



Access to Mobile Services and Proof of Identity 2020: The Undisputed Linkages

March 2020





GSMA Digital Identity

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 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)

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

Erdoo Yongo (Policy & Advocacy Manager, Digital Identity, GSMA)

Yiannis Theodorou (Senior Director, Policy & Advocacy, Digital Identity, GSMA)

Contents

1	Context	2
2	Mobile penetration	3
3	Prepaid mobile SIM penetration	6
4	Countries with mandatory SIM registration policies	7
5	SIM registration implementation models	8
6	Linkages between access to identification and access to mobile	11
7	Data protection and privacy frameworks	16
8	Proof of identity in humanitarian contexts: the impact on forcibly displaced persons' (FDPs) access to mobile	18
9	Annex: policy landscape, by country	22

01

Context

This paper is intended to provide updates to the 2019 edition of the GSMA's 'Access to Mobile Services and Proof of identity' series¹ which explores various correlations between people's access to formal identification (ID) and their ability to register for mobile services where governments mandate proof of identity requirements.

In addition to the GSMA's own data and original research, this report reflects insights from sources such as the websites of national telecommunications regulators, the International Telecommunications Union (ITU), the World Bank, various United Nations Institutions, government, media and civil society reports.

This publication omits the updated figures on the 'global identification outlook' which featured in previous editions in this series. Those figures were based on the World Bank's ID4D Dataset, an update of which is not expected until later in 2021. For this reason, all references to identity penetration in this Addendum are based on the latest Global Findex Database published by the World Bank.

1. <https://www.gsma.com/mobilefordevelopment/accesstomobileservices>



02

Mobile penetration

The reach of mobile continues to grow year upon year. With more than 5.1 billion individuals with a mobile subscription,² there are more people connected to mobile than any other communications platform. Over the last decade (2009-2019), access to mobile has grown considerably, both in terms of unique subscribers as well as in terms of total mobile connections. Unique

mobile subscriptions have increased from 40 per cent (of the global population in 2009) to 67 per cent in 2019, while mobile connections have risen by 38 percentage points between 2009 and 2019 (as can be seen in Figures 1 to 4). During this period, the biggest growth, in terms of unique mobile subscribers, was in Asia.

2. GSMA Intelligence

Mobile penetration in 2009 and 2019

Unique subscribers

Figure 1

Unique mobile subscribers as a percentage of total population (2009)

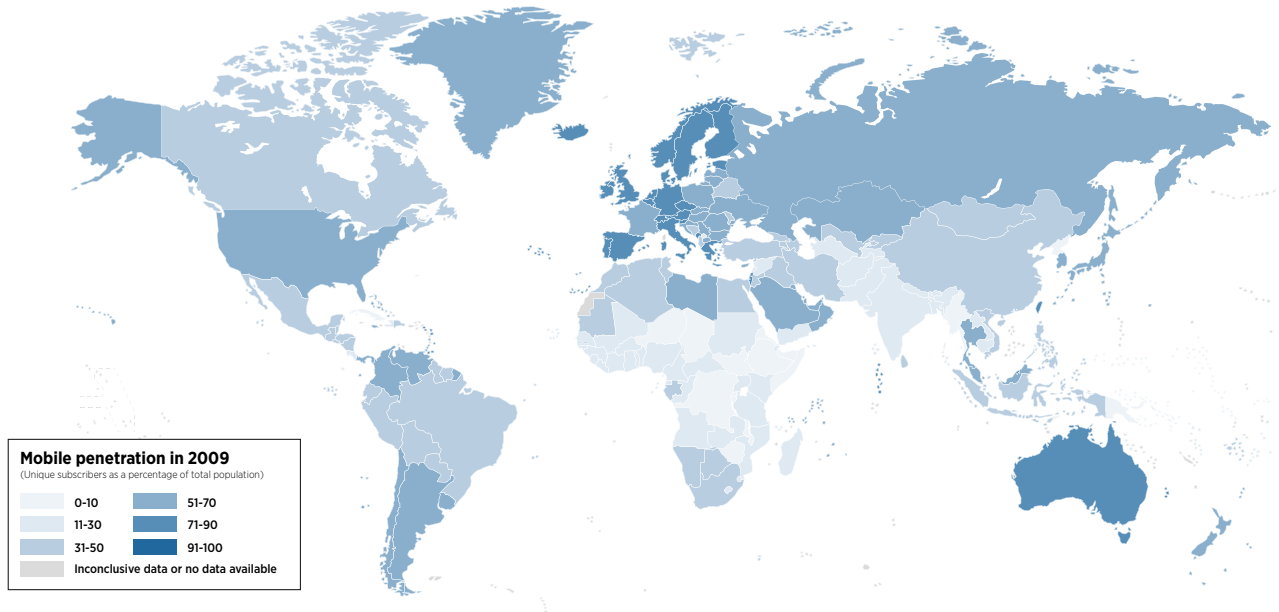
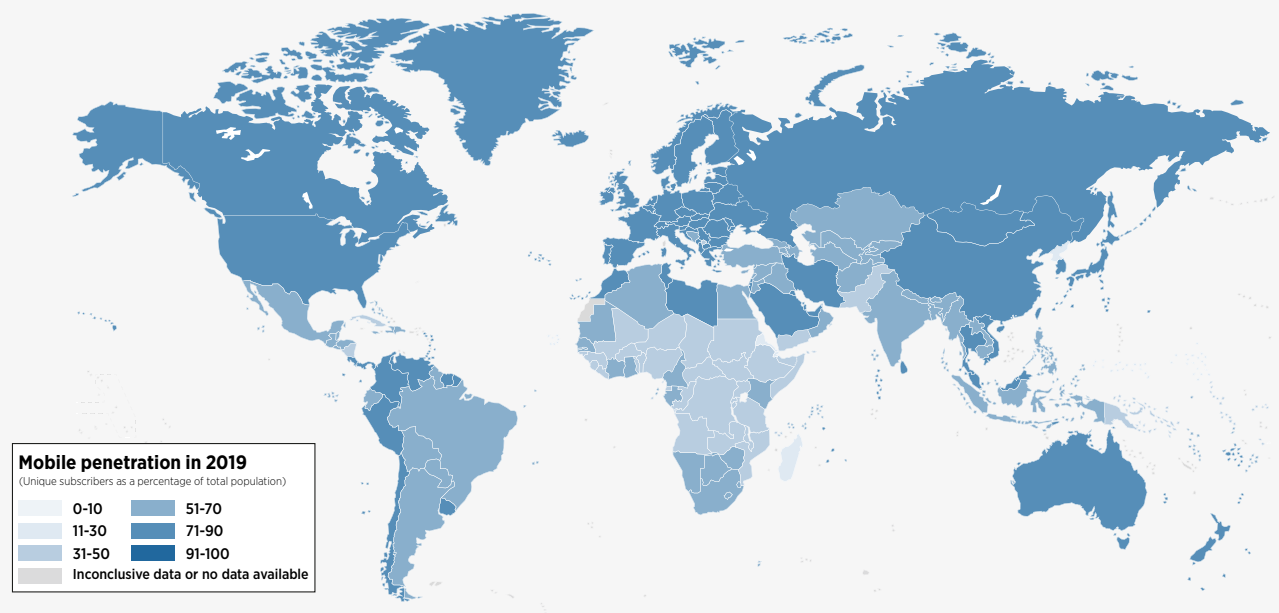


