



Access to Mobile Services and Proof of Identity 2019:

Assessing the impact on
digital and financial inclusion





The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 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 the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

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

Follow the GSMA on Twitter: [@GSMA](https://twitter.com/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](https://twitter.com/GSMAM4d)

AUTHORS

Yiannis Theodorou (Director, Policy & Advocacy, Digital Identity, GSMA @yiathe)
Ken Okong'o (Manager, Policy & Advocacy, Digital Identity, GSMA)
Erdoo Yongo (Policy Analyst, Mobile for Humanitarian Innovation, GSMA)

Contents

1	Executive summary	2
2	Introduction and context	4
3	Methodology	5
4	Mobile penetration over the last decade	6
5	Access to identity and mobile: the policy linkages	10
6	Proof of Identity in humanitarian contexts: The impact on refugees' access to mobile	26
7	Conclusion	30
8	Annexes	32
	Annex 1 Selected country case studies: The identity, mobile and privacy landscape	33
	Annex 2 Select country case studies: Access to identity, mobile connectivity and financial services for persons of concern (PoC)	42
	Annex 3 Policy landscape, by country	46

01

Executive summary

This report is intended to update and build on the GSMA's first ever global research of its kind¹, published in early 2018, exploring correlations between people's access to formal identification, their ability to meet proof of identity regulations and the consequent impact on their ability to register for mobile connectivity and mobile money services.

Mobile continues to connect more people than any other communications platform. By the end of 2018 more than 5.1 billion individuals have a mobile subscription, amounting to 67 per cent of the total population (up from 66 per cent a year ago). The African continent still lags behind the rest of the world but unique mobile subscribers have grown by one percentage-point to 49 per cent. At a global level, 4G is expected to become the leading mobile network technology by number of connections², with the majority of those connections linked to prepaid Subscriber Identity Module (SIM) cards. In fact, the majority of mobile connections (75 per cent worldwide and 94 per cent across Africa) are based on a prepaid SIM card. Ninety per cent of these are active in countries where an acceptable proof of identity is required to register and use a SIM card in one's own name.

As of December 2018, an estimated 150 governments impose proof of identity requirements on individuals wishing to activate a SIM card to use mobile services. At the same time, the World Bank estimates³ that about one billion people worldwide lack any legal (State-issued or recognised) identification and are therefore at a higher risk of being digitally, socially and financially excluded. This is because for billions of people the mobile device is no longer just a tool for communication but has become the only means of accessing the internet and a plethora of life-enhancing services⁴, including financial, educational, health and utilities. As more economies undergo a digital transformation, these services will increasingly be available online and on the move. Consequently, individuals' ability to prove their identity (ID) in digital forms and via mobile networks will be essential⁵ in securing access to these life-enhancing services in their own right.

Key insights highlighted in this research report

Robust identity verification is still nascent in the context of mobile SIM registration: A number of studies by the World Bank suggest that an inclusive and robust⁶ digital ID ecosystem can offer significant benefits to private⁷ and public⁸ sector entities by enabling strong, remote verification of individuals' identification credentials which then unlocks access to a host of relevant services. Despite the high number of governments mandating mobile SIM card registration, only 11 per cent of these enable mobile network operators (MNOs) to verify customers' identification credentials against an approved government database to facilitate the accuracy of the validation process.

Millions of undocumented people are still financially excluded but mobile money offers a huge potential to bridge the gap: The impact of mobile money in supporting the financial inclusion of the world's underserved populations is well documented⁹. Due to the convenience, safety and affordability of transacting via mobile money over traditional financial institutions, the industry will continue to play a key role in bringing the 1.7 billion people who remain financially excluded into the formal financial sector¹⁰. However, while mobile money services are available in 90 countries worldwide¹¹, an estimated 456 million individuals across these countries may be 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.

Lack of official identification is disproportionately impacting women — especially those in low income countries — as well as forcibly displaced populations. As the World Bank's latest Global Findex survey shows, applying for mobile SIM card or mobile services is the most prevalent use of identification across all countries for both men and women. However this is also the use with the greatest gender gap indicating that many more women than men lack the required proof of ID to access mobile services. In addition, the humanitarian community is increasingly focused on how to ensure

beneficiaries are equipped with acceptable forms of identification which would allow them to access mobile connectivity and mobile money services in their own name. One hundred and seventy-three countries are hosts to 19.9 million refugees. Yet, 75 per cent of these countries legally require people to present an acceptable form of identification in order to register for a mobile SIM card. Similarly, 81 refugee-hosting countries offer mobile money services which could potentially be available to 54 per cent of all refugees (but for their ability to meet the KYC requirements for opening a mobile money account in their own name).

A significant number of countries lack a comprehensive privacy framework which impacts trust in the digital ID ecosystem: Legal frameworks that uphold consumers' privacy and data protection continue to play a key role in building trust within the digital ecosystem, especially as digital value chains become more complicated¹². A critical emerging question of concern for sustainable development in the digital ecosystem is whether adequate privacy and data protection frameworks exist to present mobile users with confidence and trust in adopting and using mobile based services linked to their identity. The GSMA found that only 61 per cent of countries mandating SIM registration have a Privacy and/or Data Protection framework in place — the same applies to 54 per cent of all African countries. While all these legal frameworks seek to meet mobile users' privacy needs and expectations¹³, their actual scope varies from country to country.

The development and pervasiveness of the wider mobile ecosystem and its catalytic role in accelerating countries' digital transformation, poses a number of challenging questions relating to the role of government policy in enabling individuals to access life-enhancing mobile services. As the reach of mobile connectivity and mobile financial services expands, modernised regulatory and policy options are required to cater for the needs of underserved populations in order to avoid the risk of social, digital and financial exclusion.

1. GSMA, Access To Mobile Services and Proof of Identity: Global Policy Trends, Dependencies and Risks <https://bit.ly/2DYV9LS>
 2. GSMA's Mobile Economy 2018: <https://www.gsma.com/mobileeconomy/>
 3. <http://id4d.worldbank.org/global-dataset>
 4. GSMA's Mobile Economy: Sub-Saharan Africa 2018: <https://www.gsma.com/mobileeconomy/sub-saharan-africa/>
 5. GSMA, Access To Mobile Services and Proof of Identity: Global Policy Trends, Dependencies and Risks <https://bit.ly/2DYV9LS>

6. World Bank, G20 Digital Identity Onboarding accessed at https://www.gpfi.org/sites/default/files/documents/G20_Digital_Identity_Onboarding_WBG_OECD.pdf
 7. World Bank, Private Sector Economic Impacts from Identification Systems, 2018 accessed at <http://pubdocs.worldbank.org/en/219201522848336907/PrivateSectorEconomicImpact-sIDSystems-Web.pdf>
 8. World Bank, Public Sector Savings and Revenue from Identification Systems, accessed at <http://pubdocs.worldbank.org/en/745871522848339938/PublicSectorSavingsandRevenue-IDSystems-Web.pdf>
 9. World Bank Group (2014) *Global Financial Development Report 2014: Financial Inclusion*
 10. World Bank Group (2018) *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*
 11. 2017 State of the Industry Report on Mobile Money
 12. GSMA, Data Value Chain: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/07/GSMA_Data_Value_Chain_June_2018.pdf
 13. GSMA's Mobile Privacy Principles: <https://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacyprinciples20121.pdf>

02

Introduction and context

The number of unique mobile subscribers surpassed 5.1 billion at the end of 2018¹⁴, largely driven by developing countries including India, China, Pakistan, Indonesia and Bangladesh, as well as the Sub-Saharan Africa and Latin America regions. While there are around nine billion mobile connections in total¹⁵, the speed of growth, particularly in the developed world, is slowing. However, significant new growth is expected to occur in mobile data¹⁶ use, largely driven by mobile internet access. In fact, the number of mobile internet users is increasingly becoming a key metric of mobile value and is estimated to reach the five billion mark by 2025¹⁷. Mobile technology is currently driving a significant (digital) transformation in many development-related sectors including health, education, financial inclusion, humanitarian assistance and food security. Thus, mobile offers the opportunity to leapfrog over more traditional methods of service delivery to achieve greater impact¹⁸, while the mobile industry was the first in the world to commit¹⁹ to the delivery of all UN's Sustainable Development Goals (SDGs)²⁰.

A prerequisite for mobile-enabled services to achieve their true potential is ensuring that individuals have access to them in their own right. A key determinant of mobile access in the majority of the world is the legal requirement to present proof of identity, as demonstrated by the GSMA's first global research on this topic in 2018²¹. Our

latest research found that SIM registration is now mandatory in 150 countries. Such policies continue to present challenges to the more disadvantaged and underserved groups of society, particularly the one billion people worldwide who, according to the World Bank, have no official means to prove their identity²². Women and forcibly displaced persons (FDP) make up a large portion of this figure as they are frequently unable to fulfil the necessary proof of identity criteria²³ and cannot therefore access mobile communications and mobile money services in their own name.

While the growth of the mobile ecosystem over the last decade is undisputed²⁴, widespread access to mobile-enabled services requires continued policy modernisation that keeps pace with the evolving digital ecosystem. Digitally proving one's identity is at the heart of most online transactions²⁵, and there is a need for accurate and secure identification systems. In order to deliver services, many companies in the digital ecosystem — including financial, aviation or digital e-commerce platforms — are required to verify or authenticate the identities of their users at a point in the customer lifecycle²⁶. Given that the source of verifications for these transactions is typically a government-issued or recognised identification credential²⁷, where such credentials are unavailable, individuals may be excluded from large portions of the formal digital (and mobile) economy²⁸.

14. GSMA Intelligence: <https://www.gsmainelligence.com/>

15. Ibid.

16. GSMA's Mobile Economy, 2018: <https://www.gsma.com/mobileeconomy/>

17. Ibid.

18. GSMA's 2016 Mobile Industry Impact Report: SDGs https://www.gsma.com/betterfuture/wp-content/uploads/2016/09/UN_SDG_Report_FULL_R1_WEB_Singles_LOW.pdf

19. <https://www.gsma.com/newsroom/press-release/mobile-industry-accelerating-delivery-of-sustainable-development-goals/>

20. ITU's State of Broadband 2018: <https://www.itu.int/pub/S-POL-BROADBAND19>

21. GSMA, Access To Mobile Services and Proof of Identity: Global Policy Trends, Dependencies and Risks <https://bit.ly/2DYV9LS>

22. World Bank ID4D

23. GSMA, Refugees and Identity: Considerations for Mobile Enabled Registration and Aid Delivery <https://www.gsmainelligence.com/research/?file=1cb984aae8f279c617fb30b-151bad5a8&download>

24. 2017 State of the Industry Report on Mobile Money

25. World Bank's Private Sector Economic Impacts from Identification Systems: <http://pubdocs.worldbank.org/en/219201522848336907/PrivateSectorEconomicImpactsIDSys-tems-Web.pdf>

26. Ibid.

27. Ibid

28. A Joint World Bank Group – GSMA Secure Identity Alliance Discussion Paper: <http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUB-LIC-WB-GSMA-SIADigitalIdentity-WEB.pdf>

03

Methodology

Building on the GSMA's original research²⁹ on this topic and an earlier white paper published in 2016³⁰, this report seeks to offer an updated global perspective and identify trends between mandatory SIM registration policies, the official identification coverage and the level of mobile penetration across different markets. The case studies presented and insights deduced are largely based on analysis from desk-research, various academic and industry studies and other research that the GSMA had commissioned or supported (e.g. with the United Nations High Commissioner for Refugees (UNHCR)³¹) over the last year.

Developments across the globe on personal data protection laws and mandatory SIM registration were extensively reviewed, primarily relying on the websites of national sector regulators, the International Telecommunications Union (ITU), World Bank, UNHCR, government, media and civil society reports.



29. GSMA's Access to Mobile Services and Proof of Identity: Global Policy Trends, Dependencies and Risks <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf>

30. GSMA's Mandatory Registration of Prepaid SIM cards: Addressing Challenges Through Best Practices https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016-Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

31. UNHCR, 2019 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>

32. GSMA's Mobile Connections: <https://www.gsmainelligence.com/metrics/3/1630/data/?report=5bfbfed503a98>

04

Mobile penetration over the last decade

The number of mobile connections globally as at the end of 2018 reached nine billion, an eight per cent increase from 2017³² and almost doubled from a decade ago, both in terms of number of unique subscribers but also in terms of total number of mobile connections (See Figures 4.1 to 4.4). Mobile broadband is currently seen to complement fixed broadband but is shifting to becoming a sole and dominant mode of internet access in many countries³³. In fact, an additional one billion people have accessed the internet via mobile in the last four years³⁴.

It is estimated that mobile internet subscriptions will reach five billion in 2025³⁵. Despite this remarkable progress, significant connection barriers still exist preventing the ubiquity of mobile internet³⁶. Though these barriers vary from geography to geography, they tend to relate to infrastructure development, cost of mobile enabled services, consumer readiness, relevance of digital content and last but not least, individuals' ability to meet proof of identity requirements to register for a mobile SIM card.



33. Ibid.
 34. GSMA's Connected Society: State of Mobile Internet, 2018 <https://www.gsmainelligence.com/research/?file=c0bcc185be555f77478a8fd986ea318&download>
 35. GSMA's Mobile Economy, 2018: <https://www.gsma.com/mobileeconomy/>
 36. GSMA's Connected Society: State of Mobile Internet, 2018: <https://www.gsmainelligence.com/research/?file=c0bcc185be555f77478a8fd986ea318&download>
 37. GSMA's Mobile Economy 2018: <https://www.gsma.com/mobileeconomy/>

4.1 Mobile penetration in 2008 and 2018 – Unique subscribers

Figure 4.1

Unique mobile subscribers as a proportion of total population (2008)

