Data for Better Lives: Use & Governance of Private Sector Data for Common Good - Mastercard Perspective

30 JUNE 2020

Foreword

Mastercard is grateful to the World Bank for the opportunity to comment on the Concept Note for the World Development Report 2021 on *Data for Better Lives*. The focus of the World Development Report on data could not be timelier. It comes at a time when data is emerging as a key instrument for fighting a global pandemic and when the international trade system is battling deglobalization pressures that threaten free flow of data as much as other goods and services, and when governments are struggling to identify those most in need and to ensure the effectiveness of large scale social assistance programs. We support the World Bank's effort to cultivate dialogue and inform convergence around data governance framework that enables responsible leverage of data for development purposes.

Mastercard is a global technology company that enables over a billion secure transactions per day through over 40 million merchant locations, working with around 25,000 issuer banks, leveraging more than 3,000 strategically distributed network endpoints across 210 countries in 150 currencies. Non-cash payments are data flows. As such, payment services are highly sensitive to the rules and frameworks of data governance. An efficient, safe and secure payment systems is therefore highly influenced by the quality of the rules governing data curation, use and sharing. Hence our keen interest and appreciation for the opportunity to bring the perspective of the payment sector to bear through this consultation.

The Concept Note divides the discussion into description of opportunities to put data to use for the common good and the governance framework that will help realize these opportunities. We organize our submission into two pillars that mirror the structure of the Concept Note.

In Part I, our submission describes the ways in which Mastercard puts data and data science in the service of the common good. This is done through three key modalities that are described with examples in the text:

(1) Through philanthropic collaboration.
(2) Through public private partnership for development & inclusive growth.
(3) Through data and data science services provided to governments and businesses on commercial basis.

Part II goes on to share with the World Development Report team, recommendations regarding best practices in data governance that were found to be most conducive for a well-functioning payment system. This part of the report is organized around six composite principles:

(1) Data governance should be principle-based, flexible and pro-competition.
(2) Sustainable data sharing should be proportional and should consider all interests.
(3) Free flow of data across borders is key to a resilient, secure and efficient payment system.
(4) Anonymization is a risk management protocol that is both an enabler and a safeguard.
(5) Greater convergence and interoperability of data protection and data sharing frameworks are needed.
(6) Focus on data quality, not just data quantity**.**

Before we delve into the details of our input, we leave you with one key thought as you take your worthy initiative forward, data and data use are highly diverse and diffused in all aspects of economic activity. Payment systems are a key building block of the economic system and one that is highly sensitive to data regulation. Any data governance framework must remain flexible and principle- based or it risks stifling the data benefits to development where it intends to enable them.

We look forward to continued engagement.

Table of Contents

Why Data Matters?

Data plays a critical role in driving inclusive economic growth and can be leveraged to benefit individuals and society. Used intelligently and responsibly, it can help uncover insights, reduce information inequality and advance social good. Data offers a way to identify needs and opportunities so that companies can design more useful products, and for civic and government organizations to build more impactful programs for the people and communities they serve. With accelerating digitization, data will be the fuel of the next century of innovation.

Electronic payments have been a growing driver of commerce for more than six decades. As economies evolve and become more digital, consumers, merchants, banks, governments, aid and philanthropic organizations need to trust that payments—domestic and cross-border—will go through securely, quickly and seamlessly. A trusted system for payments is necessary for firms and households to rely on to thrive and grow.

Non-cash payments are data flows. Non-cash transactions are estimated to reach 779.2 billion transactions in 2020 according to Capgemini's World Payments Report 2019 and total transaction value is projected to reach $4.5 trillion according to Statista.[1,2] It is therefore evident that payment services are highly sensitive to the rules and frameworks of data governance and that payments channels alone can magnify the economic impact of changes to the rules and regulations on data collection, processing, use and access.

Mastercard is a global technology company that connects billions of consumers, millions of businesses, tens of thousands of banks and hundreds of governments around the world through its payment network infrastructure. We enable over a billion secure transactions per day through over 40 million merchant locations, working with around 25,000 issuer banks, leveraging more than 3,000 strategically distributed network endpoints across 210 countries in 150 currencies. Mastercard handles up to 10,000 transactions in any given second, all while moving $20 billion globally on a daily basis. As such, Mastercard is heavily invested in the transparency, quality and effectiveness of data governance around the world.

Key Messages

Data governance has direct impact on the functioning of the payment system. Payment systems are a necessary building block of the economy. Their effective operation is directly impacted by the legal and regulatory framework governing use, management, protection and movement of data in each country. Any effort to shape or influence the governance framework for data locally or globally should be cognizant of the implications for the functioning of the payment system.

Data governance should be principle-based, flexible and pro-competition. Legal and governance frameworks—applying to both private and public sectors—should be principle-based, flexible, and ensure a level-playing field. Prescriptive and top-down approaches to regulation can halt innovation. Differential application of regulations can also undermine competition.

---

[1] https://worldpaymentsreport.com/resources/world-payments-report-2019/
[2] https://www.statista.com/outlook/296/100/digital-payments/worldwide

Sustainable data sharing should be proportional and should consider all interests. Data sharing triggers competing interests: national interest, public interests, private sector interests and individual interests. Balancing these interests is key. It is crucial that data sharing does not negatively affect the incentives which existed for the collection of the data in the first place.

Free flow of data across borders is key to a resilient, secure and efficient payment system. Legal and regulatory frameworks need to enable the flow of data across international boundaries. Data localization is not only a barrier to market access but it also hinders competition, increases security risks and threatens system resilience.

Anonymization is a risk management protocol that is both an enabler and a safeguard. Anonymization enables responsible use of data for common good, while minimizing privacy risks. To play its dual role, it needs to be approached with a risk management mindset that incorporates the principles of flexibility, balance and realism.

Greater convergence and interoperability of data protection and data sharing frameworks are needed. While countries are at different levels of development and institutional capacity, which merits a locally differentiated approach to data protection standards, interoperability and harmonization remains key to the functioning of cross-border data value chains like payments. This will require international development institutions to play an active role in norm dissemination and capacity building.

