The Rise of The Attribute Economy 2.0

meeco

Attribute

In computing, attributes are pieces of information, which determine the properties of a field or tag in a database, or a string of characters in a display.

In more human terms, attributes are qualities, features, characteristics or inherent parts of someone or something.

In The Attribute Economy, these attributes often represent human beings. They are individual characteristics such as age, gender or education level. They are also characteristics that give context to someone’s life, such as browsing history, financial information, emails and messages, health records and social media profiles.

Soon these attributes, rather than being exchanged in the background without people’s full knowledge, will be exchanged on the explicit terms of the person they relate to.

This is the Attribute Economy 2.0.

Contents

Contributors

Katryna Dow
Founder & CEO, Meeco

Nathan Kinch
Head of Experience and Labs - Meeco

Richard Gomer
University of Southampton, Meaningful Consent in the Digital Economy Project

Rob Lawrence
Director – Innovate Identity

Dr. Rachel O'Connell
Director – Trust Elevate

Joss Langford
Director - Coelition

Mark Lizar
Director – Open Consent Group

James Harvey
Head of Design - Yoti

Joerg Resch
Managing Director – KuppingerCole

The Rise of The Attribute Economy 2.0

Foreword

Here we are, almost twenty per cent of the way into the 21st Century. Since the year 2000, amazing things have been accomplished in technology, science and transport. We have witnessed the rise of social networks and the emergence of Internet of Things. These changes herald our advancement towards the connected everything. Technology has escalated innovation across society, fuelled by the global economic crisis that began around 2007, together with increasing environmental changes, we have witnessed new capabilities in finance, robotics, auto manufacturing and energy.

Yet, whilst we have found a way to socially connect 1.6 billion people, we haven't seen participation, consumption and business models keep pace or evolve in parallel. As the planet began to connect across networks, the only business model we came up with was more ways to advertise more stuff.

Katryna Dow
Founder & CEO, Meeco

Katryna Dow is the founder and CEO of Meeco. Katryna has subject matter expertise in strategy, psychographic segmentation, neuro-economics and change management. She co-founded the Zemu think tank and incubator, founded Meeco and MeCast, speaks globally on privacy and data innovation, and consults to leading enterprise and governments on business model innovation and new value chains through Meeco Me2B Labs

We didn't take the time to understand all the possibilities a networked society could enable. The millions and millions of ways tiny bits of value could be created, recorded, attributed and collected through these new chains of connection and value. We haven't worked out yet how to make the digital world private and safe, whilst staying open and secure.

However, I believe we are on the brink of all this changing.

We still haven't figured out that the family that wants to buy 'the' hybrid car today is worth so much more to Toyota than the 15,000 bots that will click the Google ads that the Saatchi team has worked around the clock to design and deploy. We don't yet understand the efficiency uplift of our refrigerators ordering our food or our Nespresso self-stocking its own pods.

In the not too distant future, arriving home will mean discovering what ‘things’ our ‘things’ have ordered and had shipped because their sensors sensed stocks were low, prices were good or our calendars knew friends were expected on the weekend.

More importantly, we don’t yet understand the implications of what happens when our refrigerator and coffee machine talk to our electricity providers. Will we end up with the advertised decrease in health insurance cover, or will our device manufacturers sell us out to higher policies for the kick back they get from our data?

> “I believe that personal data controlled by individuals will revolutionise the creation of new value, in the same way just-in-time transformed manufacturing”

We need to start thinking about data as an asset, every bit as valuable as a critical part in a manufacturing line, a currency to complete a transaction or vital information to enable a decision.

If we begin to reframe the use of personal information as an asset to accelerate industry, commerce, education, health and finance it will free up a powerful new-networked economy, where the value of data will be realised as both an asset and an annuity.

However, up until now, what have been missing are the legal rights, business models and technologies to enable this.

The good news is that we are beginning to see this change. The governance and market-regulating factors are beginning to come into play for personal data, affording us the protections and rights of an asset class, like property and currency.

That’s exactly what needs to happen now.

