Private-Sector Digital Identity in Emerging Markets

OMIDYAR NETWORK

Caribou Digital PUBLISHING

The following Caribou Digital authors wrote this report:
Bryan Pon, Chris Locke, Tom Steinberg.

ISBN 978-0-9935152-7-9 Private-Sector Digital Identity in Emerging Markets

Omidyar Network provided support for this research to evaluate and project future scenarios of the roles and activities of non-state actors involved in digital identity. While Omidyar Network is pleased to sponsor this report, the conclusions, opinions, or points of view expressed are those of the authors and do not necessarily represent the views of Omidyar Network.

Recommended Citation:
Caribou Digital, *Private-Sector Digital Identity in Emerging Markets*
Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2016.

E-mail us at: info@cariboudigital.net

Visit us at: www.cariboudigital.net

Contents

Glossary

Glossary

Anti-money laundering (AML)
General term used to refer to those regulations requiring financial institutions to perform certain checks to mitigate fraud and money laundering.

Authentication
See "verification."

Attestation
Documented support that a claim or attribute is true, typically from a trusted organization or individual.

Attribute
See "claim."

Claim
Similar to an attribute, a claim is a declaration that a trait should be associated with an individual; e.g., a date of birth, membership, nationality.

Credential
A set of identity attributes or claims that bestow on the individual a permission or authorization; e.g., a Web site log-in, passport, or social security number.

eID
Electronic identity, used interchangeably with digital identity.

Identity provider
An entity that allows the user to create a digital identity; in some cases, this identity may be based on an analog credential, while in other cases it may be a stand-alone digital account.

IDP
Stands for "identity provider," but is typically used to refer to that subset of online services that allow their users to log in to other third-party services (relying parties) with the same credentials, e.g., Facebook Connect.

Identity verification provider
An entity that evaluates an individual's identity claims, and typically provides an assessment or score for how likely it is that the individual is who they claim to be.

Know your customer (KYC)
General term used to refer to those regulations requiring organizations to perform due diligence in establishing a customer's identity.

Knowledge-based authentication (KBA)
Method of verifying identity online by asking the user multiple-choice questions about their personal history, including former addresses, amount of car or home loans, bank accounts, and so on; also referred to as static verification because it relies on historical data.

Level of assurance (LoA)
The evidence and verification process that is required to verify an identity; different LoAs are typically codified in regulations according to different types of activities, with less risky activities (sending $5 payment) only requiring a low LoA, and higher-risk activities (opening new bank account) requiring higher LoA.

Personal identifying information (PII)
Data about an individual considered to be sensitive and thus subject to security and privacy protections.

Proofing
See "verification."

Relying party
An organization or firm that needs to verify the identity of the end-user; typically, the relying party contracts out with an identity verification provider to perform that function.

Verification
Also referred to as "authentication" and "proofing," the process by which an identity verification provider evaluates an individual's claims; typically involves examining source documents and third-party data sources to triangulate the claims or credential.

Zero-knowledge proofs
A method of proving an attribute or other information is true without revealing the underlying details, typically using cryptography.

Introduction

Identity is a complex, multi-faceted concept. We often think about our own "identity" as something that is singular and unique, something that reflects our particular mosaic of personality and character traits. But this construction of self is relational, and should be seen as a process embedded in—and constituted by—the social environments in which we live, work, and play.[1]

In this sense, our "expressed" identities are just as much about the social groups that we identify with—e.g., Hispanic, father, Muslim, athlete, Democrat, queer—as much as our individual selves.[2] So while governments (and Facebook) insist that individuals have only a single, fixed identity, in reality we all cultivate and present different aspects of ourselves in different social contexts; "identity" is shorthand for a range of dynamic and iterative social processes.

These tensions between the singular and the plural, the individual and the state, the static and the dynamic, are not new—but they are being complicated by the digitization of identity. New technologies and systems are making identity not only more flexible—e.g., we can create alternative, multiple, pseudonymous (or anonymous) identities—but also more decomposable and extensible—e.g., granular personal data drives lucrative new business models in highly scaled and integrated networks. Companies such as Facebook, Google, WeChat, Amazon, WhatsApp, and Apple have built powerful technology platforms with billions of users worldwide, making them the dominant brokers of digital identities—despite the fact that user identity, per se, is not the product, but a means to a (commercialization) end.

Introduction

For governments, however, providing identity is a fundamental goal that underpins its ability to measure, manage, and control.[3] Digitization in the public sector is moving much more slowly, but the transition away from analog is well underway. Smart identity cards, NFC-enabled passports, and digitally stored biometrics are being used by states around the world as they upgrade legacy identity systems. The benefits of digitization for governments—increased efficiencies, lower costs, reduced fraud and corruption, easier surveillance, better data sharing within government—are clear and significant. And for those countries who haven't yet been able to establish a highly successful analog identity program, the potential of leapfrogging to a fully digital infrastructure is very appealing. Most importantly, the advantages of digital systems have the potential to expand access to identity for otherwise marginalized and vulnerable populations. The benefits of a legal identity for these groups can be tremendous, and the U.N. formally recognized these advantages in 2015 by codifying them into Sustainable Development Goal 16.9: "By 2030, provide legal identity for all, including birth registration."

In almost every way, our Facebook identity and our government identity are worlds apart. They serve very different functions, are managed by very different institutions, and manifest in daily life in completely different ways. But the digitization of identity, and the use cases it enables, has ushered in a range of private sector actors with identity solutions that may start to overlap with the role of state-based identity. Of course, governments already depend on back-end solutions providers such as Morpho, Gemalto, and Forgerock to manufacture smart cards and build databases, and MasterCard has made headlines for its government contracts to provide identity solutions. But a new class of start-ups are embracing advances in mobile devices, biometrics, encryption, and distributed computing to try new models for stand-alone identity solutions. Most of these start-ups are still trying to establish trust in their systems as official identity solutions, and therefore are being primarily used in instances where the "level of assurance" is relatively low, such as single sign-on to Web sites. But over time, these systems may become increasingly robust and credible, either through improved technology or simply their track record and network of partners who trust their solution. The result may be a classic low-end disruption process, whereby these models that originally were only considered good enough for logging into Web sites gradually become seen as viable alternatives for use cases that currently require state-based identity.

To complicate the landscape further, the emergence of blockchain and distributed ledger technology offers new capabilities for open-source, decentralized systems for identity that can be outside the control of any firm or government. This idea of "self-sovereign" identity, where an individual's identity is an irrevocable record under his or her own control, is clearly attractive to those who are hesitant to grant ownership of their digital selves to powerful and profit-driven corporations. But decentralized systems also seem to fit with our increasingly globalized world, where the fluid movement of individuals and organizations challenges the relationship between physical borders, political systems, and the individual. Estonia's e-residency program, for example, is granting limited legal benefits (not citizenship) to "e-residents" anywhere in the world, embracing the idea of a borderless state.[4] Meanwhile the refugee crisis in Europe has highlighted the plight of those caught in-between, as more than 1 million individuals in 2015 alone overwhelmed the political and operational systems unable to cope with the volume of stateless people passing through multiple countries under the care of myriad NGOs and international institutions.

The digital identity industry is currently enjoying a resurgence of interest, as new technological innovations in biometrics, encryption, distributed ledgers, and smart devices have enabled new models for managing identity. Some of these innovations are complicating long-standing ideas about how we express, engage with, and manage our identities, while new organizational structures are challenging traditional roles and power relationships. This research is an effort to explore these themes, with an aim to be speculative, opinionated, and forward-thinking in our analysis. The key goal is to provide an understanding of how new business models and technologies in the private realm may be used in emerging markets—by firms, states, or NGOs—to provide more inclusive identity solutions.

1 Erving Goffman, *The Presentation of Self in Everyday Life* (Harmondsworth, 1978).

2 David Buckingham, "Introducing Identity," in *Youth, Identity, and Digital Media* (MIT Press, 2008).

3 James C. Scott, *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed* (Yale University Press, 1998).

4 Taavi Kotka, Carlos del Castillo, and Kaspar Korjus, "Estonian E-Residency: Redefining the Nation-State in the Digital Era," September 2015, http://www.politics.ox.ac.uk/materials/centres/cyber-studies/Working_Paper_No.3_Kotka_Vargas_Korjus.pdf.

Key findings

Key findings

Despite the critical nature of digital identity as the key enabler of so many of today's services and transactions, we found relatively few firms that are building solutions for managing identity. There is considerable innovation in component technologies, such as biometrics, algorithmic analyses, and distributed ledgers, but much less in actually building new businesses to fundamentally change the current models of identity provisioning. And while the identity landscape is very broad, most of the innovation is concentrated on specific use cases (financial services) and markets (primarily the U.S. and U.K.), no doubt drawn to the perceived higher-value business needs. In short, innovation in this space is happening and on the rise, but is still relatively limited in scope and distribution.

Key findings from the research include:

Few ventures are targeting emerging markets

Digital platforms in emerging markets tend to be dominated by a few global technology firms and the local mobile operators, and this is no different in the digital identity sector. Outside of Facebook and messaging services such as WhatsApp, only the banks and some mobile network operators (MNOs) have any significant base of digital accounts, and neither group seems prepared to build out identity solutions in the near term (see "Banking industry platforms" and "GSMA Mobile Connect," respectively, for more details). Among the start-ups we interviewed, only one firm is actively working on an identity system in an emerging market (Consent, in South Africa).

This is unsurprising at one level, as digital identity is a market with unproven business models in the West, which makes the business case even less clear in developing markets. Add to this significantly lower levels of digital inclusion and disposable income, and the incentive to serve a small online population with an unproven business case is not there. However, the lack of many state-led digital identity platforms does provide a large, if potentially difficult to serve, addressable market over time—if Europe is forecast to have a $1 trillion digital identity market,[5] the potential for Sub-Saharan Africa and other similar regions to establish sizable digital identity markets would be expected to scale alongside the growth in the adoption of Internet services.

Fintech and KYC/AML compliance is driving most business models

Most business cases from the private sector are built out of fintech product experience, looking to create better KYC/AML products, or building on fintech consumer behavior as an "on-ramp" to other digital identity use cases. This is making the new ventures relatively generic, with few innovators looking at other use cases outside of the fintech value-chain (customer onboarding, payment authorization, fraud detection, etc.). Digital credit-rating companies such as Cignifi and Lenddo are showing that building out from products that use basic transactional data, such as mobile phone top-up patterns, can provide estimates of a customer's risk profile, which clearly could evolve into transaction-based or algorithmically derived identity verification for thin-file clients (see topic "Algorithmic models to verify identity are emerging" for more on this topic).

A side-effect of the majority of innovators emerging from the fintech industry is that as regulation (such as open bank identity standards) or technologies (biometrics or distributed ledgers) evolve, it is this that is often driving innovation and new businesses, not a clear understanding of user wants and needs. At best this means the use of technology is often "because it's there" rather than because it creates a solution for a consumer need—for example, when we asked innovators why they are using blockchain, not all could immediately answer—which suggests that user needs are not primary considerations, a factor some commentators are pointing to as the failure inherent in many early blockchain projects.[6]

When regulatory change happens, such as the U.K.'s Open Banking Standard,[7] we see this driving innovation but again without a clear vision of what the end-user benefit is—new products that are possible within the new regulation but perhaps not desirable to the end-user are being created, i.e., we think the businesses are assuming the presence of a market enabled by the regulatory change that may not actually exist.

5 John Rose, Olaf Rehse, and Björn Röber, "The Value of Our Digital Identity," *BCG Perspectives*, November 20, 2012, https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/.

6 For example, see Bedeho Mender, "Why Your Ethereum Project Will Most Likely Fail," March 9, 2016, https://medium.com/@bedeho/why-your-ethereum-project-will-most-likely-fail-d14b6d8f1c7c#.k4fhexhcm., for a good discussion of how most Ethereum-hosted blockchain projects cannot point to a clear end-user benefit

7 "UK Open Banking Working Group Publishes Report Setting out Open Banking Standard | News," *Open Data Institute*, August 2, 2016, https://theodi.org/news/uk-open-banking-working-group-publishes-report.

Key findings
continued

Open, decentralized, "self-sovereign" platforms have appeal, but need use cases

The emergence of new trust-based architectures using blockchains, IPFS (interplanetary file system[8]), and other distributed computing technology has enabled fully decentralized solutions for managing digital identity. Open-source, standards-based platforms such as Blockstack Labs, Evernym, and Open Mustard Seed have a key advantage over proprietary systems in that there is no inherent platform lock-in, and the exposure of the codebase leads to better security and confidence in the system. Back-end solutions provider ForgeRock has proven the demand for open-source identity solutions with its full stack of enterprise identity services,[9] and for state governments, open-source or non-proprietary systems avoid the political risks of perceived public-private malfeasance.[10]

The decentralized aspect of these systems adds a different dimension. While there is certainly a small set of end-users that are attracted to the libertarian ethos that comes with decentralized systems, the broader appeal is for institutions that want the benefits of such a system, but cannot or prefer not to manage their own identity infrastructure. Proponents of decentralized systems cite the Internet itself as an example of what is possible with open and decentralized architecture, yet even the Internet is (to some, overly) reliant on authorities such as ICANN (for DNS) and Verisign (as PKI certificate authority).[11] For governments, decentralized systems may be a double-edged sword: on the one hand, an open and decentralized digital identity infrastructure would be an invaluable public good that the state would not have to manage; on the other hand, states will be reluctant to cede control over identity structures, even though they would maintain control of the actual state-issued credential.

While the potential for these systems is immense, the incentive structure for adoption is diverse across stakeholders, with many of the benefits either long-term, shared (i.e., a commons), or both. Because decentralized systems will be especially reliant on third-party participation to design and provide new services, reaching critical mass that drives the ecosystem becomes crucial, and requires a compelling use case(s) to spur initial adoption by institutional participants.

Algorithmic models to verify identity are emerging, but still niche

There is great promise in probabilistic verification or assessment using algorithms, and firms such as Lenddo and Veridu are already offering verification solutions based on social network data. But there are still many unanswered questions—for example, these models rely on the underlying service to not only provide the raw data, but also on their internal processes for how the data is collected. If Facebook changes its rules for onboarding and ensuring unique accounts, this impacts the verification services. Likewise, if Facebook updates its own algorithms—say, for determining which news feed posts are shown at the top—this can have knock-on effects for user behavior, and possibly change the output of the downstream third-party algorithms that use that data as inputs.

But most importantly, algorithmic approaches are not explicitly supported in the key KYC/AML regulations, which significantly reduces their range of use cases. Although regulations are evolving away from traditional static verification, it will likely be years before policymakers are confident enough in the performance of algorithmic models to codify them in regulation. For example, serious questions around how biases in machine learning manifest—and how to design transparency and accountability into such systems—will have to be addressed.[12] As algorithmic methods become more trusted and eventually legally compliant for an increasing range of uses, we may see a shift in power in identity ecosystems, as data and machine learning supplant the function of certified authorities, including the state.

8 "InterPlanetary File System," *Wikipedia*, July 7, 2016, https://en.wikipedia.org/w/index.php?title=InterPlanetary_File_System&oldid=728691175.

9 "Identity and Access Management Platform from ForgeRock," *ForgeRock.com*, April 14, 2015, https://www.forgerock.com/platform/.

10 Note, for example, the backlash in Nigeria over the recent identity card system with MasterCard, where critics complained about the highly visible MasterCard branding on the cards representing "stamped ownership of a Nigerian by an American company": Clement Ejiofor, "We Don't Want Your ID Card: Nigerians Furious Over MasterCard Logo," *Naij.com*, August 29, 2014, https://www.naij.com/282606-dont-want-id-card-nigerians-furious-mastercards-logo.html.

11 Many argue that the original design of the Internet was overly optimistic regarding security and trusted parties, leading to many of the security challenges we face today. Or put another way, that trust and identity are missing layers from the current incarnation of the Internet. For example, see the perspective of Internet pioneer Dave Clark in this summary article: Muneeb Ali, "Fixing Flaws in the Original Design of the Internet: Trust-to-Trust Principle — Blockstack Blog," *Medium*, March 15, 2016, https://blog.blockstack.org/next-steps-towards-a-secure-internet-a057217acebb#.quf0hukok.

12 For example, algorithmic assessments for prison sentencing show racial bias: Julia Angwin et al., "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks." *ProPublica*, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Key findings
continued

Local drivers to adoption will play key role

State-led identity systems can wield the stick of legal requirement to drive adoption, whereas private-sector identity systems require a clear and significant carrot to drive users to create and use their digital identity, so understanding and designing new products around drivers to adoption is key. Identity use cases are driven very strongly by local regulatory and market needs, but these use cases may be specific to a single market—for instance, Turkcell and other mobile operators in Turkey have had mobile-enabled digital signature services since 2007[13] to meet the intense local bureaucratic need for users to sign many documents for many services, but this product has not transferred outside of Turkey in less bureaucratic business and social environments.

In the U.K. the new identity start-up Yoti, funded by the entrepreneurs behind successful gambling software company Gamesys, seems well-positioned to serve new markets opened up by the U.K. government's desire to have stronger age verification for access to online services such as porn and gambling.[14] This will be a strong market in the U.K., but serves what is at the moment a specific, one-country regulatory use case. Also, as increasing local or regional laws regulating the handling of personal digital data emerge—whether this is the "right to be forgotten" or data sovereignty laws aimed at increasing the taxation of digital businesses—products will find it harder to scale a single solution across multiple markets.

There are few clear paths to scale

Partly as a consequence of our analysis that a lot of the products are building out of largely fintech-led business models, often based on regulatory and technology innovation rather than customer need, and often appealing to niche local needs rather than universal needs that could turn into a platform, we don't believe many of the new entrants profiled have the potential to scale up to be global platforms.

Many may succeed in niche local markets that support their business model, and many may be acquired, but we also think that many may find their product absorbed into the operating systems of the mobile phone platforms. And, ultimately, as at the moment the primary digital identity many emerging market users are adopting as they come online is a Facebook one, new entrants into this space will have to navigate a layer that may look like a sandwich filling between two slices of bread, one being Facebook's (at the moment) light verification identity platform and the other being any state-led identity platform—in other words, at both ends of the spectrum there are incumbents which will be difficult to compete against.

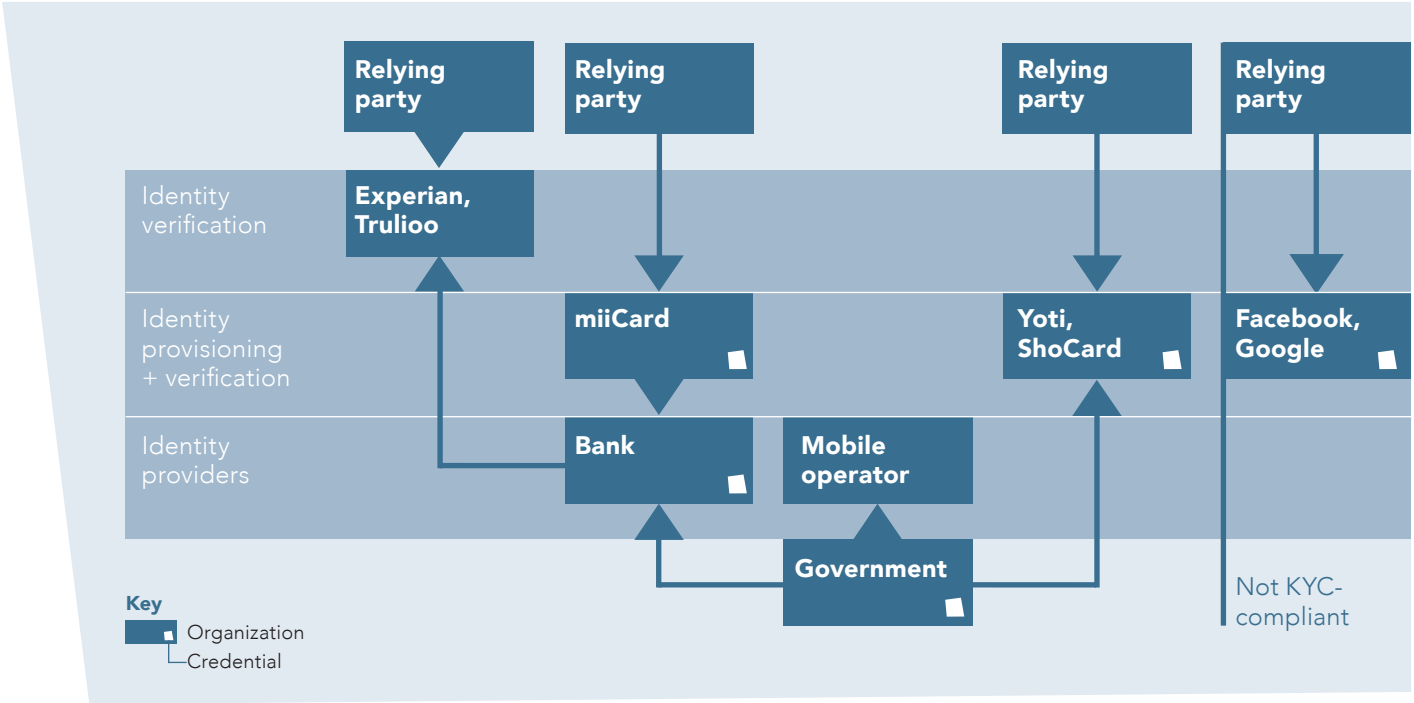
13 "Mobile Signature in Turkey – A Case Study of Turkcell: MobilImza" (GSMA, July 3, 2013), http://www.gsma.com/mea/mobile-signature-in-turkey-a-case-study-of-turkcell-mobilimza.

14 Matt Burgess, "UK's Porn Age Checks Set 'Dangerous' Precedent," *Wired UK*, February 16, 2016, http://www.wired.co.uk/news/archive/2016-02/16/porn-uk-age-check.

Part 1
Industry landscape

Part 1
Industry landscape

Figure 1. Industry structure of digital identity providers



Current industry structure and functional roles

What we may call the digital identity industry is actually the convergence of multiple ICT sectors, each of which have different business models, core competencies, and strategic goals regarding identity. Interestingly, what may be the two most diametrically opposed sectors—the traditional back-end IT systems providers (e.g., Morpho/Safran and Gemalto), and the giant Internet platforms (e.g., Facebook and Google)—are similar in that identity is actually only a means to an end for their business.

