Digital Identity 3.0
The Platform for People

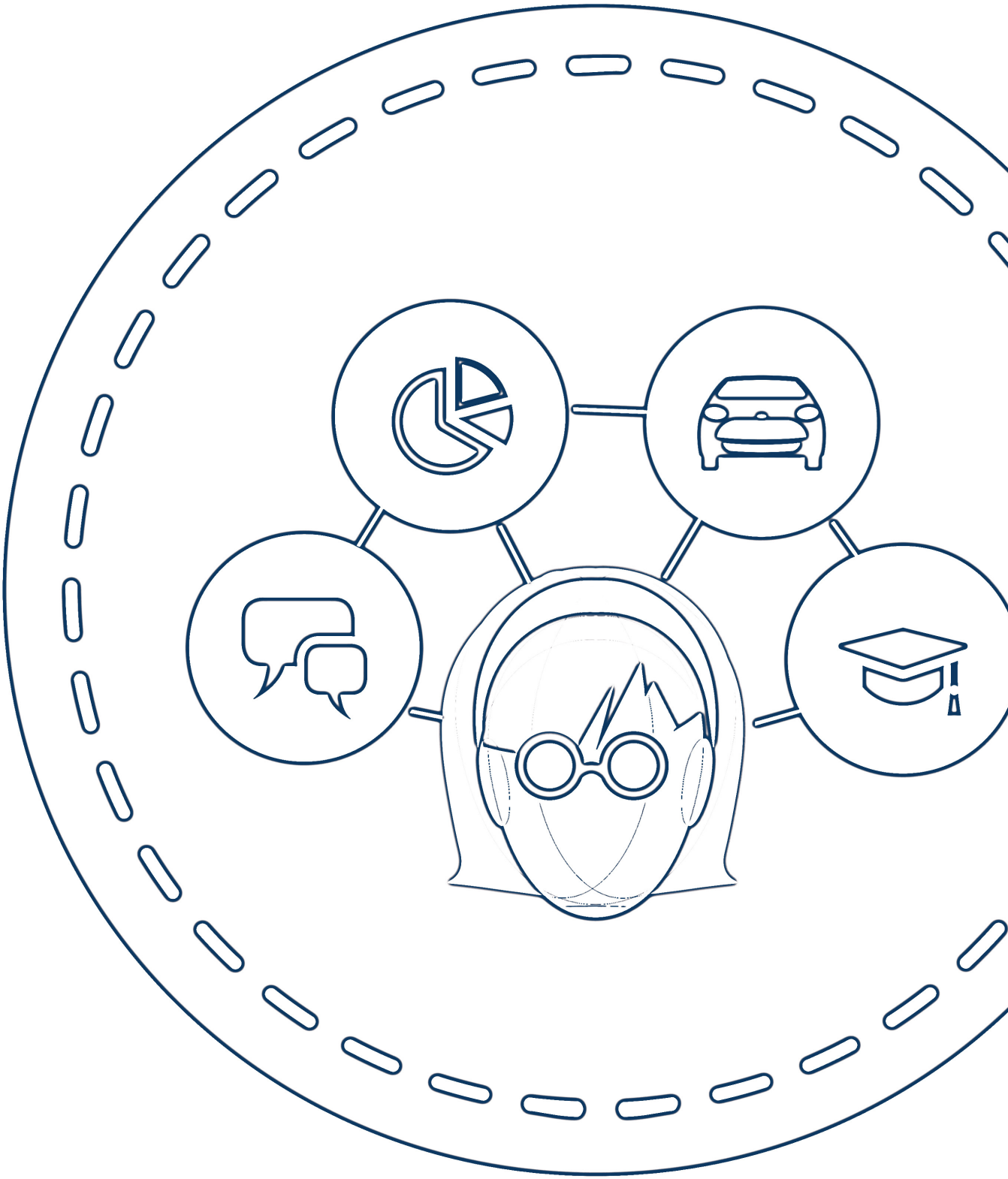
Working Paper No. 2

Acknowledgements

This working paper was prepared by the PwC Chair in Digital Economy Team, with lead authors Dr Willem Mertens and Prof Michael Rosemann.

We would like to thank Australia Post for their support in developing the findings and concepts presented in this paper. Not only did Australia Post initiate the overall idea, the countless creative input we received in multiple workshops over the past months has helped us tremendously in structuring Digital Identity 3.0.

Special thanks also goes to Anna Dixon form PwC for the beautiful designs, and to our very own Amanda Briggs for the designs, communications and organisational miracles, and for the overall wonderful support.



Executive Summary

Developed economies are moving from an economy of corporations to an economy of people. More than ever, people produce and share value amongst themselves, and create value for corporations through co-creation and by sharing their data. This data remains in the hands of corporations and governments, but people want to regain control. Digital identity 3.0 gives people that control, and much more.

In this paper we describe a concept for a digital identity platform that substantially goes beyond common concepts providing authentication services. Instead, the notion of digital identity 3.0 empowers people to decide who creates, updates, reads and deletes their data, and to bring their own data into interactions with organisations, governments and peers. To the extent that the user allows, this data is updated and expanded based on automatic, integrated and predictive learning, enabling trusted third party providers (e.g., retailers, banks, public sector) to proactively provide services. Consumers can also add to their digital identity desired meta-data and attribute values allowing them to design their own personal data record and to facilitate individualised experiences.

In this paper we discuss the essential features of digital identity 3.0, reflect on relevant stakeholders and outline possible usage scenarios in selected industries.

Introduction

Developed economies around the world are changing at a pace that is unseen in history. **Rapid digitization is disrupting traditional business** models and industry barriers, while giving rise to new opportunities (Weill & Woerner, 2015). The low cost of light-asset business models, the digitization of the society and increasing levels of digital literacy allow entrepreneurs and corporations to quickly acquire value and market share, disrupting existing business and in some cases even entire industries (Gimpel & Westerman, 2012).

At the heart of this disruption are people. Affordable, powerful mobile devices, intuitive apps and hyper-connectedness via social media platforms have accelerated the integration of people into economic value chains. Consumers have become co-designers, co-producers and self-servicing using public forums to discuss and assess corporate services Take the example of Tripadvisor, where users of the platform are in fact the ones that 'advise', monitor and review. In some cases,customer-to-customer transactions are becoming so popular (e.g., social trading, peer-to-peer lending, car sharing, social learning) that they may even replace dominating B2C value chains.

Through these shifts, people have gained power. They can share their voice, influence others, find information and consume products and services from anywhere in the world. This increased empowerment and the more active role of consumers have moved people to the very heart of the economy; where the 20th century was dominated by corporations, **we now see the emergence of the economy of people** (PwC Chair in Digital Economy, 2015).

