Digital Identity Toolkit

Section 3: Digital identity explained

Published by the Social Purpose Team at Yoti

January 2020

What is this Toolkit?

Digital identity is a relatively new but rapidly evolving sector that can and will affect many aspects of our everyday lives.

Digital identities verify and authenticate someone's identity. They can then be used to access a wide range of services and opportunities, from health and education services, voting and travelling, through to online shopping and dating. Governments and the private sector are developing and implementing digital identity solutions, and they're likely to become increasingly common in the future.

While there is already a lot of information on this topic, much of it is in lengthy, technical reports that hasn't been collated into a simple format that non-technical people can understand. We hope this Toolkit can help close that gap.

This Toolkit has been designed to help you find everything you need to know about digital identity. Before producing it, we spoke with individuals and non-profits around the world to get a sense of what they'd like to know about digital identities.

The audience for this Toolkit are members of the public, non-profits, entrepreneurs, developers, journalists and academics who want to learn more about digital identity and how digital identities might be relevant to them in their lives or work.

We hope you find this Toolkit helpful and welcome your feedback about how it could be improved.

Contents

Introduction

Digital identity provides a way of electronically verifying that somebody is who they say they are, normally online, so that they can access services both from government (for example, healthcare, education, grants) and the private sector (for example, banking and e-commerce).

The most trustworthy type of digital identity is called a **verified** digital identity. It can be made up of a number of attributes (or different bits of information) depending on what the digital identity will be used for, and could comprise of one or more of the following: your email address, digital photographs, even usernames and passwords or biometric information, or any other information about a person that can be accessed digitally. With many digital identity solutions, you can decide which attributes (or elements) of your identity, such as your age or nationality, you are comfortable sharing when requested. However, the provider of the service you are accessing usually dictates which attributes you must provide in order to access their service. Your identity is verified using documents or other data, such as fingerprints or passports, which can confirm that you are who you say you are. This Toolkit mainly focuses on this type of identity.

Unverified digital identities also exist, and they are created by signing up to certain websites such as Twitter, Facebook or Amazon. Through your use of these sites your preferences are recorded (your likes on Twitter, for example) and create a digital footprint, which becomes unique to you as an individual. This information is sometimes considered sufficient proof that you are who you say you are and can be used to access other websites and services. For instance, you can use a Google login to sign on to other websites. However, as you can provide a false name and other information on sign-up, these unverified digital identities can't be used to access public services such as healthcare, or private services such as banking.

There is a great deal of international interest in digital identity. It has been prioritised in the United Nations' Sustainable Development Goals (SDG target 16.9) and governments across the world, particularly in developing countries, are driving progress and adoption. National digital identities based on biometric data have been introduced in India and Pakistan and are being used to help citizens access public and private services, including education, welfare and e-commerce.

Digital identity also has the potential to protect the vulnerable, including the estimated 1.1 billion people globally who still lack an official ID. It is hoped that digital identities will enable global transactions across borders, help to prevent digital fraud, lower the costs and increase the efficiency of delivering services. It has the potential to strengthen democracies by enabling digital voting, and can be used to provide more personalised services to individuals. Adopting secure, verifiable digital identities has the potential to open up new markets and grow economies by billions. It is hoped that blockchain technologies might also help to put individuals in better control of their personal information.

Without a digital identity people are at risk of being unable to access critical public services and commercial services, including purchasing property, owning land, buying a car, being able to vote and reducing the risk of becoming homeless or stateless. These challenges disproportionately affect poor and marginalised communities, further increasing their vulnerability.

You can learn more about the different types of digital identity and why they matter in this section of the Toolkit.