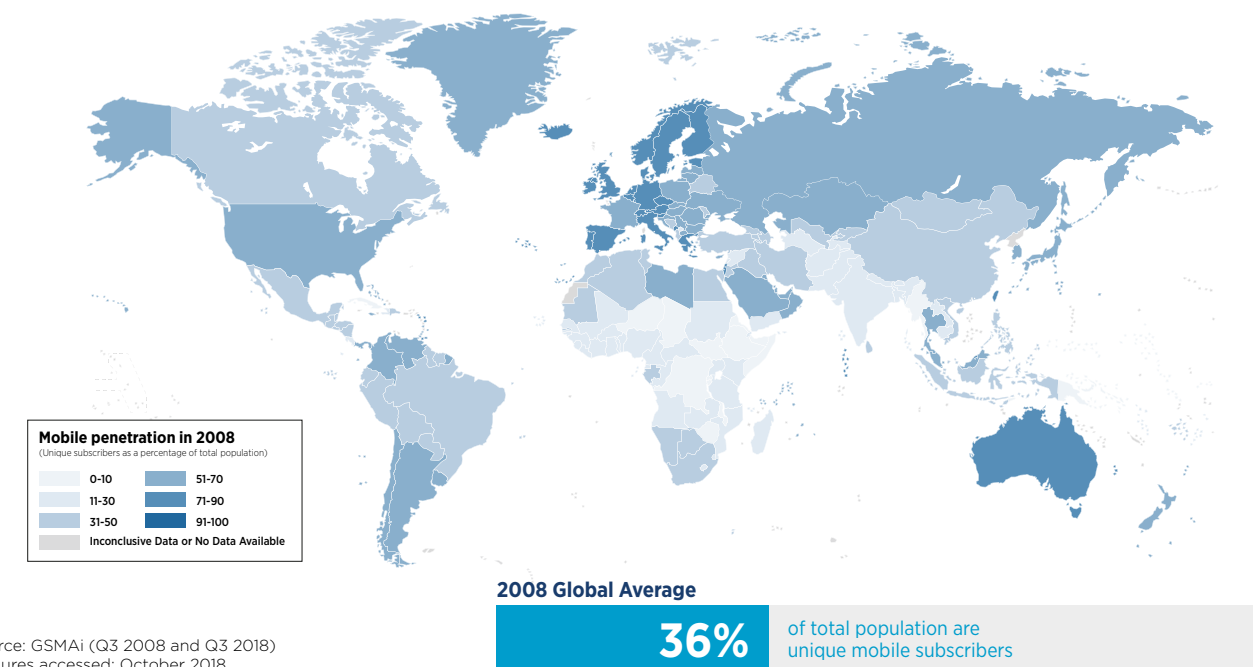
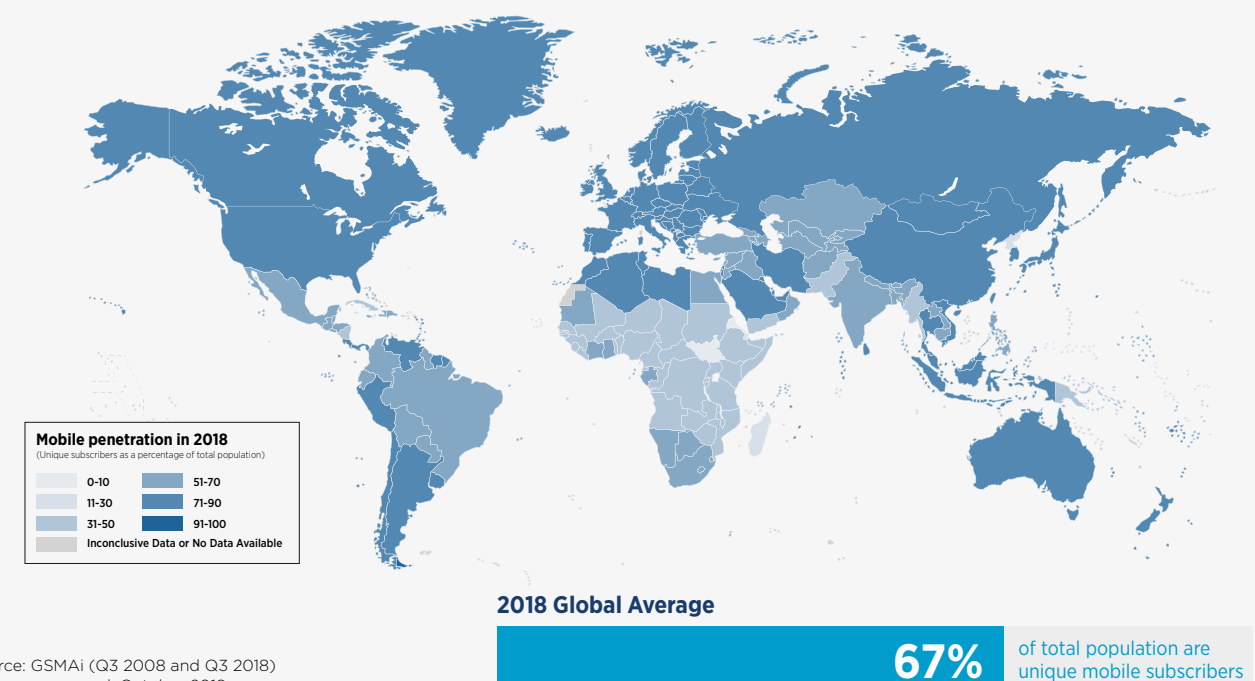


Figure 4.2

Unique mobile subscribers as a proportion of total population (2018)



4.2 Mobile penetration in 2008 and 2018 – Total connections

Figure 4.3

Aggregate mobile connections as a proportion of total population (2008)

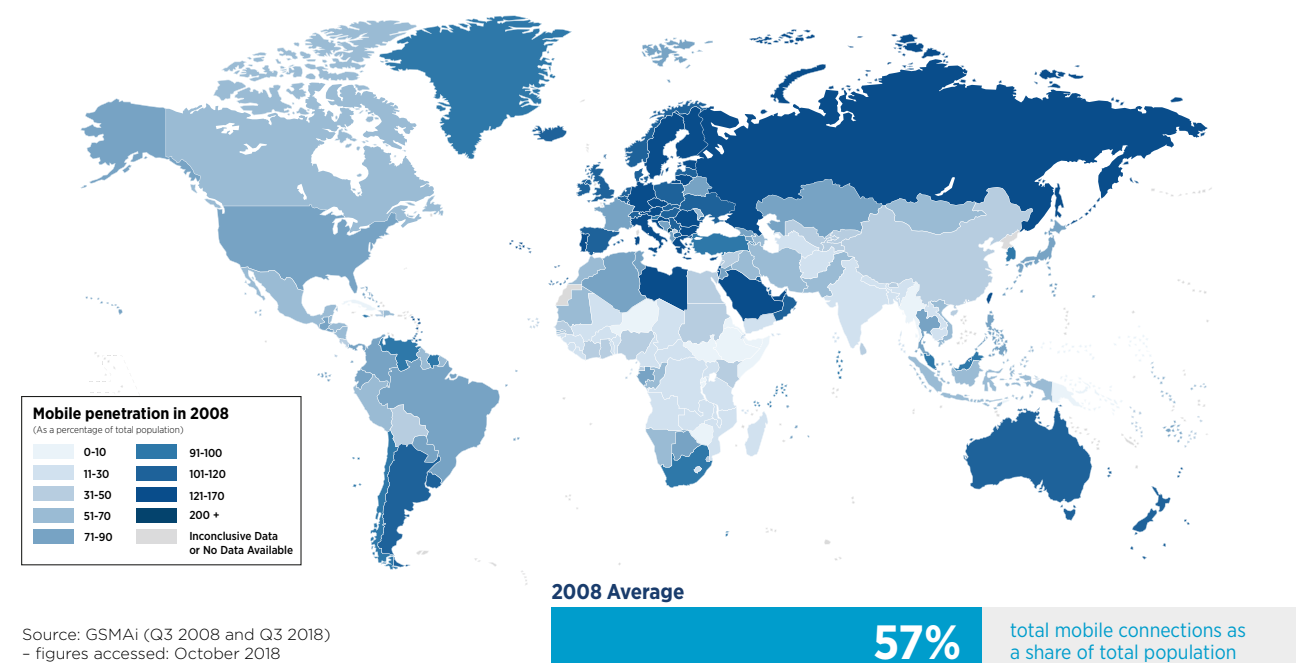
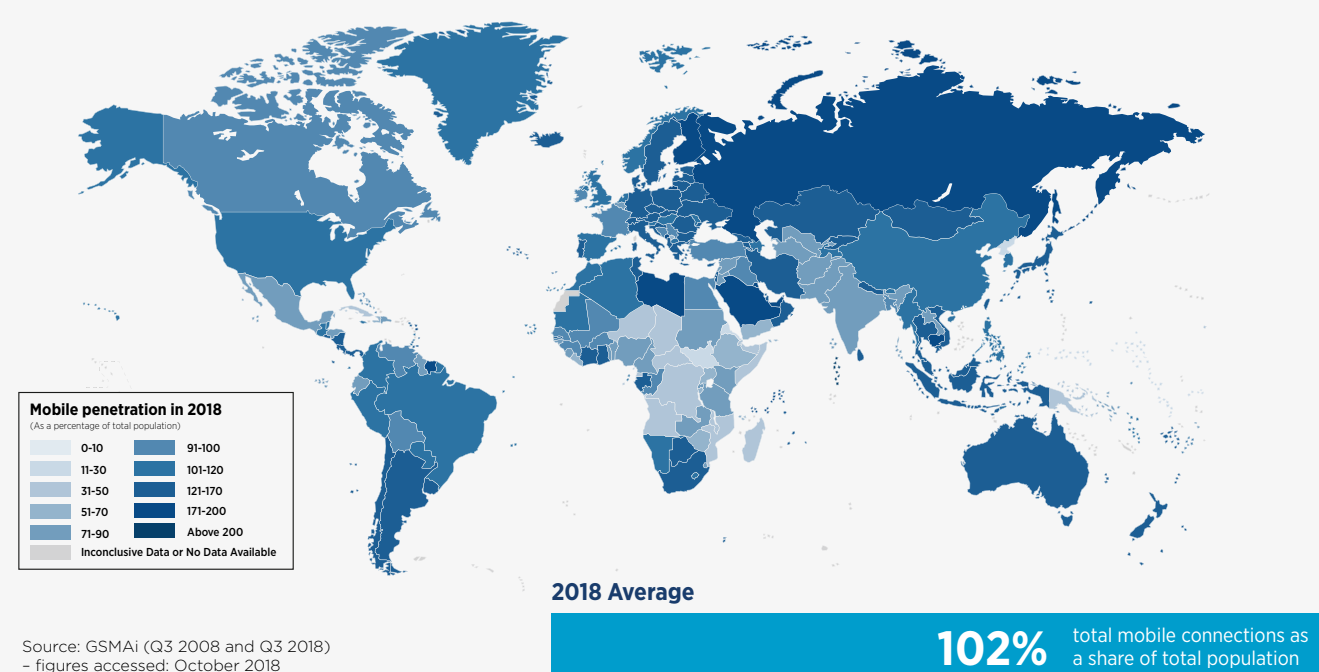


Figure 4.4

Aggregate mobile connections as a proportion of total population (2018)



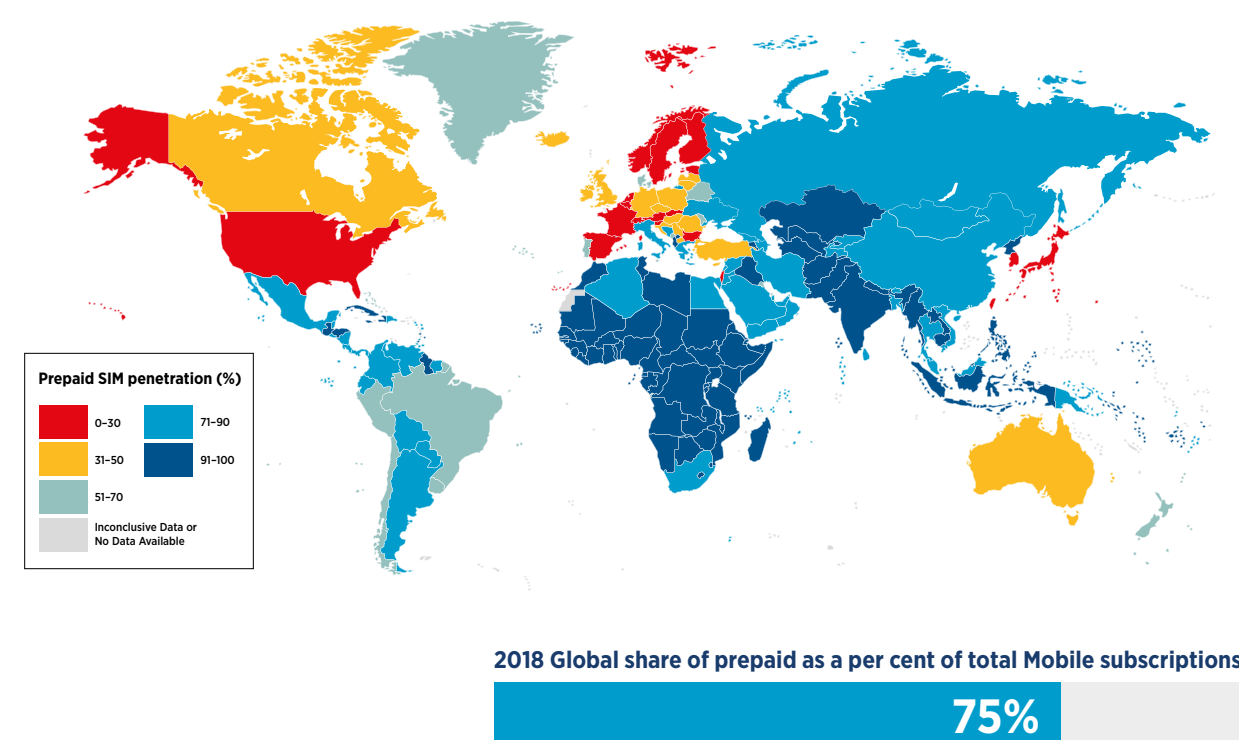
4.3 Penetration of prepaid SIM cards

Unlike post-paid SIM cards, which are usually linked to fixed term contracts with a mobile network operator and which tend to involve creditworthiness checks, prepaid SIM cards are simpler to obtain and remain the preferred option for mobile users seeking more flexible options. The average share

of mobile subscriptions (excluding Machine-to-Machine (M2M)) that are prepaid across Africa is 94 per cent, Central America is 87 per cent, Asia is 80 per cent, Southern America is 70 per cent, Europe is 52 per cent, and North America is 21 per cent.

Figure 4.5

Share of prepaid connections as a percentage of total mobile subscriptions



05

Access to identity and mobile: The policy linkages

The widespread use and applications of mobile technology across the globe has been remarkable over the last decade. The impact of mobile is also evident across all the 17 United Nations (UN) SDGs and can be seen in the collaborative works of governments and MNOs aligning their business plans with the SDGs and integrating the SDGs into their core strategies³⁷. These commitments have been accompanied by the development and adoption of associated policies, regulations and practices in the mobile industry.

5.1 Countries implementing SIM registration

This section focuses on the impact of proof of identity requirements for the registration of SIM cards to access mobile services. Where such policies are implemented, users are required to supply personal information such as their name, national identification number, address, photograph, fingerprints, among other biometric characteristics, as a set of pre-requisites to register or activate

mobile SIM cards. As a standard practice, existing users who fail to register their SIMs within a government-mandated time period face network disconnection³⁸, resulting in loss of access to mobile services. The GSMA found that mandatory SIM registration policies are implemented in 150 countries as of December 2018.

