Emerging Data Sharing Models to Promote Financial Service Innovation:

Global trends and their implications for emerging markets

Rafe Mazer[1] – June 2018

[1] Rafe Mazer is a consultant specializing in consumer protection and competition in financial services (Contact: rafe.mazer@gmail.com) This research was supported by The Bill & Melinda Gates Foundation. All opinions are solely those of the author.

Table of Contents

The author would like to thank the reviewers who offered invaluable feedback on this report both in the planning and drafting stages: Katharine Kemp, Himanshu Nagpal, John Ndunguru, Malavika Raghavan, Jeremy Shapiro and Adam Sorensen.

I. Executive summary

Data sharing models refer to a service, platform, or product that **collects and/or creates digital records for individuals** including financial history and alternative data (e.g. web history or phone records); and allows individuals to **determine when and how this data will be made available to multiple third parties** offering products and services.

i. Data sharing matters for financial inclusion

Whether directly led by consumers or primarily managed by firms, in order to support financial inclusion a data sharing model should have at its core an element of openness that enables greater sharing of information. Enabling of greater sharing of information is essential for data sharing models to realize four potential benefits for financial sector development:

1. Increased financial access
2. Financial service innovation
3. Increased competition
4. Improved pricing and product quality for consumers.

There currently exist many bilateral arrangements where a firm collects data on a customer—such as their credit history, mobile phone records or social media activity—and then shares or sells this data to a third-party. While technically this is a model where an individual's data is shared, its impact on enabling greater sharing of information is limited due to the inability of providers or consumers to share this data with multiple third parties beyond the bilateral arrangement.

This contrasts with the data sharing approaches reviewed in this report, which are generally more consumer-centric and in many cases engage multiple actors who provide and/or receive information. These models are rapidly increasing across the globe, both in developed and emerging markets. This report presents three pieces of research to help advance the discussion on data sharing models:

1. A set of considerations for developing data sharing models;
2. A scan of emerging data sharing models globally;
3. The potential of data sharing models in the markets of Kenya, Tanzania and Uganda.

ii. Considerations for determining which data sharing path to take

This report utilizes the global review of data sharing models to propose **ten considerations for developing data sharing models** that can be used when deciding the right path to promote data sharing in emerging markets (see table i).

Table i. 10 Considerations for Developing Data Sharing Models	
1. Level of public versus private-sector leadership	Would a government-led data sharing model be appropriate and feasible, or are fully private models a better approach?
2. Strength of existing policy mandate: Competition and coverage	Is there a strong competition or similar such mandate to impose data sharing requirements on providers? Is there wide regulatory coverage of financial service providers and technology firms to ensure a level playing field?

3. Data sharing: Mandated versus voluntary	Is data sharing voluntary or mandatory, and which sectors and information types does the mandate cover?
4. Data categorization: Level of openness	Is the data restricted to specific types or industries (e.g. official IDs, bank data) or open to wide-ranging traditional and alternative data?
5. Data privacy, protection and liability laws	Are there existing data privacy laws or regulations that cover topics such as consumers' rights to data security; consumer control over sharing of their data; rules on providers' data handling practices; and liability for data breaches?
6. Consumer control over data: Direct versus indirect	Are consumers given case-by-case control over the sharing of their data and revocability of such permissions; or are providers permitted to use general consent to share data with third parties at their discretion and with limited consumer visibility?
7. Data storage: Centralized versus dispersed	Is data stored in a centralized location or dispersed across various data collectors?
8. Minimum digital financial infrastructure	Do the preconditions for financial inclusion exist, including high digitization of financial services and interoperability?
9. Government infrastructure	Is the government at a minimum providing a reliable, electronic identity verification system? Beyond ID, are there government-controlled economic information sources (e.g. tax records, property records) that are made available to consumers?
10. Inclusiveness of approach for base of pyramid consumers	Does the model have an explicit objective to serve base of pyramid consumers and the financial services and providers they use? Is the model not easily accessed by base of pyramid due to technology interface (e.g. personal computer, smartphone app) or data types (e.g. bank records only)?

iii. The data sharing community is rapidly expanding across the globe

The report uses these ten considerations to assess and categorize a range of different public and private sector data sharing models emerging globally (see tables ii and iii).

Table ii. Public Sector Data Sharing Models Reviewed in this Report		
Model	**Summary**	**Indicative Examples**
Open banking	Government-mandated porting of consumers' banking information and accounts.	Australia, United Kingdom
Digital locker	Government-run set of APIs where citizens can upload, share and e-sign information such as ID and tax returns.	India
Open API standards	Requirements for banks to make available APIs to let third-parties integrate, including to receive information from consumers regarding their bank accounts.	Japan, Mexico
Table iii. Private Sector Data Sharing Models Reviewed in this Report		
Model	**Summary**	**Indicative Examples**
Consumer-centered, open networks	Connect multiple firms with consumer information through a private, voluntary set of rules and platform(s).	MyData, Open Banking Nigeria

Personal data management services	Support consumers to collect and manage their information from multiple sources.	Digi.me, Optimetriks
Interoperable payments platforms	Connect payment providers, creating a potential infrastructure for consumers to capture and share useful payments history.	Pagos Digitales Peruanos, Weilan (China)
Real economy data aggregators	Digitize economic activity and related transactional information in sectors such as agriculture, health, and retail.	AgriFin Accelerator, Arifu, BRCK, Maisha Meds, Sarafu, Syngenta
Private marketplaces	Facilitate the use of consumers' financial and other information to receive financial product offerings.	Chimoka, Destácame, Safaricom Credit Score
Credit reference bureaus and aggregators	Existing integrators of financial services, and collectors of consumer information which could be adapted for data sharing platforms.	Various East African aggregators and credit bureaus

To compare and contrast the various models' strengths and weaknesses the report uses a subjective "High-Medium-Low" ranking of each model against the "10 Considerations for Data Sharing Models" table. This is not meant to determine a single favorite—or set of favorites—models, but rather to explain the trade-offs that these models entail. For example, the Private Sector Marketplaces model uses traditional and alternative data to help generate new credit scores and provide leads for financial products and services for "thin-file" and other underserved consumers. This gives the model high ranking on it's inclusivity to base of pyramid consumers, and its ability to easily integrate diverse data categories. However, this private sector solution does not have mandatory data sharing rules that would help address competition barriers that may emerge if the ability of the consumer to leverage their credit score is restricted by the preferred partners of the firm that runs the marketplace.

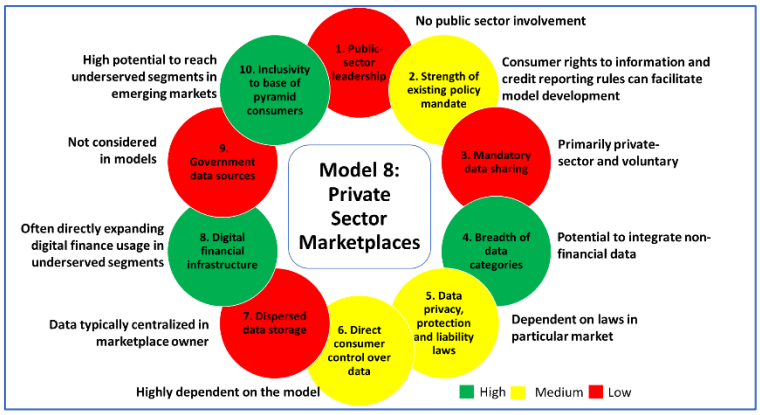


Figure 1: Ranking of attributes of private sector marketplaces for data sharing against "10 Considerations for Data Sharing Models."

This can be seen in practice with a pilot credit score developed by Kenyan Mobile Network Operator Safaricom, which is being tested with several FinTech lenders consulted for this report. The data in the scorecards includes mobile money, airtime, and digital credit history. However, the data is not disaggregated, and lender access to this data is at the discretion of the data holder, in this case the MNO. This means that consumers do not have as wide a choice of firms and products, and since the loan data includes loans originated by banks, it may also undermine the credit reference bureau system by offering a way for firms to access this data without participating in the credit bureau system, and by independently setting the cost of a credit scorecard at 100 Kenyan Shillings each. This example demonstrates how private sector data sharing models may need to be complemented with new rules, or enforcement of existing rules, to ensure that the principles of consumer control and openness are enabled to facilitate increased financial access, innovation and product diversity. This complementarity can be seen in MyData, another private sector model reviewed in this report, which has leveraged the new binding standards on issues such as data portability and consent of the European Union's General Data Protection Regulations (GDPR) and the Second Payment Service Directive (PSD2) in developing their private-sector solution.

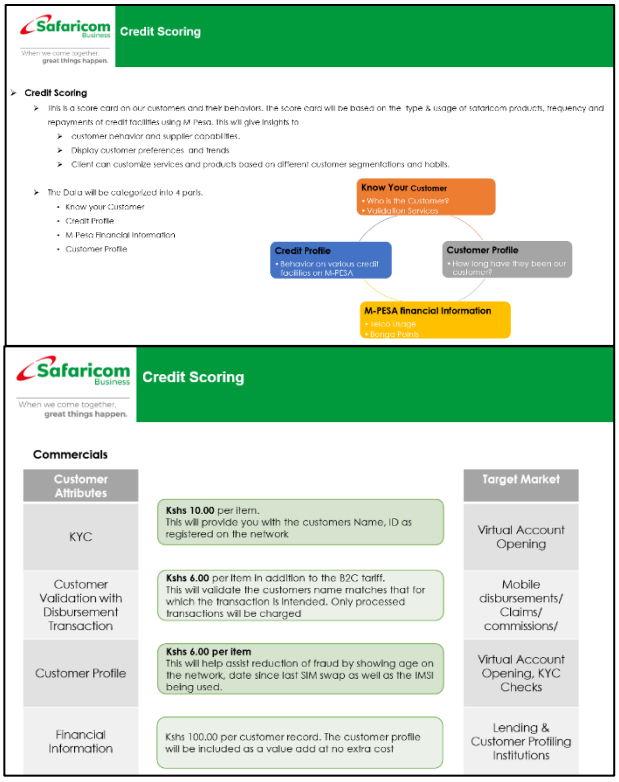


Figure 2: Safaricom credit scoring services

iv. Data privacy cannot be ignored

The analysis of data sharing models is complemented by a review of data privacy policies in the European Union, India and the Philippines that set important standards and obligations for data sharing models. Data privacy laws should be viewed as essential elements to any public-sector data sharing model, yet in many emerging markets data privacy laws are outdated or scattered across various sector laws instead of under a single, economy-wide privacy law. For this reason, it is worth emphasizing that, *given the significant risks data sharing may create for consumer harm and data breaches, any markets operating without data privacy laws may want to begin with data sharing models that only share limited sets of data—such as financial account statements and KYC verification—to reduce the consumer harm of data breaches while a data privacy law is yet to be issued*.

v. There is a path for data sharing in emerging markets—but basic enablers are missing

The report concludes by analyzing how ready Kenya, Tanzania and Uganda are for data-sharing models in financial services. In the policy space, the three markets each have important reforms that are needed

to support models similar to the public sector models reviewed in this report. However, the market-readiness varies considerably across the three markets.

Kenya appears on the verge of being able to implement a government-led data sharing model due to several factors: Robust online ID system; deep penetration of digital financial services and payment interoperability; competition laws to complement financial sector laws; and recently announced data privacy and financial market conduct bills being considered. To achieve this objective, Kenya will still need to identify the proper authorities to implement such a model, the mandate to require financial information porting, and determine the porting standards and information types to require the financial sector to provide consumers access to.

Uganda has seen significant progress on the implementation of an electronic national ID system in the past year, in large part due to the requirement made in 2017 that all SIMs be registered with the national ID or be shut off. There is also an advanced-stage Data Protection and Privacy Bill and the recent expansion of market coverage through the Uganda Microfinance Regulatory Authority. However, Uganda lacks a competition authority or similar such mandate, and while digital financial services have expanded considerably, mobile money account ownership is still only 43%.[2] This means that Uganda may need to take a more incremental approach to any public-sector data sharing models than Kenya, although could still consider such an approach in the longer term.

Tanzania faces the most significant challenges to public-sector data sharing models of the three markets. This is due to the challenges in rolling out the national ID, lack of wide regulatory coverage of financial service providers, and a more limited competition mandate of the Fair Competition Commission in banking and telecommunications than is enjoyed by the Competition Authority of Kenya. Yet Tanzania also has high digital financial services penetration with robust interoperability, and an exciting cohort of private sector actors that are digitizing key parts of the economy such as agriculture, wholesale and retail commerce, and government services. This means that the playbook in Tanzania may be to develop private sector cohorts which could begin by sharing identity data to help reduce fraud and overcome the gaps in the national ID system, and layer on top of this some form of sharing of financial and other information if the consumer requests this.

[2] http://finclusion.org/country/africa/uganda.html#dataAtAGlance

II. Introduction

In countries as diverse as the United Kingdom, India, and Mexico, there is momentum to increase consumers' ability to access, manage, and control their digital identity and history. Whether this is government records, bank account data, or web browser activity, providing consumers with the ability to access and share their digital identity and records could increase competition and innovation by letting financial service providers better target and price products to consumers. Similarly, when consumers can freely bring their data to an open market, this could increase choice and push more competitive pricing and product terms.

To carry out these mandates for greater consumer access and control over their digital identity, a range of public and private sector data sharing models are being developed. These models offer insights into the rules needed to enable greater data sharing; how to balance data privacy with data portability; data sharing platform architecture; and data classifications and definitions. For the purposes of this research, we define a data sharing model as follows:

> *Data sharing models refer to a service, platform, or product that* ***collects and/or creates digital records for individuals*** *including financial history and alternative data (e.g. web history or phone records); and allows individuals* ***to determine when and how this data will be made available to multiple third parties*** *offering products and services.*

Whether directly led by consumers or primarily managed by firms, a data sharing model should have at its core elements of consumer rights to their data and openness to different providers that enables greater sharing of information at the consumer's discretion. Enabling of greater sharing of information is essential for data sharing models to realize four potential benefits for financial sector development:

1. Increased financial access
2. Financial service innovation
3. Increased competition
4. Improved pricing and product quality for consumers.

There currently exist many bilateral arrangements where a firm collects data on a customer—such as their credit history, mobile phone records or social media activity—and then shares or sells this data to a third-party. While technically this is a model where an individual's data is shared, its impact on enabling greater sharing of information is limited due to the inability of providers or consumers to share this data with multiple third parties beyond the bilateral arrangement. This contrasts with a range of new data sharing models that to differing degrees are offering increased choice, control and openness. (See Tables 1 and 2)

Table 1. Public Sector Data Sharing Models Reviewed in this Report

Model	Summary	Indicative Examples
Open banking	Government-mandated porting of consumers' banking information and accounts.	Australia, United Kingdom
Digital locker	Government-run set of APIs where citizens can upload, share and e-sign information such as ID and tax returns.	India
Open API standards	Requirements for banks to make available APIs to let third-parties integrate, including to receive information from consumers regarding their bank accounts.	Japan, Mexico

Table 2. Private Sector Data Sharing Models Reviewed in this Report		
Model	**Summary**	**Indicative Examples**
Consumer-centered, open networks	Connect multiple firms with consumer information through a private, voluntary set of rules and platform(s).	MyData, Open Banking Nigeria
Personal data management services	Support consumers to collect and manage their information from multiple sources.	Digi.me, Optimetriks
Interoperable Payments Platforms	Connect payment providers, creating a potential infrastructure for consumers to capture and share useful payments history.	Pagos Digitales Peruanos, Weilan (China)
Real Economy Data Aggregators	Digitize economic activity and related transactional information in sectors such as agriculture, health, and retail.	AgriFin Accelerator, Arifu, BRCK, Maisha Meds, Sarafu, Syngenta
Private Marketplaces	Facilitate the use of consumers' financial and other information to receive financial product offerings.	Chimoka, Destácame, Safaricom Credit Score
Credit Reference Bureaus and Aggregators	Existing integrators of financial services, and collectors of consumer information which could be adapted for data sharing platforms.	Various East African aggregators and credit bureaus

Ideally, data sharing models should shift the balance of power over financial and alternative data back into the hands of the consumer, and lead to increased choice and competition. This report considers how data sharing models are achieving these goals of choice and competition through the increased digitization and consumer-led sharing of the following types of data:

1. **Public data.** Data collected or produced by the government, such as identity documents, tax returns, or education records.
2. **Demographic data.** Data that either provides or confirms personal characteristics such as age, gender, or location.
3. **Economic data**. Data on individual or business financial transactions, cash or inventory flow, assets and similar such data.
4. **Alternative data**. Data that captures an individual's activities, preferences, and behaviors via data sources that are neither an official piece of public nor economic data. This data may be less structured or not as easily placed into standardized categories as data types 1-3.

This report presents three pieces of research to help advance the discussion on data sharing models:

1. A set of considerations for developing data sharing models;
2. A scan of emerging data sharing models globally;
3. An initial analysis of the potential of data sharing models in the East African markets of Kenya, Tanzania and Uganda.

The report begins by articulating the benefits of shareable digital identity for financial inclusion, competition and consumer welfare. Next ten considerations are presented for understanding the types of data sharing models emerging, as well as the policy and design choices they provoke (see Table 3). The report then reviews examples of emerging public and private-sector data sharing models and the features of each that could be useful for other providers or governments looking to enable data-sharing models. Finally, the report reviews the potential of data sharing models in three leading digital financial services markets in East Africa: Kenya, Tanzania and Uganda.

