Regulatory and policy trends impacting Digital Identity and the role of mobile

Considerations for emerging markets

October 2016

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

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

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

Digital Identity

The GSMA's M4D Digital Identity programme works with the mobile industry, governments and the development community to build the capacity and partnerships required to deliver scalable digital identity solutions in emerging markets that will accelerate greater social, political and financial inclusion.

For more information, please visit the GSMA Digital Identity website at **www.gsma.com/mobilefordevelopment/ programmes/digital-identity**

Contents

Report authors:
Michael Kende
Rory Macmillan (Macmillan Keck)
Yiannis Theodorou (GSMA)

Executive Summary

The United Nations' Sustainable Development Goals (SDGs) aim for every person to have a legal identity by 2030[1]. Currently, over 1.5bn people lack any form of legally recognised identity and this disproportionally impacts rural residents, poor people, women, children, and other vulnerable groups in Africa and Asia. Identity systems increase in utility as they become digital. Using mobile operators' unique resources, mobile-based digital identity offers a unique, secure and scalable form of identity, catalysing greater socio-economic impact in emerging markets.

To facilitate the introduction and take-up of digital identity solutions, key stakeholders need to take into account several emerging trends that are influenced by – or help shape – policy and regulation. Several country-specific factors present opportunities and risks that may impact the effectiveness, reputation and commercial viability of digital identity solutions. For example, whether a country has built or plans to develop a centralised identity ecosystem, whether such ID system is digital or paper-based, the applicable data protection and privacy laws and regulations, and the security and surveillance context.

This report reviews the gathering momentum towards digital identity programmes and the implications for mobile operators' role in enabling identity solutions (Trend 1). There is considerable diversity in approaches to digital identity, making harmonisation, standardisation, federated approaches and interoperability particularly important (Trend 2).

In some countries, mobile operators are already subject to identity-related requirements, such as mandatory SIM registration and know-your-customer (KYC) obligations for mobile financial services. Taking an integrated policy approach to these requirements would boost momentum towards mobile-based digital identity and the activities mobile operators already engage in, as well as developing models for mobile operator engagement, such as public private partnerships (Trend 3).

The importance of a robust 'trust framework' is increasingly appreciated. This comprises the technical specifications, standards and procedures, data protection, privacy and other identity-related laws, regulations, and consumer expectations. For digital identity to grow, these must be aligned to ensure operational effectiveness and a viable allocation of risk and opportunity through rights and liabilities, while ensuring respect for privacy (Trend 4).

Finally, increasing reports of government requests to access communications pose a risk to consumers' trust and perceptions of digital identity solutions. Regulators, policymakers and mobile operators need to promote transparency and proper lawful management of government access requests (Trend 5). Government leadership to bring together key stakeholders is essential. Equally, mobile operators should engage with governments, regulators, standards-setting bodies and others to demonstrate the opportunity of mobile-based digital identity services in support of the SDGs.

1 SDG 16.9

Introduction

The ability to prove that you are who you say you are is a fundamentally important building block of economic, financial and social development and inclusion. Proof of identity is generally necessary to access basic services such as healthcare, education and financial services, and to vote in elections. Yet the World Bank estimates that more than 1.5 billion people do not have access to formal identification documentation – and this disproportionately impacts vulnerable groups in developing countries across Africa and Asia.[2]

Recognising this, the SDGs aim for every individual to have "free and universal legal identity, including birth registration by 2030."[3] Because they can be used to access multiple different public and private services, effective identity systems are instrumental for realising other SDGs.[4]

Many countries are beginning to roll out identity systems, with different designs, involving different institutions, and with different levels of adoption. Some countries are beginning to 'leap-frog' directly to digital identity systems.

A robust digital identity framework could offer new opportunities, particularly for countries with currently low identity coverage. As we advance into the digital age where more transactions take place online, the ability to prove a unique identity in the virtual world, as well as the analogue world, becomes increasingly important for economic and social inclusion. Widespread availability and adoption of digital identity is necessarily a key element in reducing the divide between those who have access to and use digital services and those who do not.

Robust digital identity systems can deliver major gains in coverage, cost and reliability. India's Aadhaar programme aspires to full coverage by bringing the entire population into a digital identity system to serve as a cornerstone for all interactions with government.[5] Using iris scanning, and monitoring the enrolment process for quality, the cost of each Aadhaar identity number was assessed in 2013 to be "the lowest recorded for any authentication system worldwide."[6]

Operating the most widespread digital communication system in any given developing country, mobile operators can play a valuable role in digital identity systems, including notably in remote and rural areas.[7] This, combined with their nationwide agent networks, connections to digital devices in peoples' pockets, know-your-customer (KYC) processes and customer relationships, positions them well to be involved at various stages of digital identity systems, which is the focus of this report.[8] The opportunity for mobile operators arises in registering individuals and their attributes, verifying government-issued identity credentials against a centralised database in real time, authenticating identity in transactions, and may extend to certifying and time-stamping documents and signatures.

Mobile operators may be particularly useful in helping governments establish identities, and in introducing or complementing national identity systems, such as for birth registration, driving licences and a variety of other public sector uses. Mobile operators have been involved in birth registration systems for instance in Tanzania, Uganda, Ghana, Senegal, Pakistan and several other countries, playing a vital role in bringing the population into a government identity system.[9]

2 World Bank, ID4D Strategic Framework, January 2016, available at http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf

3 SDG 16.9. The full list of SDGs is available at http://www.un.org/sustainabledevelopment/sustainable-development-goals/

4 Mariana Dahan and Alan Gelb, The Role of Identification in the Post-2015 Development Agenda, World Bank Working Paper 2015.

5 Aadhaar is administered by the Unique Identification Authority of India (UIDAI); see https://uidai.gov.in/ for more details on the program.

6 At a cost of under US$3 per head, UIDAI keeps costs low by relying on remote cell-phone authentication against the central data base—rather than issuing a costly card to enable off-line authentication— and by requiring minimal information from enrolees. Further certification, proof of nationality for example, must be done in a separate process. Having a unique Aadhaar number issued by UIDAI itself entitles the holder to no specific privileges or programs. Alan Gelb and Julia Clark, Center for Global Development, 2013, Performance Lessons from India's Universal Identification Program, available http://www.cgdev.org/sites/default/files/biometric-performance-lessons-India.pdf

7 See ID4D Strategic Framework at footnote 2

8 Further discussion of the utility of this combination of resources for digital identity appears in other GSMA publications. See for example the GSMA, World Bank Group, and Secure Identity Alliance paper, 2016, Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, at http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf

9 See, for instance, Mobile Birth Registration in Sub-Saharan Africa: A Case Study of Orange Senegal and Uganda Telecom solutions, by the GSMA Mobile Identity Team, at http://www.gsma.com/personaldata/wp-content/uploads/2013/05/Mobile-Birth-Registration-in-Sub-Saharan-Africa.pdf

Box 1. Birth registration by mobile in Tanzania and Pakistan[10]

Tanzania's Registration Insolvency and Trusteeship Agency (RITA) worked with UNICEF and the mobile operator Tigo to develop a SIM Application Toolkit (STK) application, which functions on GSM feature phones for submission of birth data. The data is sent to the SMS gateway server over the mobile network and delivered to RITA's central server, which decodes the message and stores the birth certificate in a central database, and sends an SMS to the registrar confirming that they can issue the birth certificate to the child. A more scalable version that can be used across different networks has been introduced as an Android application. The programme registered 100,000 in just the first 6 months.

In a UNICEF pilot programme in Thatta district in Pakistan's Sindh Province, a health worker feeds the date and time of the child's birth, parent's names, National Identity Card (NIC) numbers and their address into a smart phone along with photographs of the parents' NICs and transfers these online to the Dhabeji Union Council office for verification. The data is delivered to a council secretary's tablet, verified and approved, whereupon the data is uploaded into the council office database with a Civil Registration Management System (CRMS) number. The parents are then informed that they may visit the council office and receive the birth certificate, at which point the data is transferred to the provincial office of Pakistan's National Database and Registration Authority (NADRA), and then onward to its head office as a permanent record. In 2015, 95 per cent of new-born children in the region were registered within the first six months of their birth, compared to approximately 5 per cent in 2014.

10 See GSMA (2016), Birth Registration in Tanzania: Tigo's support of the new mobile birth registration system. Also, UNICEF Dec 2015 http://www.unicefstories.org/2015/05/11/new-simplified-birth-registration-initiative-for-children-under-five-in-tanzania/, http://www.unicefstories.org/2015/10/16/in-tanzania-you-can-now-get-your-birth-certificate-by-mobile-phone/, and http://www.unicef.org/health/pakistan_90880.html.

The mobile platform extends digital identity to mobile networks, data and devices, whether in registration, provision of attributes, authentication or other parts of identification processes. To exploit the potential for mobile operators to contribute to the development and widespread adoption of digital identity, they and governments face significant challenges. These include: establishing the robustness of the digital identity system, generating trust in that system (and any with which it is interoperable), giving users control over their digital identities, and providing a convenient experience for the consumer. The opportunity for mobile operators to engage in national identity systems is determined by:

- On the supply side, the state of evolution of the identity ecosystem (including, existing penetration of analogue and digital identity, plans for developing these further, and readiness of relevant firms to play a role); and
- On the demand side, the degree to which government and business (especially retail) have been digitised to create a pull for adoption and usage.

This report provides an overview of key regulatory policy trends that will affect how digital identity ecosystems may evolve in developing and emerging markets. It builds upon the GSMA's Mobile Identity, A Regulatory Overview (second edition) published in January 2015 and Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation published jointly in July 2016 by the GSMA, the World Bank Group and Secure Identity Alliance. This report is intended both for mobile operators, to highlight the favourable regulatory trends for offering mobile-based digital identity, and for policymakers to help define an enabling regulatory environment within which mobile networks can be used to help meet the SDGs, starting with establishing identity. It explores five broad trends and offers analysis and considerations as to how these impact mobile operators, policymakers and the development community seeking to reap the benefits of the digital identity opportunity. The themes explored are:

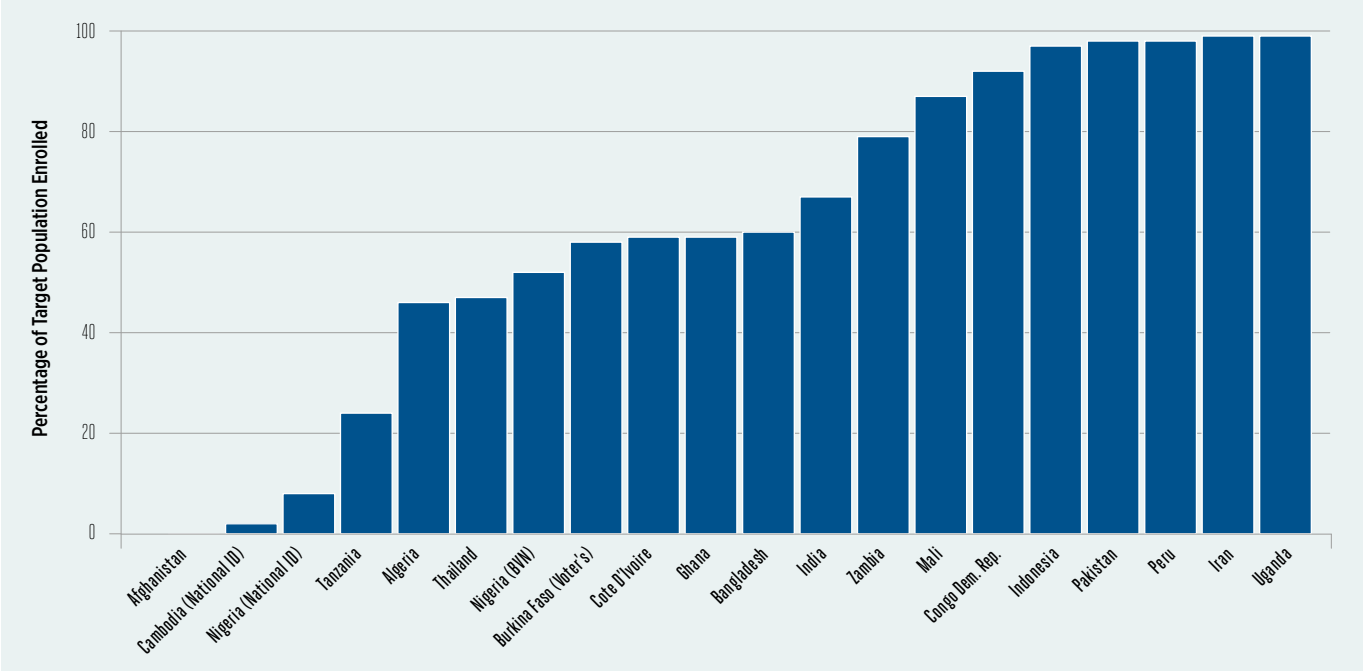
1. The **growing momentum to fill the identity gap,** as reflected in the SDGs and led by efforts to develop national identity systems;
2. The **diversity of approaches** to leap-frogging analogue identity programmes to move to digital systems;
3. The degree of **integration of government policies** on identity-related requirements applicable to, and activities of, mobile operators (registration of subscriber identity modules (SIM) and KYC in mobile financial services) and development of structures for mobile operators to participate in digital identity;
4. The **trust framework** necessary to produce robust, successful digital identity systems, comprising technical specifications, standards and procedures, the regulatory framework relating to data protection and privacy, and the rights and liabilities under broader law; and
5. The **impact of government surveillance requirements** on that trust framework and trust itself.