The back-end identity systems providers design, build, and manage large enterprise IT systems; the fact that employee or user identity is a critical element of their offering is less important than the scale, technical expertise, and vertically-integrated capabilities that they bring to the table. Likewise, the Internet platforms are not focused on helping users create an identity per se, as much as they are providing a means for sharing and engaging online with other users, and thus supporting advertising revenue.

But there are also a number of new start-ups whose business models are built around providing digital identity for end-users; some of these are focused on consumer products while others are also trying to build open platforms and protocols for integration. Therefore, while many of these firms are superficially providing the same service—a form of digital identity—their underlying businesses are fundamentally different. This means that competition, where it exists, may be asymmetric and harder to recognize and evaluate. In this dynamic, swiftly moving market we expect to see significant moves and transitions up and down the value chain and across sectors.

Given the wide range of models and technologies, we have chosen to focus this analysis on the use cases, customers, end-users, and revenue models of these firms in order to better understand the opportunities and challenges within this quickly evolving market.

The diagram above (Figure 1) represents a simplified view of the digital identity industry, with a focus on the key functional roles and the relationship between actors. While not perfect—it's hard to fit a diverse and complex ecosystem into simple charts—it shows the foundational role of state-based identity credentials and how they underpin the private-sector ecosystems that are built around them.

Figure 1 shows how most of the private-sector identity industry is built on government-based identity credentials, typically a national ID card, driver license, passport, or voter ID card. The two dominant private providers are banks and mobile operators, both of whom are heavily regulated and

Part 1
Industry landscape
continued

must follow thorough customer due diligence (KYC, AML) procedures based on the individual's government credentials.[15] The bank account, which typically includes online access, is then itself often used to open other accounts (e.g., miiCard, PayPal) because the original due diligence is presumed to be strict and thus can be leveraged by subsequent actors, creating a linear value chain starting from the state identity. On the other hand, while mobile operators perform due diligence when onboarding, the vast majority have not leveraged these to create official, KYC-compliant digital identities. This remains a tremendous opportunity for the operators, which we discuss at length in the section "GSMA Mobile Connect."

Typology of firms

To better understand the different business models, strategies, and opportunities of private-sector identity firms we present a simple typology based on functional role, categorizing the firms into four groups, and explaining for each group the key characteristics, opportunities, and challenges. Then in Appendix 1, "Company Profiles," we present representative case studies of individual firms that we interviewed.

Types:

- Enterprise back-end identity solutions provider (e.g., Gemalto, Morpho/Safran)
- Identity provider (e.g., Yoti, ShoCard, Facebook, Google)
- Identity verification provider (e.g., Experian, Trulioo)
- Decentralizied identity framework (e.g., Blockstack Labs, Open Mustard Seed)

Enterprise back-end identity solutions provider

These firms typically provide complete back-end identity solutions to enterprises, managing everything from hardware and back-end system design to implementation and ongoing service management. They are large, global firms with vertically integrated products and services offerings, enabling them to provide complete turnkey or custom solutions. While the focus is on large enterprise, they are often the key contractors used to implement government identity systems. For example, Gemalto-owned subsidiary Trüb makes both Estonia's and Nigeria's e-ID cards, ForgeRock built Norway's government e-services portal, and Morpho/Safran has implemented more than 50 government programs, including U.S. driver licenses, India's Aadhaar database, and biometric voter registration kits in Kenya.[16] These types of contracts will continue, as few governments possess the capabilities for designing and deploying their own systems completely in-house, and the relatively small number of firms in this group are possibly the only companies capable of implementing such wide-ranging and large-scale implementations.

Despite the millions of end-users of their respective systems (Morpho/Safran claims to have issued 2.8 billion identity documents),[17] the firms in this category are not positioned to create their own stand-alone identity systems, as they don't own the end-user relationship—the enterprise (or government) does. But there are no indications that any of these firms are looking to build their own proprietary systems, and given the quickly growing market for biometrics and cloud-based (IDaaS) systems for user authentication, their current role is likely substantial enough to maintain their business models in the medium-term. However, given their scale and deep involvement with state-based programs, the technologies and processes used by these firms—everything from tamper-resistant identity cards to cloud-based authentication services—shape the design of state solutions and the industry more broadly. One trend to watch in this regard is whether ForgeRock, which is a relatively small player, is able to gain widespread traction with its solutions, which are all based on open-source technologies and protocols.

15 While banks in general are fairly consistent in following robust procedures, there are instances of some MNOs following lax enforcement of customer registration processes; for example, see MTN in Nigeria: Tony Chinonso, "BVN Registration: As with Telecom Operators, Would so Be for the Banks?," *Vanguard News*, October 28, 2015, http://www.vanguardngr.com/2015/10/bvn-registration-as-with-telecom-operators-would-so-be-for-the-banks/.

16 Trüb makes Nigeria's most-recent national ID card, launched in 2014 in partnership with MasterCard. See "Government ID Solutions to Facilitate and Secure Identity Management," *Morpho*, February 10, 2015, http://www.morpho.com/en/government-id-solutions-facilitate-and-secure-identity-management.

17 Ibid.

Part 1
Industry landscape
continued

Identity provider

This category includes a broad range of firms, which we divide into two groups: verified identity providers, and non-verified identity providers. The first group is composed of firms that enable end-users to establish a digital identity that is verified or proofed against official documents, i.e., a high level-of-assurance (LoA) verification. In the analog world, this role has been played by banks and mobile network operators (MNOs), who both have to follow KYC and AML regulations to authenticate the identity of new customers when they open an account. Because of this due diligence exercised by banks and MNOs, these accounts have become source credentials that other companies will verify against—for example, PayPal famously invented a method of onboarding new customers by making deposits into their existing bank account, and by verifying that the individual has access to that account, satisfying KYC/AML regulation simply by nature of the bank having already conducted that process. While most banks create secure online accounts that can serve as verified digital identities, MNOs typically do not link their customer due diligence to an online account—a missed opportunity that we return to in the section "Three scenarios for private-sector entry."

There is a host of new start-ups entering this space, and the functional role of providing a verified digital identity is one of the two areas (along with identity verification, below) that is seeing the most innovation due to new technologies and business models. Unlike banks and MNOs, who establish authenticated identity as a means to an end, the majority of new start-ups are focused on the creation of digital identity as their raison d'être. Companies such as Yoti, miiCard, ShoCard, and Global ID are enabling users to create digital identity accounts that can be used in a range of different contexts, from signing up for an online loan to purchasing alcohol in a physical store. The use cases are therefore varied, but the core idea is the ability to create a singular identity that can serve in essentially all instances where digital identity credentials are required.

One of the key value propositions for all of these companies is that they give the user more assurances of transparency and control of their personal information, including what claims or attributes are included in their profile and who they share that information with. For example, a user of Yoti or ShoCard, which are both based on the mobile device and thus work in offline contexts, could show a store owner that the individual is of the requisite age to purchase alcohol, without revealing their name, address, or actual birth date. This granular control of what information to share, and of only revealing the required authentication instead of actual data—known as zero-knowledge proofs—is part of the broader trend toward better user control of personal information.

Most of these start-ups are leveraging smartphone technology to create and authenticate the user's identity, typically through some combination of scanning official documents, such as passports, taking a self-portrait or "selfie" to match the photograph, and storing these data in a secure account.[18] Then when the user needs to access a third-party service that requires identity verification or authentication of a certain attribute, the user consents to having the third-party service connect to their secure account to verify the information required. Firms are storing the PII (personally identifying information) on the mobile device, in proprietary databases, on distributed ledgers, or some a combination thereof.

In terms of regulation and official identity, many of these firms employ a graduated model, whereby the level of assurance—whether and to what degree it complies with KYC/AML regulation—is variable and depends on the amount of information the user submits to their profile. Therefore, someone who only wants a single sign-on for social networks would have to do little to no verification, while someone who wants to use their new identity for getting an online loan would have to go through KYC/AML-compliant verification, which most of these services state they can offer.[19]

18 Some firms have invested significantly in building their technological capacity to detect fraud. For example, Yoti uses 5-second videos instead of selfie photos (better "liveliness" validity) and also verifies the built-in NFC chip in most U.K. passports (better document validity).

19 There is some uncertainty whether the selfie/document scanning model used by Yoti, ShoCard, and others, completely satisfies KYC/AML regulation in different jurisdictions, as it relies on an uncertified copy of the original document. See section "Technology evolution vis-à-vis policy."

Part 1
Industry landscape
continued

In terms of the business model, all of the firms we interviewed provide the service for free to end-users, and earn revenue by charging the relying party, or third-party service, that seeks to verify the end-user. In this way, they are creating two-sided markets around their identity system, and must successfully drive adoption of their service by both end-users and by relying parties in order to gain scale. Put another way, the value of the identity service for each group is directly proportional to the size of the other group; if there are no relying parties who will accept Yoti, then it is not very valuable for end-users to have a Yoti account, and vice-versa. This also means that many of the firms in this category of "verified identity providers" also operate in the category of "identity verification provider"; we discuss the implications of performing multiple roles in the section "General platform strategies."

The second type of firm in this category is non-verified identity providers, led by the large Internet giants, including Facebook, Google, QQ (Tencent), Twitter, Alibaba, Amazon, and Apple, which all have hundreds of millions (over a billion for Facebook) of user accounts worldwide. Many of these firms, but especially Facebook, have increased their reach by allowing their users to log-in to third-party Web sites using their Facebook (or Twitter or Google, etc.) credentials. For many of these firms, serving as online identity providers (IDPs) is not constrained to simply opening up their authorization APIs, but also includes sharing other information about the user (e.g., Facebook posts). The information sharing can go both ways: Facebook and Twitter allow the relying party Web sites to write information back to the user's account; for example, if the user logs in with Twitter credentials and then performs some action, the relying party Web site may then post a summary of that action as a tweet to the user's account.

Figure 2.
Top identity providers (IDPs):

Rank	Service	Protocol
1	facebook.com	OAuth
2	twitter.com	OAuth
3	qq.com	OAuth
4	google.com	OpenID/OAuth
5	yahoo.com	OpenID/OAuth
6	sina.com.cn	OAuth
7	openID	OpenID
8	vkontakte.ru	OAuth
9	weibo.com	OAuth
10	linkedin.com	OAuth

Source: Vapen et. al., Third-party identity management usage on the web. 2014

Of course, the dominant business model for the top IDPs is advertising, and in this sense the creation and management of user identities is simply part of the overall mechanism for attracting user eyeballs. These identities, however, are important: given the near-saturation of user adoption in industrialized countries, the Internet giants have turned to ever more sophisticated ad targeting to drive revenue growth, and that targeting relies on ever more sophisticated data collection and algorithmically determined profiling that can be monetized at increased values.

This represents one of the core tensions within the digital identity space, between user profiles that are actively created by the user vs. those that are passively compiled by the platform firm, and the implications for privacy and user control of personal data.[20] While it is clear that most of the value to end-users is derived from their actively created identities—these are the mechanisms by which users connect, share, communicate, purchase—it is when these profiles are combined with passive data—device type, browsing history, email contents—that they become most valuable to the platform owner. While it's debatable whether, as the advertisers claim, users truly find value in better-targeted ads, there are clearly cases where some

20 For example, the WEF distinguished three categories of personal profiles: volunteered (e.g., user created), observed (e.g., GPS coordinates), and inferred (e.g., credit score). WEF. "Rethinking Personal Data," 2012. http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf.

Part 1
Industry landscape
continued

end-users do enjoy the benefits of passively mined data—for example, when a music application recommends new artists based on listening history.

Importantly, these firms do very little verification upon registering a new user, typically requiring only a valid email address.[21] Removing barriers to adoption clearly helps sign up new users, but this low level of assurance constrains the use cases that such identities can be applied to; financial institutions obviously need more assurance than simply your Facebook log-in credentials. However, the growing importance of digital payments has led many of these platforms to incorporate basic payments functionality into their products, including Apple Pay, Android Pay, Facebook Messenger, and QQ Wallet/WeChat. Some firms are also partnering with banks and financial institutions in order to enable bank customers to send P2P payments using the person's social media username, working almost as an alias for the bank account.[22] By getting users to add a bank card to their account, these platforms are potentially increasing the level of assurance associated with those accounts, and opening up new use cases and value for the end-user.

Identity verification provider

The functional role of identity verification provider has traditionally been performed by the large credit bureaus, such as Experian or Equifax, and other consumer data aggregators. These firms are used by third-party services, or relying parties, to verify the identity of a user online, and they can also be used as supplementary measures along with the primary verification (for example, after the user enters username and password, they may have to answer additional verification questions). The standard approach for verification providers has been knowledge-based authentication, or KBA, which delivers an automated set of questions based on information the agency has on the user, for example, previous addresses, year a mortgage was taken out, make and model of a car, and so on. However, as this type of static personal information becomes more and more available due to security breaches and the commercialization of such data on the dark web,[23] KBA-based approaches are becoming more problematic. We discuss this issue in more detail in the section "Technology evolution vis-à-vis policy."

The identity verification space is the second category that is seeing significant innovation and new entrants. The start-ups we spoke with employ a range of different verification approaches, including smartphone selfie/document scanning, bank account access, and social network data (notably, none use solely KBA). This wide range of approaches partly reflects different use cases, but also different interpretations of current and emerging regulation. In terms of use cases, the most prominent are within financial services, where the increasing complexity and range of financial products (e.g., P2P lending, online gaming/gambling) is meeting increasing oversight and regulation by national and supra-national policymakers. In addition, most of the new entrants we spoke with can support cross-border verification, which is another growing use case due to the effects on international business and migration from increasing globalization.

Because the vast majority of use cases for identity verification require KYC/AML compliance, the regulatory environment is a key factor shaping the technologies and business models. For example, Trulioo has established connections with data providers in over 40 countries in order to provide international verification, but only acts as an information intermediary, and doesn't hold or see the data itself, because many jurisdictions (e.g., Mexico) have stringent laws prohibiting the export of PII. The Australian firm iSignthis uses a PayPal-like method for verifying the identity of consumers making purchases, in part because it believes that regulations will soon require such dynamic approaches. On the other end of the spectrum, Veridu, a start-up using social network data to evaluate user identity, is careful to not advertise its service as KYC/AML-compliant, because at this point no jurisdictions approve such an approach. Importantly, in all cases that we are aware of, the identity verification provider does not actually issue a determination on KYC/AML due diligence, but instead provides information as to whether, and to what degree, it was able to verify the identity profile. It is up to the relying party to establish, within the context of its industry (e.g., banking) and jurisdiction, its own policies as to what processes and level of assurance are adequate.

21 For more on the history of the email address as the de facto Internet identity, including how it functions as multiple personas, see Eric Sachs, "The Hack That Makes Internet Identity Possible," https://docs.google.com/document/pub?id=1O7jyQLb7dW6EnJrFsWZDyh0Yq0aFJU5UJ4i5QzYlTjU#h.i2ivn11phwa5.

22 Jeevan Vasagar, "Singapore Banks Eye Facebook IDs for Transfers," *Financial Times*, July 3, 2016, http://www.ft.com/cms/s/0/b2dd2cd8-3f39-11e6-8716-a4a71e8140b0.html.

23 "A Buyers Guide to Stolen Data on the Deep Web," *Dark Web Reviews*, http://darkwebreviews.com/a-buyers-guide-to-stolen-data-on-the-deep-web-darkmatters/3615/.

Part 1
Industry landscape
continued

Just as in the previous category of "identity providers," the revenue model of the firms in this category is essentially the same: They charge relying parties on a per-transaction basis for performing the identity verification. Depending on the use case and jurisdiction, the relying party may have to also perform subsequent checks of the same user, which typically incurs a lower cost. The costs are obviously a fraction of what it would cost for in-person verification, though for many use cases the competing alternative is relatively low-cost KBA verification. Some of the new firms we spoke with argued that while KBA is cheap, it often returns false negatives and therefore requires expensive customer service support (e.g., when users can't remember their previous address and have to call in to verify themselves).

And finally, some of the firms that act as identity providers also fulfill identity verification roles. Companies such as Yoti and miiCard enable users to create identities, but also provide verification services to commercial clients. The non-verified providers, such as Facebook and Google, also serve both roles due to their IDP function. In these latter cases, however, the verification is not directly monetized (the firm does not charge the relying party to use the IDP service) because the firm earns revenue through advertising.

Decentralized identity platforms

There is a small number of organizations and firms working to develop open and decentralized technology frameworks that support individual identity solutions. These solutions are typically aimed at creating the enabling infrastructure, standards, and APIs that will allow ecosystems of third-party providers to develop the products and services that meet customers' needs. The organization behind the framework is often not itself a provider of identity services, but instead just establishes the framework for certification and credentialing.

The Open Mustard Seed (OMS) project, from the MIT Media Lab offshoot ID3, is an early archetype for this kind of ambition. It proposed an independent, decentralized trust framework for individually managed digital identities, in line with the vision laid out by John Clippinger and others in the Windhover Principles.[24] It would enable users to create core identities, verify different attributes using whichever identity provider the user desires, and record those verifications on the blockchain as part of the user's immutable record. The OMS framework would provide an open-source platform and APIs to support the technological infrastructure, but more importantly, would codify the trust framework that enables all actors to enter into agreements and transactions, including self-executing smart contracts, according to individual preferences.

This decentralized approach to identity provisioning is increasingly referred to as "self-sovereign" identity, in that the individual is in control over his or her credentials—not a central authority—and can manage the ways in which different attributes or credentials are shared. Other organizations in this category include Evernym and Blockstack Labs, both of which also rely on distributed ledger technology as the foundation for their platforms. We discuss this model in more detail in the following section.

Models for identity provisioning

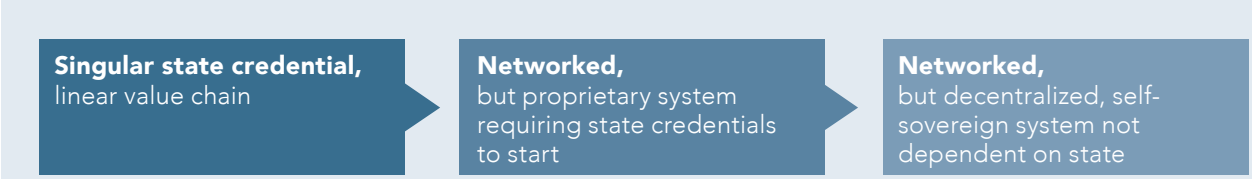
Among organizations that provide digital identities, there are different models for how the identity system is structured. Some differences are in the technical implementation, but more important are the high-level design decisions for how the ecosystem (and business model) function, including incentives for participation, relationships between actors, and issues of power and control.

To illustrate these distinctions, we abstract and simplify three models as archetypical references, starting with the default, state-based system where a single government credential (usually an analog document) forms the basis for a linear value chain of all other identity services. At the other end of the spectrum is a decentralized, self-sovereign model, where a networked identity "container" may include state credentials, but is not dependent on them, and exists outside of any public or private control. And in-between these two is a hybrid model, which includes a networked identity container, but that container is owned by a private firm, and requires a state credential before it can be established.

24 "The Windhover Principles," *ID3*, https://idcubed.org/home_page_feature/windhover-principles-digital-identity-trust-data/.

Part 1
Industry landscape
continued

Figure 3. Identity provider models seem to follow typical technology evolution



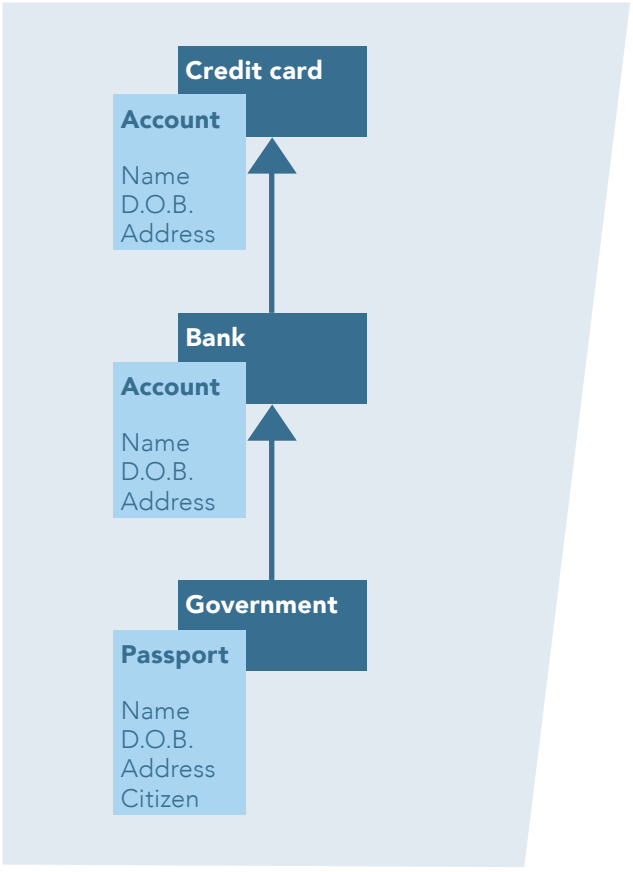
The structure of these oversimplified models suggests a typical form of technology evolution, from a linear value chain to a decentralized and open network (Figure 3). But the integral role of government as sole issuer of legal identity complicates the viability of any model where ownership is divested to either the private sector or individuals. We discuss each of the three types below.

