirus-covid-19-israel-natanyahu-cellphone-data-tracking.

229 Hui, Mary. "Singapore wants all its citizens to download contact tracing apps to fight the coronavirus," Quartz, April 21, 2020, https://qz.com/1842200/singapore-wants-everyone-to-download-covid-19-contact-tracing-apps/.

as broader testing and the quarantining of vulnerable populations segments, for the app to help effectively contain the virus.[230]

Other countries such as Australia, India, and Israel have implemented laws that are harder to opt out of. In India, several government offices require clearance by the exposure notification app before permitting workers to enter. Western Australia's Emergency Management Amendment (COVID-19 Response) Bill 2020 empowers the state to install surveillance devices in homes, and direct individuals to wear an approved electronic monitoring device.

CONTAINMENT ENFORCEMENT

Governments around the world, including Singapore, India, Thailand, Vietnam, South Korea, Hong Kong, Israel, Taiwan, and China are combining phone data with human efforts to help enforce quarantine compliance.[231]

- To limit the spread of COVID-19, Taiwan has developed a geo-fence, or "electronic fence," which uses mobile phone location-tracking to ensure people who are quarantined stay in their homes. Those who are placed in high-risk groups or identified with COVID-19 are given government-issued mobile phones and monitored via location tracking. This technology monitors phone location data and alerts authorities when quarantined individuals leave their designated shelter locations or turn off their mobile devices.

- In Poland, the Home Quarantine app requires people at risk to upload several pictures of themselves to assure the government of their compliance with quarantine norms.

Data Governance Challenges

Amassing and using large volumes of personal data in the fight against the spread of COVID-19 can pose risks to the rights of individuals and communities. Beyond immediate risks that endanger physical security, user applications without the right safeguards can lead to disproportionate loss of privacy, long-term risks to freedom, and civil liberties.

Commercial sources of location data vary widely in their accuracy, precision, and volume. Importantly, anonymization of location data can prove to be a complex challenge, even with the application of privacy-enhancing technologies (PETs). Research has shown that complex data sets of personal information cannot be protected against re-identification by current methods of "anonymizing" data—such as releasing samples (subsets) of the information.[232]

The use of technologies that rely on collecting and processing highly sensitive personal data has the potential to enhance government surveillance capabilities and/or the power of commercial technology providers. The speed with which many apps were designed and deployed has, in some cases, preempted careful consideration of the safeguards required to instill the necessary public confidence in the systems. The absence of preexisting, well-defined data sharing policies has in many cases exacerbated the issue. The push to design and deploy apps to notify people of possible exposure to the virus has exposed a consequential power imbalance between the world's largest digital technology providers and sovereign states. Early technology design aggregated users' data on a central server to give epidemiologists and policymakers the ability to analyze how the virus spread within and between countries. The updates Google and Apple made to their mobile operating systems,

230 University of Oxford. "Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown," April 16, 2020, https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown.

231 TechUK. "How Taiwan used tech to fight COVID-19," March 31, 2020, https://www.techuk.org/resource/how-taiwan-used-tech-to-fight-covid-19.html.

232 Rocher, L., Hendrix, J.M. and de Montjoye, Y. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3.

however, prevents user data from being centralized, fearing such an approach could enable undue state surveillance of mobile phone users.[233] Currently, a multistakeholder consortium, the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) group is developing contact tracing technologies in compliance with European privacy and data protection laws and principles.

In addition to the push and pull between governments and technology companies, public outcries questioning aspects of the technical specifications and policies associated with state-issued apps in countries such as India and Australia[234] have led to revisions of app features and enabling legislation in hopes that strengthening trust will increase their utility in fighting the virus. The example of the Indian government's Aarogya Setu ("bridge to health care" in Hindi) highlights the importance of calibrating consent policy, transparency measures, the proportionality of data captured, purpose limitation, and data destruction policy to enabling trust in systems that share personal information directly with the governments.

Careful design of safeguards for data collection and sharing can help mitigate some of the risks posed to protecting personal data by user applications. Good practices include the collection and use of health data for health purposes only, and where possible, to collect and analyze aggregate data. When this may not be possible, the use of privacy enhancing technologies (e.g., differential privacy) should be adopted. Data destruction policies—such as where data is destroyed after 14 days unless there is a positive exposure notification—and sunset clauses on emergency measures adopted during COVID-19 should be considered and implemented where feasible, as well.

CALL DATA RECORDS TO ANALYZE COVID-19 TRANSMISSION

One source of data that has assumed importance is the use of Call Data Records (CDRs). A key driver to understand the transmission of COVID-19 is population mobility, density, and behavior. Anonymized and aggregated data from mobile phones (CDR-derived indicators) can act as a proxy to study human mobility.