Figure 2

Unique mobile subscribers as a percentage of total population (2019)



Mobile penetration in 2009 and 2019

Total connections

Figure 3

Aggregate mobile connections as a proportion of total population (2009)

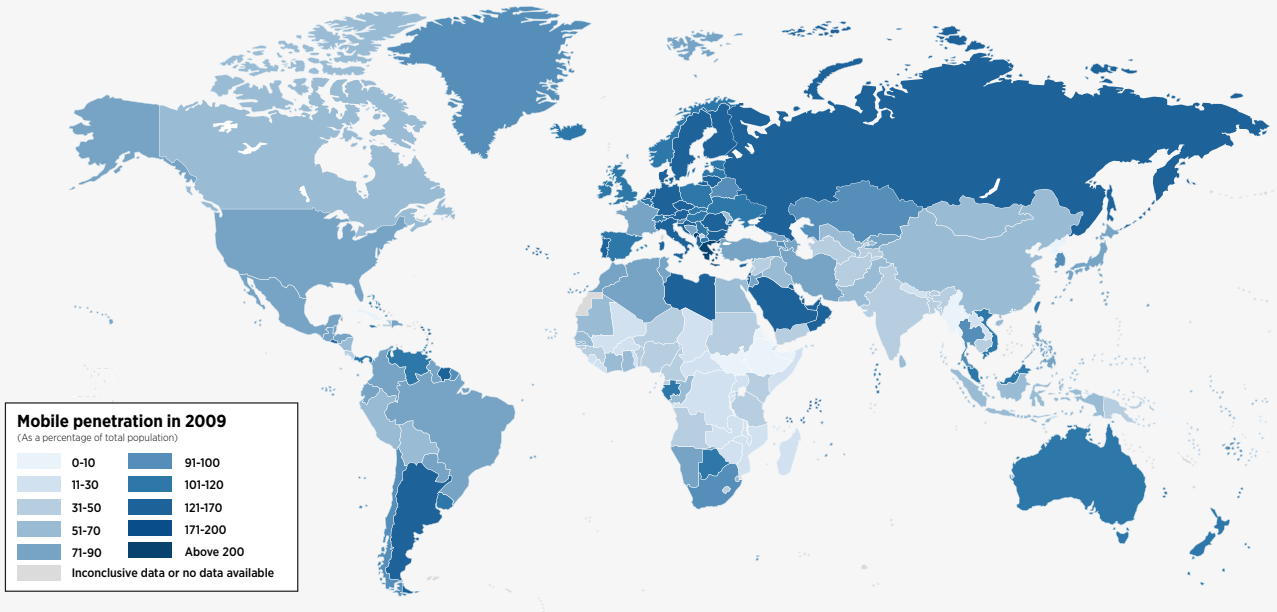
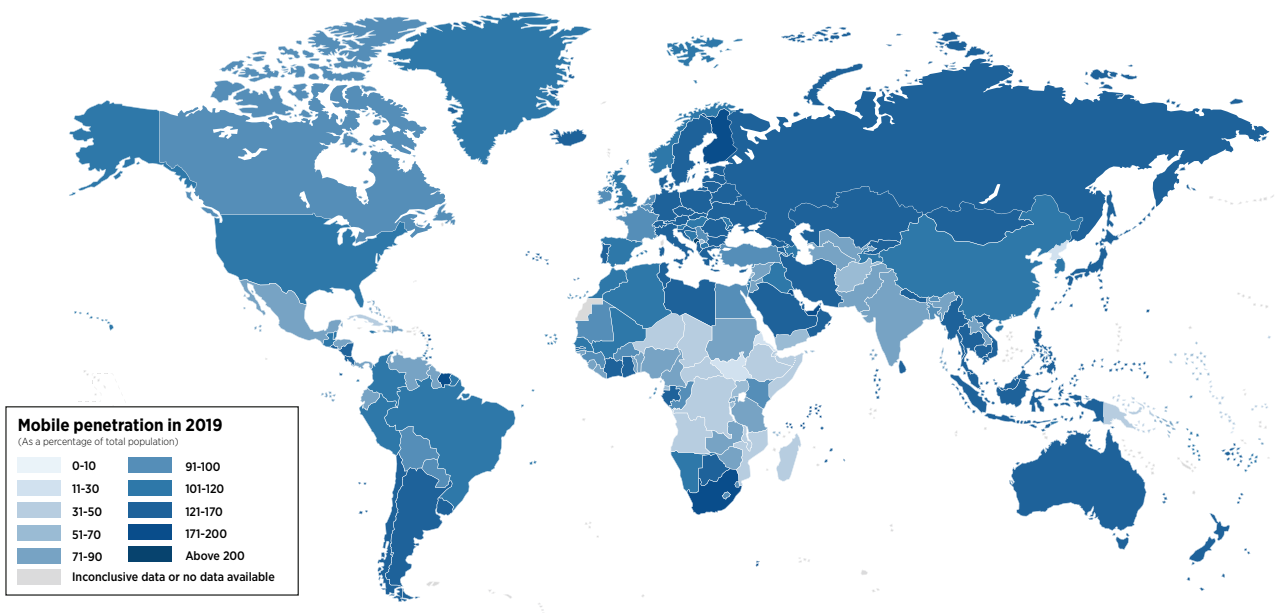


Figure 4

Aggregate mobile connections as a proportion of total population (2019)