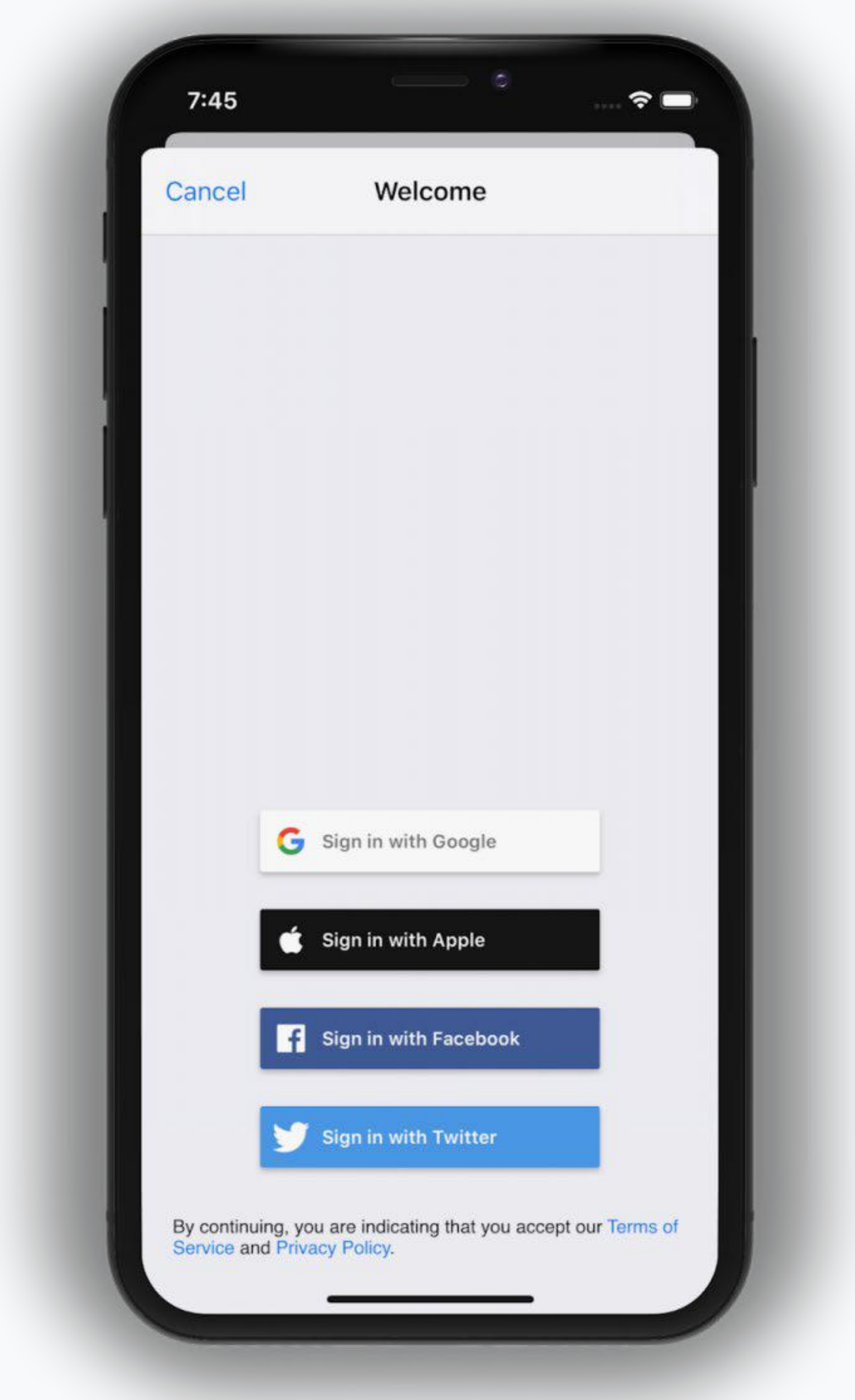
What is digital identity?

Put simply, it is a way to verify that somebody is who they say they are digitally (normally online) so that they can access services both from government (for example, healthcare, education, grants) and the private sector (banking and e-commerce).

A digital identity is comprised of a number of characteristics or data attributes. Examples of what a digital identity might include are:

- usernames and passwords for online accounts
- email address
- online search activities, such as electronic transactions
- date of birth
- social security number
- medical history
- purchasing history or behaviour
- personal website
- LinkedIn profile
- blog address
- biometric data, for example, thumbprints, DNA, face recognition, retina scanning
- digital photographs
- scanned passport images
- social media posts
- online accounts
- comments on articles and social media
- likes, posts, reposts, and shares on social networks
- signed online petitions
- created identity on forums
- credit card number
- qualifications
- memberships

> The term 'digital identity' describes *'technology-based solutions for identification in order to uniquely establish a person's identity and to credential it, so that the identity can be securely and unambiguously asserted, and verified through electronic means for delivery of services, across sectors including healthcare, safety nets, financial services, and transport'*.
>
> *World Bank: Digital Identity Toolkit*



By continuing, you are indicating that you accept our Terms of Service and Privacy Policy.

Types of digital identity

It may be helpful to consider two different types of digital identity: verified and unverified.

Verified

Verified digital identities are created just once and include verified (confirmed) attributes – proof that someone is who they say they are – from documents such as passports, driving licenses, birth certificates and biometric scans. Once this identity is created it can be used like a passport around the web to access a whole range of other services. This is the most trustworthy form of digital identity and is the type of identity that we focus on in this Toolkit.