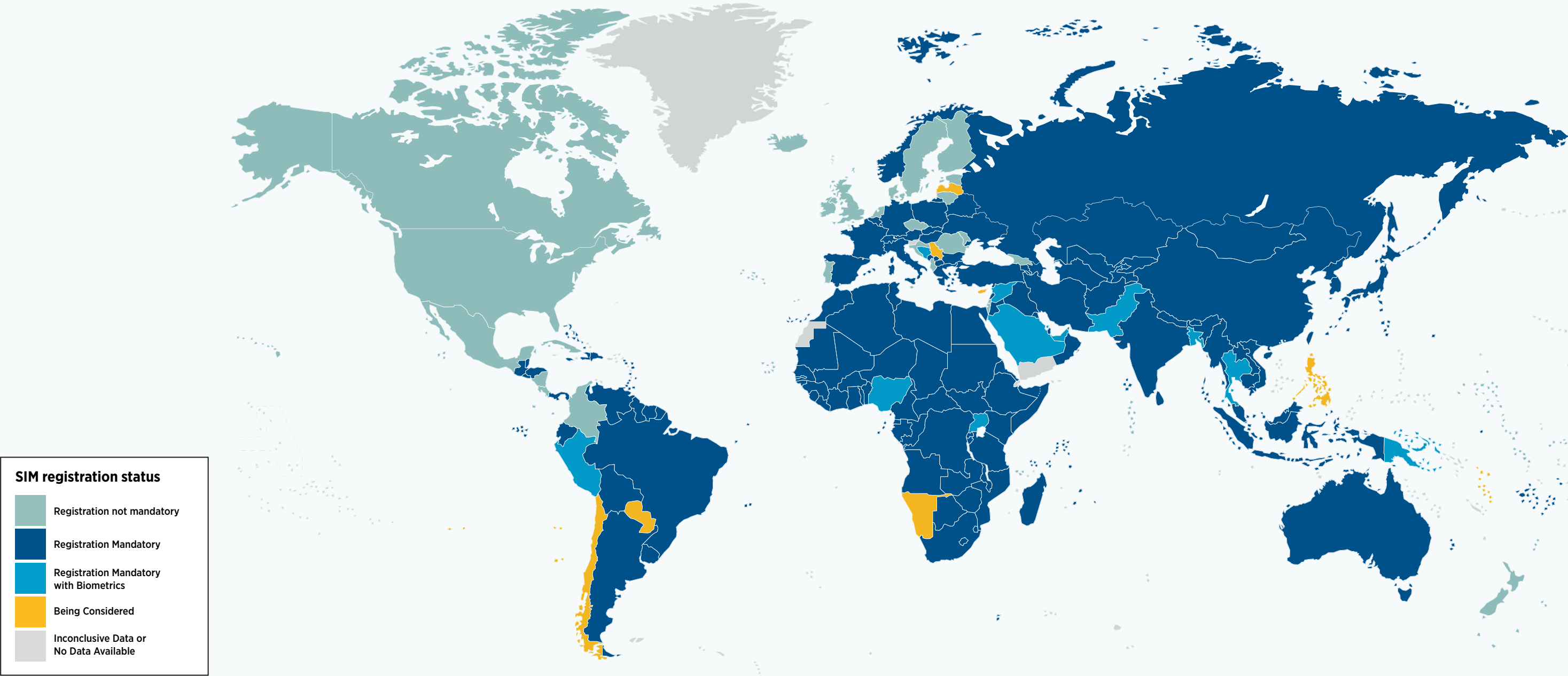


38. The Rise of African SIM registration by Donovan and Martin: <https://firstmonday.org/ojs/index.php/fm/article/view/4351/3820>

39. See Annex 3

Figure 5.1

Status of SIM registration policies (2019)



Source: GSMA research from publicly available information (December 2018)

5.2 SIM registration implementation models

The GSMA found that mobile users in at least 150 countries³⁹ are required to prove their identity in order to register and/or activate their prepaid SIM cards; governments take different approaches to implementing SIM registration policies. The GSMA has grouped these approaches into the following three categories⁴⁰:

► Capture and Store

MNOs are required to capture and keep a record of a set of personal information about the SIM user. The required information varies from jurisdiction to jurisdiction. As of December 2018, about 85 per cent of the countries mandating SIM registration follow this approach.

► Capture and Share

MNOs are required to proactively capture and share the SIM user's personal information with the government or regulator, rather than upon demand. As of December 2018, roughly four per cent of the countries mandating SIM registration follow this approach.

► Capture and Validate

MNOs are required and enabled to validate their customers' identification credentials against a central government database (usually maintained by a Government Authority or regulator). As of December 2018 only 16⁴¹ of these countries (11 per cent) mandating SIM registration follow this approach while 11 countries (seven per cent) require MNOs to use biometric-authentication processes when registering their prepaid SIM customers.

It should be noted that where jurisdictions do not have credible databases against which verification can be conducted, the approach to proof of identity varies across the country. For example, in some countries attestation letters from employers or village elders, as in the case of Nigeria⁴², are acceptable forms of identification for SIM registration. However, such approaches are often criticised for being less robust and leave room for identity theft. It is not surprising therefore that governments, international organisations, such as the World Bank, and industry associations such as the GSMA seek to support partnerships⁴³ between the public and private sectors with a view to developing more efficient, innovative and robust digital identity ecosystems.

40. GSMA, Proof of Identity and Access To Mobile Services 2018: <https://bit.ly/2DYV9LS>

41. See Annex 3

42. *Traditional Rulers and Local Government in Nigeria: a Pathway to Resolving the Challenge*. O.Osemwota and D.A. Tonwe, 2013.

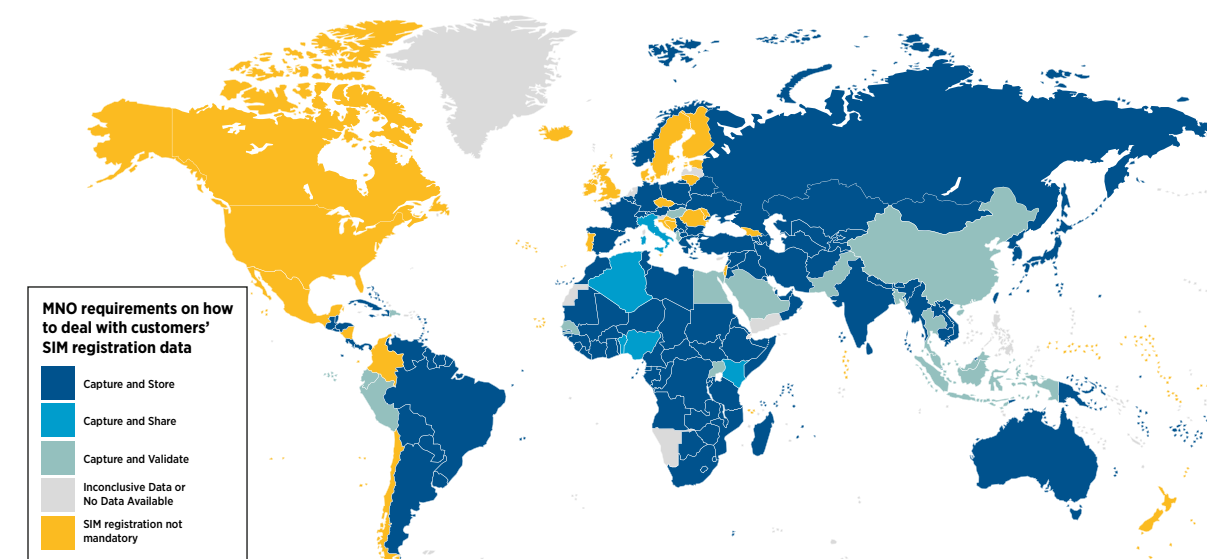
43. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation <http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUB-LIC-WB-GSMA-SIADigitalIdentity-WEB.pdf>

44. World Bank's ID4D Data: Global Identification Challenge by the Numbers : <http://id4d.worldbank.org/global-dataset>

Figure 5.2

Source: GSMA research from publicly available information (December 2018)

Type of mandatory SIM registration policy, by country



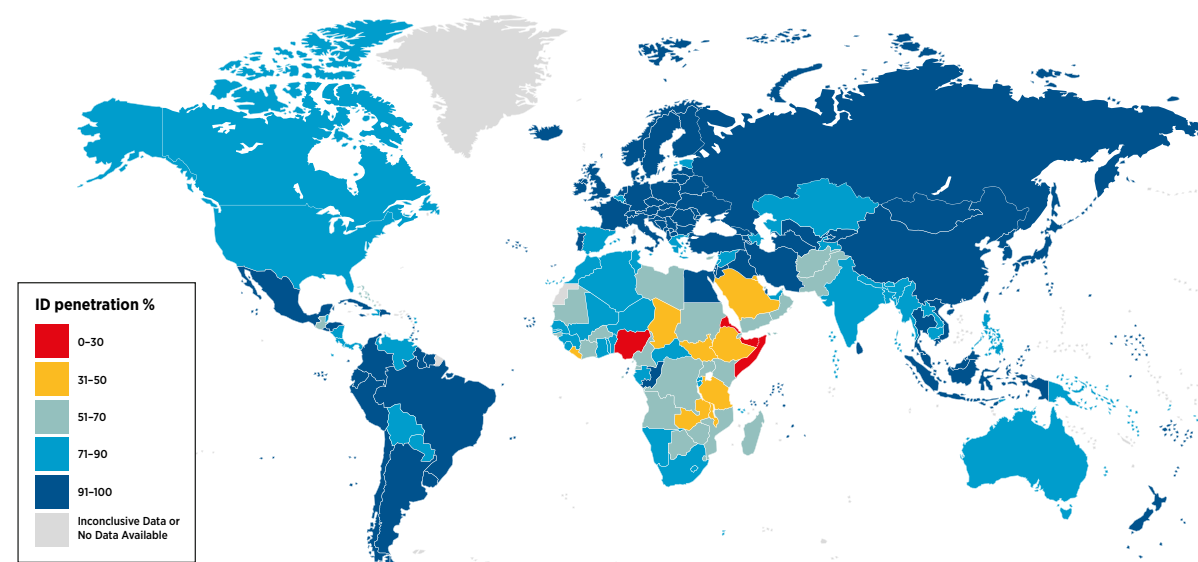
5.3 Access to a government-recognised proof of identity

As noted earlier, the World Bank estimates that about one billion people still lack an official proof of identity⁴⁴. 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 5.3 below provides a global

snapshot showing the proportion of each country's total population that is officially registered. This is based on the World Bank's 2018 Identification for Development (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 identification⁴⁵.

Figure 5.3

Share of total population estimated to have an official form of identification (2018)



Source: World Bank Identification for Development (ID4D) Dataset⁴⁶, 2018

Focus on Africa

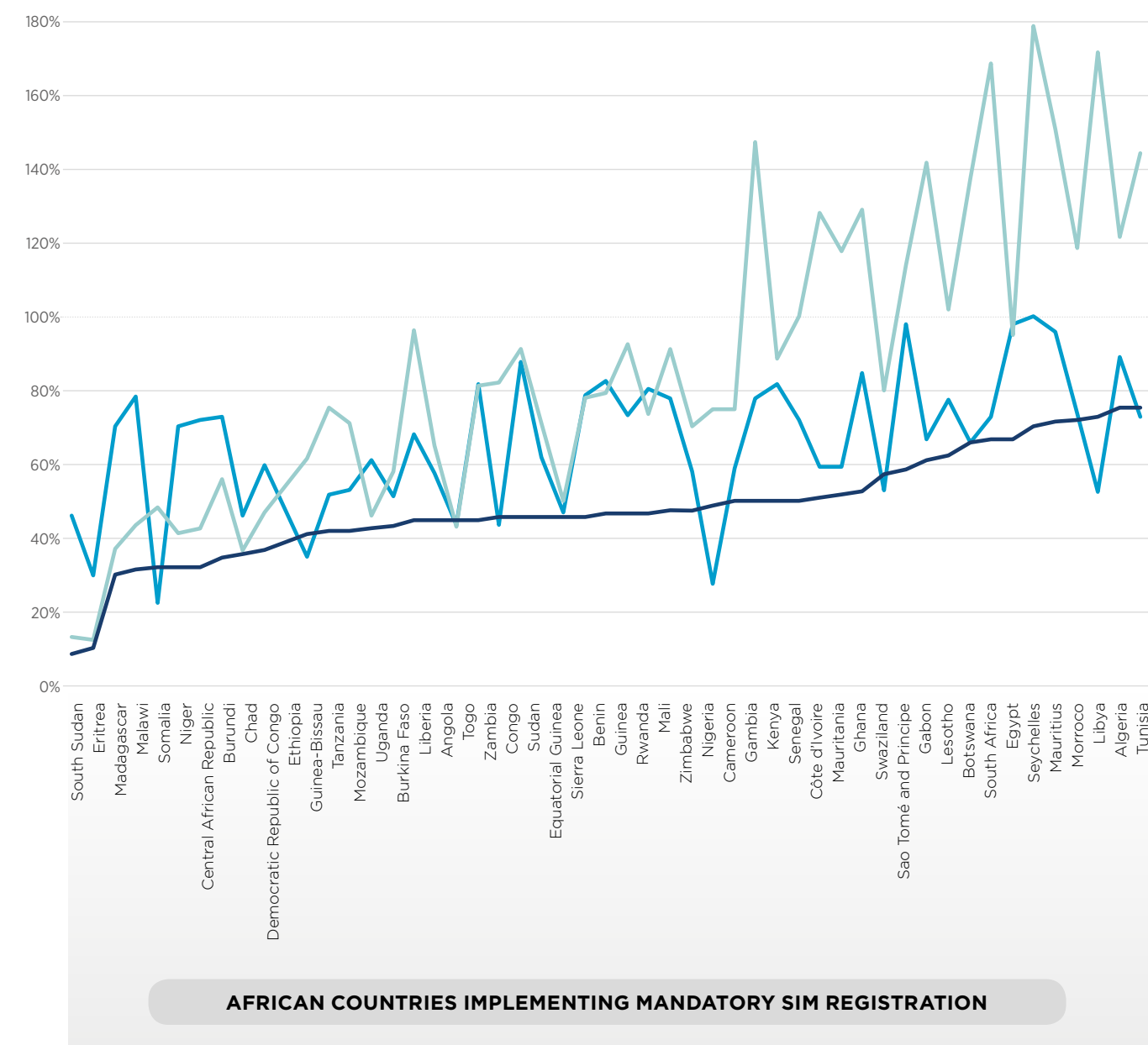
Figure 5.4 illustrates the relationship between official identification coverage and mobile penetration across African countries where SIM registration is mandated. In six markets (Nigeria, Somalia, Ethiopia, Swaziland, Zambia and Angola), it appears there are more people with a unique mobile subscription than an official proof of identity.

This may present an opportunity for governments in Africa to partner with local MNOs to expand ID coverage by leveraging their reach and nationwide retail presence (e.g. by supporting enrolment efforts, public awareness campaigns etc). This model is currently being explored in Nigeria.