The shift to the economy of people has one very distinct consequence: **people produce and share an exponentially increasing amount of data, i.e. big private data**. In a matter of years, it has become mainstream to trade goods and services using a mobile device and with anyone—other consumers, corporations or governments. As these transactions take place in a digital environment, each transaction requires the exchange of trusted master and transaction data. It typically consists of data that allows others to ascertain that they are dealing with a real person and—increasingly—information about past transactions that is supplied by others (e.g., reviews).

Currently, however, **this data is still largely in the hands of corporations** and data in B2C relationships is typically produced in corporate platforms leading to unbalanced relationships. Corporations create industry-specific, comprehensive customer master records and collect transaction data as their customers interact with them. They mine the data in search of their most profitable customers and ways to make these customers even more profitable (Mitchell, Henderson, & Searls, 2008). People are asked to share the same data over and over again with any organisation or government they interact with, and have to sign away the rights to using that data by agreeing to the terms and conditions of corporations. Research has shown that people do not mind sharing data if they see value in the transaction, yet they have an **increasing need to regain and retain control over their own data** (Maler, 2009; Satchell & Foth, 2008; Satchell et al., 2006; Satchell, Shanks, Howard, & Murphy, 2011).

People want to decide how much data to share and when, and they want to be able to revoke their data. Moreover, users want to choose which data to share. Most users maintain multiple digital identities, private as well as work-related, and value the independence of

A word on 1.0, 2.0 and 3.0

When reading the term digital identity 3.0, one may wonder what that 3.0 refers to. It refers to a paradigm shift. From our perspective, 1.0 refers to a one-way street. In the first iteration of the internet, for example, most things went one way: data was loaded onto the web for people to read. Web 2.0 changed that paradigm by allowing all users to create content. An example of digital identity 1.0 is a digital driver's licence. It allows me to show my licence on a device instead of a card, nothing more. Digital identity 2.0 would be something like OpenID or an extended version of MyGov: a digital identity that allows online authentication (please refer to the fine print at the end of the paper for a definition). Online authentication, in turn, facilitates the online exchange of services and products. The paradigm shifts to a two-way street. The next step, then, is not a street, but a city. In fact, the 3.0 in digital identity 3.0 refers to a world of possibilities. That is what 3.0—what we call a platform—allows: by connecting and facilitating exchange between anyone and everyone, and by facilitating the exchange of whichever information or value people desire, two dimensions are not enough to grasp everything that is possible.

those different online personas. At the same time, people have a desire for an integrated way to manage independent digital identities (Satchell et al., 2006, 2011). Indeed, as people and their data become central to value creation, they have to get organised.

Vendor Relationship Management (VRM) systems have emerged as a dedicated type of software to provide a people-first approach to B2C relationship management. VRM has been defined as "a set of tools, technologies, services and new business models that help individuals build and use their own personal data stores, choose who to share which portions of these data with, on what terms, for what purposes, send messages to suppliers and/or the market, and put customers in a much better to position to manage their relationships with vendors (existing and potential suppliers)" (Mitchell et al., 2008, p. 4).

In this paper, we present a concept for a digital identity platform that we believe can give people the full control described by VRM and unlock entirely new business models and experiences. This concept is not new (Narayanan, Toubiana, Barocas, Nissenbaum, & Boneh, 2012), but we believe that a matured digital economy has allowed digital identity 3.0 to become a reality. In the following, we describe **what** exactly we mean when we refer to a digital identity platform, and explore **why** people would use such a platform and **what for**. Finally, we explore **how** such a platform could be introduced and grown.

Digital Identity 3.0: identity meets digital platforms

Digital Identity 3.0 has aspects of classical digital identity concepts and of platforms. With classical digital identity we refer to a digital representation of a person or thing that consists of a collection of structured attributes (please refer to the fine print at the end of this paper for precise definitions). Platforms, on the other hand, are products or services that facilitate interactions between users in two-sided networks (Eisenmann, Parker, & van Alstyne, 2006). Two-sided networks consist of a platform facilitating interactions between two groups of stakeholders, for example a group of service providers and a group of consumers. A digital platform—typically a website or an app—facilitates this interaction online. Well known examples of digital platforms are AirBNB, Uber, eBay and Gumtree.

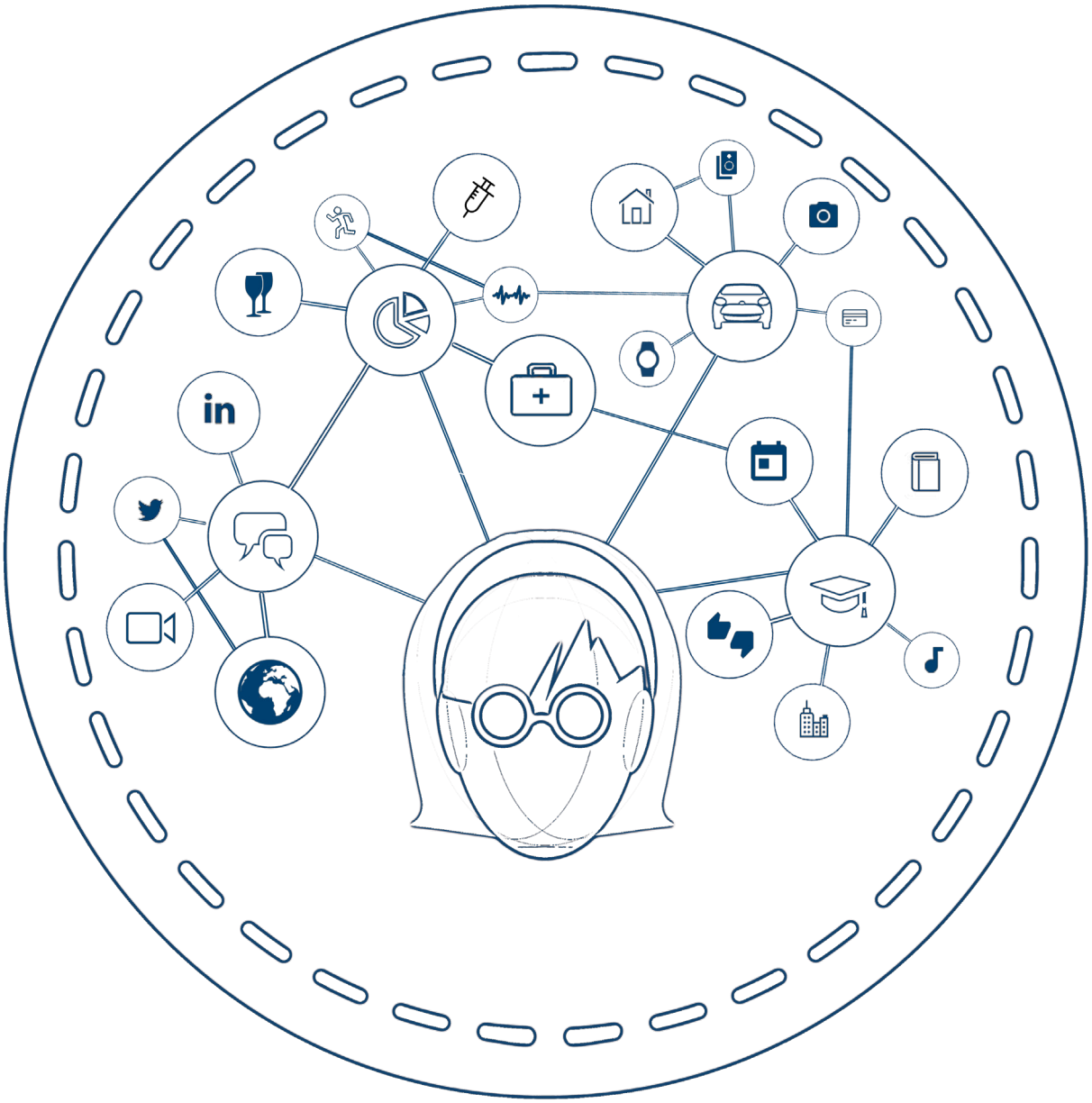
> *Digital identity 3.0 is a private and integrated master record that exists independently of any immediate commercial or legal context. It empowers people to create new attributes, share these attributes selectively as they connect with others, and create experiences and value beyond what can be predicted.*