Trend 1: Digital identity gathering momentum

From identity to digital identity

The first trend is an increased drive by governments to establish identity, a trend that the SDGs seek to accelerate. This is building the demand that mobile operators can help meet. There is a marked growth in governments introducing new, or developing existing, national identity programmes, with many being adopted within the last 5 – 10 years.[11] Some national programmes have already achieved substantial coverage, as shown in Figure 1.

FIGURE 1. COVERAGE RATES OF NATIONAL ID PROGRAMMES.



Source: ITU Review of National Identity Programs 2016

A core objective of such programmes is to ensure that all persons have a 'foundational' identity, issued and recognised by government, typically according to law, for inclusion in government programmes and services. At the same time, many government departments and commercial firms issue 'functional' identities, i.e., developed to access the service concerned, such as a social security number, driving licence, healthcare ID or financial services ID.

The drive to build national identity systems promises huge benefits in terms of:

- Increasing access to government, financial, health and other services;
- Improving lower income, gender and rural inclusion (in other words, helping to meet a number of the other SDGs[12]); and
- Reducing losses from fraud and inefficiencies from bureaucratic paperwork.

11 Of the 48 identity programs the ITU reviewed in a recent study, 29 were introduced in the past decade, and 14 of those in the past five years. See ITU, Review of National Identity Programmes, available here.

12 The UN Sustainable Development Goals include increasing access to healthcare (SDG 3), education (SDG 4), financial services (SDG 8 and 9) among other goals whose access requires an individual to be able to assert and verify their identity. See http://www.un.org/sustainabledevelopment/economic-growth/ for more details on the SDGs.

As noted above, these systems can leap-frog traditional identity programmes in countries where little identity has been established. In countries with established programmes, they can be used to extend reach to the 'last mile' of unregistered citizens, widening access to identification itself in countries where many do not have a foundational identity. At the same time, those with existing identification can migrate to the new digital identity system to access e-government, e-commerce and a host of other digital services including financial services.

International donor organisations have been deeply involved in supporting national digital identity systems, largely with a view to economic and social development. Among other drivers of this change, the World Bank's Identification for Development (ID4D) programme and the GSMA's Digital Identity programme seek to increase developing countries' use of modern technologies for national identity systems.[13] For example, the UK Department for International Development (DfID) has provided catalytic funding to the GSMA Digital Identity Programme to help develop and drive how mobile technology can enable inclusive and socially impactful digital identity (see Birth registration by mobile in Tanzania and Pakistan on page 5). The GSMA and the World Bank collaborated together on the Shared Principles paper discussed above.[14] The Inter-American Development bank has supported several civil registries, and the United Nations Development Programme (UNDP) assists with strengthening electoral systems.[16]

Implications for mobile-enabled digital identity

With this wave of activity at national and donor level, there is scope for governments and mobile operators to collaborate, and to engage with donors, to realise the potential for mobile in digital identity systems. This would include seeking the systematic integration of mobile networks and technology, and mobile operators themselves, into donor programmes. Such collaboration might start by analysing the existing digital infrastructure in a country embarking on developing digital identity, considering how existing communications channels (SMS, USSD, 3G, 4G) could be employed, examining the potential for SIM-based mechanisms for authentication, and ensuring that any existing mandatory KYC processes such as SIM registration are coordinated (and in some cases integrated) with digital identity programmes. (See Trend 3 below.)

In addition, governments run and donors support many demand-side programmes, i.e., applications that require identification services. Where these services can be accessed through mobile phones, or where the mobile phone could be a component in authenticating the user, there is scope for strengthening the role of mobile operators in providing identity services. Such initiatives would support a more holistic development strategy for identity, ensuring that identity is not merely a cost item in individual programmes but is addressed across sectors, bringing value both to users, the private and public sectors.

Thus, and as further discussed below, mobile operators can play a substantial, positive role in helping governments to meet their goals while also using identity to offer new value added digital services. However, as seen in the next trend, how they do so will depend on the policy approach in any given country or region to digital identity.

13 New systems are being established, for instance building on an existing World Bank cash transfer programme in Guinea after the Ebola crisis to help people receive essential services such as healthcare and access financial services such as loans. In Ghana, the World Bank is helping the country's National Identity Authority institute a national identity card that uses fingerprints for registration. The project targets Ghana's entire population of 25 million, and will better connect citizens to social and other services, as well as giving the government a better sense of the needs of its citizens. See World Bank Group, Brief on Digital Identity, available at http://pubdocs.worldbank.org/pubdocs/publicdoc/2016/2/332831455818663406/WorldBank-Brochure-ID4D-021616.pdf.

14 See http://www.gsma.com/mobilefordevelopment/programme/digital-identity/digital-identity-takes-look-tigos-support-new-mobile-birth-registration-system.

15 See footnote 8.

16 See Mariana Dahan and Alan Gelb at footnote 4.

Trend 2: The diversity of digital identity

Digital identities are 'two-sided markets'. On the one side, the success of a national identity system depends on the number of citizens who sign up to use it, and on the other side, on the number of services and other uses that accept national ID. Increased adoption on one side can increase adoption on the other side, in a virtuous circle.

The proliferation of digital identity is on the rise, both at a national level (government issued IDs linked/offered in digital form) as well as at the functional level (e.g. private sector actors issuing identity credentials to their customers facilitating access to a specific service). However, there is significant diversity in the evolution of digital identity among and within countries. This presents a high risk of fragmentation among resulting systems, limiting the virtuous circle of 'network effects' in the two-sided market. This may also result in wasted cost and lost opportunity to exploit efficiencies of scale and scope. The proliferation of identities and credentials from multiple identity systems is also difficult for the average user to manage, leading to risky practices, such as writing down or reusing passwords, making the user more vulnerable to identity theft or other harms.

In this context, the degree of harmonisation of new systems, interoperability among systems and mutual recognition of digital identities affects the viability of the digital ecosystem and the opportunity for mobile operator involvement.

Variety of approaches to identity systems

Foundational and functional identity systems

Some countries have a strong, centralised national digital identity programme, based on a legally-sanctioned foundational identity, often linked to the particular credential of a national identity card and a central registry. Some countries have instead introduced identity cards only for particular functional purposes, and as a result the shift to digital identity may be more fragmented.[17] India's Aadhaar system leap-frogs past identity cards, relying on direct iris and fingerprint scans for authentication. It serves multiple functions, including recognition by the Reserve Bank of India for opening bank accounts and receiving public subsidies.[18]

The more diverse the types of traditional identity, the greater the potential variety of digital identity systems that may be developed. Even foundational identity programmes differ in terms of who they capture, with most but not all registering only citizens, as opposed to all residents.[19]

The distinction between functional and foundational identity systems is not always clear.[20] For instance, foundational identities may also be useful for commercial, financial and other purposes, where the functional identities used specifically for access to such services can 'piggy back' on the established national identity and authentication systems. For example, by linking a functional registry of one hospital to the national registry, patients can validate themselves at other hospitals linked to the system, and authorise access to their medical records. This may result in a less fragmented system.

17 See ITU, Review of National Identity Programmes, at footnote 10, which found that while national identity programmes usually involve a national ID card (38 out of 48 programmes studied), some countries have introduced voter cards (e.g., Burkina Faso, Zambia, DRC and Bangladesh), many of which have become de facto national IDs. Some have introduced identity cards for ascertaining entitlement to financial services (e.g., Nigeria's Bank Verification Number, or BVN), government services targeted at population segments in poverty (e.g., Cambodian Identification of Poor Households Programme). In some cases, identity cards are issued by regional governments where there is no national ID (as in Ethiopia).

18 See https://eaadhaar.uidai.gov.in/.

19 Some also register residents that are nationals, and others such as Tanzania register also refugees. See ITU, Review of National Identity Programmes, at footnote 10. India's Aadhaar system registers non-national residents. See https://eaadhaar.uidai.gov.in/

20 See Dahan and Gelb at footnote 4.

Attribute requirements

Where countries have national identity programmes, national law will typically require the relevant identity system to comprise a minimum set of attributes.[21] However, there is no internationally recognised definition of identity attributes or credentials other than the standards of the International Civil Aviation Organisation (ICAO) for international travel.[22] Thus there are varied approaches to which attributes should be used in a digital identity, which may depend on the purpose for which the identity is to be used. How this affects mobile operators seeking to provide digital identity services depends on the kind of service to be provided. Mobile operators may be in a position to collect various attributes from their customers, subject to their consent. In accessing some services, it may be that only select attributes need to be confirmed in the authentication process.

Levels of assurance

Different types of services and transactions require different levels of assurance (LoA) that the digital identity being claimed is correct and being used by the individual in question.[23] In each case, the level depends on the degree of confidence in the identity that is invoked, characterised by the technical specifications, standards and procedures employed with a view to decreasing or preventing misuse or alteration of the identity.

The level of assurance sought will depend on an assessment of the level of risk of failure or breach and the sensitivity of the service provided. Access to Government, health and financial services will often require a higher level of assurance than other services, for instance an age verification service enabling teenagers to watch an age-restricted movie at a movie theatre.

Mobile operators are particularly well-suited to providing high levels of assurance using various control mechanisms, such as multi-factor verification, and thus can confidently handle such robust system requirements.[24] But electing how to design a digital identity system will depend on what is required for the purpose of the system, as well as what is required by law (see Trend 4 and also Box 2 on the GSMA's Mobile Connect solution).

Federated identity

Given the range of services requiring identity, the need for efficiency in the provision of identity systems has led to the emergence of identity provider platforms that are able to manage identities and credentials for multiple service providers. A common example is the use of government IDs for other services. In some cases, service providers may actively seek to rely on government IDs as a sensible short cut – a 'one-stop shop'. In others, the government may actively require the service provider to rely on the government-issued ID (e.g. to access services involving high-value monetary transactions).[25]

Service providers increasingly rely on federated identity, where a third party carries out the identification process. This enables secure exchange of identity credentials between organisations. The identity data is thus 'portable' across different systems and service providers, allowing the user to use the same credential and authenticator in transactions with more than one service provider. The GSMA Mobile Connect[26] is based on an open standard solution that utilises the OpenID Connect protocol and offers broad interoperability between mobile operators and service providers (including governments in the case of e-Gov services – See Box 2).

In the case of identities used to access government services, governments have tended to prefer to manage enrolment, credentials and authentication themselves, procuring systems as needed. Yet, over time, governments may, when considering the costs, risks and adequacy of procedures involved, become willing to rely on other carefully selected players. This might include relying on identity assertions by reliable third parties such as banks or telecommunications operators, based on suitable screening processes.

21 Typically required attributes are name and date of birth. Other attributes, such as previous names, place of birth, address, gender, marital status, parents' names, whether a person has children, and others may be relevant in particular contexts.

22 See Dahan and Gelb at footnote 4 and http://www.icao.int/Security/mrtd/Pages/MRTDGlossary.aspx.

23 The required level of assurance is assessed by each organisation in light of factors such as inconvenience, risk of financial loss or liability, harm to the entity's programmes or public interest, unauthorised release of sensitive information, personal safety, and civil or criminal violations. For more information on levels of assurance, see Shared Principles at footnote 8.

24 Identity can be authenticated in various ways over mobile phones. These include generating and receiving one-time log-in passwords, storing credentials on the device's secure element for purposes of logging in, as well as signing and encrypting documents, or using NFC (where it is enabled) to store and use credentials. See Smart Card Alliance, Mobile Devices and Identity Applications (2012).

25 This is particularly so where the government ID has been established with a view to providing access not merely to government services but to other services such as financial or telecommunications services.

26 http://www.gsma.com/personaldata/mobile-connect

For instance, the UK's GOV.UK Verify allows certified companies to act as 'identity providers' who, when following prescribed procedures and standards with requisite levels of assurance, will verify an individual's identity for purposes of accessing government services.[27] No ID card is issued, and indeed no central identity register is established. The US NSTIC and Connect.gov system is taking a similar approach.[28] In Canada, customers of enrolled financial institutions can use their existing banking credentials to access online Canadian government services under the SecureKey Concierge system.[29]

How this will evolve in the context of government identity systems elsewhere may depend on the degree to which these are centralised or decentralised. Countries with centralised government or an existing non-digital national identity system are more likely to adopt centralised digital identity registration. Those with more decentralised government (e.g., larger number of regional governments and government agencies) are more likely to allow decentralised identity registration, working on the basis of federation agreements for single sign-on. The structure of the digital ID systems may depend on how any non-digital ID systems functioned historically.[30]

The use of federated identity creates numerous complex regulatory issues, in particular around the responsibility an identity provider bears to parties that rely on the correctness of the identity established, data about the person (e.g., date of birth) included in the identity attributes, as well as the credentials used. Whether such responsibilities are contractual, determined by warranties given, or imposed by statute or tort law, can become a complex issue, and (as discussed in Trend 4) uncertainty over this may impede the development of identity systems, including the participation of mobile operators in them.

