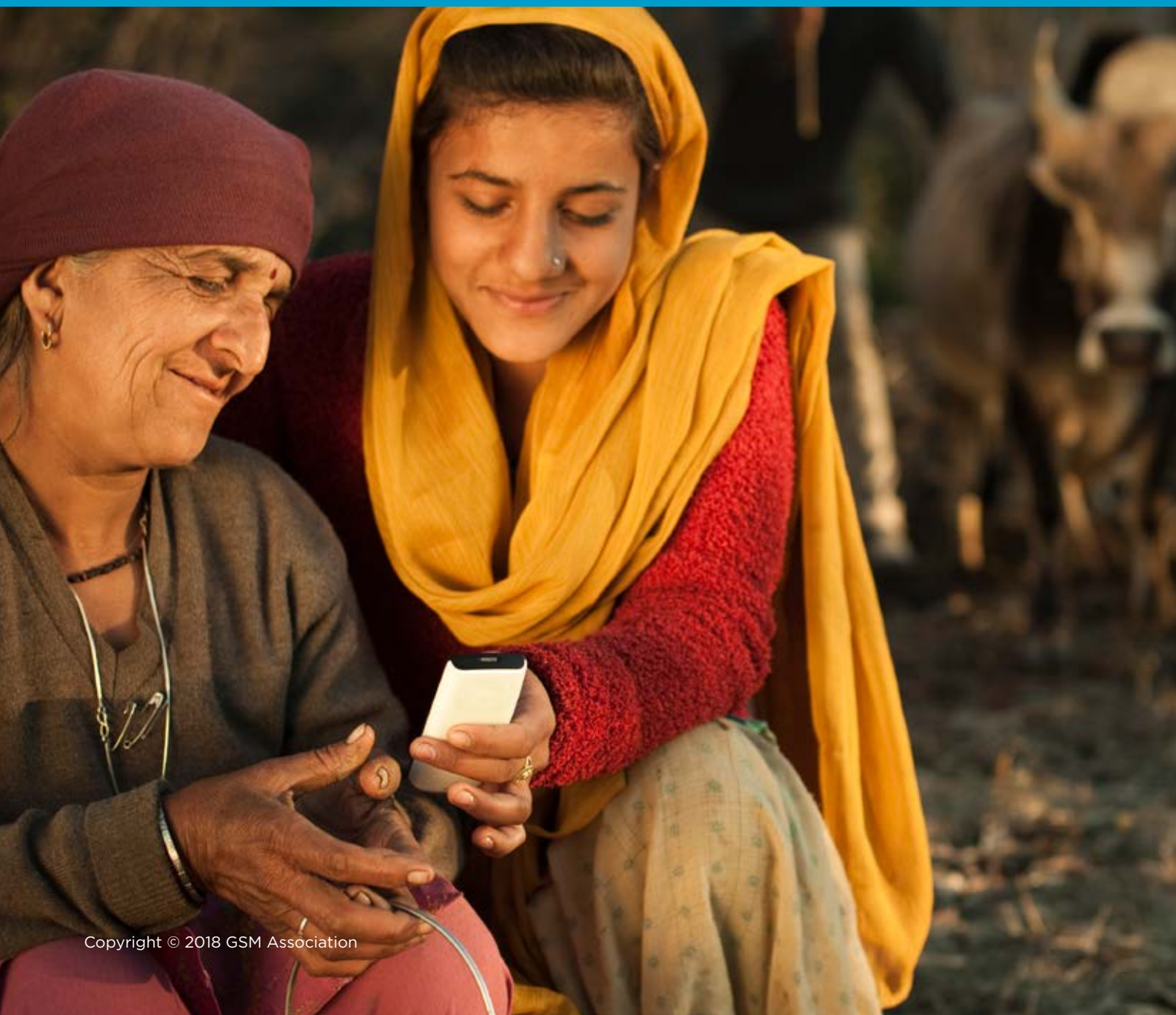
Access to Mobile Services and Proof-of-Identity:
Global policy trends, dependencies and risks



The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**

Follow the GSMA on Twitter: **@GSMA**

GSMA Digital Identity

The GSMA Digital Identity Programme is uniquely positioned to play a key role in advocating and raising awareness of the opportunity of mobile-enabled digital identity and life-enhancing services. Our programme works with mobile operators, governments and the development community to demonstrate the opportunities, address the barriers and highlight the value of mobile as an enabler of digital identification.

For more information, please visit the GSMA Digital Identity website at **www.gsma.com/digitalidentity**

Follow GSMA Mobile for Development on Twitter: **@GSMAm4d**

AUTHORS
Yiannis Theodorou – Director of Policy & Regulatory Affairs, Digital Identity, GSMA @yiathe
Erdoo Yongo – Policy Analyst, Digital Identity, GSMA

ACKNOWLEDGEMENTS
The GSMA would like to express its sincere appreciation to the World Bank and the office of the United Nations High Commissioner for Refugees (UNHCR) for sharing their insights and peer reviewing this report. NB. The data sources for this report are outlined in section 3 yet the data analysis, methodology and conclusions are the GSMA's.

Contents

01

Executive Summary

The ability to prove one's identity is essential to securing both rights and access to a number of life-enhancing services including healthcare, voting, education, financial services, employment and social protections. As we continue advancing in the digital age, identification becomes ever more critical to gaining access to mobile connectivity and a range of mobile services particularly across more than 140 countries where 'mandatory SIM registration' policies are in place.

The World Bank estimates that 1.1 billion[1] people worldwide lack any legal (State-issued or recognised) identification, predominantly in Africa and South Asia. Vulnerable groups – including migrants and refugees – in these regions who lack recognised identification are at a higher risk of being digitally, socially and financially excluded.

World leaders at the World Economic Forum 2018 have committed[2] to strengthening multistakeholder cooperation and collective action to pursue the opportunities that come with digital identities and ensure protection of rights in a sustainable and responsible manner. The United Nations had previously recognised the importance of addressing the 'identity gap' through its Sustainable Development Goal (SDG) 16.9 to 'provide legal identity for all, including birth registration, by 2030'[3].

The mobile industry was the first to publicly commit to addressing all 17 SDGs. With a global subscriber base that surpassed 5 billion[4] in 2017, the mobile ecosystem has created a global digital platform that is increasingly connecting everyone and everything. Individuals' ability to register for a mobile subscription in their own names could unlock access to a plethora of mobile-enabled services, such as Mobile Money[5] accounts, Pay-as-you-go Utility services[6], educational, health and other digital services.

But where proof-of-identity is required for a prepaid mobile subscription, it is important to ensure that identification barriers are addressed so that everyone is able to access these services. Mobile Network Operators (MNOs) have the ability to accelerate the scale and reach of digital identities that can empower citizens, while respecting their privacy and stimulating economic[7] and social development.

This report highlights that mobile penetration worldwide (in terms of unique subscribers) has increased over the last ten years from 39% to 66%[8]. In 2016 alone, the number of global unique subscribers grew by 5%[9]. Yet, a number of emerging markets – particularly across the African continent – are still lagging behind the rest of the world with less than 50% of the African population having a unique mobile subscription. The majority of mobile subscriptions (76% worldwide and 95% across Africa) are based on prepaid SIM cards and 92% of all prepaid SIMs are active in countries where SIM registration is mandatory.

1. World Bank ID4D initiative: http://www.worldbank.org/en/programs/id4d
2. https://www.weforum.org/press/2018/01/digital-identity-why-it-matters-and-why-it-s-important-we-get-it-right/
3. https://sustainabledevelopment.un.org/sdg16
4. https://www.gsma.com/newsroom/press-release/number-mobile-subscribers-worldwide-hits-5-billion/
5. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2016.pdf
6. https://www.forbes.com/sites/tobyshapshak/2016/01/28/how-kenyas-m-kopa-brings-prepaid-solar-power-to-rural-africa/#4ca459082dbf
7. https://www.gsma.com/mobileeconomy/
8. GSMA Intelligence Mobile Penetration (unique subscribers as a percentage of the total population) Q3 2007 and 2017, accessed on 20/10/2017
9. GSMA Intelligence Global Data, accessed 16/11/17.

ACCESS TO MOBILE SERVICES AND PROOF-OF-IDENTITY

The majority of markets with low mobile penetration are also characterised by low levels of registered populations, suggesting a direct relationship between people's ability to access a government-recognised proof-of-identity and the level of mobile penetration in that market.

Other key insights highlighted in this research report

- Only 11% (16) of 147 countries mandating prepaid SIM registration enable MNOs to validate their customers' identification credentials against a central Government database to facilitate the accuracy of the validation process;
- 7% (11) countries require MNOs to use biometric-authentication processes when registering their prepaid SIM customers;
- While Mobile Money services are available in 92 countries worldwide, an estimated[10] 530 million individuals across these countries are at risk of financial exclusion due to their inability to meet the identification / Know Your Customer (KYC) requirements for opening Mobile Money accounts in their own names.
- Globally, only 50% of countries mandating SIM registration have a Privacy and/or Data Protection framework in place – the same applies for 40% of all African countries. While other regulations and licence conditions may provide consumers with varying degrees of protection, the absence of comprehensive frameworks may lead to consumer calls for increased transparency on how personal data are used. Additionally, transparency to consumers about how their data is used is important for maintaining high levels of trust in digital and mobile ecosystems, and maintaining trust helps encourage adoption of mobile-enabled digital identity services.

10. Estimates based on analysis from World Bank's Identification for Development (ID4D) Dataset – see footnote 1

ACCESS TO MOBILE SERVICES AND PROOF-OF-IDENTITY

02

Introduction and context

In 2017 the number of unique mobile subscribers worldwide-surpassed 5 billion[11] with the total number of mobile connections rising to 7.8bn of which 5.9bn (76%) are based on prepaid (pay as you go) SIM cards. While in many countries – including the UK and USA – consumers are able to buy and activate prepaid SIM cards without any proof-of-Identity, this is not the case in 147 countries where governments currently require Mobile Network Operators (MNOs) to capture, store and/or validate customers' identification credentials before activating their SIM cards. 92% of all prepaid connections are based in countries where SIM registration is mandated. A small but an increasing number of governments are also now requiring MNOs to implement biometric-authentication processes before registering a customer's SIM card.

Beyond the ability to communicate, a mobile subscription can enable access to a number of life-enhancing services such as mHealth, mEducation, financial products – such as Mobile Money – and social protections. Despite the significant number of countries where proof-of-identity is mandatory to register a mobile SIM, many of them lack a comprehensive national identification system. In fact, an estimated 1.1 billion[12] people worldwide lack any legal (State-issued or recognised) identification, and this predominantly affects vulnerable groups in developing countries across Sub-Saharan Africa and South Asia but also Forcibly Displaced Persons (FDPs) including refugees.

FDPs often relocate within their own countries or to other countries without any form of legal identification as these may have been forgotten, lost, destroyed or stolen during their journey, while those who are fleeing persecution based on some aspect of their identity (e.g. nationality, religion, ethnic group, sexual orientation, membership of a particular social group or political affiliation etc.) may decide not to travel with documentation[13].

The United Nations has recognised the importance of addressing the 'identity gap' through its Sustainable Development Goal (SDG) 16 to 'provide legal identity for all, including birth registration, by 2030'[14]. At the World Economic Forum 2018 in Davos, leaders from government, business, international organizations (including the GSMA), civil society and the humanitarian community have called for greater multistakeholder cooperation on digital identity and announced their commitment to strengthen collective action[15] to pursue the opportunities that come with digital identities and ensure protection of rights in a sustainable and responsible manner.

As we continue advancing in the digital age, the ability to prove one's identity becomes ever more critical to gaining access to mobile connectivity and a range of mobile services. Individuals with no proof-of-identity therefore face a higher risk of social, digital and financial exclusion where SIM registration is mandatory.

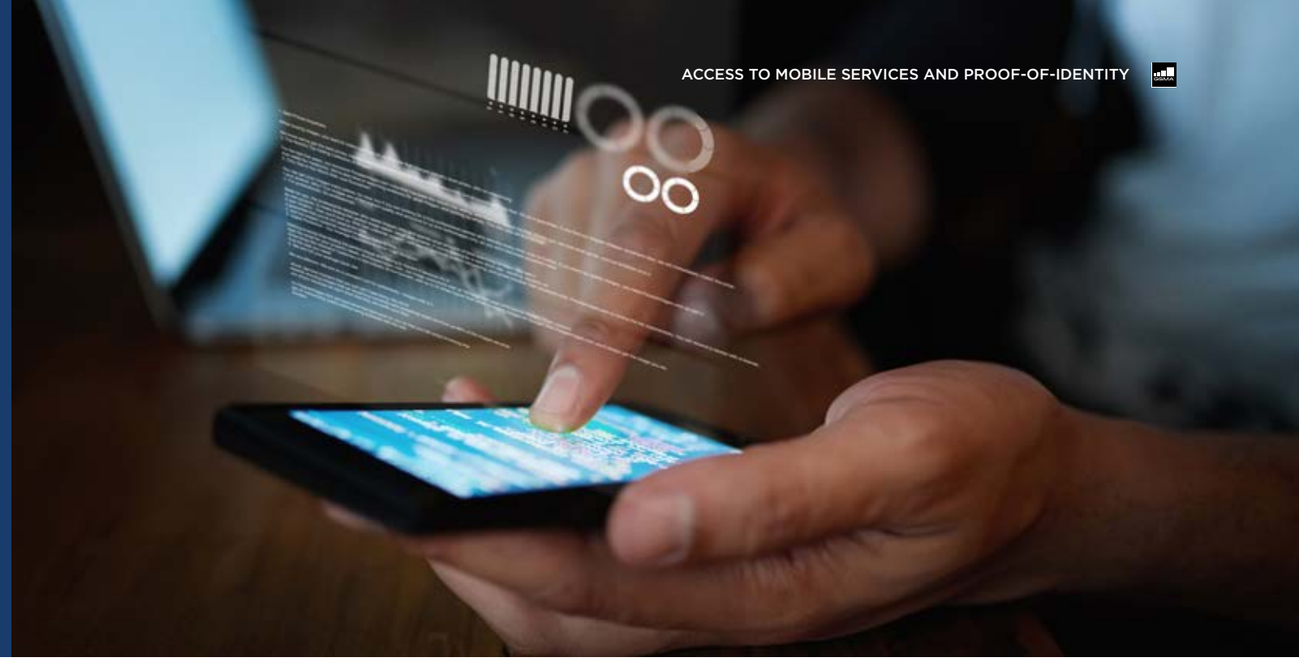
Any privacy concerns consumers may have could have an impact on their willingness to adopt or use identity-linked mobile services[16]. Countries embarking on their digital transformation journeys with inadequate privacy / data protection frameworks are therefore likely to face calls for stronger regulatory measures and policies that promote transparency on how personal data are used, and tools for consumers to make simple and meaningful choices about their privacy.

The mobile industry has worked to educate consumers and developed new features that have built trust in its services. Each new iteration of technology has introduced new features, such as encryption and user identification validation, which have made mobile services increasingly secure and minimised the potential for fraud, identity theft and many other possible threats[17]. Maintaining high levels of trust in digital and mobile ecosystems is important for consumers to remain engaged in – and actively adopt – mobile-based digital identity services.

11. https://www.gsma.com/newsroom/press-release/number-mobile-subscribers-worldwide
12. World Bank ID4D initiative: http://www.worldbank.org/en/programs/id4d
13. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Refugees-and-Identity.pdf
14. http://www.un.org/sustainabledevelopment/peace-justice/
15. https://www.weforum.org/press/2018/01/digital-identity-why-it-matters-and-why-it-s-important-we-get-it-right/
16. https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf
17. Ibid

03

Research hypotheses, methodology and data limitations



ACCESS TO MOBILE SERVICES AND PROOF-OF-IDENTITY

This research report aims to offer a global overview and identify trends between mandatory SIM registration policies, the official identification coverage and the level of mobile penetration across different markets. It builds on the GSMA's two earlier reports[18] which highlighted challenges, insights and best practices from several countries mandating SIM registration as well as recommendations for policymakers who are considering mandating or updating such policies.