The first part of this definition refers to **a privately owned and integrated master record**. This is our definition of the 'digital identity' part. A master record is a set of attributes of a person or thing. Contrary to a transaction record, a master record is not transient; it has a long lifespan. Some of the attributes in the record, however, may be transient or dynamic (see fine print). A private master record is uniquely related to one person or thing, is not part of a larger repository of master records and is managed by the person or thing the attributes refer to.

In other words, this first part of the definition refers to a set of **attributes that are linked to the person or thing who owns and manages it**. Figure 1 illustrates what such a private master record could look like, and which attributes and clusters of attributes the owners may want to add and maintain. Indeed, the` owner can write, read, change and delete any attribute, and has full control over who else can execute these functions. This is contrary to the classical master record that exists in most organisations today, where, for example,

a customer relationship management system maintains master records of customers, but controlled by corporations and not by the customers themselves. This is also different to online platforms such as the Australian MyGov, where citizens do maintain their own data, to a certain extent, but have limited control over what the master record owner (i.e. the government) does with their data.

Figure 1. Illustration of a private master record and its possible clusters of attributes



This brings us to the second part of the definition, which states that this private master record exists **independently of any immediate commercial or legal context**. Most master records that exist today are created and maintained because they serve a commercial or governmental purpose. Organisations keep master records of their customers to have a stable point of reference for all their interactions including quotation, delivery or invoicing. Aggregating such transactions over time allows insightful customer analytics. Governments keep master records about citizens for various public services related to licenses, permissions and personal records. The individual is merely a stakeholder in all of these scenarios: a citizen, a customer, a patient, etc. The private master record we describe in this paper, however, does not exist to create value for organisations or governments—*it primarily creates value for people.*

The third part of the definition refers to the platform element, stating that **it empowers people to** create new attributes, share these attributes selectively as they connect with others, and create experiences and value beyond what we can predict. This is the key differentiator between what we call digital identity 2.0 and digital identity 3.0. Most digital identity solutions that exist today serve one purpose only: authentication (see fine print for a definition) assuring the other party that the digital identity is providing a trusted authentication of the user behind the identity. As a consequence, the meta-data of such authentication-driven identities represent a minimal set of demographic data. Digital identity 3.0 serves the purpose of enabling people to create value. That's why we call it a platform. Platforms allow users to create, exchange and consume value (Bonchek & Choudary, 2013; Choudary, retrieved 2015). This means that users, by stepping into a producer or a consumer role, create value for themselves. Defining Digital Identity 3.0 as a platform means facilitating usage scenarios that are designed by the owners and consumers of the data, not the platform provider.

Before we cover scenarios that a digital identity platform could unlock, we will discuss the five key characteristics that make up this definition: Digital Identity 3.0 is consumer empowered, learning, proactive, open, and connected.

Core Characteristics

Consumer Empowered

The first core characteristic of digital identity 3.0 is that consumers are in charge. As mentioned before, people own their private master record, and have full control over who can read, write, change and delete the attributes of their digital identity. Research has shown that people crave this sort of control (Satchell et al., 2006):

- People want to control how their digital identity grows and is maintained (**write** and **change**). Other parties—including devices and things—may be given rights to add, update or authorize data, but users want to be able to have full control of the user management of their digital identity.

You have the right to remain anonymous

Many transactions require people to share more data than necessary. In protest, some people will share fictitious attributes (e.g. a fictitious name, date of birth or address). Legally, it is not necessarily unacceptable to go by the name of Clark Kent.

Jacinta Buchbach, who researches digital identity as part of her research in the regulation of social media and work at QUT, explains: “It can be legally acceptable for people to engage in anonymity or pseudonymity practices in their dealings with some entities. Australian Privacy Principle (APP) 2 of the Privacy Act 1988 (Cth) provides that individuals must have the option (emphasis added) of dealing anonymously or by pseudonym with an APP entity. The exceptions to this being: the entity is required or authorized by law or a court or tribunal order to deal with identified individuals; or it is impracticable for the entity to deal with individuals who have not identified themselves. While ‘anonymity’ and ‘pseudonymity’ are two different concepts, the principle requires that both options be made available to individuals dealing with an APP entity unless one of the two exceptions applies. “ A consumer empowered identity platform could provide such fictitious and untraceable pseudonyms. People could use these when an organization asks for more data than it needs, or when sharing data does not increase the value of the transaction for the customer.

- People also want to control who has access to which information and for how long (the **read** function). People should be able to share single or logical clusters of attributes (see figure 1), and these clusters should be personalized automatically yet open to be changed by the user. It should also be possible for clusters of attributes to be shared without disclosing an identity. A person could, for example, share information for a quote about an asset that is to be insured (e.g. a car), without sharing information about the owner of the asset.

- Finally, people want to be able to withdraw information after it has been shared (the **delete** function) and know what third parties they shared their information with.