Interoperability

Closely related to federated identity is the question of interoperability, where identities generated under different identity systems will be recognised by other systems in a manner that makes them operationally effective.

One example of a major effort to increase interoperability is Europe's eIDAS Regulation[31], which sets a framework for mutual recognition among member states of digital identities established and managed according to standards, including different levels of assurance. As a result, various services are now officially recognised in the region, including electronic authentication, electronic seal (electronic signature for legal entity), electronic time-stamp, electronic documents, electronic delivery services, and website authentication. While national governments still have the prerogative to determine electronic identification, whenever an electronic identification is used, the other European member states are obligated to recognise it. To implement this, an interoperability framework is required, including minimal technical requirements relating to the connection of nodes of different systems, protection of privacy and confidentiality of data exchanged, storage of data, data integrity and message formats.[32]

Where different levels of assurance frameworks are used by different digital identity systems, a key element in enabling interoperability is 'mapping' the relevant level of assurance from one system to the other.[33] The meri t of standards lies in the establishment of common references for these matters.[34] This makes it more feasible to develop interoperability of identity systems and federated identity, i.e., establishment of an identity that is usable for various different purposes, recognised by each of them.

27 Companies such as Verizon, Experion, Barclays, the Post Office, the Royal Mail and others have become certified identity providers. See https://identityassurance.blog.gov.uk/tag/certified-companies/.

28 See https://www.nist.gov/itl/nstic.

29 See http://www.skconcierge.us/the-canadian-experience/.

30 See OECD (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. Available at http://dx.doi.org/10.1787/5kgdzvn5rfs2-en

31 Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

32 Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

33 Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

34 ITU-T Recommendation X.1254 | ISO/IEC DIS 29115 -- Information technology – Security techniques – Entity authentication assurance framework, available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138

Implications for mobile-based digital identity

Where none exists, there is significant opportunity to involve mobile operators in developing a foundational digital identity that can be used for multiple purposes. Where a foundational digital identity programme exists, mobile operators may be able to bring to it the functionality of mobile ID, with additional benefits of convenience and security. Where no national identity programme is planned, mobile operators could alternatively become involved in developing particular functional identities, which may even become usable for many purposes beyond the primary function.[35] The extent to which this may occur depends on the degree of interoperability and federated identity.

There may also be opportunities for mobile operators in a fragmented identity environment, i.e., where government is decentralised, where decentralised non-digital systems exist, or where decentralised digital systems exist but have not achieved interoperability through federation agreements. Digital identity furnished by mobile operators or with their cooperation could be a common platform for sign-on across different national and regional government bodies and agencies.

Where a mobile-based digital identity is to be used to access government services, there may be both a commercial incentive and a public benefit to ensuring interoperability among mobile operators from the outset in order to achieve maximum utility and scale of use for the identity.[36] This might for example involve enabling a user to authenticate him or herself to a service provider on any mobile network using his or her mobile phone number and a PIN after a prompt.[37] The GSMA Mobile Connect digital authentication solution offers users a secure way to log-in to websites and applications quickly without the need to remember passwords and usernames.[38]

The bridge that mobile identity can offer between public and private makes it all the more useful. Private participation in the design of public identity systems may lead to improved interoperability and standardisation not only among public bodies but also with private commercial service providers.

Where government agencies may focus on identity for accessing government services, private firms will recognise the commercial potential for interoperability, have an incentive to seek the broadest possible usage and return, and bring experience from private sector identity systems to bear, enhancing digital government and the digital economy together.

In face of the significant diversity that exists, consistent use of technical specifications, standards and procedures would increase interoperability internationally and simplify the user experience. This could also be expected to foster an open market in identity services, resulting in innovation, cost reduction and growth in take-up and use. Ensuring interoperability and consistent use of technical specifications, standards and procedures would also reduce risk of potential competition problems where dominant players control access to or use of a given digital identity system.[39]

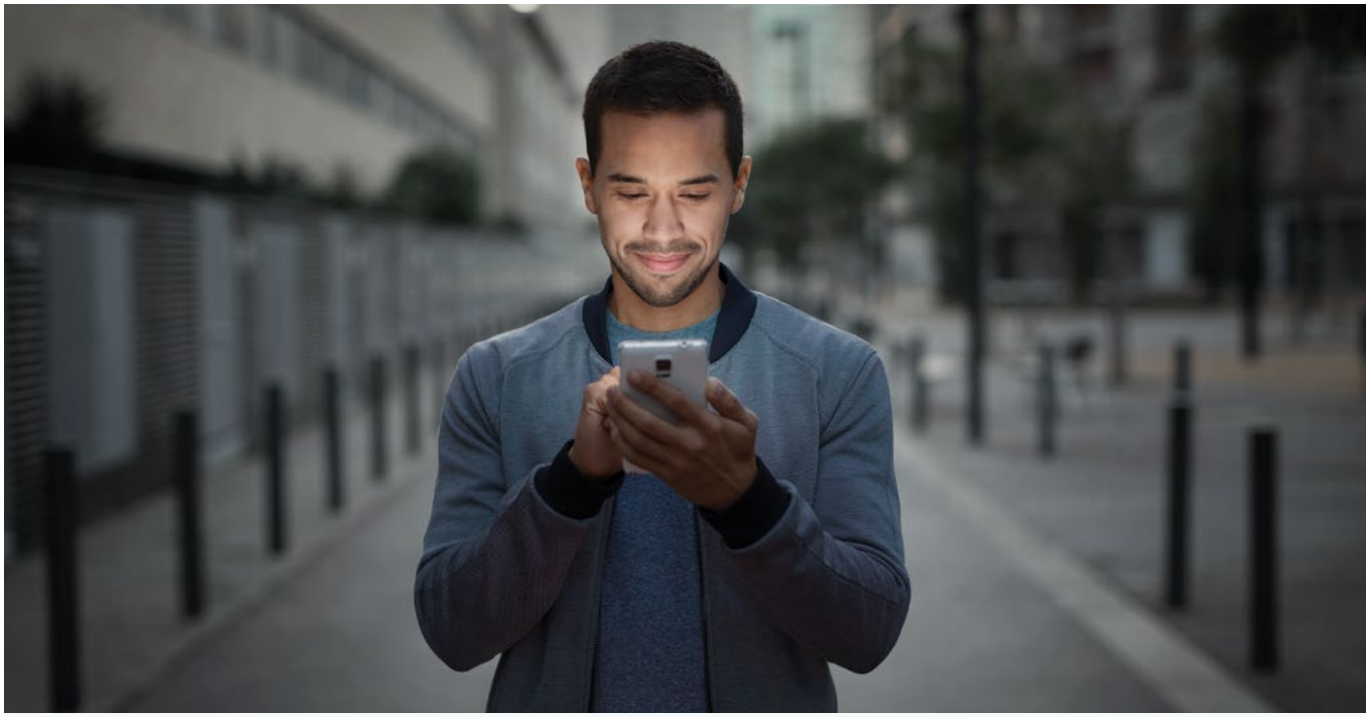
35 Sometimes, functional identities become used in practice as foundational identities, i.e., being accepted for various uses beyond the original purpose (social security numbers, voter registration and driving licences are often used as if they are foundational).

36 See Finnish Mobile ID at footnote 37.

37 In some cases, this can already allow the user to access services that have agreements only with mobile operators other than his or her own mobile operator, as in Finland. See for example interoperability in Finland's mobile identity system: GSMA, Alix Murphy, 2012, Finnish Mobile ID: A Lesson in Interoperability, available at http://www.gsma.com/personaldata/wp-content/uploads/2013/03/GSMA_Mobile-Identity_Finnish_Case_Study.pdf

38 http://www.gsma.com/personaldata/mobile-connect

39 Competition problems could arise, for instance, if one already-dominant player played a central role in developing and operating an identity system in which its platform becomes the only practical or affordable way to access such mobile financial services or government services. This might also advantage its ability to collect transaction and behaviour data of customers that can be leveraged into related markets.



Box 2: Mobile Connect solution

The GSMA's Mobile Connect has a single global interface that supports authentication, authorisation, identity and attribute sharing or verification for service providers, while putting the user in control. By combining the inherent security of mobile devices, the SIM element, operator business processes and mobile network, Mobile Connect enhances user security and reduces the risk of identity theft while enabling access to a wide variety of use cases.

Mobile Connect is a digital identity solution that supports scale via a set of consistent set of technological, commercial and regulatory specifications that meet the rising regulatory trends in the digital identity ecosystem. The solution offers a seamless consumer experience that's safe and secure and doesn't share personal information without the affected user's permission. Since Mobile Connect was first introduced in Mobile World Congress 2014, 42 operators across 22 countries have implemented Mobile Connect, making it available to nearly 3 billion customers.

The flexibility of Mobile Connect allows the users and service providers to meet different and multiple security assurance levels, ranging from low-level website access and registration to highly-secure, authorisation and legally binding mobile signature services[40] typical of e-government and online financial services transactions.

Outspoken privacy focus

A core principle of Mobile Connect is to protect end-user privacy, through transparency of any information being shared and allowing for anonymous authentication. (See Box 2 on Mobile Connect Privacy Principles).

40 Mobile signatures are based on W-PKI (Wireless Public Key Infrastructure) technology which adds the requirement of non-repudiation of legal identity and the generation of digital certificates for identity validation.

Trend 3: Integrating identity-related policies

Mobile operators are already dealing extensively with identity in numerous ways, sometimes as part of a commercial offer and other times because regulation requires them to do so. Whether in order to provide mobile financial services, to comply with SIM registration requirements, or for other services requiring knowledge of the customer, mobile operators already often engage in forms of enrolment, credential management and authentication.

The general trend by governments towards establishing identity programmes, as well as specific moves to establish digital identity systems, may allow mobile operators a significant opportunity to leverage their assets and existing identity-related practices. However, the degree to which this cluster of identity-related activities can develop into a fuller role for mobile operators in digital identity depends on whether governments pursue 'joined up thinking' to integrate the security concerns that drive SIM registration, the financial inclusion objectives that drive mobile financial services KYC rules, and the overall development objectives of digital identity itself.

Mandatory SIM registration

In an increasing number of countries, registration of prepaid mobile SIM cards is mandatory, primarily serving security concerns. In such countries, mobile operators already go to some lengths to identify their customers when allocating or activating a secure SIM.[41] Where this is the case, mobile operators are required to check or, where possible verify customers' identification documents before offering telecommunications services.

In some countries, SIM registration is based on biometric verification linked to national identity systems, such as in Bangladesh, India, Indonesia, Pakistan, Peru, Saudi Arabia and the United Arab Emirates.[42] Where the national identity system is already digital, the verification of biometric attributes against the national registry can be subject to rigorous security controls over access to the national identity database.[43] The result is a high level of assurance as to the identity of the individual registered to the SIM.

This would allow the mobile registration to be used for identity-verification purposes, for example with the mobile operator using the mobile phone to assure identity for other service providers. This spinoff benefit from mandatory SIM registration could be more efficient than requiring the individual to go through the more cumbersome authentication process of the national identity system (e.g., full biometric verification) for every subsequent transaction.

Practices vary depending on the existing identity systems in place:

- SIM registration may be linked to a biometric national registry, as described above (e.g. Pakistan);
- SIM registration may involve the mobile operator verifying the person's identity against the national identity register without biometric verification (e.g. Ecuador and Rwanda);[44]
- The SIM registration may not be verified against a national ID at all, but may rather be recorded in a special database. In Nigeria, for example, the mobile operator must capture and transmit biometric data and personal information to the Central Database of the Nigerian Communications Commission, but it is not verified against a national database;[45] and
- Mobile operators might have to use one of a variety of authorised personal IDs as evidence of identity when registering a SIM.[46] For example, in Kenya, the mobile operator must register the new SIM upon verifying the original national identity card, an original passport, original service card of the Kenya Defence Forces, or original birth certificate.[47]

41 A fuller review of mandatory SIM registration may be found in GSMA, April 2016, Mandatory Registration of Prepaid SIM Cards, http://www.gsma.com/publicpolicy/mandatory-sim-registration

42 For instance, Pakistan's NADRA identity system requires the mobile operators to verify identity of customers by access to the NIDRA system, including checking biometric features. See http://id.nadra.gov.pk/ Similarly in Peru, SIM registration requires biometric matching against the national ID programmes. See http://www.biometricupdate.com/201506/peru-to-implement-biometric-identification-for-prepaid-phone-activation.