The report also seeks to draw inferences on possible consumer risks – for example, privacy risks in countries where SIM registration is mandated but no privacy framework exists, as well as the risk of financial exclusion where consumers lack the required proof-of-identity to meet Know-Your-Customer (KYC) compliance rules even in countries where Mobile Money services are offered.

Depending on each country's context, a mandatory SIM registration policy can have a significantly positive or negative impact on people's lives and the local economy. For example, the ability of consumers to register for a mobile subscription in their own names, could unlock access to a plethora of mobile-enabled services, where the identification and authentication of the user is essential – such as Mobile Money[19] accounts, Pay-as-you-go Utility services[20], educational and health services and other digital identity services.

For the purposes of this report, the two most significant contextual factors contributing to the effectiveness of a country's mandatory SIM registration policy are:

(a) Individuals' ability to access a government-recognised proof-of-identity to meet the registration requirements: Where a large proportion of a country's population lacks official identification, it is assumed that the risk of exclusion from mobile access is higher. This is because the strict enforcement of SIM registration rules is likely to prevent vulnerable people (including forcibly displaced persons[21] who cannot meet the identification requirements) from accessing mobile services registered in their own names;

(b) Mobile operators' ability to validate (existing or new) customers' identification credentials at the point of registration: A SIM registration exercise is considered more robust where mobile operators are empowered to validate their customers' identification credentials against a central Government database or using other approved means to do so, including smartcards (see Section 7). Such validation capabilities are likely to add confidence to the process and mitigate the incidence of fraud. However, this has to be balanced against the risk of data misuse and mobile users' rights and legitimate expectations, for example in the context of privacy and data protection (See section 8).

Building on these assumptions, a key objective of this report has been to understand and analyse the possible linkages between access to official identification and mobile penetration, where proof-of-identity is mandatory for registering a SIM card in a subscriber's name. This involved extensive research to ascertain as much factual information as possible from various sources, while acknowledging that data from some countries' publicly available databases may not have necessarily been up to date.

18. Mandatory registration of prepaid SIM cards - https://www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards
19. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2016.pdf
20. https://www.forbes.com/sites/tobyshapshak/2016/01/28/how-kenyas-m-kopa-brings-prepaid-solar-power-to-rural-africa

21. GSMA report: 'Enabling Access to Mobile Services for the Forcibly Displaced' -https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/09/Policy-Note-FDPs-and-Mobile-Access.pdf

For example, the data on identification coverage has been derived exclusively from the World Bank's Identification for Development (ID4D) 2017 dataset, which, as the World Bank explains[22], was put together with a number of caveats in mind: (a) The estimated number of 'registered individuals' is taken as a proxy for the number of people with an official identification in each country, and the figures are generally based on data reported in the public domain by national authorities and some of which may date back several years. (b) Voter registration coverage data is used as a proxy indicator for national ID coverage of adults in 163 economies because actual national ID coverage data from national ID agencies or national statistics offices are not available. The use of voter registration coverage data excludes persons who choose not to or are unable to register to vote (e.g. non-nationals). Additionally, in countries where the number of registered voters exceeds the estimated number of people of voting age, the latter is used instead of the former. (c) Birth registration rates (from UNICEF) are used to estimate the number of children under the legal age for obtaining a national ID or registering as a voter. (d) Finally, the total number of the registered population is a dynamic number, which changes daily, and thus an exact measure is not possible.

Data on mobile penetration was sourced from the GSMA intelligence[23] database, based on the latest figures reported by Mobile Network Operators at the time of conducting the research.

Data on the existence of privacy and/or data protection frameworks across the world was predominantly sourced from databases maintained by the United Nations[24] and DLA Piper[25] but excludes any references to other legal protections a country's consumers may have, for example through multinational treaties or licence conditions. At the time of writing, 22 countries were considering introducing or revising such policies – these are outlined in Annex 10.

Finally, the status of mandatory SIM registration policies worldwide was based on a combination of desk research from publicly available sources and feedback from GSMA members. At the time of writing, 8 countries were considering the introduction of mandatory prepaid SIM registration policies – these are outlined in Annex 2.

22. See: https://data.worldbank.org/data-catalog/id4d-dataset
23. https://www.gsmaintelligence.com/
24. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
25. https://www.dlapiperdataprotection.com/index.html

04

A glance at mobile penetration over the last decade

Over the last decade, mobile penetration has increased exponentially – both in terms of absolute numbers (unique mobile subscribers) but also in terms of mobile connections as a proportion of the total population. (See Figures 4.1, 4.2, 4.3 and 4.4)

On average, mobile penetration (as a percentage of the total population) worldwide has nearly doubled over the last ten years from 60% to 113%[26]. As of 2017, one hundred and twenty countries maintain mobile penetration over 100% as the total number of mobile connections exceeds the total population of these countries.

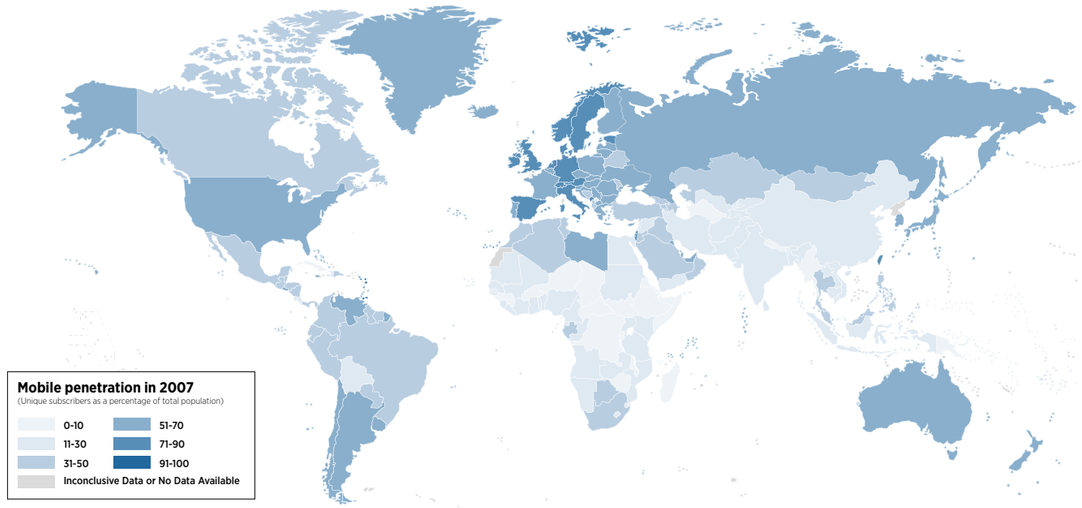
In terms of unique subscribers, mobile penetration worldwide has increased over the last ten years from 39% to 66%[27]. In 2016 alone, the number of global unique subscribers grew by 5%[28]. Yet, a number of emerging markets – particularly across the African continent – are still lagging behind the rest of the world with less than 50% of the population having a unique mobile subscription.

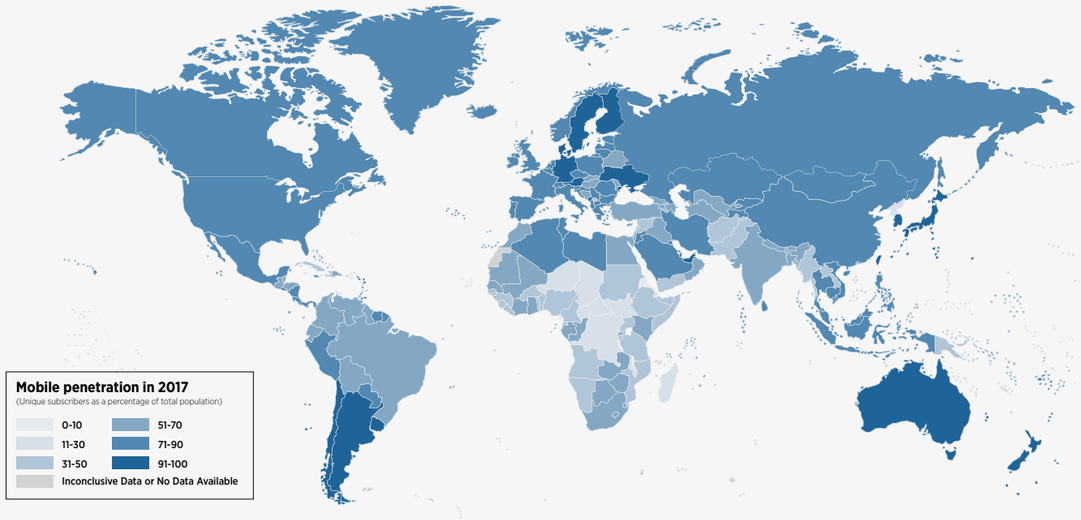
26. GSMA Intelligence: Mobile Penetration (as a percentage of the total population) Q3 2007 and 2017, accessed on 20/10/2017
27. GSMA Intelligence Mobile Penetration (unique subscribers as a percentage of the total population) Q3 2007 and 2017, accessed on 20/10/2017
28. GSMA Intelligence Global Data, accessed 16/11/17.

Figure 4.1 and 4.2

Mobile Penetration in 2007 and 2017 (Unique Subscribers)

Unique Mobile Subscribers as a Proportion of Total Population



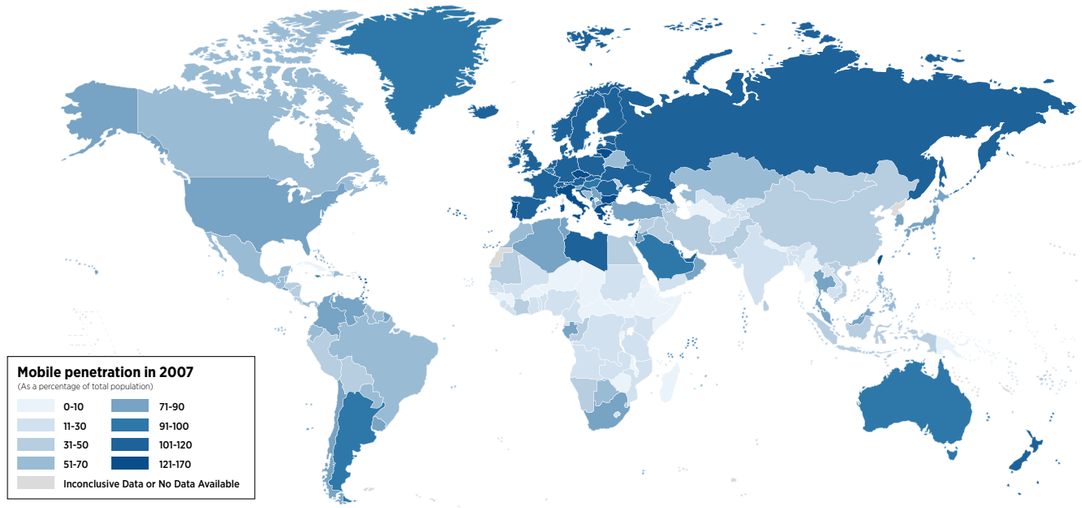


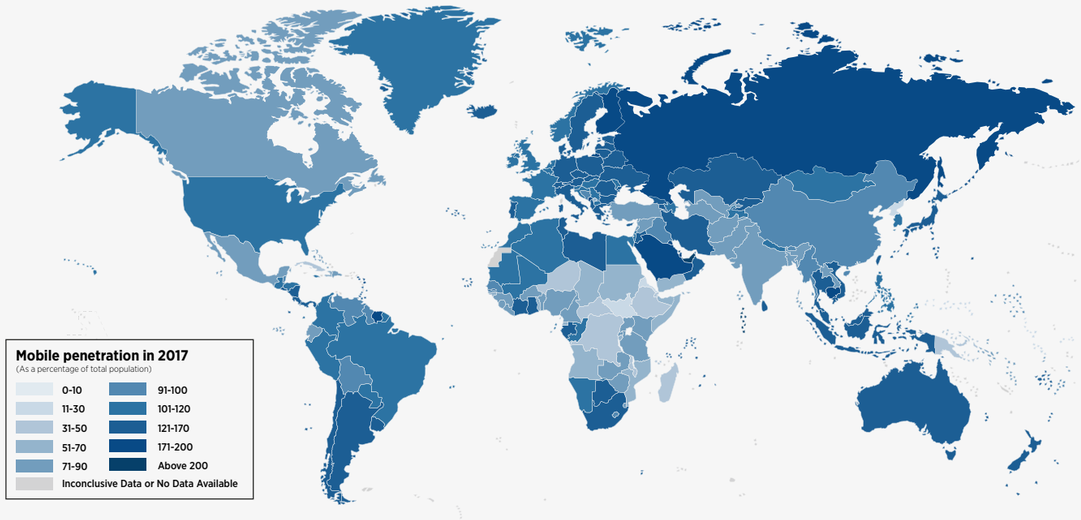
Source: GSMAi (Q3 2007 and Q3 2017) – figures accessed: October 2017

Figure 4.3 and 4.4

Mobile Penetration in 2007 and 2017 (Total Connections)

Aggregate Mobile Connections as a Proportion of Total Population





Source: GSMAi (Q3 2007 and Q3 2017) – figures accessed: October 2017

The majority of mobile subscriptions worldwide are prepaid (pay as you go)

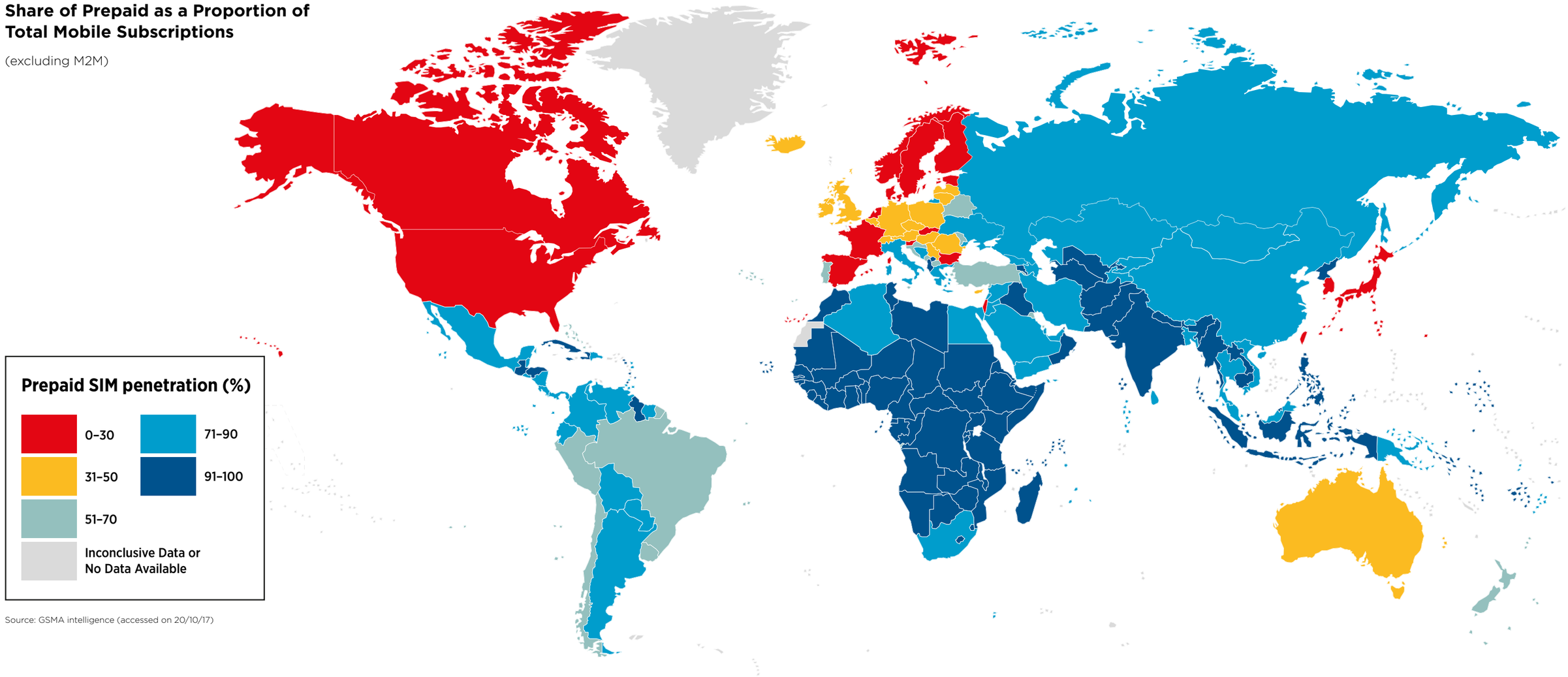
As Figure 4.5 below shows, an overwhelming majority of mobile SIM cards are based on prepaid (pay as you go) subscriptions - particularly across the developing world where consumers tend to be less able to meet the creditworthiness requirements associated with contract (pay monthly) subscriptions, or sign up to fixed term 'lock in' periods. Instead, these individuals prefer the flexibility to switch more easily between competing mobile networks. The average share of mobile subscriptions (excluding M2M) that are prepaid across Africa is 95%, followed by Central America at 86%, Asia at 82%, South America at 72%; Europe at 52% and North America at 22%.