But first, we need to understand and put in place the techno-legal frameworks to accelerate this market. In simple terms, we see the following steps are giving rise to the business model innovation that will lead to the evolution of our society, empower an emerging generation and make the things of the past no longer acceptable.

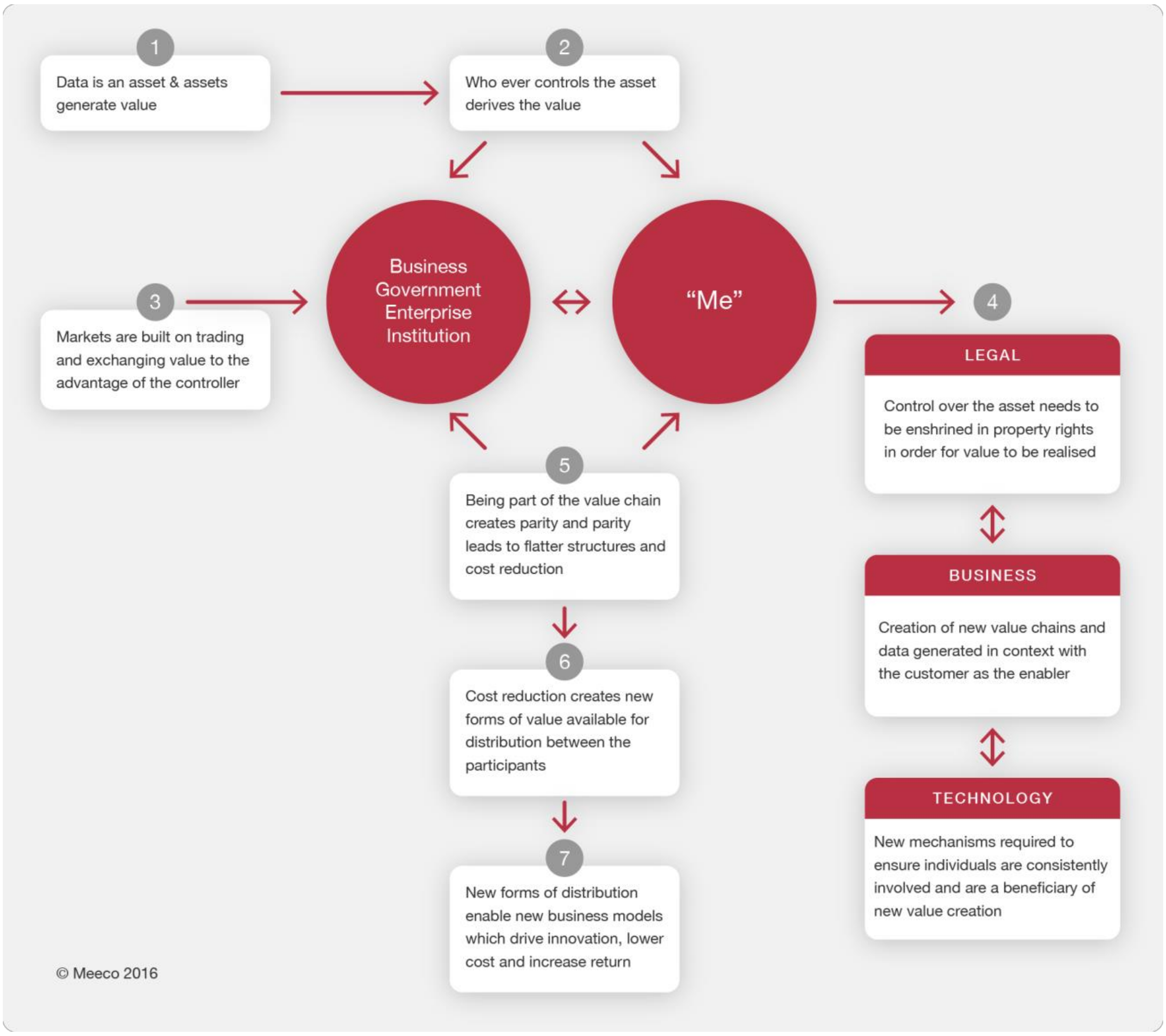

1
Data is an asset & assets generate value
2
Who ever controls the asset derives the value
Business
Government
Enterprise
Institution
"Me"
3
Markets are built on trading and exchanging value to the advantage of the controller
4
LEGAL
Control over the asset needs to be enshrined in property rights in order for value to be realised
BUSINESS
Creation of new value chains and data generated in context with the customer as the enabler
TECHNOLOGY
New mechanisms required to ensure individuals are consistently involved and are a beneficiary of new value creation
5