Focus on data quality, not just data quantity. Obtaining the *right* data of the right *quality* is central to making informed policy decisions. Ensuring the quality of data is costly. It needs alignment of incentives for society to generate, process and retain the high-quality data needed to improve lives.

Data Responsibility Principles[3]

As part of its Data Responsibility Imperative, Mastercard has established and committed to a core set of principles that guide the ethical collection, management and use of personal data. These Principles are centered around integrity, putting control back in the hands of individuals, staying ahead of the rapidly changing regulatory environment and securely leveraging data insights to help improve people's lives.

These principles underpin Mastercard's approach to data governance and to the use of data to achieve public good as elaborated in the remaining sections of this document.

Mastercard Data Responsibility Principles

- **Security & Privacy:** Companies and public authorities must uphold best-in-class security and privacy practices.

- **Transparency & Control:** Companies and public authorities should clearly and simply explain how they collect, use and share an individual's data and give individuals the ability to control its use.

- **Accountability:** Companies and public authorities must keep consumer interests at the center of their data practices.

- **Integrity:** Companies and public authorities must be deliberate in how they use data in order to minimize biases, inaccuracies and unintended consequences.

- **Innovation:** Companies and public authorities should be constantly innovating to ensure individuals benefit from the use of their data through better experiences, products and services.

- **Social Impact:** Companies and public authorities should use their information to identify needs and opportunities to make a positive impact on society.
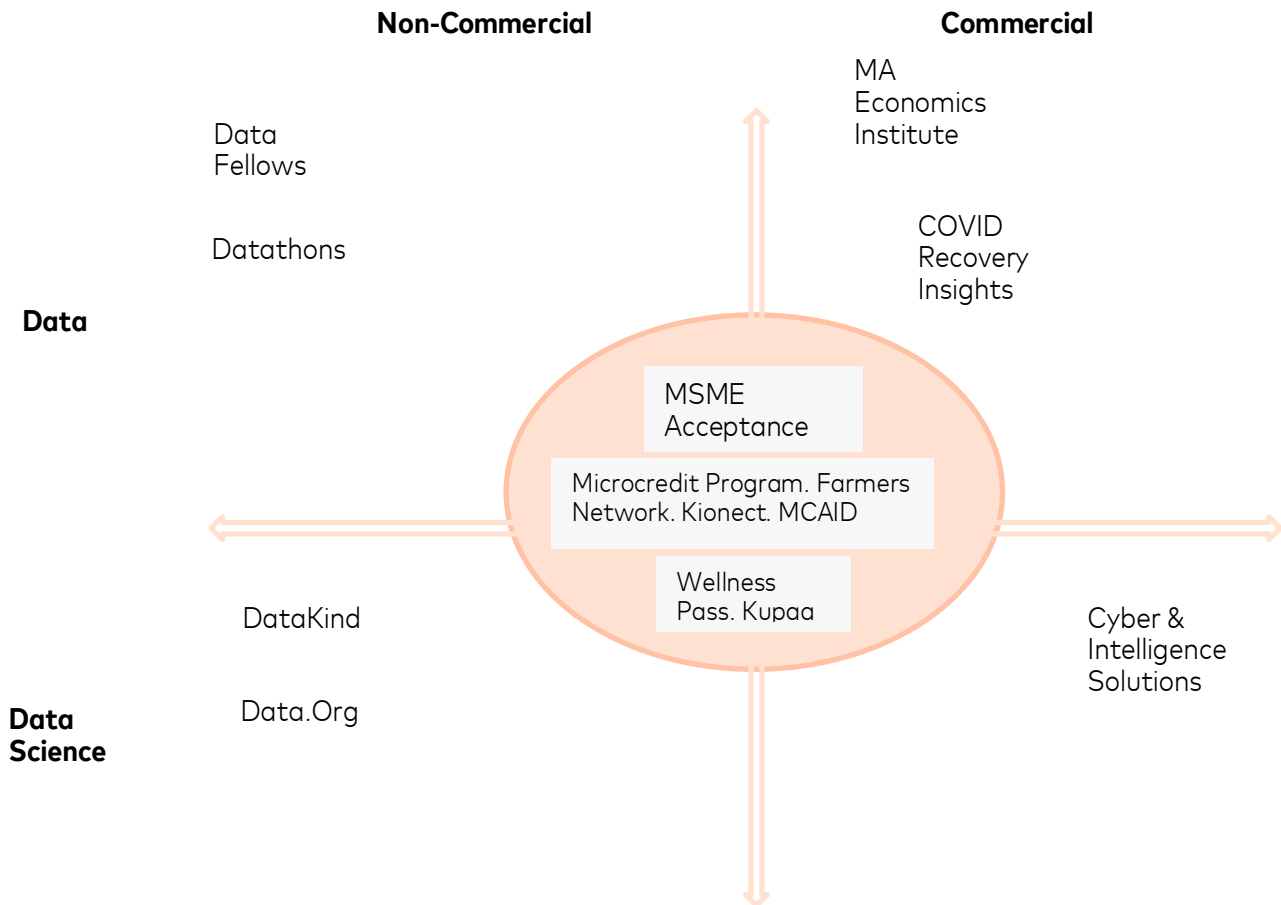
---

[3] https://www.mastercard.us/en-us/vision/corp-responsibility/data-responsibility.html

Part I: Making Data Work for the Common Good: Mastercard Approach

As a leading global payments and technology company connecting consumers, businesses, merchants and governments around the world, Mastercard possesses deep expertise in data science and access to a unique set of global transaction data. Such data, when processed expertly and responsibly, can: improve public services, enable new services (including for vulnerable populations), and support better government decision-making. Mastercard makes this possible through different instruments and initiatives that are summarized in the matrix below:

Non-Commercial   Commercial

Data
Fellows   MA
                                     Economics
                                     Institute
Datathons
                                     COVID
                                     Recovery
Data   Insights

                    MSME
                    Acceptance

            Microcredit Program. Farmers
            Network. Kionect. MCAID

                    Wellness
                    Pass. Kupaa

DataKind   Cyber &
                                     Intelligence
                                     Solutions
Data.Org
Data
Science

Mastercard deploys its data assets and data science expertise towards public interest in three ways:

(4) Through philanthropic collaboration.
(5) Through public private partnership for development & inclusive growth.
(6) On commercial basis through data and data science services to governments and businesses.