ACCESS TO MOBILE SERVICES AND PROOF-OF-IDENTITY

Figure 4.5

Share of Prepaid as a Proportion of Total Mobile Subscriptions

(excluding M2M)



Source: GSMA intelligence (accessed on 20/10/17)

05

Examining the link between access to identification and access to mobile

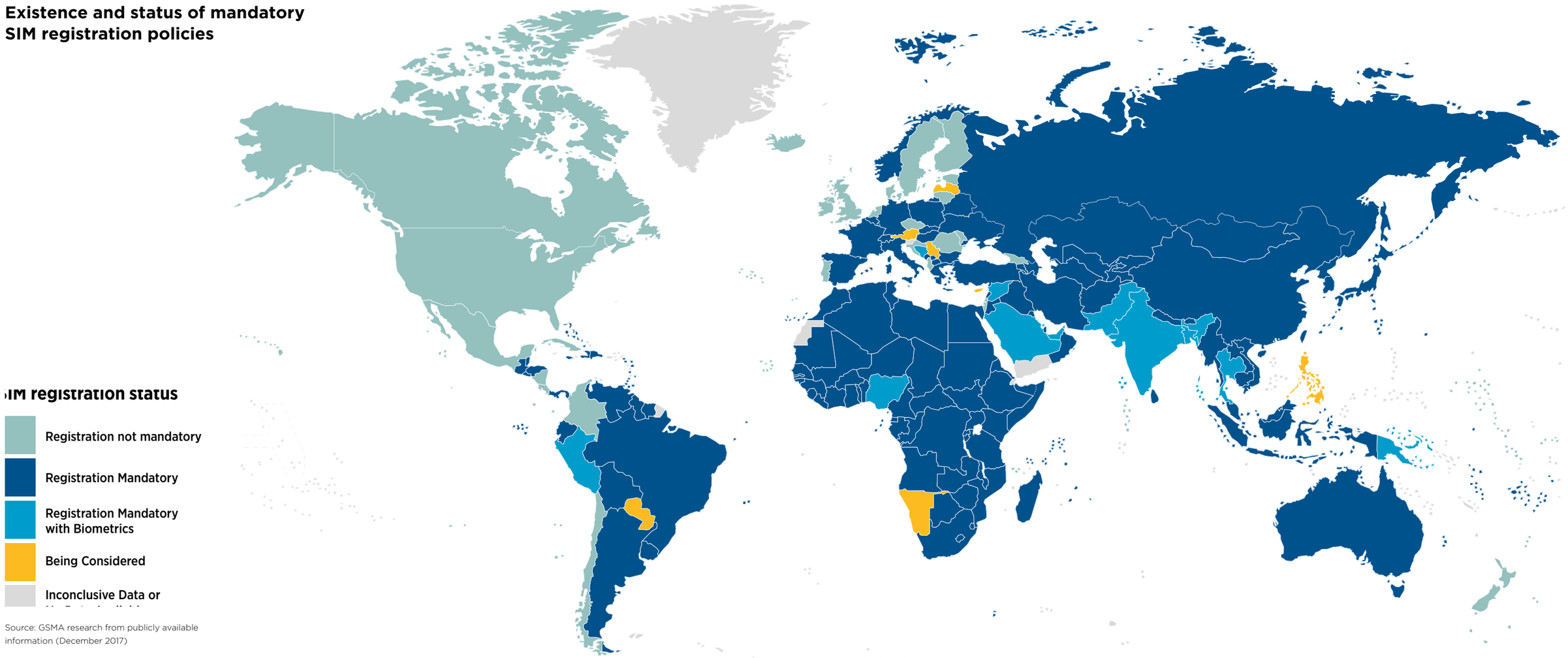
Most countries now require proof-of-ID for prepaid SIM card registration

The GSMA found that mobile users in at least 147 countries are required to prove their identity in order to register and/or activate their prepaid SIM cards; Only 16[29] of these countries (11%) enable MNOs to validate their customers' identification credentials against a central Government database and 11 (7%) require MNOs to use biometric-authentication processes when registering their prepaid SIM customers;

A number of governments adopt this policy primarily as part of efforts to help mitigate security concerns and to address criminal and anti-social behaviour. To date, there has been no empirical evidence that a mandatory SIM registration policy directly leads to a reduction in crime but governments perceive the process as a deterrent to the use of mobile platforms in supporting criminal activity.[30]

Figure 5.1

Existence and status of mandatory SIM registration policies



Source: GSMA research from publicly available information (December 2017)

29. See Annex 8
30. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

ACCESS TO MOBILE SERVICES AND PROOF-OF-IDENTITY

Access to a government-recognised proof-of-identity

The World Bank estimates that 1.1bn people across the globe lacked official identification in 2017. The overwhelming majority of these people are in developing countries across Africa and Asia where proof-of-identity is required to register a mobile SIM card and/or to open a Mobile Money account.

Figure 5.2 provides a global snapshot showing the proportion of each country's total population that is registered (based on the World Bank's 2017 ID4D dataset which, in the absence of data on national ID coverage, primarily reflects the latest data on voter registration as a proxy for official identification)[31].

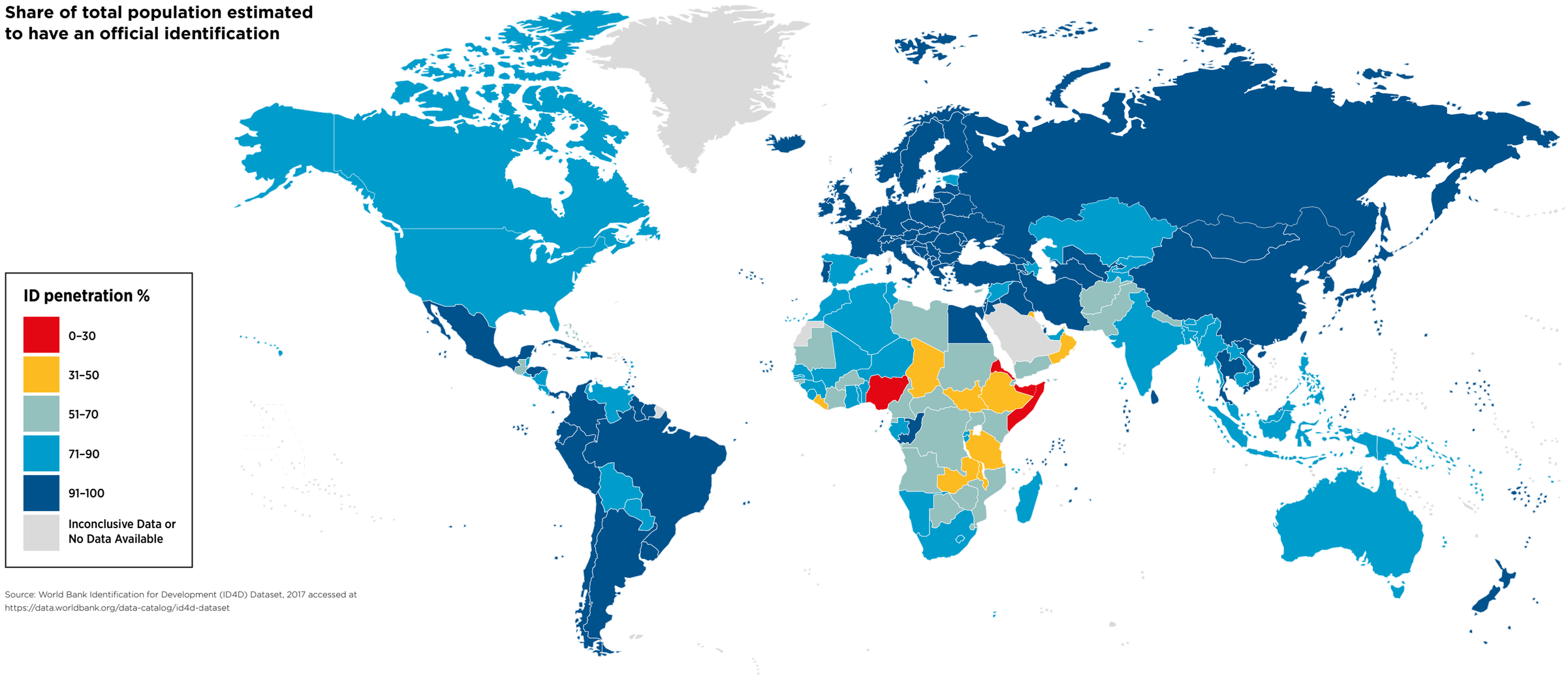
31. As the World Bank explains in its ID4D dataset, ' a number of caveats about these estimates should be kept in mind. First they are generally based on data reported in the public domain by national authorities and some of which may date back several years. Second, voter registration coverage data is used as a proxy indicator for national ID coverage of adults in 163 economies because actual national ID coverage data from national ID agencies or national statistics offices are not available. The use of voter registration coverage data excludes persons who choose not to or are unable to register to vote (e.g. non-nationals). Additionally, in countries where the number of registered voters exceeds the estimated number of people of voting age, the latter is used instead of the former. Finally, the total number of the registered population is a dynamic number which changes daily and thus an exact measure is not possible'. See: https://data.worldbank.org/data-catalog/id4d-dataset

As many of these countries with low ID coverage work to implement national digital transformation strategies, they are faced with policy decisions regarding spectrum harmonisation, rural connectivity, job creation and digital skills. Beyond addressing these objectives, having an enabling policy environment to facilitate access to identification is likely to be a key determinant to the success and inclusivity of a Government's digital transformation strategy (see Section 9).

In view of this, and despite the caveats around the data sources supporting Figure 5.2, there is a strong indication that individuals across the African continent are more likely to lack official identification compared to the rest of the world and arguably face a higher risk of digital, social and financial exclusion.

Figure 5.2

Share of total population estimated to have an official identification



Source: World Bank Identification for Development (ID4D) Dataset, 2017 accessed at https://data.worldbank.org/data-catalog/id4d-dataset

A closer look at Africa: Linkages between access to identification and access to mobile

Figure 5.3 illustrates the relationship between the official identification coverage (based on World Bank figures as explained above) and mobile penetration, across African countries where SIM registration is mandated. Mobile penetration is illustrated both in terms of aggregate subscriptions as well as in terms of unique mobile subscriptions as a proportion of each country's total population.

For the majority of African markets there seems to be some association between official identification and mobile penetration. Furthermore, in seven markets (Somalia, Nigeria, Zambia, Botswana, Zimbabwe, Mauritania and Libya), it appears that more people have a mobile subscription than an official proof-of-identity. This may suggest a number of inferences, for example that:

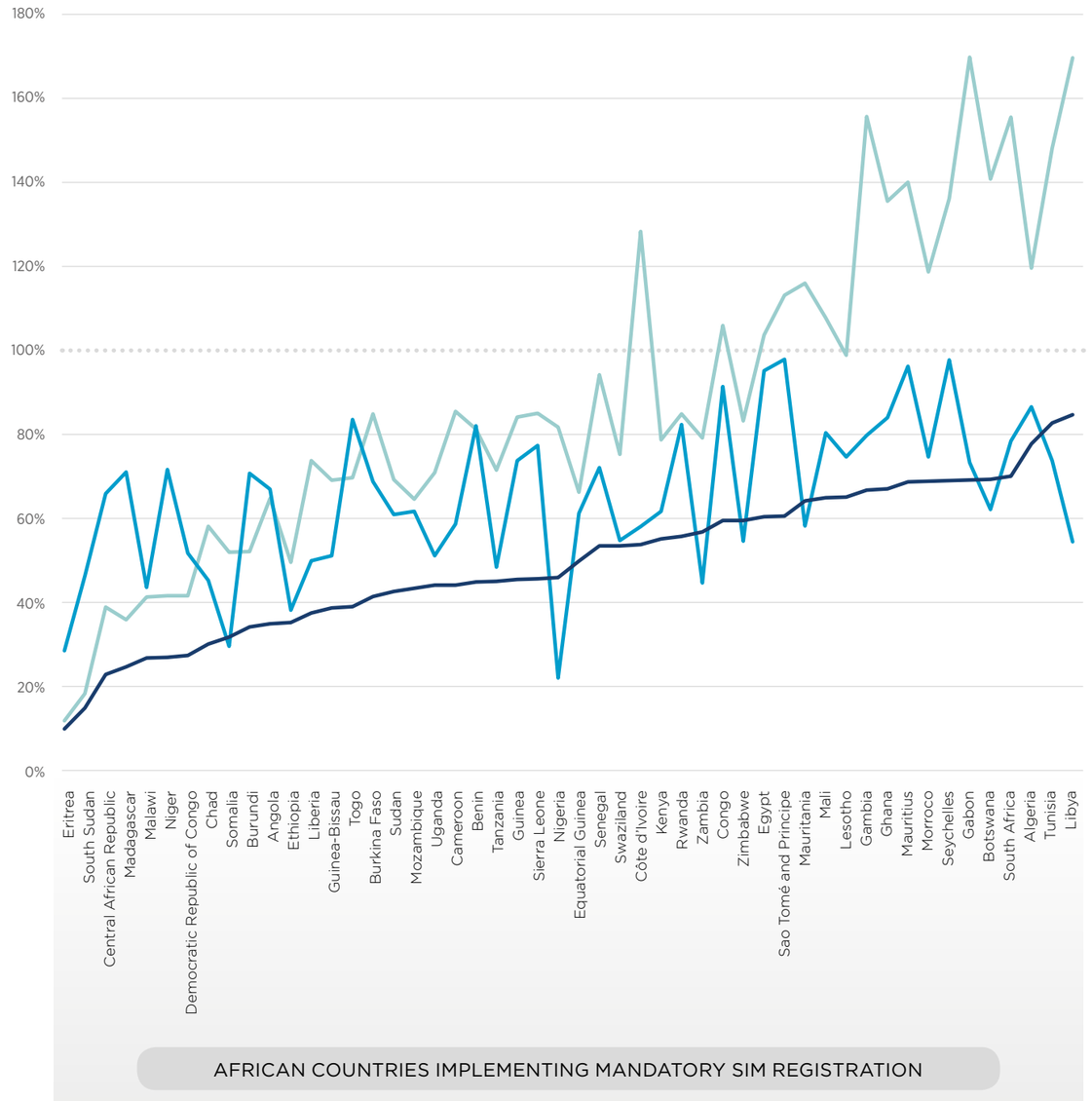
- in countries with low ID coverage and high mobile penetration, it is possible that people may have relied on someone else (e.g. agent, friend, family-member) to procure or register a SIM card on their behalf;
- the identification coverage figures may be understated or that the publicly available information has not been recently updated;
- the acceptable proof-of-identity credentials for SIM registration may include documents not necessarily issued by the Government (such as a letter from the village ward vouching for someone's identity), thus making it easier for someone without a recognized proof-of-identity to register for a SIM card;
- a larger number of existing mobile users may risk having their mobile SIM cards deactivated if the governments were to enforce stricter proof-of-identity requirements;

This presents an opportunity for governments to work with mobile operators to expand ID coverage, for example through the use of mobile networks and/or agents to facilitate registration or information sharing.