03

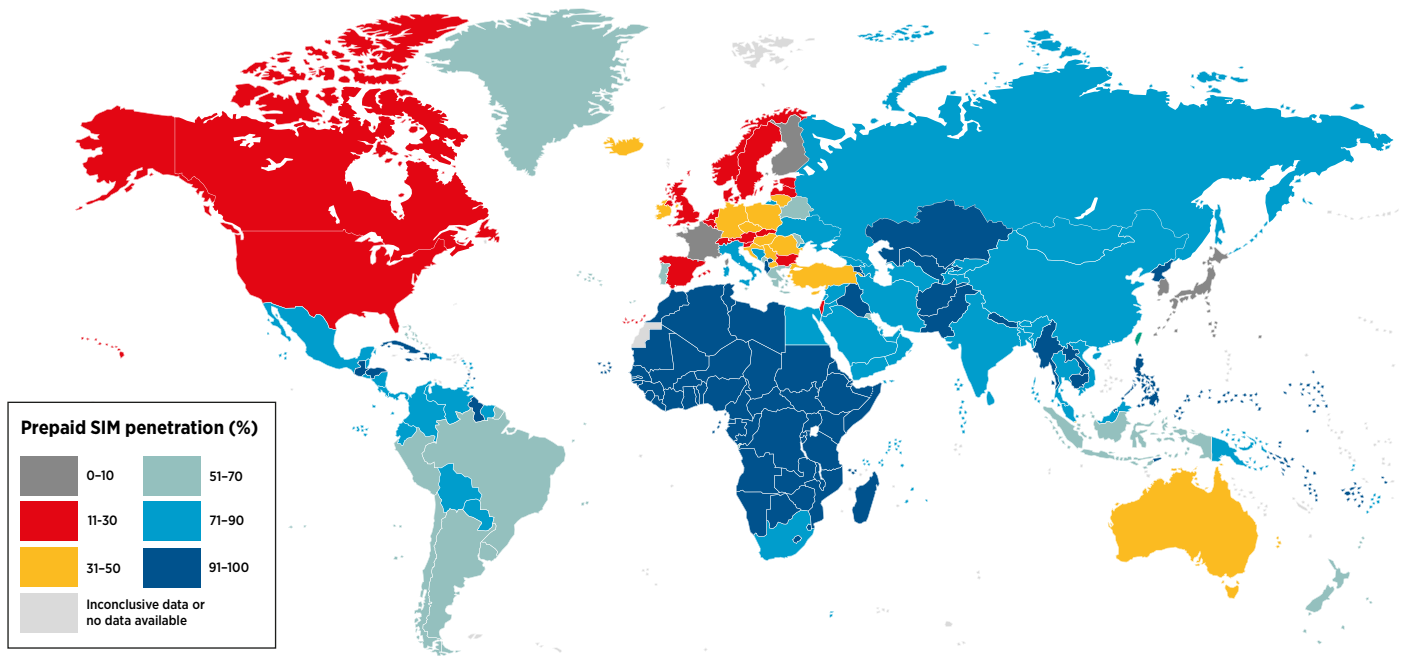
Prepaid mobile SIM penetration

Post-paid SIM cards are usually linked to fixed term contracts with a mobile network operator and tend to involve creditworthiness checks. In contrast, prepaid (widely known as pay-as-you-go) SIM cards are simpler for individuals to obtain. Prepaid SIM cards seem to be preferred option for many mobile users, especially since 73 per cent of all SIM

cards globally are prepaid. 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 79 per cent, Southern America is 68 per cent, Europe is 50 per cent, and North America is 21 per cent.

Figure 5

Share of prepaid connections as a percentage of total mobile subscriptions



04

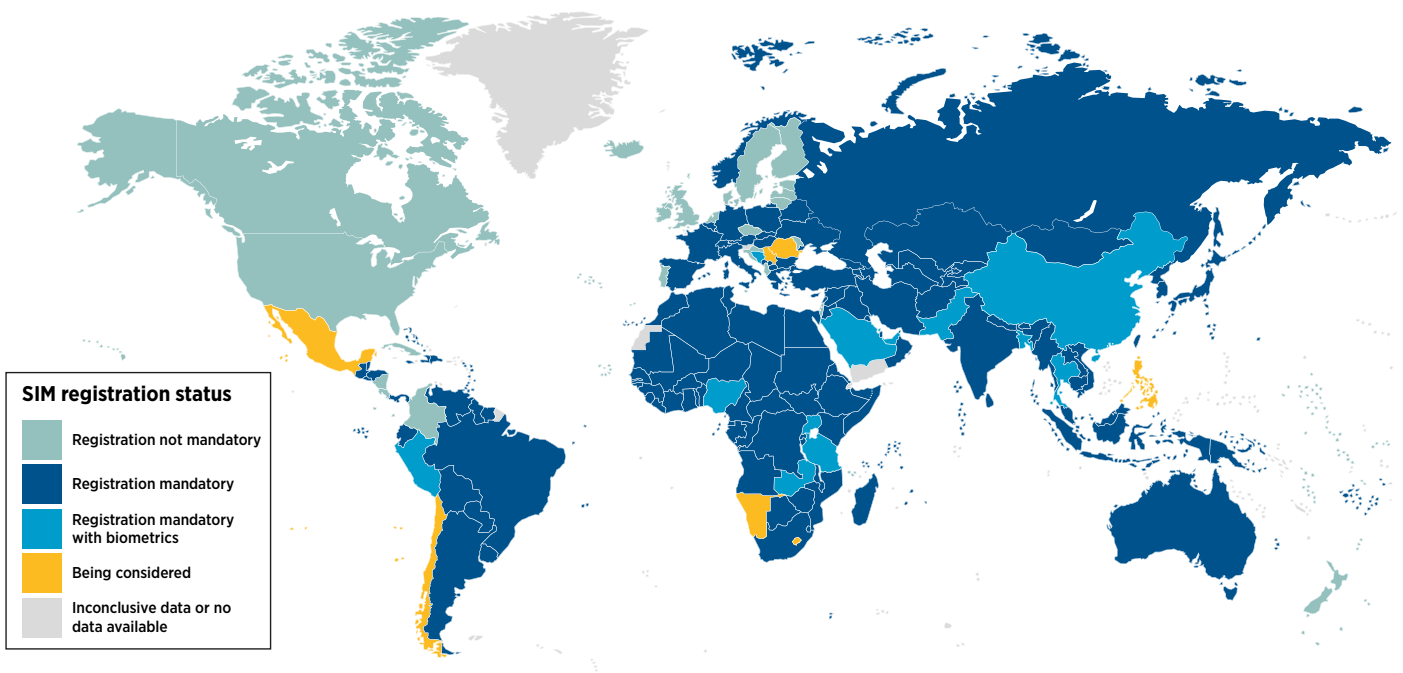
Countries with mandatory SIM registration policies

Mandatory SIM registration is a policy requiring users to provide personal information such as their name, national identification number, address and proof of identity credentials in order to register for or activate a prepaid SIM card. As a standard practice, existing users who fail to register their SIMs within a government-mandated time-period face network disconnection, resulting in loss of access to mobile services. As of January 2020, GSMA research found that the governments of 155 countries mandate SIM registration policies.³

In some circumstances, governments require MNOs to capture a photograph, fingerprints, and other biometric attributes of users in order to complete SIM registration. Eight per cent of countries require mobile operators to use biometric authentication processes when registering their prepaid SIM customers.⁴ In a few countries, MNOs are proactively introducing biometric authentication processes in anticipation of the government mandating this.