In short, a consumer empowered digital identity platform will allow consumers to **bring their own data** into transactions with peers, corporations and governments, and enforce their own terms and conditions where needed. People no longer want to be the one populating corporate data and being enforced to use corporate data (e.g., using bank account details when dealing with a bank), but instead interact based on the provision of their own data.

Learning

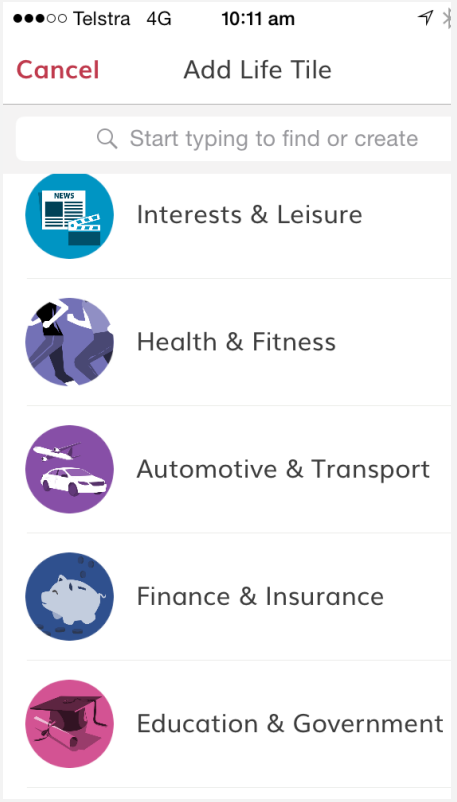
Digital identity 3.0 learns from your online and offline behaviour—to the extent that you allow it to. This learning consists of three aspects: automation, integration and prediction. **Automation** means that learning is effortless. Currently, most data on popular platforms such as LinkedIn, Facebook etc. is either supplied by profile owners or by peers. Updates of that data happen largely manually, and learning about preferences is still mainly based on active input from users. Spotify, for example, will make suggestions based on songs that were actively added to 'your music' or skipped, and many other service providers learn about preferences by letting people hit 'like' buttons. When automated learning does occur, it mostly serves the purpose of customising advertisements or suggesting products that users might like (e.g. Amazon). A digital identity platform would learn about preferences and attributes effortlessly, and use continuously updated data to allow providers to personalise services and products even further.

Integration means that various data streams and clusters of attributes are all part of the same data record and that learning occurs across all boundaries. This is contrary to the

Illustration: Meeco

i.e.

A good example of a platform that aims to put people in charge of their data and facilitate collaboration with others on the terms of the platform owner is Meeco. Meeco is a 'life management platform' that helps people centralize and organize their data and share selected (clusters of) attributes. The scree shot to the right illustrates what that could look like in practice.



current situation, where data is fragmented and each fragment is in the hands of a different organisation, creating so called "walled gardens". This becomes painfully obvious, for example, when changing address. It is up to the consumer to notify the bank, government, Internet service provider, employer, etc. In a consumer empowered digital identity, an address would be updated once and this information would be pushed out to all parties that the owner has chosen to share that address with.

True integration would mean that even that initial 'push' is unnecessary, and that lateral learning occurs automatically. A new mortgage or rental application would trigger the 'housing' cluster of attributes to inform all other clusters that the attributes describing the owner's address are about to change. In another example, a student could choose to share information to the government about different clusters of attributes including the student's work cluster, study cluster and financial cluster. All these clusters would be held

up to date automatically and constantly, allowing the government to define at any point in time whether the student is eligible for welfare payments, and if so, for how much and how much longer.

Prediction refers to the longer-term possibilities that arise from automated and integrated learning: your digital identity would know so much about you and your habits that it could predict events, changes in attributes and even changes in habits. Automated predictions are generally based on machine learning. Machine learning is a scientific field studying algorithms that autonomously find patterns in data, generate predictions by extrapolating these observed patterns, and continuously refine and alter these predictions based on continued observation. A well-known and often criticised example of machine learning is Facebook's news feed ranking. Based on observations of the pages viewed and the

Illustration: Nest

i.e.

A good example of automated, integrated and predictive learning is provided by Nest, which started out as a smart thermostat and now is connected to a whole range of smart home appliances.

The Nest system effortlessly learns from behaviour: by connecting to fitness trackers, it knows when house owners get up and go to bed, allowing it to adjust the temperature in the house in a timely manner. It also connects to the owners' car so it can warn them that they left the oven on when they are leaving, and instructs the washer and drier to keep the laundry wrinkle-free until someone is home again. As such it integrates data from different sources and allows learning crosses these different sources and data streams.

After some time, it will get to know the family's habits so well that it can predict when they get up, when they leave for work and when they likely will arrive home again. Although Nest is not an example of an identity platform, it illustrates that the rapid uptake of wearable technology and the coming of age of the Internet of Things (IoT) will allow a smart digital identity to effortlessly learn from every aspect of our digital and physical world.

amount of time spent on them, pictures liked and messages sent, Facebook will narrow down the list of friends, events and suggestions that appear in news feeds.

In summary, automated, integrated and predictive learning allows digital identities to know and selectively release information about people that in turn unlocks the next characteristic, proactivity.

Proactive

Proactivity is another central element to the shift from the economy of corporations to the economy of people; it means that **corporations come to people**, instead of people coming to corporations.

Most organisations today are still focused on their own operations. They constantly aim to increase their productivity and the quality of their offerings. While they often claim to do this for the sake of the customer, this customer remains a stakeholder to the organisational processes (Trkman, Mertens, Viaene, & Gemmel, 2015). Proactivity means that the organisation becomes a stakeholder in the customer's processes. Instead of organisations pulling customers into their processes, people's digital identity would pull products and services towards the customer.

The key measure for proactivity and for the quality of service providers will be **service latency**. Service latency refers to how long it takes before an emerging need is satisfied by a service or product. For example, how long does it take Nest to warm up the house when someone gets up or comes home. Based on predictive learning, service latency could be reduced to the point where the satisfaction of a need is triggered before the need emerges. The government could send me a new passport before my old one expires. Or going back to the example of student welfare payments, the government would pick up that a student is about to turn 22—which means students' rights change—and inform the student of any upcoming changes well in advance. In short, proactivity is about **satisfying needs before they have emerged**. Besides the accelerated provision of the service, it also allows the user to rely on such proactive notifications (e.g., what government services are relevant at what stage of life) as opposed to investing time into searching for such information.