The Matrix above organizes these activities along two axes:

(1) Data v. Data Science: The common good may be advanced through the sharing of aggregated and anonymized data to support decision-making or deployment of public services. It may also be achieved through data science by deploying a stakeholder's expertise in data collection, processing and use or stakeholder's AI and machine learning technological capabilities.

(2) Non-Commercial v. Commercial: Using data or data science to advance public good can be offered through philanthropic partnership with researchers, charitable and academic organizations or civil society. It is also achieved through data and data analytics services that are provided to governments and businesses through the normal conduct of business.

At the center of the Matrix, a group of initiatives straddles both commercial and non-commercial activities. This is where public private partnerships are needed to make data-driven solutions accessible to last mile consumers and communities.

The paragraphs below describe real-life examples of the use of data and data science for public good through these three different modalities.

Data-Focused Philanthropic Collaboration

At Mastercard, we are using data and data science to accelerate social impact through research, skill building and the development of new technology platforms. These include the following initiatives led by the Mastercard Center for Inclusive Growth:

- *Data Science for Social Impact* in collaboration with the Rockefeller Foundation. This is the idea that building the field of data science within the social sector will help ensure every organization has the tools and capabilities to harness data science to improve lives. It launched with a joint US$50 million commitment over five years, including US$20 million to DataKind, a global platform for meeting the data science needs of the social sector.

- *Data.org*, a new platform for partnerships to build the field of data science for social impact. We are hoping to drive transformational progress by demonstrating the power of data as a tool for solving long-standing and seemingly intractable social problems. Towards this end, we committed US$28 million over the next three to five years and will collaborate with strategic funding partners to support specific initiatives that leverage data science to tangibly improve lives. We are also partnering with universities around the world to create a core curriculum on data science for social impact. The Rockefeller Foundation's *Universal Labelling Project* is investing in training data for machine learning applications for high-social value.

- The Mastercard Center is looking ahead to future needs so that this now-fledgling field has a powerful base of resources, including datasets, case studies, research, investment and technology. It has also initiated a public advocacy campaign to encourage technologists to work on pressing social issues and are helping create a pipeline of projects in the field.

- Our *Data Fellows program* leverages Mastercard's anonymized and aggregated transaction data to support and empower thought leaders in advancing social impact and inclusive growth. The Fellows, data scientists from diverse academic and government institutions, collaborate with our own data scientists to identify patterns, develop research papers and glean insights that drive economic growth for underserved segments of society. The 2019 inaugural class of Data Fellows delivered groundbreaking research demonstrating the power of data philanthropy to address social issues around inclusive growth.

Data for Good - Combining Open Source and Private Data to Track the Effectiveness of Public Policy

The Inclusive Growth Score combines Mastercard proprietary data with open source data to score neighborhoods on inclusive growth. The tool allows users to benchmark and measure changes in levels of inclusion in pre-defined geographic zones.

The tool measures each zone against 18 metrices, which include public source data such as: population growth, home value, internet access, commute time, female poverty rates. Combined with payments aggregated and anonymized payments data, the tool can reveal average spend growth or commercial diversity.

The tool creation was inspired by the "Opportunity Zone" incentive established by the U.S. Congress in the Tax Cuts and Jobs Act of 2017. The incentive seeks to encourage long-term investment in low-income urban and rural communities across the United States. *The question is whether the incentive is benefiting the target neighborhood and their communities.*

By setting a baseline and using high-frequency payments data to monitor trends, the tool helps policymakers see whether indicators of inclusive growth are moving in the right direction.

Understanding the data requires knowledge of local context, for that, the Mastercard Center for Inclusive Growth partnered with civil society organizations in the United States.

As countries around the world work to make growth more inclusive by targeting their lagging regions and communities, innovative ways of harnessing data in real time and at a local level will be needed to inform geo-specific policies and measure their impact.

The Center for Inclusive Growth is committed to using data science for social impact because better inputs can lead to better outcomes. A much needed current and quantitative approach to decision-making can help lift communities everywhere. The Inclusive Growth Score is the Center's contribution to that ongoing effort.

For more information, please see: www. mastercardcenter.org/ insights/measuring-opportunity-one- neighborhood-at-a-time

Public-Private Partnership for Development & Inclusive Growth

Mastercard has also initiated cross-sector collaborations and programs using data and technology which promote inclusive growth and financial inclusion, including:
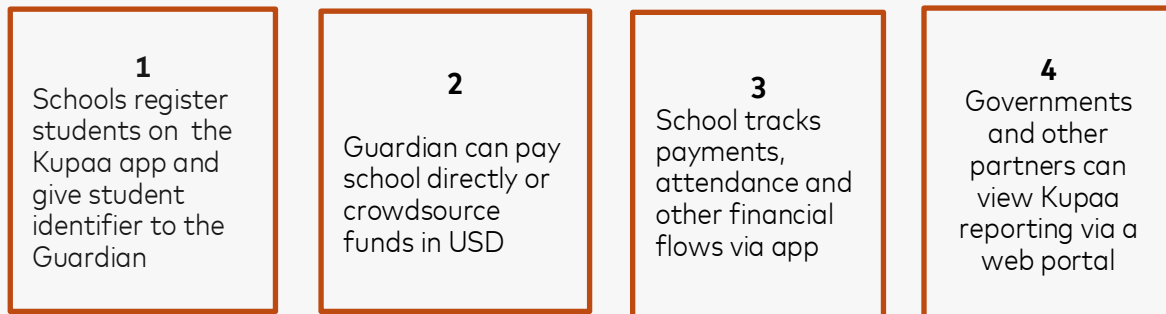
- *Mastercard Farmer Network* digital agricultural marketplace and *Mastercard Microcredit Program* which are providing smallholder farmers and micro-retailers with the digital identities and financial histories needed to access mobile-based lending, and enabling financial institutions to develop data-driven savings and loans products;

- *Kupaa* which provides a secure and accessible mobile payments service for families and friends to pay children's school fees in directly to schools; and

- *Wellness Pass* which enables medical clinics to maintain records of vaccinations and provide SMS reminders of appointments to caregivers.