Singular state credential

The single, state-issued credential describes the current or default model, where one (or sometimes multiple) government credentials form the basis of a value chain of identity services (Figure 4). The state verifies core identity attributes to create a "breeder" document or credential (e.g., birth certificate or passport), and subsequent organizations refer back to this original credential when creating new credentials. In the digital realm, this can result in a value chain: For example, an individual uses a passport to open a bank account, and then uses the bank account to open an account with miiCard or PayPal. A single state credential may thus be used for multiple new identities in a one-way flow of data originating with the breeder document. As a result, all the subsequent credentials exist in silos: private firms can't access each other's data, and must copy any attributes into their own credentials, which means that if the individual changes name or address, that change has to be manually updated across all credentials. Low LoA (level of assurance) providers such as Facebook don't typically use an official state credential, but they also lead to linear relationships with service partners.[25]

- Linear, value-chain structure
- Requires state-issued identity as baseline for any official identity
- Data and credentials in silos, resulting in duplicate data across providers
- Individual cannot control sharing on per-credential basis

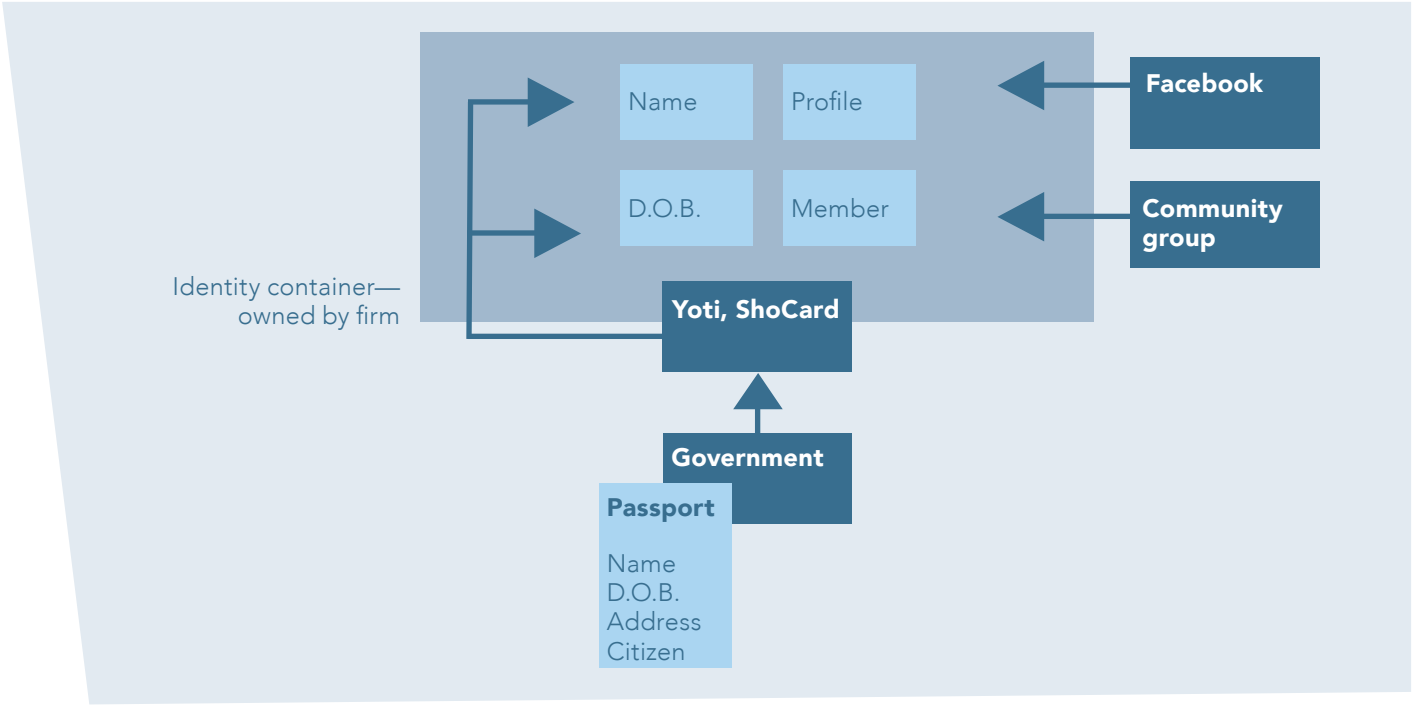
Figure 4. Linear, state-issued credential model



25 Facebook has a "real name" policy, and sometimes requires users to verify their identity if it believes an account is fraudulent. The list of options for verifying one's identity has recently expanded beyond government credentials, and now includes library cards and addressed mail. "Confirm Your Identity with an ID," *Facebook*, https://www.facebook.com/help/contact/319547548123767.

Part 1
Industry landscape
continued

Figure 5. Networked, provider-owned identity container



Private identity provider

Private identity providers typically base their solution on importing existing, state-issued credentials such as a passport or driver license (Figure 5). Once they verify official attributes, they create a digital identity "container," that the user can populate with other credentials, such as Web site log-ins. Because these are typically proprietary systems, the identity provider maintains control over the identity container, leading to de facto lock-in for users to that platform.[26]

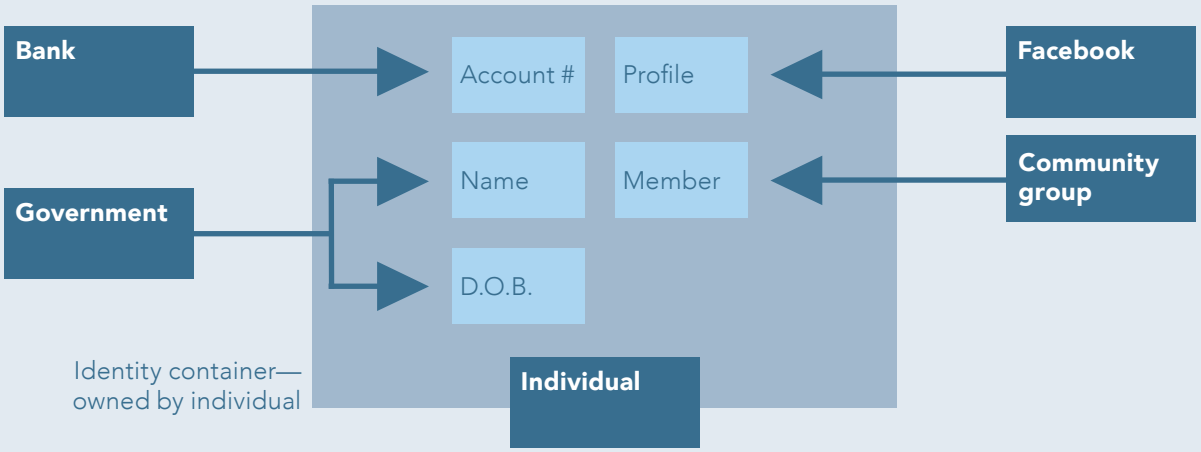
Most importantly, because these solutions are targeting high LoA use cases, they typically require an official state-based credential in order to create the identity. This requirement obviously excludes some users (e.g., thin file or undocumented individuals), but perhaps just as importantly is a barrier to adoption in that it forces users to have their analog documents in hand in order to sign up.

- Typically requires state-issued credentials as baseline identity
- Provider owns the identity container
- Because the state is not verifying attributes—the identity provider is—it is unclear whether these identities will be sufficient for regulated (KYC) use cases
- Typically enables more granular sharing of credentials
- Examples: Yoti, ShoCard, miiCard (based on bank account, which is based on state credentials)

26 One identity provider asserted that the individual's data and credentials belong to the individual, and thus there is no lock-in. But when we asked how the provider has enabled data portability, and whether the data is in a standard format that could be easily ported to another system, they replied that there was no process in place to explicitly enable such a transfer.

Part 1
Industry landscape
continued

Figure 6. Decentralized, networked identity model



Decentralized platforms

Open, decentralized systems enable individuals to fully own and manage their own identities, leading to the idea of "self-sovereign" identity systems (Figure 6). These systems use combinations of distributed ledger and encryption technology to create immutable identity records that cannot be revoked by any government or firm. The individual creates an identity "container" that allows them to accept attributes or credentials from any number of organizations, including the state, in a networked ecosystem that is open to any organization to participate (e.g., to issue credentials). Each organization can decide whether to trust credentials in the container based on which organization verified or attested to them; in other words, a mortgage company may accept a credential issued by a leading global bank, but not one issued by a local bank. Importantly, this model does not require a state-based credential to be initiated (the state credential can be added at a later time, or not at all), which removes a barrier to adoption. We explore this model in greater detail, including implications for emerging markets, in the section "Open-source platforms."

- Can operate with or without state credentials
- Individual owns and manages the identity container
- Non-revocable by state or private firms (individual credentials can still be revoked)
- Typically enables granular sharing of credentials
- Requires trust framework(s) and open architecture
- Examples: Evernym, Blockstack Labs, Open Mustard Seed

Part 1
Industry landscape
continued

The interplay of regulations and technology

The interdependencies between regulation and technology in the digital identity space are strong and important enough to warrant a dedicated analysis. In this section we summarize the relevant policy issues, and then explore how they impact business model and product innovation.

There are three broad categories of relevant regulation:

- Explicitly identity-related policies
- Data protection/privacy policies
- KYC/AML policies for financial services

Firstly, as part of the EU's Digital Single Market, the EU eIDAS regulation that comes into force in 2016 establishes rules for interoperability of government-issued ID in Europe.[27] It specifies three levels of assurance (LoA) for identity verification/proofing, documenting the procedures and checks that need to be performed to certify identity at the three different levels of risk. In doing so, the eIDAS sets EU-wide standards for the due diligence required, reducing uncertainty in cross-border compliance. Furthermore, eIDAS requires that all EU member states accept as valid any national identity credential from another EU member state for similar LoA use cases. This means that a national ID from France should be accepted by the German government for access to relevant government services; more interestingly, it means that an ID from the U.K.—which can be verified by a private-sector firm—should also be accepted by the German government. We explore this topic more in the section "Three scenarios for private sector entry to emerging markets."

Secondly, new EU regulations around data protection and privacy are affecting firms collecting personal data in the EU. The General Data Protection Regulation, signed in December 2015 to replace the 1995 Data Protection Directive, updates the law to enshrine protections for the "right to be forgotten," easier access to one's data, data portability, and stronger fines for infringements.[28] The weight of the EU in setting these types of policies, especially in regard to American Internet service providers, is influencing the technical architectures and business practices of firms globally. This is in addition to existing national policies restricting the storage or transport of data outside of the country. Among the identity providers we spoke with, some have cited the impending EU regulation—especially data portability—as a reason to move toward open systems or away from holding PII (personally identifying information) at all. For example, Trulioo cited the data retention regulations of Mexico of an example of why it doesn't store data itself, instead just passing credentials from its source providers to its clients.

27 "EUR-Lex – 32015R1501," *EUR-Lex*, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL_2015_235_R_0001.

28 "Reform of EU Data Protection Rules," *European Commission*, http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

Part 1
Industry landscape
continued

Thirdly, KYC/AML regulations have a significant impact on the industry. Because the vast majority of private-sector identity solutions target financial sector use cases, they fall under regulations for customer due diligence and anti-money laundering. While the FATF (Financial Action Task Force) and other regional bodies set international regulations for the industry, each jurisdiction interprets these policies into local law, leading to a heterogeneous landscape of regulation that global providers must adhere to.[29] This diversity in last-mile regulation is made more complicated because local laws are often unspecific, leading to uncertainty by firms as to whether a process or data point is in compliance or not. The result of such uncertainty is of course a lower appetite for innovation. Another relevant fintech regulation is the EU's PSD-2 directive, which seeks to regulate financial transactions within the Digital Single Market.[30] It requires banks and other financial services providers to open up parts of their systems for interoperability, with the goal of fostering innovation and a level playing field for new entrants. This has directly enabled new business models; for example, miiCard's verification approach is built on the ability to access account information from other financial services providers.

Targeting fintech means designing for regulations

In our interviews, every firm we spoke with named the financial services sector as a primary target segment. The increasingly diverse range of digital financial services—e.g., Internet-based banking, gambling, e-commerce, crypto currencies, remittances, investing, P2P lending, P2P payments, etc.—is accompanied by increasing scope of regulations. The result is that a broad range of firms are now required to comply with customer due diligence procedures, creating a large market for identity service providers to serve. Therefore, we see KYC/AML compliance being a critical component of most product or service offerings, across both the "identity provider" and the "identity verification provider" categories, though it is perhaps especially strong in the latter.

While traditional banks with physical branches have long had customer onboarding procedures that included due diligence, many of the newer uses cases are completely digital, and thus require an option for "remote" identity verification. This role has been traditionally filled by credit bureaus such as Experian, as well as other forms of data aggregators, using online knowledge-based authentication (KBA).[31]

29 "Countries List," *Financial Action Task Force (FATF)*, http://www.fatf-gafi.org/countries/#FATF.

30 "Directive on Payment Services (PSD) – *European Commission*," European Commission, http://ec.europa.eu/finance/payments/framework/index_en.htm.

31 KBA is typically executed by presenting the user with a series of automatically generated multiple-choice questions, such as selecting the correct year they took out an auto loan, or the street address(es) they previously lived at. The accuracy of the responses is computed to determine the likelihood of fraud or a genuine response. However, given the high rate of data leaks of personal information, KBA has become less effective as criminals can easily purchase much of this type of information online.

Part 1
Industry landscape
continued

New identity verification providers are using new technology or business models to meet this business need in more cost-effective and secure (less vulnerable to fraud) ways. iSignthis is focused on high-volume international transactions, including sports betting and remittances, and patented an approach similar to PayPal: When a user needs to make a purchase that is regulated, the relying party Web site patches in the iSignthis service, which breaks up the payment into two random amounts, effectively charging the user twice. The user then has to check his or her bank statement to verify what the two amounts were, thereby verifying that they have access to that bank account and satisfying due diligence requirements for many firms. Jumio[32] targets some of the same cross-border financial services with its technology solution, which uses the device camera to scan official documents such as a driver license or passport as part of the verification procedure. So although some companies are providing radically different approaches to solving the same customer needs, those solutions are tightly aligned with legal interpretations of what is necessary to satisfy KYC/AML regulations.

Technology evolution vis-à-vis policy

Laws and regulations in most industries struggle to keep up with the pace of technology development, with the resulting delta creating both opportunities and constraints. In the digital identity space, new entrants using innovative technologies or processes must demonstrate compliance with existing policy, which is often vague and open to interpretation. For example, Yoti, ShoCard, and Jumio use self-portraits, or selfies, and device cameras to scan documents in order to verify identity (and in the first two instances, create new credentials). But many of the key customer due diligence regulations were written before pervasive digital cameras and biometrics, and are therefore tilted toward KBA-style verification when physical presence isn't possible. iSignthis CEO John Karantzis argues that approaches that use (digital) copies of documents fail to satisfy many due diligence regulations (e.g., U.K. guidelines 5.3.68 – 5.3.71) because the copies are not independently verified.[33]

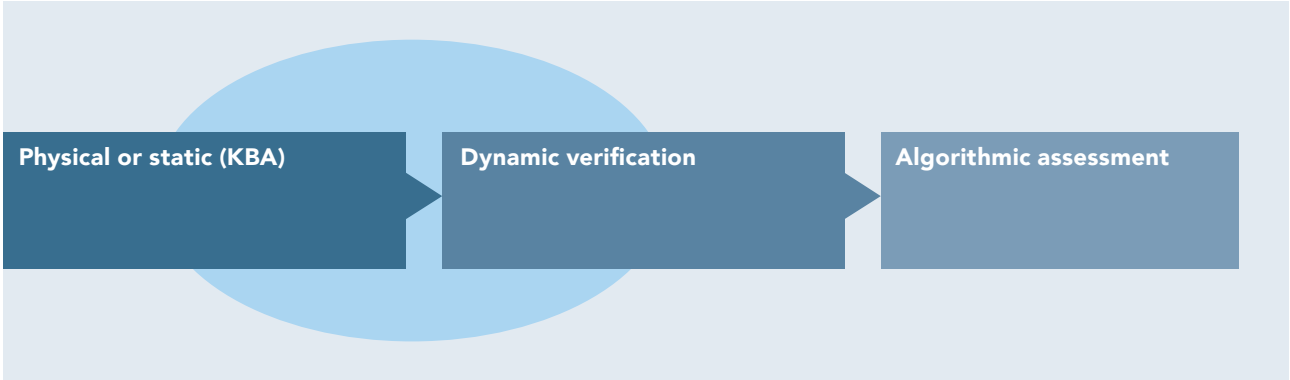
A more important technology that is yet to be explicitly supported in regulation is probabilistic assessment via algorithmic methods. A number of firms are already doing this: Cignifi analyzes mobile phone data to determine risk scores or credit-worthiness for otherwise thin-file individuals, and Lenddo does similar credit assessments using social network data. Veridu takes an approach similar to Lenddo, but is targeting identity verification use cases. All of these firms use large data sets and sophisticated machine learning to develop algorithms that can assess the likelihood that we will pay our loans, or that we are who we say we are.

32 Jumio was interviewed, but after filing for Chapter 11 bankruptcy in March 2016 did not respond to further requests.

33 John Karantzis, "Uploading Document Copies Is Not KYC," *LinkedIn Pulse*, September 14, 2015, https://www.linkedin.com/pulse/uploading-document-copies-kyc-john-karantzis.

Part 1
Industry landscape
continued

Figure 7. Evolution of identity verification, showing scope of existing regulation (oval)



We can put algorithmically defined approaches at the current endpoint of technology evolution for identity verification (Figure 7). Current regulation is explicit on how to handle physical verifications or KBA for remote (online) verifications, and is starting to move toward requiring more dynamic approaches.[34] But it is still far away from trying to accommodate algorithmic assessments into law. This is partly due to the fact that algorithmic approaches are still new, and must be tested and proven. But it's also possible that there will be some resistance toward enshrining legal responsibility in the underlying equations that determine the output of the black box. Data-analytics firms such as Palantir are already using their systems to search for anomalous behavior that could indicate criminal activity,[35] but it's not clear how issues such as legal liability for bias (i.e., illegal discrimination) or false-negatives would be handled.[36]

34 The move toward dynamic approaches (for example, PayPal verification through accessing a bank account) is due in large part to the large number of data breaches, which make personal information traditionally used in KBA easy to purchase on the dark web and thus unsuitable for high levels of assurance.

35 "Counter-Terrorism Tools Used to Spot Fraud," *Palantir*, https://palantir.com/pt_media/counter-terrorism-tools-used-to-spot-fraud/.

36 For more on the social and policy implications of algorithms, see Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).

Part 2
Industry platforms and standards

Part 2
Industry platforms and standards

The nature of digital identity requires a network or ecosystem of participating actors in order for the identity to have value, as a socially constructed identity is inherently relational. In this section we look beyond the firm to analyze the broader ecosystems in which they exist and act within, and highlight some of the key dynamics that are shaping the industry.

We first discuss some general strategy concerns that apply to all of the platform initiatives, specifically bottlenecks, network effects, and technical standards. Then, in the latter half of this section, we use a platform lens to evaluate four very different approaches to establishing industry-wide identity platforms: government-led brokered platforms; banking industry platforms, operator-led Mobile Connect; and decentralized identity platforms.

The bottleneck is from state identity to private profiles

In any given industry, but especially in those characterized by technology platforms, there are typically bottlenecks, or control points, that are critical elements of the overall value chain or ecosystem, and that have high barriers to entry or otherwise defensible characteristics.[37] These characteristics allow a firm to maintain control over the bottleneck and thereby command an outsized proportion of overall industry value.

In the private-sector identity ecosystem, there is a clear bottleneck at the point at which official government identity credentials become translated into a format that is managed by the private sector. This transition from state to private has historically been performed primarily by banks and MNOs (though these latter don't typically create digital identities), but has many new entrants from the likes of Yoti, ShoCard, miiCard, and more, fulfilling the functional role we deem "identity provider." Many of these start-ups employ some form of camera-enabled scanning plus selfie to verify possession and matching of an official government identity document, while others build on the due diligence procedures that banks or other institutions fulfill.

The bottleneck is the result of a combination of technological and regulatory challenges. Technologically, remote verification or proofing requires a process that can reasonably detect fraudulent source documents as well as verify that the person presenting the documents matches the person who was issued the documents. Other steps may include searching international watch lists to ensure the person has not been flagged. These technological challenges are made more difficult because they are dependent on regulatory guidance that is intentionally technology-agnostic. That is, in order to not be overly prescriptive or biased toward a certain approach, and to ensure a longer runway of relevance, policymakers generally aim for regulations that outline abstract principles instead of specific technologies and processes. One result is that legal liability may be unclear—if a firm uses a new technology or process for translating the state credential that isn't explicitly covered by regulation, any mistakes in the due diligence may expose liability.

Solving this problem of the translation of public sector identity into private sector identity may therefore be a critical position in the broader ecosystem. The multiple new entrants that are aiming to serve this role are testament to the potential commercial value it has. However, owning and operating the bottleneck doesn't necessarily lead to a dominant position in the ecosystem—the firm still has to find a way to grow its user base. Therefore, we can foresee a scenario in which one or more of the new entrants that are applying technological innovation to this bottleneck become acquired by larger firms with more established user bases. For example, any of the Internet giants that have huge user populations but no formal verification process could easily buy that capability to create a formidable enhancement of their own identity platform, and solidify their ownership of the ecosystem (although they still would face localized regulatory issues in establishing verification market to market).

Network effects and two-sided markets

Every identity system requires critical mass to become most effective. Network effects, where the value of being a part of the ecosystem increases as the number of other users increases, can help drive adoption, but each ecosystem needs a compelling use case to kick-off that growth. This is especially true for those firms trying to fulfill multiple roles, i.e., providing identities as well as verifying identities. We can say that these firms are creating two-sided markets, whereby they need to incentivize both end-users and relying parties to adopt their solution for a closed-loop ecosystem.[38] Just as the value of having a Visa credit card depends on how many places you can use that card, the value of having an identity document or digital identity is a function of how many service providers accept it.

37 For more theory on bottlenecks, see Michael G. Jacobides, Thorbjørn Knudsen, and Mie Augier, "Benefiting from Innovation: Value Creation, Value Appropriation and the Role of Industry Architectures," *Research Policy* 35, no. 8 (October 2006): 1200–1221, doi:10.1016/j.respol.2006.09.005.

38 David S Evans, "How Catalysts Ignite: The Economics of Platform-Based Start-Ups," in *Platforms, Markets and Innovation*, September 2008 vols., 2009.

Part 2
Industry platforms and standards
continued

To overcome the "chicken-and-egg" challenge, firms creating two-sided markets typically subsidize one side of the market in order to spur adoption.[39] Among those firms that we spoke with that are building two-sided markets, all of them are subsidizing the end-user by providing the service for free, and charging the service provider (relying party) on a per-transaction basis. But the firm must still develop a sound value proposition for two categories of users, and determine how it will allocate its resources between the two.