Open

The characteristic of openness can again be subdivided into three different aspects. The first one we mentioned before: digital identity 3.0 is **not confined to one organisation, ecosystem or purpose**. Instead, it is open to be used for any purpose the owner wishes to use it for. Apple's keychain or Google's extensive authentication support in Chrome and Android devices are examples of digital identity solutions that are not open. They are confined to their own ecosystem: an operating system and/or a certain browser. The 'sign in with Facebook' solution is slightly more open, because you can use it for purposes outside of Facebook's immediate control, but whether you can use it is still in the hands of service providers. As such, it is not entirely open.

The second aspect relates to the creation of attributes: an open platform allows users to create previously unspecified attributes. This means that **users can specify new meta data**, not just new values. An example of a meta data is age, with values that are typically discrete numbers. Most online platforms that let users share information today allow users to complete values in prespecified fields only: address, company name, degree, favourite book etc. A digital identity 3.0 platform would allow users to invent new fields, i.e. new meta data. I may, for example, want to add the suddenly squealing sound of my car engine to my digital identity and share it with my mechanic, so my mechanic can listen and advise me whether I should bring my car in for a check-up. This means I would add the meta data 'car engine sound' and the value would be a short audio recording.

This example illustrates the third facet of openness: **it allows people to create entirely new scenarios and business models**. YouTube, for example, is not open in the sense that it is confined to one purpose—sharing videos—and that it doesn't allow users to specify new meta data. However, it has allowed users to create entirely new scenarios and business models. Just to give one example, who could have predicted that someone could make a more than decent living ($7m in 2014) by recording himself while playing video games (BBC News, 2015).

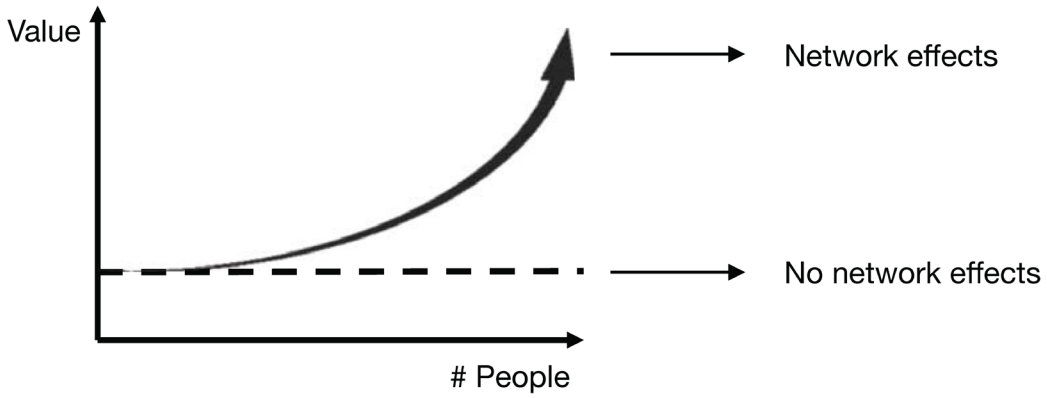
Some of these new meta data and scenarios may exist only temporarily. In areas and times of increased fire risk, I could for example temporarily request updates about bushfires and express my willingness to volunteer. I could also temporarily provide access to the data

collected by a privately installed weather station and a webcam on the roof to keep track of wind and smoke in my area.

Connected

The fifth core characteristic of digital identity 3.0 is that it is connected, which is a core characteristic of platforms in general and the **key value driver behind the sharing economy**. The exponential growth that is so often seen when platform businesses gain traction is only possible because of **network effects**, which emerge when anyone can offer a product or service to everyone (Eisenmann et al., 2006). The value of a platform that allows users to do that increases in value with each new consumer or producer that joins. This leads to 'winner takes it all effects' that can be observed with many digital companies who have a market share beyond 50% (e.g., Facebook, Linkedin, Google search, Pinterest). Figure 2 illustrates this trend.

Figure 2. Network effects cause exponential growth in value



Network effects are accelerated even further when people can **bring their own network**. This accelerating effect is commonly referred to as viral growth. When a video 'goes viral', it means that people share the video on existing platforms and with their established networks. Any platform that can tap into people's existing networks has more value to the user, and a greater chance at success. That is why Digital Identity 3.0 should allow users to bring their own network and use this to connect their digital identity with those of other users.

For a digital identity platform, connectedness has a personal and a social element. Personally, my digital identity would be connected to all my devices and to all my service providers. These connections enable the learning and proactivity we discussed in the sections above.

Socially, connectedness refers to the fact that my digital identity will connect me to people, corporations and governments that are complementary or supplementary to me. Connecting based on complementary attributes means connecting to others like you. One example of a platform that facilitates **complementary** connections is PatientsLikeMe, which—as the name suggests—helps people to connect to others that have similar health issues. An example of a platform that facilitates connections based on **supplementary** attributes is LawAdvisor, which connects people in need of legal advise to lawyers that can likely help them. Many platforms facilitate connections to others based on complementary as well as supplementary attributes; they match you with others that are like you, yet at the same time have something you desire—does Tinder ring a bell?

The natre of the connection between two digital identities can take many forms, for example:

- John **endorses** Mary to pick up his daughter Jane
- John **instructs** Jane to mow the lawn
- John **assigns** one Netflix movie to Jane (she mowed the lawn)
- John **seeks** proximity to Mary and avoids Jeff
- John **follows** all public activities of Kim Kardashian (and of Jane)
- John **shares** a really interesting article with Mary (not about Kim)
- John **sends** flowers to Mary
- Mary **avoids** proximity to John and seeks proximity to Jeff

Industry-specific Affordances of a Digital Identity 3.0

We believe the possibilities of what a digital identity platform affords are endless. Just to give you some inspiration, this section presents three industry-specific examples of scenarios that may unfold once digital identity 3.0 is a reality.

Education

The general affordances of Digital Identity 3.0 as outlined earlier in this paper will be of high importance for the education sector for two reasons.

First, the disruptive power of the digital economy requires entire new levels of educational well-being among the members of future societies. If forecasts are correct that more than 40% of all jobs are in danger due to developments such as robotics and machine learning over the next 20 years , lifelong learning will become an even more important necessity. As much as digital technologies are disrupting the revenue streams of established corporations, they do exactly the same with individualized revenue streams. In other words, individual employees need to assess the extent to which their very own income stream is in danger. Similar to the impact on corporations, the widely cited Oxford study quoted above showed that most jobs are at least to a certain extent under danger of being either completely or partly automated. In this context, it is essential that members of the workforce keep on continuously up-skilling their own capabilities via training and education to stay in demand in a world of fast changing job descriptions.