Data Partnerships - Improving Access to Education for Marginalized Communities through Data Infrastructure

Kuppa, "to fly high" in Swahili, is an interoperable digital infrastructure that improves the efficiencies of schools in marginalized communities in managing the collection of fees and tracking attendance. The platform allows guardians to pay school fees digitally and remotely using mobile money and provides schools with the ability to digitally track students' attendance and payments in real time.

The platform also enables "crowdfunding" by allowing family and friends to pay on the platform towards the students' school fees.

How it Works:

1	2	3	4
Schools register students on the Kupaa app and give student identifier to the Guardian	Guardian can pay school directly or crowdsource funds in USD	School tracks payments, attendance and other financial flows via app	Governments and other partners can view Kupaa reporting via a web portal

Kupaa brings many benefits:

(1) It enhances transparency for education authorities allowing them to track school grant disbursements as well as spending against grants.

(2) It improves the operational efficiency of the school by giving it a view of payments in real-time thus simplifying accounts management.

(3) It increases safety for the schools by sparing the schools the risk of keeping large volumes of cash.

(4) It frees school administration time and resources from waste in manual collection of payments and management of accounts.

Data and Data Science Services to Governments & Businesses

Mastercard's offerings go beyond transaction processing. We harness the power of real-time, anonymized and aggregated transaction data, powerful software platforms and data science expertise, to enable customers-- both businesses and governments—to take a holistic view of consumer behavior and distill actionable insights and make more data-driven decisions. All this is done while using privacy-enhancing techniques, such as world-class anonymization and aggregation to protect individuals' privacy and security.

The *Mastercard Economics Institute* was launched in 2020 to analyze macroeconomic trends through the lens of consumer transactions and behavior. It comprises a team of economists, analysts and data scientists drawing on Mastercard insights—including Mastercard SpendingPulse™—and other publicly available data to deliver tailored and actionable insights on economic issues for key customers, partners and policymakers.
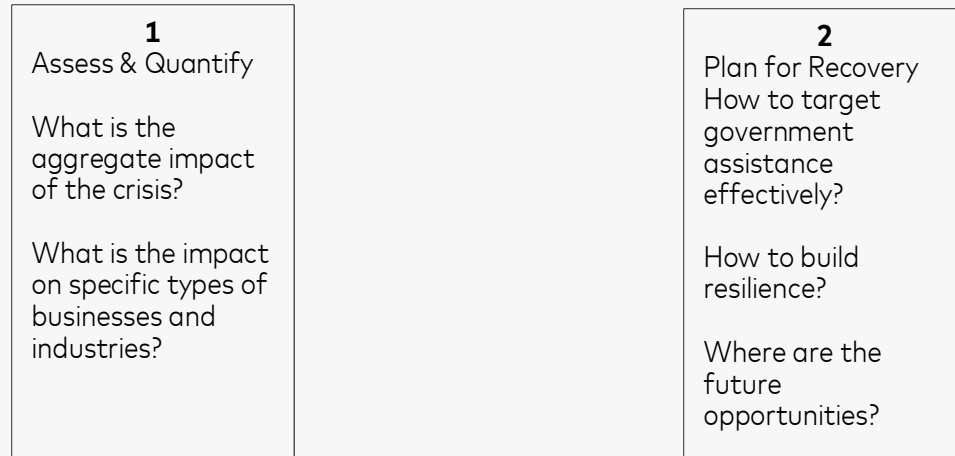
Mastercard SpendingPulse provides market intelligence based on national retail sales across all payment types. The findings are based on aggregated sales activity in the Mastercard payments network, coupled with survey-based estimates for certain other payment forms, such as cash and check. This analysis allows users to answer questions such as: Is spending in a particular area expanding or contracting? Which regions and segments are seeing the most strength in spend?

COVID Recovery Insights - Evidence-based crisis management with high frequency data

Businesses and governments across the globe are looking for resources to help better manage the health, safety and economic risks presented by the recent pandemic. To assist in these efforts, Mastercard has launched Recovery Insights, a set of tools, innovation and research drawing on aggregated and anonymized spending insights to provide an ongoing view of economic health. As part of this initiative, Mastercard is making certain insight-driven tools available at no cost to governments and select businesses.

To assess the local effects of COVID-19 and build a foundation for an inclusive recovery, dozens of cities and national governments are now using Mastercard tools. These solutions help inform budget planning, optimize aid disbursement, understand which merchants are open for business, and prioritize investment to support those most impacted by the pandemic.

1
Assess & Quantify

What is the aggregate impact of the crisis?

What is the impact on specific types of businesses and industries?

2
Plan for Recovery
How to target government assistance effectively?

How to build resilience?

Where are the future opportunities?

Mastercard Geographic Insights: With an interactive mapping interface, Mastercard Geographic Insights provides a clear picture of performance across geographies and merchant categories. Governments, businesses and others can evaluate the retail performance of locations based on spend, ticket size, accounts, frequency and more.

Mastercard Business Locator: This tool offers the most accurate, up-to-date and comprehensive view of merchants open for business on any given day, delivered by API or data. The solution can help governments gain insight into the operating status of businesses in local areas to ensure that the needs of citizens can be met and to understand the short- and long-term economic impact of policies. They can also share these insights (as in the case of Italy and UK) with residents to help them better understand which of their local businesses are open.

Part II: Powering Payment Systems with Effective Data Governance

Data governance frameworks for public and private sectors should be principle-based, flexible, and should ensure a level-playing field.

Trust is at the heart of the payment system as it facilitates confident transactions between strangers. Data governance and data security are key drivers of trust in payments since trust is generated by the resilience and security of the system as much as by the standards and governance that underpin its operation.