Being part of the value chain creates parity and parity leads to flatter structures and cost reduction
6
Cost reduction creates new forms of value available for distribution between the participants
7
New forms of distribution enable new business models which drive innovation, lower cost and increase return
© Meeco 2016

Figure 1 – The Path to New Value
© Meeco Planet, 2016

We at Meeco see a clear path forward to a new marketplace, one that is based on transparency, opt-in and trust. We believe the hallmark of a future proof organisation will be the willingness to share the data it collects about its customers directly with them for mutual value.

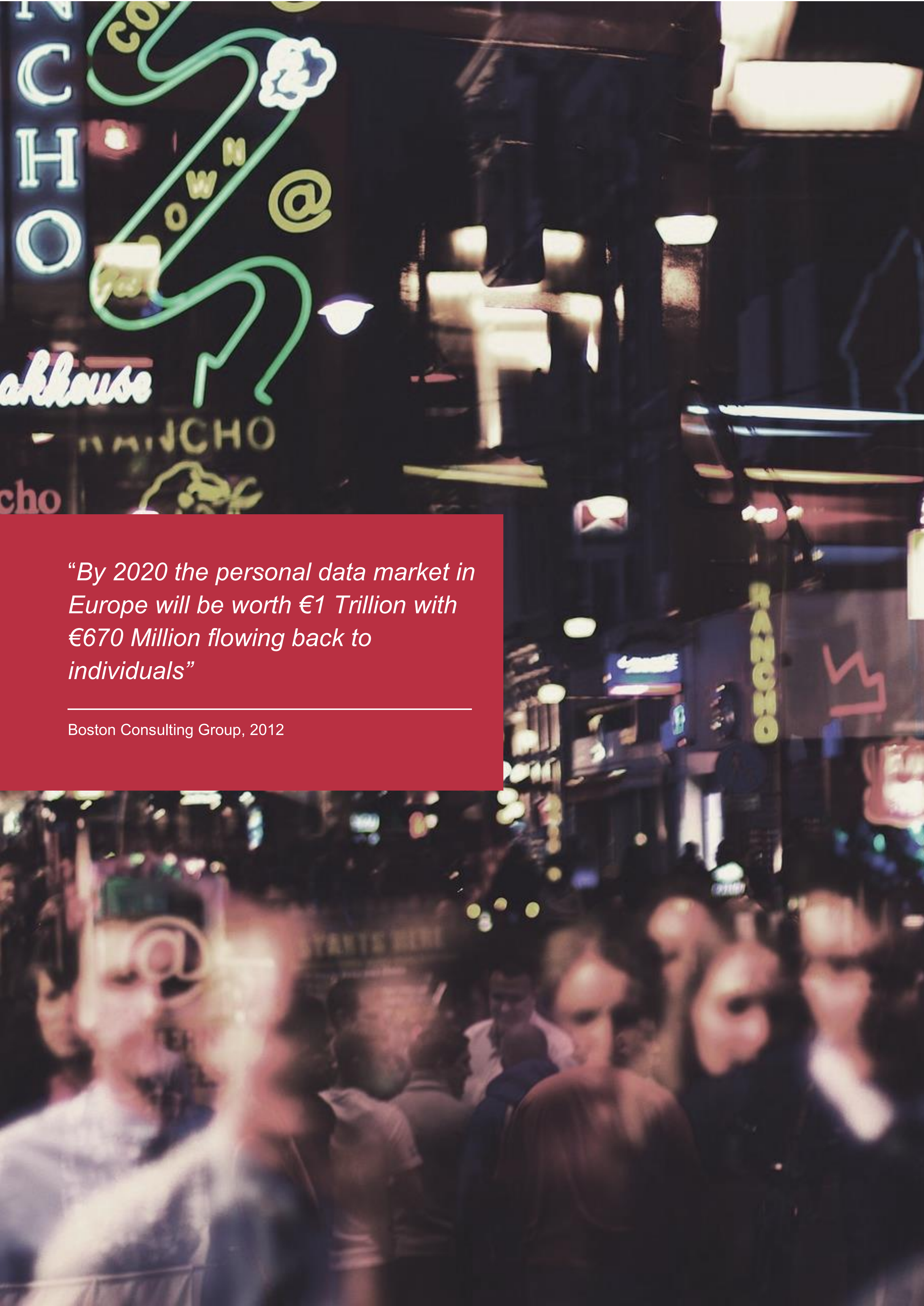
The good news is that all the research indicates that transparency actually leads to people sharing more data rather than less, providing they understand why it is being collected and how it is used. This is the basis of network economics and the ‘Attribute Economy’.