Second, the high speed in which new technologies and scenarios for their deployment emerge make it increasingly difficult to comprehend what needs to be known, i.e. it can be expected that the levels of unconscious incompetence are increasing. Classical education, however, is largely based on the notion of conscious incompetence leading to well-articulated demands for educational services. In this environment, reactive learning dominates, i.e. learners consume services (e.g., enrolling in a MOOC, a vocational training course or a degree) after being aware of their learning demands. An increasing unconscious

incompetence, however, will require changing the direction of the education supply chain and moving towards more proactive educational offerings.

In order to support entire new levels of personal educational well-being based on a model of proactive learning, a digital identity record with populated educational attributes is required. These attributes could cover groupings capturing existing capabilities as documented in the form of qualifications or skills as well as requirements related to the position and its context (for example industry sector from which relevant industry standards could be derived).

The individual learner could allow educational providers to populate and monitor these attributes. Based on these attributes and environmental changes, the provider would as part of a personal learning assistant offer relevant educational services.

In this context, it could be imagined, for example, that universities would offer their graduating students a subscription-based model where based on the documented academic record (history), articulated preferences (e.g. preferred units/lecturers/topics) and shared, personal contextual variables (e.g., company, job, client characteristics) relevant educational services are offered.

Based on the previously introduced features of a Digital Identity the learner would be able to configure in an open environment learning attributes (e.g., what content, instructor, media is preferred), self-populate or have third parties populating the attributes. The education partner would monitor these attributes and relevant environmental changes (e.g., the release of a new standard) and based on these attributes provide learning recommendations.

In such an environment, citizens would rely on selected educational well-being partners to provide the most relevant learning modules in the desired media and in an accepted pricing model.

Retail

The retail sector has been one of the most advanced in terms of analysing and deriving insights from the behaviour of their customers. Complex shopping basket analysis, for example, has allowed some retailers to derive private attributes. A by now famous case is the retailer Target who figured out that a female customer was pregnant and used this fact for a personalised marketing campaign. Her upset father had to find out via Target advertisements for baby clothes and cribs that his daughter was pregnant. This shows how corporations try to populate attributes of the digital identities of their customers by deriving insights from big data analytics.

True, people-centred and owned Digital Identity 3.0 concepts will have the potential to dramatically influence current B2C relationships in the retail sector. As shopping behaviour is largely correlated with personal attributes such as family composition, income, allergies or preferences, attributes that go beyond what is immediately visible from shopping behaviour will be critical to provide more personalized services. For example, a customer who might have certain allergies could be guided by the retailer up to the point that a warning at the checkout is provided. Other examples are related to open life events (such as hosting a party), which could be used by the customer to request tailored offers.

Purchased retail items with a longer lifecycle and higher value could lead to personal assets connected to the digital identity including overall value (relevant for home and content insurance) or data such as warranty (prompting when about to be expired) or technical details (for shopping advice in terms of compatibility)

Connected digital identities would allow the definition of alternative drop-off points for home delivery or could lead to endorsed digital identities for pick-up from defined collection points.

A challenge for retailers will be to integrate their already very comprehensive customer master records with such emerging digital identities, to identify those attributes and life events of relevance for them and to create and sustain compelling value propositions based on such a digital identity.

Personal asset control

Digital Identity 3.0 will not only impact the way citizens deal with corporations, but also influence how we live and interact with our very own assets.

One example is be the integration of digital identity concepts into the notion of the smart home. For example, the idea of endorsed digital identities could be connected to a secure home and doors might only open for those owners of digital identities who have been endorsed by the home owner. This would further extend already available solutions such as Lockitron and will become even more relevant with stakeholders conditioned to the sharing economy and in particular familiar with

facilitators-based solutions such as AirBNB. The idea of using digital identities to control access to private assets could be extended beyond the home and encompass other assets such as fridges, separate spaces of a home, sporting equipment or entertainment solutions.

Another main asset that could be controlled would be of course the car. With the increased digitization of the car and the emergence of the driverless car, ‘bringing your own data’ into the interactions with a car will become even more important. A car owner could allow, or explicitly disallow, specific digital identities to use his/her car. Furthermore, location relevant attributes of a driver, or passenger, such as home location or location of next meeting could be used as input for the navigation system. In a similar way, information about favorite hotels, retailers or petrol stations could provide valuable input to the navigation system.

Further affordances of the digital identity in the context of a car will be unlocked when the driverless car becomes a reality. In order to comprehend the possible impact, it is required to calculate the ‘amount of digital attention’ that will be made available by driverless cars. There are currently far more than one billion cars on this planet . Even if only 1% of all of these cars would become driverless and if we very modestly assume that a car is used on average 60 minutes per day, this would provide 60 million hours per day or more than 400 million years of attention per year globally.

The availability of this amount of time will most likely see an increased demand for

personal recommender systems which might guide the passengers of the car in terms of communication, education and entertainment whilst being driven. Such concepts can already been observed in the integration of Spotify-attributes into the Uber account enabling passengers to conveniently listen to their own favorite music while being driven in an Uber car.

In order to utilize a digital identity for the scenarios that have been outlined here, it is required to being able to bring the digital identity into these interactions with real world Internet-of-Things-enabled items such as homes or cars. A prerequisite for digital security will be biometric solutions such as face, iris, fingerprint or voice recognition in order to conveniently provide authentication and access control as part of such interactions.

Where to start?

It is all nice and easy to talk about platforms that can do everything for everyone. It is more difficult to answer the question of how to build and grow such a platform. Let us explore.

A technical perspective

From a technical perspective, history has shown that making digital identity 3.0 work is not an easy feat. A consumer-empowered system like the one we described has been referred to by other researchers as a **decentralised personal data architecture** (Narayanan et al., 2012) and the first concepts for these systems emerged in the late 1990s. Many have since attempted to build and grow such a platform, but the failure of all early attempts led to dwindling interest and disillusionment.

One of the main challenges that could not be overcome relates to people owning and storing their own data, and having full control over changes and additions to the data. In such a paradigm, it is very difficult to maintain **compatibility and interoperability**—the extent to which different systems can work together effortlessly. A lack of interoperability would dramatically reduce the affordances of the private master record. Therefore, Narayanan et al. (2012) suggest that there will be a need for an intermediary, and that this intermediary will have to work with regulators and powerful industry stakeholders to work towards technical standardisation and interoperability. In other words, the full independence from an ecosystem will be difficult to achieve, but the ecosystem can guard consymers' empowerment by also being open and collaborative. Collaboration will be the key in using as well as building the platform.

Further, when users have full control, **privacy** becomes harder to safeguard. Even if your system uses state-of-the-art technical data protection measures, it cannot control what people do with their data. People are often quick to share data without sufficiently reflecting on the consequences. Therefore, Narayanan et al. (2012) recommend that not only technical privacy measures are considered, but also socio-legal approaches to privacy.