Figure 5.4

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

Percentage of population



45. As the World Bank explains in its ID4D dataset, 'a number of caveats about the estimates should be kept in mind. First, the global (1 billion) estimate of the unregistered population is based on data from 151 economies. The inclusion criteria is explained in the notes section in the methodology. Second, although we make every effort to use the most up-to-date information, the data on which the country estimates for the unregistered population rely may be several years old. Third, voter registration data is used as a proxy indicator for national ID coverage of adults in 120 economies where national ID coverage data are not available. Voter registration data excludes persons who choose not to or are unable to register to vote (e.g. non-nationals)'. See: <https://data.worldbank.org/data-catalog/id4d-dataset>

46. accessed at <https://data.worldbank.org/data-catalog/id4d-dataset>

47. The Global Findex Database, 2017 <http://id4d.worldbank.org/global-dataset>

Source: GSMA Intelligence, Market Penetration - Q3 2018 (Accessed November 2018) and The World Bank, ID4D 2018 (number of registered individuals as a % of the population, taken as a proxy for identity penetration)

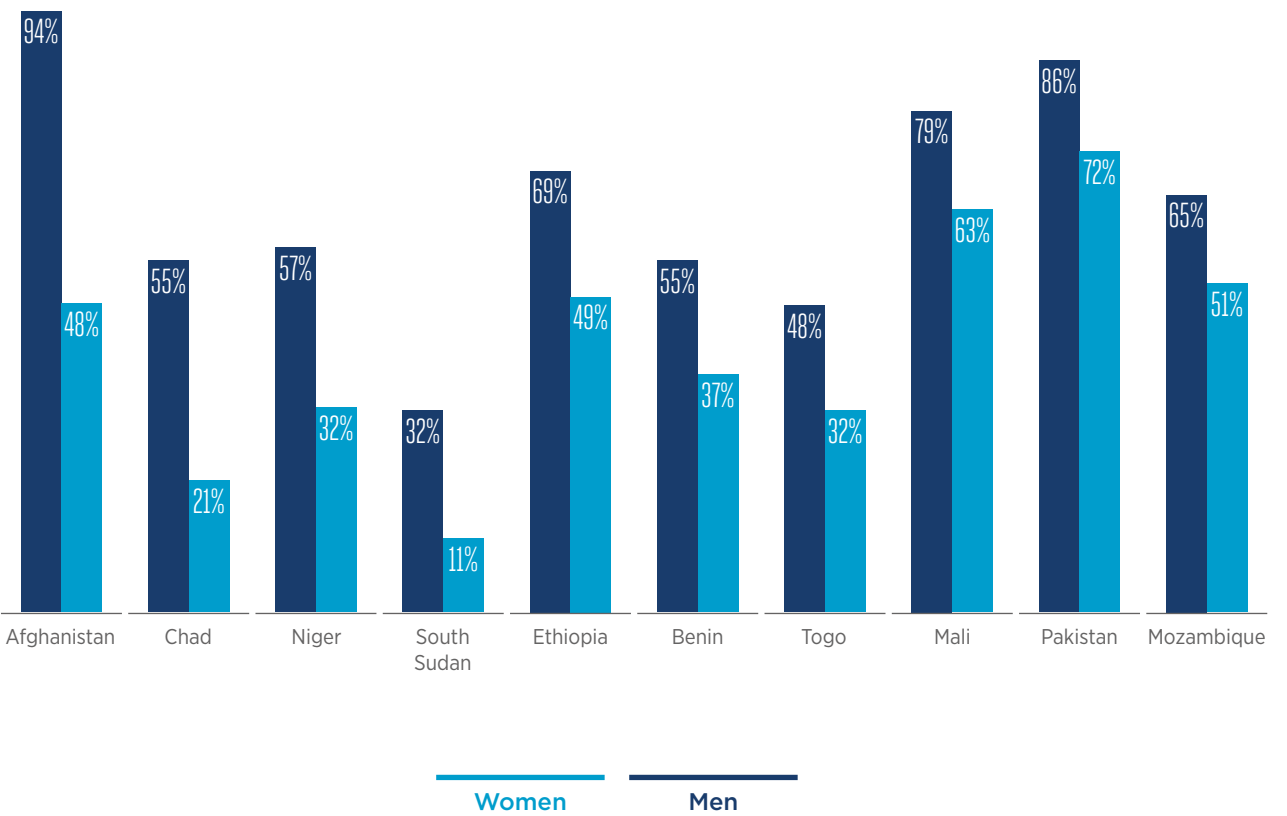


5.4 Proof of identity and mobile: The gender dimension

Research shows that lack of official identity disproportionately impacts women compared to men⁴⁷. In Afghanistan — the country with the largest gender gap in identity ownership — 94 per cent of men possess an identity card, compared to only 48 per cent of women⁴⁸ (see Figure 5.5). Eight of the 10 countries with the largest gender gap in identity ownership are in Sub-Saharan Africa. On average, 71 per cent of men in Sub-Saharan Africa have an ID compared to 63 per cent of women⁴⁹.

Figure 5.5

Countries with the largest gender gap in identity ownership



Source: The Global Findex Database, 2017⁵⁰

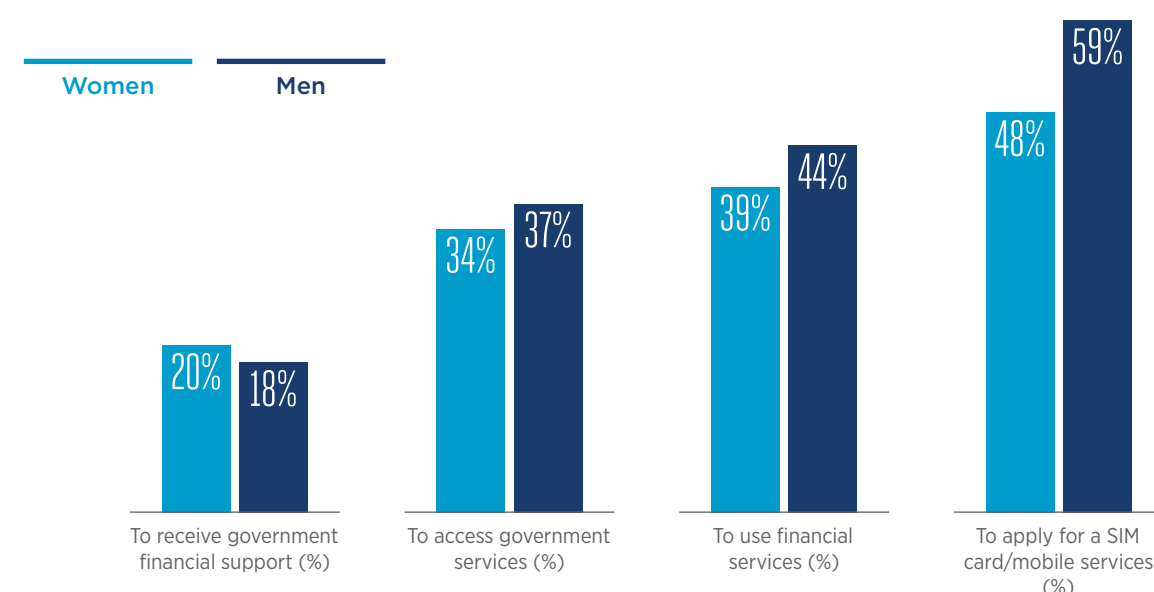
48. Ibid
49. Ibid.
50. Ibid
51. The World Bank and ID4D collected economy-level aggregates on the share and number of the population without a foundational/national ID, based on surveys covering over 100,000 people in 97 economies—representing 74 per cent of the world’s population

Registering for a mobile service is the most prevalent use of identification among both men and women

The World Bank's 2017 FINDEX survey gathered data from several countries on the different services people use their official identification to access⁵¹. (See Figure 5.6)

Figure 5.6

How men and women use their national ID card



Source: The Global Findex Database, 2017⁵² (Gender disaggregated responses to 'Have you ever used your national ID card to do any of the following?')

The survey showed that applying for mobile SIM card or mobile services is the most prevalent use of identification across all countries for both men and women. However, the overall gender gap is also highest in relation to the use of identity to apply for a SIM card or mobile services. Across the countries surveyed, 59 per cent of men used their identity card to apply for a SIM card or mobile services. Against 48 per cent of women. The gender gap in the use of ID to apply for a SIM card or mobile services is highest in African markets (67 per cent of men against 55 per cent of women)⁵³.

On average, men are more likely than women to use their identity card to access and use financial, government and mobile services⁵⁴. The only instance where women were more likely than men to use their ID to access a service was in the context

of receiving government financial support — though the average gender difference across all surveyed markets was only two per cent.

Men (37 per cent) were more likely than women (34 per cent) to use their identity card to access government services. The gender gap in relation to the use of identity to access government services was largest in Asia.

The gender gap is higher in the use of ID for registering for financial services and applying for a SIM card or mobile services. Forty-four per cent of men against 39 per cent of women said they use their ID to access financial services⁵⁵. The gap was highest in Africa and the Caribbean and Latin America where the difference in male and female use of ID to access financial services was seven percentage points.



5.5 Proof of identity and mobile: The financial inclusion context

Mobile money services have revolutionised and increased the reach of financial services across the globe. They have also proven to reduce costs, improve transparency and create an opportunity for people to be financially empowered⁵⁶. Due to the convenience, safety and affordability of transacting via mobile money over traditional financial institutions, the industry will continue to play a key role in bringing the 1.7 billion people who remain financially excluded into the formal financial sector. So far, mobile money services have reached just over 690 million registered mobile money accounts across 90 countries at the end of 2018⁵⁷.

To register customers for a mobile money account, all Financial Service Providers (FSPs) — including Mobile Financial Service (MFS) Providers — need to comply with Customer Due Diligence (CDD) requirements, commonly referred to as Know Your Customer (KYC). KYC requirements for financial

services tend to be mandated by Central Banks and are often separate to those for SIM registration which are generally imposed on mobile operators by telecommunications regulators⁵⁸.

Figure 5.7 illustrates the level of identification coverage among the eligible population (usually above 16 years old) in countries where mobile money services are offered. It demonstrates that a significant proportion of the population in these countries who still lack an official form of identification⁵⁹ face a higher risk of being financially excluded even where mobile money services are available in their countries. We estimate that 456 million persons across the 90 countries where mobile money services are available still face a risk of financial exclusion due to their inability to meet the KYC requirements for opening mobile money accounts in their own names⁶⁰.

52. <http://id4d.worldbank.org/global-dataset>

53. Ibid.

54. Ibid.

55. Ibid.

56. GSMA's Mobile Money : Competing with Informal Channels To accelerate Digitisation of Remittances: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/05/Mobile_Money_Competing_with_informal_channels_to_accelerate_the_digitisation_of_remittances.pdf

57. GSMA's 2017 State of Industry Report on Mobile Money: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/GSMA_State_Industry_Report_2018_Ex-Sum_WEBv1.pdf

58. 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>

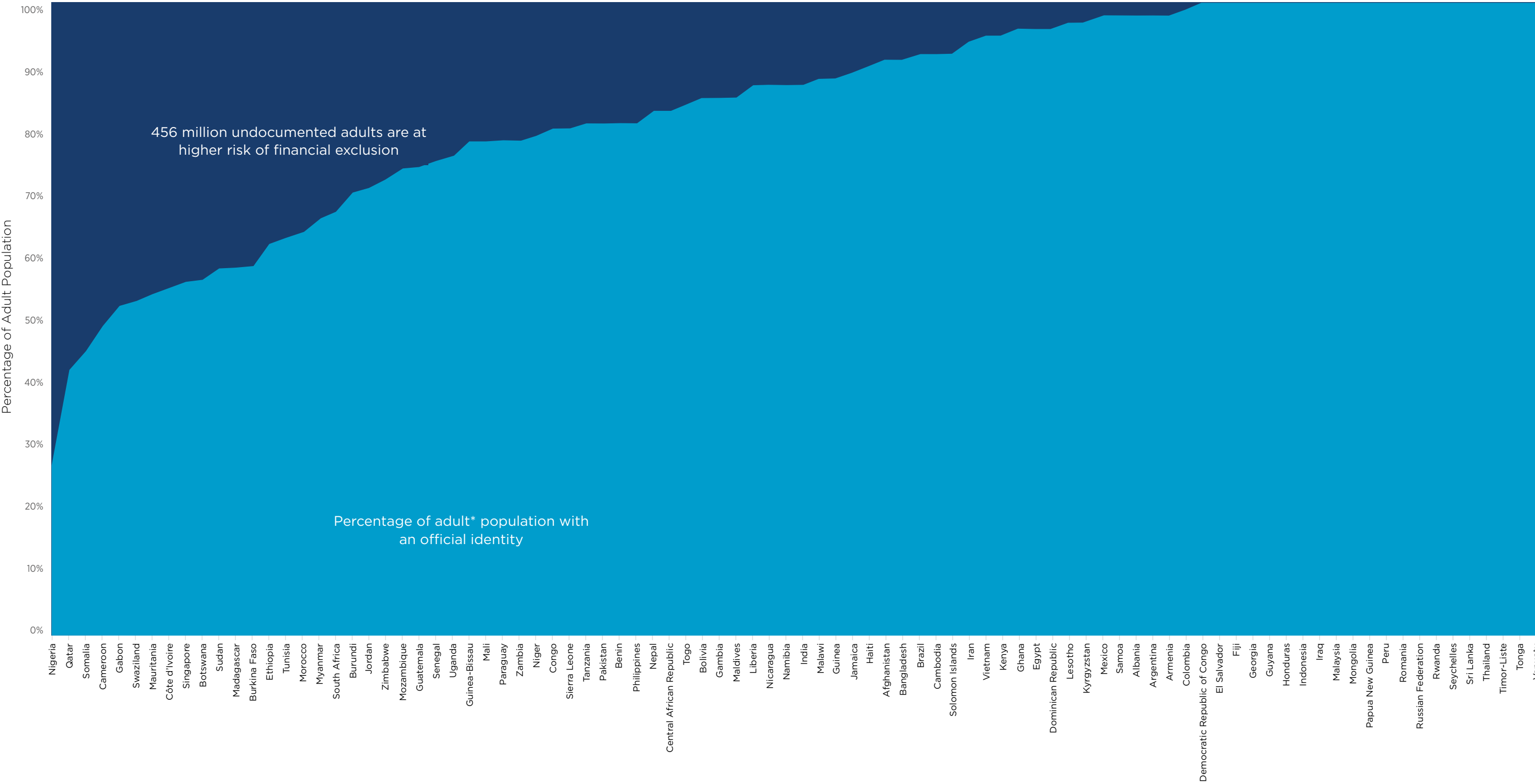
59. World Bank's ID4D Data: Global Identification Challenge by the Numbers: <http://id4d.worldbank.org/global-dataset>

60. GSMA's Mobile Money Policy and Regulatory Handbook: <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/GSMA-Mobile-Money-Policy-Handbook-2018.pdf>

Figure 5.7

Identification coverage in countries where mobile money services are available

Source: The World Bank ID4D 2018 and GSMA



COUNTRIES WHERE MOBILE MONEY SERVICES ARE AVAILABLE

COUNTRIES WHERE MOBILE MONEY SERVICES ARE AVAILABLE

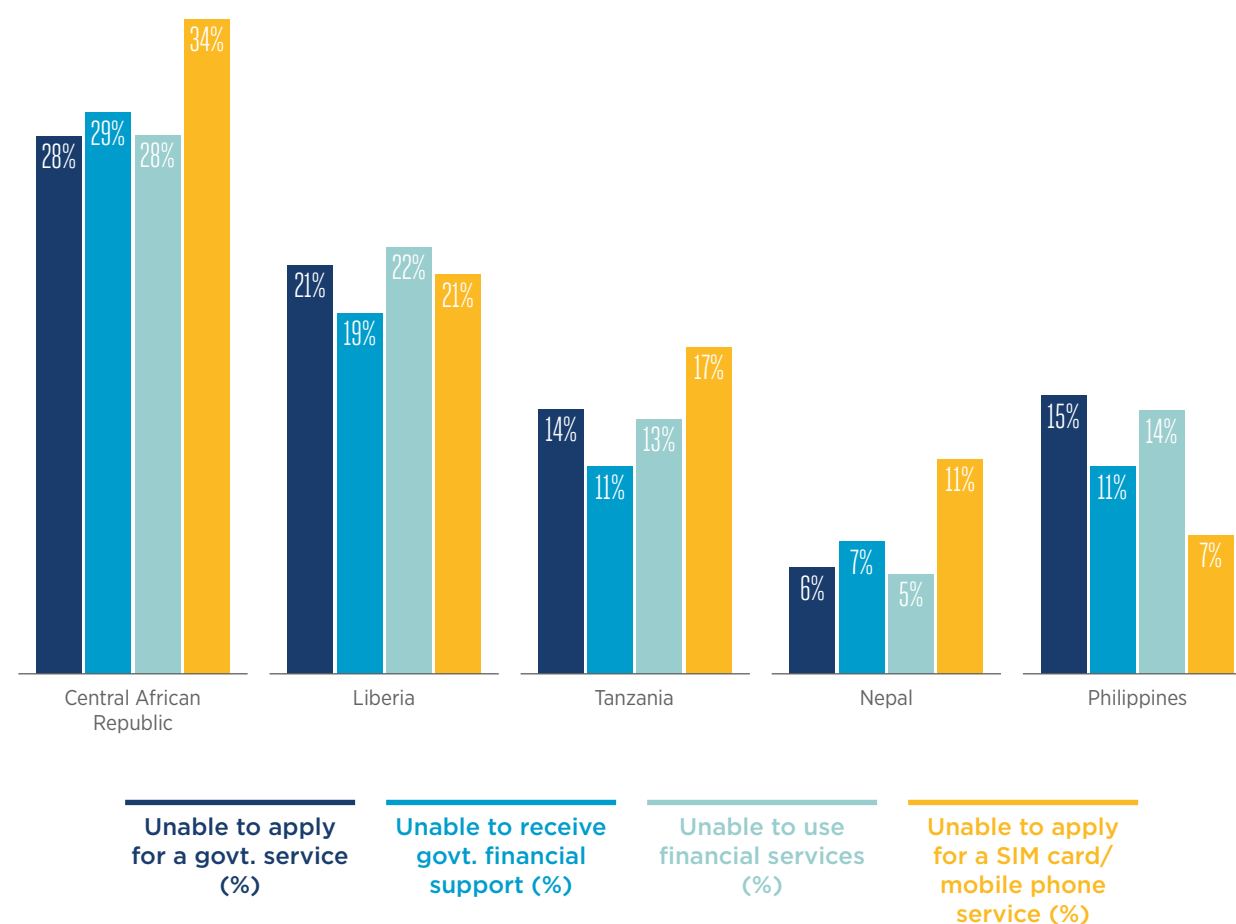
In the 2017 Findex survey, the World Bank posed the question ‘Have you ever not been able to do any of the following because you did not have the necessary identification documents?’ to participants in five territories — Central African Republic, Liberia, Tanzania, Nepal, and Philippines⁶¹. The results are shown below in Figure 5.8.