Unverified

Unverified digital identities are created when people register on websites with their name, date of birth and other personal details. Over time, they go on to create a history on those sites. For example, Facebook captures information about people's friends, the content they like and their personal interests. In this way, a person creates a digital footprint which helps make up their online presence/identity. After a period of use, some sites use this interaction to confirm that you are the person you say you are beyond reasonable doubt. This is still a form of digital identity, which will allow access to other services (for example, you can sign up to some other websites using your Facebook login) but there are many duplicates and fake profiles set up on many sites using false names or other false information. This would not be possible with a verified digital identity, which is why you are unable to use unverified identities to access government services and banking, for example.

Definitions of unverified digital identity are broad and include any information recorded about you digitally, including social media posts, your search history, digital photographs, likes, comments and so on. This type of digital identity can be regarded as *'your entire, unique digital footprint on the internet and in databases'*. [1]

The Techopedia definition states that: *'A digital identity is linked to one or more digital identifiers, like an email address, URL or domain name'*. [2]

Because identity theft is common, authentication and validation measures are needed in order for digital identities to be trusted, and to ensure web and network infrastructure security in both the public and private sectors.

Validation ensures that identity providers allow for individuals to prove who they say they are. When using a digital identity, authentication enables users to prove that it really is them who is using their digital identity online.

Identity is clearly a complex, multi-faceted concept. Digital technologies add new layers of complexity as they make identity more flexible. For example, we can have multiple alternative identities depending on the sites you use, and how you have decided to build your profile on them. Digital identity is becoming more extensive than paper-based equivalents as we begin to collect extremely granular, detailed personal data on people from multiple platforms rather than more static information such as name, date of birth and so on.

The videos overleaf will help you to better understand digital identity.

What is digital identification (digital ID)?

Digital Identity Explained with Examples

Identity in a Digital World

Online Basics, Online Identity

Every ID Has a Story

[1] TechFunnel - https://www.techfunnel.com/information-technology/why-digital-identity-is-important-in-todays-world/
[2] Techopedia - https://www.techopedia.com/definition/23915/digital-identity

What digital identity is not

Digital identity is often mistaken for things that are actually only a component of digital identity. These include the following.

Device identity

This would create too much uncertainty as people upgrade and switch devices. They can also be stolen, used by more than one person or hacked.

An example of this would be the bank sending an access code to your mobile to check that it is really you logging in when you access online banking.

Personally identifiable information

Such as your full name, date of birth or a number assigned to you by your government (social security number in the USA or national insurance number in the UK). Passwords and secret questions can also fall into this category. These aren't considered sufficiently secure as fraudsters could purchase this information and use it to open new accounts in your name.

As an example, an identity thief could use your full name, email address and a password to access your emails, or open an online shopping account and make purchases while pretending to be you.

Behavioural analytics

Such as clicks, purchasing patterns and navigation paths. They can give a good sense of the type of user and their demographics but won't provide a definite link to an individual.

For example, many social media users create a digital footprint by clicking on likes, following certain pages and choosing certain friends. Over time, these sites can get a good sense of the type of person you are, including your political preferences, hobbies and personal interests, but anyone could use your account if you haven't signed out, or they could create an account in your name with false details without you knowing.

Why does digital identity matter?

Technology is making it cheaper and easier to identify people accurately, and the growing online world is increasing the need to prove one's identity. Governments around the world are investing in national identification systems, and other related solutions are being established for a wide range of purposes including voting, banking and money transfers. Identification systems are being used in areas as far reaching as social protection, migration, coping with natural disasters, financial inclusion and criminal justice.