Our own research bears this out: 93% of consumers surveyed are more likely to trust a company that commits to data responsibility principles.[4] Concerns around security and privacy were also the major reasons cited by individuals in Europe for their reluctance to share their financial information with third parties.[5] This underscores the need for legal and regulatory frameworks that embody these principles in order to engender trust.

We now operate in a rapidly changing world with many disruptive forces. Security and protection concerns should not lead to rigidity that stifles innovation. Connected to the notion of a principle-based regulatory framework, approaches to data governance need to remain **flexible** to account for these rapid changes, and to avoid check-box approaches to compliance.

Legal and governance frameworks should also promote **a level-playing field** within sectors and across sectors. The data governance framework should ensure that existing and new participants are neither differentially preferred nor barred by the regulatory requirements. This is especially important in the context of data sharing where the dissemination of large quantities of data to a larger number of entities will increase the potential for data breaches and the misuse of the data.

Recommendation: Data governance and sharing frameworks should be principle-based, flexible and ensure a level playing field.

The Principles in data governance frameworks consist of accountability, transparency, individuals control over their data, fairness and integrity, and security.[6]

Flexibility is needed in the following areas:

- **Data Sharing Modalities.** While mandatory rules for data sharing could make sense in situations of urgent humanitarian crises and natural disasters, the standard for collaboration should be one in which clear safeguards, roles and responsibilities are mutually agreed upon by all parties. Importantly, the sharing of data is not always the most effective, proportionate or efficient way of achieving the public policy objective. Other options include sharing of the data science behind the data as well as the development and retention of data skills. These other, know-how sharing options may often be better solutions to the issue at hand, maximizing the benefits while minimizing the threat to user trust in the payment system.

---

[4] https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/global-data-responsibility-whitepaper-customer-10232019.pdf

[5] Open Banking: Open Minds? Consumer Appetites for New Banking Services, November 2019, Mobey Forum

[6] These are commonly adopted data protection principles which can be found in international and regional data protection frameworks such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Data, the APEC Privacy Framework, and the ASEAN Framework on Personal Data Protection.

- **Technology-neutrality & non-prescription**. Regulatory frameworks and standards, including those relating to cybersecurity, should be technology-neutral and non-prescriptive, in order to cater for market and technological developments.

- **Industry-led technology standards**. Interoperability through standardized APIs, which are developed and managed by industry, may be superior to government-enforced standards. Government established or endorsed bodies setting standards on behalf of industries they oversee should be avoided. These bodies may stifle innovation and lead to delays or unnecessary costs. For example, the OpenAPI Specification was developed by industry participants, and is currently managed by the OpenAPI Initiative.

A Level Playing Field is achieved when:

- All actors within the chain from data origination to data re-use have the same standards, responsibilities and restrictions for data of the same type and level of sensitivity. For example, if a bank cannot use transaction data to market to a customer, the same restriction should apply to a downstream fintech that receives or originates the transaction data.
- Data governance frameworks apply to all entities regardless of nature, size or revenue. In order to build a trusted ecosystem for data use and sharing, the confidentiality and protection of personal data are fundamental elements, which all parties in that ecosystem must be subject to. Exceptions to this – either for the public sector or small enterprises - will only result in accountability gaps in the ecosystem.
- The creation of asymmetries in access to data is avoided. Mandatory or even voluntary release of data may result in further concentration of power in favor of local incumbents. Enabling one-way access to datasets may exacerbate dominance and competition issues. Therefore reciprocity should be a key feature of data sharing frameworks.

Sustainable data sharing should be proportional and consider all interests.

Data sharing mandates and modalities come with risks including privacy, security and liability concerns, and the risk of disincentivizing data collection, management and processing. We believe that, in order for data sharing to be sustainable, it is necessary for all interests to be considered: the national interest, the public interest, the firms' interests, and the interests of the individual. It is crucial that data sharing does not negatively affect the incentives which existed for the collection of the data in the first place.[7]

Common concerns include:

- The use of data for purposes beyond the public interest. Delineation of the scope of public interest is often unclear and undefined;
- Potential distortion of competition. Data access regulations may give competitors access to data which allows the competitor to discern output, customers or strategies of another competitor. This is especially so in a market with only a few providers, and where it may be relatively easy to identify the provider which the data relates to;
- Loss of compensation for datasets accessed. Organizations may have made significant investments in ensuring data quality and data cleansing. Data needs to be standardized to be transformed into a format suitable for processing or analysis. Duplicates of a record need to be removed to ensure accuracy in the analysis. Various tools and techniques may be also deployed to inspect and verify the

---

[7] OECD Report, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across societies, accessible at https://www.oecd-ilibrary.org/sites/276aaca8-en/1/2/4/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book

data for errors. Software may be used to assess quality of the data, and to identify potential errors. Organizations may use vendors for data storage, and also incur expenses for building and maintaining mechanisms for data extraction and access;

- Liability and responsibility for incorrect data, lost or stolen data and misuse of data by recipients;
- Existing intellectual property rights and any other rights in databases or derivatives of information;
- The risk of re-identification arising from the combination of datasets from different sources (see comments below regarding anonymization); and
- Legal authority to share data. Organizations which act as data processors or service providers (on behalf of the data controller or their clients) and which may have access to data, may not have the legal authority to share data without the permission of the client / data controller.

Recommendation: Data sharing frameworks should be subject to a well-defined regulatory impact assessment that evaluates the following.

- The demand for access to a particular dataset and its benefit against the costs associated with such access. This includes the administrative cost to the organization in managing access as well as the costs associated of loss of return on investment in developing the datasets and any possible competition or liability costs.
- The rights and protections relating to the data including intellectual property and privacy protections, contractual rights and rights granted under existing laws.
- The privacy and security concerns that may arise from data sharing. Besides the potentially increased risk of loss or misuse of data, there are also concerns regarding third parties who may utilize access to network or transaction datasets to circumvent the protections afforded by information security and fraud prevention tools; and
- Consumers' attitudes around data sharing. Detailed research of public attitudes towards data sharing should be a precursor to regulations relating to data sharing. Regulations that are not grounded in an understanding of the public's concerns and attitude towards data security and privacy may either be too restrictive that it undermines innovation or too permissive that it undermines trust.