The future of privacy: don't share your data

Currently, when we share data online with an organisation or other person, we share it in the literal sense of the word: we give the other party a portion of our data and can never get it back. We lose control over it because it's a physical copy. The other party can then go on to copy this data, share it with others again, and use it for various purposes that suit them. This means that we have very little control over our data—we send it into the cloud and off it goes. The recent security breach on adultery website Ashley Madison (AM) was particularly revealing: their clients paid for a service that would let AM wipe out their data, yet still they didn't. All their personal data was still stored on their servers and got exposed when AM was attacked. In the near future, however, we may have alternatives to just giving our data away.

One option that seems attractive at first sight is making data impossible to copy. If data was impossible to copy, it would be safe to share it with third parties. Dr Soeren Balko, Open Data Markets expert at QUT, explains: "A number of robust encryption techniques are starting to emerge that can make data truly impossible to copy. Homomorphic encryption, for example, encrypts your data on you local machine. This encrypted data can be sent to a third party that can offer data analysis services that do not require de-crypting the data and will produce a still encrypted result. This result, in turn can only be decrypted or 'unlocked' by the data's owner who is in possession of the encryption key. There is one minor issue with this approach, however. If data can't be deciphered, it can't be used for many useful purposes. In other words, such a solution would give people full control and absolute privacy, but wouldn't enable any interactions, transactions or even connections to others."

An alternative consists of bringing the cloud to the data, instead of sending the data into the cloud. QUT professor Alexander Dreiling, specialised in Digital Transformation explains: "Bringing the cloud to our data sounds like it would be hard to accomplish, but the principle is actually quite simple. When organisations use our data, they run a number or queries or algorithms on our data. Usually these involve quite simple computations. Bringing the cloud to our data means running these algorithms locally, on private machines instead of in the cloud. Bringing algorithms to data means that data doesn't have to be shared." While this sounds sensible, Dr Soeren Balko warns that this is no perfect solution either. "We of course have to remain vigilant about the algorithms that investigate our data. An algorithm could simply say "copy data", which again would threaten privacy. There would have to be an intermediary or a system that inspects the algorithms that want to query personal data, and only allows those algorithms that users agree to (in general terms) and that don't contain any malicious aspects.

Finally, Narayanan et al. (2012) recommend that future endeavours explore whether there are sufficient **economical incentives** for both sides of the platform to join, and gaining deep consumer insights to find out if the problem that is being solved is actually a problem worth solving. Further, on top of the platform solving a worthy problem, it should offer the kind of value that makes people join a platform. This often means it should have features that people find exciting. All this, however, is much easier to achieve when starting small, i.e. with a minimum viable product that just works. As we will discuss in the next section, these last two recommendations are important from a social perspective too.

A social perspective

Taking a social perspective on how to build a digital identity platform calls for a reference to the classic **Diffusion of Innovations theory** (Rogers, 2003). This theory proposes that five different cohorts adopt innovations more or less successively. The first group,

Why Google+ failed

Many hypotheses of why Google+ failed have been proposed, and we have a few of our own. Instead of delivering initial value for a targeted eco system or subgroup (Edelman, 2015), Google+ targeted the masses straight away. They tapped into their existing user groups, and hoped that network effects would take no time to materialise. However, the first users to come on board (us included) quickly noticed that there was no stand-alone value over and above existing social platforms, that the mass adoption wasn't there, and that without it Google+ had no value whatsoever.

Google saw this problem and started narrowing the scope of their target group towards a niche. They attracted and marketed a number of famous photographers, i.e. 'marquee users' (Edelman, 2015), and focused on the image sharing strengths of their platform (value without network effects). By that time, however, it was to late for a niche to drive growth, because the early adopters had already been disappointed and had left the platform for dead. Google+ RIP.

Google+ RIP.

the innovators, make up merely 2.5% of the population that wants to try out the latest innovations even before they are mature. They are the beta-testers. The second group, early adopters, make up an estimated 13.5% of people. They adopt products as the products grow out of early bugs and glitches. The early majority is next, the 34% that jump on the bandwagon once the innovative product is widely known and becomes 'mainstream'. The late majority (roughly 34% again) waits for the rest of the world to lose excitement, and comes on board once the price drops or the product or service is so mainstream that it becomes hard not to participate. Laggards, finally, are those 16% of people that really don't want do adopt the innovation, but reluctantly do so eventually.

What makes or breaks **the success of platforms often lies in the early stages**, where innovators and early adopters need to find value in using the platform (Edelman, 2015); in order to become successful, a platform needs to convince more people to join the platform quickly in that first stage so network effects can emerge. It can do that by tapping into existing user groups or publicly available data, offering value even without the network created by many users, convincing really well known users to join the platform, and/or by making it cheap or even lucrative for people to join. Technically, the platform should also be compatible with existing systems that your target audience uses (Bonchek & Choudary, 2013; Edelman, 2015).

In practice, platforms often get through that first stage successfully by amassing a critical user base within a certain eco system, and by offering value-adding yet limited functionality at first. In other words, they offer value that exceeds mere privacy—or any other hygiene factor—and with a minimum viable product (Narayanan et al., 2012). The first 'mass' adoption of Airbnb, for example, happened within a specific niche: people that needed accommodation in San Francisco to visit large events and conferences. A sufficient number of people from this specific group and with that specific purpose adopted the platform, which allowed it to spread to a wider eco system: San Francisco as a whole. Only then did true network effects and exponential growth begin. The excitement factor consisted of people not only getting a bed to sleep in, but a localised cultural experience as well. The fact that it was so easy and more affordable didn't do any harm. In summary, the key seems to be to start within a niche and with a specific purpose, deliver stand-alone value to the innovators and early adopters within the targeted subgroup, and let maturity and functionality grow with the user base.

Conclusion

In summary, Digital Identity 3.0 is a platform that puts customers in charge of their data, integrates that data into an evolving and comprehensive representation of their digital and physical world, allows people to share that data selectively in order for the platform to pull proactive services towards them, and unlock new experiences as they connect to their world in new and exciting ways.

The fine print: digital identity concepts in a nutshell

An **identity**, in the narrow sense of the word, is "an abstract (mental) picture of an entity, such that […] an entity's identity is logically equivalent to the physical presence of this particular entity" (Glässer & Vajihollahi, 2010). In other words, an identity is a non-physical representation of a physical person or thing.

Accordingly, a **digital identity** is a digital representation of a person or a thing. For a person, such a digital identity can include a whole range of attributes.