Table 3. 10 Considerations for Developing Data Sharing Models	
1. Level of public versus private-sector leadership	Would a government-led data sharing model be appropriate and feasible, or are fully private models a better approach?
2. Strength of existing policy mandate: Competition and coverage	Is there a strong competition or similar such mandate to impose data sharing requirements on providers? Is there wide regulatory coverage of financial service providers and technology firms to ensure a level playing field?
3. Data sharing: Mandated versus voluntary	Is data sharing voluntary or mandatory, and which sectors and information types does the mandate cover?
4. Data categorization: Level of openness	Is the data restricted to specific types or industries (e.g. official IDs, bank data) or open to wide-ranging traditional and alternative data?
5. Data privacy, protection and liability laws	Are there existing data privacy laws or regulations that cover topics such as consumers' rights to data security; consumer control over sharing of their data; rules on providers' data handling practices; and liability for data breaches?
6. Consumer control over data: Direct versus indirect	Are consumers given case-by-case control over the sharing of their data and revocability of such permissions; or are providers permitted to use general consent to share data with third parties at their discretion and with limited consumer visibility?
7. Data storage: Centralized versus dispersed	Is data stored in a centralized location or dispersed across various data collectors?
8. Minimum digital financial infrastructure	Do the preconditions for financial inclusion exist, including high digitization of financial services and interoperability?
9. Government infrastructure	Is the government at a minimum providing a reliable, electronic identity verification system? Beyond ID, are there government-controlled economic information sources (e.g. tax records, property records) that are made available to consumers?
10. Inclusiveness of approach for base of pyramid consumers	Does the model have an explicit objective to serve base of pyramid consumers and the financial services and providers they use? Is the model not easily accessed by base of pyramid due to technology interface (e.g. personal computer, smartphone app) or data types (e.g. bank records only)?

To compare and contrast the various models' strengths and weaknesses the report uses a subjective "High-Medium-Low" ranking of each model against the "10 Considerations for Data Sharing Models" table. This is not meant to determine a single favorite—or set of favorites—models, but rather to explain the trade-offs that these models entail. In each discussion of the models, the section commences with a graphic assessing the model against the 10 considerations. (See Figure 3)

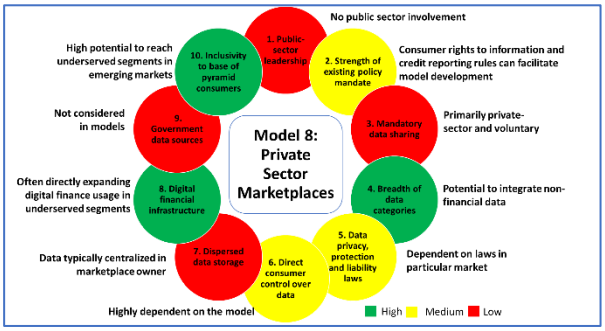


Figure 3: Ranking of attributes of private sector marketplaces for data sharing against "10 Considerations for Data Sharing Models."

III. Why is data sharing important for financial inclusion?

The increasing use of mobile phones, apps, and electronic financial services such as payments networks, online banking and financial apps has increased the amount of financial and economic information that is being generated by low-income households. This data is already being leveraged to better assess needs and provide new financial and non-financial services to underserved populations. Consider, for example, the way in which insurance providers are leveraging new data sources to improve underwriting and enrollment processes.[3] In developed economies this includes the use of sensors and social media data for underwriting or monitoring of consumer behavior to offer individualized premium pricing. In emerging markets innovations in insurance products include using the digitization of input purchases by farmers to offer bundled insurance products with automatic payout triggers, or the use of satellite and geo-location data to provide more customized policies and payouts for individual farmers.

Irrespective of the market or the data type, the wide range of use cases being developed that leverage digital data trails for financial services make clear the importance of this data for the future of financial services. Yet in emerging markets like the three East African markets considered in this report, there is often a limitation to the use of this data since the data is concentrated in "data silos." In these data silos the firm that generates or collects the data on the consumer defines the terms of use of the data up front in a way that limits the consumer's right to access this data or share it, while giving wide-ranging and often ill-defined rights to the firm to share and sell consumers' account data to third party service providers.[4] (See Figure 4)

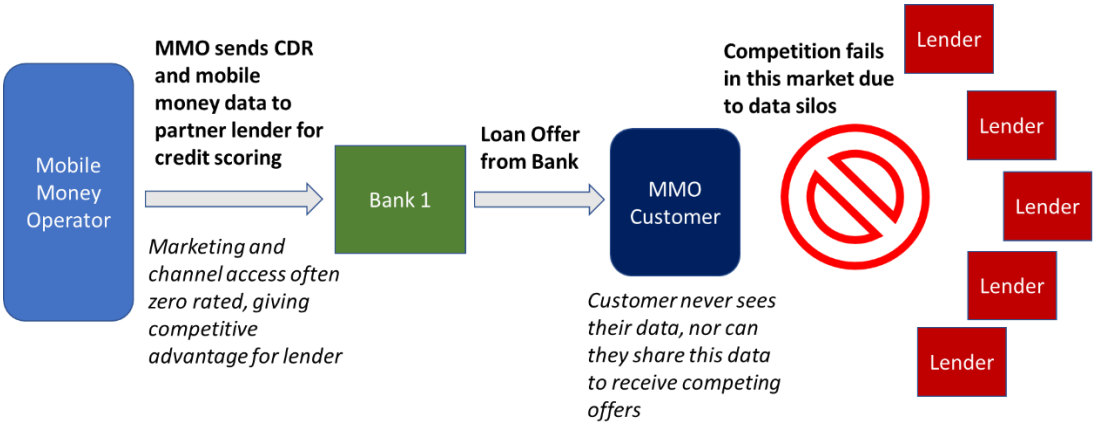


Figure 4: Closed loop digital credit model

Data silos limit the potential of data trails to further transform financial inclusion. To realize the full potential of new data sources in financial inclusion will require providers, policymakers and market

[3] https://www.ft.com/content/bb9f1ce8-f84b-11e6-bd4e-68d53499ed71; http://blog.mondato.com/inclusive-insurance-bought-not-sold/?utm_source=Mondato+Newsletter&utm_campaign=d4c3115a70-Inclusive+Insurance&utm_medium=email&utm_term=0_b4cb05c7b7-d4c3115a70-407541781

[4] Sarah Ombija, "Review of DFS User Agreements in Africa: A Consumer Protection Perspective New", International Telecommunications Union, January 2017. http://www.itu.int/en/ITUT/focusgroups/dfs/Documents/01_2017/ITU_FGDFS_Report-on-Review-of-DFS-User-Agreements-in-Africa.pdf

facilitators to break down these silos and enable consumer-led, cross-provider data sharing. The potential benefits of consumer-led, open data-sharing models for financial inclusion are several:

1. *Increased financial access.* With more and more easily accessible data on consumers and businesses, financial service providers will be better able to identify and qualify these consumers and businesses for financial services. This may be particularly true for underserved segments such as lower-income households, microenterprises, and rural populations.
2. *Financial service innovation*. Increased diversity of data can help financial service providers to better segment consumers and offer greater customization to existing products or new products.
3. *Increased competition.* As financial and other electronic transactions increasingly concentrate on channels of large mobile network operators (MNOs) and internet platforms such as Google and Facebook, these firms' power to determine which financial service providers can and cannot leverage consumer data and delivery channels increases.[5] With data access and porting rights for consumers in an open marketplace, competition will likely increase as more firms can access consumers' data to make risk assessments and recommend financial products and services.
4. *Improved pricing and product quality for consumers*. With increased access, product innovation and competition, financial consumers should start to receive more competing product offers that are better adapted to their needs, and more competitive pricing for these products.

[5] http://wiredspace.wits.ac.za/bitstream/handle/10539/21629/AJIC-Issue-17-2016-Mazer-Rowan.pdf?sequence=3&isAllowed=y

IV. Key considerations for developing data-sharing models

While open, consumer-led data sharing in financial services is a relatively new development, there are emerging models that offer insights on key features and design elements public and private actors should consider in developing data sharing models. The global review of data-sharing models has identified ten key considerations for their development, which are summarized below.

1. Level of public versus private-sector leadership. Several of the most ambitious data sharing models to emerge, such as Open Banking or the India Stack, are led by public actors. There may be first-mover challenges where each individual actor bears greater risks than benefits in sharing their information if their rivals are not compelled to do so as well. Therefore, a public set of standards applied equally within firm or data types may be needed. The primary benefits of public sector leadership are the ability to set mandatory standards for data sharing, compel participation by firms, and provide standards on access to and handling of data across provider types. This helps set a level playing field for all data of a particular type and allows all consumers of that type—irrespective of the provider they use—to leverage said data.

However, policy can be a slow-moving process, and may not always include the most leading-edge types of data being captured and leveraged for financial services. For example, there is a range of interesting experiments occurring with use of sensor technology to capture difficult data points in emerging markets such as address, business inventory, or farm location and plantings. This type of data may be relatively unproven and difficult to capture, as well as hard to define legally, but carries significant potential if pilot projects prove successful, which may require a lighter treatment for data sharing purposes. Or the data may not be widely useful to most citizens in a market, but highly useful to a subset of users. In these cases, letting private sector actors lead without mandatory data-sharing for those data types could be an appropriate path to take.

2. Strength of existing policy mandates in competition and market coverage. Data sharing models can impact a wide range of financial and non-financial jurisdictions, so the mandate to issue laws or rules regarding data sharing models may not sit with one ministry or sector regulator. This has been addressed in a variety of ways: Issuing rules for data sharing via competition mandates that are cross-economy; Issuing new legislation (e.g. FinTech laws, data privacy laws, and payments directives) that include mandatory data sharing and connectivity for at least some segments of financial services; or development of new government agencies that both administer and manage data sharing platforms. In emerging markets two of the most important policy mandate considerations with respect to data sharing models are 1. The existence of a competition authority or competition mandate to impose data sharing; 2. Comprehensive regulatory coverage of financial service provider types and products.

3. Mandated versus voluntary data sharing. For the public-led data sharing models reviewed, this may be the most important differentiation in model design. In India, where banks are not required to let consumers port their financial history to other firms, there was a new regulation issued in 2016 to allow licensing of data aggregators who could help to facilitate data sharing by consumers and financial service providers. However, according to interviews with experts familiar with the licensing window, there was little interest from the private sector in this new licensing window. By contrast, the mandatory porting of bank account data within the UK Open Banking regime only took effect in January 2018, but already several new licenses have been issued for Account Information Service Providers to

help consumers leverage this data. While mandatory sharing of financial data is not the only reason for the different depth of data aggregators in the two markets, mandatory access to a minimum level of financial data by consumers likely helped firms decide to invest in these new licenses in the United Kingdom.

4. Open or restricted data categorization. Clear categories of data can support consistency in data submissions and help consumers actively sort and manage access rights to their data. For models focused on financial inclusion, there should at a minimum be clear definitions for financial data—what it is and how granular the data is, e.g. account summaries or transaction level data. However, some alternative data types—such as satellite data or social media usage—may be difficult to define or easily order in categories across data collectors. Data sharing models may need to allow for flexibility to adapt to the emergence of new data sources, with more rigid data categories for traditional data sources.

5. Data privacy, protection and liability laws. Data privacy rules can complement and even enable data sharing models. They are also important to help mitigate the risks that are inevitable with any increase in data sharing. In emerging markets this risk may be compounded by more basic interfaces such as mobile handsets, lower literacy levels, and limited supervision. This could risk consumers suffering information asymmetries where even if they are managing their data in name, their ability in practice to view and manage access rights for this data falls short of either the rules or objectives of a data sharing model. Where data privacy rules are not in place, consumer protection is limited, and supervisory capacity is weak, launching data sharing models could invite significant risks to consumers, firms and the government.

Wherever possible data privacy laws should be updated to reflect principles such as: Consumers' ability to access and manage their data; consumer rights to authorize and revoke sharing of data a case-by-case basis; and clear liability of data collectors and data management services for data breaches. *Given the significant risks this creates for consumer harm and data breaches, any markets operating without data privacy laws may want to begin with data sharing models that only share limited sets of data—such as financial account statements and KYC verification—to reduce the consumer harm of data breaches while a data privacy law is yet to be issued*.

6. Direct versus indirect consumer control over their information. In many consumer/service provider arrangements, consumers consent to a wide range of usage and sharing of their account data by the provider, with limited ability to control the terms of such data sharing by their service provider with third parties. This indirect control via one-time consent does not support the objectives of consumer protection, competition and control over their information. This contrasts with new data privacy laws such as the European Union General Data Protection Regulation which provide consumers with greater rights to manage how their data is shared by their service provider with third parties. Emerging data sharing models should incorporate strong consumer consent and control over how their data is shared. This includes letting consumers determine on a case by case basis whom they will share data with, dividing such rights to use across different data sets the consumer controls, specifying restricted permissible uses for that data, and even time limits on access to this data.

7. Centralized versus dispersed data storage. The simplest way to help consumers access—and manage others' access to—their data would be a centralized repository. However, centralized data storage raises the "honey pot" risk that if the centralized repository is breached the entirety of a consumer's data is

compromised, as was the case with the Equifax credit bureau breach in the United States.[6] To avoid the "honey pot" risk some data-sharing models use a series of bilateral connections between data holders and their designated data users, only centralizing the consumer's consent management process and their controls on firms' access privileges to consumer information.

8. Minimum digital financial infrastructure. Where financial services have been heavily digitized, there will be a larger body of available financial data and related web and mobile data that can be integrated into data sharing platforms immediately. Similarly, where there are firms offering services such as payments integration across financial service providers, or interoperable platforms and switches, these solutions may be adapted to support storing and sharing of digital data for consumers and businesses. Yet even where there are existing firms offering these services, there will still be a need for new licensing categories. The Account Information Service Provider (AISP) licenses in the European Union and United Kingdom is a leading example of a new license class that is important for data sharing models.[7]

9. Existence of government infrastructure for identification and other personal information. The presence of a robust online identity verification system allows data sources shared by consumers to be linked to a single individual with relative certainty. In addition, as governments make more documents and services available to consumers online, such as tax returns, these sources of information become useful complements to data generated by private sector actors. These data sources also have the advantage of not being controlled by any firm that could try and restrict its usage, so may offer a first set of information types if providers are unwilling to initially participate in a data-sharing model. The India Stack has begun with these sources of data, with the hope that financial and other private-sector data will be included in the future.

10. Inclusiveness of approach for base of pyramid consumers. Data sharing models can explicitly target underserved, base of the pyramid consumers. In some private sector data sharing models in East Africa, there is an explicit focus on segments like smallholder farmers, savings groups, or social welfare beneficiaries that are disproportionately comprised of lower-income consumers. By contrast, choices on data types and interfaces can reduce the applicability of a model for base of the pyramid consumers. Some developed economy data sharing models focus on product classes—e.g. banks only—that are not as relevant to base of pyramid consumers; or rely on computer-based interfaces that might not be as useful or accessible for consumers who may only possess a feature phone.

[6] https://www.ftc.gov/equifax-data-breach
[7] https://www.fca.org.uk/account-information-service-ais-payment-initiation-service-pis

How blockchain and distributed ledger are relevant to data-sharing models

Blockchain and distributed ledger technologies are providing new models for decentralized sharing, storing and processing of information. These solutions may play an important role in data-sharing models such as those discussed in this report. Some of the more promising features of blockchain and distributed ledgers for data-sharing models include:

- Open and verifiable ledger. Blockchain keeps the entirety of information kept by multiple parties in its ledger, with the ability of all parties to check and verify the integrity of the ledger.
- Immutable. Since every operator of the ledger accesses the whole database of all transactions since its inception.
- Flexible. The open nature of these systems makes them adaptable to a wide range of both information types and entities providing information.
- Highly relevant for identity creation and verification. The Sovrin Foundation has proposed the use of distributed ledger technology in their global identity system. Further, they argue that such a solution will dramatically transform four relevant industries: Identity and access management, cybersecurity, RegTech, and data integration.[1]

At the same time, there are also some limitations and concerns related to blockchain and distributed ledger technologies for data sharing models for financial services in emerging markets:

- There have been a number of serious security breaches for distributed ledgers, including the losses of billions of dollars in value in multiple crypto-currency exchanges.[1]
- In financial services there may often be a need for a centralized point of control in a data-sharing model, especially if the model is advanced by a regulator or includes official ID or banking data. In these cases having a distributed ledger system that at some point centralizes may lose some of the benefits of openness and universal verification in distributed ledger systems, and so a single centralized system will be more efficient.
- Related to the above, one financial sector regulator interviewed piloted a distributed ledger technology for purposes of data management and verification, but discontinued its usage due to security concerns.
- Running distributed ledgers on mobile phones may be technically difficult. According to an expert interviewed, “running a DLT [distributed ledger technology] on a mobile phone will kill the data allocation of the person using it. You will also still need a central serve all mobile devices communicate with and [which] runs the DLT.”

At least one of the interviewees in this report is utilizing a blockchain for information sharing in financial services, which means that there are certainly relevant use cases for these technologies in data sharing models for financial services in emerging markets. This includes management of cross-border transactions; development of alternative identification where a reliable single ID exists; and for integrating multiple partners who wish to share information but do not necessarily have the same types of information or methods for storing this information digitally. This means that these technologies will likely be of greater benefit for private than public-sector models in the near future.

V. Public sector-led data-sharing models

Some of the more compelling arguments for data-sharing models are the increased choice, switching, product diversity and personalization of financial services they may facilitate. These benefits should transfer to the private sector as well through reduced risk and room for new firms and products to emerge. However, benefits may not always be immediate nor evenly distributed amongst existing providers and new entrants, particularly in markets where there may be dominant actors or even monopoly-level market concentration. In some markets we may expect private sector actors to resist consumer-led data sharing models, limiting the potential for private-sector led approaches to achieve equal provision of, and access to, data generated by consumers' various service providers.

In these cases, public sector leadership in data sharing may be appealing where the local policy mandate and political economy permit. Public sector leadership can take a range of forms and levels of effort. The three public-sector models described in this section—open banking, digital lockers, and open API requirements—demonstrate the range of approaches policymakers can choose.