The firms we spoke with acknowledged the challenge of onboarding both relying parties and end-users simultaneously. miiCard emphasized that its model is less tightly coupled, and that it has built out its identity verification business independently from the end-user identity registration side. This makes sense, given that the commercial verification is the side of the business that earns revenue, but it also highlights the challenge of gaining critical mass of end-user adoption in this space: If the firm offers the basic service for free for end-users—and that is the most common model for highly scaled digital services—it requires a significant amount of funding (typically, VC) to cover operations until it can scale to the point where the revenue model is providing sufficient income. Small start-ups without significant VC money may find it difficult to dedicate the ongoing resources required for highly scaled consumer software systems.

Technical standards and trust frameworks

Any effort to build an industry ecosystem of complementary actors relies on establishing shared standards for interoperability. These can be closed and proprietary, with integration occurring through tightly defined APIs (think iOS), or completely open-source standards defined by the community (think the Web), with advantages to both and most efforts falling somewhere in the middle of the spectrum.[40] In this section we describe some of the organizations working to promote interoperable, open, standards-based systems, including industry associations and formal standards-setting bodies. Some of these efforts are aimed at defining technical standards, while others are more focused on establishing coherent cross-border or cross-sector policies.

At the most technical level, a number of primarily non-profit organizations are working to develop shared technical standards for managing authorization, credentials, and other elements of identity systems. Organizations such as Open ID Foundation (Open ID),[41] IETF (OAuth working group),[42] OASIS (SAML),[43] FIDO Alliance,[44] and W3C (credentials working group)[45] typically follow traditional de jure processes, including multi-stakeholder groups, open and transparent development, and efforts toward consensus. The key actors in these standards-setting processes are typically industry associations, NGOs, and relevant private-sector firms, all of which may have competing standards and agendas. Importantly, adoption and interoperability of standards isn't a binary variable, as organizations may adopt partial standards and supplement with proprietary code (e.g., Facebook building its custom IDP solution on top of OAuth2).

A different layer of interoperability and standardization is enabled by trust frameworks—those policies that define the rules for engagement for all actors in an ecosystem. Trust frameworks are less about technical standards, and more about the business processes, data handling, and regulations that create an environment for trusted transactions. For example, a trust framework might specify how personally identifying information must be stored and transmitted, what privacy policies must be adhered to, and which general system security measures must be followed. Establishing and agreeing to a trust framework gives all parties confidence that the other actors are acting in alignment, enabling increased trust in transactions. The United Kingdom's GOV.UK Verify and United States' Connect.gov platforms had to establish their own trust frameworks in order to set the rules for certified identity providers to participate in the ecosystem. Other organizations working

39 Jean-Charles Rochet and Jean Tirole, "Platform Competition in Two-Sided Markets," *Journal of the European Economic Association*, 2003.

40 For a review of strategies on open vs. closed, see Joel West, "How Open Is Open Enough?: Melding Proprietary and Open-Source Platform Strategies," *Research Policy* 32 (2003): 1259–1285.

41 "OpenID Foundation," *OpenID Foundation*, https://openid.net/foundation/.

42 "OAuth Info Page," *IETF*, https://www.ietf.org/mailman/listinfo/oauth.

43 "SAML Wiki," *OASIS*, https://wiki.oasis-open.org/security/FrontPage.

44 "FIDO Alliance," *FIDO Alliance*, https://fidoalliance.org/.

45 "WC3 Credentials Community Group," *WC3*, https://www.w3.org/community/credentials/.

Part 2
Industry platforms and standards
continued

on trust frameworks include Respect Networks,[46] Mydex,[47] DIACC,[48] and Georgia Tech Research Institute (GTRI).[49]

The GTRI is a NSTIC pilot grantee trying to create a meta-framework that can interconnect multiple trust frameworks, starting with U.S. federal agencies. To do this, it is modularizing all the components of a trust framework into hundreds of more granular "trustmarks" that specify how the organization manages specific issues. For example, one trustmark specifies how long records will be kept for audit purposes, and another the procedure for inspecting analog documents. By atomizing these policies into individual components, the GTRI hopes to enable organizations that do not share the same overall framework to nevertheless evaluate those specific policies that matter, and therefore determine the potential for trusted transactions.

Government-led platforms

While most countries manage their identity programs fully within the administration, both the United Kingdom and United States are building identity programs based on participation by private-sector firms.[50] These "brokered" identity programs are a distinct mix of public- and private-sector involvement, and offer insights into potential routes to market for private identity firms more broadly. In addition to the U.K. and U.S. brokered schemes, we also describe in this section the national identity programs of Estonia and India, which provide sharp contrast in their structure and function, yet are also designed to include participation from private firms.

While currently in the global minority, the models being tested by these countries may demonstrate proof-of-concept for other nations to follow, and have the potential for stimulating increased private-sector involvement. We explore the implications of these government platforms initiatives in more detail in the section "Three scenarios for private-sector entry to emerging markets."

GOV.UK Verify

After considerable debate and user research the U.K. government launched a program called GOV.UK Verify, which is an identity system that has no physical card and no single central population register. GOV.UK Verify mandates that citizens who are trying to obtain a public service log in to that service using an account held with a private sector Identity Provider. The government sets rules about the background checks that identity providers have to perform before an account can be granted, and audits companies on their compliance with these rules. But, crucially, while these rules are comprehensive they have been intentionally authored to allow for companies to differ in terms of what methods they use to establish that an applicant is who they claim to be. This is particularly important since some potential registrants don't have much of a credit history or other official activity on file—so-called "thin file" individuals—and thus require alternative methods of verification.

The government is actively trying to encourage more companies to enter the market as Identity Providers; it wants this market to be diverse because it wants as many people as possible to successfully be able to get an account, and thus avoid the failure scenario where the government must itself go through a slow manual process of paper and in-person verification. An interviewee told us that the government has nearly agreed terms with a mobile phone operator to become, or support, an identity provider. This would be significant since there is a hard-to-reach tranche of the population that has very little in the way of credit history, but which does have mobile phone numbers and histories of mobile billing and usage.

Furthermore, a secondary market is slowly opening up which is to provide data and services to identity providers themselves. These companies do not get paid if users fail to create accounts, so it is worth them investing in anything that can get more people successfully onboard. Companies

46 "Respect Network," *Respect Network*, https://www.respectnetwork.com/.

47 "Ensuring Trust," *Mydex*, https://mydex.org/about/ensuring-trust/.

48 "Digital ID & Authentication Council of Canada," *DIACC*, https://diacc.ca/.

49 "GTRI NSTIC Trustmark Pilot | Sponsored by the National Institute of Standards and Technology," *GTRI*, https://trustmark.gtri.gatech.edu/.

50 Both the U.K. and U.S. populations have historically shown strong resistance to national identity cards or similar federal systems, leading the governments to explore other, less centralized, approaches. While we focus on the U.S. and U.K. here, other countries, including Canada, are also following a brokered approach.

Part 2
Industry platforms and standards
continued

with a lot of proprietary data are more likely to win such contracts than those with algorithmic or social-network based suppliers, which the U.K. government has not yet formally shown any signs of trusting.

There is the prospect that GOV.UK Verify accounts will become accepted outside of U.K. government services, i.e., as proof of identity when supplying private sector goods and services. The crucial unknown here is that it is not known (nor indeed decided) whether the government will definitely allow a non-government service to accept login via Verify accounts. It is thought that this decision will not be made for at least a year, as the government assesses the success of the program in its primary role of facilitating public service delivery. As of April 2016, GOV.UK Verify was about to leave beta status and enter the canon of mainstream government services.

U.S. NSTIC and Connect.gov

The U.S. government's NSTIC (National Strategy for Trusted Identities in Cyberspace)[51] was created by the Obama administration in 2011 in order to guide the development for an identity ecosystem that would support private-sector provisioning of user identities. NSTIC coordinates efforts between the public and private sector, including hosting stakeholder workshops and working with non-profit groups like OIX,[52] to establish shared standards for a trust framework. It also supports a number of pilot projects (15 are active in 2016) to demonstrate potential identity solutions and stimulate the market.[53]

NSTIC has clearly been influenced by the GOV.UK Verify program: The Verify team visited NSTIC in 2012 to share its learnings,[54] and NSTIC explicitly mentions the Good Practice Guide as a reference. Unsurprisingly, then, the initial NSTIC model is very similar: private-sector companies that meet government-defined requirements (currently, Verizon and ID.me) can provide digital identity credentials that are used to access a range of U.S. government services. NSTIC hopes that this marketplace for accessing government services—called Connect.gov—will prove the concept and jump start user adoption, but that the identity ecosystem framework will be used across other sectors as well. While NSTIC is behind Verify in terms of implementation (the NSTIC technical guidelines were just released in October 2015[55]), it seems to have strong stakeholder participation and industry momentum.

The active role NSTIC is playing in funding pilot projects highlights its intention in finding market-based solutions. Recent NSTIC pilots include one led by MorphoTrust, with the goal of creating new digital identity credentials in North Carolina based on the state driver license (miiCard is one of the partners on the project, apparently providing some of its back-end verification technology). Another pilot is led by the GSMA, which secured funding to work with the four largest U.S. mobile operators to explore the integration of Mobile Connect. Therefore while still in its early stages, the NSTIC program and Connect.gov in particular are being designed to facilitate private-firm participation based on a government-defined platform.

Estonia's ID-kaart and X-Road

First issued in 2002, Estonia's "ID-kaart" has become an international eGovernment symbol for just how transformative and all-pervasive a modern identity system can be. Card ownership is reported as being above 90 percent of the population, a number reached through the tactical deployment of carrots, rather than sticks. The incentives for using the card include higher limits on bank transfers, faster tax refunds, ticketless public transport, e-signing official documents and, most striking and unprecedented of all, to vote in national elections.

The card contains encryption keys but no biometrics, and in truth most of the impressive services that citizens get are not due to the physical cards themselves, but rather due to the sophisticated information architecture of the Estonian government. Key to this is a piece of connective software that allows queries to flow between government databases, named X-Road. It is this X-Road system of joined-up databases that allows the company registration process to automatically check for the criminal histories of applicants, as well as their alacrity at paying taxes. Estonia is keen to see its technology adopted more widely, and has convinced Finland to adopt the X-Road system and certain data-sharing agreements;[56] Sweden is also reportedly interested.[57] By signing deals with other Baltic/Nordic states to use its

51 "About NSTIC," *NSTIC*, http://www.nist.gov/nstic/about-nstic.html.

52 "OIXnet," *OIXnet*, http://oixnet.org/.

53 "Catalyzing the Marketplace: NSTIC Pilot Program," *NSTIC*, http://www.nist.gov/nstic/pilots.html.

54 "Identity Assurance Goes to Washington," *GOV.UK*, https://gds.blog.gov.uk/2012/05/29/identity-assurance-goes-to-washington/.

55 "IDEF Core Documents," *IDESG*, http://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents.

56 "X-Road Between Finland and Estonia," *E-Estonia*, https://e-estonia.com/x-road-between-finland-and-estonia/.

57 "Sweden Interested in Estonia's X-Road Platform," *The Baltic Course*, http://www.baltic-course.com/eng/good_for_business/?doc=114572.

Part 2
Industry platforms and standards
continued

software platform, Estonia makes up for its small user population and positions itself to take advantage of the EU's eIDAS regulations when they go live in July 2016. The X-Road system may not have the largest user base of any national program, but its long track record and cross-border implementations will be compelling selling points once the other EU member states are forced to find ways of ensuring system interoperability.

And the Estonian system has significant cross-pollination with the private sector in multiple ways. For example, it is very common for citizens and residents to log in to their own online banking using their identity card, instead of the bank's own log-in, as it is more convenient and enables a full range of banking services (in particular you cannot send more than 200 euros a day unless you log in via your ID card). Estonian mobile operators have also integrated their systems, offering specially issued SIM cards that essentially replace the ID smart card, and mean that transactions can be carried out online that would previously have required a computer, a card reader, and an ID card. Specific examples of private firms building on the national ID platform include currency transfer service Transferwise and the digital signing company Signwise, both based in Estonia.

Finally, Estonia's "e-residency" program is a relatively new initiative that allows non-citizens and non-residents to get a form of the Estonian identity card, which while not conveying legal status does allow the holder to perform certain limited actions, such as opening a bank account or registering a business in Estonia.[58] Amid much fanfare and hype, Estonia has said it hopes to acquire 10 million such members over time, and considers this form of virtual migration key to its plans for offering "country-as-a-service" or CaaS.[59] Verifying these new e-residents remotely may be yet another use case for private firms to get involved in the Estonian identity ecosystem.

India's Aadhaar

Aadhaar is a unique model of state-based identity, in that it creates a digital identity that is divorced from citizenship or legal status. This has been a primary factor in its rapid adoption—not having to navigate and satisfy the complex sociopolitical issues around citizenship and legal residency greatly simplifies enrollment.

And the Aadhaar program has been a tremendous success in terms of enrolling individuals, with well over 1 billion now in the system. It has already resulted in cost reduction in service provisioning, with claims of over $1.5 billion in savings from the LPG fuel subsidy program in one year alone.[60] Recent research from Microsave points to other efficiencies, with up to Rs 100 billion in savings from e-KYC services based primarily on using the customer's 12-digit Aadhaar number to verify identity.[61]

While Aadhaar is a state-based program, its architects envision the unique identity database as a core element of open services and protocols that can stimulate and support private sector involvement in India, what former Chairman of the Unique Identity Authority of India, Nandan Nilekani, has referred to as a "Cambrian explosion of innovation inside and outside government."[62] This idea is central to the India Stack, which is a "unified, integrated layer of digital tools and services leveraging Aadhaar on which the private sector can build customer-facing solutions."[63]

58 "Taavi Kotka Promises 10 Million „e-Estonians" by 2025!," *E-Estonia*, http://e-estonia.com/taavi-kotka-promises-10-million-e-estonians-2025/.

59 Oscar Williams-Grut, "Estonia Wants to Become a 'Country as a Service' and Already Has 10,000 Virtual Residents," *Business Insider*, http://uk.businessinsider.com/interview-with-estonia-cio-taavi-kotka-2016-4.

60 Nilekani Nandan, "Basis of a Revolution," *The Indian Express*, March 9, 2016, http://indianexpress.com/article/opinion/columns/aadhaar-bill-lpg-subsidy-mgnrega-paperless-govt-basis-of-a-revolution/.

61 "Aadhaar Enabled E-KYC Can Save Rs 10,000 Cr over next 5 Yrs," *Business Standard*, http://www.business-standard.com/article/economy-policy/aadhaar-enabled-e-kyc-can-save-rs-10-000-cr-over-next-5-yrs-survey-116031800760_1.html.

62 Ibid.

63 "About India Stack," *India Stack*, http://www.indiastack.org/About-India-Stack.

Part 2
Industry platforms and standards
continued

Private sector use of Aadhaar is growing but remains limited, however. Financial providers are starting to use Aadhaar for KYC. In one notable case, Microsoft is reportedly trying to integrate its Skype VoIP service with Aadhaar in an effort to provide verified digital communications from individuals to government (e.g., users could self-verify using biometrics and connecting to the Aadhaar database in order to have an official video chat with a government agent).[64] It was previously unclear if Aadhaar would continue when the new government come into power in 2014. But the new government has embraced Aadhaar as a foundational building block for some of its key programs.[65] Additionally, interviews with experts and industry insiders suggests that private sector use of Aadhaar is now expected to increase following recent parliamentary backing for its use for government services.

Banking industry platforms

For the banking industry, increasingly stringent KYC regulations have led financial institutions to develop expertise and robust processes for verifying identity and onboarding customers. The level of oversight has engendered trust in their processes, and banks have long served as the principal entity translating state-based identity credentials into private-sector digital credentials such as an online bank account or eID.

The incentives for banks to manage identity well include both internal operational savings (e.g., reducing fraud and other forms of identity-related losses) and avoiding fines for non-compliance from regulatory bodies, which have been on the rise[66] due to increased scrutiny after the financial crisis and in response to terrorist financing. New technologies in distributed ledgers, encryption, and biometrics are causing many organizations to explore options for upgrading their legacy identity systems, which are often disconnected from other parts of the business, resulting in duplicate data, incomplete views of the customer, and perhaps most importantly, higher costs and challenges for preventing fraud.[67] Implementing more robust and secure identity management solutions can therefore help financial institutions capture significant savings while also improving the customer experience. This potential is attracting technology providers such as Credit.Vision and Gem, which are offering blockchain-based identity solutions specifically designed for financial institutions.

Given their expertise and strong incentives, financial institutions are seen by many as the primary drivers of next-generation digital identity solutions.[68] And in some markets, banks have already assumed a primary role in providing digital identity solutions beyond their own operations. In the U.K., Barclays joined the GOV.UK Verify program in April of 2016 as one of its certified companies offering digital credentials for users to access U.K. government services.[69] In Canada, a scheme managed by SecureKey enables customers of multiple financial institutions to use their existing credentials to access dozens of Canadian government services online.[70]

64 "Microsoft Runs Pilot on Linking Skype and Aadhar," *The Times of India*, February 19, 2016, http://timesofindia.indiatimes.com/tech/tech-news/Microsoft-runs-pilot-on-linking-Skype-and-Aadhar/articleshow/51055959.cms.

65 Anirban Sen, "Budget 2016: Nandan Nilekani Lauds Decision to Give Aadhaar Statutory Backing," *The Economic Times*, February 29, 2016, http://economictimes.indiatimes.com/news/economy/policy/budget-2016-nandan-nilekani-lauds-decision-to-give-aadhaar-statutory-backing/articleshow/51195080.cms.

66 Recent examples include a £72 million fine on Barclays in 2015 for inadequate customer due diligence, a £7.6 million fine on Standard Bank for AML lapses, and a more systemic violation by three state banks in India drawing a Rs4.5 crore fine for inadequate KYC processes; see, respectively: The Financial Conduct Authority, "FCA Fines Barclays £72 Million for Poor Handling of Financial Crime Risks – Financial Conduct Authority," https://www.fca.org.uk/news/fca-fines-barclays-72-million-for-poor-handling-of-financial-crime-risks; The Financial Conduct Authority, "Standard Bank PLC Fined £7.6m for Failures in Its Anti-Money Laundering Controls – Financial Conduct Authority," https://fca.org.uk/news/standard-bank-plc-fined-for-failures-in-its-antimoney-laundering-controls; B. S. Reporter, "RBI Fines Three Govt-Run Banks for Violating KYC Norms," http://www.business-standard.com/article/finance/rbi-fines-three-govt-run-banks-for-violating-kyc-norms-115043000029_1.html.

67 "The Power of Identity in Retail Banking" (ForgeRock), https://www.forgerock.com/app/uploads/2015/10/ForgeRock-Retail-Banking-USA.pdf.

68 For example, see "The Future of Digital Identity Is Up to Banks," *American Banker*, http://www.americanbanker.com/news/bank-technology/the-future-of-digital-identity-is-up-to-banks-1079943-1.html; David Birch, *Identity Is the New Money* (London Publishing Partnership, 2014).

69 "New Certified Companies Now Connected to GOV.UK Verify," *GOV.UK Verify*, https://identityassurance.blog.gov.uk/2016/04/06/new-certified-companies-now-connected-to-gov-uk-verify/.

70 "The Canadian Experience," *SecureKey*, http://www.skconcierge.us/the-canadian-experience/.

Part 2
Industry platforms and standards
continued

A different but notable example is MasterCard, which has been increasing its presence in the identity field through partnerships with NGOs[71] and governments, including Nigeria and Egypt.[72] The Nigerian government has contracted MasterCard to provide smart cards that not only serve as identity credentials, but also enable financial payments.[73] The project has been met with criticism over the corporate branding on a national ID card,[74] though it appears that the program will be run and administered by the Nigerian National Identity Management Commission, with MasterCard only one of several contractors. In this sense the project is not a bank-led effort, but a government initiative with a strong financial institution as key partner.

The longest-running and most advanced bank-led models are probably in Northern Europe, where many countries have been using bank-issued digital identities (typically referred to as eID in Europe) for a decade or more. All of these programs include tight integration with the state, with online access to government services a primary use case for the bank eID. But there are important differences in how the programs have evolved, and the current state of functionality, that are instructive. For example, when the Swedish government sought to establish a digital identity standard for accessing state services, it recognized the popularity of online banking and consumer trust in banks, and worked with a consortium of banks to develop a new eID in 2002. This BankID has seen strong adoption, especially with the addition of a mobile version by local operator Telia, to an estimated 80 percent of adults, but its use has been limited to online banking services and government services, without broader adoption in the commercial sector.[75]

In contrast, in Norway the banking industry came together to launch its collaborative identity platform, also called BankID, in 2003 without direct involvement of the government. The government eventually sought a private-sector solution to providing eID to citizens, but could not come to agreement with the banks over security features and costs. After eight years of mounting political pressure over budget overruns with its own solution—during which time the BankID platform continued to grow in popularity—the government was forced to compromise with the banks and integrate with the existing BankID standard.[76] The system is currently used by 3.5 million of a total population of 5 million, for everything from e-commerce to real estate to auto sales, in addition to banking and government services.[77]

Finland followed a similar path as Norway, with the banks developing an industry standard digital identity, TUPAS, independent of the government. The Finnish government launched its own national identity standard, FINEIED, but saw relatively little uptake, and eventually bestowed equivalent legal validity to the TUPAS format, even though it is less secure than FINEIED.[78] And finally, in the Netherlands a new bank-led program is being piloted in 2016. Facilitated by the Dutch Payments Association and Innopay, the iDIN program builds on existing inter-bank relationships to allow users to conduct commercial and government transactions online using their bank identity, as well as authenticate themselves across 3rd-parties with granular controls for which personal data to share.[79]

While in both Norway and Finland the banks' identity solution was initially launched as a commercial solution that was only later adopted by the government, in all cases the

71 "MasterCard to Expand Digital Aid Distribution Services," *MasterCard*, http://newsroom.mastercard.com/press-releases/mastercard-to-expand-digital-aid-distribution-services/.

72 Ibid.

73 Alex Court, "Branding Nigeria: MasterCard-Backed I.D. Is Also a Debit Card and a Passport," *CNN*, September 25, 2014, http://edition.cnn.com/2014/09/25/business/branding-nigeria-mastercard-backed-i-d-/.