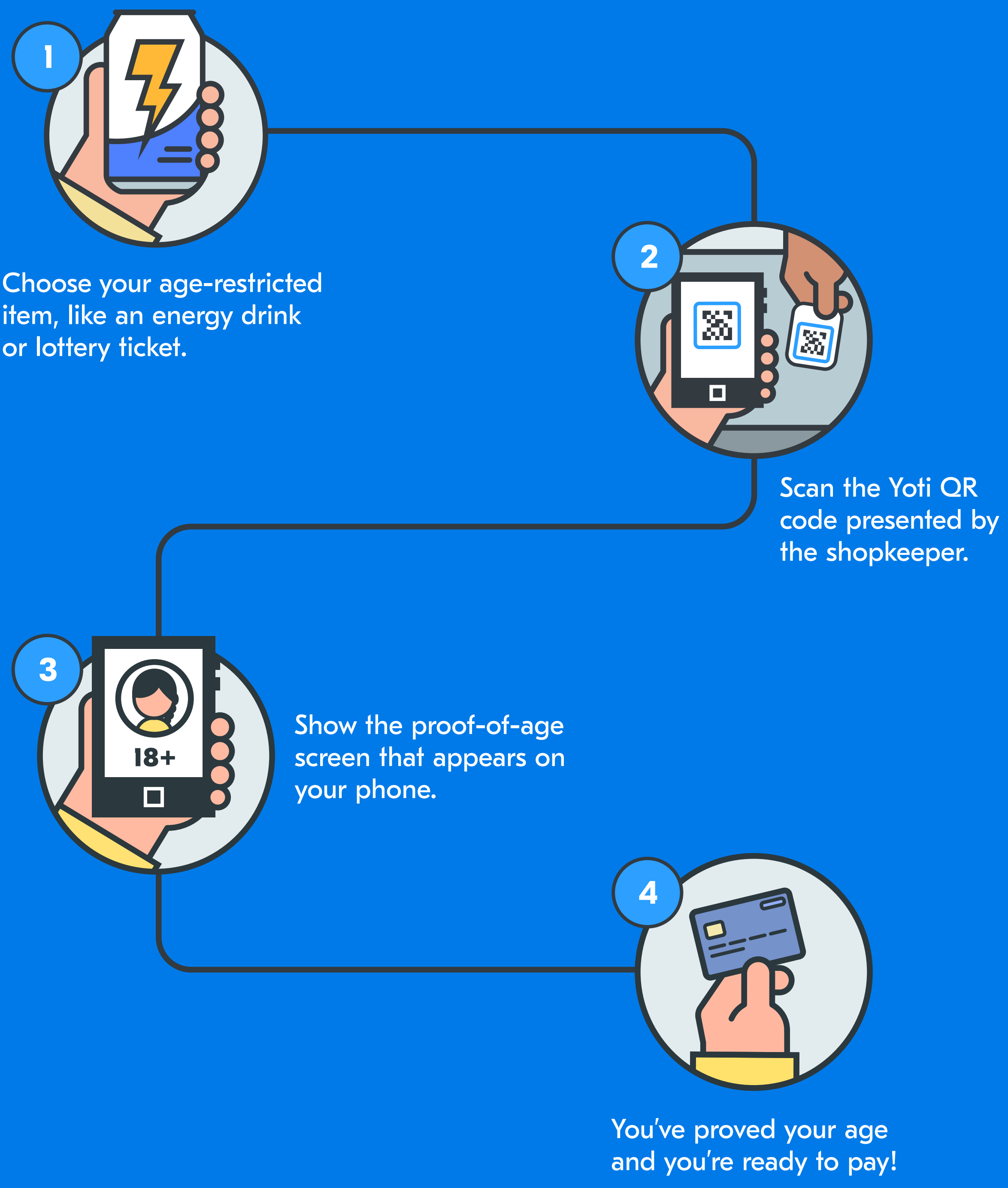
Having an identity is a human right. Article 6 of the Universal Declaration of Human Rights (published in 1948) states that: 'Everyone has the right to recognition everywhere as a person before the law.' In 2015, in response to the importance of digital identity, the United Nations' Sustainable Development Goals (SDG target 16.9) set out the objective of ensuring that everyone in the world has a legal identity. This commitment was strengthened two years later by the Principles on Identification for Sustainable Development: Towards the Digital Age.

Governments in developing countries have taken the lead in driving progress, particularly in southeast Asia where digital identification, based on biometrics, have reached most of the adult population in Pakistan, India and Bangladesh. These systems are gradually being integrated into the delivery of services and goods in both the private and public sectors.

The greatest identity gap remains in sub-Saharan Africa. The World Bank's Identification for Development (ID4D) programme's database states that over 40 percent of those lacking identification live here.

In Section 2 (Identity Basics), we discussed why identity is important. This Section aims to give an overview of why digital identity matters and what it can be used for.

YOTI Age Check



1 Choose your age-restricted item, like an energy drink or lottery ticket.

2 Scan the Yoti QR code presented by the shopkeeper.

3 Show the proof-of-age screen that appears on your phone.

4 You've proved your age and you're ready to pay!

Yoti Age Check - How to prove your age in convenience stores: https://agecheck.yoti.com/

Access services

You need an identity, or some way of proving who you are, to access a whole range of opportunities in the modern world. Examples include: accessing public services, such as healthcare and education; receiving public support, such as pensions, unemployment benefit and loans; travelling to another country; voting; buying or selling land; and accessing commercial opportunities, such as opening a bank account, buying a mobile phone or SIM card, employment in the formal sector or shopping online.