For example, the three models have different levels of government activity in building the data-sharing architecture. India's digital lockers have been developed by the government and managed by a new government agency. Similarly, the United Kingdom's open banking has included a special purpose vehicle chaired by the Competition and Markets Authority to develop a single set of APIs for banks, while in Mexico the new FinTech Law only requires that providers make their APIs available to third parties, but does not put government in a role to build out any data-sharing platform. The three models also differ in the level of mandating of data sharing. Both the UK and Mexico require banks to let customers access and port their financial information if desired, while India does not have any such requirements. A final important contrast is that India's digital locker system takes a more consumer-centric and consumer-driven approach, by setting up lockers for each citizen, versus the UK and Mexico models, which center on platforms and information-sharing arrangements that are housed within banks and other financial service providers.

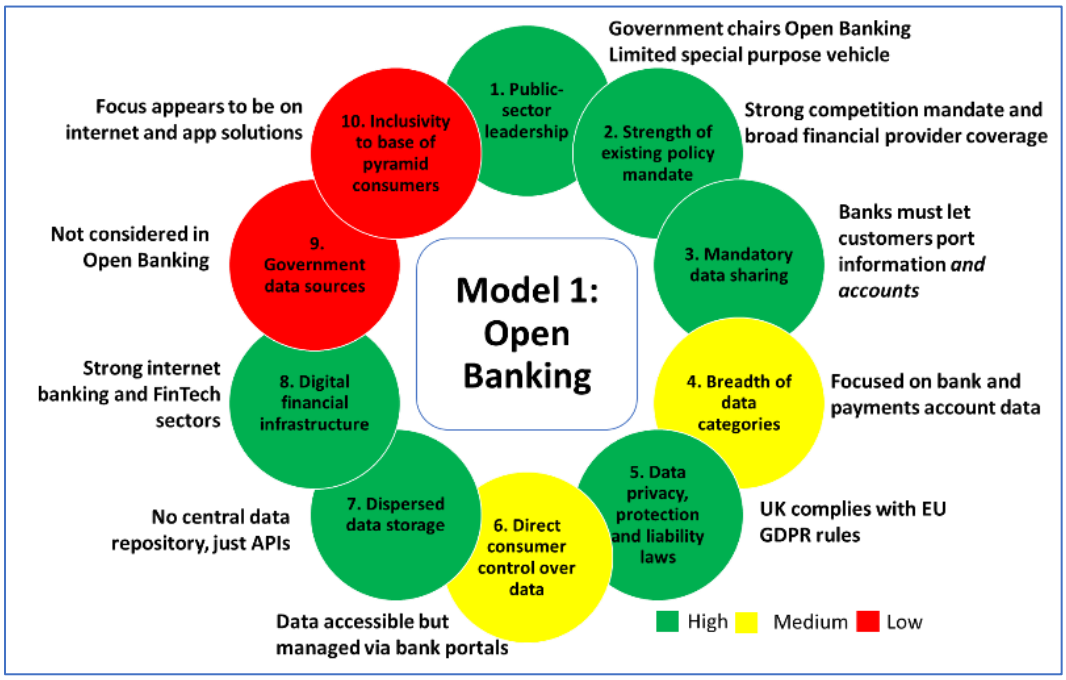
1. Open banking

Three key features of Open Banking:

- Rooted in competition mandate, addressing market concentration and switching issues in the banking sector, and as such involves wide range of financial and non-financial sector authorities.
- Requires mandatory porting of financial information—and accounts in the United Kingdom—for bank customers.
- Establishes new licensing classes for firms that can receive and manage financial information on consumers' behalf.

Open Banking seeks to make it easier for bank customers to both leverage their banking data across various financial service provide and to move accounts. Open banking policies have been developed as a response to perceived barriers to consumer switching in banking, lack of effective price competition, and barriers to entry for smaller banks and non-banks. Open banking addresses these competition challenges by focusing on the ability of consumers to leverage their financial history more effectively

and easily with a broader range of financial service providers. One of the primary aspects of Open Banking architecture is mandatory data porting and interconnectivity of banks and other financial service providers. Two leading examples of this approach are the United Kingdom and Australia, which are briefly summarized below.



United Kingdom Open Banking

The United Kingdom's Open Banking began with an inquiry by the Competition and Markets Authority (CMA) that identified barriers to competition in current accounts and SME finance—which they attributed in part to data silos tying borrowers to one lender.[8] The inquiry's report included three rules applied to the largest nine banks in the United Kingdom that promote connectivity and data sharing:

1. Mandatory porting of consumer data if they request. For example, if a customer of Bank A wishes to share their account data with Bank B for a loan, Bank A must honor that request.
2. Mandatory switching of accounts for consumers if they request. For example, if the customer takes a loan with Bank B, and finds their services preferable, they can request an automatic account transfer from Bank A to Bank B, and even have all their standing orders (e.g. direct deposits and automatic payments) re-routed.[9]
3. A set of Applied Program Interfaces being developed by Open Banking Limited, a Special Purpose Vehicle composed of the industry and chaired by an CMA appointee, to make sure these features are standardized for all providers and their customers. The Open APIs "will

[8] Competition and Markets Authority. "Making Banks Work Harder for You."
[9] Interestingly, Open Banking does not require account number porting, as the CMA argued that "Open APIs will themselves fundamentally change customers' experience of banking and reduce the role of bank account numbers."

permit authorized intermediaries to access information about bank services, prices and service quality and customer usage,"[10] and allow consumers to manage accounts through a single application. Open Banking Limited acts as a venue for banks to work together to implement standards for the APIs, and is funded by the banks. However, when banks cannot agree on the approach for a particular API, there is a CMA appointed chair of the SPV that intervenes and exercises veto powers to avoid the implementation process getting stalled.

According to a CMA official involved in the Open Banking project, they expect that the mandatory APIs will particularly benefit smaller FinTechs, and that the standard APIs will make data access technology more accepted by the customers, as there is can be as high as an 80% drop-off of users at the data access consent page on some data scraping apps, which is where a scraper asks for your password and username. With open APIs consumers may not be as reluctant to share their data to avail of new financial services if they are not required to share sensitive account credentials to do so.

To help consumers manage data and seek competing services, Open Banking includes a new license type for Account Information Service Provider[11] (AISP), which can receive consumers financial data and store and manage it for the consumer. These AISP licenses are administered through the Financial Conduct Authority[12], with all AISP or PISP firms that began operations after January 12, 2016 required to be registered or authorized by the FCA before January 13, 2018. The AISP licensing structure is based on the Payment Service Directive 2 (PSD2) from the European Union, and the Financial Conduct Authority has encouraged the three new PSD2 license types—Account Servicing Payment Service Providers [ASPSP], Account Information Service Providers [AISP], and Payment Initiation Service Providers [PISP]—to "work towards using the Open Banking API Standards as the basis on which secure API access to other payments accounts is provided in the future."[13]

Open Banking has benefited from the UK's adherence to the PSD2 rules, which meant that while payments were not included in the CMA's inquiry, they can easily be integrated into the Open Banking model and its data porting requirements. Similarly, the EU's General Data Protection Regulations have provided an essential set of data protection standards that will apply to Open Banking. Open Banking has also benefited from the CMA's powerful competition mandate which permitted them to require data and account porting as a remedy to lack of competition in the banking sector. Many emerging markets do not have as strong of a competition mandate or even a specific competition authority, which could limit their ability to impose such requirements and adopt a full Open Banking approach.

Australia Open Banking Inquiry

The Australian Government has embarked on a similar initiative to the United Kingdom, which they have also termed Open Banking. This initiative builds on the 2014 Financial System Inquiry and the 2015 Competition Policy Review, the latter of which recommended consumers have access to their own data

[10] Competition and Markets Authority. "Making Banks Work Harder for You."
[11] This license type is being developed as part of the United Kingdom's implementation of the European Union's Payment Services Directive 2.
[12] Open Banking is a cross-market effort that includes the Financial Conduct Authority, Treasury, the Department for Business, Energy and Industrial Strategies, Bankers automated clearing system, CASS Business School, and nesta.org.
[13] "FCA Expectations for Third Party Access Provisions in PSD2." Financial Conduct Authority. 2017.

across the economy, and the ability to direct their data to other consumers or nominated third parties in a machine-readable format.[14]

Per the Australian Government's Open Banking Issues Paper, "Open Banking is an example of the increasing trend by governments around the world to find ways to allow greater choice for customers, in this case by giving them easier access to, and more control over, data relating to their finances and transactions held by their banks."[15] The central pillar to the Open Banking reforms is the Productivity Commission's January, 2018 report "Competition in the Australian Financial System."[16] The inquiry has several findings and recommendations relevant to data-sharing models:

- *Consumer Access to and Control of Data.* "The Open Banking system proposed for Australia should be implemented in a manner that enables the full suite of rights for consumers to access and use digital data."[17]
- *Increased Non-Bank Access to Data.* Facilitation of third-party access to the New Payments Platform, including transaction-level data and a requirement that industry will "consult the Australian Competition and Consumer Commission on the final design of the data sharing obligations."[18]
- *Increased Policy Emphasis on Competition in Financial Services.* An increased competition mandate for all the regulatory bodies that are members of the Council of Financial Regulators "to address gaps in the regulatory architecture related to lack of effective consideration of competitive outcomes in financial markets."[19]

During the public comment period of the Open Banking Issues Paper that was the precursor to the "Competition in the Australian Financial System" report, Australian banks raised several issues that will likely impact the manner of implementation of the findings from the report[20]:

- **The need for a new privacy law that will support Open Banking**. This would include an "accreditation utility" that issues standards, authorizes and monitors compliance for data handlers; a de-centralized model for data access where consent originates on a banking app to reduce the "honey pot" risk; and consumer ability to control the level of detail and types of products or activities shared individually.
- **Liability rules**. This includes making data receivers responsible for data security after the data leaves the bank's platform and removing banks' liability for any subsequent consumer losses; and a non-judicial channel for consumers to easily bring cases of misuse of data against the data receivers.
- **Definition of data types**, including clarity that the data will only be a subset of data collected on the customer and not proprietary data.
- **Standardized data usage fees** to provide consistency and avoid excessive charging by data providers.

[14] http://competitionpolicyreview.gov.au/final-report/
[15] "Review into Open Banking Issues Paper." Australian Government. August, 2017.
[16] https://www.pc.gov.au/inquiries/current/financial-system/draft/financial-system-draft.pdf
[17] https://www.pc.gov.au/inquiries/current/financial-system/draft/financial-system-draft.pdf
[18] https://www.pc.gov.au/inquiries/current/financial-system/draft/financial-system-draft.pdf
[19] https://www.pc.gov.au/inquiries/current/financial-system/draft/financial-system-draft.pdf
[20] http://www.zdnet.com/article/australian-banks-and-fintechs-weigh-in-on-open-banking-regime/

Similar to the United Kingdom, implementation of Open Banking in Australia will be a cross-regulator initiative. According to interviews with local experts, Open Banking will likely become an amendment to the Competition and Consumer Act, with the Australian Competition and Consumer Commission administering accreditation for participants in Open Banking. However, other regulatory agencies such as the Australian Information Commission, Australian Prudential Regulatory Authority, and the Australian Securities and Investments Commission will oversee different aspects of Open Banking, while a data standards body will function in a manner similar to the Open Banking Limited SPV in the United Kingdom.

Emerging Lessons from Open Banking

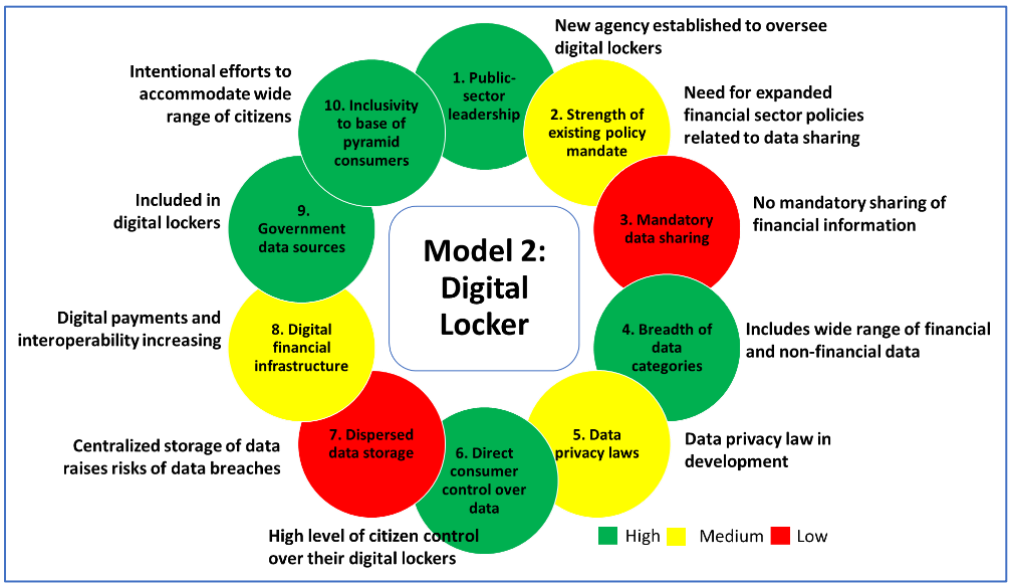
Open Banking offers an appealing—if ambitious—path for public-sector data sharing initiatives. The experiences of the United Kingdom and Australia raise several considerations for setting specific rules on data sharing and provider connectivity:

- **The need for strong policy mandates**. Both Australia and the United Kingdom have strong financial sector oversight, as well as robust competition mandates. This has facilitated using competition mandates to require data sharing, while leveraging the capacity of the financial sector authorities to support the implementation and supervision of open banking across the financial sector. In many emerging markets the competition mandate and financial sector oversight may need to be expanded first to develop an open banking approach.
- **Preparedness to develop complementary policy measures**. In the United Kingdom this includes the new rules set forth by PSD2, while in Australia it includes the need for new rules on data privacy to assure safe and responsible data sharing. Emerging markets exploring open banking should also set complementary policy development agendas—especially on data privacy.
- **Development of technology and infrastructure.** The United Kingdom has deployed a public-private Special Purpose Vehicle to develop the technological standards and Open APIs necessary for open banking. In emerging markets where this may be too resource-intensive a role for government, they could consider self-regulatory organizations or delegated supervision models that allow industry to lead technical development of Open Banking while the government maintains a direct advisory and oversight role.
- **Financing of costs.** The cost of developing and managing an open banking system need to be financed, which could be a challenge for budget-constrained government agencies in some emerging markets. This may require the use of a taxation on the industry, or perhaps permitting membership or data usage fees to be assessed on participants in the open banking scheme.

2. India Stack's DigiLocker

Three key features of DigiLocker:

- Wide range of information included, including government records, making potential use cases much broader than financial services.
- Consumer-centric design, where individuals manage their lockers and functions such as e-signatures.
- Lacks mandatory financial information porting, which may be limiting financial sector use cases to date.



While the India Stack does not have the direct data-sharing mandate of the UK and Australia Open Banking regimes—though this is under consideration for banking data—it is the most ambitious and robust public data-sharing model in an emerging market to date. The India Stack is a series of APIs that allow Indian citizens to store, e-sign and share a range of public and private records for different needs and opportunities. These APIs include the Aadhaar biometric ID system, eSign, the Unified Payments Interface—a fully interoperable payments platform—and the Digilocker. The India Stack also benefits from the government's Jan-Dhan initiative, which has opened more than 250 million new basic savings accounts. The underlying ID, accounts and payments infrastructure demonstrates the importance of building this public infrastructure for emerging markets exploring data sharing models.

Of particular relevance to this research is the Data Empowerment and Protection Architecture, which is the consent and data sharing layer of the India Stack.[21] This Architecture is managed by the Ministry of Electronics and Information Technology (MeitY), which has issued standards for Electronic Data Consent[22] and the Digital Locker System,[23] while the Unique Identification Authority of India (UIDAI) manages Aadhar and the e-KYC process that is a key enabler of data sharing, including requests from Authentication User Agencies (AUAs) and e-KYC User Agencies (KUAs) who wish to authenticate an

[21] Tanuj Bhojwani. "The Best Way Forward for Privacy is to Open up Your Data." iSpirt. 2017.
[22] http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf
[23] http://dla.gov.in/sites/default/files/pdf/DigitalLockerTechnologyFramework%20v1.1.pdf

individual's identity via the Aadhar system. There is then a sub-AUA/KUA layer, which lets entities engage with an AUA/KUA for a specific service, creating a federated model of different authentication hubs and entities linked to them.

The India Stack utilizes layered data classifications and a proportional approach to data sharing that differs from traditional consent-based models by allowing consumers to manage sharing of their data in a more granular and case-by-case manner. As Bhojwani notes, "Consent is more nuanced than a simple yes or no. By forcing consent into a binary, data providers reduce their offerings to a 'take it' or 'leave it' choice. This is a meaningless choice for the consumer."[24] Some of the most interesting consumer control elements include:

- Definition of, and differentiated responsibilities for, data provider, data consumer and consent collector.[25]
- What information is shared and any usage restrictions for this information is recorded alongside the consent to share itself. To facilitate this record keeping, each "e-document" stored in the digital lockers must have a Document Unique Record Identifier (URI).[26]
- For each process of consent, there is a Consent Artefact in XML format that shows the privileges and restrictions on data access and sharing for each instance of data sharing. This is intended to move consent away from standard form contracts, where consumers do not have ability to customize consent at the individual data source or data recipient level.
- A proposed "federated approach" to data storage, where there would not be a single, central repository for consumers' data, but instead several central repositories for different types of data—e.g. health, education. A federated system would likely create a new layer of "super-aggregators", which could be public or private entities, and would manage these central repositories. However, this model has not yet been accepted across all government authorities.