Figure 5.3

Identification coverage and mobile penetration across African countries where mobile SIM registration is mandatory

Percentage of population



Source: GSMA Intelligence, Market Penetration - Q3 2017 (Accessed October 2017) and The World Bank, ID4D 2017 (number of registered individuals as a % of the population, taken as a proxy for identity penetration)

06

Implications for Digital and Financial exclusion

For millions of people in developing markets where mobile infrastructure has leapfrogged 'bricks and mortar' services, mobile is not just their only means of communicating with relatives and accessing the internet, but also the only means of accessing financial services – through Mobile Money.

Currently, Mobile Money services are offered in 92 countries worldwide[32]. Sub-Saharan Africa has been a major driver of this success[33], playing host to almost half of all Mobile Money deployments worldwide, as well as almost half of all countries where Mobile Money is available.

A few key findings from the GSMA's latest State of the Industry Report[34] include:

- 30 Mobile Money markets had 10 times more active agents than bank branches
- More than 40% of the adult population in 8 countries (7 of which are in Sub-Saharan Africa) are using Mobile Money on an active basis.
- At the end of 2016, there were over 277 million registered Mobile Money accounts in Sub-Saharan Africa – easily surpassing the number of bank accounts in the region (estimated at around 100 million)[35] and contributing to increased financial inclusion in the process.
- The improvement in financial inclusion across Sub-Saharan Africa has reduced inequality, particularly in line with 11 of the UN's 17 Sustainable Development Goals (SDGs), including those focused on alleviating poverty (SDG 1), decent work and economic growth (SDG 8), and reducing inequality within countries (SDG 10).

32. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2016.pdf
33. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/07/2016-The-State-of-Mobile-Money-in-Sub-Saharan-Africa.pdf
34. Ibid

To open a Mobile Money account, consumers need to provide proof-of-identity as all Financial Service Providers (FSPs) – including Mobile Money operators – have to comply with Know-Your-Customer (KYC) requirements and follow best practice. This is necessary both to ensure the commercial reliability of the financial services as well as to comply with financial regulators' rules on KYC, particularly for the purposes of anti-money laundering (AML) and counter financing of terrorism (CFT) policies. KYC identification requirements for financial services (usually imposed by Central Banks and Finance ministries) are often additional to those for SIM registration, which are usually imposed by Telecoms Regulators[36].

The proof-of-identity requirements for both SIM registration and KYC contexts raise a 'flip side' concern, that they actually deny segments of the population access to basic mobile communications and Mobile Money services if they lack a form of acceptable identification. Such vulnerable groups therefore face a dual risk of being both digitally and financially excluded – even in countries where Mobile Money services are available.

Each country has a different age limit above which an individual is eligible to obtain national identification. The legal age ranges from birth to when someone turns 18 years old. Similarly, individuals generally need to turn 18 years old to open a bank or Mobile Money account upon meeting the KYC identification requirements.

While undoubtedly the lack of identification has an impact on the overall digital and financial exclusion of vulnerable groups (due to proof-of-identity being an access requirement as explained above), there is insufficient evidence to quantify the exact level of impact. However, Figure 6.1 illustrates the proportion of the population that is eligible to access official identification (i.e. those above the legal age limit - predominantly adults - in each country) across the 92 countries where Mobile Money services are available.

The GSMA estimates[37] that around 530m individuals across these 92 countries are unregistered and therefore unlikely to meet the KYC requirements for opening Mobile Money accounts in their own names. Put differently, these individuals would have been able to be financially included in their own right by accessing Mobile Money services in these countries but might be unable to do so due to lack of identification. This estimate does not take into account any network coverage issues and is based on the assumption that all individuals in these countries have access to Mobile Money agents.

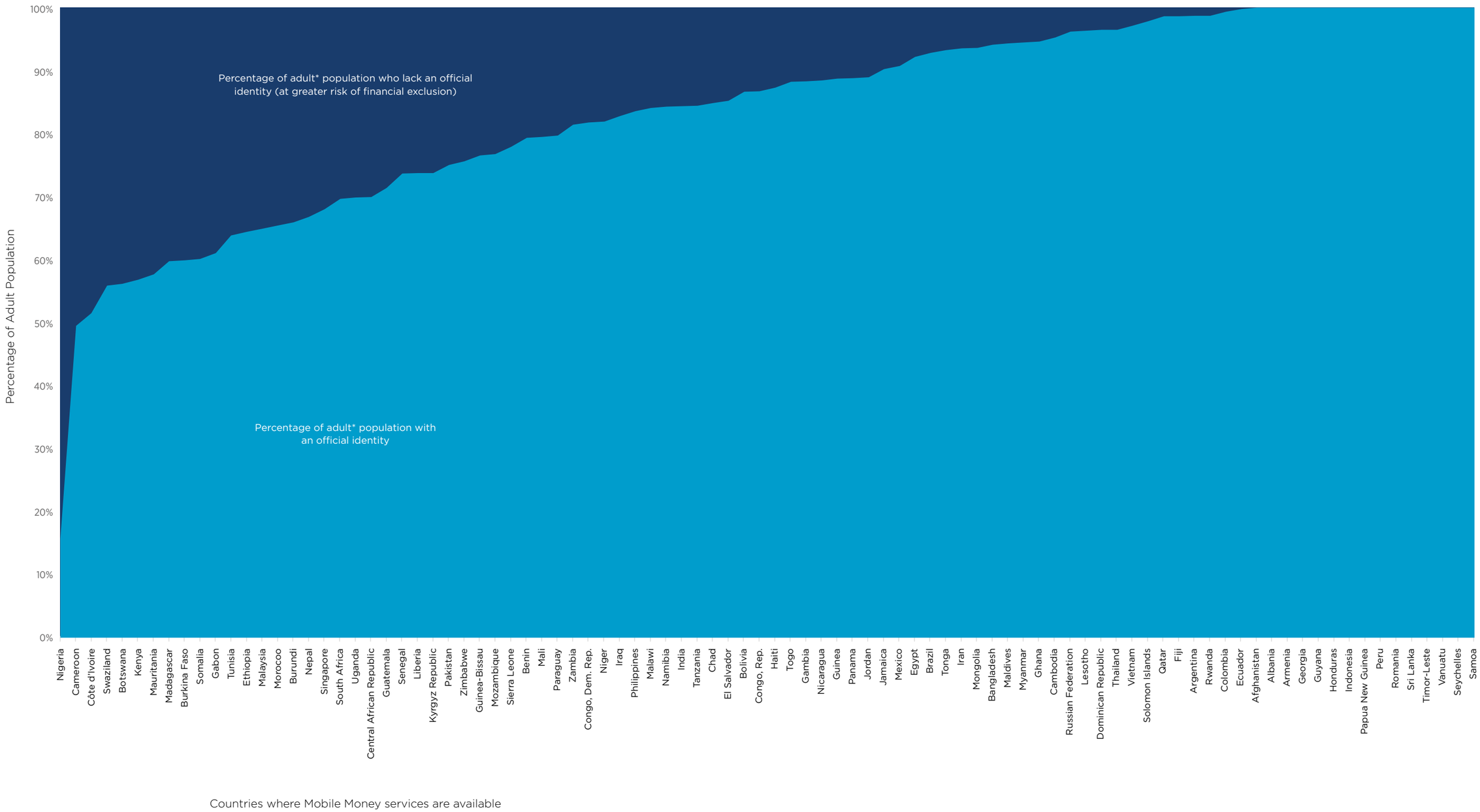
35. https://www.afdb.org/fileadmin/uploads/afdb/Documents/Knowledge/AEB_Vol_6_Issue_5_2015_The_Banking_System_in_Africa__Main_Facts_and_Challenges-10_2015.pdf
36. GSMA: 'Regulatory and policy trends impacting Digital Identity and the role of mobile' - https://www.gsma.com/mobilefordevelopment/programme/digital-identity/digital-identity-regulatory-trends-and-the-role-of-mobile
37. *The World Bank ID4D's dataset for 'registered people above the legal ID age' is used as a proxy for the number of adults with an official identity in each country though the GSMA recognises that countries' policies over the mandatory age of registration vary – usually ranging from Birth to the age of 18.

ACCESS TO MOBILE SERVICES AND PROOF-OF-IDENTITY

Figure 6.1

Identification coverage among eligible[38] population, in countries where Mobile Money services are offered

Source: The World Bank ID4D 2017 and GSMA



38. Ibid

The Case of Refugee Populations

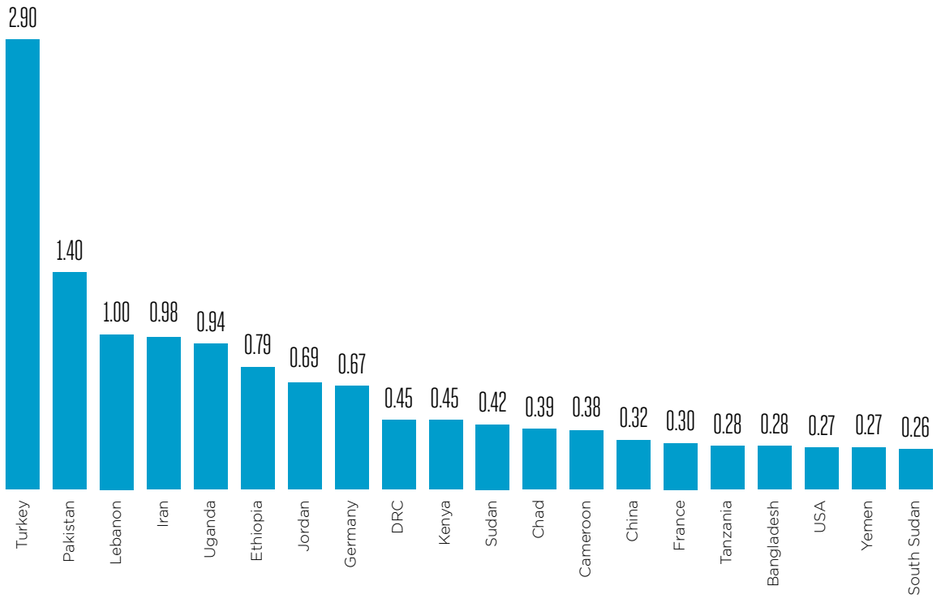
The risks outlined above are exacerbated for forcibly displaced persons (FDPs)[39]. The United Nations High Commissioner for Refugees (UNHCR) estimates that, as of 2017, more than 65 million people are forcibly displaced worldwide[40], many of who have been forcibly displaced for over two decades[41]. An additional 25.4 million people are displaced every year due to natural disasters and climate-related events[42]. FDPs often relocate within their own countries or to other countries without any form of legal identification as these may have been forgotten, lost, destroyed or stolen during their journey, while those who are fleeing persecution based on some aspect of their identity (e.g. nationality, religion, ethnic group, sexual orientation, membership of a particular social group or political affiliation etc.) may decide not to travel with documentation[43].

In 2017, the UNHCR estimated 22.5 million people across the world maintain refugee status – 17.2 million of these fall under their mandate[44]. GSMA research found that all but one of the top twenty refugee-hosting countries (see Figure 6.2) have mandatory SIM registration policies in place[45] in addition to KYC identification compliance requirements for opening Mobile Money accounts. To the extent that refugees are unable – at least in the short term – to meet these requirements, they risk being excluded from accessing both mobile communication and Mobile Money Services.

Figure 6.2

Top 20 Refugee-Hosting Nations

Refugee population (in millions)



Source: Data extracted from UNHCR Global Trends Report 2016[46]

39. For the purposes of this report, the term 'FDPs' includes refugees, internally displaced persons (IDPs) e.g. those fleeing a war zone and/or relocating in the aftermath of a natural disaster, asylum seekers and other persons who have had to leave their homes as a result of a natural, technological or deliberate event. (Definition adapted from http://iasfm.org/)
40. UNHCR: http://www.unhcr.org/uk/figures-at-a-glance.html
41. UNHCR: Global Trends, http://www.unhcr.org/576408cd7.pdf
42. CGAP/World Bank report: The role of financial services in humanitarian crises - http://www.cgap.org/publications/role-financial-services-humanitarian-crises
43. GSMA report: Refugees and Identity: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Refugees-and-Identity.pdf
44. UNHCR. http://www.unhcr.org/globaltrends2016/
45. GSMA report: Mobile Money, Humanitarian Cash Transfers and Displaced Populations': https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/05/Mobile_Money_Humanitarian_Cash_Transfers.pdf
46. Global Trends: Forced Displacement in 2016. UNHCR, 2017. http://www.unhcr.org/5943e8a34.pdf

Recent GSMA reports[47] highlighted that enabling access to mobile services can lead to positive outcomes not just for refugees themselves, but also for humanitarian agencies[48], host governments and local communities.

Where refugees are able to open Mobile Money accounts in their own names, humanitarian aid organisations are able to reach beneficiaries directly, improving transparency, expediency and operational efficiency of their funds' disbursement process. However, this approach by itself may not always be helpful in the case of FDPs who have not been able to obtain UN-issued Identity documentation – which can include internally displaced persons – or those who choose not to officially register with the Government authorities if they fear deportation or detention.

Interestingly, the identification / KYC requirements imposed on refugees seeking to open a Mobile Money account[49] are sometimes stricter in some countries (such as Kenya), compared to those needed to open a Bank account or a third party money transfer service[50].

The GSMA has published policy recommendations[51] for host-country governments on how to address the identification barriers and enable FDPs to access mobile services. These are outlined below in figure 6.3.

Figure 6.3

Summary of Recommended Considerations for Policymakers on Enabling Mobile Access for Forcibly Displaced Persons (FDPs)

In an effort to promote an enabling policy and regulatory framework, host-country governments and regulators (including Central Banks) should consider adopting flexible and proportionate approaches towards proof-of-identity requirements for forcibly displaced persons to be able to access mobile services, particularly in emergency contexts. Such approaches may include:

1. Providing clear guidelines on what identification is acceptable for FDPs to access mobile services, and ensuring that a critical mass of FDPs has access to an acceptable proof-of-identity;
2. Allowing the use of UNHCR-issued identification, where available, to satisfy any mandatory SIM registration or 'Know Your Customers' (KYC) requirements for opening Mobile Money accounts;
3. Enabling lower, 'tiered' thresholds of KYC requirements to allow FDPs to open basic Mobile Money accounts, particularly in emergency contexts;
4. Harmonising identity-related SIM registration requirements with the lowest-tier of KYC requirements in countries where SIM registration is mandatory;
5. Establishing proportionate Risk Assessment processes that take into account the diverse types of FDPs when considering 'proof-of-identity' policies;
6. Exploring the use of new Digital Identity technologies;
7. Promoting robust identification-validation processes while adopting consistent data protection and privacy frameworks.

47. See GSMA report: 'Enabling FDPs access mobile services' - https://www.gsma.com/mobilefordevelopment/programme/digital-identity/enabling-forcibly-displaced-persons-access-mobile-services-addressing-identification-barriers
48. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/11/Humanitarian-Payment-Digitisation.pdf
49. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Refugees-and-Identity.pdf
50. https://newsroom.mastercard.com/wp-content/uploads/2017/06/Mastercard_Western-Union-Refugee-Settlement-Report-FINAL.pdf
51. https://www.gsma.com/mobilefordevelopment/programme/digital-identity/enabling-forcibly-displaced-persons-access-mobile-services-addressing-identification-barriers

Case Study A

Jordan

Identification and Mobile Access for Refugees in Jordan

Upon arrival to the Jordanian border, refugees are required to register with UNHCR and with the Jordanian Ministry of Interior (MoI) at the joint Raba Al Sarhan Registration Centre, which is located close to the border. For refugees heading towards refugee camps, UNHCR issues a 'proof of registration' document[52], while refugees that are eligible to live outside of camps are provided with asylum certificates so they can receive humanitarian assistance and access additional services in the urban areas[53]. Regardless of whether they have registered with UNHCR as refugees, all Syrians living in Jordan are required to register with the MOI and receive Ministry of Interior Service card ("MoI card"), which is valid only if the Syrian remains living in the district where the card was issued[54]. Upon registration with the MOI, the refugees are given a unique serial number by the MOI and the card issued also shows UNHCR's unique identifier. The MOI card enables refugees to register for a SIM card and open a Mobile Money account, at the service providers' discretion.