For example, the European High-Level Expert Group on B2G data sharing proposed a balancing test: the public interest should be balanced against the interests of stakeholders - such as industry and individuals;[8] the cost should be balanced against the benefit, and the risk of harm if the data is not used. The Expert Group also recommended the creation of a principle of non-discrimination, and the non-use by public-sector bodies of private sector provided data for commercial purposes.[9]

Legal and regulatory frameworks need to enable the flow of data across international boundaries .

Local data storage requirements, also known as data localization, are a barrier to market entry and operations for payment service providers. These requirements hinder cross-border payment services because data is essential in every step of transaction processing[10] The supply of payment services often requires the cross-border flow of data, not only in settling cross-border transactions, but also in domestic transactions, when both the merchant and the consumer are located in the same market but the processing of the transaction (or parts of it) are carried out elsewhere.[11]

---

[8] Final Report of the High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European Strategy on business-to-government data sharing for the public interest*, 2020, accessible at: https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf
[9] ibid at page 80
[10] APEC, Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses, Chapter 4: Payment Services
[11] World Economic Forum, "Addressing E-Payment Challenges in Global E-Commerce"

Countries enact data localization in response to technological innovation for a variety of well-intentioned but misguided reasons, such as addressing privacy and cybersecurity concerns, allowing their government's access to payments data, and encouraging domestic industries and economic growth. Data protection regimes like the EU GDPR and others demonstrate that it is possible to ensure a high level of protection and privacy without prohibiting offshore data transfers or the use of offshore infrastructure. Such data protection regimes are designed to provide individuals a high level of protection *while* facilitating data flows.[12] Further, a growing body of research suggests that data localization fails to achieve many of these goals and adds significant costs to the local economy, increases security risks, and does not improve consumer privacy.[13] For instance:

- A McKinsey analysis reports that open data flows more broadly are actually critical to future economic growth and likely increase world GDP by 10.1% over the past decade.[14]
- The Faculty of Economic & Political Science at Cairo University found that restrictions on international data transfers hinder "the necessary and essential role of global trade in realising economic development", and went on to say, "this is evident in production costs as reflected in the increase in the prices of goods, which would lead to a decline in incomes."[15]
- A European Commission Impact Assessment on the free flow of data found that deploying cloud data centers beyond the needs dictated by the market, or limiting choices for the location of a planned data center can have serious cost and environmental implications.[16] The report estimated that the average lifetime cost of a cloud data server in the EU was 276.9 million Euros and suggested that the additional cost would cascade down the value chain to the consumer eventually. The report also highlighted that the proliferation of data localization restrictions could have a negative environmental impact, and could hamper the development of innovative energy optimization or efficiency in data centers, e.g., maximizing the use of renewable energy by shifting the loads of data processing to a data center where renewable energy is available at a particular moment.

Data localization has negative effects for both foreign and domestic payment service providers. It discriminates against foreign firms as it makes their services more costly or complicated in comparison to local firms, while local firms are more likely to use local data storage services. However, many local firms (especially start-ups) increasingly rely on cloud computing services to manage data and process transactions, which would be prohibited under many data localization measures, resulting in increased costs for local firms.[17] In this way, many of the costs of data localization are not passed along to foreign companies but to local start-ups, financial institutions and, ultimately, consumers. Furthermore, data localization requirements impede the free flow of data, which affects the use of integrated, secure and efficient payment systems worldwide, with consequences for innovation, fraud, and security.[18]

---

[12] For an overview of the various cross-border data transfer mechanisms which can be found in modern data protection laws, please refer to Centre for Information Policy Leadership White Paper, Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy, September 25, 2017, accessible at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf

[13] Meltzer, Joshua, and Peter Lovelock, Regulating for a digital economy: Understanding the importance of cross -border data flows in Asia, Brookings, 2018; Cory, Nigel, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", Information Technology & Innovation Foundation, 1 May 2017

[14] Manyika, James, et al., "Digital globalization: The new era of global flows", McKinsey Global Institute, 24 February 2016

[15] Mona Farid Badran, (2018) "Economic impact of data localization in five selected African countries*", Digital Policy, Regulation and Governance,* Vol. 20 Issue: 4, pp.337-357, available at: https://doi.org/10.1108/DPRG-01-2018-0002

[16] Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (2017) https://eur-lex.europa.eu/resource.html?uri=cellar:51c9c47e-985c-11e7-b92d-01aa75ed71a1.0001.02/DOC_1&format=PDF

[17] Thaker, Aria, "India's data localisation plans could hurt its own startups the most", Quartz India, 16 October 2018; Leviathan Security Group (2015), Quantifying the Cost of Forced Localization, http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization

[18] APEC, Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses, Chapter 4: Payment

Other practical challenges can also arise if data transfers are prohibited. For example, COVID-19 triggered shutdowns had resulted in disruptions in call centers within countries. According to one account, a service provider had moved more than 50% of call center volumes from Philippines to India, due to the lockdown in the Philippines.[19] The ability to shift call volumes to other call centers in other countries would not have been possible without the ability for data (both the call and the consumer's details) to be transferred to an offshore call center.