I would especially like to acknowledge the co-authors of this Paper; Nathan Kinch, Richard Gomer, Rob Laurence, Dr Rachel O’Connell, Joss Langford, Mark Lizar, James Harvey and Joerg Resch. Their combined expertise made this paper possible.

This paper focuses on the emerging single digital market in Europe. Our contributors are all leading thinkers in the fields of identity, research, market analysis, standards, protocols and user experience design. This convergence of thinking includes the important work of the past decade, demonstrating how that foundation is now accelerating personal tools that will enable each of us to participate on our terms in the digital economy.

We trust the following research, case studies and insight will help you and your organisation understand the opportunities to build and benefit through greater trust and transparency in the Attribute Economy 2.0.

Katryna Dow
February 2017



“By 2020 the personal data market in Europe will be worth €1 Trillion with €670 Million flowing back to individuals”

Boston Consulting Group, 2012

Introduction and Purpose

Nathan Kinch, Head of Experience and Labs - Meeco

For the past decade, personal data has been the fuel of the digital economy, yet people – the data subjects - have not participated in the direct value realisation of these economic models. Residing in aggregate form on the balance sheets of large corporations and within governments' deep silos, the potential for accurate personal data, real-time, in context and matched with intention, has not yet been realised.

However much of this is now changing. People are gaining power. The capabilities to support explicit consent and permissioned use of our personal data now exist.

Nathan Kinch
Head of Experience and Labs - Meeco

Nathan is Head of Experience and Labs at Meeco where he leads global experience strategy, as well as execution of Meeco Labs across Europe. Prior to this Nathan managed product innovation portfolios for large corporates in Australia, and was founding CEO of a sports analytics start-up. In a previous life he was also an elite golfer.

The societal and economic impact of this power-shift is significant. Liberty Global and The Boston Consulting Group estimate that by the year 2020, the use of citizen-controlled Digital Identity, (if trust and transparency are established), represents a trillion euros of new economic value in Europe alone.

> "People are gaining power. The capabilities to support explicit permissioned use of our data now exist"

The purpose of this White Paper is to introduce the Attribute Economy 2.0, whilst exploring the societal and economic implications of an Attribute Economy controlled largely by the people the attributes pertain to.

This Paper showcases the insight of peers who are working to make the Attribute Economy 2.0 a desirable, viable and feasible reality. Thought leaders from KuppingerCole, digital identity specialists such as Innovate Identity and Trust Elevate, open standards bodies such as Coelition, consent experts from the Open Consent Group and person first technologies such as Yoti have all contributed to support a holistic view of this shifting market.

The Attribute Economy 1.0

The Attribute Economy 1.0 is a global marketplace of data buyers and sellers, and a highly lucrative environment. Entire businesses, and in fact, industries have been built from a core capability to acquire various personal attributes and exchange those with other organisations for a fee.

However, within this model, consumers (we) have participated through access to 'free' services. Unlike the cartoon, what we've come to realise, is that free comes at a price.