Data Aggregation Services

Similar to most market-wide data sharing models, the India Stack will likely need account aggregators to facilitate consumer-led data sharing. In 2016 the "Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions" (2016) was issued by the Reserve Bank of India (RBI), and has been updated as of February, 2018.[27] However this Direction's impact to date may be limited due to several features of its design:

- Loan records are not explicitly mentioned in the list of financial information an aggregator may collect, although they are not explicitly prohibited either, as the list of financial information includes "any other information as may be specified by the Bank for the purposes of these directions, from time to time." There was also a June, 2018 announcement of a new Public Credit Registry, which will consolidate loan information that is currently disbursed across various

[24] Tanuj Bhojwani. "The Best Way Forward for Privacy is to Open up Your Data." iSpirt. 2017.
[25] "Electronic Consent Framework: Technology Specifications, Version 1.1." Digital Locker Authority of India.
[26] "Digital Locker Technology Framework: Version 1.1." Digital Locker Authority of India.
[27] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598&Mode=0, for all references to the Master Directions in this discussion.

different credit information repositories in India, which operate under different standards and rules.[28] Such a registry could be a complement to the aggregator model.

- The Directions do not permit the aggregators to store consumers' information accessed, nor to process transactions on behalf of the consumer. This contrasts with the ability to store information and to facilitate transactions within the various licenses created by the EU's PSD2.
- The Directions set requirements for Financial Information Providers to allow access for aggregators if they can verify the consent artefacts provided by their customer requesting the aggregator to access such information. However, the Directions do not establish any standard APIs or other such connections, and so aggregators must enter into individual agreements with all financial information providers they will seek information from on behalf of consumers. This could make the process time consuming, would require financial information providers have the necessary technological capabilities to support such integration, and could make it easier for unwilling providers to delay reaching integration agreements with individual aggregators. It will also mean consumers have to sign up for stand-alone aggregation services, which may prove cumbersome or confusing to consumers who primarily engage with and know their existing finacncial information providers, and are not familiar with aggregator services.
- The Directions define the "business of an account aggregator" as "retrieving or collecting such financial information pertaining to its customer, as may be specified by the Bank from time to time; and consolidating, organizing and presenting such information to the customer or any other financial information user as may be specified by the Bank." This narrow definition omits some of the non-financial data use cases identified by the Digital Locker Authority, and so there will be a need for new aggregator rules from an authority with a mandate beyond financial services, or the issuance of parallel, harmonized rules from authorities across sectors of the Indian economy.

Despite these limitations, there are several aspects of the Directions that offer useful policy templates for markets seeking to issue similar such rules:

- Consolidation of consent processes by requiring that the financial institution provides the customer consent artefact to the account aggregator, and the aggregator does not seek the consent itself. This helps to keep consumer consent within the scope of the data issuers and not scattered across data issuing and receiving entities.
- Limitations on aggregators using log-in credentials of consumers—"Account Aggregator shall not request or store customer credentials (like passwords, PINs, private keys) which may be used for authenticating customers to the Financial Information providers." This would prohibit current practices of third-party who log into consumer accounts on their behalf and scrape their data. However, without a standard process for aggregators to integrate with financial information providers removing the ability to login on behalf of consumers could reduce the ability of aggregators to access information without offering a safer alternative.
- There are several consumer protection-relevant sections, such as Rights of the Customer, Data Security, Customer Grievance and Pricing that should give the RBI the ability to act against consumer protection abuses.

[28] https://timesofindia.indiatimes.com/business/india-business/rbi-to-set-up-public-credit-registry-on-all-borrowers/articleshow/64482736.cms

Mandatory or voluntary data porting?

An open question for the India Stack is whether sharing of financial or other data will be mandated, as there are draft regulations from the Reserve Bank of India that would do so, but this is not certain to be issued as such. When the 2016 Account Aggregator licenses were issued they did not initially receive any applications—and recent reports indicate only a handful of applications pending—which may indicate a limited business case for an aggregator in the present voluntary data sharing environment. One local expert noted the current Aggregator rules are further challenged by a lack of clarity as to how data providers will engage with these aggregators; a use limitation provision in the license, where the aggregators cannot collect data to facilitate a financial transaction; and the license only covering financial institutions supervised by the RBI.

The experience with the Account Aggregator licenses may serve as a caution that policy approaches that do not include some form of mandatory, consumer-controlled data porting for financial services may not immediately catalyze financial sector participation. According to one local expert, whether financial data porting ends up being mandated will likely depend upon how the final version of the Data Protection Law being developed by the Ministry of Information Technology treats this subject, showing yet again the centrality of data privacy laws to data sharing models. Another local expert argued that even if financial data sharing is not mandated, the lending industry will make financial data sharing happen because they have a strong interest in the use case of this data for risk management. They also noted that the government, by sharing data in the DigiLocker such as tax records, has set an important precedent for financial data that will encourage the financial sector to voluntarily allow consumers to share their financial account data.

Data Privacy Concerns in the India Stack

There has been a significant amount of criticism and public debate regarding the India Stack and the Aadhaar system. A series of cases have been brought to the Supreme Court, including whether an Aadhar card can be mandatory to avail of government and other services,[29] and a 2017 declaration by the Supreme Court that Indians have a fundamental right to privacy.[30] Concerns have also been raised regarding participants in the Aadhar system not properly protecting individuals' information, leading to leaks of Aadhar numbers and related personal information,[31] and at least one case where software has been sold that lets a user view individuals' Aadhar-linked data in the UIDAI system.[32] There are also reports of high failure to match rates in the Aadhar system.[33] Specifically in financial services, the UIDAI in December, 2017 suspended Airtel from conducting Aadhar-based SIM verification, as a response to their automatically enrolling consumers in payment banks accounts without consumers' consent.[34] These concerns offer a note of caution for the development of data sharing models absent robust data

[29] https://www.moneylife.in/article/aadhaar-linking-supreme-court-says-it-will-pass-appropriate-interim-order-at-right-time/53186.html
[30] https://timesofindia.indiatimes.com/india/supreme-court-gives-india-a-private-life/articleshow/60215360.cms
[31] https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/view
[32] http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html
[33] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5741784/
[34] http://www.thehindu.com/business/Industry/uidai-suspends-airtel-airtel-payments-banks-ekyc-licence/article21822439.ece

privacy laws, as well as the need for emerging markets to significantly increase their supervisory capacity if they are to embark on a data sharing model as ambitious as the India Stack.

Emerging Lessons from DigiLocker

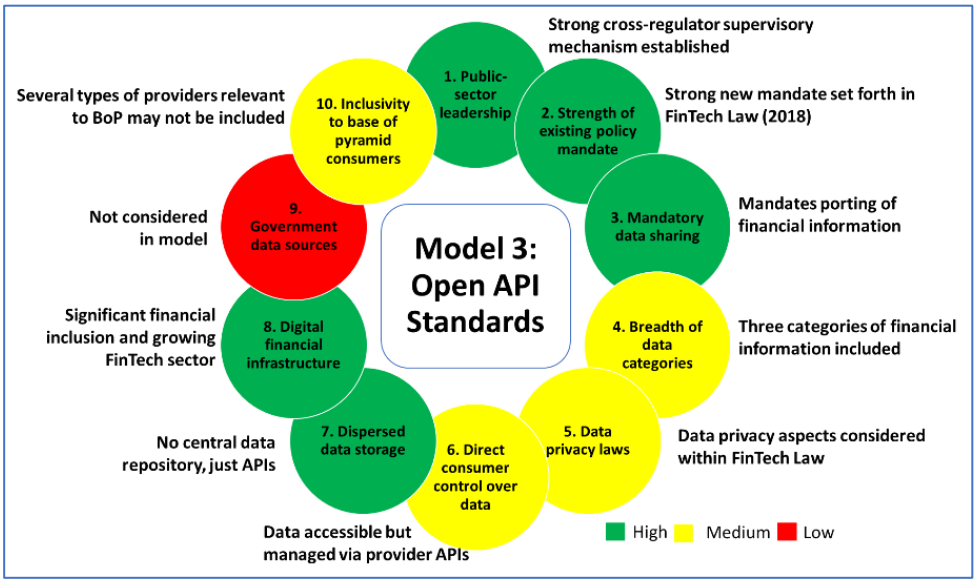
The state of financial inclusion, infrastructure and policy oversight in the Indian market is likely more analogous to the context of many emerging markets than either Australia or the United Kingdom. For example, oversight of the financial sector in India is more disbursed and internet access/internet literacy lower than developed economies. The path India has taken to achieve the considerable success already with the India Stack offers several lessons for emerging markets looking to pursue data sharing policies:

- The data sharing component of the India Stack has been incremental, beginning with identity and government data, and hopefully building upon this with other data such as financial and economic data. Many emerging markets lack sufficient e-government infrastructure or reliable identity verification services, so this innovation alone may add significant value irrespective of the economic data layered on top of it.
- India has invested extensively in increasing the footprint of digital financial services, which is likely a prerequisite for any emerging market data sharing model in financial services. This includes deposit account penetration, an interoperable payments platform, and a new Payments Bank licensing window for actors such as MNOs and agent networks.
- The DigiLocker is overseen by the Digital Locker Authority (DLA), established under the Ministry of Electronics and Information Technology, whose mandate is "to establish, administer, and manage Digital Locker system to preserve and retain information for efficient delivery of services to the users." The DLA also will be responsible for licensing Digital Locker Service Providers. There may not be an existing government institution in other emerging markets that can effectively oversee and manage licensing for data sharing models like the DigiLocker, so policymakers may want to consider creating a new supervisory body similar to the DLA. However, this could have a significant cost element, as the digital locker is currently run for free by the government for free, although there is the intention to bring in private actors to build a business model around the locker system in the future.

3. Open API Standards

Three key features of Open API Standards:

- Mandates data portability like Open Banking, but does not create a central platform for this, instead requiring banks to issue their own APIs.
- Links data portability requirements to legislation that expands oversight of FinTechs.
- May offer a less resource-intensive data sharing model than Open Banking and DigiLocker that could appeal to resource and capacity-constrained emerging market authorities.



In many emerging markets there are a substantial number of unregulated financial service providers. This increasingly includes FinTechs, who are using data-driven approaches to offer financial services via mobile, app and web channels. FinTechs create new challenges for financial sector oversight, as they use new delivery channels, leverage new alternative data sources, and often offer unique products—such as crowdfunding platforms—that blur lines between different types of financial services. In some markets data sharing rules and standards are being integrated into an expansion of oversight of FinTechs. In two of these markets—Mexico and Japan—the push for greater oversight of the FinTech sector is also enabling new standards for data-sharing models that integrate FinTechs alongside traditional financial service providers, which offers a lighter-touch but powerful alternative to Open Banking and Digital Locker models.

The Mexican Financial Technology Law

Approved in March 2018, the Financial Technology Law covers a wide range of FinTech topics relevant to data sharing.[35] This includes a new licensing window for FinTechs, administered via the National Banking

[35] The Financial Technology Bill amends a wide range of laws, including: the Law of Credit Institutions, the Securities Market Law, the General Law of Organizations and Auxiliary Activities of Credit, the Law for the Transparency and Financial Services, the Law to Regulate Credit Information Societies, the Law Of Protection and Defense of Financial Services Users, Law to Regulate Financial Agencies, the Advanced Electronic Signature Law, the Commission Act National Bank and Securities, the Federal Law for the Prevention and Identification of Operations with Resources of Illegal Origin and the General Law of Titles and Operations of credit.

and Securities Commission (CNBV), and increased competition by opening the market to new entrants. The Law also establishes a cross-authority Committee on Financial Technology Institutions that will oversee the implementation of the Financial Technology Law, comprised of the Ministry of Finance and Public Credit, the National Banking and Securities Commission and the Bank of Mexico.

Of particular relevance to data sharing is the requirement in the FinTech Law that financial institutions have open APIs that make possible—pending consumer authorization—connectivity and access for financial institutions, FinTechs and other third parties, for the purposes of sharing and transacting data and information, and to test new products and services before being offered to the public.

The data that may be shared under the FinTech Law has been classified in three types with different levels of openness to data sharing:

1. Open data, which is non-personal such as products on offer or branch locations.
2. Aggregated data, which is operational data but cannot be disaggregated to reveal individuals' data. This data is only accessible to entities who have in place authentication mechanisms set out by the relevant supervisory agencies.
3. Transactional data, which is for all open accounts, explicitly including credit products. This data can only be used under terms and purposes set forth by the client, and financial institutions must remove third-party access to this data as soon as a client requests, data is compromised, or the third party does not comply with T&Cs for exchange of information.

Unlike Open Banking in the UK, the Mexico FinTech Law does not establish a central set of APIs, rather it requires banks to publish and make available their own APIs. The Law also does not detail how data will be shared, and instead leaves it to the Committee on Financial Technology Institutions to establish standards for exchange of data in areas such as interoperability, security mechanisms for access to data, sending and acquiring of data, as well as consent mechanisms.

Perhaps the most interesting aspect of this Committee is that the Law provides the Committee with a competition and consumer-protection relevant mandate to set standards for exchange of data that ensure fairness, transparency, and no formal, regulatory, economic or practical barriers to entry for firms. Finally, the Committee is given strong punitive power in that it can suspend access and sharing of data temporarily or permanently.

Japan Banking Act Amendment (FinTech Bill)

Japan promulgated an amendment to the Banking Act that seeks to support the recommendations of the "Open Innovation" report of the Financial System Council, including establishing new rules on bank-fintech integration and sharing of account information by consumers.[36] The Bill was issued on June 2, 2017, with a date of enforcement to be determined, but not to exceed a year after date of promulgation.[37] The Bill has two main elements of relevance to data-sharing: 1. Requiring banks to publish their API standards; and 2. Creating licensing and integration processes for third-parties that will integrate with these APIs.[38]

[36] https://www.lexology.com/library/detail.aspx?g=43ab6b64-61ad-469e-9ef4-aa43141ad31c
[37] https://www.torys.com/insights/publications/2017/07/update-on-japanese-fintech-law
[38] http://techintokyo.com/fintech/revised-banking-act-in-japan

Similar to PSD2 in the European Union, the Bill establishes a new third-party service provider class, "Electronic Payment Intermediate Service Providers (EPISP)", and a registration process for EPISPs. Japan will however require these EPISPs to have a contract with a financial institution in place before offering their services to customers. To facilitate this linking between EPISPs and financial institutions, the bill also requires financial institutions to publish standards for EPISPs that allow them to conclude these contracts by nine months after promulgation of the FinTech Bill. The financial institutions will also be required to develop processes for introducing an Open API either by the data prescribed in a future Cabinet Order or not exceeding two years from the FinTech Bill's enforcement date.[39]

Emerging Lessons from Mandatory Open API Standards and FinTech Legislation.

For other emerging markets considering developing data sharing models, some of the key lessons from Japan and Mexico include:

- The embedding of data sharing rules into a broader bill that expands coverage of the financial sector. This could be a useful model for markets with gaps in oversight to address jurisdiction and enforcement limitations alongside data sharing rules. As a complement to the Bill in Japan, the Financial Service Agency is also considering reforms that would create equal coverage and requirements for banks and non-bank financial service providers.[40]
- Mexico's Oversight Committee is a formal cross-regulator supervisory body with powers of enforcement. This creates a formal, cross-sector authority without necessitating establishing a new agency.
- Both Mexico and Japan mandate Open APIs. Unlike the United Kingdom, they have not set up a new entity to develop common APIs, instead letting banks develop their own standards that they must publish, and in the case of Japan placing a time limit for when these standards must be published. For markets where an entity such as Open Banking Limited may not be feasible, this approach offers an alternative that still mandates Open APIs.
- In Mexico the Oversight Committee has a competition mandate to address issues such as barriers to entry related to data sharing, yet this was achieved without having to invoke the jurisdiction of any competition authority. Where competition authorities do not exist, this approach may be an alternative to developing a new competition law and related authority.

[39] https://www.torys.com/insights/publications/2017/07/update-on-japanese-fintech-law

[40] https://www.bloomberg.com/news/articles/2018-02-26/japan-finance-regulation-shakeup-seen-as-game-changer-for-banks

VI. Data privacy rules to enable data sharing

Three key features of data privacy rules to enable data sharing:

- Set requirements for consumer access to, and portability of, the personal information, paving the way for financial information sharing by consumers.
- Improve upon "check-the-box" consent practices by using design elements such as default opt-out for data sharing, restrictions on purpose and time of data usage, and prohibiting the requirement to share information with third parties as a condition of acquiring a product or service.
- Set liability requirements for data controllers regarding third-party data recipients, increasing incentive for firms to properly vet those they will share consumers' information with.

While traditional data privacy rules emphasized disclosure and consent, there is growing recognition that consent is not always effective to ensure data privacy and consumer control.[41] Modern data privacy laws are moving from a consent-based to a rights and usage based approach to privacy. This shift has significant positive implications for development of data sharing models as they often include specific discussion of data sharing, including data security, consumers' rights to manage their data, and when and to whom consumer data is shared.

Two recent privacy laws—the European Union's General Data Protection Rights, and the Philippines Data Privacy Act and the related Implementing Rules and Regulations—as well as the "White Paper of the Committee of Experts on a Data Protection Framework for India" demonstrate how certain data privacy principles can both support consumer-led data sharing and ensure that the proper set of protection and consumer rights are developed hand-in-hand with the data sharing models. Several examples of provisions in modern data privacy laws of relevance to data sharing are summarized below.

Data Portability

Most important for the advancement of data sharing models, new privacy laws like GDPR and the Philippines Data Privacy Act often include the right for consumers to port their data to third-parties they designate to receive such information, and in fact data portability is one of the fundamental consumer rights in both laws. In the Philippines this includes the right for data subjects to "obtain a copy of their personal information in a commonly used electronic or structured format so that it can easily be moved to a new controller, thus preventing customer 'lock-in.'"[42]

Right to Be Informed

In the Philippines the data subject must be informed regarding a range of aspects of the data processing: The information to be entered; the purposes for which it will be processed; the scope and method of the processing; the recipients or classes of recipients to whom personal data will be disclosed; methods for automated access to the data; the identity and contact details for the data controller, and the period for

[41] See, for example, Center for Financial Services Innovation, "Liability, Transparency and Consumer Control in Data Sharing"; "Reserve Bank of India's "Rights-Based Data Protection Framework for Financial Information"; Rahul Matthan, "Beyond Consent: A new paradigm for data protection"

[42] https://iapp.org/news/a/gdpr-matchup-the-philippines-data-privacy-act-and-its-implementing-rules-and-regulations/

which the personal data will be stored; and their rights to access and correct the data or lodge a complaint before the National Privacy Commission.