Attributes are qualities or characteristics that are considered to belong to or describe a person or thing. Attributes can vary along a number of dimensions. Closest to the physical, unique identity of a person and least dynamic are attributes are demographics such as someone's name, birthday and -place, and physical properties such as fingerprints, iris and genetic code (Glässer & Vajihollahi, 2010). These are typically attributes that are stable and uniquely linked to you. Other attributes are more dynamic, such as attributes related to one's physical and mental health and fitness. More dynamic again are attributes related to activities and behaviour—both online and offline—and the assets that someone owns. Examples of assets are someone's house, car, savings, etc..

Increasingly, however, people do not have one, but a myriad of digital representations that each describe part of who they are. These subsets of personal data are generally referred to as **partial identities** (Clauß & Köhntopp, 2001) and are made up of purposefully or logically clustered attributes. Examples of partial digital identities include the digital representation of a person's work identity, a person's leisure

identity, etc. (for examples, see Figure 2). Some of these identities are unique to one person and allow a person to be unambiguously identified (Clauß & Köhntopp, 2001). Other partial identities will be more generic or share characteristics with other peoples' identity and will vary in the degree to which they allow identification (Satchell et al., 2006). Non-unique partial identities are generally linked to pseudonyms.

Pseudonyms act as identifiers and keep partial identities from being completely anonymous—i.e. not (re-)identifiable (Clauß & Köhntopp, 2001). Pseudonyms will vary in their divergence from reality; some pseudonyms may be very close to anonymity, while others may allow people to be identified (e.g. your work email). Pseudonyms share five key characteristics: (1) whereas pseudonyms do not allow a person to be fully identified, they are still held by one person only. This means that, initially, (2) a person will have to reveal part of its real identity to obtain the pseudonym. (3) The same pseudonym can be used across different contexts, and these different uses can be linked because the pseudonym is identifiable. Not only the pseudonym, but (4) attributes of pseudonyms can be shared across contexts as well. Moreover, sharing of attributes does not necessarily require revealing the pseudonym. Finally, (5) attributes of partial identities can be authorized by third parties—with or without revealing the full identity or pseudonym.

This last point in particular is an interesting one. With the rapid growth of the sharing economy and the uptake of digital services by organizations and governments alike, the **authorization** of attributes of pseudonyms and autonyms becomes increasingly important (The Global Identity Foundation, 2013). The authorization of an attribute, in the context of digital identity, refers to the acknowledgement by a trusted party that an attribute of a person or thing is real and belongs to the person of thing the attributed has been linked to. Who that trusted party is depends on the attribute. For a degree, for example, the trusted party may be a university.

Authentication, finally, is using attributes to establish confidence in an identity. The nature of these attributes and how they are to be supplied depends on the level of assurance the authenticating party requires. For non-critical interactions or transactions, a simple password is generally sufficient; this is an example of a knowledge factor. You prove knowledge of a secret that only you should know, which gives the other party trust that they are dealing with you. Transactions that require more assurance generally require multi-factor authentication. A typical example is the use of a code that is sent to you by SMS. On top of something you know (password), you also prove ownership over something (a mobile device) that is linked to the identity you are using to authenticate. And remember, this identity can be a pseudonym—authentication does not necessarily require you to reveal your full identity.

References

BBC News. (2015). YouTube gaming star PewDiePie 'earned $7m in 2014'. Retrieved 23 August, 2015, from http://www.bbc.com/news/technology-33425411

Bonchek, M., & Choudary, S. P. (2013). Three Elements of a Successful Platform Strategy. Harvard Business Review, January 2013.

Choudary, S. P. Why Business Models Fail: Pipes vs. Platforms. Platform Thinking. Retrieved 20 August, 2015, from http://platformed.info/why-business-models-fail-pipes-vs-platforms/

Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. Computer Networks, 37(2), 205-219.

Edelman, B. G. (2015). How to Launch Your Digital Platform: A Playbook for Strategists. Harvard Business Review, 93(4), 90–97.

Eisenmann, T. R., Parker, G., & van Alstyne, M. (2006). Strategies for Two- Sided Markets. Harvard Business Review, 84(10).

Frey, C. B., & Osborne, M. (2013). The Future of Employment: How Susceptible are Jobs to Computerisation? Oxford Martin School. Retrieved from http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

Gimpel, G., & Westerman, G. (2012). Shaping the future: Seven enduring principles for fast-changing industries. Working papersOctober. MIT Center for Digital Business. Retrieved from http://bit.ly/1Px2COl

Glässer, U., & Vajihollahi, M. (2010). Identity Management Architecture. In M. C. C. C.C. Yang, J.-H. Wang and H. Chen (Ed.), Security Informatics, Annals of Information Systems (pp. 97–116): Springer.

Maler, E. (2009). The design of everyday identity. Online Information Review, 33(3), 443-457. doi: 10.1108/14684520910969899

Mitchell, A., Henderson, I., & Searls, D. (2008). Reinventing direct marketing -- with VRM inside. Journal of Direct, Data and Digital Marketing Practice, 10(1), 3-15. doi: http://dx.doi.org/10.1057/dddmp.2008.24

Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., & Boneh, D. (2012). A Critical Look at Decentralized Personal Data Architectures. Retrieved from http://arxiv.org/abs/1202.4503

PwC Chair in Digital Economy. (2015). Digital Economy: Our Perspective Working Paper no 1.

Rogers, E. M. (2003). Diffusion of Innovations, 5th Edition: Simon and Schuster.

Satchell, C., & Foth, M. (2008). The Re-creation of Identity in Digital Environments and the Potential Benefits for Non-Profit and Community Organisations. 3C Media(4), 16-27.

Satchell, C., Shanks, G., Howard, S., & Murphy, J. (2006). Beyond security: implications for the future of federated digital identity management systems. Paper presented at the 20th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artefacts and environments, Sydney.

Satchell, C., Shanks, G., Howard, S., & Murphy, J. (2011). Identity crisis : user perspectives on multiplicity and control in federated identity management. Behaviour and Information Technology, 30(1), 51-62.

The Global Identity Foundation. (2013). Global Identity: Challenges, pitfalls and solutions. Retrieved 19 August, 2015, from http://www.globalidentityfoundation.org/downloads/Global_Identity_Foundation_-_Identity_White_Paper_v1.0.pdf

Trkman, P., Mertens, W., Viaene, S., & Gemmel, P. (2015). From business process management to customer process management. Business Process Management Journal, 21(2), 250-266. doi: doi:10.1108/BPMJ-02-2014-0010

Weill, P., & Woerner, S. L. (2015). Thriving in an Increasingly Digital Ecosystem. MIT Sloan Management Review, 56(4), 26-34.