74 Ini Ekott, "SCANDALOUS: Outrage in Nigeria as Government Brands National ID Card with MasterCard's Logo – Premium Times Nigeria," Premium Times Nigeria, August 29, 2014, http://www.premiumtimesng.com/news/headlines/167479-scandalous-outrage-in-nigeria-as-government-brands-national-id-card-with-mastercards-logo.html.

75 Åke Grönlund, "Electronic Identity Management in Sweden: Governance of a Market Approach," *Identity in the Information Society* 3, no. 1 (July 2010): 195–211, doi:10.1007/s12394-010-0043-1.

76 Ben Eaton et al., "Achieving Payoffs from an Industry Cloud Ecosystem at BankID," *MISQ Executive* 13, no. 4 (2014), http://misqe.org/ojs2/index.php/misqe/article/view/550.

77 "Areas of Use – BankID," BankID, https://www.bankid.no/en/company/areas-of-use/.

78 Teemu Rissanen, "Electronic Identity in Finland: ID Cards vs. Bank IDs," *Identity in the Information Society* 3, no. 1 (July 2010): 175–94, doi:10.1007/s12394-010-0049-8.

79 "Dutch Interbank Digital Identity Service Announced," *Innopay*, https://www.innopay.com/blog/dutch-interbank-digital-identity-service-announced/.

Part 2
Industry platforms and standards
continued

state saw value in supporting a private-sector, banking industry eID for access to its own services. For the government, there are many benefits to relying on a market approach anchored by banks, including lower costs for users due to competition among providers, faster scale-up due to leveraging the existing customer base of bank customers (in many cases), and reduced development and ongoing operational costs to the government for building and maintaining the system.[80]

Outside of Europe there are few examples of bank-led identity solutions. We spoke with an association of U.S.-based credit unions that is exploring potential distributed ledger-based identity solutions, with the goal of extending the system externally into a commercial platform. In addition to the fraud reduction and other internal cost savings, they described a top benefit being the ability to increase their speed to market with new products, as their current identity systems require lengthy integration efforts across legacy systems, which is especially challenging when working with third-party vendors. Another possibility is the R3 consortium,[81] which includes 40+ primarily global financial institutions, and could in theory build out the identity component of its collaborative distributed-ledger technology into an extensible identity platform.

One lesson from the Northern European countries is that the successful identity platforms were built by industry associations, not individual firms, which were able to leverage the user base of all member institutions to reach scale with a solution that then becomes adopted more widely. Both the Norway and Finland cases demonstrate the power of this technological path dependency, where the private sector solution reached critical mass to the point where government felt compelled to accept it. It's important to note, however, that this outcome may partly be due to the relatively small populations and markets of the Nordic countries, where the number of financial institutions required to collaborate might be more manageable, and the absolute numbers for reaching critical mass are much lower.

Another factor whose impact is difficult to assess is the effect of cultural attitudes toward privacy and trust in institutions. One comparative case study found that individuals in the Nordic countries report more trust in banks compared to other European countries, which helps explain the success of the bank-led model there, but other correlations—for example, trust in government agencies—were less clear.[82] In the U.S., the global recession of 2008 and changing attitudes toward Wall Street have led to a low point in trust and positive opinions of banks in some markets: For example, only 27 percent of adults have confidence in banks, half of the proportion prior to the 2008 recession.[83] While this distrust is evenly spread across political groups, there is a clear difference between generations, as younger adults—e.g., the "Millenials"[84]—have a much lower opinion of traditional banks. A Facebook study of Millenials showed that compared to other generations, they are more likely to switch banks, less trusting of financial institutions, and less likely to feel that their bank understands them or their financial needs.[85] Another research study on Millenials indicated that 73 percent would be more excited about financial service offering from the large tech companies—Google, Apple, PayPal, or Square—than their own bank, and perhaps most damning, 71 percent would rather go to the dentist than listen to what banks are saying.[86] Attitudes toward financial institutions will vary by country and demographic, but these studies highlight the possibility that in some markets, banks may not be considered the most trusted entity to manage something as personal as a digital identity. Instead it may be those firms which have deeper or more personal relationships with consumers—for example, personal technology firms such as Apple or Facebook—that consumers trust with their digital selves.

80 Grönlund, "Electronic Identity Management in Sweden."

81 "R3," *R3CEV*, http://r3cev.com/.

82 Herbert Kubicek and Torsten Noack, "Different Countries-Different Paths Extended Comparison of the Introduction of eIDs in Eight European Countries," *Identity in the Information Society* 3, no. 1 (July 2010): 235–45, doi:10.1007/s12394-010-0063-x.

83 "Americans' Confidence in Banks Still Languishing Below 30 percent," *Gallup*, http://www.gallup.com/poll/192719/americans-confidence-banks-languishing-below.aspx.

84 Definitions vary, but one study defined the group as those born between 1981–2000, which makes them at 84 million the largest generation of working age in the U.S.

85 "Millennials + Money: The Unfiltered Journey" (Facebook, January 2016), https://fbinsights.files.wordpress.com/2016/01/facebookiq_millennials_money_january2016.pdf.

86 "The Millennial Disruption Index" (Viacom), http://www.millennialdisruptionindex.com/.

Part 2
Industry platforms and standards
continued

GSMA Mobile Connect

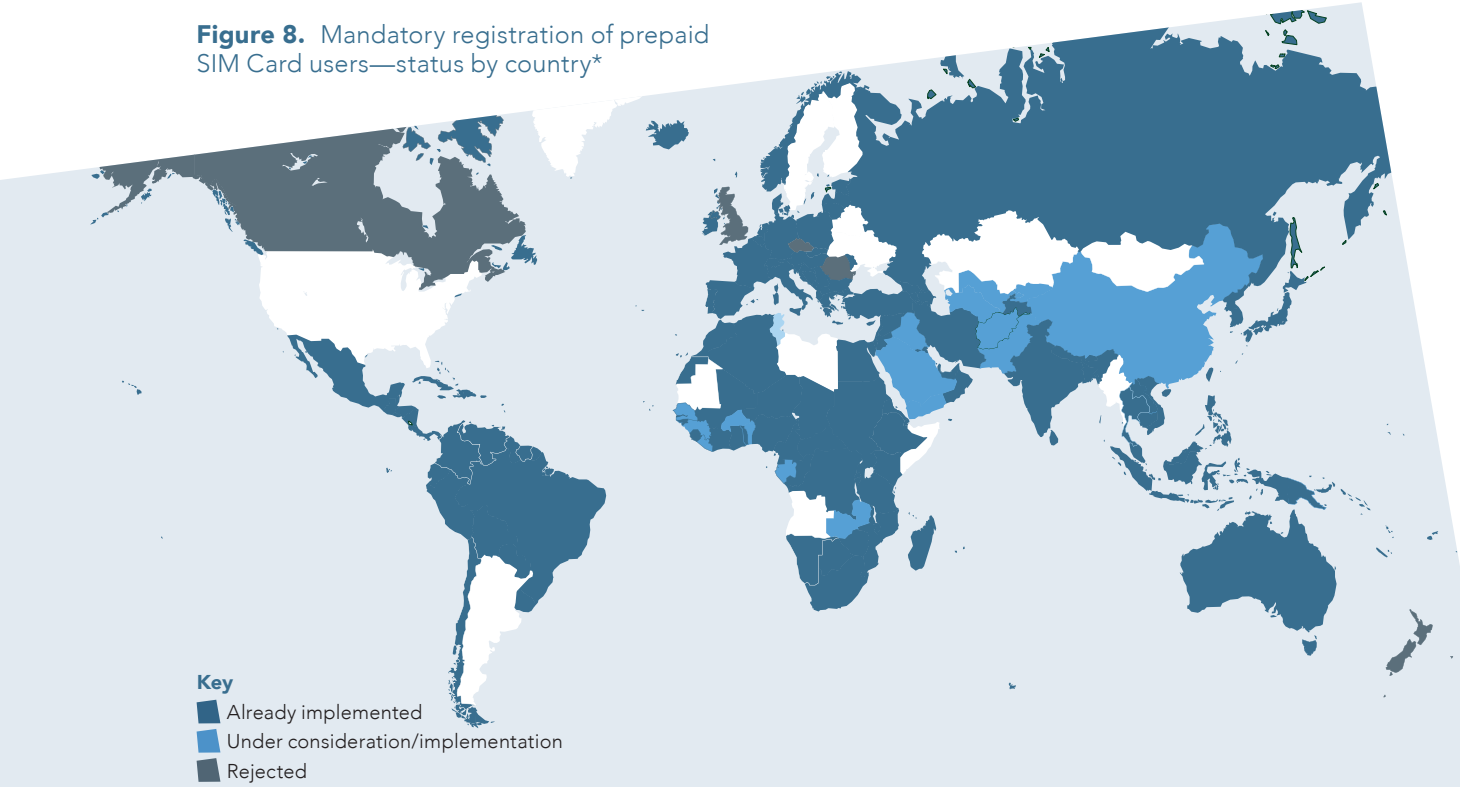
Launched in 2012, the GSMA's Mobile Connect initiative is an ambitious attempt to open up probably the world's most ubiquitous identity technology—the mobile phone SIM (subscriber identity module)—into a platform with the potential to connect private sector companies with a user base of, at time of writing, over 4.7 billion mobile subscribers.[87] There are other factors that benefit the mobile industry's ability to play within this space, and that makes Mobile Connect a platform with strong potential.

Firstly, in most markets, and increasingly in emerging markets, governments require that mobile operators verify SIM cards against a form of ID at the time of purchasing. This is particularly increasing for pre-paid SIM cards, which as they don't require credit in the same way pay-monthly contract SIM cards do, are otherwise vulnerable to usage by those who seek to maintain their anonymity for nefarious purposes. This has meant that SIM card verification is a contested area between governments and mobile operators, with the former blaming the latter for perceived laxity in times of crisis and terrorist atrocity.[88]

In emerging markets mobile operators have extensive agent networks selling airtime and signing up new customers, which gives them a phenomenal existing network to physically register customers and overcome issues such as reaching rural populations and overcoming literacy issues. Partly as a result of these vast agent networks, mobile money has been successful at driving digital inclusion in emerging markets, with 271 services now live in 93 countries.[89] This base of transactional, KYC-compliant consumer identities tied to a mobile SIM card should be a tremendous asset to help the mobile operators achieve scale.

Mobile Connect as a product—unlike many other digital identity platforms we have researched—has a strong base of consumer research underpinning it, and as such it is a

Figure 8. Mandatory registration of prepaid SIM Card users—status by country*



87 Intelligence GSMA, "GSMA Intelligence," https://www.gsmaintelligence.com/.

88 Mark Okuttah, "CEOs of Telcos Face Arrest over Sim Card Crimes," October 7, 2013, http://www.businessdailyafrica.com/CEOs-face-arrest-for-Sim-card-crime/-/539546/2023132/-/cjtbdt/-/index.html.

89 Janet Shulist, "What Is the Availability of Mobile Money Services in 2015?" (GSMA Mobile for Development, 2016), http://www.gsma.com/mobilefordevelopment/programme/mobile-money/what-is-the-availability-of-mobile-money-services-in-2015.

Part 2
Industry platforms and standards
continued

leading source of data to understand the potential use cases for digital identity. There has been significant investment from the GSMA in researching consumer needs and sizing the potential for digital identity as a product, particularly in markets such as the EU[90] and U.S.[91] This should serve two distinct purposes: driving mobile operator productization of the Mobile Connect platform towards use cases which build on actual end-user needs, and also encouraging third-party developers to consider using the platform, given the scale of potential revenues described. Partly as a result of this research, the GSMA has put in place a very strong privacy framework within the Mobile Connect product, which serves to position the mobile operators, with the SIM card at its core, as a strong advocate of consumer privacy concerns.

However, while the most recent announcement from the GSMA points to a potential addressable market of 2 billion users on the Mobile Connect platform, actual active user numbers are harder to come by, and it's not clear how many of the mobile operators who have signed up to the service have deployed the platform at scale.

Also, at the moment the Mobile Connect platform is primarily a challenger for Facebook at a relatively low level of assurance for verification, with most use cases and implementations driven by user registration and logging on to Web sites using Open ID Connect and OAuth2 standards,[92] in a similar way that Facebook Connect is used as an IDP by relying parties. O2 and Vodafone in the U.K. are now trialing Mobile Connect for transactions sharing more complex user data,[93] and the expectation is that new developers and partners coming online will increase the sophistication and usage of the platform.

As mentioned above, respecting end-user privacy is constantly referred to as a significant attribute of the Mobile Connect platform, something we hypothesize impacts across two potentially opposed vectors of travel for the mobile operators: first, that privacy management can be positioned as a perceived product differentiator and consumer benefit; and secondly, that it can help move mobile operators into the advertising value chain.

As a product differentiator, privacy is an issue that the GSMA's own research has shown to be a key issue for consumers, and mobile operators see the robustness of the SIM as a unique basis for delivering strong consumer privacy. Other industry players such as Apple have strived to differentiate themselves from advertising-led competitors such as Google by taking user privacy and the sanctity of their encryption and personal data protection systems to extreme lengths against the government.[94] Like Apple, mobile operators do not at the moment make their income from selling users' personal data for advertising purposes, and therefore can position themselves as trusted managers of user privacy in what is an increasingly febrile environment between platforms and their users.

On the other hand, in terms of entering the advertising value chain, operators could use Mobile Connect to insert themselves into the personal data value chain for Web and app services if they want to monetize their users' personal data. The GSMA has previously tried to establish global advertising platforms on behalf of the mobile industry, looking to divert up to 25 percent of advertising revenue into the mobile operator businesses,[95] without success. This has the potential to position the mobile operator as a "dumb pipe"—and even worse, as a free bearer of the data required to serve advertising to the end-user, while not benefiting at all from the revenue. Mobile operators are starting to fight back, with the Israeli start-up Shine[96] getting traction from operators wishing to block ad traffic directly at the network level as a way of discouraging the creep of end-user data consumption by ad traffic software. The deployment of such ad blocking software at the network level is positioned strongly as a response to consumer needs and as a campaign on behalf of the consumer's benefit, in line with the positioning of Mobile Connect. But it's noticeable that operators are reserving the right to still serve advertising, but give the user "more control"[97]—which may indicate

90 "Mobile Connect Consumer Research Report: European Union" (GSMA, 2015), http://www.gsma.com/personaldata/mobile-connect-consumer-research-report-european-union.

91 "Mobile Connect Consumer Research Report: United States" (GSMA, 2015), http://www.gsma.com/personaldata/mobile-connect-consumer-research-report-united-states.

92 "Mobile Connect Developer Portal," *Mobile Connect*, https://developer.mobileconnect.io/content/overview.

93 "GSMA's Mobile Connect Available to 2 Billion Consumers Globally," Personal Data, February 22, 2016, http://www.gsma.com/personaldata/gsmas-mobile-connect-available-to-2-billion-consumers-globally.

94 Dan Levine, "Apple Could Use Brooklyn Case to Pursue Details about FBI iPhone Hack: Source," *Reuters*, March 30, 2016, http://www.reuters.com/article/us-apple-encryption-idUSKCN0WU1RF.

95 "Triad Case Study," *Triad*, http://consulting.triad.co.uk/cs-gsma1.html.

96 "Shine Technologies," *Shine Technologies*, https://www.getshine.com.

Part 2
Industry platforms and standards
continued

that ad-blocking is an entry point for the mobile operator to re-enter the advertising value chain. A combined approach—blocking "over-the-top" ad networks on one hand with products like Shine, while inserting the mobile operator into the personal data value chain via Mobile Connect—would position the mobile operators as a strong force in the advertising value chain, with a strong story aligned to protecting consumer's privacy and rights.

Decentralized identity platforms

As we discussed in the section "Models for identity provisioning," the decentralized and networked identity solution embodied by Evernym or Blockstack Labs seems to represent the current endpoint for the evolution of digital identity systems. One of the key distinctions of this model of identity is that it does not require state-based credentials to function—the state is just one of many different entities that can attest to a credential that is placed within the individual's identity "container." This flexibility mirrors the approach taken by Aadhaar in India—instead of basing the entire identity system around an official credential that bestows legal status, Aadhaar deliberately provides only a unique number, allowing each government agency to issue official credentials on top of that number according to their own criteria and, importantly, timeline. For Aadhaar, this has vastly sped up the enrollment process, as it is not bogged down by the political ramifications of determining legal status for each individual before registering an Aadhaar number. Of course, while Aadhaar enrollment is voluntary, the incentives to do so (e.g., access to government subsidies) are so strong that over 97 percent of adults have registered.

For a system such as Evernym, the process is similar—an individual can create an identity and gather useful credentials without having to first (or ever) submit official state-certified credentials. This is helpful in situations, for example, where an individual has indeterminate legal status (e.g., a refugee), by allowing them to still create an identity even though they don't yet have a state-certified credential. The advantage of the identity container is that the individual can accumulate credentials from different sources, such that even if they are lower level of assurance, they are all tied to a single individual and thus benefit from the trust that comes from a mutually reinforcing collection of credentials. Of course, unlike Aadhaar, which is still a state-backed program, Evernym and other decentralized systems like it will have to develop an incentive structure through which individuals can register a state-certified credential in their identity container, as many if not most use cases will require it.

By removing the requirement for a formal due diligence or verification process to create a digital identity, the Aadhaar and Evernym models are not unlike the "risk-based assessment" approach advocated by financial inclusion organizations. RBA approaches allow for a set level of activity to occur without requiring customer due diligence or other regulatory burdens that have the practical end result of excluding marginalized populations. In both models, individuals can register and use the system for tasks that are considered low levels of assurance without the traditional barriers to participation. This clearly helps by providing a minimum level of service to the largest possible population segment, and also helps speed adoption of these systems, helping them grow toward the critical mass that attracts participation and innovation by third-party services. One can see this same approach employed by social networks, messaging apps, and other digital services—the platform prioritizes end-user adoption with a simplified product with low barriers to access, and then gradually adds more sophisticated functionality and other options that may require extra effort or cost by the user.

Of course, for the refugee in our example, and many others, having low LoA identity credentials may not be sufficient. To realize fully inclusive digital identity and the benefits it can provide, individuals need credentials that not only enable access to services and markets, but that provide official status that can protect their basic human rights. And this type of official or legal status can only be bestowed by the state, which is unlikely to cede this control.

But the state could maintain its monopoly over issuing credentials with legal status while withdrawing from owning and controlling the rest of the identity infrastructure. In the decentralized, networked identity model, the infrastructure could be open-source, and facilitated or serviced by any number of different for-profit or public organizations, without infringing on the state's sovereignty. The state would need to design its official credentials to interoperate with whatever open-source standards become dominant, and would be in a sense limited to advancements in those standards. But this could free the government from the substantial costs of designing, implementing, and maintaining the security of a full identity system infrastructure.

97 Natasha Lomas, "Shine Signs First European Carriers To Its Network-Level Ad Blocking Tech," *TechCrunch*, February 18, 2016, http://techcrunch.com/2016/02/18/shine-bags-first-european-carrier-as-three-uk-deploys-network-level-ad-blocking/.

Part 3
Hypotheses and discussion

Part 3
Hypotheses and discussion

Three scenarios for private-sector entry to emerging markets

In this section we explore three potential scenarios in which the private sector increases its scope in provisioning of identity systems in emerging markets.

1. Facebook expands to provide official identity

As the 800lb gorilla, Facebook holds the keys to the kingdom when it comes to reach and impact. With 1.59 billion users, 84 percent of which are outside of North America, Facebook is the largest global platform by user base.[98] But one also has to consider the user populations of its other properties—WhatsApp (1 billion), Facebook Messenger (800 million), and Instagram (400 million)—to appreciate the company's massive scale.[99]

While creating a Facebook account typically does not require anything more than a valid email address, the company does require users register with "the name you use in real life." Amid some controversy, in 2012 Facebook started reinforcing this "real name" policy after revealing almost 9 percent of its profiles were fake. A spokesperson said "Authentic identity is important to the Facebook experience, and our goal is that every account on Facebook should represent a real person."[100] While this policy is intended to help maintain trust in the network it may also serve to keep the door open for the company to move into official identity provisioning of some kind.

But perhaps more indicative of its potential move into more formal identity is Facebook's launch in 2015 of P2P payments within Messenger. The service is currently designed for casual payments among friends, as the sender and recipient have to be friends on the social network. The advantage of Facebook in this space is illustrated by the verification policies of other P2P providers: Venmo and Snapcash both have lower weekly limits for transfers ($300 and $250, respectively) until the user verifies her identity with personal information, or by linking to her Facebook account, at which point the limit increases to $3,000 and $2,500.[101] That a Facebook profile is seen as an intermediate level of assurance for these other services speaks to the potential for Facebook identity to move into more formal identity verification.

Facebook accounts are being used for payments functionality outside of the U.S. as well. In India, Axis Bank has launched a service allowing its customers to send P2P payments using only the person's Facebook, WhatsApp, or Twitter username, facilitating transfers without having to know the recipient's bank account number.[102] In Singapore, a similar service is launching in early 2017 with a consortium of 20 banks; the service will enable bank customers to register their Facebook identity to their bank account, and send immediate P2P cash transfers to other Facebook or Twitter accounts.[103]

Given Facebook's track record of acquisitions and running parallel services independently (especially Messenger), it seems clear that the company prefers to keep its core service relatively stable and focused, such that if it were to branch out into official identity services, it would probably maintain those separately from the core product. But just as Blockstack Labs and miiCard allow users to connect their Blockstack Labs or miiCard profile to all of their social accounts—thereby verifying access to said accounts—one can imagine a Facebook official identity product being a core identity that the user can associate with their Facebook, Instagram, WhatsApp, and Messenger accounts.

Zero-knowledge proofs would allow a user to communicate with another user via WhatsApp, and if they had linked WhatsApp to their verified identity profile, they could show the other user via WhatsApp that they really do live in California, or are over 18, and so on. Yoti believes there is a use case for verified identity in providing P2P trust in the sharing economy and social digital transactions; they have built the trust mechanism, and are now trying to attract users. Facebook has all the users, and could easily acquire a trust mechanism.

98 1.59 billion monthly active users; "Company Info," *Facebook*, http://newsroom.fb.com/company-info/.