Specification and Limitations of Purpose

The India White Paper proposes the principle of data minimization, in that any processing of data has to be necessary for the purposes specified in that case and should be for the minimum data needed. This is a principle echoed by both the EU and Philippines privacy laws, which increase the requirements for data collectors and processors to specify how they will use a subject's data, and place limits on this use. This contrasts with data usage clauses in standard form contracts in digital financial services such as mobile money, which often give wide ranging discretion for firms to use this data for business purposes.[43]

Consumer Ability to Access their Data

The Philippines Data Privacy Act gives a data subject the right to obtain from a data controller a copy of any personal information processed by electronic means, as well as allowing for further use of this data by the data subject.

Specific Consent and Restrictions on Data Processing

The GDPR includes several rules to avoid "tick the box" applications of disclosure, including that consent must be via a positive opt-in and not pre-checked boxes, and the consent must be separate from other Terms and Conditions.

Liability of Data Controllers

The GDPR makes data controllers liable to ensure that any contracts they have with data processors comply with GDPR. They must also keep processing records of all such data transfers to processors and the data controllers are responsible for data breaches of processors. Similarly, the Indian White Paper proposes that "the data controller shall be held accountable for any processing of data, whether by itself or entities with whom it may have shared the data for processing."[44] This may incentivize data controllers to more carefully vet and monitor those they share data with.

Technology Agnosticism

The India White Paper emphasizes the need for a new privacy law to support the Government of India's Digital India Initiative, and that such a law must not just protect consumers but facilitate digital innovation. This includes a forward-looking expectation that the Data Privacy Law "must be flexible to take into account changing technologies and standards of compliance."

Both the EU and Philippines laws are having noticeable impacts on data privacy discussions and practices in their jurisdictions. There has been significant discussion recently of how the GDPR is causing major web platforms like Facebook and Google to significantly modify their privacy and data collection and usage practices.[45] Meanwhile, in the Philippines a cross-regulator National Privacy Commission has

[43] https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/01_2017/ITU_FGDFS_Report-on-Review-of-DFS-User-Agreements-in-Africa.pdf
[44] http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf
[45] https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html

been set up to implement the Data Privacy Act across different sectors of the economy. According to one local policymaker, the Philippines has formed a working group with industry associations to review how the Act will affect the regulations set forth by the Central Bank, how to harmonize financial sector regulations with the Act to limit reporting burdens or redundancies on firms, and how they can support consumer awareness of their new rights under the Act in financial services.

In India the debate around the development of the Data Privacy Law is occurring within the context of the India Stack and DigiLocker. This has shifted discussions on data privacy from discussions centered on categories of information—e.g. health, financial, identity—to use of data. A use-based approach would classify data as sensitive or non-sensitive data based more on the use of the data than the type of data. This may be better suited to respond to the wide range of new data types that are feeding into financial service provision and making traditional classifications of data types more difficult. To this end, Dvara Reseach have proposed a helpful data usage limitation definition: "limited to what is necessary for performance of a service or provision of a product or at a stage immediately prior to performing the service or providing a product, and where no less intrusive means are available.[46]"

While a usage-based approach could reduce the ill-defined data sharing practices common in DFS, such an approach will necessitate abandoning the "check-the-box" approach to supervision that a consent-based regime may require, and a movement to what Dvara Research call "ex-ante enforcement tools and incentives that can engender better data practice before a data breach occurs" to monitor the various data collectors and receivers and how they uphold consumers' privacy rights.[47] Such an approach makes sense to ensure that the robust data protection and consumer rights advocated for in modern privacy laws are upheld. However, many supervisors in emerging markets currently struggle with even basic market conduct supervision such as transparency and suitability enforcement, so likely will not be ready to effectively lead ex-ante supervision of data sharing arrangements currently. This means that in addition to advocacy for new privacy laws to complement data sharing models, market facilitators will need to invest substantial effort in building the tools and internal capabilities for authorities—whether existing authorities like a financial sector regulator, or new authorities such as India's Digital Locker Authority—to supervise data sharing arrangements on a continuous basis.

[46] https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf
[47] https://www.dvara.com/blog/2018/02/07/our-response-to-the-white-paper-on-a-data-protection-framework-for-india/#

VII. Private Sector Data Sharing Models

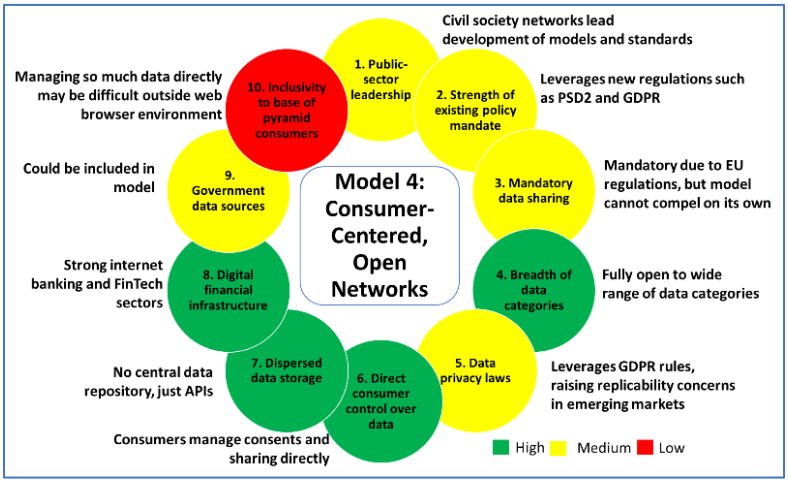
There are a wide range of private sector approaches to data sharing emerging. These models range from multi-party collaborations within industries such as payments services; to single actors aggregating data and making a data sharing marketplace for sectors of the economy; to third-party data management services that allow consumers to collect and organize the various data sources they have created through their personal, economic and social activity.

The sheer size of the private sector globally, as well as the wider range of options that exist compared to those available within the constraints of financial sector policymaking, means that this review of private sector models will not be close to exhaustive of all private data sharing models emerging globally. Instead, this section offers a few indicative examples of different ways in which private sector actors are collecting, structuring and allowing consumers to share their data in the context of financial services. The private sector typologies discussed are: 1. Consumer-centered, open networks; 2. Personal data management services; 3. Interoperable payments platforms; 4. Real economy data aggregators; 5. Private marketplaces; and 6. Credit reference bureaus and aggregators.

4. Consumer-centered, open networks

Three key features of personal data management services:

- Closest replication of public data-sharing models in the private sector.
- Emphasis on transparency in governance and openness to wide range of participants.
- Commonly involve the philanthropic and civil society sectors.



Consumer-centered, open networks bring together multiple participating data collectors and data recipients to let consumers share a wide range of information from their personal and economic lives. Consumer-centered, open networks differ from other private sector data sharing models discussed in this report due to their decentralized governance which does not place control of the network in the hands of any one firm, a transparent set of standards, and an openness to a diversity of firms and organizations.

These private networks may in fact bear less resemblance to other private sector models than the public-sector models discussed previously. They should then be viewed less as an alternative than a complement to public sector models. For example, a private network can help address the limitations on data types of a public network, by including new data types that regulators may not want to supervise yet, while still ensuring some standards for protection are in place instead of no oversight by either public or private actors. Public networks can in turn support private open networks by mandating sharing of highly useful data such as financial information, which could form the base data set and business viability for a private network to then build off with other voluntarily provided data sources. Similarly, while private networks lack the rule-making power of governments, they utilize codes of conduct or similar such self-regulatory approaches that could expand upon the minimum legal standards set forth for data-sharing. These networks could also complement government oversight and enforcement of minimum standards through their supervision of members and how they handle consumer information. Finally, the existence of data privacy laws can set minimum binding standards which private open networks can leverage to set rules for how participants in their network will comply with these requirements—as is the case with the MyData network and Open Banking Nigeria described below.

MyData (mydata.org)

MyData is a global network of data advocates for open, consumer-led data sharing approaches, and offers a good example of how private sector open networks can support similar objectives to public sector networks. While MyData does not follow a single set of data sharing rules or protocols, MyData centers around three principles:[48]

1. Human centric control and privacy. This places control over the information to be shared and the rights granted to firms to access this data in the hands of the individual directly so they can directly manage their data and privacy.
2. Usable data. Ensuring that the data shared is available in easy to access and use formats so that individuals and firms can make sense of and utilize this data.
3. An open business environment. A shared infrastructure so that data storage can be decentralized, firms can easily connect, and individuals can port their data and not be tied to a single data collector or repository.

Customer Custodianship of Data. MyData seeks to address a market inefficiency, where "Personal data is presently an underused 'raw material' for new services due to the lack of interoperability and portability between datasets across services and sectors."[49] Underlying the MyData approach is a consent-driven process, as opposed to a custodian-driven process. As such a MyData platform would be primarily a channel to manage consents, as "the data itself is not necessarily streamed through the services where the MyData

Figure 5: MyData consumer-centric model (https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/)

[48] https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/
[49] https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/

account is hosted."[50] (See Figure 5) Decentralizing data but centralizing consents is a design principle that helps to emphasize consumer control without placing an undue burden on the consumer to handle the actual data.

This consumer-centric system would still utilize data service providers similar to the AISP license in the UK and European Union, but would be a single operator each consumer selects, that they can easily cancel and change as needed. To implement such a platform, there would likely need to be a strong role of government, and the authors propose a public governance system as one of MyData's principles, which is supported by the fact that Finland is covered by the EU's PSD2 and GDPR legislation.

Global Standards for Local Adaptation. Implementation of MyData began with a sandbox testing with select operators in 2016 in Finland. According to one of the authors of the MyData concept, since that sandbox they have developed a new data sharing architecture called Sovrin (sovrin.org), which provides identity and data access and management technology and governance, to implement the coding concepts from the MyData architecture in a more scalable manner. Sovrin is a distributed-ledger based digital information and identity system, which its developers argue will "transform at least four major markets: identity and access management, cybersecurity, RegTech and data integration."[51] MyData is currently working with Finnish industry partners to put Sovrin into product use.

The vision of the MyData community is not to bring Sovrin or any other single model to a global scale, but rather to let domestic MyData communities use the MyData principles as adapted to their local market context. As one of the authors of the MyData concept explained, "MyData is a high level concept that can and will be implemented with many different approaches."[52] To this end several other markets are building their own interpretations of the MyData model, such as MesInfos in France, the Green and Blue Buttons in the United States, the My Data Store in Italy, and the midata.coop and the Health bank both in Switzerland. However, to date there do not appear to be any emerging market implementations.

Public, Private, or Both? The development of the MyData community and pilot in Finland makes clear that the private sector can play a role in promoting open data sharing models. While a model like MyData raises new challenges in managing participant incentives and rules-setting that models based on government decree may not, private models can offer flexible solutions that are often developed and improved upon in an open-source manner similar to the origins of the internet itself. For emerging markets where the government may not have the capacity to build their own Open Banking or Digital Locker equivalent, a private sector but open governance model like MyData could help governments struggling to turn their principles-based data sharing mandate into a well-functioning, open and consumer-led data sharing marketplace that is led by the private sector.

Open Banking Nigeria

In Nigeria a diverse set of technology and financial services firms have recently launched Open Banking Nigeria (https://openbanking.ng/about/). Open Banking Nigeria will develop common standard APIs among banks and other financial institutions, provide a sandbox for testing of Open Banking tools before they are certified, and promote the adoption of Open Banking across Nigeria. While still in early stages,

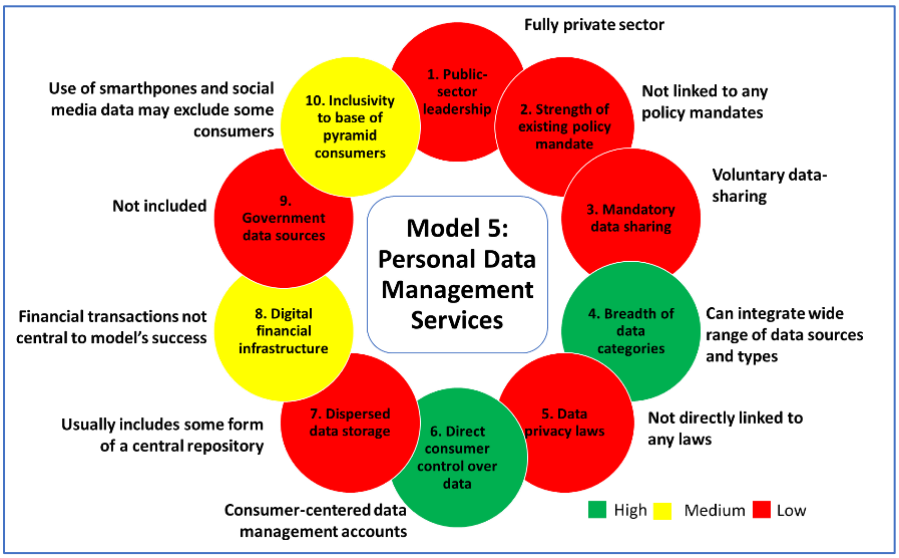
[50] https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/
[51] https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf
[52] Email correspondence with author, December 20, 2017.

this initiative is a promising development for African markets, and there is discussion that the private sector model may be complemented with government reforms, which would lend important support and increase participation in Open Banking Nigeria.

5. Personal data management services

Three key features of personal data management services:

- Provide highly-personalized tools for consumers to manage their wide-ranging online information.
- Offer high level of adaptability to different categories of electronic information.
- Likely to provide greatest value if they can support implementation of new rules and standards on data privacy and data management.



In the absence of—or perhaps as an input to—a private data sharing network like MyData, there are also firms that are developing data management services for individuals. Personal data management services help consumers by offering a combination of three services: 1. Collection of data across consumers' various accounts in a single point of storage; 2. Secure sharing of this data with third-parties; 3. Direct generation of new data sources. Central to this model is the challenge that while consumers would like to make use of their data, they do not necessarily know how to access and make sense of this data, nor can they independently identify the economic benefits they could derive from using this data. Data management services

Perhaps one of the most useful roles for personal data management services is to collect and make sense of a wide range of alternative data. For example, UK-based data management services firm Digi.me offers a mobile and desktop-enabled app that lets consumers create their own cloud-based data repository. The consumer connects Digi.me to a range of personal data sources, such as social media, and the app then keeps these records up to date for the consumer by pulling data from the consumer's handsets to the cloud. As third-parties need access to a consumer's data, Digi.me manages the authentication process, including consent and the limits on the specific set of data to share. An interesting data protection aspect of Digi.me is that the app pulls the data from the user's cloud account

and provides access for the third-party on the Digi.me platform, thereby keeping providers from directly accessing consumers' handsets where the original data is accessed. As a final security layer, Digi.me also does not hold any of the encryption keys, as the encryption occurs locally on the user's handset.[53]

Data management services in emerging markets. These data management services are beginning to appear in emerging markets. As an example, Optimetriks collects and makes sense of retail data, with a focus on helping small retailers in Kenya seeking to better capture data on their sales, stock and inventory. Optimetriks deploys data collection tools that include a mobile app, scraping of Google Streetview, Facebook Messenger chatbots, and satellite data. Optimetriks is also developing sensor cameras to monitor inventory and sales, as well as a new identity project called Gravity, a sort of Facebook connect for the offline world. Gravity aims at creating a digital identity platform leveraging blockchain, where users' self-declared identity attributes go through a verification mechanism that combines both official verification and peer-to-peer certification. The secure identity created via Gravity can then be easily shared with other stakeholders such as MNOs and fast-moving consumer goods (FMCG) companies, for whom establishing KYC data for their consumers or retailers is crucial to provide services.

The centrality of identity verification in the Optimetriks model demonstrates how data management services in emerging markets may end up offering a different suite of services based on the more limited availability of traditional data such as ID systems, asset registries, and business registries. We may therefore expect to see services in emerging markets offering a wider suite of services than in developed economies, where the existing identity and registration systems are more comprehensive and reliable. The adaptability of these services to differing degrees of information availability in a market or even across consumers makes these models an important complement to sector-specific data sharing models.

How to define the alternative data market?