Figure 6

Status of SIM registration policies (2020)



3. See countries in the Annex

4. See countries in the Annex

05

SIM registration implementation models

While, 155 countries require individuals 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 categories:

- **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 January 2020, about 81 per cent of the countries (126 of the 155) mandating SIM registration follow the capture and store approach.⁵

- **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 January 2020, six per cent of the countries (10 of the 155) mandating SIM registration follow this approach⁶

- **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) or against a credential held by the customer (such as a chip-based smart ID card). As of January 2020, twelve per cent of countries (19 of the 155) who implement SIM registration allow mobile network providers to verify customers' identification credentials against an approved government database or credential to facilitate the validation process.⁷

In countries where governments do not have credible databases against which mobile operators could conduct identity verification, the approach to proof of identity varies. For example, in some countries an attestation letter from their employers or village elders, as in the case of Nigeria, are acceptable forms of identification for SIM registration.⁸ However, such approaches are increasingly being phased out as they are perceived to be less robust and leave room for identity theft. An increasing number of governments, particularly in Sub-Saharan Africa, are seeking to establish comprehensive digital identification systems as part of their digital transformation strategies, seeking to achieve more robust identity verification when citizens and consumers attempt to access a suite of digital or electronic services (online or offline).⁹

5. See countries in the Annex

6. Ibid.

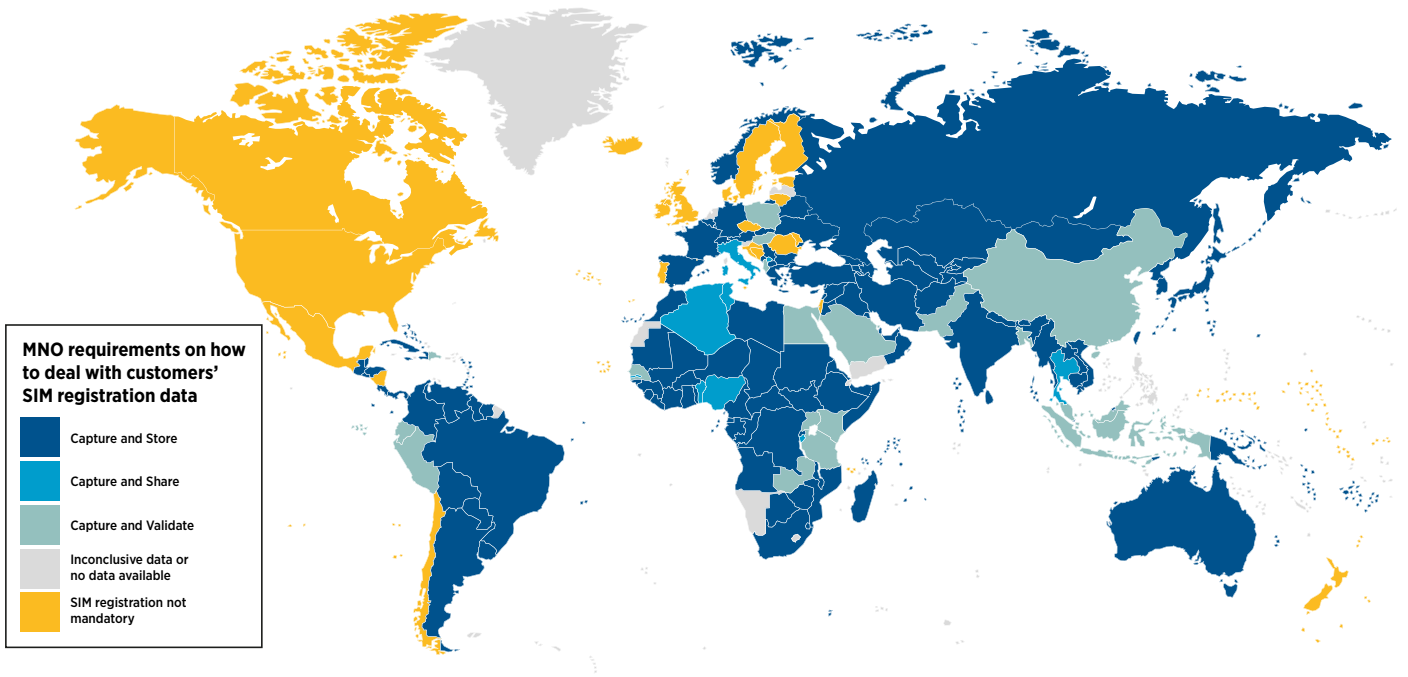
7. Ibid.

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

9. GSMA, 2019, 'Access to Mobile Services and Proof of Identity' - <https://www.gsma.com/mobilefordevelopment/resources/access-mobile-services-proof-identity-global-policy-trends-dependencies-risks/>

Figure 7

Type of mandatory SIM registration policy, by country





06

Linkages between access to identification and access to mobile

Figure 8 illustrates the relationship between identity coverage and mobile penetration across countries where SIM registration is mandated. In seven markets (Armenia, Benin, Guinea, Laos, Malawi, Tajikistan and Togo), more people appear to have a mobile subscription than an official proof