43 See e.g., MNO KYC using India's Aadhaar identification data at page 17.

44 See Mandatory Registration of Prepaid SIM Cards at footnote 42.

45 Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011, available at https://toluogunlesi.files.wordpress.com/2015/11/legal-regulations-registration_telecom_subscribers_2011.pdf.

46 See Mandatory Registration of Prepaid SIM Cards at footnote 42.

47 The Kenya Information and Communications (Registration of SIM Cards) Regulation 2015, available at http://www.ca.go.ke/images//downloads/sector_regulations/Registration per cent20of per cent20SIM per cent20 per centE2 per cent80 per cent93Cards per cent20Regulations, per cent202015.pdf.

The process of SIM registration could be a significant element in the creation of a new digital identity where none may exist as yet. Where the SIM registration requirements would not produce a robust mobile identity, mobile operators could combine additional verification processes at the enrolment stage to improve the robustness of their digital identity solutions.

The resources that mobile operators must devote to establishing and operating a SIM registration system are substantial, and leveraging these to deliver the additional benefit of a mobile-based digital identity would serve policy objectives and present commercial opportunities for offering other digital services of value to users.

Box 3. MNO KYC using India's Aadhaar identification data

In August 2016, India established procedures providing for mobile operators to access its major national digital identity programme, Aadhaar. The Ministry of Telecommunications issued an order[48] requiring mobile operators and their agents to obtain customers' digitally signed electronic KYC data and Aadhaar numbers from the UIDAI database, and store it on their databases for purposes of issuing mobile connections. The mobile operator staff or agents must sign into the UIDAI database through the Aadhaar authentication system, as does the customer, with the latter's demographic data (name, complete address, date of birth, gender, photograph) being made available to the former. The agent must record in the customer application form that he or she has seen and matched the customer with his or her online photograph received from UIDAI, and that the SIM card has been handed over to that customer. The finger print/iris of the customer and of the agent (used for the authentication) are not to be stored and displayed on the Point of Sale (POS) device terminal during the process. Rather, the mobile operator must store the demographic data directly in its database and be available for compliance audit purposes. The POS then accesses the mobile operator's server to verify the identity. Other data that is not UIDAI demographic data (e.g., name of spouse, and nationality) are provided by the customer directly to the agent.

48 File No 800-29/2010-VAS, dated 16 August 2016, on Use of 'Aadhaar' e-KYC service of Unique Identity Authority of India (UIDAI) for issuing mobile connections to subscribers.

Mobile money KYC

The existing practices and requirements for customer identification for mobile money services also present an opportunity for policymakers and mobile operators seeking to develop mobile identity services.

Mobile financial services (MFS) are available in over 93 countries, with over 271 different mobile money services available, and over 411 million registered accounts of which 134 million were active as at the end of 2015. The pace of growth in services and accounts is rapid. Although mobile operators are excluded from providing such services in a number of countries, those countries that have seen the greatest ignition and take-up of services have mobile financial services led by mobile operators.

Best practice requires providers of MFS to carry out some form of customer identification as well as to track and report suspicious activities. This is necessary both to ensure the commercial reliability of the financial services as well as to comply with financial regulators' rules on KYC, particularly for the purposes of anti-money laundering (AML) and counter financing of terrorism (CFT) policies.

So, for instance, the Bank of Uganda requires mobile operators and their agents to verify the identity of the customer using either a valid passport, driving permit, identity card, voter's card, financial card, local administration letter or business registration certificates. The Central Bank of Kenya requires a mobile payments services provider to independently verify the customer's identity card number or passport through the Integrated Population Registration System database or such other means as the Central Bank may approve.

The Financial Action Task Force (FATF) recommends a proportionate, risk-based approach to KYC , and indeed some countries operate a tiered approach to KYC for financial services. Low-tier KYC MFS are often associated with restrictions on the type and/or value of transactions that are possible (e.g. a cap on the amount that a customer can send or receive per month). In such cases where the amounts involved are typically quite small, mobile payment services are typically considered low in criminal and security risk. In countries that have developed successful mobile money services, this results in KYC requirements that do not generally exceed the SIM registration requirements, even if the provider is often accountable to different regulators (the telecom regulator for SIM registration and the financial regulator for mobile financial services KYC).

In some cases, such as in Kenya, the SIM card registration process is deemed sufficient for the purposes of mobile financial services. In Sri Lanka also, mobile payments providers rely on the SIM registration process, which involves capturing a digitised copy of the national ID in a one-time process.

Implications for mobile-based digital identity

From mobile KYC to mobile identity

The prospects for building mobile identity services from such KYC processes depend in part on the strength of the mobile operator's initial registration process. There remain vulnerabilities to fraudulent registrations arising through failure of the KYC process to verify the identification documents or other credentials presented. The use of agents and retailers for KYC processes increases this risk. Alternatively, documents presented might themselves be fake or fraudulently obtained in the first place, a risk that is harder to control without an effective verification system matching them to the central registry.

As in any identity system, there is always a trade-off to be considered between the utility of the system and the risks it presents. Indeed, this is the reason for assessing levels of assurance for identity systems. Such trade-offs may be viewed differently in countries where there is a lack of digital identity yet significant demand for it. Mobile operators may actually be able to provide a supporting function for governments in creating unique identities where none exist, as well as providing credentials and authentication services.

27 Companies such as Verizon, Experion, Barclays, the Post Office, the Royal Mail and others have become certified identity providers. See https://identityassurance.blog.gov.uk/tag/certified-companies/.

28 See https://www.nist.gov/itl/nstic.

29 See http://www.skconcierge.us/the-canadian-experience/.

30 See OECD (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. Available at http://dx.doi.org/10.1787/5kgdzvn5rfs2-en

31 Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

32 Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

33 Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

34 ITU-T Recommendation X.1254 | ISO/IEC DIS 29115 -- Information technology – Security techniques – Entity authentication assurance framework, available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138

To spur on such initiatives requires avoiding unnecessary barriers such as, for example, duplicative processes for SIM registration, mobile money registration and then also further registration for the purposes of establishing a digital identity. It is also important to ensure that all such steps are done transparently with the affected customer's knowledge and consent.

In both the cases of SIM registration and mobile financial services KYC, the registration requirements raise a 'flip side' concern, that they actually deny segments of the population access to the services due to lack of reliable identification. Here, the opportunity is for mobile operators and policymakers to develop acceptable substitute processes with lower levels of assurance to assist in establish a trusted identity, potentially as part of a broader national identity drive (see the Box on Tanzania below).

Box 4. From SIM registration to mobile identity in Tanzania[58]

The mobile operators in Tanzania are working together to establish a common process for electronically registering their mobile customers to comply with mandatory SIM registration rules. Currently, the level of assurance by which a mobile operator verifies its customer's identity generally depends on the type of identity document that the customer physically presents at the point of registration. In the short to medium term, it is envisaged that the 'e-KYC' process may foreseeably result in the creation of verified customer identity profiles with different levels of assurance. Higher levels of assurance would result from real-time verification of a national ID card issued by the National Identification Authority (NIDA), accompanied by a digital photograph, and could be used for a range of use-cases such as opening a bank account or accessing a health service. Lower levels of assurance would apply where the customer has no such ID card but can present a letter from the village leader or other accepted non-government documents, and might be used for small digital payment transfers or for accessing websites requiring log-in credentials. The GSMA Digital Identity programme is working with mobile operators and partners on identifying and outlining areas where mobile identity solutions could have commercial and social impact.

58 Source: GSMA.

The scope for mobile operators to leverage SIM registration and mobile financial services KYC processes to build digital identity services thus depends on the extent to which such processes are required, their robustness, and of course demand for mobile-based identity, whether as a new service or a complement to a national identity system.[59] It could be that countries that have allowed mobile operators to provide such services will also be among the early ones to allow digital identity services to grow.

If the cluster of mobile operators' identity-related activities and regulatory responsibilities does come together to allow mobile operators to become trusted providers of a variety of enrolment, credential management and authentication services, there are numerous ways[60] in which they might contribute. They can do so, for instance, through enabling birth registration certificates, as part of birth registration systems, as seen in Tanzania, Senegal and Uganda (see Box 4 on Tanzania above). This might extend into health and vehicle registration (see Box 5 on Nigeria below) and other areas besides mobile financial services.

Box 5. Introducing mobile ID through vehicle registration in Nigeria[61]

Nigeria is currently allowing smartphones to securely carry biometrically enabled mobile IDs based on identification from the Nigerian Police Biometric Central Motor Registry (BCMR) vehicle registration card programme. The BCMR, which plans to register all motor vehicles, gives real-time access to ownership, accident, crime and insurance information on vehicles and biometric and other identification data on their owners. The data is available in real time using users' credentials and police officers' smartphones, which can act as mobile readers.

With such official data available on smartphones, Nigerians will be able to prove ownership of vehicles rapidly and easily. The mobile ID data is installed on the SIM, so that it does not depend on having a network connection, and can be communicated by Bluetooth or NFC, so that the user is not required to physically hand over the phone. The process is integrating the mobile ID into Nigeria's current efforts to roll out IDs to the population at large and may over time spur migration to mobile IDs.

While this initiative is focused on the limited function of vehicle registration, and can be offered using the mobile phones but without the direct involvement of the mobile operator, it suggests there is demand for mobile ID solutions. Mobile operators could pursue this potential, for example through developing functional mobile IDs with government departments using a consistent approach that allows interoperability and reduces the current fragmentation in Nigeria's digital identity landscape.

59 In countries such as Bangladesh or Nigeria, where the mobile operators are not permitted to provide mobile money services, the opportunity and potential of mobile identity services may be more limited in the short term. In other countries, like Kenya, Tanzania, Uganda and Zimbabwe, the mobile operators are allowed to offer mobile money services, and have greater incentive to facilitate KYC processes and verify customers for the purpose of offering mobile money and other services either during or shortly after registration. See GSMA, Who can offer Mobile Money Services, available at http://www.gsma.com/mobilefordevelopment/programmes/mobile-money/policy-and-regulation/guide/who-can-offer-mobile-money-services.

60 Including, through the GSMA Mobile Connect solution (see Box 2)

61 HID Global Launches First Mobile ID Program in Nigeria with Partner Media Concepts. See https://www.hidglobal.com/press-releases/hid-global-launches-first-mobile-id-program-in-nigeria-partner-media-concepts (site visited on 1 September 2016).

Encouraging mobile operators' participation

The prospects for mobile identity services to grow and strengthen the digital economy, support digital and financial inclusion, and offer the benefits of convenience and reach to the population are greatly strengthened where government develops a national strategy. Where a strategy is already well underway for national digital identity, the challenge is to integrate mobile identity into the system. Where a national digital identity strategy is still in its early stages, governments may be encouraged to integrate mobile as a central component, creating the opportunity to leapfrog paper-based identity systems.

Where government policy evolves to embrace a role for mobile operators in digital identity, there are various forms that such role could take. Mobile operators might merely use national ID systems as a means of fulfilling mandatory SIM card registration systems, where permitted or obligated to do so. Mobile operators might act as service providers, providing attributes or authentication services to relying parties, i.e., service providers that do not seek to operate their own identity systems.[62] They might even offer 'identity as a service' to users who wish to hold an identity established independently of any particular service in order to access multiple services.[63]

Where governments seek to leverage mobile network capabilities to enhance national ID programmes, mobile operators might participate in public private partnerships (PPPs) for developing and offering unique national ID systems.[64] These could be used to access a variety of services including tax reporting and payments, social security payments, and healthcare services among others. For instance, Uganda's birth registration programme involved a PPP agreement between operator UTL, UNICEF and the Ugandan authorities.[65]

Under a PPP, the government benefits from the private sector involvement, which may be less expensive, more innovative and more efficient than the government could achieve itself. In turn, the mobile operator benefits from being able to offer a recognised form of ID that consumers would use to access value added services over mobile networks.

Data protection, privacy, and surveillance issues will directly impact the risk and reward of entering into a PPP with the government. Here, the mobile operator has a long-term role, which provides added incentive to help establish a 'trust framework' (discussed below in Trend 4). Use of PPPs will raise new issues for consideration. For instance, a mobile operator in a PPP may find itself bearing some financial and reputational risk if government access to data takes place outside of clearly defined and transparent frameworks. Governments may also struggle with mechanisms to ensure accountability for public systems operated by private operators, and face criticism where they encounter problems.[66]

The different functions in the identity ecosystem and the variety of possible business models give rise to different incentives for mobile operators' participation. Some elements involve costs (e.g., of regulatory compliance), some may generate direct revenue for the service from usage, and some may be expected to produce longer term benefits in terms of customer acquisition and retention, growth in data traffic, and centrality of the operator's place in the digital ecosystem. The outcome will depend, in part, on the establishment of a trust framework within which the mobile operator will provide identity services.