Protect the vulnerable

More than 1 billion people globally still lack an official ID, with the poor, rural and marginalised being the most affected. Unable to access some of the critical services and opportunities outlined above, they risk becoming even more vulnerable. Those without identification are also at risk of becoming stateless, which leaves them legally and politically invisible and destined to a life of poverty. See, for example, the case studies in Section 2.

Enable global transactions and activities

Today, identification is becoming increasingly important as people become more mobile and services become increasingly globalised. Digital identities make it possible to be recognised in different countries and jurisdictions, online and in person. Many of the most critical and urgent issues affecting humanity are global, rather than local, challenges. These include climate change, inequality and forced migration. Global challenges require global solutions.

More human activities and transactions are taking place online, which creates both opportunities and vulnerabilities.

Increase security

The threat of digital fraud is one such vulnerability, something which is increasing our need for secure digital identities. A recent surge in high profile data breaches has helped to raise awareness of how vulnerable people's data can be.

'Sixty-eight percent of Indians said they are worried about becoming victims of a data breach in the near future.'

> **'A digital identity system offers a secure alternative, and many companies are already turning to biometrics in a bid to combat fraud, increase security and enhance the customer experience. Users no longer have to remember passwords and they can appreciate the ease and simplicity that biometric technology can offer.'**
>
> *The News Minute*

A secure digital identity system allows people to prove their identity without showing paper documents. They can help confirm the identity of people you meet online, or help you log into websites securely without passwords. This makes both online and offline interactions safer for individuals and businesses. Digital identities can help strike a balance between privacy, security and convenience.

'In government, as in business, knowing who you're dealing with is essential when using any form of electronic communications. Businesses need identity assurance for commercial enterprises, such as e-commerce, online banking and trading, internet-based enterprise solutions for process automation or digital form signing. At the same time, government entities are in the business of keeping our nation, its people, and its physical infrastructure secure. Part of how they do that is by limiting access to mission-critical information or applications, so that "need to know" security is maintained. They do this by implementing a certificate-based public key infrastructure to confirm identity, and using digital encryption to protect documents to only be opened by the intended recipients.'

'Digital certificate-based identity assurance protects the government's physical and logical infrastructure restricting access to buildings, office suites, firewalls, virtual private networks (VPNs), servers, directories and enterprise resources that help government agencies and organizations achieve their mission.' [3]

Increase efficiencies and improve due diligence

Digitisation has the potential to lower costs, increase efficiencies, and reduce corruption and fraud. Businesses can confirm customer identities with less information, safe in the knowledge that every identity is verified. Digital identification can also enable companies to undertake accurate due diligence faster and cheaper.

> **'Without reliable and trusted data, companies have to spend countless hours manually checking and cross-referencing multiple data sources to verify customer identities to meet anti-money laundering (AML) and know your customer (KYC) requirements.'**
>
> *Trulioo*

'Digital identity can effectively remove some of the barriers that make public services complex and hard to access for users, increasing both convenience and the user experience in general.

Having a digital identity means users do not have to be physically present to gain access to many services, while online service delivery means users can benefit from 24/7 service availability.'

> **'Another important benefit derives from the fact that users do not need to remember different usernames and passwords for each of the services they employ. This simple but critical factor exponentially simplifies authentication processes, which in turn increases the popularity of a digital identity system for users.'**
>
> *International Telecommunication Union*

Give power to the people

A digital identity can put individuals in control of their personal information. It can give them greater transparency over who has access to their data and can limit the amount of information they share. Blockchain technologies can be used to create global digital identities which could enable planning, decision making and service delivery at a global level. This has the potential to put the control of identity into the hands of an individual as opposed to a government or private corporation that may not put their best interests first.

One example of this is Kenya's micro-lending app Tala. It allows microentrepreneurs to access credit by creating trust, using non-invasive analysis of behavioural data collected from their smartphone usage. This new form of distributed trust is opening up new financial markets without relying on formal verification of identity by a nation state or private company.