People in Central African Republic, Nepal and Tanzania felt the greatest impact in lacking the necessary identification when applying for a SIM

card or mobile services. Eleven per cent of people in Nepal, 17 per cent of people in Tanzania and 34 per cent of people in Central African Republic were unable to apply for a SIM card or mobile services because they were not in possession of the necessary identification. Respondents in Liberia felt the impact of lack of access to necessary documentation most when attempting to access financial services. While in the Philippines lack of access to necessary documentation prevented most individuals from applying for government services.

Figure 5.8

How the lack of identification impacts people’s lives



Source: The Global Findex Database, 2017 (Country-level responses to ‘Have you ever not been able to do any of the following because you did not have the necessary identification documents?’)

61. Note: Only respondents in economies with no NID system or one with very limited coverage were asked the question whether they had ever not been able to do the activities/trans-actions listed above due to not having the necessary documents.

5.6 Data protection and privacy frameworks

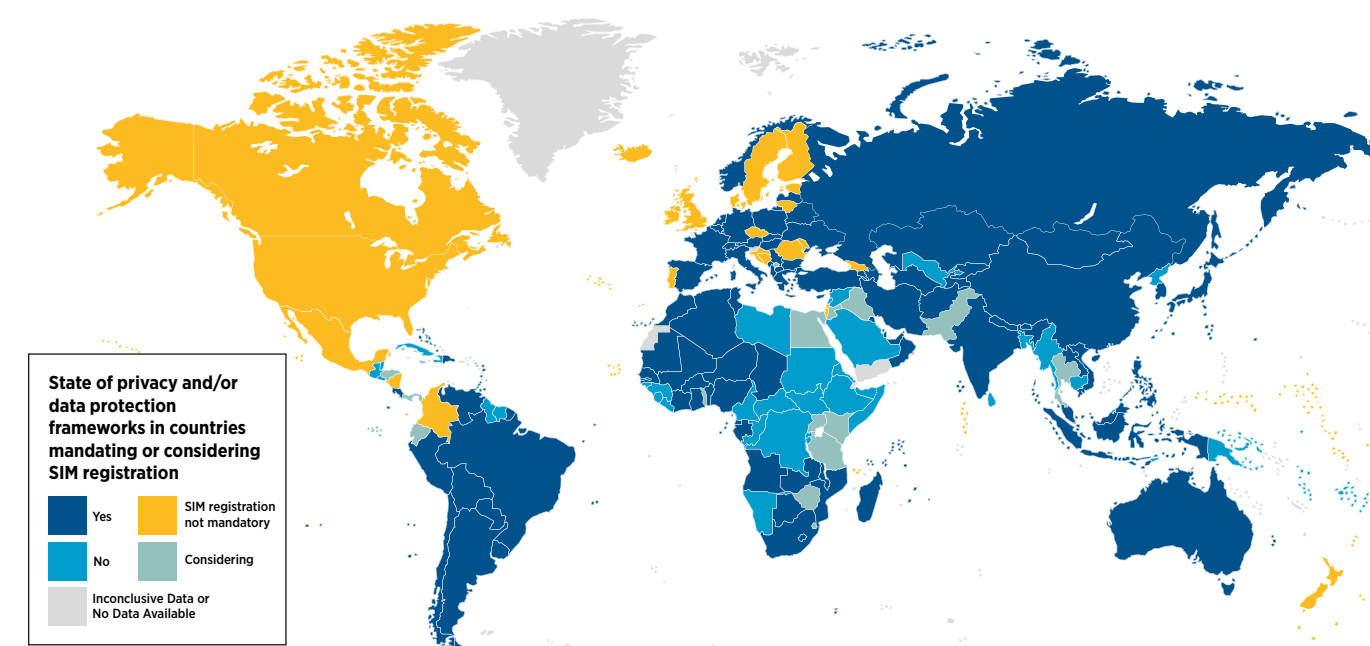
As outlined earlier, consumer concerns (whether actual or perceived) related to their privacy may impact on the level of trust they place in mobile and mobile financial services⁶². The situation is likely to be worse in countries without any privacy or data protection legal frameworks⁶³. Indeed, with the growth of the mobile industry and the corresponding rise in subscriber numbers, there is a need to adopt practices that assure trust and confidence among users of the mobile platforms.

As evident in Figure 5.9, while the majority of countries across the world have put privacy frameworks in place as at the end of 2018⁶⁴, many still lack such frameworks⁶⁵. Of the countries mandating SIM registration:

- In Africa, 16 countries have no privacy or data protection frameworks in place while seven more are actively considering it.
- In Asia, 17 countries have no privacy or data protection frameworks in place while four more are actively considering it.
- In Central and South America, eight countries have no privacy or data protection frameworks in place while six more are actively considering it.

Figure 5.9

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



Source: GSMA research from publicly available information (December 2018)

62. Mandatory SIM registration: policy and regulatory perspectives in the absence of data protection laws: <https://www.gsma.com/mobilefordevelopment/programme/digital-identity/mandatory-sim-registration-policy-and-regulatory-perspectives-in-the-absence-of-data-protection-laws/>

63. Ibid.

64. UNCTAD’s Data Protection Regulations and International Data Flows: https://unctad.org/en/PublicationsLibrary/dtstict2016d1_en.pdf

65. See Annex 3

06

Proof of identity in humanitarian contexts: The impact on refugees' access to mobile

In 2018, the United Nations High Commissioner for Refugees (UNHCR) estimated that over 135 million people needed humanitarian assistance and protection. Approximately 50 per cent of these individuals were likely to be persons of concern (PoC)⁶⁶ for UNHCR, a term⁶⁷ which includes refugees, asylum seekers, internally displaced persons (IDPs), stateless persons, returned refugees and IDPs, and others of concern.

This chapter explores how proof of identity requirements may impact PoC's access to mobile connectivity and mobile financial services.

6.1 Mobile access and proof of identity for forcibly displaced persons: Policy trends

Current trends suggest the need for humanitarian assistance will grow more complex and that protracted humanitarian emergencies will outstrip current capacity. The humanitarian sector recognises that in order to meet future needs, mobile will have a stronger role to play in the delivery of humanitarian assistance to beneficiaries. However, a number of GSMA research studies⁶⁸ found that a significant barrier that forcibly displaced persons face in this context is their inability to meet the proof of identity requirements to legally register a mobile SIM card or open a mobile money wallet in their own name⁶⁹. They are therefore at a higher risk of becoming further marginalised and disempowered as access to

information, communication, cash assistance or transfers is severely limited.

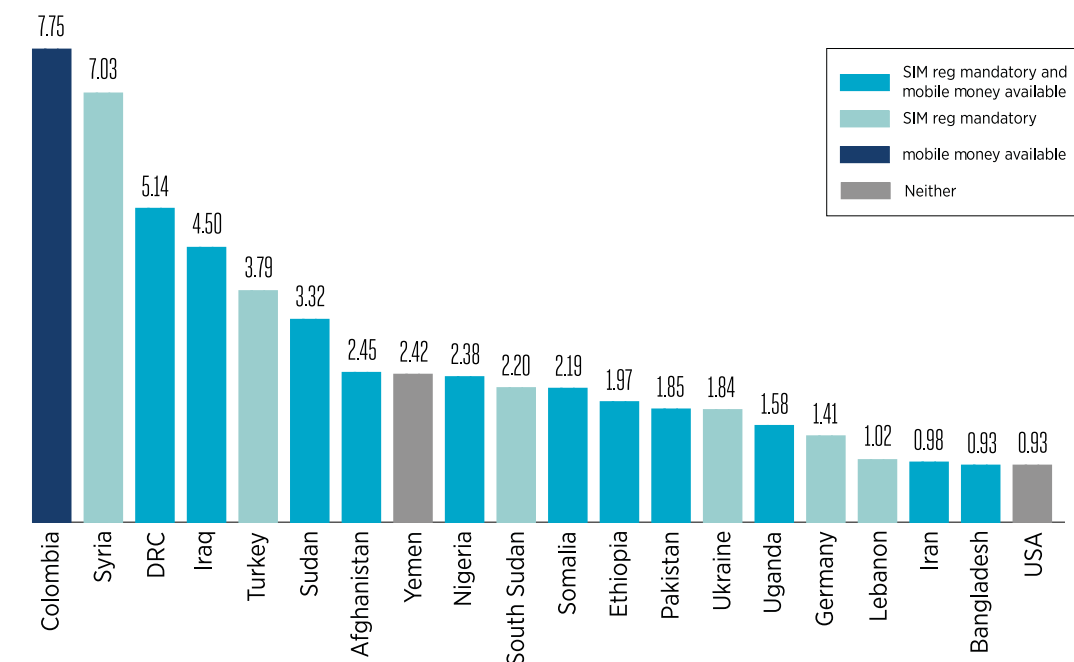
Over the last year, we have found that out of the 150 countries implementing SIM registration policies, 136 host⁷⁰ PoC⁷¹.

The GSMA estimates that 57.6 million PoC (an equivalent to 81 per cent of all PoC) are hosted in a country that mandates SIM registration. As shown in Figure 6.1, 17 of the top 20 host countries (to PoC) mandate SIM registration.

Figure 6.1

11 of top 20 PoC hosting countries mandate SIM registration and offer mobile money services

PoC population (in millions)



66. Based on UNHCR's 2017 Global Trends statistics http://popstats.unhcr.org/en/overview#_ga=2.29630588.298189533.1544429383-477750216.1511171156

67. Ibid

68. GSMA, 2017, Enabling Access to Mobile Services for the Forcibly Displaced <https://bit.ly/2Sg8rqE>

69. UNHCR 2019, 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>

70. UNHCR's 2017 Global Trends statistics http://popstats.unhcr.org/en/overview#_ga=2.29630588.298189533.1544429383-477750216.1511171156

71. Serbia and Kosovo have been excluded from our statistics because the data for PoC is joint for both countries, so it is difficult to treat them as separate.

More than 96 per cent of countries that offer mobile money services, are host to PoC. An equivalent of 44.7 million PoC therefore have the potential to access mobile money services if they are able to meet the KYC requirements of their host country. Twelve of the top 20 host countries (shown in Figure 6.1 above) offer mobile money services.

Overall, around 63 per cent of all PoC reside within host countries that offer mobile money services.

Refugees

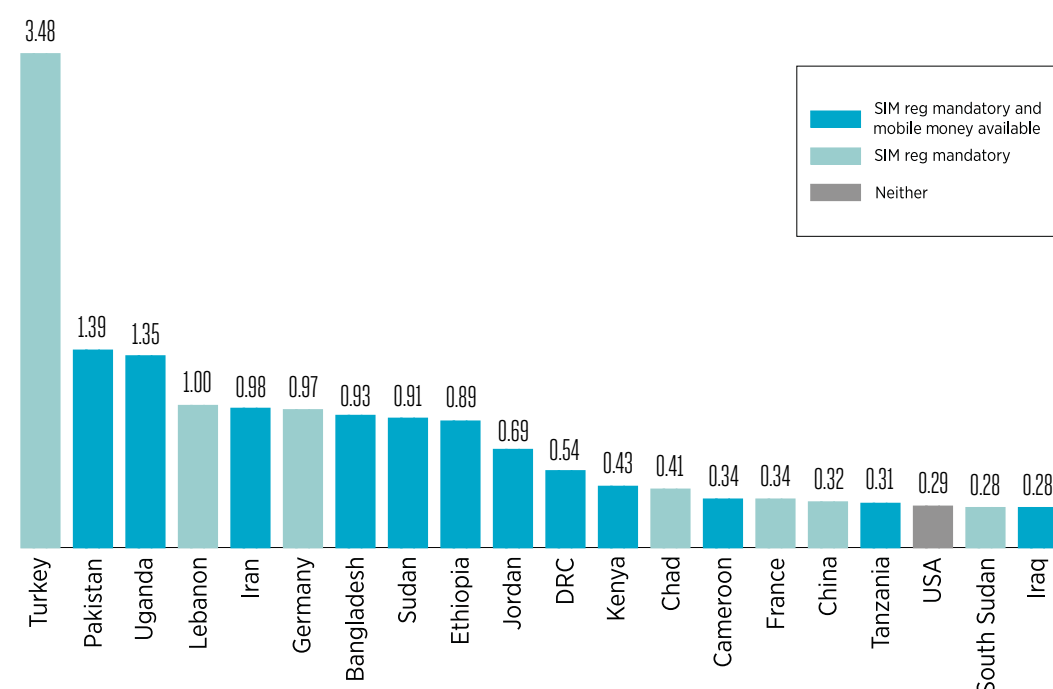
Refugees make up 28 per cent of PoC. This research found that:

- 173 countries host 19.9 million refugees
- 129 refugee-hosting countries mandate SIM registration, meaning that 18.6 million refugees (93 per cent of the total) are subject to proof of identity requirements in order to access mobile services
- Nineteen of the top 20 refugee-hosting countries mandate SIM registration, the United States being the only country that does not (see Figure 6.2).
- 80 per cent of all refugees live within these 20 countries and so are required to present an acceptable proof of identity to register for a mobile SIM in their own name
- Furthermore, 81 host countries have the potential to deliver mobile money services to 10.8 million refugees.