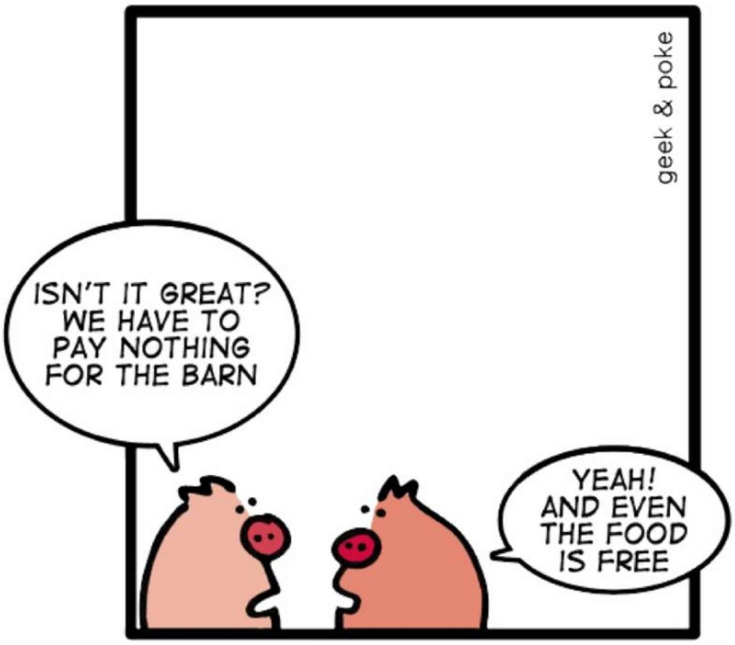

geek & poke
ISN'T IT GREAT? WE HAVE TO PAY NOTHING FOR THE BARN
YEAH! AND EVEN THE FOOD IS FREE

Figure 2: "Pigs eat free" – Geek & Poke

Have you ever given thought to the impact your 'private' Facebook profile might have on your life? How about the friends you are connected to on Facebook? What about the things you post about your kids? Have you ever wondered if those photos or posts will have an impact on their lives?

Well Facebook[1] certainly have, filing a patent that would effectively enable them to provide information about your friends to banks so that an average credit rating can be calculated, and used to assess your loan application. But they[2] aren't alone. Entire industries have[3] been built using our personal data as the raw material.

Currently, everything we do online is captured and fundamentally says something about us. Whether or not the inference drawn is 'right or wrong' doesn't matter all that much to those tracking.

[1] Could A Bank Deny Your Loan Based on Your Facebook Friends? – The Atlantic, Sep 25, 2015

[2] A Data Broker Offers a Peak Behind the Curtain – New York Times, Aug 31, 2013

[3] What Are Data Brokers – And What Is Your Data Worth [Infographic] – WebpageFX, Apr 15, 2015

However, what does matter is that our attributes are used to our benefit[4] but also to our detriment; in ways that we may not be fully aware[5] of.

So how lucrative is this model? In 2015, Facebook[6] made $13.54 in revenue per US and Canadian user. Granted this doesn't sound all that impressive, but when you multiply this number by the user base, it's fairly staggering.

In another example, as part of the 'Economics of Identity' series, OIX[7] released a white paper detailing the ARPU (Average Revenue Per User) potential for Telecommunications companies[8] if identity provision were to become an ancillary service offering. In this paper, they highlighted, at depth, the multi-billion-dollar opportunity associated with the use of our identities in the U.S. alone. The big upside of this model is that OIX promote people being in control of their personal information and having agency of their identity. The telco in this example becomes the custodian, the pathway towards new trust building and transparent services.

Lastly, here's what our personal data could be worth[9] on the black market. As a general rule, it probably fetches around $20. However, the rising cost of lead generation across sectors such as health, insurance and automotive, demonstrate the fierce competition for personal data.

Although these serve as high-level examples only, they speak volumes to the nature of the current Attribute Economy. Little agency exists within a business model of which we are the product.