Passively generated Call Detail Records (CDR) capture the geolocation and time of phone activity (calls and texts). The analysis of these CDR-derived indicators, often in conjunction with other publicly available data sets can offer valuable and near-real time insights into the impacts of mobility in a public health and epidemiological context.

In some countries, CDR-derived insights are being requested directly by governments and enabled through flexing regulation and privacy legislation. For example, the European Commission released guidance clarifying the permissible use of location data under GDPR for pandemic response and there has been unprecedented collaboration between governments and MNOs around the use of this data in several European countries.[235]

Used effectively and responsibly, this data offers the potential to support improved preparedness and rapidly inform more effective policy and operational responses. CDR-derived indicators can support forecasting and early warning modelling based on historical patterns of transmission and mobility. During social distancing, lockdowns, and mobility-based travel restrictions, CDR data can be analyzed to assess policy effectiveness. Analysis of CDR data can inform

233 https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/.

234 Greenleaf, Graham and Kemp, Katharine. "Australia's 'COVIDSafe App': An Experiment in Surveillance, Trust and Law," University of New South Wales Law Research Series, May 18, 2020, https://poseidon01.ssrn.com/delivery.php?ID=634087103098022017106084120024112070055022030067038035066070070118003106076074125073107013020035005031116084117018107005004115017036066065011127119092073001028050009035101017068007091027089101064112104072020103098008102065099071080008015006108078&EXT=pdf.

235 European Commission. (2020) Coronavirus: Commission adopts recommendation to support exit strategies through mobile data and apps. 8 April 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626.

resource allocation, such as where to place handwashing stations, high-traffic corridors, and areas that may be vulnerable to food insecurity where supply chains may need to be bolstered. Analysis of CDR-derived indicators can also support ongoing epidemiological modelling to inform decisions on reopening regions and sectors of the economy.

Countries are already utilizing this data with some success. The World Bank has facilitated data sharing for pandemic response through the COVID-19 Mobility Task Force. The task force was formed to establish partnerships and data sharing agreements with Mobile Network Operators (MNOs) and client country governments to support access to anonymized and aggregated mobility data for COVID-19 response and recovery efforts.[236]

Data Governance Challenges

As mobility data becomes more ubiquitously used for public policy, the public benefit of the proposed data use should be clearly articulated and be sufficient to justify potential risks. Especially as mobility data can be highly sensitive, using anonymized and aggregated data wherever possible should be preferred to granular, small-cell data. The use of the best quality data at a granularity to answer research questions without compromising privacy and security should be promoted.

Beyond its negotiated access, due regard should be paid to modelling likely risks in research scenarios using CDR data with or without additional data sets on a case-by-case basis, so that appropriate safeguards can be applied, and results interpreted accurately.

DATA COLLABORATIVES

Accelerating data sharing to address knowledge gaps related to the pandemic holds clear potential. However, the utility of some new data sharing applications remains unclear given a range of constraints, from a lack of relevant data to "train" and verify computational models to the enduring "digital divide," which leaves many of the world's most vulnerable beyond the reach of mobile telephones and internet access. Some of these applications involve sharing personal or otherwise sensitive data, raising concerns about how to best balance individual rights such as privacy against public safety. Questions of efficacy aside, the new forms of data sharing prompted by the pandemic are forcing quick decisions on trade-offs between competing interests that will provide important lessons going forward. As one academic researcher noted, this crisis has prompted data sharing arrangements in weeks that typically take years to negotiate because of the complexity of protecting data privacy and security.[237]

Computational modelling is being used to predict and monitor the disease across populations, to accelerate the discovery of a vaccine and therapeutics, to optimize medical supply chains, and to improve the effectiveness of policy measures such as social distancing and stay-at-home orders, among other applications. This type of data sharing, between institutions, is increasingly taking place within a new construct known as "data trusts" or "data collaboratives."

Data collaboratives are an emerging form of collaboration in which proprietary data held by a private sector entity is leveraged in partnership with another entity, often from the public sector or civil society, in order to create new public value from the exchange. Such collaboratives, or pooling of data between and across sectors, rely on governance models in which

236 World Bank COVID-19 Mobility Analytics Task Force. 2020. https://github.com/worldbank/covid-mobile-data#readme.

237 The Economist. "Countries are using apps and data networks to keep tabs on the pandemic," March 26, 2020 Edition, https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic.

the data holders agree to shared terms around the use and processing of the data, as well as the terms of releasing insights derived from analyzing the combined data sets.[238] Different forms of data collaboratives have emerged as governments, the global scientific community, and the health care industry work to understand COVID-19 and mitigate its impact.