62 See the GSMA Mobile Connect digital authentication standard, at http://www.gsma.com/personaldata/mobile-connect

63 See Mobile Connect, Box 2, above

64 For a more detailed discussion of PPPs in mobile identity services, see Shared Principles, at footnote 8.

65 See footnote 9.

66 See for example IMANI Report: Don't Mess up the National ID System, 2016, available at http://www.imaniafrica.org/2016/02/08/imani-report-dont-mess-up-the-national-id-system/

Trend 4: The robustness of the 'trust framework'

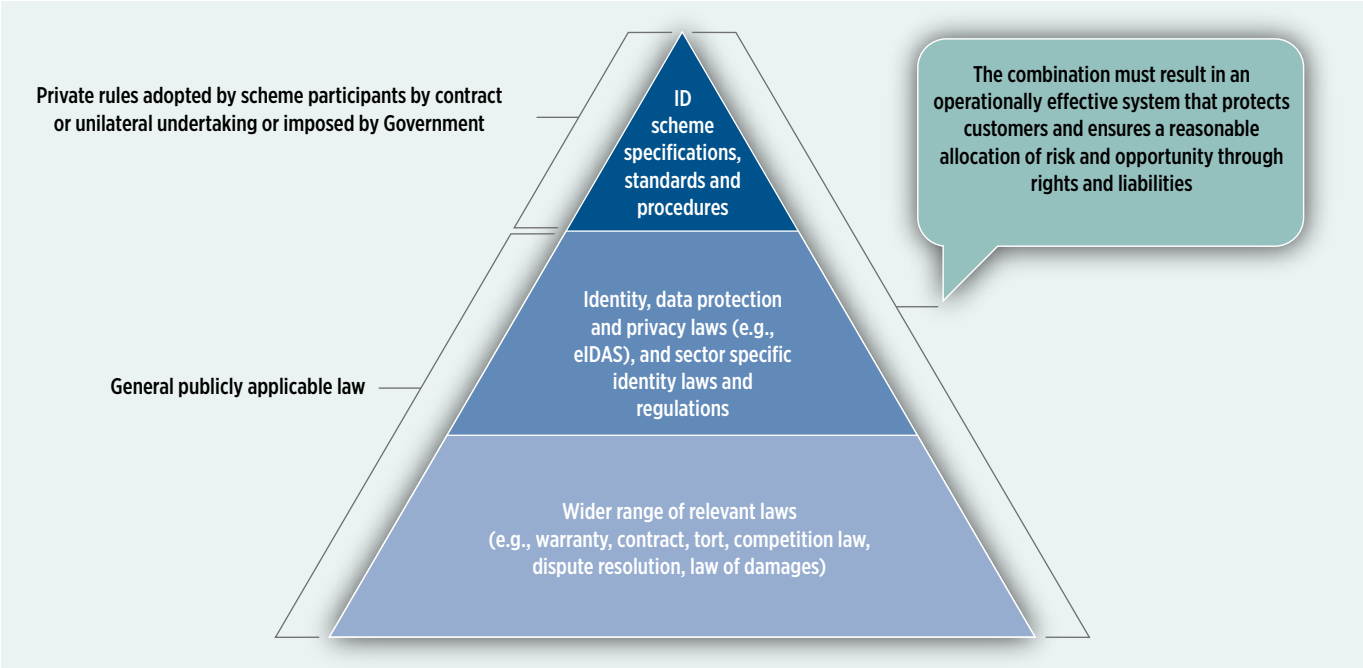
A digital identity system must be built on a foundation of trust if it is to generate widespread acceptance among users that unlocks revenues in value added services, while also helping governments achieve the related SDGs.

The roles that mobile operators might play in the identity realm raise important issues of regulatory policy relating to trust. Customers and service providers are relying on the effectiveness of the system, while the mobile operators and other participants in the system are often handling customers' personal data, including unique attributes and credentials.

As such, the parameters within which mobile operators participate, at any level in the identity system, greatly affect whether the system will take-off and achieve scale beyond mandatory government uses. In turn, this influences whether mobile operators will have an incentive to participate in building mobile-based digital identity systems.

A core aim of regulatory policy is to ensure that technical specifications, standards and procedures are legally binding. These define the legal rights and obligations of the participants in the identity system. This not only anchors the intended framework in law, but establishes incentives and clarity among participants as to what resources they will devote and where they will devote them to ensure the system functions as intended. The result is a system partly developed by standards bodies, partly by participants in a given identity system, and ultimately enforceable by regulators and courts.

FIGURE 2. THE RULES COMPRISING A TYPICAL TRUST FRAMEWORK FOR IDENTITY SYSTEMS



The combination of these elements is often referred to as a 'trust framework'. As illustrated in Figure 2 and discussed below, there are several dimensions to this:

- The technical specifications, standards and procedures must produce an operationally effective system;
- Appropriate data protection and respect for consumers' privacy are essential for the transactional purposes for which the data is used and to ensure customer trust; and
- The rights and liabilities under general supporting laws (e.g., contract, warranty and tort) must be clear and effective.

Overall, the combination of the above must result in reasonable allocations of risk and opportunity through rights and liabilities.

Technical specifications, standards and procedures

At the core of any digital identity system is the suite of rules that make sure it actually works as intended, resulting in identity that has the desired level of assurance and interoperability, while generating trust among the participants. These specifications, standards and procedures apply in the phases of:

- Enrolment, where users apply for and are initiated into the identity system, data is captured and verified to identify them ('identity proofing'), and a record of enrolment is established;
- Creation, issuance, activation and storage (as well as suspension and revocation) of credentials (e.g., PINs and passwords); and
- Assertion by users of credentials to service providers (or 'relying parties') in the authentication process.

Governments and mobile operators seeking to establish digital identity systems need to ensure that the design is effective operationally.

The design of the system will depend on the level of assurance sought. Identification methods need to be designed to be proportionate to the security needs of the relevant situation. Higher levels of authentication security are needed to access government (and financial and health) services than to access most email accounts for instance. This means that multi-factor authentication options are needed depending on the level of security required. Where strong authentication is needed, for instance to authorise a legally binding transaction, mobile signatures relying on PKI may be appropriate, which also enable production of digital certificates that validate identity.

Higher levels of assurance depend on information security and risk management practices, policies that must be documented, and of course integrated into information technology hardware and software. For mobile operators to manage the cost and complexity of the system, the level of assurance sought needs to be proportionate to the use to which the identity will be put and the associated risks.

Adopting technological neutrality in the specifications will allow mobile operators to use a variety of means for providing digital identity services. This may lead to innovation in use of the secure element, embedded smart cards and other channels, and at the connectivity level, for using the internet, SMS, USSD, NFC, WiFi or other technologies. The framework would provide for the key objectives and security requirements, and allow the providers to use the approach of their choice provided that they can demonstrate that it meets the objectives and requirements.

Standardisation is a central element of the design of digital identity systems. Where consistent standards can be established, efficient, large scale deployment becomes possible. For example, India's UID programme resulted from a strongly standards-based procurement model that ensures competition among suppliers, and monitors them carefully in real-time. This avoids being locked into a particular technology or hardware, thereby increasing choice and keeping costs under control. Some have suggested that such an integrated identity system with a competitive procurement mechanism could be provided on an aggregated basis to multiple countries, perhaps being launched with support from donors.[67] Mobile operators could act as platforms for these, particularly where their operations have a wide footprint.

67 See Performance Lessons from India's Universal Identification Program at footnote 6.

Data protection and privacy

Effective law and regulation

Mobile-enabled digital identity, as with any identity system, involves personal information about users. The collection, storage and sharing of personal attributes collected in identity registration processes, or used in identity authentication processes, represent the kind of information that data protection and privacy policies, laws and a host of regulatory agencies are concerned to protect – and which citizens expect will be protected.

Where such policies, laws and regulatory agencies are not well developed, they need to be established as a matter of priority if digital identity is to flourish. In countries where these are already established, the priority is to ensure accountability, impartial adjudication and ability to adjust to changing conditions.

A primary concern in designing and operating any identity system is to protect data from being obtained by third parties for purposes other than operating the identity system itself. This means, for instance, that where an identity assurance provider delivers information to a relying party, it should not provide all of the data it may hold on an individual, but only the minimum necessary to complete authentication; If only one specific attribute is required by the relying party then the identity assurance provider only needs to share or confirm that specific attribute. For example, an identity provider that is requested to confirm that the user is above a certain age may not have to supply age or even date of birth details, only confirmation that he or she is indeed above the specified age. This results in less data being transmitted and stored, protecting privacy and thereby trust in the system.

Some identity systems incorporate security arrangements specifically targeted at protecting privacy, such as India's UIDAI clearance levels for accessing the UID database[68] and Pakistan's NADRA's use of software allowing citizens to see who has accessed their data.[69] The Indian order of August 2016 (see Box 3 on page 17) illustrates the importance to security of the physical location of identification data. There, demographic identification data must be stored on the mobile operator's server, while storing it on the agent's point of sale (POS) device is prohibited. Similarly, where mobile devices are used, identification data is most safely stored on a secure element, whether on the SIM card or a microSD card embedded in the mobile device.[70]

Data protection laws typically address more than the collection, storage and transfer of data for the purpose of identity systems, and cover the broad use of personal data. Data protection and privacy laws typically define 'personal data' (and similar terms) as information relating to a person who is identified by or identifiable from such information. This may include a vast range of attributes and behaviours that a person has or the digital trail he or she leaves behind in electronic interactions.

Precisely because such data are used in identity systems to register users, and may be used to authenticate them, unprotected storage and sharing of such data creates risk of identity theft, fraud and numerous economic and even national security risks. Such data may also be used for unwanted commercial approaches and spam, for discriminatory purposes on the basis of race, religion or gender, or for other problematic or unlawful purposes. Personal identity data also needs to be protected from accidental destruction, loss, alteration, and unauthorised disclosure or access.

Fit-for-purpose data protection laws will thus typically impose responsibilities on data controllers or data users – government departments, businesses and other organisations that hold and use such data – regarding how they store and share it. This may extend to a wide variety of organisations, from banks, insurance, telecom operators, health care providers, utilities, airlines, law firms, accountancy firms and others, some of whom may be required to register with and report to the data protection authorities.

In effective trust frameworks, data controllers must obtain consumers' consent before collecting and disclosing personal data, and maintain secure systems to protect the data. They are also often required to disclose to consumers the kinds of uses they may make of data that they collect, including whether (and if so for what purpose) it may be shared with third parties. They may also be required to notify the data protection authorities and/or users of relevant data breaches.

68 See Box 3 on page on 18, MNO KYC using India's Aadhaar identification data.

69 See footnote 11.

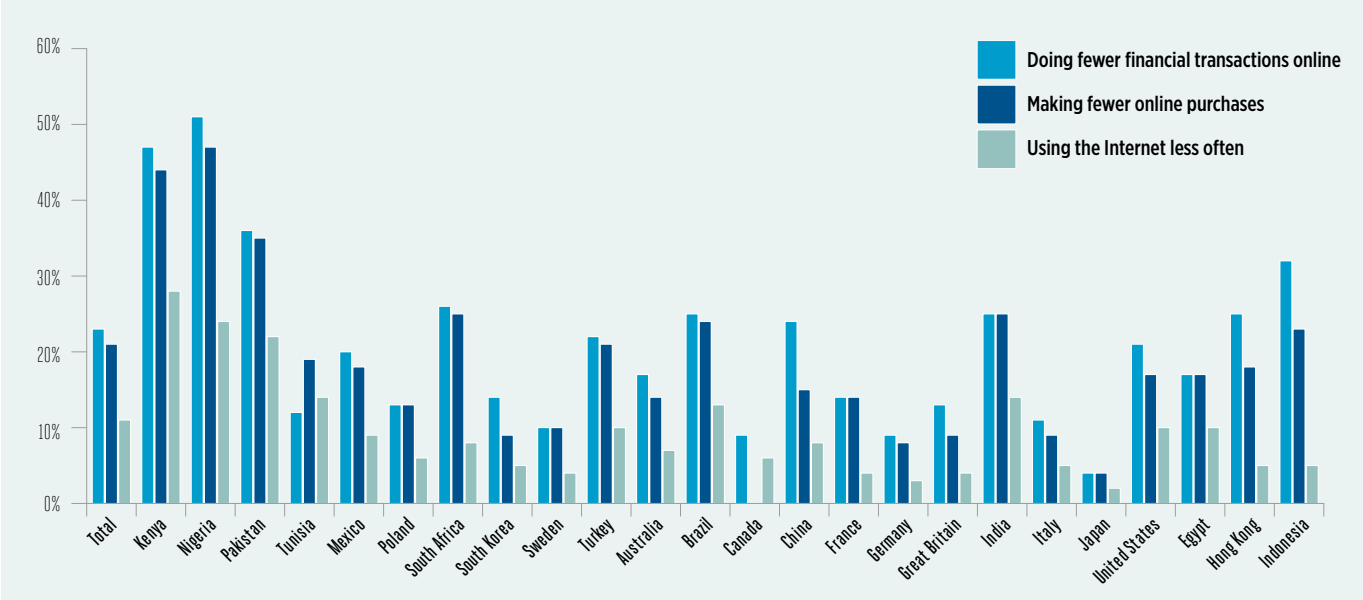
70 See The Open Identity Exchange, Exploring the Role of Mobile in Digital Identity Assurance (2014)

Globally, a large and growing number of countries have adopted data protection legislation. In recognition of the need to generate trust, according to the United Nations Conference on Trade and Development (UNCTAD), 108 of their member countries have complete or partial data protection laws, while the other 30 per cent do not.[71] In countries that have established such laws, that is the beginning of the process, not the end, as data protection authorities are needed to monitor compliance and for enforcement.