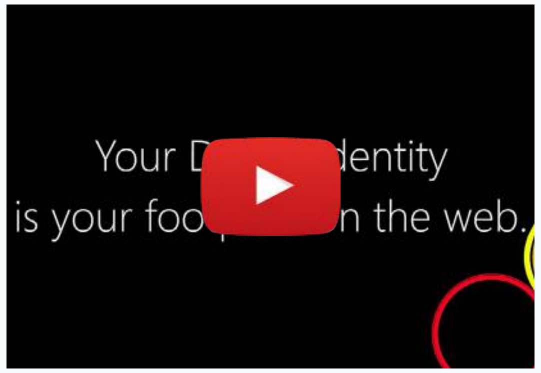
[3] Open Research Consultants - https://www.orc.com/home-page/the-importance-of-digital-identity/

More benefits

Digital identity has the potential to strengthen democracies by enabling digital voting, and it can be used to provide more personalised services to individuals. Adopting secure, verifiable digital ID forms has the potential to open up new markets and grow economies by billions. In countries without effective analogue identity programmes, leapfrogging to a digital-first system makes sense. As well as improving efficiencies, digital systems are also likely to expand access to more marginalised and vulnerable populations.

This video from Sheffield Hallam University helps to describe what digital identity is and why it's important:

What is a Digital Identity – And why is it important?



And this talk by *Subhashish Bhadra*, a digital identity specialist, helps to explain how a digital identity can be used as a force for individual empowerment and encourage inclusion:

Why Does Identity Matter?

The implications of having no digital identity

Section 2 described the implications of not being able to prove your identity. As the world becomes increasingly digital, it's likely that it will become harder to access the essential government and commercial services without a digital ID. Lacking a digital ID already shuts you out of lots of opportunities in today's world, as Laura Cox, an expert from Disruption Hub, explains:

'Without a digital identity, individuals and corporations are shutting themselves off from much of modern society. Retailers continually move online, as well as banking companies and government administrative bodies. If you're digitally non-existent in an increasingly digital world, you can't progress within it – you'll always be a few steps behind.'

'The internet allows for real-time worldwide communication, convenient and instant purchases, the huge accessibility of information and so much more. Without a digital presence, that world is closed off. Imagine applying for jobs without the internet. Even with access to a list of vacancies, it's hard enough to find employment. However, it's not just those without digital identity that will suffer from their own reluctance. Businesses that rely on digital custom are challenged with convincing technophobes that the advantages of online services are worth the risks. For governing powers, the problem is less to do with making money and more to do with knowing who actually exists. For instance, where digital identity leaves a biometric audit trail, that can pose a deterrent to fraudsters who do not want to leave a breadcrumb trail behind them. There's been so much focus on cybercrime that standard real-world crime may see an opportunistic upsurge. Even so, most people have a digital footprint even if they don't know it. You might post a photo of your technophobe grandparents on social media, for example, which enters their physical identity (at least) into cyberspace.' [4]

[4] Laura Cox, Disruption Hub - https://disruptionhub.com/importance-digital-identity/

Digital ID trends and developments

Digital ID has attracted a lot of interest in recent years. Here are some key trends that TechFunnel, a technology news website, has identified.

- Biometrics (such as fingerprint or iris scans) are increasingly used as an identification method, from national e-ID initiatives to identifying the correct use of a mobile phone or tablet to allow access.
- Prior to 2017, the UN and World Bank ID4D set up initiatives with an ambitious goal of providing everyone on the planet with a legal ID by 2030.
- Digital driver's licence projects have gained traction in the US, Australia and the Netherlands. Digital driver's licences would allow for legal IDs to be stored on your smartphone for additional convenience and enhanced identity protection.
- Traditional passwords are becoming less effective and less important in facilitating digital access. The website *ThreatMatrix* notes that biometrics, behavioural analytics, device recognition and other signals that cannot be faked or stolen will become increasingly crucial in digital ID. Password breaches have been involved in over 80 percent of documented data breaches.
- Some businesses are going to see a more immediate benefit to requiring digital identity than others. Banks, airports, human resource management groups, healthcare systems and government offices, all feature very sensitive information or are part of a programme or system that requires the most secure access and ID authentication. Digital identity certification helps safeguard digital spaces and information sources, as well as protect physical infrastructure by restricting access to buildings, office suites, firewalls, VPNs, servers, directories and other resources.

Adapted from TechFunnel - https://www.techfunnel.com/information-technology/why-digital-identity-is-important-in-todays-world/

How to create a trusted digital ID

A trusted digital identity consists of a set of verified attributes (taken from such things as official identity documents or biometric scans) to provide a certifiable link between an individual and their digital identity. Consumer engagement begins with trust, and trust often begins with a trusted digital identity.