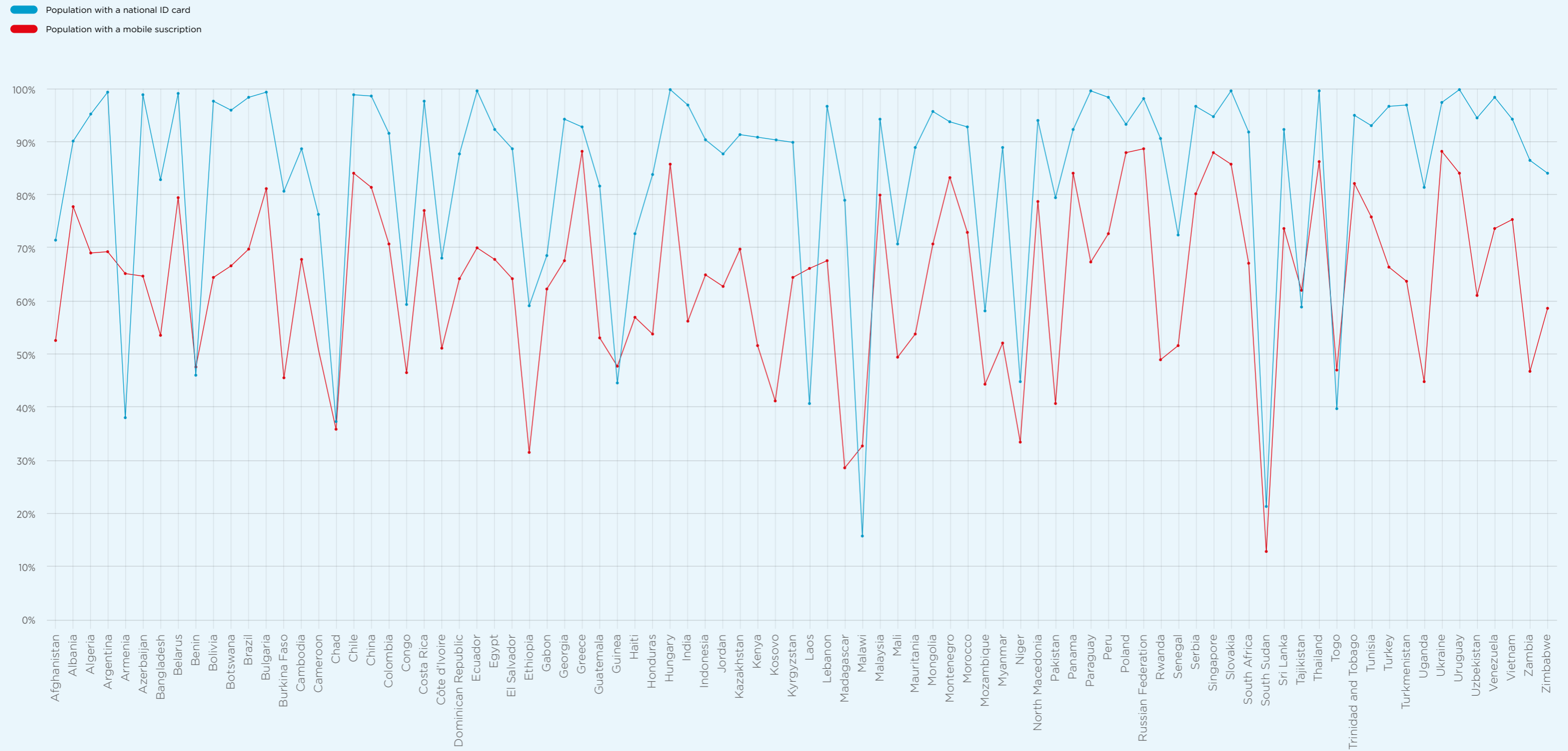
of identity.¹⁰ This may present an opportunity for governments in to partner with local MNOs to expand ID coverage by leveraging their reach and nationwide retail presence (e.g. by supporting enrolment efforts, public awareness campaigns etc).

10. Source: Global Findex Database – data from responses to the question – ‘Do you personally have a [local terminology for national ID card]?’ – posed to individuals in the World Bank’s Findex survey as a proxy for the portion of the population who have an official proof of identification. We also used data from GSMA Intelligence in relation to unique mobile subscriptions as a proxy for the proportion of a country’s population maintain a mobile subscription.

Figure 8

The link between access to ID and access to a unique mobile subscription

Source: GSMA Intelligence, Market Penetration - Unique Mobile Subscribers Q3 2019 and The World Bank, 2017 FINDEX dataset



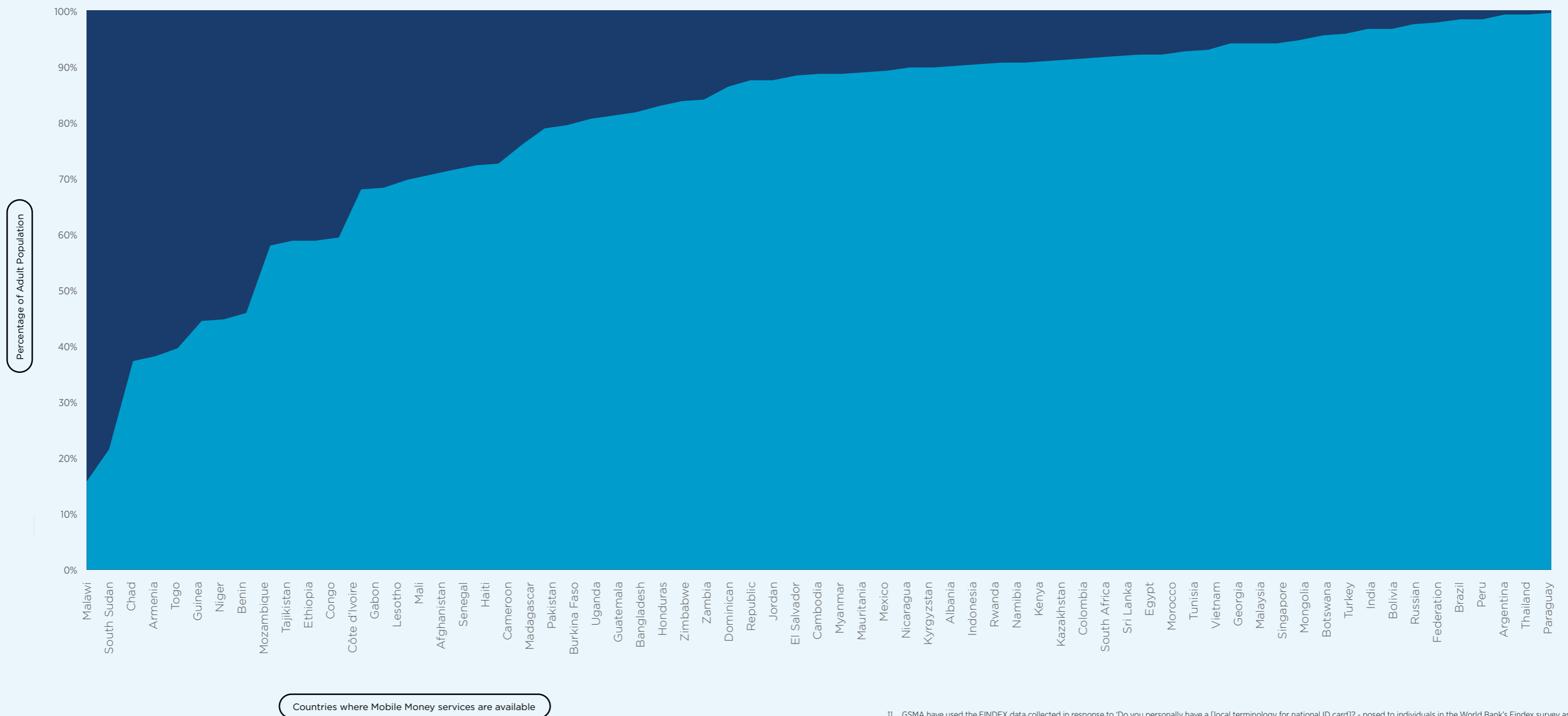
Selection of countries where SIM registration is mandatory from World Bank Findex dataset 2017