In 2015, the Jordanian government introduced new biometric MoI cards for all Syrians. To receive it Syrian refugees living in the urban must present their identification, asylum seeker's certificate, health certificate and proof of address at their local police stations. The new biometric MoI cards are nationally-recognised identification cards, and permit refugees to travel freely throughout Jordan, apply for work permits and access public services within the district of issuance[55].

52. *Securing State: Syrian refugees and the documentation of legal status, identity, and family relationships in Jordan.* NRC, November 2016. https://www.nrc.no/globalassets/pdf/reports/securing-status.pdf
53. Ibid.
54. Ibid
55. *Securing State: Syrian refugees and the documentation of legal status, identity, and family relationships in Jordan.* NRC, November 2016. https://www.nrc.no/globalassets/pdf/reports/securing-status.pdf

07

Variations of 'proof-of-identity' requirements on Mobile Operators

While the main objective governments cite when implementing SIM registration policies is to be able to link a mobile SIM card to a real individual, each government approaches proof-of-identity differently. The variations tend to focus around the types of identification credentials that consumers can provide as well as on the actions mobile operators are required to take with their customers' data during the SIM registration process.

Mobile operators' ability to validate (existing or new) customers' identification credentials at the point of registration

While all mandatory SIM registration policies require MNOs to capture customers' personal information and recognised identification credentials, only a minority of governments[56] enable MNOs to validate those credentials (whether paper-based or biometric) against a central Government database in real time, at the point of registration. Such validation capabilities do not tend to involve giving MNOs access to customers' personally identifiable information that the Government holds in those databases. Instead, they allow MNOs to query a customer's identification credential against the database, and in turn the relevant authority confirms whether the credential matches the one stored in their own database.

In the majority of countries where Mobile SIM registration is enforced – and usually as part of complying with their license conditions or local laws – MNOs must relay data about specific customers at the government's request. However, in a few countries, (such as Italy[57], Nigeria[58] and Kenya[59]) MNOs are required to share their customers' registration details with the government on a proactive basis rather than upon a formal access request or a warrant for national security reasons etc.

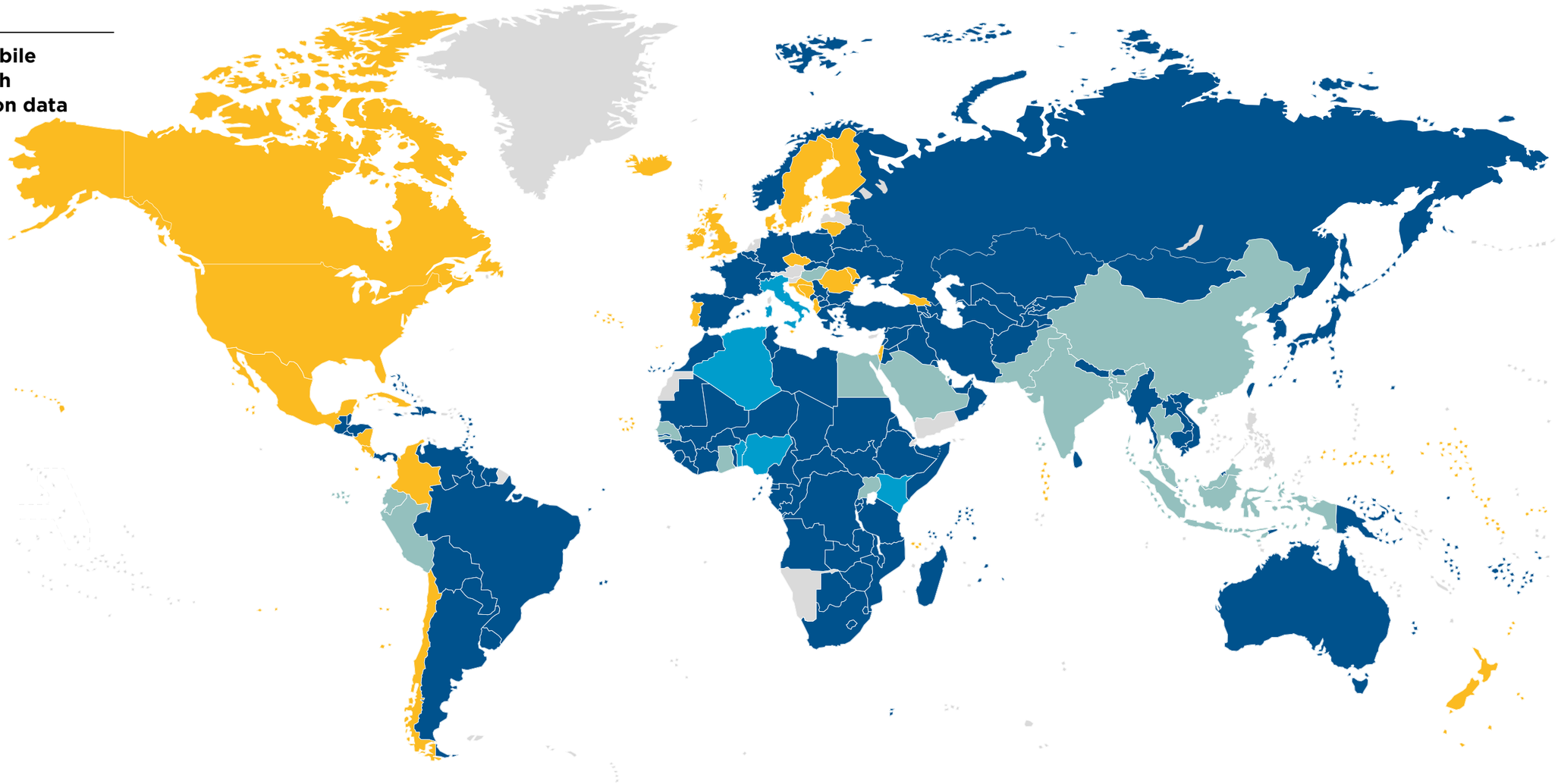
56. See Annex 9
57. Decreto Legislativo 1 agosto 2003, n. 259 http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259!vig=
58. *Registration of Telephone Subscribers Regulation.* Nigerian Communications Commission, 2011. https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file
59. The Kenya Information and Communications (Registration of SIM cards) Regulation 2015: http://ca.go.ke/images//downloads/sector_regulations/Registration%20of%20SIM%20%E2%80%93Cards%20Regulations,%202015.pdf

Figure 7.1 below illustrates how the requirements imposed on MNOs differ[60] across the 147 countries where prepaid SIM registration is mandatory. For the purposes of this report the requirements were grouped into 3 categories:

- **Capture and Store:** (85% of the countries mandating SIM registration) – MNOs required to copy or otherwise keep a record of the required identification credentials which may include: a passport, national identity card, driver's licence, voter's registration card etc;
- **Capture and Share** (4% of the countries mandating SIM registration) – In addition to capturing and storing copies of their customers' identification credentials, MNOs in this category are required to share their customers' full or partial registration profiles with the Government proactively rather than upon demand; This may arguably raise privacy concerns particularly in countries with no or limited privacy and data protection frameworks (see chapter 8);
- **Capture, validate and store** (11% of the countries mandating SIM registration) – Before storing their customers' identification credentials MNOs are required to validate the document presented and/or biometric details of the customer, usually by querying a central government database. In many cases, MNOs also face compulsory charges / fees based on the number of validations/queries they initiate over a given period. The validation process leads to either a successful or rejected registration.

Figure 7.1

Requirements on how mobile operators should deal with customers' SIM registration data



Source: GSMA Research - See Annex lists 6, 7, and 8 for the category breakdown

60. as of December 2017

Key Observations:

- MNOs are required to capture and store their customers' identification credentials in most countries where prepaid SIM registration is mandatory
- Nine of the 16 countries[61] where MNOs are required and empowered to validate customers' identification credentials are in Asia and the Middle East
- Most African countries implement SIM registration yet only four[62] require (and enable) MNOs to validate customers' identification credentials against a central government database. Given the comparatively low incidence of official identification across most African markets, the lack of validation capabilities suggests that mobile operators can mainly rely on the 'best efforts' of their agents and retailers to verify customers' identification credentials.

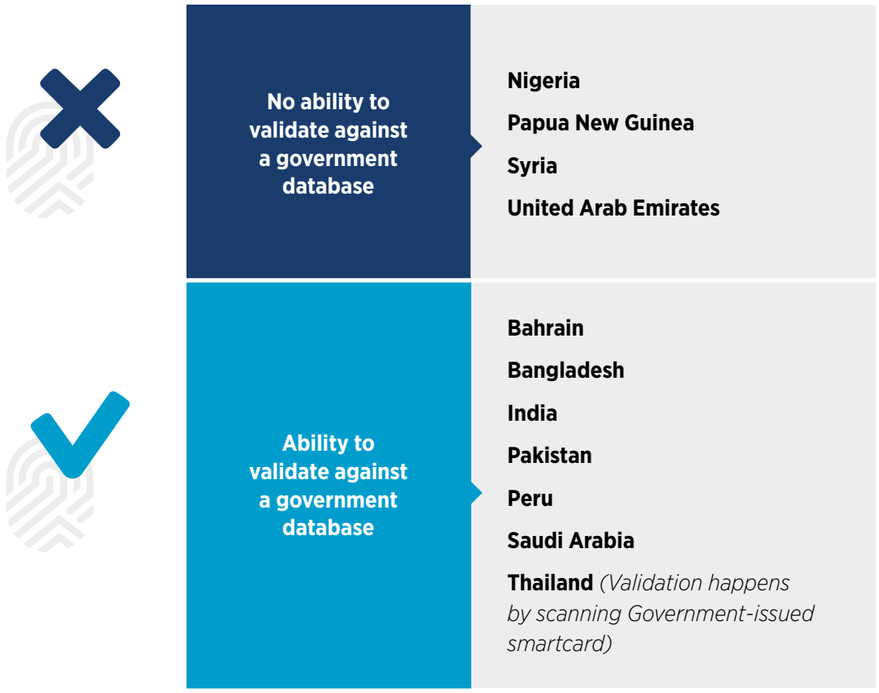
61. Bahrain, Bangladesh, China, India, Indonesia, Malaysia, Pakistan, Saudi Arabia and Thailand.
62. Egypt, Ghana, Senegal and Uganda.

Biometric SIM Registration

Technological advancements that improve uniqueness in the identification and authentication space have emerged in recent years, with an increasing number of governments implementing biometric processes to reduce duplication of entries, welfare program leakages and improve administrative efficiencies.

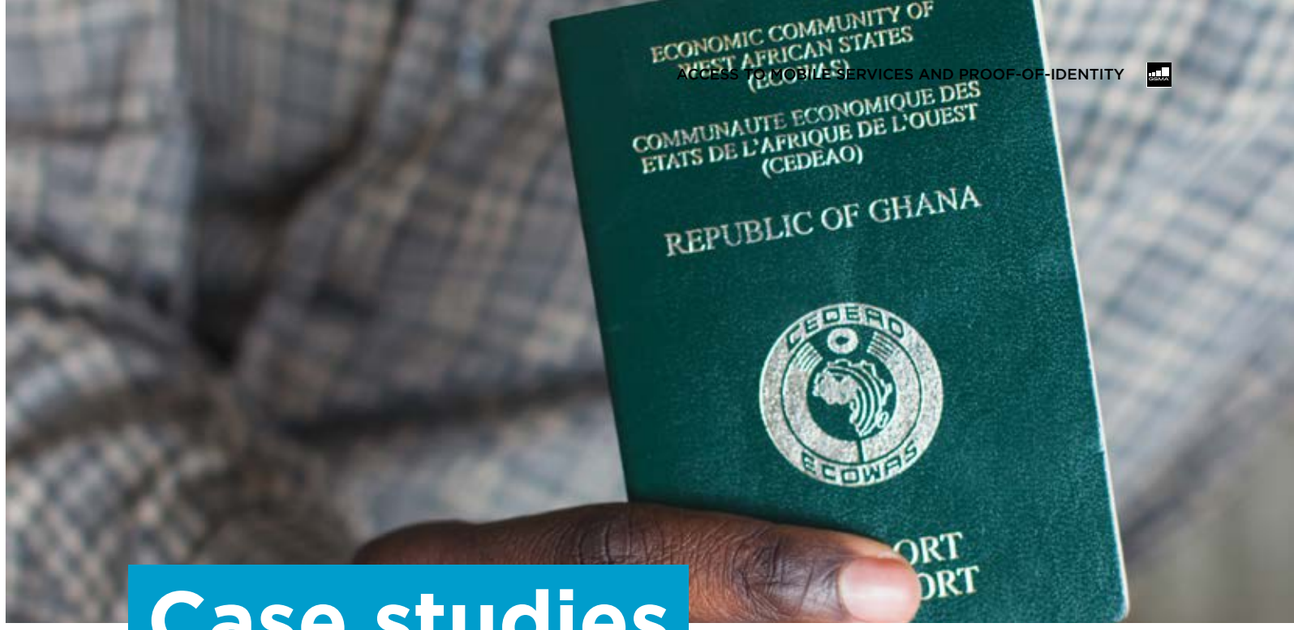
Figure 7.2

Countries where biometric SIM registration of SIM cards is mandatory



This trend towards biometric identification systems is also slowly expanding into the SIM registration context: As Figure 7.2 shows, 8% of governments (11 countries) enforcing SIM registration have made it mandatory to do so using biometrics – i.e. predominantly capturing customers' fingerprint templates and/or iris scans in in addition to (or instead of) paper-based identification.

However, only 7 of the 11 countries actually enable MNOs to validate their customers' biometric details against a government database (or a smartcard in Thailand's case) where the same details are stored.



Case studies

Case Study B

Brazil

Identification and SIM Registration – 'Capture & Store'

The Identification Context

The Justice Ministry began issuing the biometric identification cards in 2008[63], five years following the introduction of the SIM requirements. Using their identification cards, holders can obtain a driver's license, open a bank account and travel within Mercosur countries[64]. All citizens over the age of 18 are required to hold a formal state identification. 94% of Brazilians are registered with a form of national identification[65]. However, at the end of 2017, the President announced the government's intention to create a new identity document for Brazilians – a National Civil Identification (INC)[66]. Rather than maintaining separate systems, the government is planning to integrate citizen information from the General Registry, Electoral Registry and Individual Registry into the INC database. Yet, the National Driver's License (CHN) and Passport systems will be unaffected, and will continue to operate separately.

Identification for mobile access

SIM registration has been mandatory in Brazil since 2003[68] and all mobile users are required to show proof-of-identity in order to obtain a SIM card. According to the National Telecommunications Agency (ANATEL), Brazilians can use a range of documents, which include their Cedula de Identidade (the official identification card), driver's license, and taxpayer number, to complete SIM registration.

Mobile network operators must store the full name, address and identification number of each customer in a database. Despite the prevalence of biometric identification cards, MNOs cannot validate customers' biometric information for mobile SIM registration purposes.

63. http://www.identity-cards.net/record/brazil
64. https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Brazilian_Identity_Card.html
65. World Bank ID4D Dataset 2017, based on Brazil's Voter Registration database
66. *Temer sanciona lei que cria document de identifição.* Gustavo Aguiar. https://g1.globo.com/politica/noticia/temer-sanciona-lei-que-cria-documento-de-identificacao-unificado.ghtml
67. Ibid.
68. *Lei no 10.703, de julho de 2003.* ANTEL, July 2003. http://www.anatel.gov.br/legislacao/leis/469-lei-10703

Case Study C

Tanzania
SIM Registration – Capture & Store

The Identification Context
In 2012, the National Identification Authority (NIDA) began registering citizens for the country's new electronic national identification card. The Tanzanian ID card includes the fingerprints, photo and personal information such as the full name and date of birth of each cardholder. Tanzanians must be over the age of 18 to obtain a national identification card, and can do so free of charge.