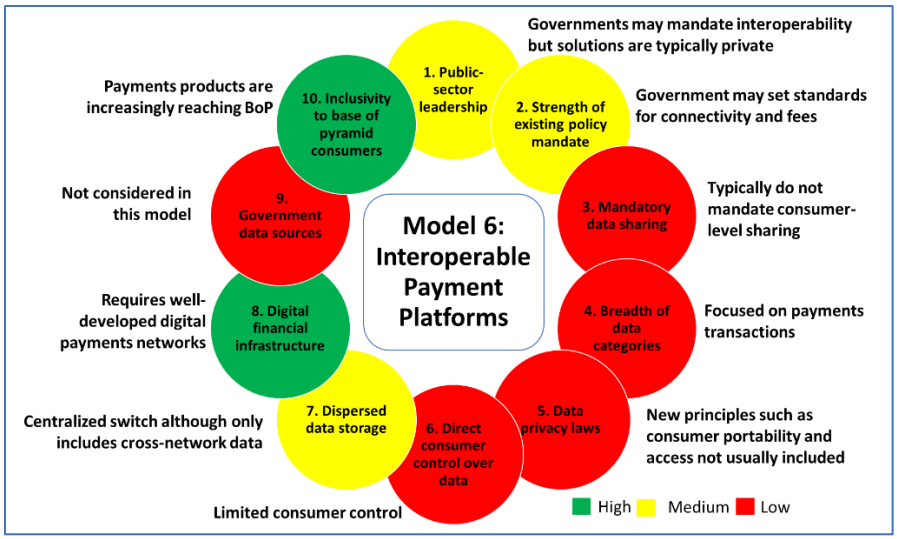
While the diversity of data collected by personal data management services will lead to an improved range of services for consumers, this diversity does pose a challenge to define and set rules for the handling of alternative data by these services. Even where there are not rules set forth by a government or collective like MyData, ensuring consumer protection and privacy is the responsibility of all data management services. However, monitoring and verifying the data protection practices of each start-up in this space could prove difficult if each firm is left to develop their own standards. This may call for a set of basic data management standards that all these firms can build their data privacy processes on. To this end, the Kantara Initiative Consent Management Solutions Working Group is creating "the world's first open, interoperable standards and certification to manage consent and privacy policies during the entire customer lifecycle journey." The initiative will provide tools for organizations that collect personal information using individual consent, with a specific focus on the EU General Data Protection Regulations (GDPR) requirements Such approaches will be important to ensure data management services maintain a focus on consumer control and data security. While private sector standards should always be complemented by data privacy law, in the near-term data management services may need to develop their own standards to help determine what is and is not responsible practice in this emerging industry.

[53] https://techcrunch.com/2017/08/17/digi-me-and-personal-merge/, https://techcrunch.com/2016/06/30/digi-me-bags-6-1m-to-put-users-in-the-driving-seat-for-sharing-personal-data/

6. Interoperable payments platforms

Three key features of interoperable payments platforms:

- Emerging market models do not yet include consumer-led data sharing features.
- Integrate many large financial service providers serving tens or hundreds of millions of consumers in a market—high potential for impact.
- Utility of data sharing may depend on whether payments services emerged after banking sector achieved high financial inclusion, or as a response to the lack of inclusion via traditional banking.



Mobile money and related services such as mobile delivered banking products have created a wealth of new data about consumers' and small businesses' economic activity in emerging markets such as Kenya, Tanzania and Uganda. This data has significant potential to help consumers to present a more fulsome picture of themselves and their economic activity to financial service providers and other firms. While electronic payments services and related platforms are becoming increasingly interoperable, they are not currently being maximized for data sharing benefits in emerging markets, even if they have the potential to serve such a role for their members. A natural first step would be to implement data-sharing rules similar to the EU's PSD2 for these platforms, enabling base-of-pyramid consumers in emerging markets to leverage this data in an open way that would offer an alternative to data silos such as the digital credit example described in Section 1. To help think through the potential and challenges of converting interoperable payments platforms into data sharing platforms, this section considers the potential for data sharing of payments platforms in Peru and China.

1. Pagos Digitales Peruanos (PDP) is an interoperable e-money payments platform and industry association in Peru that was formed to link e-Money Issuers with each other.
2. Wanglian is an operating company with 44 financial institution members, including payments giants Alibaba and Tencent, with members required to complete routing of transactions through

Wanglian by June 30, 2018.[54] Wanglian replaces the existing bilateral bank and payment service provide connections with a new centralized payments platform.

Data sharing potential

Both models do not explicitly mandate data sharing currently. In PDP data is accessed by each individual payment provider but is not shared across providers, with the only existing data sharing function of PDP being aggregated data analysis for market trends and a blacklist database that firms can access, which is primarily in place to comply with AML rules. While the details of Wanglian's rules on data sharing and usage are not clear yet, Wanglian will at a minimum shift data visibility on payments from solely the purview of the sender and receiver firms, as Wanglian will also now hold records of these payments transactions.[55] This could open the door for provision of this data to other members of Wanglian, and at a minimum will lead to more government monitoring and use of this payments data. The wide market coverage of both these platforms and the fact that aggregated data is already being collected and analyzed by the platform raises the potential to develop aggregated data for each consumer participating in the platform, ideally linking them across their multiple accounts.

Privacy concerns with expanding data sharing mandates

The integration of data-sharing functions into these payments platforms need to be considered in a manner that ensures appropriate data privacy protections. In particular the ability of a consumer to access their information needs to be checked against any potential for third-parties to share this information without the consumer providing explicit and limited consent. In Peru the privacy rules of the central bank in Peru afford the customer and provider co-ownership of the data (similar to the laws in Chile and Mexico that facilitate the Destácame platform described later on.) This means that it would be legally possible for a consumer to share their data, even if not technically possible in PDP currently. This co-ownership could be expanded to not only allow the customer access to such data, but mandate that such access be easy and this data be portable to authorized data recipients at the consumer's discretion. While nothing within PDP precludes their members from sharing data in this manner, there may be some reluctance to do so for competitive reasons. Similarly, PDP lacks account portability, so a consumer has to open a new account to switch providers even though it is an interoperable platform, which could limit the switching impact of a more open data sharing arrangement. There might be a need for the financial sector authority to mandate consumer-led data sharing as the industry could be reluctant to do so on their own volition. However, it is not hard to imagine a future where the PDP, if data sharing rules were expanded by the members or the government, could easily integrate data sharing and account porting into their interoperable payments platform in a manner similar to the EU and United Kingdom.

The Wanglian platform operates in a data privacy context that raises significant concerns as to whether such arrangements will be open, fair and pro-consumer. There is already significant use of both financial and alternative data for credit scoring and a wide range of other products and services in China.[56] For example, payments giant AliPay's Zhima Credit (or Sesame Credit in English) gives users a credit score

[54] http://www.scmp.com/business/companies/article/2105825/china-sets-clearing-house-online-payment-services-alipay-and
[55] http://technode.com/2017/08/09/chinas-central-bank-takes-more-control-over-mobile-transactions-wanglian/
[56] https://www.wired.com/story/age-of-social-credit/

based on the data they generate use AliBaba's various products and services.[57] Zhima Credit uses five dimensions of information to build this score: personal information, payment ability, credit history, social networks and behaviors, although details of the data and the algorithm are of course not publicly known.[58] AliPay reports more than 100 million users have take out loans to data, and they and Tencent are expanding partnerships with FinTechs—such as Tencent's new partnership with China Rapid Finance—and other sectors such as educational institutions and investment firms.[59] This shows the high value of payments and other digital data for consumers' benefit in acquiring new products and services.

In China these scores are being linked to the Chinese government's "social score," used by the Chinese government to punish those who do not pay back loans, court fees or other infractions with a range of restrictions, including the banning of more than six million Chinese citizens from air travel.[60] This is happening with little transparency or clear rules, and seemingly at the discretion of the government. This may explain why amidst all the debate in China there is virtually no discussion of consumer rights over their data or privacy, which may mean that the potential benefits of consumer-led data sharing in markets like China do not outweigh the risks of abusive practices and violations of consumers' privacy.

A need for data sharing rules for interoperable platforms?

The European Union's Payment Services Directive 2 (PSD2) requires consumers be allowed to port their payments account data to a new class of Account Information Service Providers. Could such a concept be expanded to interoperable payments platforms like in Peru and China, and would this be a relatively simple yet powerful step towards data sharing that sparks increased choice and competition in financial services? The answer to this question may depend on the availability of other useful sources of data. When the idea of an open platform was presented to one of the architects of PDP, they provided several features of the Peruvian market that may hinder this potential:

- Only 4 in 10 Peruvians have at least one mobile money account, while almost all Peruvians have a government ID and government records, which means a data sharing platform that begins with government information may be more impactful across all Peruvians.
- The difference in size of firms in their platform (both the biggest and smallest banks in Peru) could limit the ability to align incentives and voluntarily build a data-sharing platform. This would be a similar concern in China, especially with the rise of Alibaba and Tencent.
- In Peru there is comprehensive coverage by the credit bureaus and financial institutions have data analysis skills that means they can already pull useful data from all lender types and things like utilities payments without using e-money payments data, so the relative benefits of this payments data for value-added services may be smaller than in other emerging markets.

In contrast with Peru, the potential benefit of implementing data sharing on the back of interoperable payments platforms in the three East African markets analyzed in this report is considerable. Mobile money has surpassed the reach of any other form of financial service, ID systems after often weak,

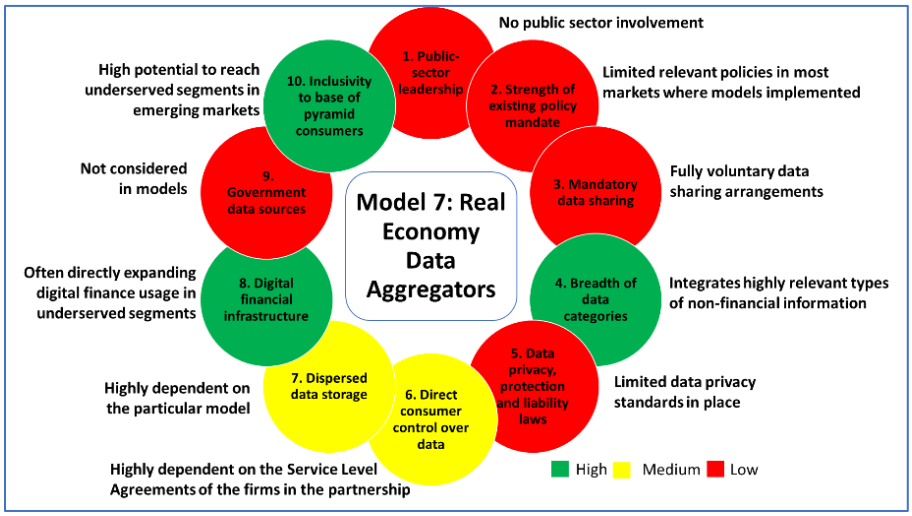
[57] https://www.wired.com/story/age-of-social-credit/
[58] https://www.cnbc.com/2017/03/16/china-social-credit-system-ant-financials-sesame-credit-and-others-give-scores-that-go-beyond-fico.html
[59] http://www.foxbusiness.com/features/2017/06/15/baidu-with-move-into-fintech-gets-wary-credit-ratings-look.html
[60] https://www.cnbc.com/2017/03/16/china-social-credit-system-ant-financials-sesame-credit-and-others-give-scores-that-go-beyond-fico.html

credit bureaus include mainly bank loans. As such the opening up of payments data for consumers to share more broadly via interoperable platforms and payments associations could be an important step to rein in the risks of market concentration and anti-competitive behavior that are common in some mobile-money dominated markets.[61]

7. Real economy data aggregators

Three key features of real economy data aggregators:

- Primarily seeking to digitize and improve services in real economy, not financial services.
- Typically view their role more as a platform for small enterprises to access financial services, rather than being a financial service provider themselves.
- In markets where public-sector approaches may not be feasible, these actors could form a private-sector data-sharing model with considerable positive impact.



Perhaps the most exciting aspect of the potential of data sharing models in Kenya, Tanzania, Uganda, and similar markets is the ways in which it could unlock improved services for the real economy that could foster economic growth. Kenya, Tanzania and Uganda all have significant informal sector employment, micro and small enterprises, and a large portion of the economy connected to agriculture. These sectors have suffered from information scarcity that can make it difficult to provide them with financial and business services. As mobile phone and web usage increases more financial transactions and business activities are digitized, informal sector activity is better measured, and these consumers and businesses can receive new products and services.

There are a growing number of private sector actors in these countries that are increasing the digital transactions and account ownership for these segments of the real economy, the "Real Economy Data Aggregators." These firms are not primarily focused on developing data sharing models, but through their work digitizing value chains they are increasing the number of digital financial service account

[61] http://wiredspace.wits.ac.za/bitstream/handle/10539/21629/AJIC-Issue-17-2016-Mazer-Rowan.pdf?sequence=3&isAllowed=y

holders, moving more economic activity into digital records, and coordinating dispersed small and often informal firms. All of these activities help build the enabling environment for data sharing models to be launched. These Real Economy Data Aggregators are also integrating financial service providers into their platforms, in many cases through multi-provider partnerships instead of bilateral "data silos." They lack the conflict of interest of being both the channel provider and the financial service provider, which means that these actors may be more interested in supporting increased consumer choice through data access and portability. Several of the more promising use cases for Real Economy Data Aggregators found in Kenya, Tanzania and Uganda are highlighted below.

Small business inventory

Much of the data sharing innovations in Kenya, Tanzania and Uganda have focused on unsecured consumer lending, leveraging personal transactional data such as CDR and Mobile Money Data. New innovations that are capturing financial and economic activity more closely linked to businesses may provide the needed economic information to provide a more diverse set of digital products beyond short-term consumer lending. In Tanzania one example of this is Sarafu, a project of the Azam Group, one of the leading consumer goods manufacturers in Tanzania. Sarafu is an app-based approach to move Azam's wholesale sales away from cash. The app allows customers to register an account and link funding sources including local banks and mobile wallets, to facilitate payments for goods and services right now from Azam and eventually other partners. The app will track new and historical data on turnover, transaction volumes, and what the customer is buying. Unlike MNO models where payments are the service, Sarafu approaches these transactions from a value-add perspective, providing business services such as transport, logistics, insurance and related services to facilitate transactions. Sarafu, through the Azam group, can leverage data and other kinds of information provided by the user to segment and target discounts or promotions at varying levels of the supply chain, reaching different customers with different value propositions based on their transactions volumes and business needs. For Sarafu, the business of digital payments is an entry point towards creating comprehensive businesses services that are data driven.

In Kenya, Maisha Meds is digitizing pharmacy sales records and inventory tracking via an app where users manually enter their business' transactions. This data is used to offer pharmacies automatic restocking management and wholesale sourcing with big pharmaceutical firms. Maisha Meds quickly found that their users also wanted a way to download their records to use for accessing loans, insurance, or for audits by Kenya Revenue Authority, and so developed a .csv version of these records that can be downloaded and shared. Maisha Meds is now partnering with KMET SACCO to preapprove pharmacies and clinics for credit using transaction data as KYC and provide trade credit for wholesale orders from pharmaceutical manufacturers. Going forward, Maisha Meds is considering a lead generation model for financial services, as well as aggregated, anonymized consumer data, to help pharmaceutical firms understand market trends, and a tool to help pharmacies manage in-store credit to customers.

Agricultural value chains

Given the outsize importance of agriculture in the economies of Kenya, Tanzania and Uganda, improving services that impact productivity, access to markets and inputs could improve well-being of tens of millions of smallholder farmers. There are many data sharing platforms linked to agricultural value

chains emerging in the region. This includes partnerships like MercyCorps' AgriFin Accelerate program, which connects MNOs, NGOs, FinTech firms and farmer groups to digitize smallholder value chains in Kenya, Tanzania and Zambia, and has reached over 850,000 farmers already across 40 implementation partners. The bundled services offered to farmers include digitized payments, savings, input credit and learning content delivered via USSD, SMS and mobile applications. While AFA supports some solutions which offer farmers choice of operator, other engagements support bilateral partnerships with MNOs/MMO where farmers do not have choice as to the network in order to access services on offer. Expanding choice of financial service providers is a goal for the AFA in the longer-term, however AFA noted that these bilateral partnerships matter because over-the-top plays like app-based lenders will not be a reality in rural areas for a long time, and the MNOs are best at customer acquisition.

Another innovator is agrochemical leader Syngenta, who have developed a series of partnerships with firms and farmer networks to take advantage of a wide range of alternative data sources relevant to farmers and agricultural value chains. According to Syngenta, by providing more granular data on individual farms and farmers, these data sources will allow them to both offer more tailored and comprehensive bundled services— including seed, crop protection, fertilizers and insurance— as well as more customized financial and extension services. This includes alternative data and remote sensing technologies such as Satellite and UAV data that can monitor health of farmers' plants and convert this into actionable agronomic advisory services. This allows technical advisory to target the right farmers when they are ready for inputs like seed, or when they may need in-person technical assistance to make sure the health of the plant is maintained. One of the biggest challenges Syngenta faces to scale these type of partnerships and projects is the limited reach they have to many smallholders, as many segments of agriculture sales are still primarily in cash. Were Syngenta able to easily access their financial data in a consolidated manner, leveraging new digital financial services information such as bank data or off-grid energy services, they could better identify farmers' income and cash flows and offer better product targeting and perhaps better terms to farmers. Syngenta is currently partnering with Tulaa (a digital financial services company) to take input orders on credit from farmers, track GPS coordinates, manage efficient distribution and better track yields and offtake data of smallholders to streamline our digital financial services work. Finally, Syngenta is experimenting with digital extension tools hosted by Arifu to evaluate credit scoring potential based on how farmers use the platform, including performance on quizzes. The combination of these tools is allowing Syngenta to bring input credit to both retailers and smallholder farmers at scale across multiple countries, where they are targeting a reach of 1 million accessing these digital financial services in the next few years.

Social platforms

Financial and business service providers are not the only ways in which rural consumers are increasing their digital engagement. There is a growing role of social and educational platforms in bringing rural Africans into the digital economy. Arifu is a digital platform that provides digital learning content both independently and as a white-label for banks and other providers across Africa, with a cumulative user base of 600,000 in three years of operations. Arifu learners access a wide range of learning content such as financial services, business management, and crop management, primarily via SMS. Arifu utilizes these SMS interactions with consumers to build out demographic models, leveraging in particular the free form responses from consumers. This includes categorizing the data around sentiment, grammar, language analysis, time of day to build customer segments. One of the outputs of Arifu's analysis is an identity system where they create levels of confidence of who the person is. Arifu is working to develop

direct links from the Arifu educational content to the USSD menu of a digital finance provider, as well as an API with credit bureaus where they could offer trainings on credit history and direct checking of credit history in the Arifu marketplace.