Further, there are challenges in those countries without a data protection law. A survey in the UNCTAD report indicated significant challenges in enacting and then enforcing such laws, based on costs, and a lack of skill across government, including parliament, policymakers, and law enforcement agencies.[72]

The resulting lack of trust can impact user online behaviour. For instance, in a recent global survey, in Nigeria, which has a significant history of online fraud, 69 per cent of consumers expressed that they are 'much more concerned' about their online security than they were just a year ago.[73] This affected their online behaviour, with 51 per cent less likely to do financial transactions online, and 47 per cent making fewer online purchases, as seen below. Other countries had similar results, including notably Kenya, Pakistan, India, and Indonesia, and the results were far higher than the developed countries surveyed.

FIGURE 3. IMPACT OF ONLINE PRIVACY CONCERNS ON BEHAVIOUR



Source CIGI-Ipsos Survey, 2016

71 See UNCTAD Data protection regulations and international trade flows: Implications for trade and development, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468, at page 8.

72 Id. at Figures 1 and 2.

73 See Centre for International Governance Innovation (CIGI) survey with Ipsos, at https://www.cigionline.org/internet-survey-2016

This creates both challenges and opportunities for mobile operators. Many e-commerce providers, such as Jumia (sometimes referred to as the Amazon of Africa), have had to resort to cash on delivery because of the unwillingness of Nigerians to make online payments due to worries about fraud, which of course leads to its own difficulties with regards to deliveries, robberies, and a high return rate.[74] On the other hand, this creates an opportunity for a trusted provider, such as a mobile operator, to mediate or provide online payments, based on an established identity.

There is no legal framework for data protection fully in place in Nigeria. While Nigeria is part of the Economic Community of West African States (ECOWAS), which passed a binding regional agreement that specifies a data privacy law and requires a data protection authority, Nigeria has not implemented these provisions. In this environment, even a code of conduct or other trust measures would have difficulty gaining traction.

On the other hand, Uganda, which also does not yet have a data protection law, has a law on electronic transactions, and the government has been raising awareness through workshops for all stakeholders, private and public, to help create safe online transactions, with plans to do the same when a data protection law is passed.[75]

Absent effective laws, there is scope for industry to step in to create its own code of conduct or privacy framework to build up trust. For example, incorporating privacy by design into mobile operators' processing of data on customers may be done by convention among industry participants. Similarly, the GSMA has done valuable work in developing principles that mobile operators may adopt globally to protect data.[76] These can contribute to the development of such legal rules in a manner that supports rather than stifles the development of mobile identity services.

Of course, it is not enough merely to have data protection and privacy laws – they must be well balanced. Cumbersome licensing requirements, heavy reporting obligations in case of breach and excessive penalties for violations may undermine incentives to invest, leaving no data market to protect. Some countries' laws ban the use of encryption, at least without the consent of the government, which can be burdensome to obtain, particularly if it must be obtained from more than one official body.[77] Without encryption, identity information may be subject to breach in transit or at rest (in storage), submitting providers to financial and reputational risks, and their users to privacy violations and potential identity theft. Regulatory policymakers and mobile operators thus need to assess carefully the costs and benefits of the impact of data protection and privacy legislation.

There may be merit in national regulation that generally emphasises high level principles consistent with international standards (e.g., 'privacy by design') rather than over-regulating at the local level. International principles (such as the GSMA Mobile Connect Privacy Principles)[78] and guidelines[79] may be adopted and adapted to the digital identity context by mobile operators to build trust, and act as a reference point for compliance. Likewise, national regulation might establish clear public policy objectives in relation to protection of consumer data, but leave market participants reasonable flexibility as to how they will meet these, including storing or processing data in other countries so long as the parties involved are doing so with at least a comparable trust framework (as discussed below).

74 For a description of the cost of cash on delivery by one e-commerce provider in Nigeria, who decided to stop offering it as an option, read https://techpoint.ng/2015/07/13/cash-on-delivery-free-delivery-are-2-worst-things-to-happen-to-ecommerce-in-nigeria-drinks-ng-founder-lanre-akinlagun/.

75 See UNCTAD Information Economy Report 2015: Unlocking the Potential of E-Commerce for Developing Countries, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1146, at Box V.6.

76 E.g., see GSMA, 2012, Privacy Design Guidelines for Mobile Application Development and GSMA, 2016, Mobile Privacy Principles, available at http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA-Privacy-Principles.pdf.

77 For instance, Article 64 of Egypt's Telecommunication Regulation Law No. 10 of 2003 prohibits use of encryption equipment unless with written consent from each of the NTRA, the Armed Forces and National Security Entities.

78 https://developer.mobileconnect.io/privacy-principles

79 See Shared Principles, at footnote 8, and GSMA, Privacy Design Guidelines for Mobile Application Development, available at http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf

Additional data protection and privacy considerations

Mobile operators' collection, storage and sharing of the personal data of their customers may be subject to regulation even in the absence of omnibus data protection laws. Such restrictions appear in telecommunications and information technology laws and regulations, and in the mobile operators' licences. Typically, mobile operators are subject to duties to protect their customers' privacy regarding certain personal information, and to maintain confidentiality of and refrain from disclosing certain confidential, personal and proprietary information of any customer.

As an example, while mobile operators have significant advantages in offering identity services based on their relationship with the customer, and the features of handsets, it can be difficult to get the right balance in authentication between security and ease of use. One emerging solution, based on big data, allows for continuous authentication based on the behaviour of the user, such as how they interact with their handset, their location, and other behaviours.[80] Without deviations, the user can proceed with no active authentication required, but, of course, this requires access to personal data that may not be allowed for the mobile operators in a country. For instance, a requirement to 'opt-in' for location-based data may hinder the ability to authenticate some customers based on their location, unless the mobile ID service terms specifically override that requirement, with mobile users' permission.

Box 6. Mobile Connect Privacy Principles[81]

Mobile identity services play a key role in helping individuals establish and assert their identities online. Key to realising the potential economic and social benefits of mobile identity is establishing good privacy practices that foster trust and confidence among individuals.

The GSMA in partnership with leading mobile operators have designed a set of Privacy Principles that are intended to guide the use of personal information in the provision of Mobile Connect identity services by Mobile Operators to 3rd Party Service Providers. The objective is to ensure that personal information, such as a phone number (MSISDN), is never shared with the service provider without the user's consent. Instead, a service provider-specific pseudonymous customer reference (PCR token) is shared. This token denotes a successful authentication and enables the service provider to serve a specific user. This approach means that the service provider is not necessarily able to identify the user and also cannot track a user across different services.

80 See https://techcrunch.com/2016/05/01/strengthening-authentication-through-big-data/

81 https://developer.mobileconnect.io/privacy-principles

Level playing field and consistency issues

Other aspects of data regulations can impact the usability of value-added services built on digital identity. At the domestic level, different regulations may apply to licensed telecom operators, including mobile operators, compared with other providers. There are two dimensions to this problem.

First, in some cases, mobile operators face one level of regulation on their use of customer data that do not apply to unlicensed providers of similar services, notably over-the-top providers. This could be true, for instance, in relation to the use of location data, which may be regulated for the mobile operator, but not for other providers that use location data, including the handset vendor, operating system provider, or the map app developer (which all could be the same company). This is one issue in the debate over regulation of online providers in South Africa and Pakistan, for example.[82]

Second, sector specific privacy regulations across the economy may vary, such as for health care, financial, or other, each of which may impose their own regulations and reduce the ability of an MNO to provide digital identity services, at least on a commercially viable basis, because of the increased costs of serving each sector. The US is an example of sector-specific regulations, in contrast to the EU which is more comprehensive.[83]

Cross-border restrictions

Some countries place cross-border restrictions on data delivery, storage, and processing. Selective restrictions can be part of their data protection and privacy regime ostensibly to protect their citizens from having their data moved without consent to a jurisdiction having weaker protections. Those placing such restrictions believe they can strengthen the trust framework. However, more blanket bans can also be tied to economic goals of promoting or protecting the domestic data processing industry.

As a result, requirements in one jurisdiction may not apply in another where similar activities are being carried out and where interoperability and cross-border services would be economically efficient and promote consumer welfare. Or there may be direct conflicts between requirements in two different jurisdictions. These may require duplication of systems that could otherwise serve multiple countries, thereby unnecessarily increasing cost and fragmenting data, identities and credentials.

Increasing importance of cross-border services

There are demand and supply side considerations relating to regulation of cross-border data flows which may impact mobile operators' ability to provide digital identity services.

On the demand side, populations are more internationally mobile than ever before. There is extensive trade in goods and services across borders. Whether ordering goods or engaging with a foreign service provider, the ability to carry out business across borders is increasingly important in a globalised economy. The ability to make mobile payments abroad or to borrow from abroad are obvious examples.

Similarly, international migration is today at historically very high levels. Refugees may lack a national identity from their countries of origination, or need identity in the host country in order to obtain a right of movement or work permit. The ability of refugees and migrants to establish and use identities plays a significant role in helping them access services that enable them to re-build and enhance their lives.

82 See http://www.fin24.com/Tech/Mobile/10-advantages-that-otts-have-over-networks-20160126 and the Pakistan Telecommunications Authority Consultation Paper for VoIP and OTT Services, 7 June 2016.

83 In the US, for instance, HIPAA requirements apply only to health data, see https://www.hhs.gov/hipaa/for-professionals/privacy/. In contrast, European data protection rules are broader. See http://ec.europa.eu/justice/data-protection/.

Box 7. UNHCR employing mobile to authenticate refugee identity cards [84]

In 2015, the United Nations High Commission for Refugees (UNHCR) introduced its Biometric Identity Management System (BIMS), collecting fingerprints and photographs, in its refugee identity card system, following a pilot programme in Malawi and further rollout in Thailand and South Sudan. In 2016, it introduced a mobile app (UNHCR VERIFY-MY) in Malaysia along with the identity card which enables authorities to verify authenticity of the cards by scanning the SQR code on the back of the card.

While identity is recognised as an important element in economic development and social inclusion, providing people access to services, some identity-related processes can also become a barrier to opportunity. For instance, where SIM registration is required, refugees lacking identification may not be able to obtain a mobile phone or internet connectivity where a specified form of identity is required. In some cases, UNHCR may promote looser identification requirements for SIM registration in order to enable refugees to get connectivity.

On the **supply** side, to be able to aggregate data across borders would not only allow firms to access resources abroad, but also to increase the efficiency of and innovation in service delivery. Many mobile operators have a group footprint across several countries. These, such as Orange, Vodafone, Digicel, MTN, Airtel, Etisalat, Milicom and VimpelCom, increasingly seek to capitalise on their global brands and solutions using standardised interfaces and processes, leveraging them locally.

This allows international groups to benefit from global economies of scale and scope in several areas. In the context of digital identity, they might do so by consolidating customer insights and identity procedures from, and providing a suite of identity services across several countries, such as mobile money, cloud and media services.[85]

Aggregating data for such insights, may not be possible in countries with data localisation laws that prevent cross-border transfers of data or make tailoring global solutions to local requirements excessively costly and bureaucratic. For instance, the data localisation rule in Indonesia, requiring data to be stored locally, can significantly change a business plan, by either requiring duplicate storage in Indonesia, or for all data to be processed in Indonesia for the mobile operator.[86]

84 UNHCR Launches Mobile App Alongside Biometric ID Card, 21 June 2016, at http://mobileidworld.com/unhcr-biometric-id-106217/

85 For example, the BCEAO's (Banque Centrale des Etats de l'Afrique de l'Ouest) regional approach to regulating mobile money services in the West African Economic and Monetary Union (WAEMU), comprising 8 countries (Bénin, Burkina, Côte d'Ivoire, Guinée-Bissau, Mali, Niger, Sénégal and Togo), is enabling consolidation of services. Orange, for instance, recently announced an internal group, Centre d'Expertise en Conformité Orange Money (CECOM), in Abidjan to provide compliance and risk management for its mobile money business across the region. Orange believes this will give it "more autonomy and agility, enabling it to offer customers increasingly innovative services in a shorter amount of time." See http://www.orange.com/en/Press-and-medias/press-releases-2016/Orange-accelerates-mobile-financial-services-in-Africa-and-sets-up-the-Orange-Money-Compliance-Expertise-Centre-CECOM-a-mutualized-compliance-centre-in-Abidjan-devoted-to-Orange-Money.