99 Obviously, there is much overlap between services, as many end-users multi-home between these platforms.

100 Cadie Thompson, "Facebook: About 83 Million Accounts Are Fake," *CNBC*, August 2, 2012, http://www.cnbc.com/id/48468956.

101 As of May 2016, Venmo and Snapcash have updated their policies to now require the individual's date of birth and social security number.

102 "Indian Bank Launches WhatsApp, Facebook, Twitter Mobile Payment," *Banking Technology*, http://www.bankingtech.com/297431/axis-bank-india-launches-whatsapp-facebook-twitter-mobile-payments/.

103 Vasagar, "Singapore Banks Eye Facebook IDs for Transfers."

Part 3
Hypotheses and discussion
continued

The opportunities:

- Leverage immense user base for wide-scale social impact in emerging markets (extension of Internet.org digital inclusion campaign)
- Open new use cases for Facebook Messenger payments (i.e., KYC-compliant)
- Deepen connection with users, with more lifetime value and increased switching costs
- Open new, non-advertising revenue streams with verification services

The challenges:

- Facebook is an advertising company, and as such tends to fall on the opposite side of the privacy debate than many consumer groups do; it may be hard to balance the need to mine user data for advertising revenue while developing digital identity verification revenues built around more robust user privacy management
- Entering into identity verification brings Facebook into a country-level engagement with data sovereignty, taxation, and privacy management. As a global platform, Facebook prefers to have a single product for its global audience, and enjoys the economies of scale that this brings. Managing multiple, forked identity platforms to meet the needs of local regulation might not be worth it for Facebook—and data sovereignty laws may challenge Facebook's ability to locate its value creation around personal data in the tax regime of its choice.[104]

2. Public-private models such as U.K. Verify or BankID spread

Given their similarities, the NSTIC and GOV.UK Verify approaches represent a relatively cohesive model for the provisioning of identity services within a public-private framework. The sheer weight of the institutions—the leadership role of the U.S. and U.K. in technology development, plus the hundreds of millions of U.S./U.K. residents who could participate—raises the question of whether this brokered public-private model could become the dominant format for private-sector involvement in official identity provisioning. If widespread adoption by both end-users and commercial providers occurs in these markets, it's possible that other countries would implement similar programs and possibly even the same providers (already, Verizon is a certified provider for both the U.S. and U.K. programs).

One of the most important drivers of these programs is that they are establishing clear technical and process guidelines for different levels of assurance—a trust framework—and thereby providing firms with the regulatory clarity that they require for participating in such a heavily regulated space. Clear and transparent specifications, standards, and guidelines lay the groundwork for robust and competitive private-sector involvement. But the flip side of state-based regulations is that they are limited to that jurisdiction, constraining the scale of any solutions. For example, the Financial Action Task Force (FATF) provides international policy guidelines around KYC, AML, and ATF regulations, but member states interpret those guidelines differently with domestic laws, creating a highly heterogeneous policy environment that makes it difficult for private firms to operate across jurisdictions.

The GOV.UK Verify program, however, falls under the EU's eIDAS regulation,[105] which when it goes into effect in July 2016 will specify EU-wide guidelines for digital identity provisioning. This includes the requirement that EU member states must accept digital identities provided by another member state in order to access state services—in theory, a resident of Germany should be able to use his German digital identity to access state services in France. This means that a digital identity created under the Verify scheme in the U.K. should be valid across the EU for some use cases, allowing private-sector identity services to be

104 Heather Stewart, "Facebook Paid £4,327 Corporation Tax despite £35m Staff Bonuses," *The Guardian*, October 11, 2015, http://www.theguardian.com/global/2015/oct/11/facebook-paid-4327-corporation-tax-despite-35-million-staff-bonuses.

105 Note that this analysis was written prior to the U.K. referendum, and therefore assumes EU membership. The implications of "Brexit" are not evaluated here. "Trust Services and eID – Digital Single Market," *European Commission*, https://ec.europa.eu/digital-single-market/en/trust-services-and-eid.

Part 3
Hypotheses and discussion
continued

accepted in dozens of countries. In an interview with a knowledgeable U.K. government source, we were told that embracing eIDAS was a deliberate part of the U.K. government's attempt to foster a new private-sector identity market, with the EU being the key to enough scale to make private sector investment worthwhile.

Public-private models are not limited to the U.K. and U.S. incarnations. As discussed in the section "Banking industry platforms," a number of countries in Northern Europe have successful digital identity platforms led by banks and other financial institutions as the certified providers, including the BankID programs in Norway and Sweden. Like the U.K. and U.S. brokered schemes, these bank-led programs have an explicit mandate and support from their national governments for providing digital identity solutions. But it isn't clear, however, whether any of the existing bank-led models in Northern Europe are looking to expand their solution (Estonia is clearly interested in exporting its underlying X-Road platform, but its program is essentially run by the state).

All of these public-private models—whether the brokered models of the U.K. and U.S., or the bank-led models of northern Europe—are designed to connect to the state's existing identity infrastructure. That is, the digital identity credential is created by the private sector, but is tied to the individual's existing state-based unique identity, whether a social security number, national ID card, or other form. Therefore unlike the Facebook scenario, these public-private models are best-suited for those countries that already have a robust foundational or civil registry with deep penetration among the population—countries such as Tanzania or Nigeria, where identity programs have stalled or are severely fragmented, wouldn't be prime candidates.

The examples of Norway and Finland show us that a purely commercial effort on the part of a banking industry association can successfully launch a digital identity platform without explicit support from the state. However, the incentives for the financial institutions in those cases were around growing transaction volume both internally to the banks, as well as with third-party commercial services, among a user population that was already connected and comfortable with online transactions. For banks and other financial institutions in emerging markets, the much lower rates of online banking and scarcity of other online services significantly weakens this business case in most markets. Indeed, the only example we have encountered of a financial institution in the Global South working on an identity solution is Barclays in South Africa, where its work with Consent appears to be more about reducing its internal costs of KYC compared to launching a broader identity platform.

Opportunities:

- Clear and specific policies from U.S. and U.K./Europe could set de facto global standards for private-sector involvement
- Market-based public-private approach is less costly to the state, while promising more innovation
- Governments operating these new systems represent a market for new private sector companies that can provide identity verification based on non-government proofs, e.g., banking history or mobile phone account history

Challenges:

- Public-private schemes require the state to have robust identity systems already in place, limiting the potential market opportunities
- No indication that there is a business case for banks and financial institutions to launch purely commercial platforms in emerging markets
- Regulatory environments may never align sufficiently to enable wider change beyond each market

Part 3
Hypotheses and discussion
continued

3. The mobile operators change course and enter the game

As discussed above, the unique assets of the mobile operators in emerging markets (mobile money, agent networks, deep penetration) means that they are the top private-sector challenger to Facebook in their ability to create a platform at global scale. The potential is already there for them to challenge Facebook from the opposite direction—whereas Facebook would need to deepen its verification processes and engage more with local regulators to capture more of the digital identity value chain, for mobile operators already deep into regulatory relationships at the local level, and who often already have to verify their product against state-backed identity in SIM registration, it's a simpler task from a business process perspective to move into the lesser-regulated task of lower level-of-assurance verification of digital identity for Web sites and apps.

However, deepening the verification levels in the other direction, where there is not already a link between the SIM card and the state-level identity, might not be desirable. Anecdotally, mobile operators we have spoken to have shown some concern about getting deeper into the responsibility of verifying identity, and are structurally looking to create more separation between themselves and the state's influence on their business. This is both to reassure consumers that they are not, as is often reported, in the pocket of the state as a consequence of obtaining their license to operate,[106] and also to collectively protect themselves within conflict-afflicted states where the consequences of being able to track users, send messages to them, and act as both P2P and broadcast communication channels makes them vulnerable to violent demands (the Telecommunications Industry Dialogue group[107] was launched in the aftermath of the Egyptian Tahir Square protests specifically to try and find a common industry voice of operators' concerns about undue and violent influence on them in times of crisis—it seeks to define and respect privacy and users' freedom of expression from a human rights perspective).

Finally, much rests on the continuing life of the SIM card—the physical umbilical cord between the mobile operators and their customers. In its current form it provides both a tangible connection between the mobile operator and the end-user, while also in its physicality providing a marketing and distribution role for the mobile operator as customer acquirer. This positions it well as a trusted partner for the end-user in managing personal data and privacy. However, recent technology developments are pushing the function of the physical SIM into the software stack, meaning that the need to be provisioned with a physical SIM card to start using a device is starting to recede.

At one level, the software SIM developments are a phenomenal boon for the mobile operators. They stand to benefit hugely from the growing Internet of Things (IoT) market as the connective tissue between the billions of devices—from cars to crates—which can be monitored and tracked using new technology. Indeed the Embedded SIM program at the GSMA[108] is leading the adoption of this, and talks eagerly about the revenue potential from connecting not only the 7 billion humans on the planet, but the many billions more of inanimate objects.

While this Embedded SIM product opens up the IoT market for mobile operators, similar software also simultaneously opens the door for other players to step in and sever the connection between the mobile operator and the human end-user, pushing the connectivity aspect of a device down further into the "dumb pipe" part of the value chain.

Apple has been experimenting with this software, and has deployed it initially in the iPad Air 2 and other devices over the past few years. While Apple is still reliant upon mobile operators as distribution networks it has refrained from too radical an implementation, but there is no technological reason why Apple couldn't be the retail organization the end-user has a billing relationship with, as the device surfs automatically for the best deal on connectivity based on location, availability, and price.[109]

106 Julia Angwin, "AT&T Helped U.S. Spy Internet on a Vast Scale," *The New York Times*, August 15, 2015, http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-Internet-traffic.html?_r=1.

107 "Telecommunications Industry Dialogue," *Telecommunications Industry Dialogue*, http://www.telecomindustrydialogue.org/.

108 "Remote SIM Provisioning for M2M," *GSMA*, March 28, 2012, http://www.gsma.com/connectedliving/embedded-sim/.

109 Chris Woodcock, "Five Years On, Apple's Battle to Kill the SIM Card Is Nearly over," *The Memo*, July 30, 2015, http://www.thememo.com/2015/07/30/five-years-on-apples-battle-to-kill-the-sim-card-is-nearly-over/.

Part 3
Hypotheses and discussion
continued

This severing of the billing and customer relationship management role with the mobile operator is perhaps the most significant existential challenge for the mobile industry's role in digital identity provision, as it terminally weakens the fundamental relationship between the operator and the user that the power of the SIM card is built on.

Opportunities:

- As the only interconnected industry with the scale to challenge Facebook, the opportunity to develop a platform with real network effects is palpable to the mobile operators
- The physical SIM card, for as long as it lasts, is a very secure, user-centric architecture upon which to build a digital identity product
- Existing mobile money deployments in emerging markets have blazed a trail, leaving a legacy of KYC-compliant user registration, transactional consumer behavior, and agent networks to build a user base for digital identity

Challenges:

- Operators may not wish to have deeper relationships than they already do with government in some markets, and may not want to carry the risk of being blamed when the abuse of identity platforms is figured as instrumental in crime or terrorist atrocities
- If the software-based SIM gets traction, the mobile operators may lose their status as customer-acquirers, or many even become more invisible to the end consumer, and resemble more the multitude of Wi-Fi networks users currently briefly engage with to get connectivity, but then forget

Discussion

Discussion

The traditional approach to identity provisioning—analog documents issued by the state—is clearly giving way to digital forms, which enable a wealth of new use cases, business models, and industry architectures. Our interviews with firm executives and industry experts revealed a few key themes that seem to be shaping the evolution of the industry, including the potential for applications in the Global South, which we summarize here in a final discussion.

Firstly, there is little evidence of go-to-market strategy for any of the firms profiled to enter an emerging market. Although some of the identity verification plays were explicit about their model not being applicable to emerging market users, almost all of the identity providers at least played lip service to wanting to extend their reach into the Global South (Consent, in South Africa, was the only firm we found actively working in a developing country).[110] There does seem to be enthusiasm for private sector involvement, as evidenced by the ID2020 group organizing a summit and technical workshop in May 2016 to bring together business, technical, and policy stakeholders in private-sector digital identity with the goal of discussing ways to speed progress toward the UN SDG 16.9.[111]

But the pathways for these private sector firms to enter emerging markets are not clear. This is in part because most of the private-sector identity providers are from the West, and are unapologetically designing solutions for end-users in the West; i.e., a blockchain-based identity solution that allows an individual to create a human-readable name for their Bitcoin wallet is not going to find high demand in peri-urban Mumbai. This focus is primarily strategic (there's more money in North America and Europe), but it's unclear if many of the teams have experience with understanding end-users, use cases, government identity systems, or the business environment of digital systems in emerging markets.

The challenge is all the more difficult because of the heterogeneous technical, cultural, and regulatory environments in emerging market countries. In terms of regulations, while most countries comply with international regulations from FATF or regional AML organizations, each jurisdiction interprets those differently, making high level-of-assurance use cases difficult to scale across multiple markets.[112] Multiple firms we spoke with mentioned that even though their processes probably satisfy regulations in other jurisdictions, the legal uncertainty of how local law would be interpreted results in conservative approaches. As the World Bank's ID4D group notes, the regulatory environment—everything from data protection laws to the institutional structure to the program revenue model—is key for establishing a financially sustainable ecosystem that can deliver benefits to an inclusive population.[113]

Just as important is the current status and technology infrastructure of any national identity system. As Alan Gelb and Anna Diofasi at the Center for Global Development have documented, there is immense variety in the type of technology, user penetration, system integration, and functional uses of different countries' existing identity systems.[114] Similar to any enterprise business systems provider, foreign identity firms will have to design solutions that can be integrated with the wide range of legacy systems in place, and then resource teams for custom implementations with the underlying foundations. But any solution that creates yet another (proprietary) silo of duplicated identity information—for example, certifying analog credentials through scanning documents and comparing to a selfie—is unlikely to drive innovation and widespread change in a market. On the other hand, approaches that establish basic identity infrastructure that is connected into a country's national identity systems could instead provide an open platform for other services and business models to hook into—precisely what the India Stack initiative we described earlier is trying to do.

110 We, of course, are excluding the Internet giants of Facebook, Google, etc.

111 "ID2020 Annual Summit," ID2020, http://id2020.org/; "ID2020 Design Workshop," *Web of Trust*, http://www.weboftrust.info/.

112 Of course, this also creates opportunity—South Africa's unique KYC regulations have created the need for a local company such as Consent to address the problem.

113 "Identification for Development (ID4D) Integration Approach" (World Bank, 2015), http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/09/21/090224b0830efe0f/2_0/Rendered/PDF/Identification0ation0approach0study.pdf.

114 Alan Gelb and Anna Diofasi, "Scoping Paper on Identification and Development" (Center for Global Development, 2016).

Discussion
continued

This may be an area where technical standards can play a role. The WC3's Credentials working group is one effort at codifying specifications from a wide range of stakeholders in order to enable better interoperability of identity systems.[115] One of the industry experts involved told us the group is seeing strong interest from industry, especially in the healthcare and education sectors, but also with national governments, including India and Estonia. This isn't surprising given what we know about those governments' approaches to opening their platforms, but it does suggest that buy-in from states could help drive interest and adoption of international identity standards.

This kind of leadership from the state shouldn't be underestimated. Government can leverage its own demand (i.e., for government services) to create a market for private sector firms that it certifies as approved providers, as in the brokered model of GOV.UK Verify. In these cases the state is explicitly defining the rules and approving who can participate. But government can also focus on the infrastructure layer and regulate participation through the technology—essentially, a platform model—as the Indian government is doing with its open API policy and the India Stack. Offering access to 1 billion users with APIs for verification, digital signing, and more, the Indian state is creating strong incentives for a wide range of private firms to provide new commercial services. In both of these cases the government is actively establishing rules for engagement that allow firms to enter the market with certainty, yet the models and the markets they create are very different. And while it's easy to argue that the open platform model of India is more likely to drive private-sector innovation, that option isn't realistic to all countries, as most don't have the resources or political will to implement such an ambitious undertaking. And even among those who do, those without a large population will struggle to attract private firms to provide services, as commercial developers will gravitate toward the largest or most lucrative user base.

And finally, as with most technology products, we expect that there will be different primary use cases that drive adoption in different markets. Compared to other technologies, the value of a digital identity is more tightly tied to the use cases it enables, and less about its intrinsic worth. In other words, no one wants a "digital identity"; people want the ability to easily do remote banking, file for government services, or access other commercial services. Therefore, new entrants would be wise to conduct on-the-ground research to better understand end-users and use cases in representative emerging markets, as this is one of the largest and most important knowledge gaps in the industry. Outlining the most important user needs and prioritizing use cases would help firms better understand the potential customers, partners, and business models they need to design for.

These challenges suggest an on-the-ground complexity that is not readily served by any one solution. While Facebook, Google, and the other giant technology firms leverage an essentially identical product in every country (apart from minor content exclusion exceptions), this is possible because those services can sit high up in the stack, far away from the messy reality of local infrastructure and systems. But for any digital identity solution to truly be inclusive and help the most vulnerable, it must integrate with the state in order to provide the legal benefits arising from government credentials. Therefore, despite efforts at international standardization at both the technical and regulatory levels, private sector identity players will need a more customized approach for national or regional implementations. This barrier to global scale should be seen as a positive, as it opens up opportunity for local or regional players to compete in the market.

115 "WC3 Credentials Community Group."

Discussion
continued

That optimism for home-grown solutions should be tempered, however, by the huge advantages of scale that the large technology firms and mobile operators possess. The gravitational pull of the Facebook ecosystem draws in new start-ups providing services in all sectors, and even if innovation is only incremental, the platform's scale can mean those services can grow into industry leaders. It could be that even if Facebook doesn't officially move into formal identity provisioning, growth in third-party services that leverage its profiles—e.g., the banks in India and Singapore using profiles as identity aliases for P2P payments—creates an ecosystem that becomes too big to ignore.

The digitization of identity has made a complex subject even more so. In many senses, it is very personal and dynamic, full of complexities that we negotiate and reveal through constantly shifting online structures and environments. But our identity also manifests in rigid, formal credentials issued and controlled by the state. Where and how these two models intersect—and we believe they increasingly will—is a compelling area to study, as it represents privatization of one of the most fundamental state services. And it is the very fundamental nature of identity—not only as the irreducible credential for enabling user access to services, but also as the identifier for activity that gets monetized through the billions of dollars of the digital advertising industry—that has private firms so intent on increasing the scope of their role.

Advancements in biometrics, encryption, and distributed computing are leading to sophisticated technology solutions and new business models for managing digital identity. But again we must emphasize that while the technology is easy to focus on, the "analog complements"[116] in this sector—the regulatory environments, political structures, cultural attitudes, and more—are just as critical for success, especially given their diversity across different markets. This landscape may favor not the most technologically advanced firms, but those with the best understanding of new and emerging use cases in a specific region, and creativity in developing commercial models to serve them.

116 "World Development Report, 2016 Internet for Development." (World Bank, 2016).

Bibliography

Bibliography

"A Buyers Guide to Stolen Data on the Deep Web." *Dark Web Reviews*. Accessed July 9, 2016. http://darkwebreviews.com/a-buyers-guide-to-stolen-data-on-the-deep-web-darkmatters/3615/.

"Aadhaar Enabled E-KYC Can Save Rs 10,000 Cr over next 5 Yrs." *Business Standard*. Accessed July 10, 2016. http://www.business-standard.com/article/economy-policy/aadhaar-enabled-e-kyc-can-save-rs-10-000-cr-over-next-5-yrs-survey-116031800760_1.html.

"About India Stack." *India Stack*. Accessed May 19, 2016. http://www.indiastack.org/About-India-Stack.

"About NSTIC." NSTIC. Accessed May 19, 2016. http://www.nist.gov/nstic/about-nstic.html.

Ali, Muneeb. "Fixing Flaws in the Original Design of the Internet: Trust-to-Trust Principle — Blockstack Blog." *Medium*, March 15, 2016. https://blog.blockstack.org/next-steps-towards-a-secure-internet-a057217acebb#.quf0hukok.

"Americans' Confidence in Banks Still Languishing Below 30 percent." *Gallup*. Accessed July 13, 2016. http://www.gallup.com/poll/192719/americans-confidence-banks-languishing-below.aspx.

Angwin, Julia. "AT&T Helped U.S. Spy on Internet on a Vast Scale." *The New York Times*, August 15, 2015. http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-Internet-traffic.html?_r=1.

Angwin, Julia, Jeff Larsen, Surya Mattu, and Lauren Kirchener. "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks." *ProPublica*, May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-incriminal-sentencing.

"Areas of Use – *BankID*." BankID. Accessed July 13, 2016. https://www.bankid.no/en/company/areas-of-use/.

Birch, David. *Identity Is the New Money*. London Publishing Partnership, 2014.

Buckingham, David. "Introducing Identity." *In Youth, Identity, and Digital Media*. MIT Press, 2008.

Burgess, Matt. "UK's Porn Age Checks Set 'Dangerous' Precedent." *Wired UK*, February 16, 2016. http://www.wired.co.uk/news/archive/2016-02/16/porn-uk-age-check.

"Catalyzing the Marketplace: *NSTIC* Pilot Program." NSTIC. Accessed July 9, 2016. http://www.nist.gov/nstic/pilots.html.

Chinonso, Tony. "BVN Registration: As with Telecom Operators, Would so Be for the Banks?" *Vanguard News*, October 28, 2015. http://www.vanguardngr.com/2015/10/bvn-registration-as-with-telecom-operators-would-so-be-for-the-banks/.

"Company Info." *Facebook*. Accessed May 19, 2016. http://newsroom.fb.com/company-info/.

"Confirm Your Identity with an ID." *Facebook*. Accessed May 19, 2016. https://www.facebook.com/help/contact/319547548123767.

"Counter-Terrorism Tools Used to Spot Fraud." *Palantir*. Accessed May 19, 2016. https://palantir.com/pt_media/counter-terrorism-tools-used-to-spot-fraud/.

"Countries List." *Financial Action Task Force (FATF)*. Accessed May 19, 2016. http://www.fatf-gafi.org/countries/#FATF.

Court, Alex. "Branding Nigeria: MasterCard-Backed I.D. Is Also a Debit Card and a Passport." *CNN*, September 25, 2014. http://edition.cnn.com/2014/09/25/business/branding-nigeria-mastercard-backed-i-d-/.