Another social platform with significant potential for rural Africans and their data is BRCK. BRCK provides off-grid internet access points in rural communities in Kenya and Rwanda. The BRCK box connects to GSM, satellite or fiber and provides internet access via wi-fi, and is commonly placed in central locations of small villages or public transportation. While they are not a financial service provider, their model could address infrastructure challenges that hinder data sharing for the large rural population in East Africa. Each device has up to 5TB of storage capacity, and BRCK is pre-loading educational content, software updates for their partners and other content to be downloaded or watched for free without paying for a GSM connection. BRCK have already partnered with companies like Facebook to promote their services and content via their BRCK devices, and could support financial service providers looking to reach these communities, such as through a data sharing platform with archived information for individuals that can be uploaded locally then shared via GSM.

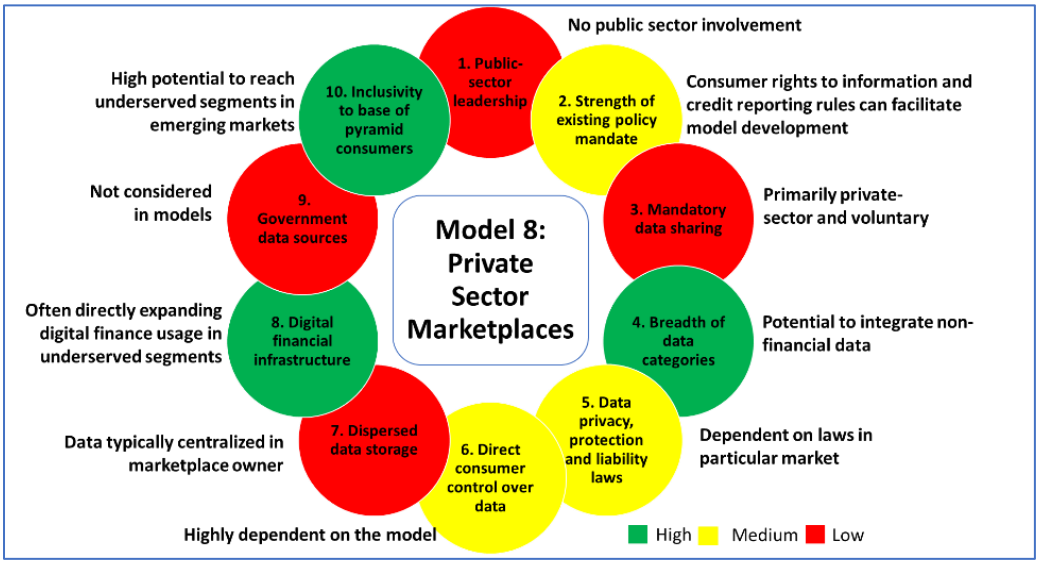
A way out of data silos?

The examples of Real Economy Data Aggregators above—which are just a small sample of those identified across East Africa—all have one important trait in common: None of them have the inherent conflict of interest of both wanting to be the platform and the provider of value added services on top of this platform. This is an important difference in these models from data silos such as closed MNO-lender partnerships that have dominated digital credit in East Africa to date. In nearly all conversations with data aggregators in East Africa there was a desire expressed to facilitate greater consumer control over their data and choice in the marketplace. Reaching this goal may be easier for over-the-top actors like Sarafu and Maisha Meds than the models who have entered into direct partnerships with MNOs and other firms that traditionally have not allowed their consumers easy access to and porting of their data. While each of these actors are still relatively small in reach, there may be potential in bringing them together to test private sector data sharing models that could cumulatively include millions of individuals and small businesses who can leverage their data in a competitive financial marketplace.

8. Private sector marketplaces

Three key features of private sector marketplaces:

- Provide analytics and scoring services similar to credit reference bureaus.
- Utilize non-traditional data sources that are not always included in bureaus.
- Could potentially be used as platforms to offer real-time choice for consumers across multiple providers, but to date that use case has been limited.



The promise of linking data aggregators together in a consumer-led data sharing platform may not be so far off. Particularly in lending, there are already platforms that link consumers' data with potential lenders, acting as a lead-generator, creating data-driven Private Sector Marketplaces. Typically, these models will accumulate data on an individual from multiple sources into a single account, provide some form of assessment of the quality of the data and/or the risk level of the individual based on this data, and then share this data with financial service providers to make offers to the individuals for products or services. The level of consumer control and competition on in these Private Sector Marketplaces can vary considerably. Some models provide the consumer with direct control over their account and information, while others merely allow the consumer to consent to this data being shared by the operator of the Private Sector Marketplace with financial service providers chosen by the operator not the consumer.

One example is Destácame, a digital financial management platform in Chile and Mexico gives consumers control over combines traditional bureau data with non-traditional data to allow consumers to obtain credit offers. According to Destacame's co-founder, most of regulations in Latin America do not let consumer data be moved without consumer consent. Instead, the regulations dictate that the data administrator (e.g. a telco) is compelled to share data with the consumer at the consumer's request, and could be fined if they refuse to do so. This has created an opportunity for Destácame to create a consumer-controlled data repository that complies with Latin American regulations, pulling both traditional credit bureau data as well as alternative data—including non-financial data—to help the consumer create an online financial profile and a proprietary Destácame score that consumers share when they want to apply to financial products with different lender partners depending on the

consumer's profile. Destácame is currently generating more than US$5M in leads every month to more than 15 lenders, often to relatively "thin-file" consumers, demonstrating the potential that a competitive platform with elements of consumer control has for improving choice and access.

Similar models are emerging in Kenya and Tanzania. CARE in Tanzania has recently launched a savings group app, Chimoka, that allows savings groups to digitize their records, which addresses the pain point savings groups face of managing their collective finances and tracking which members contributed or borrowed what. While Chimoka partner with commercial banks to offer savings accounts for the savings groups, the information generated about these accounts on the Chimoka app is not restricted to be used or controlled solely by the banks, and Chimoka hope to enable their users to share this information to a range of providers to receive competing offers. Safaricom in Kenya is also moving beyond their closed-loop bank partnerships and piloting a credit score with a select set of FinTech lenders. Safaricom is offering a set of four different scores for each customer based on deposits to account, receipts, and bank to mpesa transfers, which the lender can then weigh as they see fit within their own scoring model (see Figure 6). The model uses an API where the lender provides an applicant's phone number, name and ID, and then ping the Safaricom API for the scores. By combining the Safaricom data with the link to the national ID registry—IPRS—one lender noted they will no longer have to manually verify KYC for loan disbursement, which will reduce their time to disburse an approved loan from 3-6 hours to mere minutes.

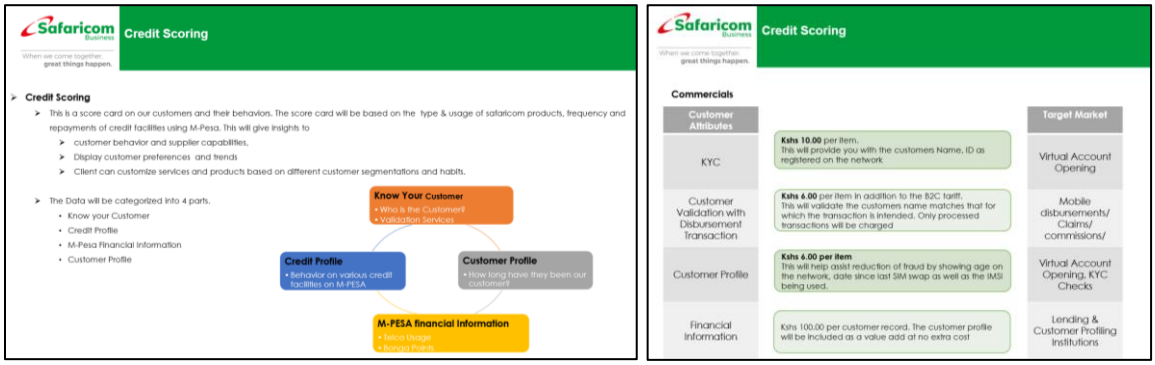


Figure 6: Safaricom Credit Score for Kenyan FinTechs

A lender who tested the new Safaricom Credit Score also found the score more accurate in predicting repayment than the app-based data scraping algorithms they have been using. This data is more accurate in part because it does not face the challenges their scraping model has with new phone customers who do not have long SMS receipt histories, as well as covering a wider set of historical data that Safaricom has and may not be in the SMS receipts over-the-top lenders scrape. This lender is also using the Safaricom data to change to more risk-based pricing, and can offer up to 250% larger loan size to first time borrowers by using the Safaricom data than their previous data sources. Another lender participating in the pilot believes Safaricom is offering the scorecard to diversify their revenue streams, "if you treat data as proprietary and limited to you, then all Safaricom will be able to do is offer a loan. They are delaying their opportunity to reap benefits right away. Data usage [e.g. M-Shwari and other direct provision models] will reach it's peak as revenue source, so what's next? Selling their own data."

Can Private Markets Really be Open Markets?

Private sector marketplaces improve upon the lack of customer data in many emerging markets, and the limited choice when the data holder—such as an MNO—only allows the consumer to share their data with one lender they have a commercial partnership with. Yet there is no guarantee these models will be truly open and consumer-led. This may mean that such models, while an improvement on existing digital lending models in emerging markets, are not a final step, but rather an intermediary step that can play two important roles within a broader data sharing model:

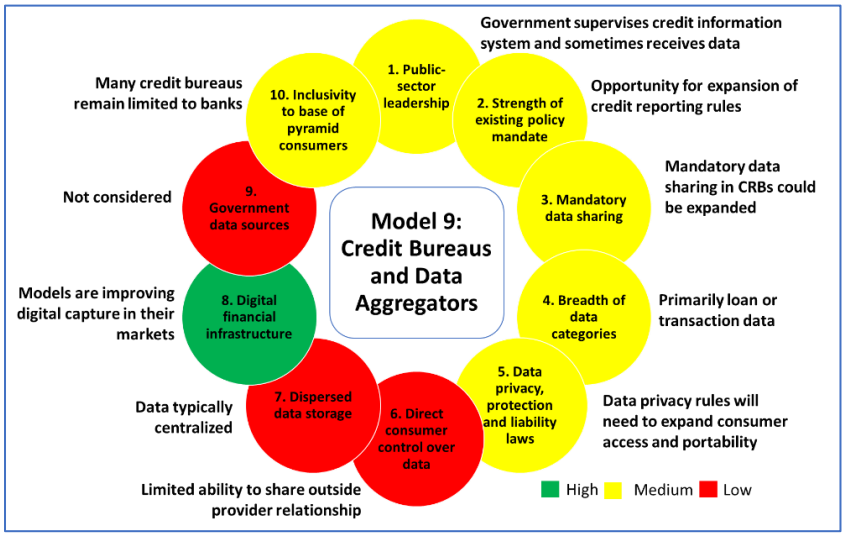
1. Converting large sets of varied data sources into a meaningful set of metrics that lenders can use to assess risk and offer loans.
2. Providing a user-friendly marketplace to receive, review and select live competing offers for loans and other financial services.

A final consideration for the private sector marketplaces is how they should be treated under existing, or perhaps new, credit reference bureau regulations. While the information these firms use is not exclusively credit history, that type of information is usually included, and these firms are generating credit scores that are being shared with others outside the credit reference bureau system. Obtaining a credit reference bureau license may be an excessive measure to impose on these types of private marketplaces. However, there is likely a need to develop some form of standards regarding how consumers' alternative data are used to build credit scores that are then shared beyond the firm doing the data collection.

9. Credit bureaus and data aggregators

Three key features of credit bureaus and data aggregators:

- Already facilitate a wide range of data-sharing and transactions in financial services.
- Aggregators currently lack ability to utilize information passing through their platforms, and may be easily adaptable to licensing windows similar to those like the EU's PSD2.
- Their roles in service facilitation versus service provision in data-sharing models would need to be well-defined to avoid conflicts of interest.



In many digital financial services markets, credit reference bureaus and aggregators are collecting and scoring financial data and alternative data, as well as integrating KYC, transactions and data processing across banks, mobile money operators and other financial service providers.[62] Several of the public-sector models reviewed in this report include new licensing regimes such as Account Information Service Providers in the United Kingdom or Data Aggregators in India, and emerging markets would likely need to develop similar such licensing windows to implement data sharing models. In Kenya, Tanzania and Uganda aggregators and credit reference bureaus have great potential to fill such roles. Some of the most appealing functions for CRBs and aggregators in these markets are described below.

Data Collection and Quality Control

Kenya, Tanzania and Uganda all have laws regarding credit reporting that compel commercial banks to report both positive and negative records to the credit reference bureaus. However, credit reference bureaus interviewed in these markets noted challenges with data quality and comprehensiveness. For example, in Uganda one bureau noted that the law currently allows an error acceptance level of 10% for data, while research by Credit Information Sharing Kenya identified inconsistencies in reporting by lenders across the three credit reference bureaus in Kenya (see Figure 7.)

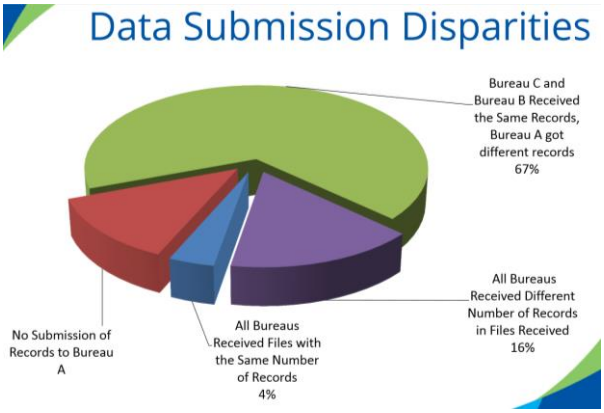


Figure 7: Differences in records submitted by banks across credit reference bureaus in Kenya, January - June, 2017. Presentation by Credit Information Sharing Kenya, September, 2017.

One possible solution to the challenges of data quality and inconsistent reporting is a data hub—a neutral entity that can receive data from a wide range of firms, manage quality and completeness, then share this data with participating credit reference bureaus. This would address the reliance on over-stretched bank supervision departments in some emerging market central banks to receive and supervise data submissions; and help remedy the practice of providers reporting different quality of data to different credit reference bureaus. Such an approach would simplify data submission for banks, help to standardize data quality, and according to one credit bureau would help FinTechs reduce fraud risk by offering an easier way to verify borrower identity. A data hub could also implement daily reporting, as the current 30-day reporting rules in markets like Kenya, Tanzania and Uganda are out of date and not useful for fast-moving digital credit products. For data sharing models more broadly, there may be a similar utility in a data hub for standardizing data quality and classification—including

[62] http://www.cgap.org/blog/aggregators-secret-sauce-digital-financial-expansion

alternative data—although such a model would also raise risks regarding data security by centralizing where consumer data sits.

Alternative Data Collection

There are credit reference bureaus in the region that are making headway on alternative data collection. In Kenya, one credit reference bureau has developed a mobile loan scorecard that is being used by several financial institutions to expand their servable base for short-term loans, as traditional scorecards were not as useful for decisioning on 30-day, small value loans. This bureau is also discussing alternative data collection partnerships with stakeholders in sectors such as agriculture value chains, and psychometric scoring firms. This reflects their view that among the most underserved segments are rural populations, where mobile money and app-based lending is not as prevalent. However, this bureau still called CDR and mobile money "the holy grail of data we would like to have access to," showing that even where bureaus are making headway with alternative data there is still much existing DFS data that is not easily accessed which could benefit borrowers.

Scoring and Analytics Services

Across the region most aggregators expressed interest in offering data analytics services, but are limited because in most cases neither they nor the consumer have control over the information generated by the financial transactions they facilitate. This leaves aggregator-facilitated transactions siloed except in rare instances (one aggregator did have data usage rights in one partnership with a bank on a merchant payments product, but this appeared to be an outlier). Several aggregators said they were working to try and secure rights to do data analytics from their partners, although it is quite possible large MNOs and banks would not be open to such an arrangement. As one aggregator noted, "this will require regulation. In [our country] we have tried to move mountains around data sharing and interoperability, but the authorities stopped halfway because MNOs were concerned about others stealing their data. We would like MNOs to be more fully integrated into the regulator's ecosystem to enable data sharing." While not all bureaus or aggregators are equally advanced in data analytics capability, there is an emerging expertise in this topic that could be leveraged to help make sense of financial, identity and alternative information in any data sharing models developed in East Africa.

Interoperable Nexus

Aggregators are already playing a leading role in enabling connectivity across financial service providers, utilities and commerce. One aggregator interviewed has gone a step further and are managing mobile money, bank and card interoperability arrangements in their market. Aggregators are also connecting financial services with government infrastructure, such as an aggregator that is developing data management and DFS use cases for hospitals and public transport. The goal of a data-sharing model is not just to make data available, but to leverage this data for greater choice and product innovation. Given the roles aggregators already play in making transactional data flow across financial service providers and linking financial services to the real economy, they could likely serve a hub role for data sharing models as well.

Financial Service Provider

Aggregators are also increasingly offering their own financial products and services. This includes offering their own deposit accounts, POS-enabled merchant payment networks, agent and card

networks, and providing digitization of dairy, maize and fish value chains for donors. One aggregator has issued their own SIM cards and trained their own agents for bulk payments in the coffee sector, which allows them to use some of the transaction data they are enabling through their services. This aggregator was even approached by one lender about offering loans to payees of bulk payments, although they have not pursued this option yet. From their view, to do such credit scoring services they would want to anonymize payees, give them a new unique ID, and only when you request the loan are you deanonymized to the lender—a good example of a privacy by design approach for data sharing models.

Aggregators and credit bureaus are already addressing data collection, data quality, data analytics and cross-firm integrations in financial services, all of which will be relevant to data sharing models. While some of the roles they are playing such as financial service provider may be a conflict of interest were they to become data sharing platforms, any licensing regimes developed should consider how the infrastructure already developed by these and other actors could be leveraged to quickly scale up data sharing models across financial services.