86 See http://cfds.fisipol.ugm.ac.id/article/23/the-potential-drawbacks-of-forced-data-localisation-in-indonesia.

Thus while some believe cross-border restrictions on data transfers can be an important element of the identity trust framework, they can also hinder mobile operators' ability to supply them innovatively and cost-effectively for the benefit of customers, governments and third parties that might rely on such identity solutions.

Box 8. Mobile operators' proof of concept for cross-border government services.

Government-led digital service platforms are key enablers for mobile identity deployments. Mobile operators are increasingly cooperating with governments at both national and international levels to integrate digital identity solutions into national and cross border digital identity strategies. For example, in November 2015, a technical pilot for Mobile Connect enabled operators to establish the first Proof-of-Concept (PoC) for cross-border authentication to e-Government services across Europe. The pilot (between Catalonia in Spain and Finland) demonstrates how mobile operators' key assets and Mobile Connect can be used to identify an EU-citizen of one Member State in order to gain access to a public service in another Member State. The pilot was the result of a collaboration between the public and private sectors seeking to accelerate the uptake of trusted and secure digital authentication services over the mobile platform in response to the eIDAS Regulation, which sets the rules for mutual recognition among EU member states of digital identities, authentication and trust services.

82 See http://www.fin24.com/Tech/Mobile/10-advantages-that-otts-have-over-networks-20160126 and the Pakistan Telecommunications Authority Consultation Paper for VoIP and OTT Services, 7 June 2016.

83 In the US, for instance, HIPAA requirements apply only to health data, see https://www.hhs.gov/hipaa/for-professionals/privacy/. In contrast, European data protection rules are broader. See http://ec.europa.eu/justice/data-protection/.

Innovation- and efficiency-oriented cross-border regulation

These factors suggest that there is merit in greater recognition in local laws of global solutions that apply technical specifications, standards and procedures that are internationally recognised and of high quality. Harmonising and coordinating legislation internationally may also be helpful. The United Nations Commission on International Trade Law (UNCITRAL) has been reviewing such issues, including potentially developing model legislation.[87]

Box 9. Restrictions on cross-border transfer of data in Malaysia[88]

Malaysia prohibits data users from transferring personal data to jurisdictions outside of Malaysia unless to jurisdictions specified by the Minister except with the consent of the person concerned, the transfer is necessary for the performance of a contract between the data subject and the data user, the data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data is protected to a similar standard as under the Malaysian law, or the transfer is necessary to protect the person's vital interests.

A multinational mobile operator in Malaysia seeking to use a data centre in another country to aggregate data and lower storage costs and garner insights across its markets will need to structure its systems to comply with such requirements, including setting up mechanisms to obtain customers' consent and to maintain alternatives where such consent is not obtained. Such requirements create barriers and disincentives for the use of services (such as cloud-based services) that can be societally and economically beneficial.

87 UNCITRAL, Forty-eighth session, Vienna, 29 June-16 July 2015, Possible future work in the area of electronic commerce — legal issues related to identity management and trust services.

88 Malaysia's Personal Data Protection Act 2010 ('PDPA'), which came into force on 15 November 2013.

Naturally, operators providing identity services within a country that depend on registration, credential management or authentication occurring through an offshore data centre that serves several countries must be accountable for the protection of the data. However, the key is not to erect a barrier that hinders offshore service provision, but rather to find mechanisms that hold the global provider accountable locally. In the case of mobile operators, this is not necessarily difficult, as group operators will invariably have a locally licensed network operator, and so a physical and legal presence that can be part of the compliance system.

Mutual recognition mechanisms can play an important role in building cross-border mobile identity usage. The eIDAS Regulation provides such a framework for the European Union. Where there is clearly demand for cross-border mobile services that depend on identity, such as mobile financial services , regional economic bodies may have a valuable role. In Africa for instance, bodies such as ECOWAS, SADC, EAC and COMESA may facilitate both regulation applicable on a region-wide basis and encourage harmonisation measures through national models for adoption by their member states.

Growth in cross-border services would also be accelerated by use of commonly recognised identities. For instance, use of cross-border mobile money services could be expected to increase, strengthening the potential for international mobile money aggregators.

Other identity-related legislation

Where mobile-based digital identity services are intended for functional as opposed to foundational purposes, e.g., to access education, health or financial services, regulatory policymakers and mobile operators will need to review the sufficiency of the laws and regulations governing such systems. Other general-purpose legislation may also be important. For example, legislation may be useful or necessary to establish that an electronic signature made with an authorised strong identification method could be treated as a legally effective signature. In countries where strong identification systems exist (e.g., in online banking), legislation might also allow for mobile ID to be issued based on such existing credentials.

The surrounding legal and regulatory regime

In addition to specific rules pertaining to technical specifications, standards and procedures, and laws on data protection and privacy, other generally applicable laws and regulations may increase or weaken legal certainty, or bolster or undermine the commercial viability of mobile-based digital identity services. Any legal system not only allocates rights and responsibilities, but it also performs a sort of cost-allocation for failures. Different approaches to responsibility and liability may apply depending on the source of legal rules. For instance, where a user asserts an identity and as a result of an error or inaccuracy the service provider suffers a loss (e.g., disbursing money to someone who was not supposed to receive it), then whether or not the identity assurance provider is liable may depend on whether it is treated as:

- A tort (fault according the applicable standard of negligence) and the kind of loss incurred (e.g., some jurisdictions do not award damages for 'pure economic loss');
- A breach of warranty in a contract or given unilaterally, in which case the fault may not be relevant, only the terms of the warranty given; or
- A breach of a statutory duty established by legislation applicable to all identity services or the specific identity services in the given sector, which may supersede tort, contract and other laws.

Each of these may apply in different circumstances with different legal consequences, and there is no one optimal approach. For regulatory policymakers designing, and mobile operators evaluating the trust framework for mobile-based digital identity services, the source of legal rights and duties must be understood, and possibly realigned to ensure that the trust framework as a whole is robust.

82 See http://www.fin24.com/Tech/Mobile/10-advantages-that-otts-have-over-networks-20160126 and the Pakistan Telecommunications Authority Consultation Paper for VoIP and OTT Services, 7 June 2016.

83 In the US, for instance, HIPAA requirements apply only to health data, see https://www.hhs.gov/hipaa/for-professionals/privacy/. In contrast, European data protection rules are broader. See http://ec.europa.eu/justice/data-protection/.

Box 10. Virginia's Electronic Identity Management Act[91]

The Commonwealth of Virginia's Electronic Identity Management Act makes an identity trust framework operator or identity provider liable for issuing an identity credential or assigning an identity attribute that does not comply with Virginia's identity management standards, as well as for noncompliance with contracts and any rules and policies of the identity trust framework of which it is a member. Conversely, it excludes liability if the trust framework operator or identity provider is in compliance (except for cases of gross negligence or wilful misconduct). Such legislative provisions usefully set clear guidance for an identity services provider such as a mobile operator by tying legal responsibility to the state's identity management standards. The success of such law depends on good design of the state's underlying identity management standards to which they attach liability.

The trust framework as a whole

The three layers of the trust framework described in the preceding sections must be knit together to produce an operationally effective and commercially viable context for mobile-based digital identity systems to develop. How the three layers interact with one another may vary, for example with some regulations prescribing detailed requirements, and others leaving market participants to adopt standards.

91 Chapter 50 of Title 59.1 of the Code of Virginia, enacted 23 March 2015.

For example, levels of identity assurance and the associated specifications and procedures vary in different jurisdictions or digital identity systems; They may be prescribed by law, adopted by industry convention, or a combination of these (e.g., where law refers to industry standards).[92]

Whatever the structure, the overall result of the trust framework must be considered by policymakers and mobile operators in any given jurisdiction with a view to ensuring:

- The right level of prescriptive regulation;
- Fair allocation of risk and responsibility;
- Minimal uncertainty; and
- Mechanisms to resolve problems and disputes as they arise.

Level of prescriptive regulation

The delicate balancing act of governments with respect to digital identity systems, as in most regulatory matters, is to determine the appropriate level of generality and specificity in intervention. Trust frameworks need to combine the technical design with the appropriate level of legally binding norms, recognising that technology, standards, usage and business models will change. To prescribe excessive levels of detail in the regulatory level risks:

- Imposing a one-size-fits-all approach that fails to meet the needs of specific situations;
- Setting the rules for each sector so inflexibly that it produces isolated silos, where the opportunity to leverage economies of scale and scope are lost; and
- Making it difficult to adapt to changing technology, standards or market conditions.

Sometimes a plain absence of law leaves it for contractual negotiations to define and allocate risk. Yet parties will often avoid negotiating thorny risk allocation issues for future contingencies when setting up a new collaboration as doing so jeopardises negotiations. Parties often do better negotiating risk allocation by adjusting rules that apply by default, rather than in a legal vacuum. A lack of legislation and regulation, or outdated or inconsistent legislation, can create significant uncertainties and have a debilitating impact on the development of identity systems.

There is thus sometimes merit in setting positions in statutes that allow for contracting parties to opt-in or opt-out of a referenced position, so that they can negotiate alternative procedures and risk allocations contractually according to the situation at hand. Where statutory rights cannot be waived contractually, it may be necessary to change the law, but this is likely to be a laborious and time-consuming process. Party autonomy that allows contractual adjustment of a default statutory position may be less appropriate in certain cases, for example where consumer protection issues are involved or where one party has significant market share or bargaining power.

Fairly allocating risk and responsibility

Parties involved in identity systems take on legal responsibilities under the legal rules discussed above. An identity system may suffer from technical failure, where the technologies do not achieve the desired result, or do not interoperate as needed. Parties also face process risks, especially where processes are complex and require coordination among several parties. The success of a system is dependent on performance of each of the parties. Failure to implement and apply the system as intended – whether at the enrolment, certification or authentication phase – may result in its failure as a whole.

Such failures may result in losses to relying parties and users, including substantial financial loss. Such loss may result from third party behaviour, such as impersonation and identity theft and hacking. How risk of, and responsibility for, such failures is allocated among participants is crucial to the identity ecosystem's prospects. Without a legal basis that allocates responsibility for another party's loss, each person will bear the losses it incurs.

92 For instance, the Entity Authentication Assurance Framework (EAAF) established under standard ISO 29115, provides for four levels of assurance (1 – 4), while the European eIDAS Regulation defines three (low, substantial and high). ITU-T Recommendation X.1254 | International Standard ISO/IEC DIS 29115 Information technology – Security techniques – Entity authentication assurance framework. The UK's classification, which is close to the European eIDAS model, is as follows:

- Level 1: there is no requirement for the identity of the individual to be proven. The individual provides an identifier that can be used to confirm their identity in the future. The identifier has been checked to ensure belongs to the individual.
- Level 2: a claimed identity, requiring evidence that supports the real world existence of the corresponding individual. The steps taken to determine that the identity relates to a real person and that the individual is the owner of that identity give sufficient confidence for it to be offered in support of, for example, civil proceedings.
- Level 3: also a claimed identity, requiring evidence that supports the real world existence of the individual to which the identity refers, and physically identifies the person to whom the identity belongs. The steps taken to determine that the identity relates to a real person and that the individual is owner of that identity give sufficient confidence for it to be offered in support of, for example, criminal proceedings.

It is important that the regulatory regime attributes responsibility in a manner that recognises the reliance that each party places on the other, on warranties and undertakings each party has given, a party's ability to control the process for which it is responsible, and the foreseeability of the harm for which there may be liability. Where the recuperation of losses between parties is likely inadequate to ensure the necessary level of performance, or where some parties (particularly consumers) are unlikely to be able to pursue claims for such losses, penalties may be a useful means of incentivising compliance. However, excessive 'strict liability' that imposes disproportionately high penalties on parties in an identity system regardless of whether, or the degree to which, they were at fault may undermine incentives to participate and thus impede the development of identity systems.

Minimising uncertainty and inconsistency

In a technology-centric, fast-developing market, some legal uncertainties are inevitable. Existing laws and regulations become outdated as technology poses new threats and offers new solutions, and participants devise new specifications, standards and procedures. Laws and regulations in some sectors (e.g., finance) may be inconsistent with those in others (e.g., health). Vague terms in mobile operator licences such as 'customer information', obligations of 'confidentiality' and exceptions to prohibitions if for 'purposes of telecommunications' often leave great uncertainty as to their scope. Enabling mobile operators to play a role in a national ID system depends on providing clarity over existing laws, regulations and licence provisions related to use of identification data. It is particularly important to avoid threats to the good standing of licences – the legal foundation of an operator's business – from uncertainties about the new identity order.