Figure 6.2

12 of the top 20 refugee hosting countries mandate SIM registration and offer mobile money services

Refugee population (in millions)



Twelve of the top 20 refugee-hosting countries offer mobile money services; 45 per cent of all refugees live within these 12 countries and could potentially be financially included subject to meeting the KYC requirements.

Yet, little evidence exists in the public domain on how many refugees possess the identity documentation required for SIM registration and KYC regulation in each host country. The UNHCR are often involved, as part of their mandate, in the registration and identification of refugees when they first arrive in their countries of asylum. However, the majority of host countries do not accept⁷² UNHCR-issued refugee IDs, for either SIM card registration or for mobile money accounts and require a government ID, which in turn depends on official recognition of refugee status — a process that can take months or years to complete⁷³.

The GSMA recently published a number of policy considerations for governments⁷⁴ in the context of addressing proof of identity barriers faced by

refugees. A key consideration in having an inclusive SIM registration or KYC policy is to understand and reflect what forms of identity most refugees have access to, for example UNHCR-issued identification, that could be deemed acceptable for meeting such proof of identity requirements.

Ensuring an enabling and proportional policy and regulatory environment and promoting dialogue between key stakeholders including mobile operators, mobile money service providers, donors, humanitarian agencies, NGOs, central banks and policymakers will be crucial to accelerating the delivery of digital humanitarian assistance.

72. UNHCR 2019, 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>

73. GSMA (2017), *Refugees and Identity: Considerations for Mobile-Enabled Registration*

74. GSMA, *Enabling Access to Mobile Services for the Forcibly Displaced: Policy and Regulatory Considerations for Addressing Identity Related Challenges in Humanitarian Contexts* <https://bit.ly/2Sg8rqE>

07

Conclusion

Mobile services, including connectivity and mobile money, are playing an increasingly significant role in providing access to life-enhancing services for billions of people. However, as this research report shows, a recognised form of identification is a pre-requisite for registering a mobile SIM card or opening a mobile money account in one's own name across 150 countries. This disproportionately impacts around one billion people who still lack a proof of identity, mostly comprising vulnerable groups of society including women and refugees, particularly across Asia and Sub-Saharan Africa.



By developing or upgrading their digital identity infrastructure and ensuring inclusive access for all residents, governments can play a key role in bridging this identity gap and nurturing an ecosystem that is crucial for achieving the digital and financial inclusion of the underserved. Governments can also partner with MNOs, seeking to leverage their extensive reach and network assets. MNOs can play various roles in such partnerships e.g. supporting identity enrolment efforts to reach traditionally underserved populations, strengthening existing verification / authentication processes and/or enabling secure access to additional identity-linked (such as e-Government) services to consumers on the move which may also incentivise uptake of digital IDs.

An advantage of a digital as opposed to a paper-based ID credential is that it can be queried and validated remotely in almost real-time. The ability of mobile operators to query and validate a customer's digital identification credential against a government-approved database (whether centralised or decentralised) could significantly

improve the robustness and effectiveness of mandatory SIM registration or electronic KYC processes. While such remote validation capabilities are currently being implemented in 11 per cent of the countries mandating SIM registration, several other countries are considering this approach.

Building and maintaining consumers' trust in digitally transformed economies is a key factor likely to impact the adoption and usage of mobile-enabled digital IDs. However, around 40 per cent of countries mandating SIM registration lack any comprehensive privacy and data protection frameworks. While other regulations and license conditions may provide consumers with varying degrees of privacy or data protection, the absence of such legal frameworks may lead to calls for stronger regulatory measures and policies that promote transparency on how personal data are used or shared in the digital ID ecosystem.

Policymakers involved in the expansion of foundational identification systems (e.g. National ID Authorities) should liaise with both privacy commissioners and sectoral regulators dealing with

proof of identity policies (e.g. telecommunications regulators or central banks) in an effort to ensure that the identity ecosystem can cater for the respective needs of each sector but also the specific needs of various consumer groups – including those marginalised and underserved. Identification requirements imposed on mobile and mobile money providers should be: (a) as harmonised as possible, (b) proportionate to people's ability to access an acceptable form of identification, (c) reflective of the risk of harm in a given context and (d) sufficiently flexible to adapt to market developments.

With just 11 years to meet the 2030 United Nations' Sustainable Development Goals (SDGs) and in particular SDG 16.9 of providing 'legal identity for all', there is a clear need for concerted action;

governments, the development community, the mobile and financial services sectors and stakeholders from the wider identification ecosystem need to do their part to jointly address the proof of identity barriers and privacy concerns preventing millions of people from accessing life-enhancing mobile services in their own name.

The GSMA is committed to supporting dialogue between these stakeholders in an effort to create more enabling environments where the needs of underserved groups are better catered for. This also involves advocating for and exploring various unique roles that its mobile network operator members can play in bringing the benefits of digital ID to many of the poorest and hardest to reach individuals around the world.

08

Annexes



Annex 1 Selected country case studies: The identity, mobile and privacy landscape

The case studies below outline the identity context, the SIM registration model and the status of privacy frameworks in a number of countries:



India

SIM registration model

Capture and Store (recently changed following a Supreme Court ruling)

The identity context

In 2009, India launched the Aadhaar program. This is a nationwide personal identification scheme based on which⁷⁵ each resident is assigned a random 12-digit number by the Unique Identity Authority of India (UIDAI) on the basis of one's biometric and demographic data. Aadhaar is considered the world's largest and one of the most sophisticated⁷⁶ biometric ID schemes. Over 90 per cent of India's entire resident population⁷⁷ is already registered, at no cost. Using their Aadhaar number, residents are therefore empowered⁷⁸ to open a bank account⁷⁹, obtain a driver's license, receive welfare payments, liquid petroleum gas (LPG) subsidies and even acquire a passport. Though the government refers to it as a strategic policy tool for financial inclusion and that it promotes hassle-free people-centric governance⁸⁰, Aadhaar has had its fair share of critics.

Identification for mobile access

SIM registration has been mandatory in India since 2005, yet the requirements for this have evolved over time. In 2017, the Department of Telecommunications (DoT) started enforcing

biometric SIM registration for issuing new mobile connections and re-verifying existing consumers⁸¹. Using their Aadhaar number, prospective mobile subscribers were required to visit an MNO retailer to complete biometric SIM registration. This enabled the validation of the Aadhaar credentials against the UIDAI database⁸². However, in a historic judgement⁸³ in September 2018, India's Supreme Court decided by a majority ruling that while the scheme does not violate the right to personal privacy, Aadhaar details should no longer be mandatory for opening bank accounts or registering a mobile SIM card⁸⁴. Thus, MNOs can only capture and store the subscriber information.

Data protection and privacy

India does not yet have any specific legislation governing personal data protection or privacy in the digital era. However, there are various legal frameworks dealing with limited aspects of personal and customer data⁸⁵ and as of November 2018 India was still in the process of debating the Personal Data Protection Bill, 2018. Though the draft Bill continues to stir debate, industry bodies are united in their stance for a guideline with a legal backing that can adequately safeguard personal data in the country's fast growing digital economy⁸⁶.

75. Aadhaar: Everything you need to know about it : https://economictimes.indiatimes.com/articleshow/60173210.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

76. <https://www.daijiworld.com/news/newsDisplay.aspx?newsID=442948>

77. https://uidai.gov.in/aadhaar_dashboard/india.php

78. Aadhaar providing a Proof of Identity to one billion : https://static1.squarespace.com/static/5769a0b5f7e0ab7b91a3362b/1/5a2576f5419202014ee6d6b7/1512405956013/INDIA_Cas_eStudy_ReachProject2017.pdf

79. <https://medium.com/wharton-fintech/your-guide-to-upi-the-worlds-most-advanced-payments-system-b4e0b372bf0b>

80. Aadhaar: India's route to digital financial inclusion : <https://news.itu.int/aadhaar-indias-route-to-financial-inclusion/>

81. 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%202023.03.2017.pdf?download=1>

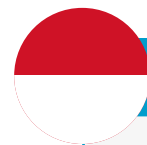
82. Use of 'Aadhaar' e-KYC service of Unique Identity Authority of India (UIDAI) for issuing new mobile connection to outstation customers and re-verification of existing outstation subscribers- regarding. DoT, 2017B. <http://dot.gov.in/sites/default/files/Outstation%2015.06.2017-final.PDF?download=1>

83. What India's Supreme Court Ruling on Aadhaar Means for the Future : <https://www.cgdev.org/blog/what-india-supreme-court-ruling-aadhaar-means-future>

84. Supreme Court of India on Aadhaar : https://www.supremecourtindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

85. Chronicles of Data Protection : <https://www.hldataprotection.com/2018/08/articles/international-eu-privacy/indias-draft-personal-data-protection-bill-2018-charting-the-fourth-way/>

86. Personal Data Protection Bill, 2018 : <https://www.pwc.in/assets/pdfs/consulting/cyber-security/the-personal-data-protection-bill-2018.pdf>



Indonesia

SIM registration model

Capture and Validate

The identity context

In Indonesia, *Kartu Tanda Penduduk*, commonly referred to as KTP, is a compulsory identity card with separate versions for Indonesian and foreign residents⁸⁷. While the card is issued upon attaining the age of 17, it must be renewed every five years for Indonesian residents, while for foreign residents it expires upon expiration of their residency permit. In 2011, the government started issuing an electronic ID card or the e-KTP (KTP elektronik), which contains an embedded microchip⁸⁸. Though the implementation is ongoing, the government's intention is not limited to personal identification. It envisages a mandatory multifunctional ID that could be used to access medical, educational, electoral and financial services⁸⁹. In addition, this is intended to solve the efficiency question of issuing identities in Indonesia and so the government is in the process of creating a single population identification number (*Nomor Induk Kependudukan*), such that each person can only have one number representing him in all his dealings⁹⁰. This number appears in the e-ID cards.

Identification for mobile access

In October, 2017 the government introduced mandatory SIM registration⁹¹. For Indonesians, the data requirements during registration is a KTP number, while for foreigners a passport suffices. The MNOs or their agents capture the KTP number and validate it against the *Nomor Induk Kependudukan* database⁹². In March, 2018 the Communication and Informatics Ministry announced that any prepaid SIM card users who had failed to register on time would be gradually blocked.

Data protection and privacy

In December 2016, the Minister of Communication and Informatics issued a regulation on Personal Data Protection in Electronic Systems⁹³ while at end of 2018 Indonesia's Ministry of Law and Human Rights was finalising the draft bill on Personal Data Protection⁹⁴.

87. Effectiveness of Evaluation of e-ID Policy in CIMAHI City, West Java Province in Indonesia: <http://www.eajournals.org/wp-content/uploads/Effectiveness-of-Evaluation-of-Electronic-Identity-Card-E-Id-Policy-in-Cimahi-City-West-Java-Province-Indonesia.pdf>
 88. How Aadhaar Compare to Other Biometric National ID Systems around the World : <https://www.firstpost.com/tech/news-analysis/how-aadhaar-compares-to-other-biometric-national-identification-systems-around-the-world-3700543.html>
 89. Ibid.
 90. Home Affairs Minister Urges People to Apply for e-KTP immediately : <https://jakartaglobe.id/news/home-affairs-minister-urges-people-apply-e-ktp-immediately/>
 91. Prepaid SIM card registration Mandatory in Indonesia : http://www.academia.edu/33225544/PREPAID_SIM_CARD_REGISTRATION_MANDATORY_IN_INDONESIA
 92. Indonesia Cracks Down on Unregistered Prepay SIM : <https://www.developingtelecoms.com/business/regulation/7761-indonesia-cracks-down-on-unregistered-prepaid-sims.html>
 93. Indonesia: Government Pushes Draft Data Protection Law: <https://globalcompliancencews.com/indonesia-draft-data-protection-law-20180518/>
 94. Ibid.



Kenya

SIM registration model

Capture and Share

The identity context

In Kenya, the Birth and Deaths Registration Act CAP 149 provides the legal basis for identification issuance⁹⁵ and the ID system can be traced to 1971 when it was already compulsory to register all births and deaths⁹⁶. The registration function is devolved and not all branches of this function have internet connectivity⁹⁷. To underscore the importance of identity, since 2016, a birth certificate is required to enrol in school and to sit examinations, while a national ID card is a requirement to access the majority of government services. Such services include social insurance, mobile-enabled cash transfers, tax-filing and voting. A range of technical checks and balances are in place to limit identity fraud⁹⁸. The data is synchronised with an Integrated Population Registration Service (IPRS), which was established to provide an integrated and unique identity service from birth. It draws from several databases involving the registration of citizens, aliens and refugees. It enables authorised entities to check the

validity of identity documents, in particular the national ID card.

Identification for mobile access

In 2013, following the enactment of the Kenya Information and Communications Act (2013), the government issued a directive to all MNOs to register all SIM card users. In 2015, East African regulators attempted to harmonise the legal and technical framework for SIM registration in the region by issuing a new directive that required all MNOs to deactivate any unregistered SIMs on their networks⁹⁹. In Kenya, MNOs are obligated to capture and share their customers' personal data with the government¹⁰⁰. Failure by an MNO to comply with the law regarding the mandatory registration of SIM is punishable with fines of up to USD 50,000¹⁰¹.

Data protection and privacy

Article 31 of Kenya's 2010 Constitution protects the right to personal privacy¹⁰² and while Kenya does not have a specific piece of legislation on personal data protection, a Data Protection Bill 2018¹⁰³ has been drafted and is being debated by the legislative body as of December 2018.

95. Births and Deaths Registrations : <http://www.kenyalaw.org/lex/actview.xhtml?actid=CAP%20149>

96. Ibid.

97. Banks reap big from digital population register: https://www.the-star.co.ke/news/2016/10/17/banks-reap-big-from-digital-population-register_c1437572

98. Integrated Data System to Make E-government A Reality: <http://www.president.go.ke/2015/03/11/integrated-data-system-to-make-e-government-a-reality/>

99. Registration of SIM cards – Regulations 2015: <https://ca.go.ke/document/registration-of-sim-cards-regulations-2015-2/>

100. The Kenya Information and Communications (Registration of SIM cards) Regulation 2015: http://kenyalaw.org/ki/fileadmin/pdfdownloads/LegalNotices/163-Kenya_Information_and_Communications_Act_Registration_of_Sim-Cards_Regulations_2015.pdf

101. Press Statement on the Findings of Forensic Audit on Registration of SIM cards : <https://ca.go.ke/wp-content/uploads/2018/09/Press-Statement-on-Forensic-Audit-on-SIM-Card-Registration1.pdf>

102. State of Privacy in Kenya : <https://privacyinternational.org/state-privacy/1005/state-privacy-kenya>

103. Data Protection Bill, Kenya (2018) : http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf



Malawi

SIM registration model

Capture and Store

The identity context

In 2017, Malawi issued biometric national IDs (NIDs) to the majority of its adult citizens under a United Nations (UNDP) spearheaded initiative¹⁰⁴. This formed part of a transformative initiative where the government's intention was to provide a recognised form of identification for all its citizens. While Malawians aged 16 and above are issued with the IDs, those below 16 are issued with national Birth Certificates.¹⁰⁵ Malawi's NID card is fully digitised and includes a chip containing selected biographic and biometric data (e.g., a photo, a signature and fingerprints). The NID is the only proof of identity that enables access to all public and private services including obtaining a driver's license, travel passport, direct cash-transfers, SIM card registration and financial services.