"Digital ID & Authentication Council of Canada." *DIACC*. Accessed May 19, 2016. https://diacc.ca/.

"Directive on Payment Services (PSD) – European Commission." European Commission. Accessed May 19, 2016. http://ec.europa.eu/finance/payments/framework/index_en.htm.

"Dutch Interbank Digital Identity Service Announced." *Innopay*. Accessed July 13, 2016. https://www.innopay.com/blog/dutch-interbank-digital-identity-service-announced/.

Eaton, Ben, Hanne Kristine Hallingby, Per-Jonny Nesse, and Ole Hanseth. "Achieving Payoffs from an Industry Cloud Ecosystem at BankID." *MISQ Executive 13*, no. 4 (2014). http://misqe.org/ojs2/index.php/misqe/article/view/550.

Ejiofor, Clement. "We Don't Want Your ID Card: Nigerians Furious Over MasterCard Logo." *Naij.com*, August 29, 2014. https://www.naij.com/282606-dont-want-id-card-nigerians-furious-mastercards-logo.html.

Bibliography
continued

Ekott, Ini. "SCANDALOUS: Outrage in Nigeria as Government Brands National ID Card with MasterCard's Logo – Premium Times Nigeria." *Premium Times Nigeria*, August 29, 2014. http://www.premiumtimesng.com/news/headlines/167479-scandalous-outrage-in-nigeria-as-government-brands-national-id-card-with-mastercards-logo.html.

"Ensuring Trust." *Mydex*. Accessed May 19, 2016. https://mydex.org/about/ensuring-trust/.

"EUR-Lex – 32015R1501." *EUR-Lex*. Accessed May 21, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL_2015_235_R_0001.

Evans, David S. "How Catalysts Ignite: The Economics of Platform-Based Start-Ups." *In Platforms, Markets and Innovation*, 2009.

"FIDO Alliance." *FIDO Alliance*. Accessed May 19, 2016. https://fidoalliance.org/.

Gelb, Alan, and Anna Diofasi. "Scoping Paper on Identification and Development." Center for Global Development, 2016.

Goffman, Erving. *The Presentation of Self in Everyday Life. Harmondsworth*, 1978.

"Government ID Solutions to Facilitate and Secure Identity Management." *Morpho*, February 10, 2015. http://www.morpho.com/en/government-id-solutions-facilitate-and-secure-identity-management.

Grönlund, Åke. "Electronic Identity Management in Sweden: Governance of a Market Approach." *Identity in the Information Society 3*, no. 1 (July 2010): 195–211. doi:10.1007/s12394-010-0043-1.

GSMA, Intelligence. "GSMA Intelligence." Accessed May 19, 2016. https://www.gsmaintelligence.com/.

"GSMA's Mobile Connect Available to 2 Billion Consumers Globally." *Personal Data*, February 22, 2016. http://www.gsma.com/personaldata/gsmas-mobile-connect-available-to-2-billion-consumers-globally.

"GTRI NSTIC Trustmark Pilot | Sponsored by the National Institute of Standards and Technology." *GTRI*. Accessed May 19, 2016. https://trustmark.gtri.gatech.edu/.

"ID2020 Annual Summit." *ID2020*. Accessed May 19, 2016. http://id2020.org/.

"ID2020 Design Workshop." *Web of Trust*. Accessed May 19, 2016. http://www.weboftrust.info/.

"IDEF Core Documents." *IDESG*. Accessed May 19, 2016. http://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents.

"Identification for Development (ID4D) Integration Approach." World Bank, 2015. http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/09/21/090224b0830efe0f/2_0/Rendered/PDF/Identification0ation0approach0study.pdf.

"Identity and Access Management Platform from ForgeRock." *ForgeRock.com*, April 14, 2015. https://www.forgerock.com/platform/.

"Identity Assurance Goes to Washington." *GOV.UK*. Accessed May 19, 2016. https://gds.blog.gov.uk/2012/05/29/identity-assurance-goes-to-washington/.

"Indian Bank Launches WhatsApp, Facebook, Twitter Mobile Payment." *Banking Technology*. Accessed July 14, 2016. http://www.bankingtech.com/297431/axis-bank-india-launches-whatsapp-facebook-twitter-mobile-payments/.

"InterPlanetary File System." *Wikipedia*, July 7, 2016. https://en.wikipedia.org/w/index.php?title=InterPlanetary_File_System&oldid=728691175.

Jacobides, Michael G., Thorbjørn Knudsen, and Mie Augier. "Benefiting from Innovation: Value Creation, Value Appropriation and the Role of Industry Architectures." *Research Policy* 35, no. 8 (October 2006): 1200–1221. doi:10.1016/j.respol.2006.09.005.

Karantzis, John. "Uploading Document Copies Is Not KYC." *LinkedIn Pulse*, September 14, 2015. https://www.linkedin.com/pulse/uploading-document-copies-kyc-john-karantzis.

Kotka, Taavi, Carlos del Castillo, and Kaspar Korjus. "Estonian E-Residency: Redefining the Nation-State in the Digital Era," September 2015. http://www.politics.ox.ac.uk/materials/centres/cyber-studies/Working_Paper_No.3_Kotka_Vargas_Korjus.pdf.

Bibliography
continued

Kubicek, Herbert, and Torsten Noack. "Different Countries-Different Paths Extended Comparison of the Introduction of eIDs in Eight European Countries." *Identity in the Information Society* 3, no. 1 (July 2010): 235–45. doi:10.1007/s12394-010-0063-x.

Levine, Dan. "Apple Could Use Brooklyn Case to Pursue Details about FBI iPhone Hack: Source." *Reuters*, March 30, 2016. http://www.reuters.com/article/us-apple-encryption-idUSKCN0WU1RF.

Lomas, Natasha. "Shine Signs First European Carriers To Its Network-Level Ad Blocking Tech." *TechCrunch*, February 18, 2016. http://techcrunch.com/2016/02/18/shine-bags-first-european-carrier-as-three-uk-deploys-network-level-ad-blocking/.

"MasterCard to Expand Digital Aid Distribution Services." *MasterCard*. Accessed July 13, 2016. http://newsroom.mastercard.com/press-releases/mastercard-to-expand-digital-aid-distribution-services/.

Mender, Bedeho. "Why Your Ethereum Project Will Most Likely Fail," March 9, 2016. https://medium.com/@bedeho/why-your-ethereum-project-will-most-likely-fail-d14b6d8f1c7c#.k4fhexhcm.

"Microsoft Runs Pilot on Linking Skype and Aadhar." *The Times of India*, February 19, 2016. http://timesofindia.indiatimes.com/tech/tech-news/Microsoft-runs-pilot-on-linking-Skype-and-Aadhar/articleshow/51055959.cms.

"Millennials + Money: The Unfiltered Journey." *Facebook*, January 2016. https://fbinsights.files.wordpress.com/2016/01/facebookiq_millennials_money_january2016.pdf.

"Mobile Connect Consumer Research Report: European Union." *GSMA*, October 14, 2015. http://www.gsma.com/personaldata/mobile-connect-consumer-research-report-european-union.

"Mobile Connect Consumer Research Report: United States." *GSMA*, October 14, 2015. http://www.gsma.com/personaldata/mobile-connect-consumer-research-report-united-states.

"Mobile Connect Developer Portal." *Mobile Connect*. Accessed May 19, 2016. https://developer.mobileconnect.io/content/overview.

"Mobile Signature in Turkey – A Case Study of Turkcell: MobilImza." *GSMA*, July 3, 2013. http://www.gsma.com/mea/mobile-signature-in-turkey-a-case-study-of-turkcell-mobilimza.

Nandan, Nilekani. "Basis of a Revolution." *The Indian Express*, March 9, 2016. http://indianexpress.com/article/opinion/columns/aadhaar-bill-lpg-subsidy-mgnrega-paperless-govt-basis-of-a-revolution/.

"New Certified Companies Now Connected to GOV.UK Verify." *GOV.UK Verify*. Accessed July 10, 2016. https://identityassurance.blog.gov.uk/2016/04/06/new-certified-companies-now-connected-to-gov-uk-verify/.

"OAuth Info Page." *IETF*. Accessed May 19, 2016. https://www.ietf.org/mailman/listinfo/oauth.

"OIXnet." *OIXnet*. Accessed May 19, 2016. http://oixnet.org/.

Okuttah, Mark. "CEOs of Telcos Face Arrest over Sim Card Crimes," October 7, 2013. http://www.businessdailyafrica.com/CEOs-face-arrest-for-Sim-card-crime/-/539546/2023132/-/cjtbdt/-/index.html.

"OpenID Foundation." *OpenID Foundation*. Accessed May 19, 2016. https://openid.net/foundation/.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015.

"R3." *R3CEV*. Accessed July 13, 2016. http://r3cev.com/.

"Remote SIM Provisioning for M2M." *GSMA*, March 28, 2012. http://www.gsma.com/connectedliving/embedded-sim/.

Reporter, B. S. "RBI Fines Three Govt-Run Banks for Violating KYC Norms." Accessed July 10, 2016. http://www.business-standard.com/article/finance/rbi-fines-three-govt-run-banks-for-violating-kyc-norms-115043000029_1.html.

"Respect Network." *Respect Network*. Accessed May 19, 2016. https://www.respectnetwork.com/.

Rissanen, Teemu. "Electronic Identity in Finland: ID Cards vs. Bank IDs." *Identity in the Information Society* 3, no. 1 (July 2010): 175–94. doi:10.1007/s12394-010-0049-8.

Bibliography
continued

Rochet, Jean-Charles, and Jean Tirole. "Platform Competition in Two-Sided Markets." *Journal of the European Economic Association*, 2003.

Rose, John, Olaf Rehse, and Björn Röber. "The Value of Our Digital Identity." *BCG Perspectives*, November 20, 2012. https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/.

Sachs, Eric. "The Hack That Makes Internet Identity Possible." Accessed July 9, 2016. https://docs.google.com/document/pub?id=1O7jyQLb7dW6EnJrFsWZDyh0Yq0aFJU5UJ4i5QzYlTjU#h.i2ivn11phwa5.

"SAML Wiki." *OASIS*. Accessed May 19, 2016. https://wiki.oasis-open.org/security/FrontPage.

Scott, James C. *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale University Press, 1998.

Sen, Anirban. "Budget 2016: Nandan Nilekani Lauds Decision to Give Aadhaar Statutory Backing." *The Economic Times*, February 29, 2016. http://economictimes.indiatimes.com/news/economy/policy/budget-2016-nandan-nilekani-lauds-decision-to-give-aadhaar-statutory-backing/articleshow/51195080.cms.

"Shine Technologies." *Shine Technologies*. Accessed May 19, 2016. https://www.getshine.com.

Shulist, Janet. "What Is the Availability of Mobile Money Services in 2015?" *GSMA Mobile for Development*, March 21, 2016. http://www.gsma.com/mobilefordevelopment/programme/mobile-money/what-is-the-availability-of-mobile-money-services-in-2015.

Stewart, Heather. "Facebook Paid £4,327 Corporation Tax despite £35m Staff Bonuses." *The Guardian*, October 11, 2015. http://www.theguardian.com/global/2015/oct/11/facebook-paid-4327-corporation-tax-despite-35-million-staff-bonuses.

"Sweden Interested in Estonia's X-Road Platform." *The Baltic Course*. Accessed May 19, 2016. http://www.baltic-course.com/eng/good_for_business/?doc=114572.

"Taavi Kotka Promises 10 Million „e-Estonians" by 2025!" *E-Estonia*. Accessed May 19, 2016. http://e-estonia.com/taavi-kotka-promises-10-million-e-estonians-2025/.

"Telecommunications Industry Dialogue." *Telecommunications Industry Dialogue*. Accessed May 19, 2016. http://www.telecomindustrydialogue.org/.

"The Canadian Experience." *SecureKey*. Accessed July 10, 2016. http://www.skconcierge.us/the-canadian-experience/.

The Financial Conduct Authority. "FCA Fines Barclays £72 Million for Poor Handling of Financial Crime Risks – Financial Conduct Authority." Accessed July 10, 2016. https://www.fca.org.uk/news/fca-fines-barclays-72-million-for-poor-handling-of-financial-crime-risks.

———. "Standard Bank PLC Fined £7.6m for Failures in Its Anti-Money Laundering Controls – Financial Conduct Authority." Accessed July 10, 2016. https://fca.org.uk/news/standard-bank-plc-fined-for-failures-in-its-antimoney-laundering-controls.

"The Future of Digital Identity Is Up to Banks." *American Banker*. Accessed July 10, 2016. http://www.americanbanker.com/news/bank-technology/the-future-of-digital-identity-is-up-to-banks-1079943-1.html.

"The Millennial Disruption Index." *Viacom*. Accessed July 13, 2016. http://www.millennialdisruptionindex.com/.

"The Power of Identity in Retail Banking." *ForgeRock*. Accessed July 10, 2016. https://www.forgerock.com/app/uploads/2015/10/ForgeRock-Retail-Banking-USA.pdf.

"The Windhover Principles." *ID3*. Accessed May 19, 2016. https://idcubed.org/home_page_feature/windhover-principles-digital-identity-trust-data/.

Thompson, Cadie. "Facebook: About 83 Million Accounts Are Fake." *CNBC*, August 2, 2012. http://www.cnbc.com/id/48468956.

"Triad Case Study." *Triad*. Accessed May 19, 2016. http://consulting.triad.co.uk/cs-gsma1.html.

"Trust Services and eID – Digital Single Market." *European Commission*. Accessed May 19, 2016. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid.

"UK Open Banking Working Group Publishes Report Setting out Open Banking Standard | News." *Open Data Institute*, August 2, 2016. https://theodi.org/news/uk-open-banking-working-group-publishes-report.

Bibliography
continued

Vasagar, Jeevan. "Singapore Banks Eye Facebook IDs for Transfers." *Financial Times*, July 3, 2016. http://www.ft.com/cms/s/0/b2dd2cd8-3f39-11e6-8716-a4a71e8140b0.html.

"WC3 Credentials Community Group." *WC3*. Accessed May 19, 2016. https://www.w3.org/community/credentials/.

West, Joel. "How Open Is Open Enough?: Melding Proprietary and Open-Source Platform Strategies." *Research Policy* 32 (2003): 1259–1285.

Williams-Grut, Oscar. "Estonia Wants to Become a 'Country as a Service' and Already Has 10,000 Virtual Residents." *Business Insider*. Accessed May 19, 2016. http://uk.businessinsider.com/interview-with-estonia-cio-taavi-kotka-2016-4.

Woodcock, Chris. "Five Years On, Apple's Battle to Kill the SIM Card Is Nearly over." *The Memo*, July 30, 2015. http://www.thememo.com/2015/07/30/five-years-on-apples-battle-to-kill-the-sim-card-is-nearly-over/.

"World Development Report, 2016 Internet for Development." *World Bank*, 2016.

"X-Road Between Finland and Estonia." *E-Estonia*. Accessed May 19, 2016. https://e-estonia.com/x-road-between-finland-and-estonia/.

Appendix 1
Company profiles

Company profiles

To provide a deeper level of insight to our analysis, we interviewed executives at a wide range of digital identity firms, as well as a small number of additional interviews with non-affiliated industry experts. The list of firms to interview was generated from our existing networks, standard Internet searches, and the "snowball" method of asking each participant for additional suggestions. Firms that did not respond to our requests were excluded; the exception is that we feature a summary of Facebook Connect, despite not being able to interview the right person at the firm. The interviews were semi-structured, and included basic questions around the business model, key product(s), customers, and the regulatory environment. All interviews were conducted between December 2015 and April 2016.

Profiled firms/organizations

- Blockstack Labs
- Consent
- Evernym
- Experian
- Facebook*
- ID³/Open Mustard Seed
- iSignthis
- miiCard
- ShoCard
- Trulioo
- Yoti

* Profile is based on secondary sources

Appendix 1: Company profiles

Blockstack Labs

- Blockstack.com
- Type: Identity provider
- Markets: International
- Based: New York City
- <10 employees

Interview

Muneeb Ali (co-founder)

Summary

Blockstack is a global Internet database, where individuals can register unique human-readable names and associate other data with these names. The technology has specific identity use cases (e.g., around identity verification), but the company's goal is broader than just personal identity, in that it wants to develop a new set of standard protocols that embed trust and security mechanisms within the infrastructure itself. In this sense, identity solutions are a key application enabled by its architecture, but not the only one.

The technology was initially launched as a Web application, called Onename, which acted as a name service for Bitcoin. Over the years, the team has focused on the underlying open-source technology (Blockstack), and worked on building the base infrastructure using distributed ledgers.

Business model

Blockstack Labs is making its technology open-source, probably a prerequisite for this type of new infrastructure layer. The company is taking a very long view insofar as a revenue model; it claims it has patient investors who support this long-term play, and there is no pressure for near-term revenues. If it is able to gain traction with its system, revenue would likely come from typical open-source software approaches, such as providing value-added services on top of the base infrastructure.

Technology

In early 2016, Blockstack Labs released a command-line interface (CLI) for the Blockstack service. Blockstack's global database enables a decentralized, open alternative to the ICANN DNS system, allowing users to create namespaces with the ".id" top-level domain. Compared to centralized ICANN, the Blockstack system is not dependent on any single authority for approval of registration, and its decentralized, network-based approval and record-keeping makes for more robust security features.

Like other infrastructure plays, Blockstack Labs is basing much of its architecture on distributed ledger technology. Unlike other efforts, the Blockstack approach is decoupled from the blockchain integration layer, allowing it to be essentially ported from one blockchain to another; while it currently uses the Bitcoin blockchain, it could move to a different one if necessary. In order to avoid the limitations of working directly with the Bitcoin blockchain (e.g., storage limitations, slow write speed, limited bandwidth) it creates a virtual blockchain and data layer that handle data routing and storage. It relies on the underlying blockchain to achieve consensus and announce state changes for immutable records.

Data

Blockstack supports two categories of data, immutable data and mutable data. Immutable data is attested to by the blockchain and requires new blockchain transactions for any updates. Mutuable data is signed by public keys associated with a name and allows for fast updating of the data. The immutable data is hashed and stored on distributed hash tables (DHTs), but the mutable data is encrypted and stored in standard open-source cloud data stores. Only the individual with the appropriate private key can write to their blockchain-based identity profile. For the .id namespace, the personal identity data might include basic details such as name, date of birth, etc., and secondary data, which might include third-party attestations/verifications or other types of credentials.

Appendix 1: Company profiles
continued

Consent

- **Consent.global**
- **Type: Decentralized identity platform**
- **Markets: South Africa**
- **Based: Registered in U.K., operating from Cape Town, South Africa**
- **<10 employees**

Interview
Shaun Conway, founder

Summary
Consent is a start-up building an open system for registering and verifying digital identities in Africa. It is using mobile and distributed computing technologies to enable individuals to register a digital identity on a blockchain, and have core identity credentials that are derived from attribute data to be verified by trusted third-parties, creating a set of immutable records controlled by the individual. Consent is launching a proof-of-concept project with Barclay's Africa in South Africa in 2016.

Consent is addressing the need for KYC-compliant digital identity verification in South Africa, where unique KYC regulations pose an expensive challenge to banks and other financial institutions, and result in the exclusion of those unable to present the required credentials to open a bank account. Through its partnership with Barclays, Consent aims to enable millions of Barclays customers to digitally register and verify their identity without having to visit a branch to satisfy KYC process requirements. As part of this effort, Consent is also working with South African policymakers in order to update regulations to more explicitly allow novel digital verification processes, including attestation of attributes by other individuals, to better accommodate thin-file clients such as children.

Business model
The Consent identity system is open-source, and is working to align itself internationally with emerging open standards and mechanisms that allow individuals to own and control their digital identities and personal data, independent of any central organization. The platform includes proprietary software that enables third-party service providers to offer value-added services, generating revenues through an innovative business model that returns a percentage of the value of each transaction back to the individual. It also allows for further innovations to be added to the platform as micro-services, e.g., a decentralized autonomous organization for personal risk insurance.

Technology
Similar to other firms, Consent is looking to use distributed computing for the foundation of its identity system. It expects to use the Ethereum blockchain as well as IPFS (interplanetary file system) peer-to-peer distributed files to record identities in a decentralized, user-controlled system. To meet its goal of enabling alternative sources for attestations or verification of attributes, the Consent system allows individuals to attest to attributes of others (e.g., community leader or doctor attesting that a child belongs to a parent), relying on the trust profile of each node in the network to establish varying levels of confidence in attestations as well as identify fraud. According to Conway, "We believe the quality and predictive power of these digital credentials perform better than analog procedures based on a piece of paper."

Data
The Consent system is designed to provide a decentralized personal data store for each registered user, where the individual can store and manage his own identity profile information, including attestations and credentials. In the long-term, Consent hopes that individual control over personal data and identity profiles can shift the standard economic models around data harvesting and advertising, leading to new forms of granular data sharing and client-led relationships.

Customers
Consent is currently working with Barclays Bank in South Africa, and is also testing versions of the platform with government social programs around youth in South Africa.

Appendix 1: Company profiles
continued

Evernym

- Evernym.us
- Type: Decentralized identity platform
- Markets: Under development
- Based: Salt Lake City, Utah
- 15 employees

Interview
Timothy Ruff, co-founder and CEO

Summary
Evernym is a small start-up building an open-source, self-sovereign identity network based on a public permissioned distributed ledger. The system will allow individuals, organizations, or other entities to create an identity and then add credentials to it over time, and also includes a robust messaging service that offers a secure communication channel with the individual. It is developing and licensing its platform as an open-source project, and then building separate, proprietary applications that utilize the platform. Evernym is just coming out of stealth mode, and has tentative agreements with a number of financial and education institutions.

Business model
Evernym's open-source platform for identity services, called Sovrin, will be freely available under an Apache license. It is building its proprietary applications to run on top of the Sovrin platform, including its Evernym application, which will be the revenue-generator. The company says that other identity services, including direct competitors, will also be able to build on the Sovrin platform, and users will be able to switch from one identity provider to the other (because their immutable data is recorded within the core Sovrin platform). The revenue model is transaction-based, with the expectation that payments (e.g., P2P) and messaging will be the primary types of transactions.