The creation process for a trusted digital ID generally includes the following three steps:

1. Capture attributes, such as ID documents or biometric data.
2. Verify the authenticity of these documents and the identity of the person presenting the document by using biometrics or third-party checks.
3. Digitise the identity to create a digital ID.

Adapted from Gemalto, a digital security company - https://blog.gemalto.com/mobile/2018/03/02/3-steps-create-trusted-digital-identity/

Establishing and managing your digital identity

Understand the extent of your digital identity

Your digital identity is made up of many things. For example, the information you provide when you register for an account, or when you give your email address or login information to access a website (as with every social media platform). It can also include your search history, credit information and criminal history. It's important to consider all of these factors when considering how to protect your identity.

Watch new technology developments

As more digitally-influenced IDs become mandatory, pay attention to what information will be required from you. Also, keep an eye on technology such as blockchain — a decentralised ledger that can be encrypted and where the information is stored in several locations (which can provide a greater sense of security). Some financial institutions use it to *manage and protect financial transactions*, and it has the potential to work for ID management as well. But beware — the jury is still out on the role of blockchain here.

Digital identities have become increasingly important as fraud and hacking continue to plague individuals and businesses. In most cases, digital identity is a more thorough, more unique way to assign or recognise identity. There's no doubt that digital identity will affect more people and become increasingly central to the way we do business, sign up for accounts, track purchases and more.

Adapted from TechFunnel - https://www.techfunnel.com/information-technology/why-digital-identity-is-important-in-todays-world/

Who creates digital identities?

The private sector is leading the digitisation of identities. Companies such as Google, Amazon and Facebook have become the dominant brokers of non-verified digital identity. They collect granular personal data, which can be used to personalise and commercialise their platforms driving new business models.

While the public sector is moving more slowly, governments also have a critical role to play in developing digital identities. The transition from paper-based to digital systems is well underway, with examples including smart identity cards, digitally stored biometrics and near-field communication-enabled passports.

While our official government-held identity often differs from our identity on commercial social media platforms, the government and private sector are beginning to collaborate. For example, governments are building some of their digital services on top of commercial back-end solutions, such as ForgeRock and Gemalto, and Mastercard has secured government contracts to provide digital identity solutions.

Start-ups are also developing standalone digital identity solutions. In most cases, it will take some time before many of these are considered trustworthy enough for government purposes.

Decentralised systems for identity are also being developed using blockchain and other distributed ledger technologies, enabling the verification of identity that is outside the control of government or any private company. This is very attractive to those who want self-control of their identity and are apprehensive about their identity being owned by government or profit-driven corporations. They are also a good fit in our globalised world, where we may need to prove our identity across borders.

Above image - New Hong Kong ID cards to be rolled out from late December: https://www.scmp.com/news/hong-kong/law-and-crime/article/2169180/new-hong-kong-id-cards-be-rolled-out-late-december

Types of digital providers

Caribou Digital have helped us better understand digital identity solutions by dividing them into four categories.

The following information is adapted from [Caribou Digital Publishing and Omidyar Network](). Private Sector Digital Identity in Emerging Markets.

Enterprise back-end identity solutions provider (for example: Gemalto, Morpho/Safran)

These firms typically provide complete back-end identity solutions — standards, application programming interfaces (APIs) and infrastructure — 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 service offerings, enabling them to provide complete turnkey or custom solutions.

These firms are often contracted by governments 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 US driver licenses, India's Aadhaar database and biometric voter registration kits in Kenya.

These firms need to work in partnership with government or enterprises who have closer relationships to end users to build digital identity systems.

Identity providers (for example: Yoti, ShoCard, Facebook, Google)

This category can be further divided into two: verified and non-verified identity providers.

a) Verified identity providers.

These solutions enable end users to establish a digital identity which is verified or proofed against official documents. This category includes mobile network operators who are heavily regulated. For example, they have to follow KYC (know your customer) and AML (anti-money laundering) regulations. Companies can then rely on this high level of diligence to build trustworthy platforms. A good example is PayPal, which enables customers to make online payments without re-entering their bank details on any site which supports the PayPal payment system.

There are also companies where users can create digital identities that can be used in multiple contexts. Examples include Yoti, ShoCard and Global ID. Part of their appeal is that they give the user greater control of their personal information. An example of this is being able to show a store owner only your age to purchase alcohol but provide more information, such as your full name and address, to a bank when you want to open an account.