Identification for mobile access

The Communications Act of 2016 gives powers to the Malawi Communications Regulatory Authority (MACRA) to enforce mandatory SIM registration. In 2017, MACRA launched a campaign to sensitise users on

the perceived dangers of using unregistered SIMs, outlining the related obligations on the part of consumers and service providers¹⁰⁶. In February 2018, it set a deadline for phone users to register their SIM cards. SIM registration rules require MNOs to capture the customers' personal data and store them in their databases. This was shortly suspended when citizens petitioned the policy citing cases of surveillance. The suspension was later lifted and in October, 2018 MACRA warned MNOs of risking license suspension if they were to fail to deactivate unregistered SIM cards using the networks¹⁰⁷.

Data protection and privacy

There has never been a specific law to safeguard the personal data of citizens in Malawi. However in October 2016 the Electronic Transaction and Cyber Security Act was assented, which includes provisions for personal data and privacy protection related to a comprehensive list of transactions in the online space¹⁰⁸. However it reportedly contains provisions that could be used to censor online content and requires service providers to hand over user-information when presented with a court-issued warrant.¹⁰⁹



Nigeria

SIM registration model

Capture and Share

The identity context

The government began issuing the Nigerian ID card in 2008. All citizens above the age of 16 can obtain a national ID card once they enrol for a National Identification Number (NIN)¹¹⁰. The National Identity Management Commission (NIMC) is in the process of upgrading to an electronic biometric identification card-based system¹¹¹ and also hopes to leverage this in support of financial inclusion¹¹². While uptake of the new National ID card is still low, the government aspires that citizens would eventually use it for all identity-based transactions¹¹³.

Identification for mobile access

The Nigerian Communications Commission (NCC) introduced biometric SIM registration in 2011. Mobile users need to present proof of identification and have their fingerprints and facial image¹¹⁴ captured by MNOs at a point of sale. While Nigerians can use seven different forms of identification for SIM registration, including the national ID card and a letter of authentication¹¹⁵ by a traditional ruler or community leader¹¹⁶, non-Nigerian nationals are required to present their passport¹¹⁷. Unlike

most countries implementing biometric SIM registration, the Nigerian government does not currently maintain a single central database against which MNOs can validate customers' biometric details. Thus, MNOs capture and send customers' biometric information¹¹⁸ to the NCC for storage. Operators can store certain personal data of their customers 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 Database¹¹⁹, which may ultimately lead to a requirement on MNOs to capture and validate customer credentials against it.

Data protection and privacy

In Nigeria, privacy is a fundamental human right guaranteed by the Constitution. In 2007, the National Information Technology Development Agency (NITDA), a statutory agency was established to develop information technology in Nigeria. The enabling legislation empowers NITDA to 'develop guidelines for electronic data interchange and other forms of electronic communication'. NITDA published Guidelines on Data Protection in 2013 with a focus on consumer data¹²⁰, and Section 1.2 of this affirms that '*a breach of the guidelines shall be deemed to be a breach of the Act.*'

104. Malawi's National ID Project Praised at Africa's Largest Forum on Digital Identity: <https://mw.one.un.org/malawis-national-id-project-praised-at-africas-largest-forum-on-digital-identity/>

105. Malawi National IDs: Great milestone with transformative promise <https://malawi24.com/2017/12/06/malawi-national-ids-great-milestone-transformative-promise/>

106. Be Patriotic, Register Your SIM card : <http://www.macra.org.mw/be-patriotic-register-your-sim-card/>

107. Deactivation of Unregistered SIM cards : <http://www.macra.org.mw/deactivation-of-unregistered-sim-cards/>

108. Electronic Transactions and Cyber Security Act, 2016 : <https://malawilii.org/mw/legislation/act/2016/33>

109. <https://freedomhouse.org/report/freedom-net/2017/malawi>

110. What is the NIN? Nigerian Identity Management Commission. <https://www.nimc.gov.ng/about-nin/>

111. Nigeria launches national electronic ID cards. BBC, 2014. <http://www.bbc.co.uk/news/world-africa-28970411>

112. Ibid.

113. 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/>

114. 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>

115. SIM registration Centers. MTN. <http://mtnonline.com/simregistration>

116. Traditional Rulers and Local Government in Nigeria: a Pathway to Resolving the Challenge. O.Osemwota and D.A Tonwe, 2013.

117. Ibid.

118. 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>

119. FG to merge BVN, driver's license, National identity card. Clement Idoko, 2017. <http://www.tribuneonline.ng/fg-merge-bvn-drivers-licence-national-identity-card/>

120. Data Protection Guidelines : <https://nitda.gov.ng/wp-content/uploads/2018/02/DATA-PROTECTION-GUIDELINES-Reviewed.pdf>



Uganda

SIM registration model

Capture and Validate

The identity context

Uganda launched a national identification registration exercise in 2014¹²¹ to establish a comprehensive National Identification Register¹²² and issue national ID cards to all Ugandans. The national ID card includes the biometric data of its holder. Citizens can use it to obtain a passport, to vote, and to access government and banking services. Only those above the age of 16 can acquire a national identity card¹²³, assuming they hold a National Identification Number (NIN). As of mid-2017, 70 per cent of citizens aged 16 and over in Uganda had registered according to World Bank figures¹²⁴. One of the challenges faced in the registration exercise was the distance required to travel to access the nearest offices of National Identification Registration Authority (NIRA)¹²⁵.

Identification for mobile access

The Uganda Communications Commission (UCC) imposed SIM registration rules in 2012¹²⁶. Up until 2015, Ugandan mobile customers were required to present any official ID document such as a driver's license or passport. Using these, MNOs were required to capture and store the details in a secure database. However, in 2015 the government changed

the requirements in line with the Registration of Persons Act 2015¹²⁷. The new rules meant Ugandans have to register their SIM exclusively using a national ID card¹²⁸ which can be verified against the central database maintained by NIRA. Foreigners must provide their passports and refugees need to present a certified document from the Office of the Prime Minister (OPM)¹²⁹. During the re-registration exercise post the 2015 Act, operators offered existing mobile users the option of authenticating their identity via a USSD service. MNOs then sent the details to NIRA for validation, upon which verified subscribers received confirmation of their re-registration¹³⁰. In 2018 the UCC introduced the use of biometric card readers¹³¹ with the intention that MNOs would register and / or replace SIMs with the help of the readers that validate, in real time, subscriber information contained in the digital ID card against the NIRA database¹³².

Data protection and privacy

In the Ugandan constitution, Article 27 provides for citizens' right to privacy, though there is no law specifically safeguarding an individual's data privacy. However, there are pieces of legislation such as the Computer Misuse Act of 2011, Access to Information Act of 2005 and Uganda Communications Act of 2013, which prohibit unauthorised access and disclosure of information¹³³.



Algeria

SIM registration model

Capture and Share

The identity context

In Algeria, advancement in the e-ID framework was marked by the 2010 law on unique National Identification Number (*numéro d'identification nationale*) and the 2015 law on the use of electronic signatures. Since then, the government has been pursuing an extensive modernisation exercise informed by the need for efficiency in governance. In 2016 it launched an advanced¹³⁴ biometric national identity card (CNIBE) to replace the older paper ID. The new microchip-enabled e-ID provides citizens with a more robust proof of identity enabling them to interface more conveniently and access e-government services such as voter registration, tax collection and passport issuance.

Identification for mobile access

In Algeria, every user of a SIM card, either prepaid or post-paid, citizen or foreigner, must have their SIM registered¹³⁵. This is a regulatory directive by the *Autorite de Regulation des Postes et Telecommunications (ARPT)* for users to access mobile enabled services. To achieve this, the user must provide an official ID or passport, whose copies must be notarised in Algeria¹³⁶. The MNOs are required to capture the customer information and share those details with the government through the *ARPT*.

Data protection and privacy

In July 2018, Algeria enacted a Law on the protection of personal data (*Law 18-07*). This applies to automated and non-automated processing of personal data and prescribes that such processing may only be carried out with the expressed consent of the person concerned.

121. Government to synchronize both SIM card and National ID registration data. Roger Bambino, 2015. <https://www.techiaja.com/government-to-synchronize-both-sim-card-and-national-id-registration-data/>

122. <https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf?sequence=1&isAllowed=y>

123. 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/>

124. World Bank ID4D Dataset 2017, based on Uganda's National Identification and Registration Authority database

125. Probe National ID Register : <https://www.monitor.co.ug/OpEd/Editorial/Probe-national-ID-register/689360-4547128-kgln30/index.html>

126. Government to synchronize both SIM card and National ID registration data. Roger Bambino, 2015. <http://www.techiaja.com/government-to-synchronize-both-sim-card-and-national-id-registration-data/>

127. Progress on the SIM card Validation/Verification Exercise. Uganda Media Centre. <http://www.mediacentre.go.ug/press-release/progress-sim-card-validationverification-exercise>

128. SIM Registration. Uganda Telecom. <http://www.utl.co.ug/index.php/sim-registration/>

129. 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>

130. 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/>

131. The Observer : Cabinet Directs UCC To Ease SIM Registration : <https://observer.ug/news/headlines/57485-cabinet-directs-ucc-to-ease-sim-card-registration.html>

132. Lifting the Ban on The Sale and Replacement of SIM card : <https://www.ucc.co.ug/wp-content/uploads/2018/05/FINAL-LETTER-OPERATORS-LIFTING-BAN-ON-SALE-AND-SWAP-SIM-CARDS-9-05-2018.pdf>

133. State of Privacy in Uganda : <https://privacyinternational.org/state-privacy/1013/state-privacy-uganda>

134. Algeria – New Biometric ID – Successful Launch : <https://www.gemalto.com/govt/customer-cases/new-national-identity-card-algeria>

135. New Compulsory decrees for tighter regulation of the mobile phone industry in Africa: <https://issafrica.org/iss-today/mandatory-registration-of-sim-cards-ingenious-idea-or-misplaced-focus-on-crime-control>

136. Prepaid Data SIM : <http://prepaid-data-sim-card.wikia.com/wiki/Algeria>

Botswana

SIM registration model

Capture and Store

The identity context

In Botswana, there is a single foundational identity management system, which creates one identity per person. It is considered a primary tool for service delivery to the public and used to facilitate the individual's access to a number of e-government services including social safety nets, health and educational programs. The foundational ID, also referred to as Omang, is a requirement for obtaining passports, driver's licenses and voter registration cards. As part of the government's 'Identity Establishment' strategy, the national ID number obtained at age 16 is the same unique identification number (UID) issued at birth registration. In fact, according to the National Registration Act CAP 01:02, it is mandatory for every citizen to undertake National Registration within thirty (30) days of attaining the age 16 or within 30 days of acquiring Botswana

citizenship. Thus, the national ID is the prima facie proof of the particulars stated on any other identity card.

Identification for mobile access

In 2008, Botswana mandated prepaid SIM registration¹³⁷. To register a SIM card, only a photo ID was required. In 2010, the registration regulations were made stricter¹³⁸ and now the use of mobile services is prohibited until a SIM card is formally registered by physically visiting a service provider and presenting its agents with identification details. The MNOs are required to capture the customers' information and store it in a secure database.

Data protection and privacy

In August 2018, the Data Protection Act came into force¹³⁹. The law provides that personal data must be processed in a lawful, transparent and fair manner. It provides for collection of data only for specific and legitimate purposes. In addition, this needs to be limited to what is necessary, be up-to-date and accurate.

Brazil

SIM registration model

Capture and Store

The identity context

In Brazil, an ID card is mandatory, however, an array of identification schemes exists which include more than 10 different types of numbers to access a variety of services such as healthcare or social grants¹⁴⁰. In Brazil, the identification of a citizen is considered a mandatory requirement for the provision of social benefits and rights¹⁴¹. In 2008, the government began issuing biometric identification cards¹⁴² which citizens can use to obtain a driver's license, open a bank account and travel within Mercosur countries¹⁴³. All citizens over the age of 18 are required to hold a formal state-issued identification document. As the ID card issuance is not carried out on a digitally integrated platform, each regional government has unique rules resulting in 27 separate ID-issuing entities. This makes it possible for a Brazilian to have more than one ID number. In an attempt to address this, in 2017, Brazilian President Michel Temer signed into a law a bill creating the Unified Registry of Identification, or RCN (*registro civil nacional*). RCN was established to address citizens' ID data aggregated from the various entities and using these, RCN would generate a card for

citizens' authentication and access to various e-government services.

Identification for mobile access

In Brazil, SIM registration has been mandatory since 2003¹⁴⁴ 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. MNOs must store all customer information in a secure database. Though biometric identification cards exist, MNOs cannot validate customers' biometric information for mobile SIM registration purposes.

Data protection and privacy

In August 2018, Brazil signed into law the new General Data Privacy Law (*Lei Geral de Proteção de Dados Pessoais* or "LGPD")¹⁴⁵. The provisions of the new legislation are said to mirror the European Union's General Data Privacy Regulation ("GDPR"). The new framework guides the use of personal data, both online and offline, both in the private and public sectors. This piece of legislation has replaced previous legal frameworks.

137. Implications of Mandatory SIM registration on Mobile Phone Users in Africa. https://www.diw.de/documents/publikationen/73/diw_01.c.394079.de/dp1192.pdf

138. BTA: two million pre-paid mobile users register their details: <https://www.telegeography.com/products/commsupdate/articles/2010/01/06/bta-two-million-pre-paid-mobile-users-register-their-details/>

139. Data Protection Act of 2018 : <https://www.bocra.org.bw/data-protection-act>

140. Global Monitor : <http://www.loc.gov/law/foreign-news/article/brazil-new-national-id-card-launched/>

141. Surveillance in Latin America http://www2.pucpr.br/sscla/papers/SessaoC_A47_pp246-255.pdf

142. <http://www.identity-cards.net/record/brazil>

143. https://ipfs.io/ipfs/QmXoypiZiW3WknFiJnKLwHCnL72vedxiQkDDPImXWo6uco/wiki/Brazilian_Identity_Card.html

144. Lei no 10.703, de julho de 2003. ANTEL, July 2003. <http://www.anatel.gov.br/legislacao/leis/469-lei-10703>

145. Brazil president approves data protection bill — but vetoes key accountability measures: <https://www.zdnet.com/article/brazilian-president-signs-data-protection-bill/>

Annex 2 Selected country case studies: Access to identity, mobile connectivity and financial services for persons of concern (PoC)

Bangladesh

Access to identity, mobile connectivity and financial services for persons of concern (PoC)

According to UNHCR¹⁴⁶, at the end of 2017, Bangladesh was host to 932,334 PoC. The majority of PoC are Rohingya refugees who come from Myanmar. UNHCR are working with the Government of Bangladesh to assign unique identification numbers to these refugees, which will result in an ID card being issued to all individuals over the age of 12, as well as a family attestation document that includes photographs and biographical information for all family members¹⁴⁸.

At the time of writing (December 2018), only four per cent of the population have registered and so (are assumed to) have identity documentation. Approximately one-third of the total Rohingya population has a SCOPE card issued to them by the World Food Program (WFP). It is also possible that Rohingya refugees may hold other documents, such as family counting cards, ration cards and cards issued by the Ministry of Home Affairs¹⁴⁹. Concerns around misuse of their personal information and fear of privacy violations have been reported¹⁵⁰ as factors possibly contributing to low registration levels among the Rohingya population.