Figure 9

Identification coverage in countries where mobile money services are available

Source: The World Bank, 2017 Finindex Dataset¹¹

■ Percentage of adult* population who lack an official identity (at greater risk of financial exclusion)
 ■ Percentage of adult* population with an official identity



11. GSMA have used the FINDEX data collected in response to 'Do you personally have a [local terminology for national ID card]? - posed to individuals in the World Bank's Finindex survey as a proxy for the portion of a country's Adult population

07

Data protection and privacy frameworks

Policy frameworks designed to build consumer trust can influence their acceptance of – and engagement with – identity-linked digital services. With the continued growth of the mobile industry and the number of people able to access mobile services, it is especially important for policy frameworks to engender trust and confidence among users of digital platforms.¹²

In 2019, GSMA conducted end-user research¹³ in four African markets exploring attitudes around privacy and trust in countries with and without comprehensive data protection frameworks, and consumers' willingness to share their personal data in order to access identity-linked digital/mobile services.

Interestingly the research showed that many consumers could not correctly identify whether or not data protection and privacy laws existed in their country. The research also highlighted that vulnerable consumers, those in rural environments with lower levels of education and more basic handsets, tended to be less aware of the risks associated with sharing data.

Overall consumers were clear that they preferred to have control and choice, with the ability to:

- Withhold information at times
- Preserve their dignity and reputation
- Keep certain information (such as financial or health related information) completely secret
- Maintain their own, or their family's safety

Women in particular expressed concerns over safety and potential harassment, a lack of digital literacy, and being less convinced that redress for data breaches would be successful.

12. GSMA, 2019, 'Access to Mobile Services and Proof of Identity' - <https://www.gsma.com/mobilefordevelopment/resources/access-mobile-services-proof-identity-global-policy-trends-dependencies-risks/>

13. GSMA, 2019, 'The role of privacy frameworks in building trust for digital identity services' - <https://www.gsma.com/mobilefordevelopment/resources/the-role-of-privacy-frameworks-in-building-trust-for-digital-identity-services/>

Overall the research showed that those in markets with legal frameworks around privacy and data protection feel more informed, supported, or confident in managing privacy rather than increasing trust in systems. It also showed that overall the appetite to access identity-linked services is universally high, regardless of the presence of legal frameworks, particularly if a clear benefit to consumers is perceived and the service is provided by a sufficiently trusted entity. Further research in additional countries is needed to substantiate these initial findings, but this research highlighted the need for MNOs to be transparent with regards to how consumers data is used, clearly articulate how identity-linked services can tangibly benefit consumers, and consider ways to build and retain consumers' trust.

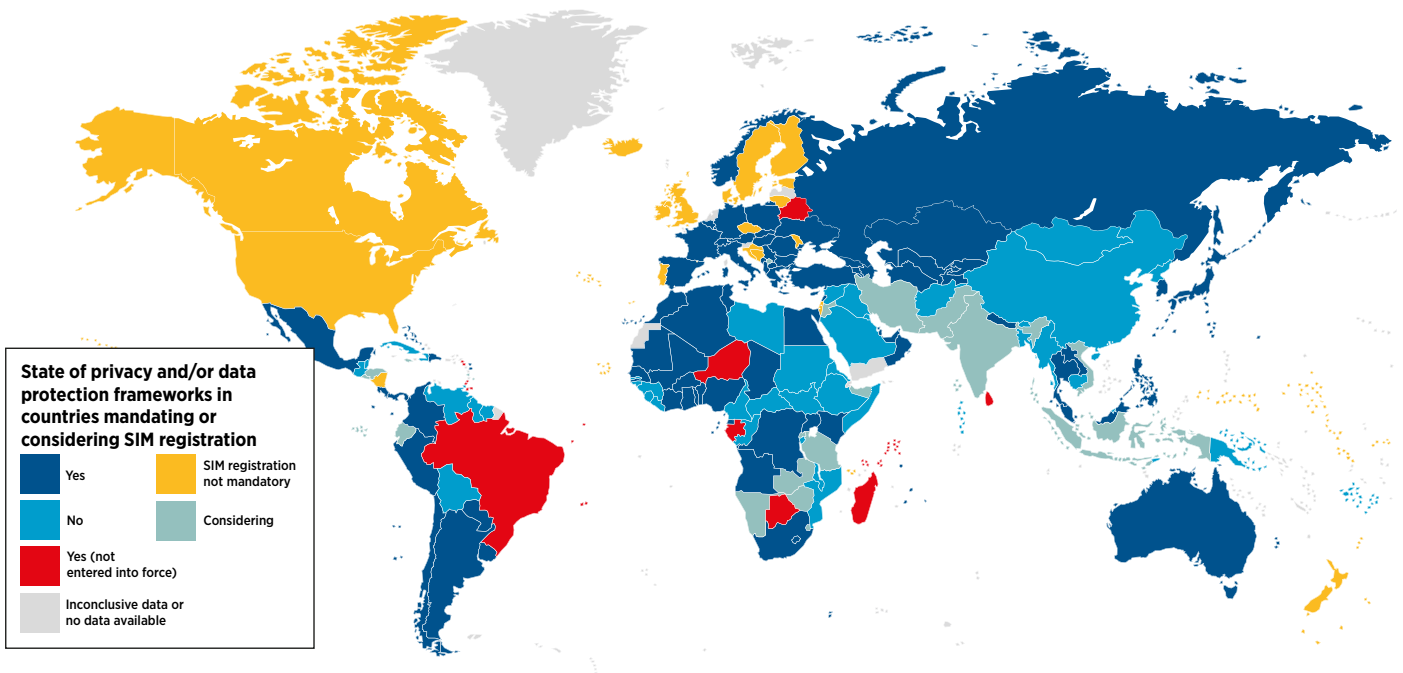
Across the world, a significant number of countries still lack a data protection/privacy framework. Globally, the GSMA found only 59 per cent of countries mandating SIM registration have a Privacy and/or Data Protection framework in place.