Identification for mobile access
The Tanzanian Communications Regulatory Authority (TCRA) formally mandated SIM registration in Tanzania in 2010. Tanzanian mobile users must present one of five acceptable identification documents – their national ID card, passport, driver's license, Zanzibar ID or Voter Registration card – in order to register for a SIM card. The process has been predominantly paper-based and involved MNO agents manually recording customers' identification credentials. In 2016, the leading MNOs established an electronic registration system, which has been referred to as the Electronic Know Your Customer (e-KYC) process. This involves the use of a smartphone app by mobile agents to fill and submit an electronic registration form as well a digital photo of each customer as well as a digital copy of their identification document. MNOs manually review the provided user data before activating the SIM card electronically. Since 2016 the National Identification Authority (NIDA) has been improving the coverage and accuracy (by removing duplicate records) of its centralised national identification database and investing in technical capabilities so that MNOs (and other approved private sector entities) could query the database to validate their customers' identification credentials.

Concurrently, Tanzanian MNOs have been working collectively with a third party software solution provider, in coordination with NIDA and the TCRA, to create a harmonised e-KYC platform for seamlessly conducting customer registration while leveraging the real-time validation capability against NIDA's database.

Case Study D

Nigeria
Biometric SIM Registration – Capture & Share

The Identification Context
The government began issuing the Nigerian identification card in 2008, three years prior to the introduction of biometric SIM registration. It is compulsory for all citizens above the age of 16 to obtain a national identification card; yet, a pre-requisite for this is that Nigerians possess a National Identification Number (NIN). Unlike the identification card, all citizens are eligible to enrol for an NIN[69]. The National Identity Management Commission (NIMC) is in the process of upgrading the national identification to an electronic biometric identification card[70] – an initiative, which the NIMC scheduled for introduction in 2013. In collaboration with MasterCard[71], the NIMC have added a payment element to the new electronic ID card, a decision made in the hope that the millions of unbanked Nigerians would be able to access financial services[72]. The Government also aspires to ensure citizens eventually use their National identification card for all identity-based transactions[73].

Identification for mobile access
The Nigerian Communications Commission (NCC) enforced biometric SIM registration in 2011.

The SIM registration process requires mobile users to present proof of identification as well as have their fingerprints and facial image[74] captured by the mobile operator(s) at the point of registration. Nigerians can use seven different forms of identification for SIM registration, including the national ID card and a letter of authentication[75] by a traditional ruler or community leader[76]. Non-Nigerian nationals are obligated to show their passport to register for a SIM card[77].

Unlike, most countries implementing biometric SIM registration the Nigerian government does not currently maintain a central database against which MNOs can validate customers' biometric details. Instead, MNOs are required to capture and send customers' biometric information, as well as their full name, gender, date of birth, address and occupation[78], to the NCC for storage. Operators can store their customers' personal data obtained during the registration exercise, but not their biometric data. The Nigerian government is currently in the process of integrating existing identification databases into a single National Identity Databas[79], which may ultimately lead to a requirement on MNOs to capture and validate customer information against it.

69. *What is the NIN?* Nigerian Identity Management Commission. https://www.nimc.gov.ng/about-nin/
70. *Nigeria launches national electronic ID cards.* BBC, 2014. http://www.bbc.co.uk/news/world-africa-28970411
71. https://www.nimc.gov.ng/the-e-id-card/
72. Ibid.
73. NIMC DG advises Nigerians on importance of National Identification Number (NIN) https://www.nimc.gov.ng/nimc-dg-advises-nigerians-on-importance-of-national-identification-number-nin/
74. *Registration of Telephone Subscribers Regulation.* Nigerian Communications Commission, 2011. https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file
75. *SIM registration Centers.* MTN. http://mtnonline.com/simregistration
76. *Traditional Rulers and Local Government in Nigeria: a Pathway to Resolving the Challenge.* O.Osemwota and D.A Tonwe, 2013.
77. Ibid.
78. *Registration of Telephone Subscribers Regulation.* Nigerian Communications Commission, 2011. https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file
79. *FG to merge BVN, driver's license, National identity card.* Clement Idoko, 2017. http://www.tribuneonlineng.com/fg-merge-bvn-drivers-licence-national-identity-card/

Case Study E

Uganda
SIM Registration – Capture & Validate

The Identification Context
At the same time that the government amended SIM registration requirements, the National Identification and Registration Authority (NIRA) launched a national identification registration exercise[80] to establish a comprehensive National Identification Register[81], providing national ID cards to Ugandans without one. The national ID card includes the biometric data of its holder. Citizens can use it to obtain a passport, vote, and access government and banking services. Only those above the age of 16 can acquire a national identity card[82] assuming they hold a National Identification Number (NIN). As of mid-2017, 70% of citizens aged 16 and over in Uganda are registered according to World Bank figures[83].

Identification for mobile access
The Uganda Communications Commission (UCC) imposed SIM registration rules in 2012[84]. Up until 2015, Ugandan mobile customers were required to present any official identification document such as a driver's license or passport and for mobile operators to record and store the details in a secure database. However, the government subsequently changed the requirements with the Registration of Persons Act 2015[85], limiting the forms of identification[86] acceptable for registration and requiring operators to verify the identity of subscribers[87] against a central database maintained by NIRA. The new rules mean Ugandans have to register their SIM cards exclusively using their national identification card, while foreigners must provide their passports and refugees need to present a certified document from the Office of the Prime Minister (OPM)[88].

During a recent re-registration exercise, operators offered existing mobile users the option of authenticating their identity via a SMS[89] / USSD service (Subscribers can dial *197#, specifying the mobile number they want to register and enter their identification number and full name). MNOs then send the details to the NIRA for validation upon which verified subscribers receive two messages, the first – acknowledging their application and the second outlining their registration status[90]. According to the UCC[91], MNOs registered 98% of SIMs during the latest re-registration exercise.

80. *Government to synchronize both SIM card and National ID registration data.* Roger Bambino, 2015.
81. https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf?sequence=1&isAllowed=y
82. *Frequently Asked Questions (FAQS) on the registration of pupils and registration project May – August 2017.* National Identification and Registration Authority, 2017. http://www.nira.go.ug/index.php/contact-us/faqs/
83. World Bank ID4D Dataset 2017, based on Uganda's National Identification and Registration Authority database
84. *Government to synchronize both SIM card and National ID registration data.* Roger Bambino, 2015. http://www.techjaja.com/government-to-synchronize-both-sim-card-and-national-id-registration-data/
85. *Progress on the SIM card Validation/Verification Exercise.* Uganda Media Centre. http://www.mediacentre.go.ug/press-release/progress-sim-card-validationverification-exercise
86. SIM Registration. Uganda Telecom. http://www.utl.co.ug/index.php/sim-registration/
87. *Government to synchronize both SIM card and National ID registration data.* Roger Bambino, 2015.
88. *What you should know about new SIM card registration.* Joseph Kato, 2017. http://www.monitor.co.ug/News/National/What-you-should-know-about-new-SIM-card-registration/688334-3889130-36h2i3z/index.html
89. Ibid.
90. *Here is how to re-register your SIM card on MTN, Airtel, Vodafone, Smart, Smile and Africell Uganda before deadline.* Onyait Odeke, 2017. http://www.dignited.com/22430/re-register-sim-card-mtn-airtel-africell-vodafone-smile-smart-uganda/
91. *UCC hails 98% success rate for SIM registration scheme.* Telegeography, 2017. https://www.telegeography.com/products/commsupdate/articles/2017/09/21/ucc-hails-98-success-rate-for-sim-registration-scheme/index.html

Case Study F

India
Biometric SIM Registration – Capture and Validate

The Identification Context
The Aadhaar is a unique 12-digit number issued by the Unique Identity Authority of India (UIDAI), available to all residents at no cost. It is a portable biometric identification, which denotes residency rather than citizenship. Once a person obtains an Aadhaar number, it is valid for the rest of their life. Using their Aadhaar number, individuals may open a bank account[92], get a driver's license and apply for a passport. The Aadhaar is the world's largest biometric ID system. As of December 2017, the UIDAI have registered more than 1.1 billion people[93] on the database – approximately 84% of the Indian population[94].

Identification for mobile access
SIM registration has been mandatory in India since 2005, yet the requirements evolved over the years. In 2017, the Department of Telecommunications (DoT) started enforcing biometric SIM registration for issuing new mobile connections and re-verifying existing consumers[95].

Prospective mobile subscribers must visit a MNO retailer to complete biometric SIM registration. New customers must complete a Customer Acquisition Form (CAF) in addition to sharing their Aadhaar number with a registration agent, they also have to have their fingerprints and/or iris iscanned using a biometric reader, which enables the validation of the credentials against the UIDAI database via an online porta[96]. MNOs are required to procure the biometric scanners, which cost approximately USD $50-$60. Assuming the biometric credentials match that on the UIDAI system, the MNO agent requests the UIDAI to send a One Time Password (OTP) to the customer's mobile number, to complete the biometric verification process[97]. Each customer can register for a maximum of nine SIM cards[98]. Unlike Indian residents, foreign visitors are not required to provide biometrics for registering a SIM card but must show their passport with a valid visa and proof of address.

While MNOs can store the personal data of their customers, they cannot retain their biometric information.

92. https://medium.com/wharton-fintech/your-guide-to-upi-the-worlds-most-advanced-payments-system-b4e0b372bf0b
93. *Enrolment Dashboard.* Unique Identification Authority of India (UIDAI), 2017. https://uidai.gov.in/aadhaar_dashboard/india.php?map_state=Assam
94. *Aadhaar Enrolment.* UIDAI, 2017. https://uidai.gov.in/enrolment-update/aadhaar-enrolment.html
95. *Implementation of orders of Hon'ble Supreme Court regarding 100% E-KYC based re-verification of existing subscribers- regarding.* Department of Telecommunications (DoT), 2017A. http://dot.gov.in/sites/default/files/Re-verification%20instructions%2023.03.2017.pdf?download=1
96. *Use of 'Aadhaar' e-KYC service of Unique Identity Authority of India (UIDAI) for issuing new mobile connection to outstation customers and re-verification of existing outstation subscribers- regarding.* DoT, 2017B. http://dot.gov.in/sites/default/files/Outstation%2015.06.2017-final.PDF?download=1
97. http://www.timesnownews.com/business-economy/personal-finance/planning-investing/article/mobile-aadhaar-linking-and-biometric-verification-at-telecom-stores-are-different-know-why/141163
98. *Having more than 9 SIMs may land you in trouble.* Sanjay Singh, November 2012 http://indiatoday.intoday.in/story/telecom-companies-subscribers-who-have-more-than-nine-sim-cards-in-their-names/1/228526.html

Case Study G

Thailand
Biometric SIM Registration – Capture & Validate

The Identification Context

In 2005, the Thai government implemented the Thai smart ID card programme, which incorporates the fingerprints of citizens issued with a card[99]. Holders can use their cards to open a bank account and access government services. It is obligatory for all citizens aged 7 and above to obtain an ID[100] which they can do free of charge. Thailand has a comprehensive identification system with 97%[101] of the population registered.

Identification for mobile access

The National Broadcasting and Telecommunications Commission (NBTC) enforced SIM registration requirements in 2013 but it was not until the end of 2017[102] that the NBTC introduced biometric SIM registration[103]. Under the new rules[104], all Thai mobile operators must capture and validate subscribers' biometric credentials (fingerprints or facial scans[105]) against the data stored on their national identification smartcards, which is identical to that in the government's central citizen database[106] managed by the Bureau of Registration Administration. MNOs are required to bear the cost of the biometric scanners and card readers needed to implement the SIM registration process[107]. Foreigners buying SIM cards in Thailand will have their faces scanned and matched against their passport photographs.

99. *Thailand introduces national ID with biometric technology.* Lauren Lowrey, 2005. https://www.secureidnews.com/news-item/thailand-introduces-national-id-with-biometric-technology/
100. https://asiancorrespondent.com/2011/06/why-thailand-wants-children-to-carry-id-cards-an-explanation-attempt/
101. World Bank ID4D Dataset 2017, based on Thailand's Department of Provincial Registration database
102. *Biometric checks for new SIM cards start next month – foreigners exempt for now.* Staff Writer, 2017. https://tech.thaivisa.com/biometric-checks-new-sim-cards-starts-next-month-for-eigners-exempt-now/25797/
103. *State of Privacy Thailand.* Privacy International, 2017. https://www.privacyinternational.org/node/967
104. *Thailand to roll out biometric checks for SIM cards nationwide*. Reuters Staff, 2017. https://uk.reuters.com/article/us-thailand-telecoms/thailand-to-roll-out-biometric-checks-for-sim-cards-nationwide-idUKKBN1D611A
105. *SIMs go biometric Dec 15.* Komsan Tortermvasana, 2017. https://www.bangkokpost.com/tech/local-news/1355955/sims-go-biometric-dec-15
106. http://www.straitstimes.com/asia/se-asia/thailand-to-roll-out-biometric-checks-for-sim-cards-nationwide-to-deter-electronic
107. *SIMs go biometric Dec 15.* Komsan Tortermvasana, 2017. https://www.bangkokpost.com/tech/local-news/1355955/sims-go-biometric-dec-15

Case Study H

Peru
Biometric SIM Registration – Capture & Validate

The Identification Context

The Peruvian National Identity Document DNI is a biometric identity card, which the National Registry of Identification and Civil Status (RENIEC) started distributing to citizens in 2009. It maintains each cardholder's unique personal data such as their full name, fingerprint, date of birth and photo[108]. The biometric ID is the primary method through which residents can access essential government services. All Peruvians must acquire a DNI at the age of 17. Although the cost of the card for citizens starts at $5 USD, 99% of over 17s own a DNI[109]. In 2013, RENIEC started allocating new electronic DNIs (DNI-e)[110], as part of the government's plan to migrate a number of their transactions to a digital environment. The new electronic identity card has an embedded cryptographic chip to store biometric information for the purposes of authentication services. As of December 2017, RENIEC has reportedly issued approximately 500,000 electronic DNIs with a plan to accelerate citizen adoption through the creation of an electronic wallet for users to store their ID card on their smartphones and use this when conducting transactions requiring proof-of-identity.

Identification for mobile access

SIM registration has been mandatory in Peru since 2007 and users' identification must be validated at the point of registration, when a subscription is ported or when the client acquires a new mobile device; the Supervisory Agency for Private Investment in Telecommunications (OSIPTEL) introduced biometric registration at the beginning of 2016[111] requiring all mobile users to register their SIM cards by presenting their (DNI) and have their fingerprint scanned. The MNO validates these credentials against RENIEC's database and must also store the full name, DNI number, telephone number, phone model and series of each mobile user on a database. Non-nationals can show either a foreigner's card or passport to SIM card retailers.

MNOs are required to procure fingerprint readers that comply with government regulations. The RENIEC has also been charging private sector entities (including MNOs) to use their database for identity-verification. The charges had been set according to the range of verification queries operators request in a month, as per below.

- **1.6 nuevos soles** (up to 30,000)
- **1.33 nuevos soles** (more than 30,000 and less than 120,000)
- **0.86 nuevos soles** (more than 120,000 and less than 240,000)
- **0.52 nuevos soles** (more than 240,000 and less than 360,000)
- **0.29 nuevos soles** (more than 360,000)

On December 7, 2017, the Peruvian government publicly noted in its official publication (Diario Oficial) that RENIEC would begin providing the biometric validation of citizens' identification free of charge in certain contexts. The implication of this policy decision on MNOs' SIM registration compliance costs (if any) has not been assessed.

108. http://www.identity-cards.net/record/peru
109. World Bank ID4D Dataset 2017, based on Peru's Voter Registration and RENIEC databases
110. *The Details of a Peruvian DNI Card.* Tony Dunnell, 2017. https://www.tripsavvy.com/what-is-a-peruvian-dni-1619655
111. OSIPTEL, 2016. http://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/ds-003-2016-mtc/DS003-2016-MTC.pdf

08

Privacy/Data Protection Frameworks and Mandatory SIM registration

Mobile devices are inherently personal as people increasingly use them beyond communicating with each other, to access the internet and importantly to share their views publicly through social networks and online media. Mandatory SIM registration policies force a link between having a personal mobile subscription with a person's ability to prove who he or she is, using a recognised identification credential. As indicated earlier in this document, the effectiveness and merits of such policies depend on several market-specific factors and individuals' ability to meet the relevant identification requirements; Where mobile users can meet these requirements, linking their identity to their mobile subscription can allow them to benefit from life-enhancing mobile and digital identity services that would otherwise be unavailable to them as unregistered users (such as opening Mobile Money accounts and accessing e-Government services).