Technology
The Sovrin network is based on a custom, public-permissioned distributed ledger using Plenum, a customized implementation of the Redundant Byzantine Fault Tolerant (RBFT) distributed consensus algorithm.[117] Privacy-preserving protocols, including zero-knowledge proofs, are used to mitigate correlation risk. Its operational layer is based on the Respect Networks trust framework,[118] which is an open-source initiative for codifying how different actors in the ecosystem can engage in trusted transactions. The framework is being implemented via the XDI protocol for semantic data interchange,[119] which supports cross-platform data integration challenges.

Data
To support the self-sovereign nature of the platform, the individual's data will be recorded by the core Sovrin platform, with the actual data stored wherever the user prefers (e.g., personal or public cloud). This means that the individual will maintain full control and enjoy data portability outside of the Evernym applications.

Customers
Evernym has tentative agreements with financial institutions and organizations within the education sector.

117 RBFT refers to the way in which all nodes in the system come to agreement on the data; see Evernym's white paper for full explanation: http://www.evernym.com/assets/doc/Identity-System-Essentials.pdf.

118 https://www.respectnetwork.com/.

119 For a primer on XDI, see http://security-architect.blogspot.com/2013/09/personal-clouds-why-xdi.html.

Appendix 1: Company profiles
continued

Experian

- www.experian.com/business-services/fraud-management.html
- Type: Identity verification provider
- Markets: International
- Based: Dublin, Ireland (operations in 37 countries)
- 17,000 employees

Interview
Kolin Whitley, Experian Fraud and Identity Solutions senior director of product management

Summary
Experian is a global information services company with a long-running fraud and identity business, with numerous related products and services for authentication and fraud detection. These services typically use static personal information compiled from multiple sources, and are complemented by Experian's consumer database of more than 220 million people. As the traditional "best practice" for online identity verification, the Experian model is explicitly embedded in much regulation around KYC/AML. However, the rise of data breaches of PII and new regulation in the EU may be forcing a movement away from the static verification approach toward more dynamic or multi-factor approaches.

Business model
Experian's fraud and identity business is a B2B business, bundling its core identity and fraud services into a range of products for different use cases, including credit card verification, employee application verification, and supplier verification. Experian also has some consumer-facing products around managing credit history and identity theft protection.

Technology
The Experian fraud and identity business relies primarily on its extensive consumer databases for its verification services. But in a move toward diversifying its approach, Experian acquired the firm 41st Parameter in 2013 for $324 million. From that acquisition Experian has a solution that can collect basic info from a device being used by the consumer, and thereby bind device identifiers to the PII that is also collected. This allows Experian to track users across different devices, creating a more comprehensive profile of data and behavior that allows Experian to more readily identify suspicious activity.

Data
Experian maintains PII and credit data on 220 million consumers, primarily in the United States, and that data has to remain in the U.S., which limits its application for international verification.

Customers
Experian customers include a wide range of financial institutions and other Fortune 500 companies.

Appendix 1: Company profiles
continued

Facebook

- Facebook.com
- Type: Identity provider
- Markets: International
- Based: Menlo Park, California
- 13,000 employees

Summary

With 1.59 billion users, 84 percent of which are outside of North America, Facebook is the largest technology platform by user base.[120] But you also have to consider the user populations of its other properties—WhatsApp (1 billion), Facebook Messenger (800 million) and Instagram (400 million)—to appreciate the company's massive scale.[121]

Business model

As an advertising company, Facebook's interest in its users' identities is a function of how that personal information can be analyzed and correlated in ways that increase the value of the ads it shows. This is especially important in the industrialized economies, where user growth has plateaued and Facebook is dependent on increasingly sophisticated targeting technology to sustain revenue growth.

While creating a Facebook account typically does not require anything more than a valid email address, the company does require users register with "the name you use in real life." Amid some controversy, in 2012 Facebook started reinforcing this "real name" policy after revealing almost 9 percent of its profiles were fake. A spokesperson said "Authentic identity is important to the Facebook experience, and our goal is that every account on Facebook should represent a real person."[122] For Facebook, minimizing fake accounts is likely part of its broader efforts to maintain a low level of harassment or other online behaviors it considers negative to the user experience. This calculation that "real" identity leads to better behavior, and thus increases trust within the network, is a strong belief among the social platforms. AirBnB changed its policies for this purpose, requiring some users to verify with both an offline credential (e.g., passport) and connect with their online account at either Facebook, LinkedIn, or Google; unsurprisingly, the move has met with some backlash.[123]

Technology

Facebook is the largest IDP globally, with almost four times as many relying party Web sites as the next largest, Twitter.[124] Its Facebook Connect product was launched in 2008, and extended to mobile apps in 2010, allowing hundreds of millions of users to use their Facebook credentials to create accounts and authenticate (log in) with third-party Web sites and apps. Facebook bases its service on Oauth2, but built a proprietary layer to allow richer, two-way data sharing with the relying party. The data that Facebook can share is broken down into over 40 different permissions; the default, "public profile," includes the individual's first and last name, age, gender, locale, picture, and more. Other data that can be shared if the user consents include friends, posts, pictures, tagged locations, and so on.[125] Similar to a few other IDPs, Facebook also allows the relying party to write information back onto the user's profile on Facebook, typically in the form of posts, photos, and check-ins. With Facebook, the user is presented with the details of what data the relying party would like to read from their account, and what data, if any, the relying party would like to write (post) to their account, but the way in which this is communicated to users leads to confusion, and is probably optimized for developers.[126]

120 1.59 billion monthly active users; http://newsroom.fb.com/company-info/.

121 Obviously, there is much overlap between services, as end-users multi-home between many of these platforms.

122 Facebook: About 83 Million Accounts Are Fake.

123 http://blogs.harvard.edu/doc/2013/05/28/lets-help-airbnb-rebuild-the-bridge-it-just-burned/.

124 Anna Vapen, Niklas Carlsson, A. Mahanti and Nahid Shahmehri, Third-party identity management usage on the web, 2014, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 151-162. http://dx.doi.org/10.1007/978-3-319-04918-2_15.

125 https://developers.facebook.com/docs/facebook-login/permissions#reference-public_profile.

126 Robinson, Nicky, and Joseph Bonneau. "Cognitive Disconnect: Understanding Facebook Connect Login Permissions WORKING DRAFT," n.d.

Appendix 1: Company profiles
continued

ID³ Open Mustard Seed

- **https://idcubed.org/open-platform/platform/**
- **Type: Decentralized identity platform**
- **Markets: Under development**
- **Based: Cambridge, Massachusetts**

Interview
John Clippinger, Ph.D.

Summary
ID³'s Open Mustard Seed initiative sets forth an ambitious vision for a new model of digital infrastructure, prioritizing open-source, decentralized, trusted, and user-centric principles in its design. The OMS framework relies on emerging technology—including distributed ledgers, hardware-based biometrics, and self-executing contracts—to provide new ways of creating and managing personal identities, transactions, and data that are not reliant on central institutions, including the state.

Business model
As a non-profit, ID³ requires funding for the development and promotion of the OMS framework, but does not have explicit commercial goals, and is not a direct provider of paid services. The design of OMS does, however, support a wide range of third-party services to participate within the framework with identity and data management services.

While its code is not being used directly, OMS has inspired and serves as a reference for a number of start-ups, including Cambridge Blockchain, Intrinsic, Hub Culture, and Consent (South Africa). ID³ is exploring new use cases for the next version of OMS, including as a platform for individuals to verify employment credentials, whereby independent contractors could attest to specific status requirements and thereby remove burden-of-proof requirements from potential employers.

Technology
The OMS framework aims to establish a new Internet technology layer that builds in security, trust, and decentralized user control into the architecture of the system. It primarily relies on a distributed ledger model and smartphone technology to enable secure and trusted identity management, transactions, and data sharing. For example, individuals can create personal identities, digitally encrypt and sign them using a mobile-based private key, and record them on the blockchain, where third-party services can verify or authenticate specific credentials. Users can create multiple "personas" (e.g., professional, family) which are linked back to their "core" identity, enabling easy and granular sharing policies for interacting with other individuals or companies. Providing users with this level of control over their data would up-end the current digital advertising model, perhaps ushering in new revenue models where users can sell or rent access to their data to marketers directly.

In principle, the OMS approach to individually controlled identity could substitute for state-based identity registration—instead of merely basing the digital identity on state documents, a completely probabilistic approach using algorithms could instead be used to establish an individual's identity, thereby bypassing the state and creating the possibility of completely sovereign individual identities, where citizenship or residency are merely credentials attached to that identity. The second version of OMS code is currently under development.

Appendix 1: Company profiles
continued

iSignthis

- iSignthis.com
- Type: Identity verification provider
- Markets: International
- Based: Melbourne, Australia
- Australian Securities Exchange (ASX) Code ISX
- Founded 2013

Interview
John Karantzis, CEO

Summary
iSignthis originally launched to help businesses combat online credit card fraud. It has patented a method for identity proofing via dynamic identity verification using electronic payments, similar to PayPal. Its focus is on high-value, high-volume, high-risk transactions, including online gambling, remittances, foreign-exchange, and securities trading. iSignthis is focused on meeting the requirements of multiple international regulations via a single unified solution, and feels that it is ahead of the curve for emerging KYC and AML requirements for dynamic verification. According to Karantzis, "We're a legal service embedded in software, rather than a technology company trying to comply with regulations it doesn't fully understand."

Business model
iSignthis operates as an electronic identity verification provider. Its customers are online service providers that need to verify users in a KYC/AML-compliant process. For example, its service allows a user located in China to open a bank account in the United States without leaving their home (in this case, the iSignthis customer would be the U.S. bank). iSignthis also offers its service for uses cases that do not require customer due diligence, but its core business is higher level of assurance, KYC/AML verification.

It charges customers on a per transaction basis, approximately AUD$15 /US$10 for an initial verification of a new user, and US$0.25 per subsequent processing and transaction monitoring of that user. This is much less than physical verification, which iSignthis estimates to cost between US$50 and $75 per initial verification.

Technology
iSignthis has registered more than 20 patents for its dynamic verification process ("Paydentity") using electronic funds transfer to verify the end-user's access to an existing bank account. In this way, it is similar to how PayPal verifies new users from a customer experience perspective and adopts similar legal reasoning to meet regulatory requirements. In the PayPal model, a new user will sign up for the service, at which point PayPal will make two random deposits of very small dollar amounts—say, $0.07 and $0.12—into the user's bank account. Once the deposits show on their bank statement, the user then reports back to PayPal the value of the two deposits. With the iSignthis model, when a new user tries to sign up for the service, and either make a purchase or deposit, iSignthis will take that amount and break it into two random amounts. For example, if the user tried to transfer $100 into a new online gambling service, iSignthis will break that up that $100 into two random amounts, say, $35 and $65, which will show up immediately as being debited from the user's existing account. If the user truly has access to that source account they will be able to see the two random debit amounts and report those back to the company, completing the verification.Because the approach relies on the debiting of funds instead of the deposit of funds, it happens much more quickly compared to PayPal.

Enhancing the verification, the process can also require that customers enter a password which iSignthis sends to their mobile device. Customers are screened for names on sanctions lists and politically exposed persons (PEP) lists. A significant amount of metadata, including geolocation and IP address, is also reviewed to identify transfers involving politically sensitive jurisdictions. The iSignthis solution is not designed for "thin-file" or unbanked end-users—it only works with those users who have an existing bank account.

Appendix 1: Company profiles
continued

miiCard

- miiCard.com
- Type: Identity provider
- Markets: United Kingdom
- Based: Edinburgh, UK
- <10 employees

Interview
James Varga, CEO

Summary
miiCard is a complete digital identity platform, with both a consumer product that allows end-users to create a miiCard "passport," and a business product that allows commercial customers to verify users electronically. They have split off the B2B bank verification side of the business as a stand-alone product, Direct ID, which is sold primarily to service providers in online lending and other consumer finance sectors.

Business model
The miiCard model is based on online bank account verification and certified bank statement data, which the company feels is the single best source for trusted verification available wholly online. The end-user trying to access a service provider is directed to either miiCard or DirectID, where they input their bank account information and verify themselves by logging into their online bank through the platform. In addition to proving they have access, the user also grants access to their most recent bank statement, typically three months' worth but now up to 12 months, depending on the bank. This additional transaction information is very valuable for not only verifying the user, but also for value-added services that miiCard can facilitate, such as understanding the credit risk. This type of information sharing is permitted under the EU's PSD2 regulation.

miiCard is building a two-sided market, but is prioritizing the commercial verification side. As Varga said, "The idea of having a personal data store provides the consumer with control, but the verification we do on the commercial side drives the convenience for both consumers and businesses." The top sectors on the commercial side are consumer finance/financial services, where miiCard's understanding of the end-user—not only the high level of confidence KYC verification, but also months of transaction history—have great value; for example, to a potential lender for a home or auto loan. A second sector is in health care, where strong privacy regulations create the need for deep trusted relationships.

Technology
miiCard's platform does not just store data on the mobile, because it feels that mobile devices are not secure enough, and have issues with loss and theft. Instead, the data is stored on miiCard's cloud, using Microsoft's Azure infrastructure.

Data
The PII is stored, individually encrypted, on miiCard's own private servers. This includes the user's bank account transaction records (but not the log-in credentials—miiCard never sees those). The bank account transaction records are only pulled one time, upon initial registration. But miiCard verifies access to the account once every day to provide a continuous record of access.

Customers
miiCard has over 50 Web sites using its service for onboarding. In terms of adoption, Varga says that when faced with the choice between having to do a physical, in-person verification vs. logging into their online bank, 80 percent of users will prefer to log in or verify themselves using a bank-based verification process such as offered by miiCard.

Appendix 1: Company profiles
continued

ShoCard

- ShoCard.com
- Type: Identity provider
- Markets: International
- Based: Palo Alto, California
- Seven employees
- Founded 2015

Interview
Armin Ebrahimi, CEO and
Ali Nazem, VP Business development

Summary
ShoCard is a new start-up hoping to earn its first revenues in 2016. It is building an "identity platform" based on users' mobile phones and a public blockchain. Personal identifying information (PII) is stored on the user's mobile device, while signed and hashed identity verification certificates are recorded on the Bitcoin blockchain, where they can be accessed by third-party identity verification providers.

Business model
ShoCard is only fulfilling a basic identity provider role, and does not verify or authenticate to KYC/AML compliance. It made the decision to avoid identity verification because it felt that there are already many identity verification services, and service providers (e.g., banks) have a wide range of differing requirements. Identity is initially registered by the scanning of a government-issued ID, which is then stored on the user's mobile. Each field is hashed, and digitally signed on the device, then encrypted data sent to ShoCard, which uses split private key to write hashed record to the blockchain. The original registration is stored on the blockchain, and then subsequent verifications (for example, by a bank) are added to this profile. These verifications are referred to as Certifications and they are signed with the bank's private key and also placed on the blockchain so other third parties can verify them without contacting the original verifier directly.

Technology
ShoCard uses public/private key encryption and hashing to store and exchange data between the user, its system, and the blockchain. ShoCard doesn't maintain a database of user data, in part because in conversations with banks and other potential customers, they would want to duplicate that data in their own internal database, so a ShoCard database was redundant and added liability.

Data
ShoCard doesn't store any PII, and PII never leaves the mobile phone.

Customers
In May ShoCard announced a partnership with SITA, which provides IT services to 90% of airlines globally. The project will allow travelers to upload their documents to the ShoCard system, where they can then be accessed securely by security personnel using a public key token, expediting the flow of passengers through borders or other checkpoints.

Other target customer segments include: e-commerce (verify credit card transaction/improve on 3D Secure protocol), call centers (verify caller identity without asking questions), airlines, and general online services (financial accounts and other Web site log-ins).

Appendix 1: Company profiles
continued

Trulioo

- Trulioo.com
- Type: Identity verification provider
- Markets: International
- Based: Vancouver, Canada
- 30-50 employees

Interview
Jon Jones, president

Summary
Trulioo is an identity verification and fraud business that operates internationally. It provides its electronic verification services via a single API for real-time online processing, allowing its clients to verify the identity of people in more than 40 countries in compliance with KYC and AML guidelines. President Jon Jones spent 20 years managing identity and fraud services at Experian.

Business model
Trulioo launched in 2011 with a focus on using alternative sources of identity information, including social and mobile data, to establish verification. In the last 18 months, Trulioo has shifted its focus to incorporate more conventional sources of data, such as credit bureaus, utility companies, electoral rolls, banks, etc. It now connects to more than 145 different data sources that it has evaluated and considered trustworthy. This allows it to verify end-users in almost all of the OECD countries, as well as China, India, Malaysia, Mexico, Brazil, and others.

Customers pass Trulioo the basic personal information (e.g., name, address, DOB, ID number, email, phone) and Trulioo then processes this against a menu of third-party trusted sources that would be relevant for a customer's specific use case. The customer chooses those, and Trulioo manages the connection to each third party, which passes back "Match or No Match" information only—no PII is returned—for each individual attribute and for each third-party data source. The customer then uses the aggregate Match/No Match information to make its own decision about end-user identity verification.

Technology
Trulioo builds connections and standardized data formats to each of the 145 third-party data sources it connects to. This means that its customers only have to connect to the Trulioo API once in order to gain access to all the third-party data sources (customers can also use a standard Web interface to access the Trulioo service). Trulioo works with each of the third-party sources to optimize, and in some cases develop, the Match/No Match response.

Data
Trulioo aims to minimize the flow of PII between the customer, third-party data sources, and Trulioo itself. This allows its service to operate in countries where regulations make it very difficult to pass PII across borders.

Customers
Customers include banks (KYC/AML), remittance companies (KYC/AML), e-Commerce (risk mitigation), and payment processors (merchant onboarding); the standard arrangement is a subscription model.

Appendix 1: Company profiles
continued

Yoti

- Yoti.com
- Type: Identity provider
- Markets: United Kingdom
- Based: London
- 75 employees
- Founded 2015

Interview
Chris Field (CMO) and Robin Tombs (CEO)

Summary
Yoti enables end-users to create digital identities using a driver license or passport along with a selfie and smartphone. Because the identity is stored on the mobile device, it enables both online (e.g., logging onto a Web site with selfie) and offline (e.g., buying alcohol at a shop) identity use cases.

Business model
Yoti provides its identity creation service to end-users for free through its mobile application. It also provides its technology for identity verification, representing the commercial side of its business, in a classic two-sided market approach based on end-users and relying parties. In terms of pricing and revenue, Yoti estimates that a basic profile verification, which would be name, photo, date of birth, and perhaps address, might be in the range of £0.25/$0.36, while a more extended verification that included credit history might be as much as £0.70/$1. For extended verification of data that's not present on the individual's official documents, Yoti would partner with a third-party identity database such as Call Credit.

While Yoti is currently focused on formal identity verification using government-issued source documents, its longer-term plan is to enable other kinds of initial registration/authentication besides government documents. For example, in regions where government issued ID doesn't exist, or consumer data sources are scarce, it might try to incorporate individual attestations or verifications (e.g., having a community member vouch for one's identity), or use social media data as a complementary data source. Yoti acknowledges, however, that its current offering requires the use of a smartphone and is therefore not available to everyone.

Technology
The Yoti technology is designed to work best with NFC-enabled passports, which have biometric data (Yoti states there are around 1 billion passports with biometric chips worldwide). To register an identity, a new user takes a picture of their document along with a selfie to create their profile; if the document is a chip-enabled passport they scan it with their NFC-enabled smartphone to check against the biometric data stored there. Yoti has developed its own proprietary liveness test to ensure that the selfie photo is actually a photo of a real person and not a photo of another photo or a 3-D model or even a mask or a video. They use a third-party facial recognition technology from a German company called Cognitec. This initial enrollment takes about two minutes. Yoti verifies the documents are not fraudulent and that the selfie is of a live person, and if the live person matches the photo on the documents it creates an account. For its verification service, instead of offering a score or a risk profile, Yoti simply provides a Yes or No as to whether the person matches with their official identity documents. The verification process also includes the ability to identify tampering with the documents.

Data
In terms of technology and data, Yoti uses proprietary data formats and protocols. While one of their principles is the idea that the user owns the data, they have no plan in place or method for users to actually extract their data from their Yoti profile to take with them if, for example, they wanted to use a competing service. Yoti encrypts all data and stores it separately; for example, first name is stored in a separate location from last name. Because all data is encrypted and only accessible via the private key that the user maintains on the device, even Yoti cannot access the user data.

Customers
For individual end-users, Yoti foresees compelling use cases that include: authenticating oneself at a club or other establishment that requires an age restriction, opening a bank account or other financial service from the convenience of your home, applying for jobs, especially when needing to prove ability to work in that country. For commercial customers, Yoti is initially targeting recruitment/HR, financial services, and real estate rentals.

Caribou Digital is the leading independent think tank on digital economies in emerging markets.

Designed by
www.wearethelangtons.com

CARIBOU DIGITAL PUBLISHING CATALOG

CAR/001 **Caribou Digital February 2015 Team Workshop**
Barton Manor, Isle of Wight, United Kingdom

CAR/002 **Inclusive Digital Entrepreneurship Platform for Africa**
Caribou Digital Publishing and Goodwell Investments

CAR/003 **Digital Lives in Ghana, Kenya, and Uganda**
Caribou Digital Publishing and The MasterCard Foundation

CAR/004 **Winners & Losers in the Global App Economy**
Caribou Digital Publishing and The Mozilla Foundation

CAR/005 **Caribou Digital October 2015 Team Workshop**
Barton Manor, Isle of Wight, United Kingdom

CAR/006 **Digital Access in Africa**
Caribou Digital Publishing and The Department for International Development

CAR/007 **Caribou Digital February 2016 Team Workshop**
Barton Manor, Isle of Wight, United Kingdom

CAR/008 **Caribou Work and Surf Week**
Longeville-sur-Mer, Pays de la Loire, France

CAR/009 **DFS Innovation Lab**
Caribou Digital and The Bill and Melinda Gates Foundation

CAR/010 **Private-Sector Digital Identity in Emerging Markets**
Caribou Digital and Omidyar Network

Caribou Digital PUBLISHING

OMIDYAR NETWORK

ISBN 978-0-9935152-7-9
CAR/010