Of the countries mandating SIM registration:

- In Africa 16 countries are without a privacy or data protection framework in place while six more are actively considering and five have expressed their intent to introduce a data protection framework, but they have not entered into force yet.¹⁴
- In Asia and the Pacific, 19 countries are without a privacy or data protection framework while six are actively considering it and one has expressed their intent to introduce a data protection law, but it has not entered into force yet.¹⁵
- In Central and South America, nine countries are without a privacy or data protection framework while six are actively considering it and four have expressed their intent to introduce a data protection framework, but they have not entered into force yet.¹⁶
- In Europe, one country is actively considering the implementation of a privacy or data protection framework and one has expressed their intent to introduce a data protection framework, but it has not entered into force yet.¹⁷

Figure 10

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



14. See countries in the Annex

15. Ibid

16. Ibid

17. Ibid

08

Proof of identity in humanitarian contexts: the impact on forcibly displaced persons' (FDPs) access to mobile

According to United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA), a record number of individuals – 168 million – will need humanitarian assistance and protection in 2020.¹⁸ Trends suggest there will be a growing role for mobile technology to play in the delivery of humanitarian assistance to those in need. A significant barrier that remains for forcibly displaced persons is their inability to meet the proof of identity requirements to legally register a mobile SIM card or to open a mobile money account in their own name.¹⁹

In 2020, GSMA found 155 countries implement SIM registration policies, 141 host Persons of Concern (PoCs) to UNHCR.²⁰ We estimate that 68.4 million PoCs (an equivalent to 92 per cent of all PoCs) are hosted in a country that mandates SIM registration. This is an increase of 19 per cent compared to last year. As shown in Figure 11, 18 of the top 20 host countries (to PoC) mandate SIM registration.

An estimated 98 per cent of countries that offer mobile money services, are host to PoCs, meaning that an equivalent of 54.6 million PoCs have the potential to access mobile money services if they can meet the Know-Your-Customer (KYC) requirements of their host country. Fifteen of the top 20 host countries (shown in Figure 11 below) offer mobile money services. All 15 of these also implement SIM registration. Overall, around 72 per cent of all PoCs reside within these countries.

18. <https://news.un.org/en/story/2019/12/1052731>

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

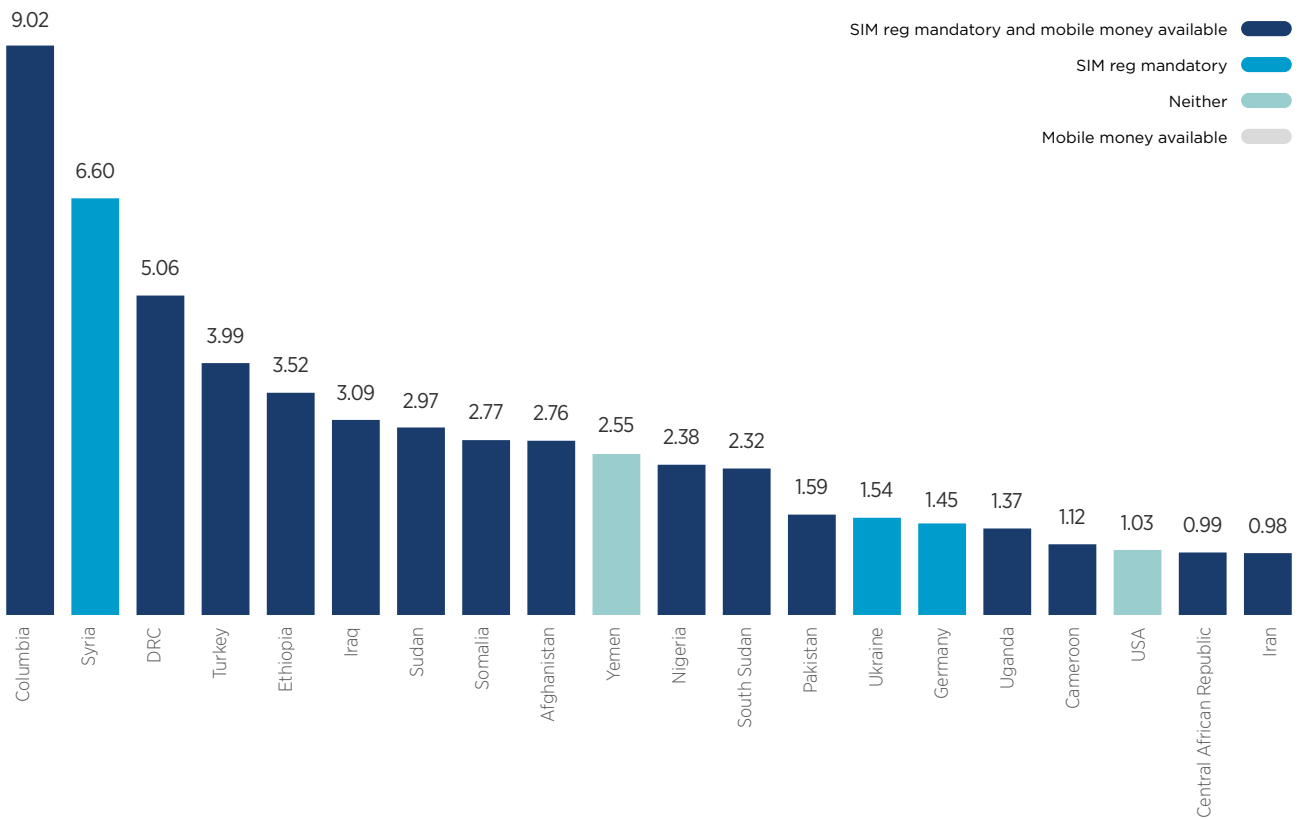
20. While Serbia and Kosovo are captured in the number of countries who host PoCs, they have been excluded from our calculations because the data for PoCs is joint for both countries, so it is difficult to treat them as separate.



Figure 11

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

PoC population (in millions)



Refugees

Refugees make up 27 per cent of PoCs.