SIM registration and financial services

Biometric SIM registration is mandatory in Bangladesh. The Bangladesh Telecommunications Regulatory Commission (BTRC) implemented biometric SIM registration

in 2015, requiring mobile operators to validate the identity of customers using their fingerprints. Bangladeshi nationals can use a number of identity documents to complete biometric SIM registration, including their national identity card, passport, and driving license. Foreigners can only use their passports to purchase a SIM card¹⁵¹. Rohingya refugees do not have passports therefore cannot meet biometric SIM registration requirements. In addition the BTRC have implemented a ban on mobile operators selling SIM cards to refugees¹⁵². Mobile operators offer mobile money services to their customers. However, without a SIM card (in their own name), refugees lack access to mobile money services.

In Bangladesh, in order to access traditional financial services, such as those offered through a bank, prospective customers must present their national ID card, citizenship certificate, or a driving license/passport, as well as proof of address in order to open a bank account¹⁵³. Without this documentation refugees cannot open a traditional bank account. However, recent research by the UNHCR suggests that the Bangladeshi Government is currently (December 2018) developing a process to sell SIM cards to the Rohingyas.¹⁵⁴ Bangladesh Bank have indicated that the UNHCR-issued Refugee ID card would be sufficient to meet KYC requirements¹⁵⁵.



Central African Republic

Access to identity, mobile connectivity and financial services for PoC

In 2017, the Central African Republic was host to 866,948 PoC. A large percentage of these are internally displaced persons and refugees who have returned to the Central African Republic (their country of origin) from other countries of asylum. The Central African Republic also plays host to 10,036 refugees, who are predominately from the Democratic Republic of Congo, South Sudan and Chad.

The National Eligibility Commission (NEC) issues refugees with an identity card and asylum seekers with an asylum seeker certificate (attestation de demandeur d'asil). Asylum seekers are expected to hold their certificates until they are officially recognised. The refugee ID card is a biometric document with a barcode that includes the cardholder's personal data. Both the refugee ID card and asylum seeker certificate are official government-recognised identity documents (bearing a UNHCR logo)¹⁵⁶.

SIM registration and financial services

SIM registration has been mandatory in Central African Republic since 2014¹⁵⁷. However, consumers still face difficulties in meeting proof of identity requirements. According to the 2017 Global FINDEX survey¹⁵⁸, a comprehensive data set about how adults save, borrow, make payments, and manage risk, 34 per cent of respondents from the CAR stated they were unable to apply for a SIM card or mobile phone services because they did not have the necessary identification documents¹⁵⁹.

Refugees can use¹⁶⁰ their (refugee) ID card to purchase a SIM card, open a bank account and register for mobile money services. However, the proportion of refugees with a Refugee ID card is unclear.

146. <https://www.unhcr.org/uk/statistics/unhcrstats/5b27be547/unhcr-global-trends-2017.html>

147. UNHCR 2019, 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>

148. Ibid.

149. Ibid.

150. <https://www.opendemocracy.net/natalie-brinham/genocide-cards-why-rohingya-refugees-are-resisting-id-cards>

151. Bangladesh will demand biometric data from all SIM card users. Zara, Rahman, 2015. <https://advoc.globalvoices.org/2015/12/22/bangladesh-will-demand-biometric-data-from-all-sim-card-users/>

152. <https://www.cbsnews.com/news/bangladesh-bans-phone-companies-from-selling-sim-cards-to-rohingya-refugees/>

153. UNHCR 2019, 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>

154. Ibid.

155. Ibid.

156. Ibid.

157. <https://www.telegeography.com/products/commsupdate/articles/2014/07/31/sim-registration-process-gets-underway-in-the-car/>

158. The World Bank launched the FinIndex data set in 2011 with funding from the Bill & Melinda Gates Foundation. The data is collected in partnership with Gallup, through nationally representative surveys of more than 150,000 adults in over 140 economies and is updated every three years.

159. https://globalfinindex.worldbank.org/#data_sec_focus

160. UNHCR 2019, 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>



Democratic Republic of Congo

Access to identity, mobile connectivity and financial services for PoC

5,144,932 PoC were based in the Democratic Republic of Congo (DRC) at the end of 2017. The majority (86 per cent) are internally displaced persons. Another large population of concern are refugees. The DRC host 537,853 refugees who originate from neighbouring countries — Rwanda, Central Africa Republic, South Sudan and Burundi¹⁶¹.

PoC are issued with a number of identity documents from the National Commission for Refugees (CNR), the Directorate General for Migration (DGM), the Commissioner for Refugees, Ministry of Home Affairs and UNHCR. UNHCR started issuing the refugee ID card in 2017. By the end of the 2018, Burundian and Central African refugees are expected to possess a refugee ID card and South Sudanese refugees are to receive their refugee ID cards in 2019¹⁶².

SIM registration and financial services

SIM registration is mandatory and has been so since 2012¹⁶³, based on a Capture and Store model. In the absence of a (comprehensive) national identity system, several forms of ID are accepted to purchase a SIM card¹⁶⁴. DRC nationals can use their passport, driver's license, voter card, student card, or service card (carte de service) to meet SIM registration requirements. Refugee ID cards (issued by UNHCR), national ID cards, passports and voter cards (from refugees' country of origin) are all acceptable forms of proof of identity that refugees can use to register for a SIM card in the DRC¹⁶⁵. Refugees can also use the same documents to open a bank account and register for mobile money services¹⁶⁶.

161. <https://data2.unhcr.org/en/documents/download/66567>

162. Ibid.

163. <https://www.leganet.cd/Legislation/Droit%20economie/telecommunication/AM.08.03.2012.htm>

164. The fact that there is not a unique type of ID widespread in the country definitely helps to provide more flexibility to the requirements.

165. UNHCR 2019, 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>

166. Ibid.



Zambia

Access to identity, mobile connectivity and financial services for PoC

At the end of 2017, Zambia was host to 68,340 PoC¹⁶⁷. Refugees make up a large proportion of PoC (60 per cent); they mainly originate from the Democratic Republic of Congo.

The Department of National Registration, Passport and Citizenship and the Office of the Commissioner for Refugees are responsible for issuing refugees with a Proof of Registration and/or a Refugee Certificate on behalf of the Government of Zambia¹⁶⁸. The Refugee Certificate is unique because it contains the block number allocated to the refugee household, so as well as a proof-of identity it can also be used as a proof-of-address¹⁶⁹. The Government of Zambia have also issued Refugee Cards and/or Alien Cards to some refugees.

SIM registration and financial services

Since 2011 SIM registration has been mandatory in Zambia based on a 'Capture and Store' model. While Zambian nationals can use a

range of identity documentation (their national registration card, passport, driver's license or voter's card), foreigners can only use their passport or work permit identification card to purchase a SIM card¹⁷⁰. Financial services can be accessed using a bank account or mobile money services. Zambian nationals are expected to present a national registration card or a valid passport or driving licence to open a bank account. Yet, foreigners must provide a national registration card or valid passport (with, where applicable, a duly issued visa). In both cases, proof of address is also required¹⁷¹.

The Zambian Information and Communications Technology Authority and Bank of Zambia have given special permission to refugees, allowing them to use their Proof of Registration, Refugee Certificates and Refugee Cards as valid proof of identity to complete SIM registration and mobile money registration¹⁷². However, refugees can use their alien card to open a bank and mobile money account¹⁷³.

167. <https://reliefweb.int/sites/reliefweb.int/files/resources/67309.pdf>

168. <http://www.zanis.com.zm/?q=article/zambia-joins-campaign-end-statelessness>

169. UNHCR 2019, 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>

170. [https://www.zicta.zm/Views/Articles/Sim%20Registration%20\(FAQ\)%20.htm](https://www.zicta.zm/Views/Articles/Sim%20Registration%20(FAQ)%20.htm)

171. UNHCR 2019, 'Displaced and Disconnected', <https://www.unhcr.org/innovation/displaced-and-disconnected/>

172. Ibid.

173. <http://www.daily-mail.co.zm/refugees-can-now-open-mobile-money-accounts-boz/>

Annex 3 Policy landscape, by country

Africa

	SIM registration mandated	SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework
Algeria	✓					✓		✓				
Angola	✓				✓			✓				
Benin	✓					✓		✓				
Botswana	✓				✓			✓				
Burkina Faso	✓				✓			✓				
Burundi	✓				✓				✓			
Cabo Verde			✓									
Cameroon	✓				✓				✓			
Central African Republic	✓				✓				✓			
Chad	✓				✓			✓				
Comoros			✓									
Congo	✓				✓				✓			
Congo, Democratic Republic	✓				✓				✓			
Côte d'Ivoire	✓				✓			✓				
Djibouti				✓								
Egypt	✓						✓			✓		
Equatorial Guinea	✓				✓			✓				
Eritrea	✓				✓				✓			
Ethiopia	✓				✓				✓			
Gabon	✓				✓			✓				
Gambia	✓				✓			✓				
Ghana	✓				✓			✓				
Guinea	✓				✓				✓			
Guinea-Bissau	✓				✓				✓			
Kenya	✓					✓				✓		
Lesotho	✓				✓			✓				

	SIM registration mandated	SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework
Liberia	✓				✓				✓			
Libya	✓				✓				✓			
Madagascar	✓				✓			✓				
Malawi	✓				✓			✓				
Mali	✓				✓			✓				
Mauritania	✓				✓			✓				
Mauritius	✓				✓			✓				
Morocco	✓				✓			✓				
Mozambique	✓				✓			✓				
Namibia		✓									✓	
Niger	✓				✓			✓				
Nigeria	✓					✓		✓				
Rwanda	✓				✓				✓			
Sao Tomé and Príncipe	✓				✓			✓				
Senegal	✓						✓	✓				
Seychelles	✓				✓			✓				
Sierra Leone	✓				✓				✓			
Somalia	✓				✓				✓			
South Africa	✓				✓			✓				
South Sudan	✓				✓				✓			
Sudan	✓				✓				✓			
Swaziland	✓				✓					✓		
Tanzania	✓				✓					✓		
Togo	✓				✓					✓		
Tunisia	✓				✓			✓				
Uganda	✓						✓			✓		
Zambia	✓				✓			✓				
Zimbabwe	✓				✓					✓		

Asia

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework
Afghanistan	✓				✓			✓				
Armenia	✓				✓			✓				
Australia	✓				✓			✓				
Azerbaijan	✓				✓			✓				
Bahrain	✓						✓	✓				
Bangladesh	✓						✓		✓			
Bhutan	✓				✓			✓				
Brunei Darussalam	✓				✓				✓			
Cambodia	✓				✓				✓			
China	✓						✓	✓				
Fiji	✓				✓				✓			
Georgia			✓									
Hong Kong			✓									
India	✓				✓			✓				
Indonesia	✓						✓	✓				
Iran	✓				✓			✓				
Iraq	✓				✓					✓		
Israel			✓									
Japan	✓				✓			✓				
Jordan	✓				✓					✓		
Kazakhstan	✓				✓			✓				
Kiribati			✓									
Korea, North	✓				✓				✓			
Korea, South	✓				✓			✓				
Kuwait	✓				✓			✓				
Kyrgyzstan	✓				✓			✓				
Laos	✓				✓			✓				
Lebanon	✓				✓				✓			
Macao		✓										✓
Macedonia	✓				✓			✓				
Malaysia	✓						✓	✓				
Maldives			✓									
Marshall Islands			✓									
Micronesia			✓									

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework
Mongolia	✓				✓			✓				
Myanmar	✓				✓				✓			
Nauru	✓				✓				✓			
Nepal	✓				✓			✓				
New Zealand			✓									
Oman	✓				✓			✓				
Pakistan	✓						✓			✓		
Palau				✓								
Palestine	✓				✓				✓			
Papua New Guinea	✓				✓				✓			
Philippines		✓										✓
Qatar	✓				✓			✓				
Samoa	✓				✓				✓			
Saudi Arabia	✓						✓		✓			
Singapore	✓				✓			✓				
Solomon Islands			✓									
Sri Lanka	✓				✓				✓			
Syria	✓				✓				✓			
Taiwan	✓				✓			✓				
Tajikistan	✓				✓			✓				
Thailand	✓						✓			✓		
Timor-Leste	✓				✓				✓			
Tonga	✓				✓				✓			
Turkey	✓				✓			✓				
Turkmenistan	✓				✓			✓				
Tuvalu				✓								
United Arab Emirates	✓				✓			✓				
Uzbekistan	✓				✓				✓			
Vanuatu		✓									✓	
Vietnam		✓										✓
Yemen				✓								

Europe

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework
Albania	✓						✓	✓				
Andorra			✓									
Austria	✓				✓			✓				
Belarus	✓				✓			✓				
Belgium	✓				✓			✓				
Bosnia and Herzegovina			✓									
Bulgaria	✓				✓			✓				
Croatia			✓									
Cyprus		✓										✓
Czech Republic			✓									
Denmark			✓									
Estonia			✓									
Finland			✓									
France	✓				✓			✓				
Germany	✓				✓			✓				
Greece	✓				✓			✓				
Greenland				✓								
Hungary	✓						✓	✓				
Iceland			✓									
Ireland			✓									
Italy	✓					✓		✓				
Kosovo	✓				✓				✓			
Latvia		✓										✓
Liechtenstein			✓									
Lithuania			✓									
Luxembourg	✓				✓			✓				
Malta		✓										✓
Moldova			✓									

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework
Monaco	✓				✓			✓				
Montenegro	✓				✓			✓				
Netherlands		✓										✓
Norway	✓				✓			✓				
Poland	✓				✓			✓				
Portugal			✓									
Romania			✓									
Russian Federation	✓				✓			✓				
San Marino	✓					✓		✓				
Serbia		✓										✓
Slovakia	✓				✓			✓				
Slovenia			✓									
Spain	✓				✓			✓				
Svalbard	✓				✓			✓				
Sweden			✓									
Switzerland	✓				✓			✓				
Ukraine	✓				✓			✓				
United Kingdom			✓									

North & Latin America

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework
Antigua and Barbuda	✓				✓			✓				
Argentina	✓				✓			✓				
Bahamas			✓									
Barbados	✓				✓					✓		
Belize	✓				✓				✓			
Bolivia	✓				✓			✓				
Brazil	✓				✓			✓				
Canada			✓									
Chile		✓										✓
Colombia			✓									
Costa Rica	✓				✓			✓				
Cuba	✓				✓				✓			
Dominica	✓				✓			✓				
Dominican Republic	✓						✓	✓				
Ecuador	✓						✓			✓		
El Salvador	✓				✓				✓			
French Guiana	✓				✓			✓				
Grenada	✓				✓				✓			
Guatemala	✓				✓				✓			
Guyana	✓				✓				✓			
Haiti	✓				✓				✓			
Honduras	✓				✓					✓		
Jamaica	✓				✓					✓		
Mexico			✓									

	Mandatory SIM registration	Mandatory SIM registration under consideration	SIM registration not mandated	State of SIM registration inconclusive	'Capture and Store' SIM user information	Capture and Share' SIM user information	'Capture and Validate' SIM user information	Mandate SIM registration and have a data privacy framework	Mandate SIM registration but lack a data privacy framework	Mandate SIM registration and are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework
Nicaragua			✓									
Panama	✓				✓					✓		
Paraguay		✓										✓
Peru	✓						✓	✓				
St. Kitts and Nevis	✓				✓					✓		
St. Lucia	✓				✓			✓				
St. Vincent and the Grenadines	✓				✓			✓				
Suriname	✓				✓				✓			
Trinidad and Tobago	✓				✓			✓				
United States of America			✓									
Uruguay	✓				✓			✓				
Venezuela	✓				✓			✓				

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