VIII. Data sharing in an East African context

Financial markets in East Africa could benefit from the development of consumer-led data sharing models. These markets have market concentration in sectors such as mobile money in Kenya and Uganda, consumers' financial history is often difficult for them to digitally access and share, and the financially underserved merchants and farmers could benefit from presenting a clearer picture of their economic lives to financial service providers. This section considers the needs and opportunities for advancing data sharing models in Kenya, Tanzania and Uganda.

1. Priority Needs for Data Sharing in Kenya, Tanzania and Uganda

Further development of competition policy mandates

The global review of public-sector data sharing models demonstrated the relevance of competition in enacting or enforcing data sharing mandates. Both Kenya and Tanzania have competition authorities, while Uganda does not have such an authority. In Kenya, the Competition Authority of Kenya (CAK) conducted a Banking Competition Market Inquiry in 2016 – 2017, which included two recommendations relevant to data sharing: 1. Review of consent practices for third-party data sharing by MNOs and DFS providers in light of both CAK and Communications Authority rules on consent; and 2. Review of open banking and other such innovations in other jurisdictions to address switching barriers identified in the Kenyan banking sector.[63] However, it is not clear if the CAK has sufficient mandate on data privacy and data usage beyond consent clauses, as there is not language directly addressing this in the Competition Act. This means policy reforms in the Competition Act or elsewhere may be needed to fully implement the recommendations set for the in the Inquiry.

In Tanzania, there may be restrictions on the ability of the Fair Competition Commission (FCC) to lead on data sharing due to jurisdiction. A local competition expert interviewed argued that this area of economic regulation would fall under the Tanzania Communications Regulatory Authority (TCRA), so they would have to refer the matter to TCRA for FCC to act. However, the expert did note that if MNOs or banks were to share data with each other, this could raise competition concerns, although FCC's role here would only be ex-post if there is no economic regulation covering the matter already, and they would not be empowered to set rules ex-ante. In reviewing the indicative data sharing models graphic developed by the interviewee (see Text Box below), the expert did believe these are integrated models that allow for competitors to have linkages and could touch upon Restrictive Trade Practices such as unwarranted agreements or horizontal arrangements that fall within the FCC's jurisdiction.

While Uganda does not yet have a competition authority, the Uganda Communications Commission (UCC) does have jurisdiction over several types of consumer data relevant to data sharing models, and a mandate that includes competition, licensing, consumer protection and anti-trust powers. One local expert argued that there could be issues of abuse of ownership of data by mobile financial service providers to maximize their market power that fits into UCC's competition mandate. Also, key data variables for financial innovation such as CDR, mobile money and SMS all touch upon regulated channels and data under UCC's jurisdiction. This may allow UCC to act regarding how this data is leveraged for

[63] Presentation by MacMillan Keck/Busara Center for Behavioral Economics of findings from Banking Competition Market Inquiry, Nairobi, September, 2017.

downstream services like financial products, rules for consent and data harvesting, cross-vendor data sharing, and interoperability of data sharing.

Increased regulatory coverage

The digital economy is blurring jurisdictional lines of financial services, telecommunications and information technology (IT). At the same time new over-the-top financial service providers are able to enter multiple markets with a low in-person presence and cost, and can be difficult for domestic authorities to track and effectively supervise. This is compounded by the fact that Kenya, Tanzania and Uganda all have regulatory coverage gaps in financial services, in particular a large collection of unregulated lenders. However, there are several promising developments that could help to address these gaps in the future:

- In Kenya the National Treasury on May 25, 2018 issued for public comment the Draft Financial Markets Conduct Bill,[64] which would establish a market conduct authority to oversee all non-banks, including currently unregulated lenders.
- The Uganda Microfinance Regulatory Authority has been established to supervise tier 4 moneylenders and MFIs. The establishing legislation, the Financial Institutions Act, also expands the potential for participation in the credit reference bureaus to a range of non-bank actors.
- The Bank of Uganda has established a Financial Services Innovation desk that will engage with FinTechs. Interestingly, in both Kenya[65] and Uganda, FinTech groups have advocated for regulation. As the head of the Uganda FinTech Association explained, regulation would help with risk of market ease of entry and scams, so investors and consumers could know which FinTechs are legitimate or not.

These steps are important to develop the supervisory and licensing arrangements necessary to ensure that data sharing rules and data intermediaries will cover as much of the market for financial services as possible. Similar to the path being pursued by Mexico with their FinTech Law, it may be possible for authorities in Kenya, Tanzania and Uganda to expand financial sector regulatory coverage at the same time as they establish new data sharing rules.

Development of data privacy legislation

All three markets lack a data privacy law, which is an important component to a national strategy on data sharing. While there are data privacy provisions in laws such as the Kenya Information and Communications (Consumer Protection) Regulations (2010) or the Tanzania Electronic Transaction Act (2014), these are not comprehensive and do not reflect modern principles of data sharing. In Kenya and Uganda there are draft Data Privacy Bills currently, while in Tanzania it was announced in December, 2017 by the Tanzanian Government that a personal data protection law was in development.[66] In Uganda a call for public comment on the Data Protection and Privacy Bill was issued in late 2017 and is progressing through the review process, while in Kenya the Minister of Information, Communication and

[64] http://www.treasury.go.ke/draft-financial-markets-conduct-bill-2018.html
[65] https://www.businessdailyafrica.com/markets/marketnews/Fintechs-call-for-own-regulator/3815534-4086808-ekrf3cz/index.html
[66] http://allafrica.com/stories/201712210571.html

Technology on June 11, 2018 announced that a new Data Protection Bill would be issued for public comment soon, and would take into account new models such as the EU GDPR.[67]

The Bill in Uganda is commendable as it introduces several important privacy principles such as requirements to notify the data subject prior to collection of the following: the purpose of data collection; the recipients of the data; whether the data collection is mandatory and the consequences of failure to provide the data; the right to access and correct the data; and the period for which the data will be retained. The Uganda Bill also requires that data controllers only allow a data processor to process personal data if they adhere to the security measures within the Bill, and prohibits their further processing of this data. There is also a duty to notify for data collectors, processors and controller of data breaches. However, the Bill in its current draft does not include data portability rights nor default opt-out settings for data sharing common in other recent privacy laws, and of benefit to supporting the emergence of data sharing models. Were these provisions to be added into the Uganda Data Protection and Privacy Bill, the Bill could offer an important architecture to facilitate data sharing models' emergence in Uganda.

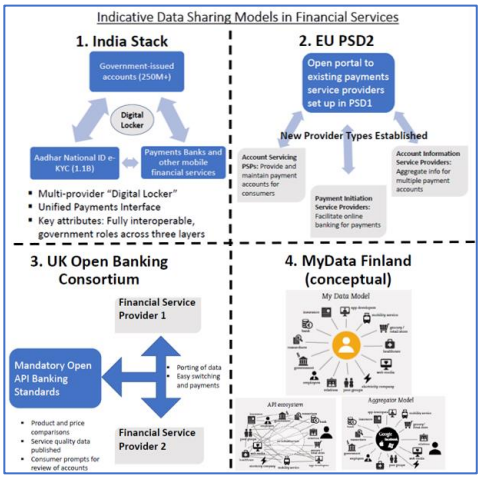
Increased regulatory coordination

To achieve policy enhancements on competition and market coverage will require substantial coordination across authorities. In all three markets there are MOUs between authorities such as communications, central bank and competition authorities. There are also coordinating bodies such as the Financial Markets Development Committee in Uganda—chaired by the Ministry of Finance, the National Council for Financial Inclusion in Tanzania, or the 2018-2022 Medium Term Plan in Kenya which will include elements regarding digital finance and innovation. These precedents speak well to the possibility that each market would be able to establish a coordinating mechanism—either within existing mechanisms or as a new entity—for data sharing policy development.

[67] https://www.the-star.co.ke/news/2018/06/11/draft-data-protection-bill-to-be-published-this-month-says-cs-mucheru_c1771558

What do East African experts think about global data sharing models' viability in their market?

As part of the research for this report, more than 50 local experts were consulted in Kenya, Tanzania and Uganda. These include government, donors and market facilitators, financial service providers and technology firms. To spark discussion, the interviewees were shown four indicative data sharing models globally, and asked to react to these models and their applicability to the East African context. (See Figure) The responses highlighted below show a mix of excitement towards data sharing models and a recognition of the current constraints that may challenge such models in East Africa.



Political Economy Challenges

- "The political economy makes these models hard to pull off in East Africa, but they would all improve highly personalized learning opportunities…Even having APIs with all FSPs would be useful to know the products and services and eligibility requirements they have. Could you apply a financial education tax to fund data aggregator and advisory services?" FinTech founder
- "I wonder if the UK model is possible in [country name]. It depends. Small banks and MNOs will accept that, but giants like [names several major MNOs and banks] won't agree unless you promise there will be a revenue share. To convince them I would start with history of interoperability, [MNO] was the last to join and this hurt them." Commercial bank
- **"**India Stack won't work here because of the political economy aspects. We can't lay the basic foundation, such as with credit bureaus and solid APIs, national ID… I am also worried this would lead to train wreck of overindebtedness like what happened in Andra Pradesh if we liberate data without having a good bureau in place yet." Government authority

Excitement for Mandatory Connectivity

- "PSD2 in particular is interesting in requiring FSPs to provide APIs. To address scraping and credential use workarounds, it would be better to simply require standards to implement API to help account owners manage their finances better using aggregated or pooled data with some mining. I would want to have read only APIs that can't originate transactions, to protect against wider data scraping. Transaction level data should be subject to tighter security standards for whoever gets access to this. The advantage would be providing unified interfaces for payments, as you have to remember many tokens and login credentials as of now." Mobile money aggregator
- "Models like this would give us a better customer base, with this kind of data we won't need to scrape as much from the handsets, and it will be much cheaper. In a competitive environment like that we will see more segmentation." FinTech lender
- "For the UK model a bank that knows what they are doing with customer experience, efficiency, and products will win. A bank only playing on the pricing, offering cheap stuff, only calling loans and deposits through shrinking of pricing, their customers will move. Eventually someone with bigger network may win. Smaller network wins only if they offer a better customer experience. One niche to target would be people at a bank only because employer has account there. Teacher's segment forced to use Mwalimu Bank. PSD2 model: I see CRBs going into AISPs license category but don't know how it will get here, because providers are not mandated to pass through bureau check currently." Commercial bank

(continued from preceding page)

Technology and Infrastructure Limitations in East Africa

- "The PSD2, UK, and MyData models are more applicable to situations where people are already accessing financial services. Here India model would be more applicable—leverage national ID to access information, open accounts and verify ID. You could start in [country] with ID, then layer on other things like health, education data. The India model also may work better because you have issues of access and capability of the consumer." Financial sector regulator
- "The easiest to adopt in [country name] is India, because we have National ID and KYC. Once you have that a digital locker can happen. EU PSD2 puts us as aggregators at an advantage, we are already account servicing PSPs and can already do predictive analytics on your payments." Mobile money aggregator
- "UK model makes a lot of sense, the customer has power to say bank A please send information to institution B. With mandatory open APIs, you will have to comply, and best part is customer is winning. This could work regardless of technology of consumer—you could do this on USSD…With this we could serve feature phone customers. We are working on feature phones now but the data we pick is very limited." FinTech lender

2. Emerging Opportunities to Advance Data Sharing in Kenya, Tanzania and Uganda

Increased digitization of government services

Here the three markets diverge considerably. Kenya has a well-functioning national ID system and an e-KYC function that, while not perfect, was cited as a significant advantage by multiple providers. Kenya is also expanding their e-government services in areas such as taxation and title deeds—including a blockchain application being developed to improve title deed accuracy.[68] In 2017 Uganda make significant improvements with National ID rollout, with interviewees reporting coverage from 80% and above after the UCC in April 2017 issued a notice that they would shut off any SIMs not registered to the new national ID.[69] The National Information Technology Authority in Uganda is now currently working on developing e-KYC services, which should greatly benefit data sharing model development. In Tanzania the national ID has only been provided to an estimated 5 million Tanzanians, and as noted in the discussion of credit bureaus, the ID lookup function is not yet automated so can be cumbersome to administer, limiting the utility of any government ID services currently.

Expanding financial and communications infrastructure

All three markets benefit from growing digital finance ecosystems, led in large part by the expansion of mobile money during the past 10 years. This has led to a greater number of consumers' financial history being digitally known, and the development of non-payment products like credit and insurance riding these mobile money rails. There is also an increasing interconnectivity of financial service providers. In Kenya PesaLink is connecting banks for small value payments, and Safaricom and Airtel launched wallet-

[68] https://www.standardmedia.co.ke/business/article/2001271535/land-register-to-use-bitcoin-technology
[69] https://www.independent.co.ug/national-ids-allowed-new-7-day-ucc-sim-card-deadline/

to-wallet interoperability on April 10, 2018. In Uganda there is interoperability between MTN and Airtel—although with off-network surcharges—and the pending National Payments System Act will likely create a national switch. In Tanzania interoperability across all MNOs has been a success and there is now a shift from bilateral connections to development of a central switch. Finally, as noted in prior sections, there is a diverse set of aggregators that are offering connectivity solutions across financial service providers already. These aggregators have expressed interest in doing more data sharing and analysis for consumers if they could adjust the terms of their Service Level Agreements with financial service providers to allow for such services to be offered.

Connecting underserved segments of the economy

The most exciting argument for data sharing models in Kenya, Tanzania and Uganda are the potential benefits to the real economy in areas such as agriculture value chains, small businesses and government services. This report highlighted a range of data collection and aggregation innovations occurring in the private sector, as well as data aggregation and customer verification occurring in the NGO space. While these innovations remain in their own siloed universes, their complementarities are substantial. There may be value in pursuing private sector solutions that connect new actors like Real Economy Data Aggregators, Private Marketplaces, with banks, MMOs, credit bureaus and data aggregators to build a more complete and centralized digital identity. With this data consolidated, there would likely be an increase in the diversity of products and services available to businesses and individuals who are currently underserved by formal financial services.

Breaking down the data silos in digital financial services

To achieve data sharing for financial inclusion, a major shift in mindset is needed for Kenya, Tanzania and Uganda's DFS sectors. Recent inquiries on issues like USSD channel access, or the need for government mandates to achieve mobile money interoperability, have laid bare the competition issues that come with market concentration in network economies such as DFS.[70] At the same time, banks and MNOs should not view data sharing as a threat or a system that makes winners and losers in a similar—if perhaps inverted—way that data silos already have. Too often we think of mobile money as the essential data source for DFS, but the breadth of new data sources being collected across so many parts of the economy will benefit banks and MNOs just as their sharing of mobile money and savings account data will benefit FinTechs. In fact, recent analysis by Caribou Digital called into question how useful mobile money data is for much beyond small value lending—a perspective shared by several of the interviewees in our research.[71] There is therefore a strong case to be made that all providers will get access to more customers and be better able to serve them while managing risk more effectively.

The use cases for a data sharing platform in financial services are far-ranging. Imagine how data sharing would help address the constant risk of fraud in mobile money or digital credit? Or how simpler a FinTech's algorithms would be if they did not have to scrape a wide range of data on consumers' phones to get the mobile money transaction receipt SMS they truly seek? As one FinTech lender noted when reviewing the UK Open Banking model, "with this kind of data we won't need to scrape as much from

[70] http://wiredspace.wits.ac.za/xmlui/bitstream/handle/10539/21629/AJIC-Issue-17-2016-Mazer-Rowan.pdf?sequence=3&isAllowed=y

[71] http://www.financedigitalafrica.org/wp-content/uploads/2018/03/FiDA-Can-Big-Data-Shape-Financial-Services-in-East-Africa.pdf

the handsets, and it will be much cheaper for us." Or imagine how data on smallholder farmers would let banks move down-market to informal sector businesses? Or conversely how access to banking data would let MNOs move upmarket to products beyond tiny loans and very basic life insurance cover? Too often we think that MNOs and banks control all the useful consumer data, but the reality is that there is so much new data being digitized across the economy that both big and small could benefit from data sharing in East Africa.

These use cases may explain why many of the banks interviewed did not fear data sharing models like the India Stack or Open Banking, but instead welcomed this as a chance to shine through better quality products and services. As one bank put it, "[In these models] a bank that knows what they are doing with customer experience, efficiency, products will win. A bank only playing on the pricing, offering cheap stuff, only calling loans and deposits through shrinking of pricing, their customers will move." The goal of a data sharing platform is not to make all financial service providers or their products the same. On the contrary such a model will lead to more innovation and better customer segmentation by giving each provider the same well-developed digital data trail that will make all providers and all products better tailored to the various segments of the real economy financial services aspire to impact across Kenya, Tanzania and Uganda.

IX. Conclusion

As this report documents, there is both a growing number of, and a growing momentum for, data sharing models globally. These models could have significant positive impact on the quality, quantity and costs of financial services in emerging markets, where many portions of the economy remain underserved despite recent improvements in basic financial access. Markets like the United Kingdom, Mexico, and India offer exciting policy roadmaps that can be pursued. Similarly, our deep dive into the markets of Kenya, Tanzania and Uganda demonstrate that there are numerous private sector innovations doing far more than just scraping phone data to offer consumer loans. There is a growing number of data sharing models that are addressing data shortfalls in important parts of these economies. Like all innovations, the biggest challenge is less the good idea, but willing the market to launch and then achieving scale, efficiency and security. This is why the single most important action to support data sharing in emerging markets is likely to be policy reforms, as experiences in other markets point to a need to compel certain minimum levels of data sharing for these models to reach a national scale. If this policy mandate can be enacted, then data sharing models could be an innovation as significant as the mobile money revolution was for emerging markets like Kenya, Tanzania and Uganda. The policy options and private sector solutions described herein offer a blueprint for data sharing ecosystems, and it is our hope that those reading this report will use these examples to begin advocating for the policy reforms needed in areas such as competition, financial service regulation, and data privacy that will pave the way for private-sector solutions.