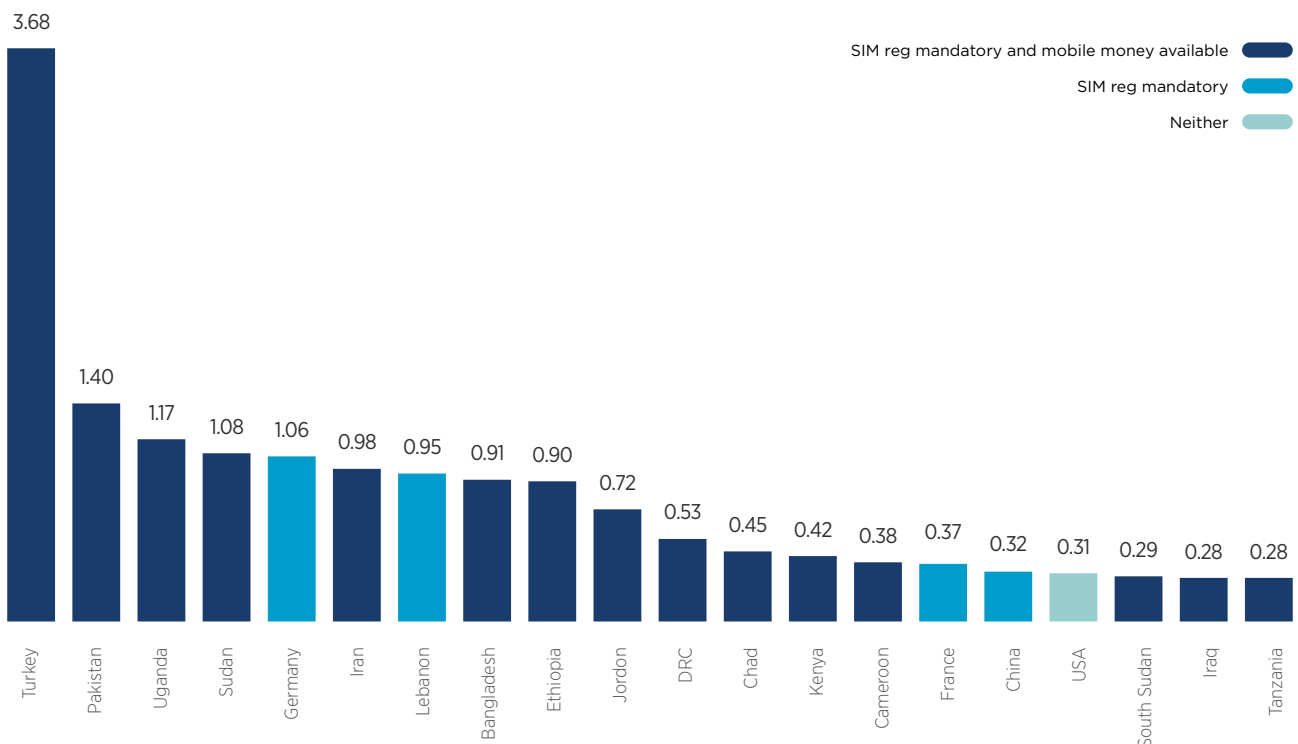
This research found that:

- 173 countries host 20.4 million refugees²¹
- 132 refugee-hosting countries mandate SIM registration, meaning that a total of 19 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 12). An equivalent of 79 per cent of all refugees live within these 19 countries
- Furthermore, 86 refugee-host countries have the potential to deliver mobile money services to 15.3 million refugees.
- Fifteen of the top 20 refugee-host countries offer mobile money services. 66 per cent of all refugees that are hosted by these countries and have the potential to access mobile money wallets.
- Fifteen of the top 20 refugee host nations implement mandatory SIM registration and offer mobile money services. 13.5 million refugees reside in these 15 countries and therefore have the potential to be digitally and financially included only if they have access to formal identification that is recognised by their host country government.

Figure 12

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

Refugee population (in millions)



21. While Serbia and Kosovo are captured in the number of countries who host refugees, they have been excluded from our calculations because the data for refugees is joint for both countries, so it is difficult to treat them as separate.



Annex Policy landscape, by country

Africa

* Countries who are in the process of introducing a data protection law, however it has not yet entered into force

	SIM registration mandated	SIM registration mandated using biometrics	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 or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Algeria	✓						✓		✓					
Angola	✓					✓			✓					
Benin	✓						✓		✓					
Botswana*	✓					✓			✓					
Burkina Faso	✓					✓			✓					
Burundi	✓						✓			✓				
Cabo Verde				✓										
Cameroon	✓					✓				✓				
Central African Republic	✓					✓				✓				
Chad	✓					✓			✓					
Comoros				✓										
Congo	✓					✓			✓					
Congo, Dem. Republic	✓					✓				✓				
Côte d'Ivoire	✓					✓			✓					
Djibouti					✓									
Egypt	✓							✓	✓					
Equatorial Guinea	✓					✓			✓					
Eritrea	✓					✓				✓				
Ethiopia	✓					✓					✓			
Gabon*	✓					✓			✓					
Gambia	✓						✓			✓				
Ghana	✓					✓			✓					
Guinea	✓					✓				✓				
Guinea-Bissau	✓					✓				✓				
Kenya	✓							✓	✓					
Lesotho			✓										✓	
Liberia	✓					✓				✓				
Libya	✓					✓				✓				



* Countries who are in the process of introducing a data protection law, however it has not yet entered into force

	SIM registration mandated	SIM registration mandated using biometrics	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 or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
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	✓					✓				✓				
Eswatini	✓					✓					✓			
Tanzania		✓						✓			✓			
Togo	✓					✓			✓					
Tunisia	✓						✓		✓					
Uganda		✓						✓	✓		✓			
Zambia		✓						✓			✓			
Zimbabwe	✓					✓					✓			

Asia and the Pacific

* Countries who are in the process of introducing a data protection law, however it has not yet entered into force

	SIM registration mandated	SIM registration mandated using biometrics	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 or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering 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	✓					✓								✓
North Macedonia	✓					✓			✓					
Malaysia	✓							✓	✓					
Maldives	✓					✓				✓				



* Countries who are in the process of introducing a data protection law, however it has not yet entered into force

	SIM registration mandated	SIM registration mandated using biometrics	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 or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering a data privacy framework
Marshall Islands				⬇										
Micronesia				⬇										
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

* Countries who are in the process of introducing a data protection law, however it has not yet entered into force

	SIM registration mandated	SIM registration mandated using biometrics	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 or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering 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				✓										



* Countries who are in the process of introducing a data protection law, however it has not yet entered into force

	SIM registration mandated	SIM registration mandated using biometrics	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 or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering 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 and Latin America

* Countries who are in the process of introducing a data protection law, however it has not yet entered into force

	SIM registration mandated	SIM registration mandated using biometrics	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 or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering 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				✓									✓	



* Countries who are in the process of introducing a data protection law, however it has not yet entered into force

	SIM registration mandated	SIM registration mandated using biometrics	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 or considering mandating SIM registration and have or are considering a data privacy framework	Considering SIM registration and have no data privacy framework	Considering SIM registration and have a data privacy framework	Considering SIM registration and have or are considering 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 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