These companies usually use smartphone technology to create and authenticate an identity. For example, they may require you to scan official documents — a passport or driver's licence — and take a selfie to match its photograph. Different amounts of this information are then accessed by a third party, with your permission, when they need to verify elements of your identity.

b) Non-verified identity providers

This category is dominated by large Internet firms with hundreds of millions (or billions) of users such as Amazon, Twitter, Google and Facebook. These firms allow users to log in to third-party websites using their credentials. To do so, information is shared between the two companies involved. Currently, only some services can be accessed with this level of verification. Most financial services require additional levels of security.

Identity verification providers (for example: Experian, Trulioo)

These firms are used by third-party service providers to verify a user's online identity. Large credit bureaus and consumer data aggregators, such as Equifax and Experian, fall into this category. These firms tend to verify identity through delivering an automated set of questions based on the information that the agency has on an individual. For example: the year the user took out a mortgage or the model of car the user drives. Unfortunately, this approach is becoming riskier due to security breaches and the commercialisation of data. As a result, others could gain access to this sort of personal information. As a result, some start-ups now verify information using other approaches, such as social network data, bank account access or smartphone selfies and document scanning.

Some firms in this category act as both identity providers and verifiers. For example, Yoti and miiCard users can create and verify identities for commercial clients.

Decentralised identity frameworks (for example: Blockstack Labs, Open Mustard Seed)

These firms develop decentralised, open technology frameworks which support individual identity solutions. They tend to create the back-end on which other providers can develop identity solutions that meet customer needs. The Open Mustard Seed (OMS) project, from the MIT Media Lab offshoot ID3, is one example under development. Its aim is to enable users to create a core identity, verify different attributes via a chosen identity provider and record verifications on the blockchain as an immutable (un-editable) record. These solutions are sometimes known as self-sovereign identities because an individual, rather than a central authority, has control over their identity credentials and how they are shared. Other examples include Evernym and Blockstack Labs.

We hope that this Section has helped to give you a clearer sense of what digital identity is (and isn't) and why it matters. In the next Section, we'll be exploring real life examples of how digital identity is being used across the world.

Further reading

Websites

- Fast Company. Inventure
https://www.fastcompany.com/3039583/inventure

- Forbes. Demystifying Digital Identity —
What It is, What It Isn't and What It Can Be
https://www.forbes.com/sites/forbestechcouncil/2018/11/15/demystifying-digital-identity-what-it-is-what-it-isnt-and-what-it-can-be/#1ecb05172af1

- Just Ask Gemalto. What is Digital Identity
https://www.justaskgemalto.com/en/what-is-digital-identity/

- ORC. the Importance of Digital Identity
https://www.orc.com/home-page/the-importance-of-digital-identity/

- TechFunnel. Why Digital Identity is Important in Today's World
https://www.techfunnel.com/information-technology/why-digital-identity-is-important-in-todays-world/

- Techopedia. Digital Identity
https://www.techopedia.com/definition/23915/digital-identity

- Techspirited. Definition and Gist of Digital Identity Explained with Examples
https://techspirited.com/digital-identity-explained-with-examples

- The News Minute. Why a Secure Digital Identity System is Needed, Here Are the Benefits
https://www.thenewsminute.com/article/why-secure-digital-identity-system-needed-here-are-benefits-86486

- The World Bank, Identification for Development (ID4D)
http://id4d.worldbank.org/about-us

- Trulioo. Innovations in Identity, the Future is Mobile and Digital ID
https://www.trulioo.com/blog/mobile-digital-id/

Reports

- Caribou Digital Publishing and Omidyar Network. Private Sector Digital Identity in Emerging Markets
https://www.cariboudigital.net/wp-content/uploads/2019/01/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf

- Future Agenda. The Future of Digital Identity
https://www.futureagenda.org/future-of-digital-identity-report-launch/

- International Telecommunications Union. Digital Identity Roadmap Guide
https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/Digital_Identity_Roadmap_Guide-2018-E.pdf

- The World Bank. The Identification for Development (ID4D) Agenda: Its Potential for Empowering Women and Girls (background paper)
http://documents.worldbank.org/curated/en/859071468190776482/The-identification-for-development-ID4D-agenda-its-potential-for-empowering-women-and-girls-background-paper

- World Bank Digital Identity Toolkit. A Guide for Stakeholders in Africa
https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf? sequence=1&isAllowed=y

YOTI

YOUR DIGITAL IDENTITY

Published by the Social Purpose Team at Yoti
www.yoti.com/social-purpose