Grievance and dispute resolution processes

Policymakers and mobile operators seeking to develop digital identity services need to ensure that grievance and dispute resolution processes exist to deal with problems that will inevitably arise in two dimensions of digital identity systems. First, within the system itself, participants may from time to time have claims against one another for performance failures or other breaches of legal duties. Secondly, users need a means to address problems such as false rejection from the registration system, wrongful attribution of identity, identity theft and identity data loss, all of which may result in losses from services for which the user intended to use the identity.

Government leadership

The technical specifications, standards and procedures that comprise an identity system and ensure it will function need to be more than operational policies voluntarily applied by participants in a given identity system. The transaction costs of collective action in face of complexity, combined with the importance of identity systems to fraud prevention, digitisation of the economy and other public interests, suggests an important role for government.

Governments may lead by bringing together adequate consensus on what specifications, standards and procedures to adopt, and then by lending the weight of law to these. They may do so by setting them out in binding regulations and rules or by imposing rights, obligations and liability for noncompliance with specifications, standards and procedures agreed among parties. The entire trust framework, as described here, is important for policymakers to establish if they are to achieve their goals for an identity ecosystem, and for mobile operators to consider when seeking a role within that ecosystem.

Box 11. Thai Government driving demand for mobile-based digital identity[93]

As part of Thailand's digital economy programme, the Electronic Transactions Development Agency (ETDA), which is part of the Ministry of ICT, is now introducing secure mobile access to digital services, including digital financial services (confirming payments, signing loan applications, etc.) using a PIN on the smartphone. This thus represents an intervention by the government to establish a trusted and simple identity system that may be used to access online banking, e-commerce, e-government, enterprise logins, and mobile payments.

93 http://www.enterpriseinnovation.net/article/thailands-etda-secure-mobile-transactions-mobile-id-authentication-1816984772

Trend 5: Surveillance and trust

Government access and perceptions

Mobile operators are often subject to laws, or license conditions, requiring them to respond to government requests for access to customers' data, to support law enforcement and national security activities.[94] In offering mobile services, operators have access to location and communications data on their customers, and these laws may require operators to retain these data. Mobile operators may also be required to have the ability to intercept customer communications following lawful demand.

National identity systems, particularly where they involve centralised systems, have the potential to aggregate large amounts of data on citizens through monitoring the usage of identities for various purposes. The more digital identities are used – and usage can only be expected to increase if it goes mobile – the more data can be accumulated on any individual's behaviour, including location and services accessed using the identity. For this reason, some governments have given security as a reason for establishing ID systems.[95]

In the wake of the Snowden revelations, there is increased awareness among citizens about governments' access to electronic data, including the content of specific communications as well as 'metadata' about general communications. Furthermore, the Snowden revelations also highlighted that citizens are not always aware of their government's surveillance actions, and thus their perception about government actions will impact their level of trust. In this environment, attempts to establish a mobile-based digital identity system may be viewed by some as enabling increased tracking of users, as the activities authenticated by the identity service are then all, by definition, identifiable (even if that was already the case using other, less obvious, identifiers).

Implications for mobile-based digital identity

Improving transparency

In this light, several indicators may impact users' perception of their government and the role that the mobile identity provider might play in assisting surveillance. Such perceptions may diminish the value, effectiveness and likely take up of mobile identities.

First, of course, there are the government laws and regulations that set out citizens' privacy rights, and the conditions under which governments may access information for law enforcement or surveillance for national security purposes. The presence of such restrictions may not dampen perceptions of mass surveillance, but the absence of restrictions would fuel them. Second is the implementation of those laws and regulation, available oversight, and the corresponding transparency. Although mobile operators often have no option but to comply with such requests, they are among a number of parties interested in greater transparency about the nature and scale of government access.

Indeed, mobile operators can take steps themselves to increase transparency. Many of the largest communications and internet content providers — including AT&T, Deutsche Telekom, Telenor, Verizon, Vodafone, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter and Yahoo! — publish periodic reports showing the types and/or volume of requests from governments for user information. Typically, these 'transparency reports' include how many of these requests resulted in the disclosure of customer information. These reports reveal not only the frequency of such requests, but some detail about the kind of information accessed: customer account information; metadata, which can reveal an individual's location, interests or relationships; and the interception of communications.

94 For more on this topic, see 'Government Access' in GSMA, Mobile Policy Handbook, available at http://mph.gsma.com/publicpolicy/handbook/consumer-protection.

95 See Kenya: President's Speech At the Launch of the Integrated Population Registration System, at http://allafrica.com/stories/201503111566.html

Transparency by governments and mobile operators both helps citizens determine the extent of lawful disclosure in a country, and helps address perceptions regarding government activities.

Finally, third parties can help to assess government activities in surveillance and law enforcement activities. For example, as part of its transparency report, Vodafone publishes a legal annex highlighting the relevant laws, disclosure, and oversight of those laws.[96] Advocacy groups also assess countries, such as the Freedom House Freedom on the Net reports ranking countries on a number of criteria, including surveillance laws and actions (in addition to obstacles to access, limits on content and other factors). For instance, for Bangladesh it notes that there are no specific privacy or data protection laws, and highlights efforts by the government to buy equipment to conduct mobile surveillance. Bangladesh receives 27 points on a scale from 0 (best) to 40 (worst) for corresponding 'violations of user rights', and overall Freedom House measures the level of Internet and media freedom in Bangladesh as being in the middle category, 'partly free'.[97]

Legal frameworks

In addition to providing transparency on government actions, these reports suggest best practices for countries to establish transparent rules for law enforcement agencies and surveillance, which help a country balance a citizen's rights to privacy with legal and national security concerns. These conditions support the trust framework for mobile identity to be established and provide services without mistrust or concern on the part of subscribers.

Mobile operators need to seek, and governments should offer, a clear legal framework that outlines, and limits, government's powers to request mobile operators for access to customers' data. A healthy surveillance regime will respect legitimate privacy expectations. The GSMA published a list of basic requirements for a healthy government access regime, as shown in the Box opposite.

96 Id.

97 https://freedomhouse.org/report/freedom-net/2015/bangladesh

Box 12. Mobile industry position on Government access[98]

Governments should ensure they have a proportionate legal framework that clearly specifies the surveillance powers available to national law enforcement and security agencies.

Any interference with the right to privacy of telecommunications customers must be in accordance with the law.

The retention and disclosure of data and the interception of communications for law enforcement or security purposes should take place only under a clear legal framework and using the proper process and authorisation specified by that framework.

There should be a legal process available to telecommunications providers to challenge requests which they believe to be outside the scope of the relevant laws.

The framework should be transparent, proportionate, justified and compatible with human rights principles, including obligations under applicable international human rights conventions, such as the International Convention on Civil and Political Rights.

Given the expanding range of communications services, the legal framework should be technology neutral.

Governments should provide appropriate limitations of liability or indemnify telecommunications providers against legal claims brought in respect of compliance with requests and obligations for the retention, disclosure and interception of communications and data.

The costs of complying with all laws covering the interception of communications, and the retention and disclosure of data should be borne by governments. Such costs and the basis for their calculation should be agreed in advance.

98 See footnote 94

Where the legal system and administrative procedures already aspire to apply such principles, then the mobile operator may only need to monitor whether they are generally being respected in practice. Where they do not, then the mobile operators in the country might reasonably draw the government's attention to good international practice. Detailed, specific procedures and standards, such as in South Africa's RICA law, support orderly and proper use of surveillance powers (see Box 13 below).

In addition, political and institutional mechanisms of control are particularly important for consideration by mobile operators, including whether national identity systems are managed by independent agencies with clear statutory functions. These would provide for controls on what data are recorded on citizens' use of their national identities, who can access it, for what purpose and in what manner (e.g., some data might be widely accessible on an anonymised basis for research purposes). The power to record and access such data should be counterbalanced by privacy protections. Information ombudsmen or commissioners who are shielded from political control in their appointments, removal, remuneration and accountability may also be useful. Such procedural protections are important not merely as a matter of civil liberties but to nurture trust that will lead to confident development and usage of a robust identity system.

In addition to building a practice and atmosphere of trust and transparency, mobile operators can press to ensure that the rule of law is being respected. It is reasonable and appropriate for mobile operators not merely to respond without question to each surveillance request for data, but to ensure that the surveillance regime is operated in a proper and legitimate manner. This means checking that surveillance requests have been properly authorised according to the applicable legal standards and procedures. While the mobile operator may not be in a position to verify the merits of each individual request, they can follow and document how surveillance requests are being made and implemented, and raise concerns where appropriate.

Box 13. Surveillance in South Africa

South Africa's RICA law[99] prohibits the interception and monitoring of communications (and real-time and archived communication information, and decryption) except by law enforcement personnel in the investigation, detection and prevention of crime. A direction or warrant of a Judge of a High Court is required. Applications to the Judge must identify the officer to carry out the interception, the person subject to interception and the service provider. They must set out the alleged facts and circumstances that are grounds for interception, the basis for believing that evidence relating to the ground of the application will be obtained, other investigative procedures attempted, the period of the interception, and other conditions. The Judge must be satisfied as to the seriousness of the offence, or necessity of gathering the information concerning an actual threat to the public health or safety, national security or compelling national economic interests. The interception direction must specify certain conditions and restrictions and be for no more than 3 months.

99 Regulation of Interception of Communications and Provision of Communication-Related Information Act no.70 of 2002

Conclusions

Any strategy to enable mobile-based digital identity services and generate usage of them will depend on collaboration among key players, particularly government and mobile operators. Additionally, regulators, data protection authorities, standard setting bodies (e.g., ETSI, Open ID Foundation) and information technology companies that may supply technical solutions have a role to play.

Such a strategy needs to keep at the forefront the long-term benefits of digitisation of government and commercial services. Mobile operators can assist by supporting efforts to introduce well-designed legislation to provide a framework for, and confidence in, mobile-based digital identity solutions. For example, laws and regulations can specify what is required to enable registration and issuance of identification for the purpose of accessing important services, such as government services and financial services. These might permit private entities such as mobile operators to issue 'strong identification' (i.e., multi-factor) tokens and services, in each case following prescribed procedures and standards.

Governments can lead the way on the demand side by promoting the development of sufficient number of important services online and incentivising investments so that a critical mass of the population is enabled to use and manage digital identity credentials. This catalytic effect will be strengthened further if government digital identity systems are interoperable with mobile identity systems.

Governments may play an important leadership role on the supply side, overcoming collective action problems by incentivising competing mobile operators to develop common, interoperable SIM registration or electronic KYC (eKYC) mechanisms. Such a collaborative effort is underway in Tanzania, where local mobile operators are working together and use the same common eKYC platform which is itself linked to the National Identity Authority's database, for the purpose of verifying customer identity documents in real time.

Mobile operators' incentives to engage in such programmes will depend on having an opportunity to generate business using the mobile identity system, for instance through offering downstream services such as mobile money, media services and electronic commerce.

This report has highlighted key regulatory policy issues and offered guidance for regulatory policymakers in building an enabling environment for mobile-based digital identity services. These can be expected to help meet government goals to establish and spread uptake of digital identity, foster greater digital engagement between citizens and their governments and consumers with commerce, and accelerate realisation of the SDGs. There are important roles for governments and for mobile operators in developing trust frameworks and the overall climate necessary to build such services.

GSMA has a continued role to play in terms of convening industry, developing material such as this report, and working with donors, NGAs, industry stakeholders and governments to help achieve goals through mobile identity solutions. International governmental organisations and donors can continue to play a role in promoting digital identity solutions that help to meet the SDG goal for identification, which will facilitate achievement of other SDG goals that can be built on digital identification.

Box 14. Public-private collaboration

Governments can and should:

- Establish and clarify their goals for digital identification, and engage with mobile operators and other service providers to plan how to achieve these goals;
- Ensure an effective legal framework governing the collection, storage and use of personal information (including across borders) that protects the data while promoting innovation and efficiency, along with a healthy surveillance regime with procedural checks and balances;
- Lead the creation of a trust framework with specifications, standards and procedures that function effectively;
- Identify roles for mobile operators in establishing mobile identity services that are interoperable with those of other providers and users of digital identity services, and the parameters within which mobile operators can themselves use the mobile identity services downstream (e.g., authenticating mobile money services); and
- Implement the regulatory framework through effective enforcement and resolution of disagreements among players in the digital identity ecosystem according to the general rule of law.

Mobile operators can and should:

- Leverage their existing assets including customer base, devices, and SIMs, into robust new identity solutions;
- Support government efforts to build trust frameworks and effective mechanisms for identity services;
- Respect customers' privacy, including developing and applying Privacy-by-Design principles and/or codes of conduct where data protection and privacy laws are weak or lacking; and
- Balance their goals of increased business opportunities and competitive advantage in offering new services with a level of interoperability that allows adoption of mobile-based digital identity services that meet government goals.

Floor 2, The Walbrook Building
25 Walbrook, London EC4N 8AF UK
Tel: +44 (0)207 356 0600

digitalidentity@gsma.com
www.gsma.com/digitalidentity