However, a primary principle in designing any identification system and/or implementing policies requiring 'proof-of-identity' (such as SIM registration) is ensuring the individuals' privacy is respected and personal data are protected against unauthorised use by third parties or for purposes other than what an individual has consented to or would reasonably expect[112]. Legal and regulatory frameworks should ensure that personal data provided for registration purposes should not be used for unwanted commercial communications, discriminatory purposes on the basis of race, religion or gender, or for other problematic or unlawful purposes. Personal data also needs to be protected from accidental destruction, loss, alteration, and unauthorised disclosure or access[113].

Where they exist, data protection and privacy laws typically impose responsibilities on data controllers or data processors – government departments, businesses and other organisations that hold and use personal data – regarding how they store and share it. These may extend to a wide variety of organisations, from banks, insurance, telecom operators, health care providers, utilities, airlines, law firms, accountancy firms and others, some of whom may be required to register with and report to the data protection authorities.

Mobile network operators are often subject to a range of laws and/or licence conditions that require them to support law enforcement and security activities in countries where they operate. These requirements vary from country to country and have an impact on the privacy of mobile users. Where they exist, such laws and licence conditions typically require operators to retain data about their customers' mobile communications, including customers' personal data, and disclose these to law enforcement and national security agencies on lawful demand.

112. See Principles on Identification for Sustainable Development: https://www.gsma.com/identity/wp-content/uploads/2017/02/Identification-Principles.pdf
113. https://www.gsma.com/mobilefordevelopment/programme/digital-identity/regulatory-and-policy-trends-impacting-digital-identity-and-the-role-of-mobile

Such laws usually provide a framework for the operation of law enforcement and security service surveillance and provide guidance for mobile operators on when and how to comply with such government access requests. They also often mitigate against possible financial and reputational risk, by ensuring that government access requests to data take place within clearly defined and transparent frameworks.

Despite the large number of countries mandating SIM registration and requiring MNOs to capture and store customers' personal data when registering customers, a significant minority of those countries do not have a comprehensive legal framework in place to guarantee mobile users' privacy and protect their data from improper use. Furthermore, a lack of clarity in the legal framework on what constitutes lawful government access to, or interception of, consumers' mobile communications creates challenges for mobile operators and risks for consumers.

The GSMA published a set of universal Mobile Privacy Principles[114] that describe the way in which mobile consumers' privacy should be respected and protected when consumers use mobile applications and services that access, collect and use personal information. The mobile industry has also worked to educate consumers and developed new features that have built trust in its services. Each new iteration of technology has introduced new features, such as encryption and user identification validation, which have made mobile services increasingly secure and minimised the potential for fraud, identity theft and many other possible threats. While MNOs overwhelmingly apply high standards of privacy, data protection and security practices with regards their customers' data, the inadequacy of legal frameworks can have an impact on customers' own perceptions around the use of their data and potentially their willingness to adopt or use their mobile devices to access identity-linked services[115].

Figure 8.1 shows the existence (or lack) of privacy and/or data protection frameworks worldwide while Figure 8.2 illustrates the same but just for the 147 countries where prepaid SIM registration is mandated. Of these 147 countries, 50 lack a comprehensive or data protection framework comprising approximately a third of all countries mandating SIM registration[116] (see Figure 8.3).

Key observations[117]:

Of all the countries where SIM registration is mandatory,

- 26 countries in Sub-Saharan Africa, do not maintain a data protection/privacy system (even though 7 are considering the implementation)
- 13 countries across the Middle East and North Africa (MENA) region do not maintain a data protection/privacy system (even though 4 are considering the implementation)
- 18 countries across Asia Pacific do not maintain a data protection/privacy system (even though 3 are considering the implementation)
- 16 countries across Central and South America do not maintain a data protection/privacy system (even though 8 are considering the implementation)
- All countries across Europe maintain a data protection/privacy framework

114. https://www.gsma.com/publicpolicy/mobile-privacy-principles
115. https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf
116. At the time of drafting this report (November 2017) a few of these countries' legislative bodies are considering proposed privacy and/or data protection Bills.
117. See Annexes 9-13

Figure 8.1

State of privacy and/or data protection frameworks worldwide

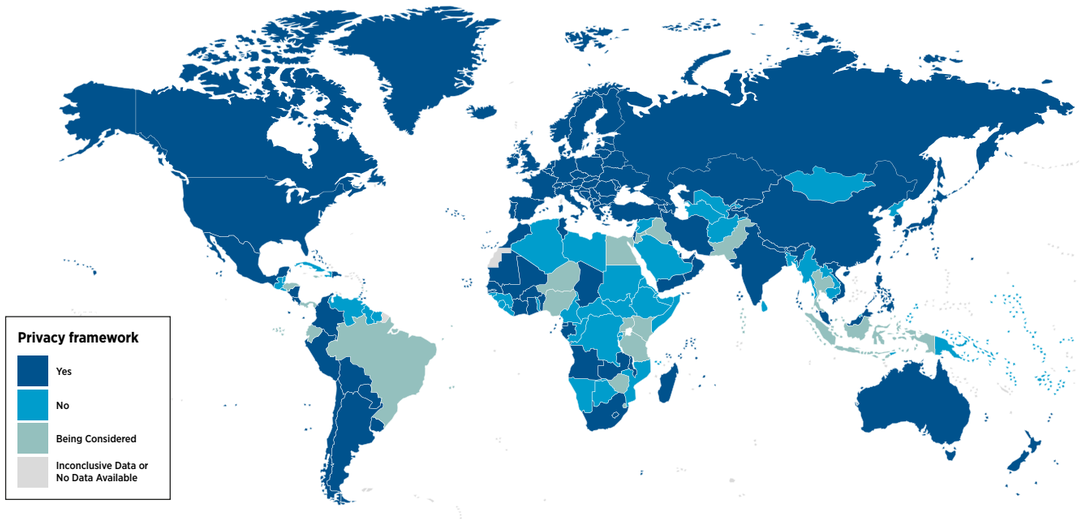


Figure 8.2

State of privacy and/or data protection frameworks in countries mandating or considering SIM registration

(Annexes 9, 10, 11, 12, 13)

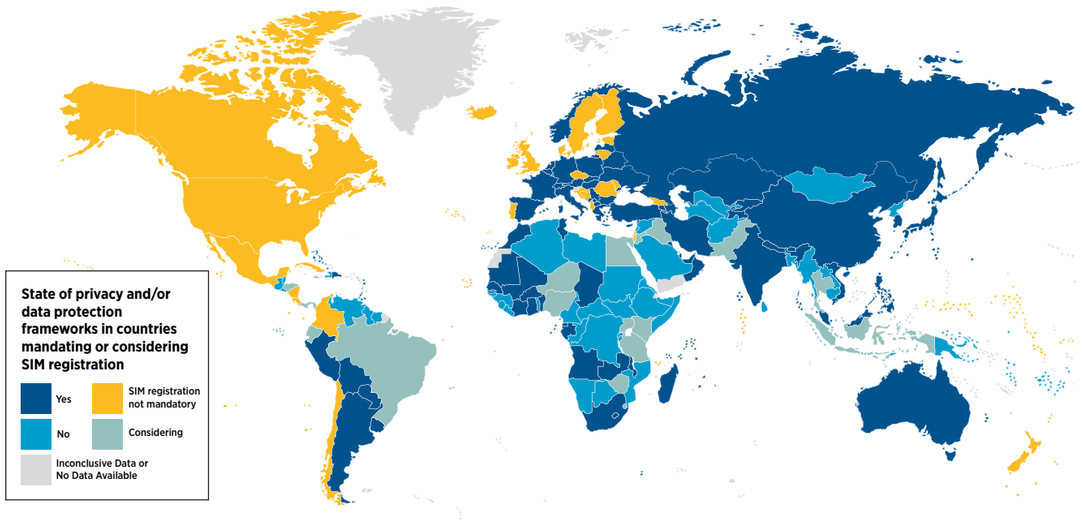


Figure 8.3

Aggregate number of countries with a Privacy and/or Data Protection framework where SIM registration is mandated or being considered

(Annexes 9, 10, 11, 12 and 13)

Privacy and/or Data Protection Framework	Mandatory SIM Registration: Yes	Mandatory SIM Registration: Considering
No	50	1
Considering	22	0
Yes	75	7

Case Study I

Saudi Arabia

Biometric SIM Registration – Capture and Validate

The Identification Context

Saudi Arabia's Ministry of Interior began issuing the Saudi electronic national identity card in 2007, nine years prior to the introduction of biometric SIM registration. It is compulsory for all Saudi citizens over the age of 15 to possess the national identity card and also acts as a travel document for those visiting Gulf Corporation Council (GCC) countries[118].

Identification for mobile access

Fingerprint-based biometric SIM registration is mandatory since 2016[119]. In order to register a SIM card, mobile customers must complete a registration form, providing their full name, identification number and other personal details[120] as well as have their fingerprint scanned on a biometric device. The biometric reader is linked to the National Information Center's database[121] so mobile operators can verify the identity of their customers in real-time before activating the customer's SIM card. The country does not have a Privacy and/or Data protection framework in place.

118. https://www.securetechalliance.org/gemalto-provides-national-e-id-cards-to-the-kingdom-of-saudi-arabia/
119. *Biometrics registration for SIM cards begins in Saudi Arabia.* Stephen, Mayhew, 2016. http://www.biometricupdate.com/201601/biometrics-registration-for-sim-cards-begins-in-saudi-arabia
120. http://www.alhayat.com/m/story/13538082#sthash.6HRXrdbf.Bb8Omvu8.dpbs
121. Ibid.

Case Study J

Ecuador
SIM Registration – Capture and Validate

The Identification Context
The Cedula de Identidad is the official national identification credential in Ecuador, issued by the Civil Registry. It includes the biometric data of each cardholder. Citizens can use their national identity card to travel within the country, register for a passport and for voting. Ecuadorians of all ages are eligible to obtain a Cedula de Identidad at cost of USD$5[122]. Ecuador has a comprehensive identification system in place with 98%[123] of the population registered. At the beginning of 2017, the government announced their intention to replace the Cedula with a new electronic identity (e-ID) card. Ecuadorians will be able to continue using the new e-ID as a travel document, as well as to access government services electronically[124].

Identification for mobile access
In 2011, the Telecommunications Regulation and Control Agency (CONATEL) made SIM registration mandatory in Ecuador[125]. MNOs are obliged to capture the full name, address, identification number and the year of issue for each mobile user, in order to complete the SIM registration process. CONATEL requires Ecuadorian citizens to use their identity card or any other official document to complete SIM registration while foreigners must present their passport.

The MNO validates the data against the Ecuadorian Civil Registry and once these are confirmed, MNOs must record and store subscribers' personal information for at least 5 years, linking the SIM card's details to the handset's IMEI number for each consumer[126]. The Minister of Telecommunications declared that if people do not register, not only the lines, but also the devices can be blocked even outside the country, stressing that agreements for cooperation were under negotiation with Colombia and Peru[127].

Ecuador still lacks a Privacy and/or Data Protection framework (although the government are considering implementing one[128]), so concerns may be raised[129] around the risk of consumer exploitation when accessing digital identity services, in the absence of proper safeguards.

122. http://cuencacultureshock.com/ecuador-cedula-requirements/
123. World Bank ID4D Dataset 2017, based on Ecuador's Voter Registration database
124. *NXP secures electronic ID cards and passports in Ecuador.* NXP Semiconductors Netherlands B.V, 2017 https://globenewswire.com/news-release/2017/05/25/995964/0/en/NXP-Secures-Electronic-ID-Cards-and-Passports-in-Ecuador.html
125. *Nine months for expectant ministry to deliver SIM registration measures.* TeleGeography, 2011. https://www.telegeography.com/products/commsupdate/articles/2011/07/12/nine-months-for-expectant-ministry-to-deliver-sim-registration-measures/
126. *NXP secures electronic ID cards and passports in Ecuador.* NXP Semiconductors Netherlands B.V, 2017
127. https://www.derechosdigitales.org/wp-content/uploads/freedom-of-expression-encryption-and-anonymity1.pdf
128. *Ecuador: Bill addresses "lack of data protection culture".* Data Guidance, 2016. https://www.dataguidance.com/ecuador-bill-addresses-lack-of-data-protection-culture/
129. https://freedomhouse.org/report/freedom-net/2017/ecuador

Case Study K

Bahrain
Biometric SIM Registration – Capture and Validate

The Identification Context
The Government of Bahrain implemented a smartcard identity project in 2007, ten years before mandating biometric SIM registration. The electronic smartcard includes the biometric data of cardholders and can act as a driving license, travel document and e-payment card. All Bahrainis are required to hold a national identity card; however, according to the 2017 World Bank Identification for Development (ID4D) data only 52%[130] of the population are registered though the reference source is dated from 2009.

Identification for mobile access
All mobile users in Bahrain must provide MNOs with a proof-of-identity and their fingerprint impression in order to access mobile services. The government introduced SIM registration requirements in 2015, yet did not enforce biometric registration until 2017 with the deadline set for March 2019 giving MNOs a reasonable timeframe within which to register and validate their existing customers' identification and biometric credentials against the Information and eGovernment Authority's (IGA)[131] database. Bahraini nationals can use a passport or identity card to complete the registration process. Foreign citizens can opt to show their passport or Gulf Corporation Council (GCC) card, if they possess one[132]. Each mobile user can register up to thirty SIM cards across the three mobile network operators in Bahrain[133].

MNOs are not authorised to store customers' biometric data[134], yet they can maintain subscriber databases based on other personal data provided during the registration exercise[135].

The Telecommunications Regulator Authority (TRA) requires MNOs to revalidate the personal details of its mobile users every 12 months from the date of registration. During the revalidation exercise, telecom providers are to ensure the unique number from the identification credential provided by an individual matches the number recorded on their subscriber database[136].

130. World Bank ID4D Dataset 2017, based on Bahrain's Voter Registration database
131. Batelco, 2017A. http://batelco.com/mobile/register-your-mobile-line/
132. Batelco, 2017A. http://batelco.com/mobile/register-your-identity/
133. Batelco, 2017A. http://batelco.com/mobile/register-your-mobile-line/
134. *The TRA's Board of Directors Resolution No. (13) Of 2015: Promulgating the SIM-Card Enabled Telecommunications Services Registration Regulation. TRA,* December 2015. http://www.tra.org.bh/media/document/SIM%20Card%20Regulation%20(FINAL)_Final%20(1).pdf
135. Ibid.
136. Ibid.

09

The role of identification and mobile in underpinning countries' Digital Transformation

As noted earlier, the UN Sustainable Development Goal (SDG) 16.9 is to provide 'a legal identity for all by 2030, including birth registration'[137].

Meeting this goal means reaching the estimated 1.1 billion individuals who currently lack a form of official identification and who risk being excluded from exercising their rights and accessing vital services such as healthcare, banking, education as well as other mobile and digital services where proof-of-identity is required.

As governments around the world are implementing their national digital transformation strategies, they are faced with policy decisions regarding spectrum harmonisation, rural connectivity, job creation and digital skills. Beyond addressing these objectives, having an enabling policy environment to facilitate access to identification is likely to be a key determinant to the success and inclusivity of a Government's digital transformation strategy.

A Government-backed or recognised identification system that is accessible by a critical mass of a country's population can not only facilitate the delivery of life-enhancing services to individuals but can also lead to a wide spectrum of benefits for governments and the private sector in terms of improved administration, more inclusive, personalised and efficient delivery of services.

A number of countries have demonstrated how investing in more innovative identification systems and technologies can help leapfrog traditional paper-based approaches and leverage the benefits of Digital Identity. For example, India enrolled over 1.1 billion people on its Digital ID (Aadhaar) platform in under seven years enabling the opening of millions new bank accounts simply by quoting their Aadhaar number and scanning their fingerprint. In Pakistan, one of the largest social protection payment services (BISP)[138] targeting the female head of household leveraged the country's Digital Identification system to ensure payments were indeed received by the female head of household.