Data localization requirements may also contravene a country's market access commitments under GATS, as the cross-border transmission of data constitutes the service being supplied (and thus blocked via data localization).[20] Forced data processing and storage also discriminates between local and foreign providers, thus breaching national treatment commitments. They may also breach provisions in the GATS Annex on Telecommunications, which ensures that foreign-service suppliers are allowed to use basic telecommunications for the movement of digitized information.[21]

Efforts should be made to promote cross border data flows through multi-lateral, bilateral and regional trade initiatives and agreements which seek to provide individuals with a high-level of protection while facilitating cross-border flows of data. For example:

- The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) reinforces and goes beyond WTO provisions on financial services though it is still limited in the scope of its commitments (e.g., the data flow provisions that prohibit barriers to data flows and forced localization do not apply to financial services, including payments); The United States–Mexico–Canada (USMCA) trade agreement goes further than the CPTPP in providing explicit, detailed protections for the free flow of data and prohibitions on data localization in the financial services chapter, and serves as a model for agreements on digital trade.[22] The USMCA also provides a clear framework to allow the free flow of data, while ensuring parties have regulatory access to data[23] This is an important development as many policymakers try to justify data localization on the belief that it is necessary to ensure a government's access to the data;
- The European Union's free trade agreement proposals with Australia, New Zealand and the UK which contain provisions on data flows which rule out forced data localization requirements;
- Ongoing WTO e-commerce talks to develop new rules which will attempt to address forced data localization requirements; and
- ASEAN's Cross Border Data Flow Mechanism which seeks to facilitate intra-ASEAN data flows.

Recommendation: There is a need for a stronger global norm against restrictions on cross-border data flows. Future trade negotiations as well as international development institutions have a role to play in promoting a stronger norm in favor of enabling cross-border data flows.

Services

[19] McKinsey Digital, How CIOs can work with outsourcing providers to navigate the coronavirus crisis, April 2020, accessible at https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/How%20CIOs%20can%20work%20with%20outsourcing%20providers%20to%20navigate%20the%20coronavirus/How-CIOs-can-work-with-outsourcing-providers-to-navigate-the-coronavirus-crisis.ashx

[20] Provision and transfer of financial information and financial data processing as referred to in subparagraph 5(a)(xv) of the Annex on Financial Services.

[21] WTO, "Annex on telecommunications, 5. Access to and use of Public Telecommunications Transport Networks and Services"

[22] Articles 17.17 and 17.18 of the USMCA trade agreement

[23] Article 17.18 of the USMCA trade agreement

Cross-border Data – The Lifeblood of Fraud Prevention

Trust in the security of data is a key enabler of data use for development. The safeguards for the protection of data also extend to the availability and effectiveness of fraud prevention and detection tools which are used to protect against malicious actors.

For example, Mastercard's Decision Intelligence™ and Safety Net™ protect individuals, banks and merchants by minimizing potential losses from fraud, and ensures confidence in electronic payments and the digital economy.

These tools rely on fraud models built from historical payment transaction information and global or multi-country data sets. In order to determine what is potentially fraudulent, the fraud models need to be trained to spot what transactions are fraudulent and what transactions are not fraudulent. The models need to score potential fraudulent activity against historical behaviors (i.e., months of transaction data) for the specific account, and against norms for all accounts. For example, if a payment account has only been used for purchases for low dollar value purchases, the fraud models may score a payment transaction for a high dollar value purchase transaction as potentially more at risk for fraud.

This ability to leverage multi-country data sets is crucial as the fraud and threat environment is constantly evolving unrestricted by national boundaries. Fraud trends which appear in one region or country will quickly appear in others as fraudsters operate in, and individuals travel to different countries and transact online with merchants in different countries.

Data therefore needs to be analyzed together as a whole in order to spot patterns of fraud. Leaving out country datasets from the analysis will only deprive the models of the training required to accurately detect fraud. The creation of data-walls around more countries and the promotion of prohibitions on the transfer of data will ultimately mean that each country will only be able to identify local patterns of fraud and will be blind to wider fraud patterns and threats. Ultimately, this would only have the unintended and undesirable consequence of benefiting criminals while leaving individuals and merchants unnecessarily exposed.

Anonymization is a risk management approach which enables responsible use of data for development, while minimizing privacy risks.

Anonymization is an important tool to enable the analysis of data (and to benefit from the data insights derived from the analysis) while protecting individuals' privacy. It is important to recognize the dual role of anonymization as an enabler and a safeguard to data use and sharing. Anonymization can act as *both* an enabler for innovation and a safeguard to ensure the protection of privacy.[24]

This dual emphasis requires a risk management approach to anonymization to avoid disruption of important public and private interests in access to and use of data.[25] A risk management approach to anonymization can also help to identify potential re-identification risks relating to the sharing and combination of non-personal datasets among entities.

Recommendation: Data governance and sharing frameworks need to adopt a balanced risk management approach to anonymization and would require:[26]

- A risk-based assessment that considers various factors including: the type and sensitivity of data being used, the potential for combination of data-sets (especially non-personal data-sets from diverse sources), and the operational, technical and legal controls to determine the *risk of re-identification;*[27]
- A flexible approach to reconciling competing interests that considers a range of technical measures (e.g. k-anonymization, pseudonymization, data swapping or suppression, etc.) and does not focus on a fixed end state of the data.[28]

Good practice risk management approaches have been adopted in several countries which recognize that the key concept is the application of risk management controls to reduce the risk of re-identification.[29]

As such, we believe that a description of a standard or framework of anonymization should incorporate a risk management approach which considers the points raised above. In doing so, anonymization can then fulfill its role as an enabler which maximizes the benefits of responsible development and safeguard which minimizes the privacy risks.

Greater convergence and interoperability of data protection and data sharing frameworks is needed.

Legal and regulatory frameworks are at various stages of development across the world. Public policy objectives and institutional capacity varies between countries at different levels of

---

[24] For example, Japan introduced amendments to its privacy law to allow for anonymization which aligned with its strategy of "revitalization of industries by utilizing data", Policy Outline of the Institutional Revision for Utilization of Personal Data issued by Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society at page 6, accessible at https://japan.kantei.go.jp/policy/it/20140715_2.pdf

[25] For examples of use cases, see Polonetsky, Tene and Finch, Shade of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) accessible at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2827&context=lawreview

[26] For a useful summary of this approach: Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymization Decision-Making Framework (UKAN, 2016) accessible at https://ukanon.net/wp-content/uploads/2015/05/The-AnonymisationAnonymization-Decision-making-Framework.pdf; and Polonetsky et al, ibid

[27] Polonetsky, Tene and Finch, ibid at page 622

[28] Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymization Decision-Making Framework (UKAN, 2016), at page 1

[29] Advisory Guidelines on the PDPA for Selected Topics, Chapter 3 accessible at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Chapter-3-9-Oct-2019.pdf; De-identification and the Privacy Act, March 2018 accessible at https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act

economic development calling for variation in approaches. Yet, the need for international harmonization abounds.