Rapid and open sharing of data is viewed as key to accelerating the scientific research and discovery needed to develop Covid-19 treatments and a vaccine. Numerous initiatives to coordinate data sharing among researchers and public health agencies have been established, including the European Union's COVID-19 Data Platform, which aims to enable the rapid collection and comprehensive data sharing of available research data from different sources for the European and global research communities.[239] The G20 endorsed such approaches, calling for collaboration to "collect, pool, process, and share reliable and accurate nonpersonal information that can contribute to the monitoring, understanding, and prevention of the further spread of Covid-19."[240]

Governments around the world are also leveraging aggregated data sets in collaborative-like structures to inform their response. In Malawi, the Ministry of Public Health is working with a team of data scientists from the nonprofit CooperSmith to build a registry of data sets that can be combined and analyzed to yield predictions for a national epidemiological model, identify the areas of the country most at risk, and determine when and where to deploy scarce resources such as personal protective equipment and testing.[241] The inputs gathered for this effort include *public data sets* from international organizations such as population information from WorldPop;[242] data on Malawi's health care workforce maintained by the WHO;[243] and, data related to secondary risk factors such as food insecurity, poverty, and whether available on the Humanitarian Data Exchange maintained by the UN.[244] This public information is supplemented by and combined with *government-held data* on disease prevalence, health outcomes, and Malawi's health care supply chain.[245] De-identified call record data from Malawi's large mobile network operator is an important source of proprietary data added to the mix to help infer population movement and mixing based on location data derived from phone usage.

Private entities are also leveraging and processing publicly available and crowdsourced data to offer insights to understand the pandemic. For example, BlueDot software in Canada uses big data, natural language processing, and machine learning to provide insights by scraping data from hundreds of thousands of sources, including statements from official public health organizations, digital media, global airline ticketing data, livestock health reports, and population demographics. In the case of COVID-19, in addition to sending out an alert, BlueDot claims to have been able to correctly identify the cities that were highly connected to Wuhan to help predict the spread of the virus through travel. Similarly, Metabiota's epidemic

238 Verhulst, Stefaan, Young, Andrew, and Srinivasan, Prianka. "An Introduction to Data Collaborative: Creating Public Value by Exchanging Data," GovLab, https://datacollaboratives.org/static/files/data-collaboratives-intro.pdf.

239 COVID-19 Data Portal, https://www.covid19dataportal.org/. Accessed May 2020.

240 SPA (Saudi Press Agency). "G20 Digital Economy Ministers Stress Promising Role of Digital Technologies in Enhancing COVID-19 Response," https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=2081034. Access May 2020.

241 CooperSmith. "How to use your data to fight COVID-19: A roadmap for countries in Sub-Saharan Africa" April 14, 2020, https://medium.com/@CooperSmithOrg/how-to-use-your-data-to-fight-covid-19-a-roadmap-for-countries-in-sub-saharan-africa-8e8b3967ce15. Accessed May 2020.

242 World Pop. "Open Spatial Demographic Data and Research," https://www.worldpop.org/. Accessed May 2020.

243 World Health Organization. "WHO Global Health Workforce Statistics," December 2018, https://www.who.int/hrh/statistics/hwfstats/en/.

244 OCHA Humanitarian Data Exchange, https://data.humdata.org/.

245 Held in Malawai's DHSI2 and LMIS systems, respectively.

tracker service is monitoring incidence across 37 countries using 39 public data sources, ranging from the Hong Kong Centre for Health Protection to the World Health Organization. An aggregated view of the data is publicly available. Metabiota has created a near-term forecasting model, which incorporates the known characteristics of the virus.

Data Governance Challenges

Data collaboratives by definition operate under specific rules agreed to by all entities and often include enforcement mechanisms to ensure that purpose limitations are observed and de-identified personal data is not re-identified. Private efforts that rely on publicly available information sources or crowdsourced information do not raise significant privacy concerns as the ingested data is either nonpersonal or anonymized. However, many governments are either imposing or contemplating far more invasive applications to control the spread of the disease, including information on individuals' health status, location, movements, and even facial recognition.

Across each phase of pandemic response and health systems strengthening, ensuring the privacy and security of the data is paramount. For countries that already have data protection regimes in place, and that have invoked extraordinary measures, a clear path to return to the status quo ante is essential.

The COVID-19 pandemic has highlighted both the value of data sharing for supporting policy and decision-making, and the importance of coordinated efforts, long-term investment, concerted capacity building and establishing standards and common approaches. It is too soon to know if these attempts to repurpose existing data sources will have a meaningful impact on the fight against this pandemic's course. However, even in exceptional circumstances, experience is showing that building trust in data protection measures is critical to enabling robust data sharing.

WORLD BANK GROUP