In the context of enabling access to mobile services, the robustness of a government-recognised identification credential and the ability of Mobile Operators to query and validate that credential against a centralised government database could significantly improve the effectiveness of a SIM registration policy (where mandated) while mitigating the risks of digital and financial exclusion.

A higher degree of confidence in the true identification of a registered mobile user can also enable Mobile Network Operators to create and enrich customers' Digital Identity profiles with additional network and context-related attributes (e.g. based on the location of their mobile handset, PIN or SMS Codes) enabling them to digitally authenticate their identity to access value added services online.

137. https://sustainabledevelopment.un.org/sdg16
138. http://bisp.gov.pk/wp-content/uploads/2017/05/BISP-Women-empower-forum-24-05-2017-latest.pdf

With more than 5 billion subscribers globally, mobile has the ability to accelerate the scale and reach of inclusive, digital identities that can empower citizens, protect privacy and stimulate economic and social development. This is already happening, worldwide. Mobile Birth registration[139] solutions; registration and authentication for eGovernment[140] through Mobile Connect[141]; blockchain-enabled platforms[142] to create KYC-compliant digital identities; and mobile apps for verifying ID cards for refugees[143] are just a few examples of the solutions that are laying the foundation for the digital identity ecosystem[144].

The prospects for mobile-enabled digital identity services to grow, accelerate a country's digital transformation, support digital and financial inclusion, and offer the benefits of convenience and reach to the population are greatly strengthened where the government develops a national strategy underpinned by an enabling policy environment. This is also likely to influence the willingness of both MNOs' to offer and of mobile users to adopt such services.

In partnership with the World Bank and other international stakeholders with a shared vision, the GSMA co-developed a set of common Principles[145] aimed at fostering robust and inclusive identification systems that enable economic opportunities and sustainable development outcomes. These are listed in Figure 9.1 below:

Figure 9.1

Principles on Identification for Sustainable Development: Toward the Digital Age

INCLUSION
UNIVERSAL COVERAGE AND ACESSIBILITY

1. Ensuring universal coverage for individuals from birth to death, free from discrimination.
2. Removing barriers to access and usage and disparities in the availability of information and technology.

DESIGN
ROBUST, SECURE, RESPONSIVE, AND SUSTAINABLE

3. Establishing a robust – unique, secure and accurate – identity.
4. Creating a platform that is interoperable and responsive to the needs of various users.
5. Using open standards and ensuring vendor and technology neutrality.
6. Protecting user privacy and control through system design.
7. Planning for financial and operational sustainability without compromising accessibility.

GOVERNANCE
BUILDING TRUST BY PROTECTING PRIVACY AND USER RIGHTS

8. Safeguarding data privacy, security and user rights through a comprehensive legal and regulatory framework.
9. Establishing clear institutional mandates and accountability.
10. Enforcing legal and trust frameworks though independent oversight and adjudication of grievances.

139. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/01/Innovations-in-Mobile-Birth-Registration_Insights-from-Tigo-Tanzania-and-Telenor-Pakistan.pdf
140. https://www.gsma.com/identity/mobile-connect-government
141. https://www.gsma.com/identity/mobile-connect
142. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf
143. http://www.unhcr.org/news/latest/2016/6/591283e37/unhcr-rolls-out-new-card.html
144. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/Regulatory-and-policy-trends-impacting-Digital-Identity-and-the-role-of-mobile.pdf
145. https://www.gsma.com/identity/wp-content/uploads/2017/02/Identification-Principles.pdf

ACCESS TO MOBILE SERVICES AND PROOF-OF-IDENTITY

10

Conclusions

As more countries – particularly in the developing world – continue to implement their Digital Transformation strategies, proving one's identity digitally will become increasingly fundamental to participation and inclusion. A key step to this inclusion is people's ability to access mobile services in their own name but this may not be possible for millions of vulnerable groups who lack the recognised identification credentials and reside in countries where prepaid SIM registration is mandated.

Building on the GSMA's previous research[146], this report offered an updated global overview and identified trends and linkages between mandatory SIM registration policies, the official identification coverage and the level of mobile penetration across different markets. It highlighted that in 147 countries worldwide, proof-of-identity is needed to register a prepaid mobile SIM card in one's own name while this is also needed to open a Mobile Money account across the 92 countries where Mobile Financial Services are available. A small but slowly increasing number of countries have adopted the use of biometric technologies for registering SIM cards while also building capabilities for enabling (and requiring) MNOs to validate their customers' identification credentials against a central database in real time.

Half of the countries mandating SIM registration have no or inadequate privacy / data protection frameworks in place with consumers potentially having limited, if any, rights to seek legal redress against possible violations of their privacy or personal data. This may not only lead to consumer calls for increased transparency on how personal data are used but could also adversely impact their willingness to register a SIM in their own names or adopt identity-linked mobile services. Additionally, transparency to consumers about how their data is used is important for maintaining high levels of trust in digital and mobile ecosystems.

This research supports the conclusion that millions of individuals who lack a proof-of-identity face a higher risk of social, digital and financial exclusion where they cannot meet mandatory SIM registration requirements.

146. https://www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards

In order to drive improved social, political and economic inclusion, as well as engender trust in the digital ecosystem, the need for enabling policy and regulatory environments should not be underestimated – particularly where SIM registration is mandated. Elements of such an environment include:

- Empowering every individual to access an official or recognised form of identification while acknowledging the central role mobile operators (due to their existing reach) can play in building or supporting the digital identity ecosystem;
- Ensuring consistency between the different legal and regulatory instruments that affect the management and the roll out of mobile identity services;
- Establishing or maintaining privacy and data protection frameworks that foster trust in mobile and digital identity ecosystems.
- Engaging with mobile operators, key stakeholders and the wider identification ecosystem to help drive innovative and interoperable solutions and encourage adoption (e.g. through eGovernment and digital social protection services).

With more than 5.1 billion unique subscribers globally, mobile networks connect people as no other technology before, providing access to a vast array of life-enhancing services. Given this scale, the mobile industry has a unique opportunity to bring the benefits of digital technology to many of the poorest and hardest to reach communities around the world, and in doing so, help deliver one of the key targets of Sustainable Development Goal 16: 'by 2030, provide legal identity for all, including birth registration'[147].

147. https://www.weforum.org/agenda/2018/01/3-ways-mobile-is-solving-the-global-identity-crisis

11

Annexes

Annex 1

Countries where SIM registration is mandatory (by region)

AFRICA

Algeria
Angola
Benin
Botswana
Burkina Faso
Burundi
Cameroon
Central African Republic
Chad
Congo
Democratic Republic of Congo
Côte d'Ivoire
Egypt
Equatorial Guinea
Eritrea
Ethiopia
Gabon
Gambia
Ghana
Guinea
Guinea-Bissau
Kenya
Lesotho
Liberia
Libya
Madagascar
Malawi
Mali
Mauritania
Mauritius
Morocco
Mozambique
Niger
Nigeria
Rwanda
Sao Tomé and Principe
Senegal
Seychelles
Sierra Leone
Somalia
South Africa
South Sudan
Sudan
Swaziland
Tanzania
Togo
Tunisia
Uganda
Zambia
Zimbabwe

ASIA

Afghanistan
Armenia
Australia
Azerbaijan
Bahrain
Bangladesh
Bhutan
Brunei Darussalam
Cambodia
China
Fiji
India
Indonesia
Iran
Iraq
Japan
Jordan
Kazakhstan
Kuwait
Kyrgyzstan
Laos
Lebanon
Malaysia
Mongolia
Myanmar
Nauru
Nepal
North Korea
Oman
Pakistan
Palestine
Papua New Guinea
Qatar
Samoa
Saudi Arabia
Singapore
South Korea
Sri Lanka
Syria
Taiwan
Tajikistan
Thailand
Timor-Leste
Tonga
Turkey
Turkmenistan
United Arab Emirates
Uzbekistan
Vanuatu
Vietnam

CENTRAL AND SOUTH AMERICA

Antigua and Barbuda
Argentina
Bahamas
Barbados
Belize
Bolivia
Brazil
Dominica
Dominican Republic
Ecuador
El Salvador
Grenada
Guatemala
Guyana
Haiti
Honduras
Jamaica
Panama
Peru
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
Suriname
Trinidad and Tobago
Uruguay
Venezuela

EUROPE

Belarus
Belgium
Bulgaria
France
Germany
Greece
Hungary
Italy
Kosovo
Liechtenstein
Luxembourg
Macedonia
Montenegro
Norway
Poland
Russian Federation
San Marino
Slovakia
Spain
Switzerland
Ukraine

Annex 2

Countries where a mandatory SIM registration policy is being considered

Austria
Cyprus
Latvia
Namibia
Netherlands
Paraguay
Philippines
Serbia

Annex 3

Countries where SIM registration is not mandatory

Albania
Andorra
Bosnia and Herzegovina
Cabo Verde
Canada
Chile
Colombia
Comoros
Costa Rica
Croatia
Cuba
Czech Republic
Denmark
Estonia
Finland
Georgia
Hong Kong
Iceland
Ireland
Israel
Kiribati
Lithuania
Macau
Maldives
Malta
Marshall Islands
Mexico
Micronesia
Moldova
New Zealand
Nicaragua
Portugal
Romania
Sweden
United Kingdom
United States of America

Annex 4

Countries where data on the state of SIM registration policy is inconclusive or not available

Djibouti
French Guiana
Greenland
Monaco
Palau
Slovenia
Solomon Islands
Tuvalu
Yemen

Annex 5

Countries where Mobile Money services are available

AFRICA

Benin
Botswana
Burkina Faso
Burundi
Cameroon
Central African Republic
Chad
Congo
Côte d'Ivoire
Democratic Republic of Congo
Egypt
Ethiopia
Gabon
Gambia
Ghana
Guinea
Guinea-Bissau
Kenya
Lesotho
Liberia
Madagascar
Malawi
Mali
Mauritania
Morocco
Mozambique
Namibia
Niger
Nigeria
Rwanda
Senegal
Seychelles
Sierra Leone
Somalia
South Africa
Swaziland
Tanzania
Togo
Tunisia
Uganda
Zambia
Zimbabwe

ASIA

Afghanistan
Armenia
Bangladesh
Cambodia
Fiji
India
Indonesia
Iran
Iraq
Jordan
Kyrgyzstan
Malaysia
Maldives
Mongolia
Myanmar
Nepal
Pakistan
Papua New Guinea
Philippines
Qatar
Samoa
Singapore
Solomon Islands
Sri Lanka
Thailand
Timor-Leste
Tonga
Vanuatu
Vietnam

CENTRAL AND SOUTH AMERICA

Argentina
Bolivia
Brazil
Columbia
Dominican Republic
Ecuador
El Salvador
Guatemala
Guyana
Haiti
Honduras
Jamaica
Mexico
Nicaragua
Panama
Paraguay
Peru

EUROPE

Albania
Georgia
Romania
Russia

Annex 6

Countries requiring mobile operators to 'capture & store' customer information as part of SIM registration requirements

AFRICA

Angola
Botswana
Burkina Faso
Burundi
Cameroon
Central African Republic
Chad
Congo
Côte d'Ivoire
Democratic Republic of Congo
Equatorial Guinea
Eritrea
Ethiopia
Gabon
Gambia
Guinea
Guinea-Bissau
Lesotho
Liberia
Libya
Madagascar
Malawi
Mali
Mauritania
Mauritius
Morocco
Mozambique
Niger
Rwanda
Sao Tome and Principe
Seychelles
Sierra Leone
Somalia
South Africa
South Sudan
Sudan
Swaziland
Taiwan
Tanzania
Togo
Tunisia
Zambia
Zimbabwe

ASIA

Afghanistan
Armenia
Australia
Bhutan
Brunei Darussalam
Cambodia
Fiji
Iran
Iraq
Japan
Jordan
North Korea
Kuwait
Laos
Lebanon
Lebanon
Mongolia
Myanmar
Nauru
Nepal
Oman
Palestine
Papua New Guinea*
Qatar
Samoa
Singapore
South Korea
Sri Lanka
Syria
Taiwan
Timor-Leste
Tonga
Turkey
United Arab Emirates*
Vanuatu
Vietnam

CENTRAL AND SOUTH AMERICA

Antigua and Barbuda
Argentina
Bahamas
Barbados
Belize
Bolivia
Brazil
Dominica
Dominican Republic
El Salvador
Grenada
Guatemala
Guyana
Haiti
Honduras
Jamaica
Panama
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
Suriname
Trinidad and Tobago
Uruguay
Venezuela

EUROPE

Belarus
Belgium
Bulgaria
France
Germany
Greece
Kosovo
Liechtenstein
Luxembourg
Macedonia
Montenegro
Norway
Poland
Slovakia
Spain
Switzerland
Ukraine

Annex 7

Countries requiring mobile operators to 'capture & share' customer information as part of SIM registration requirements

Algeria
Benin
Italy
Kenya
Nigeria
San Marino

Annex 8

Countries requiring mobile operators to 'capture & validate' customer information as part of SIM registration requirements

Bahrain
Bangladesh
China
Ecuador
Egypt
Ghana
Hungary
India
Indonesia
Malaysia
Pakistan
Peru
Saudi Arabia
Senegal
Thailand
Uganda

Annex 9

Countries mandating SIM registration and have a Data Protection and/or Privacy Framework

AFRICA

Angola
Benin
Burkina Faso
Chad
Côte d'Ivoire
Equatorial Guinea
Gabon
Gambia
Ghana
Lesotho
Madagascar
Malawi
Mali
Mauritania
Mauritius
Morocco
Sao Tome and Principe
Senegal
Seychelles
South Africa
Tunisia
Zambia

ASIA

Armenia
Australia
Azerbaijan
Bhutan
China
India
Iran
Japan
Kazakhstan
Kuwait
Kyrgyzstan
Malaysia
Nepal
Oman
Qatar
Singapore
South Korea
Taiwan
Tajikistan
Turkey
United Arab Emirates
Vietnam

CENTRAL AND SOUTH AMERICA

Antigua and Barbuda
Argentina
Bahamas
Bolivia
Dominican Republic
Peru
Saint Lucia
Saint Vincent and the Grenadines
Trinidad and Tobago
Uruguay

EUROPE

Belarus
Belgium
Bulgaria
France
Germany
Greece
Hungary
Italy
Kosovo
Liechtenstein
Luxembourg
Macedonia
Montenegro
Norway
Poland
Russia
San Marino
Spain
Slovakia
Switzerland
Ukraine

Annex 10

Countries mandating SIM registration and are considering the implementation of Data Protection and/or Privacy Framework

AFRICA

Egypt
Kenya
Niger
Nigeria
Swaziland
Tanzania
Uganda
Zimbabwe

ASIA

Bahrain
Indonesia
Iraq
Jordan
Pakistan
Thailand

CENTRAL AND SOUTH AMERICA

Barbados
Brazil
Dominica
Ecuador
Honduras
Jamaica
Panama
Saint Kitts and Nevis

Annex 11

Countries mandating SIM registration but lack a Data Protection and/or Privacy Framework

AFRICA

Algeria
Botswana
Burundi
Cameroon
Central African Republic
Congo
Democratic Republic of Congo
Eritrea
Ethiopia
Guinea
Guinea-Bissau
Liberia
Libya
Mozambique
Rwanda
Sierra Leone
Somalia
South Sudan
Sudan
Togo

ASIA

Afghanistan
Bangladesh
Brunei Darussalam
Cambodia
Fiji
Laos
Lebanon
Mongolia
Myanmar
Nauru
North Korea
Palestine
Papua New Guinea
Samoa
Saudi Arabia
Sri Lanka
Syria
Timor-Leste
Tonga
Vanuatu

CENTRAL AND SOUTH AMERICA

Belize
El Salvador
Grenada
Guatemala
Guyana
Haiti
Suriname
Venezuela

Annex 12

Countries considering the implementation of SIM registration and have a Data Protection and/or Privacy Framework

Austria
Cyprus
Latvia
Netherlands
Paraguay
Philippines
Serbia

Annex 13

Countries considering the implementation of SIM registration and do not have a Data Protection and/or Privacy Framework

Namibia

gsma.com

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601