Direct transplantation or copying of laws from one context to another would be ill-advised, yet there are benefits in achieving greater convergence in data protection frameworks. Fragmentation and inconsistencies between data protection and data sharing frameworks within and between countries will hinder collaboration, raise costs and create uncertainty for all stakeholders involved.

These inconsistencies are real and range from basic and fundamental concepts such as the scope of personal data including what would be considered as anonymized data, to different legal basis for processing and transferring personal data. A difficulty in coming to consistent definitions of what is personal data and what is non-personal data (i.e. an agreed taxonomy) will lead to disagreements as to what can and should be shared. The lack of consistency and interoperability between countries' regimes will create a reticence effect on the part of the participants when using or sharing data for public purpose.

These risks have been highlighted by the European High Level Expert Group on Business-to-Government Data Sharing, which identified that the current fragmented rules around data sharing between EU member states, and sectors leads to growing uncertainty on the rules and operating models for data sharing, and increases the cost of compliance inhibiting data sharing[30] It is worth noting that improving consumer confidence and lowering business costs was one of the key reasons for the introduction of a single data protection law in Europe, the GDPR. [31] UNCTAD has also highlighted that fragmentation in data protection and data transfer regulations could lead to barriers to interoperability.[32]

Recommendation: Greater convergence and interoperability in data protection and data sharing regulatory frameworks is needed. Initiatives like the APEC Privacy Framework[33], ASEAN's Cross Border Data Flow Mechanism to facilitate intra-ASEAN data flows[34], and the Asian Business Law Institute's work in promoting greater convergence[35], which seek harmonization of data protection regulations are positive developments which should be supported, promoted and emulated. There is a role for standard-setting bodies and international organizations, like the World Bank, to play in promoting streamlining of concepts and harmonization of regulatory standards.

Focus on data quality, not only data quantity

In *Doughnut Economics,* Raworth (2017) argues that "living metrics" are crucial to enable the shift to regenerative economics. Similarly, Standing's work on basic income (2017) discusses in detail the data requirements for running and managing successful economic support programs. Both works stress the importance of having not just large quantities of data but having the *right* data for the purpose required. Having data on the factors relevant to public policy making is *meaningless* if that data is not accurate, recent and reliable, and may even be harmful in

---

[30] Final Report of the High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European Strategy on business-to-government data sharing for the public interest,* 2020, at pages 35-36

[31] https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

[32] UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development,* 2016, at page 32, accessible at: https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

[33] https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[34] https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf

[35] https://www.abli.asia/PROJECTS/Data-Privacy-Project

generating inaccurate policy outcomes. It is the *quality* of the data that truly enables development, not just the *quantity* of data.

For example, Mastercard's Microcredit Program enables the use of wholesale transaction data for the purposes of building business records for small businesses, enabling them to apply for credit from financial institutions. The reliability, accuracy and availability of wholesale transaction data for small businesses in the program are key to allowing small businesses to build a financial history, enabling low-risk credit decisions by financial institutions, and allowing small businesses to expand their businesses, and achieve financial inclusion.

While scale matters when it comes to data, this is true only partially. A recent article in *Harvard Business Review* examined, as the name of the article suggests, "When data creates competitive advantage…and when it does not" (Hagiu & Wright, 2020). Whilst the authors accept that most businesses benefit from large volumes of data, they argue that this will not by itself build strong competitive positions. For example, differentiate between products and services with a high-inherent value for data (such as improving the accuracy of driver-assistance systems) and those where the value of learning from customers is relatively low (such as smart televisions where purchasing decisions are made more on size, quality and ease of use of the television).

Recommendation: Deep awareness and understanding is crucial amongst all stakeholders, both public and private, that obtaining the right data, and the right quality of data, is central to making informed policy decisions. Since building quality datasets requires knowledge and investment, data governance and sharing frameworks need to ensure alignment of incentives and balancing of stakeholders interests. Building the capacity of all stakeholders in the curation, processing and sharing of data is also essential for managing quality and scale and is a rich space for public private collaboration.

Conclusion

Data plays a critical role in driving inclusive economic growth and can be leveraged to benefit individuals and society. It cannot do so however unless it is used intelligently and responsibly. Private sector entities like Mastercard can help in promoting the public interest through the data they collect as well as through the expertise in data sciences that they harness. Our wide-ranging efforts in using data for good and in collaborating with others is reflected by our philanthropic efforts, our public-private partnerships for development and inclusive growth and our data science services for governments and businesses.

Underlying these efforts is a bedrock of trust which is built up through system resilience and security, and the standards and governance around the use of data (whether for payments, analytics or sharing). At Mastercard, we have strengthened this commitment to building trust through our Data Responsibility Imperative which guides the ethical collection, management and use of personal data.

Finally, the standards and governance for data sharing and use need to be encapsulated in data governance and sharing regulatory frameworks which:

- are principle-based, flexible and which applies to all participants in the eco-system;
- are interoperable and proportional; and
- incorporate enablers such as cross-border flows of data, data quality and anonymization methodologies which can encourage the sharing and use of data.

Mapping a framework for global governance of data and data flows should therefore be cognizant that the effective operation of a key component of any economy; i.e., the payment system, is directly impacted by the legal and regulatory framework governing use, management, protection and movement of data in each country. It is therefore important that:

(1) Legal and governance frameworks—applying to both private and public sectors—should be principle-based, flexible, and ensure a level-playing field.
(2) Sustainable data sharing should be proportional and consider all interests.
(3) Legal and regulatory frameworks need to enable the flow of data across international boundaries.
(4) Anonymization is approached as a risk management tool which enables responsible use of data for public policy, while minimizing privacy risks.
(5) Greater convergence and interoperability of data protection and data sharing frameworks is achieved.
(6) Focus is on data quality not data quantity

End of Submission