[4] How corporate data brokers sell your life, and why you should be concerned – The Stack, Aug 24, 2015

[5] Revealed: the 10 worst apps for taking personal details without letting you know – Mail Online, Jan 16, 2013

[6] How much are you worth to Facebook? – Guardian, Jan 28, 2016

[7] The Economics of Identity – Open Identity Exchange, May 19, 2014

[8] The Name is the Thing: "The ARPU of Identity" – Open Identity Exchange, Oct 17, 2014

[9] Here's what your stolen identity goes for on the internet's black market – Quartz, July 23, 2015

A Convergence of Trends

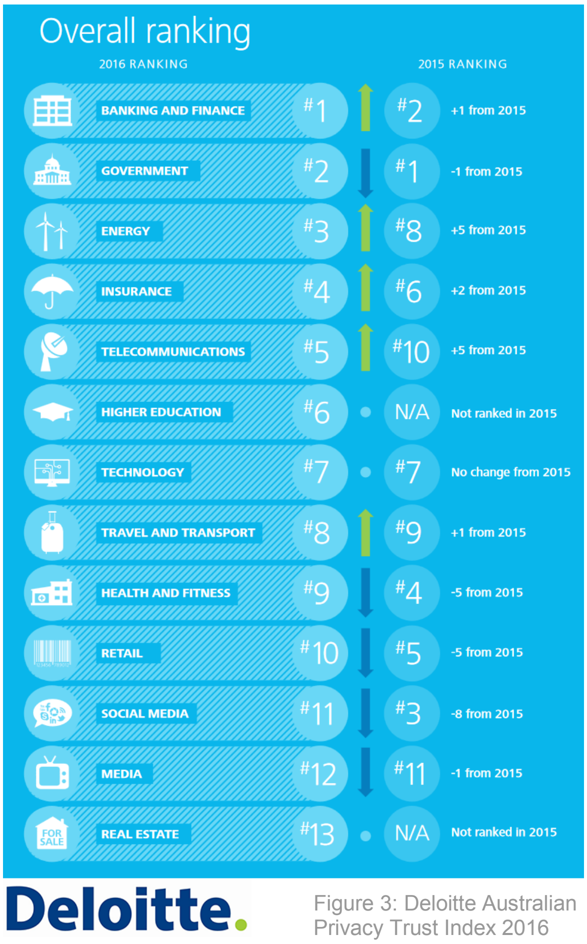
Attitudes, Sentiment and Behaviour

The Attribute Economy, in its current state, particularly as a mechanism for driving advertising revenue, faces an existential threat.

Deloitte's Australian Privacy Trust Index 2016[10] highlighted this, showing social media's move from being the third most trusted category, to near the bottom of the entire list.

This significant shift in consumer sentiment aligns closely to the state of mistrust and increase in awareness around data practices and related incidents.[11] As this has taken place, people globally have been taking action, which is demonstrated through the rise of Adblocking technology[12].

Now over 400 million people have installed Adblockers on their devices. With no signs of this slowing, there is also a call to arms for organisations to [13] modernise their approach to privacy.



Overall ranking

2016 RANKING			2015 RANKING	
BANKING AND FINANCE	#1	↑	#2	+1 from 2015
GOVERNMENT	#2	↓	#1	-1 from 2015
ENERGY	#3	↑	#8	+5 from 2015
INSURANCE	#4	↑	#6	+2 from 2015
TELECOMMUNICATIONS	#5	↑	#10	+5 from 2015
HIGHER EDUCATION	#6	●	N/A	Not ranked in 2015
TECHNOLOGY	#7	●	#7	No change from 2015
TRAVEL AND TRANSPORT	#8	↑	#9	+1 from 2015
HEALTH AND FITNESS	#9	↓	#4	-5 from 2015
RETAIL	#10	↓	#5	-5 from 2015
SOCIAL MEDIA	#11	↓	#3	-8 from 2015
MEDIA	#12	↓	#11	-1 from 2015
REAL ESTATE	#13	●	N/A	Not ranked in 2015

Figure 3: Deloitte Australian Privacy Trust Index 2016

Privacy by Design is becoming more and more mainstream whilst trust is becoming a viable business strategy[14]. To put it simply, the market is beginning to move.

[10] Deloitte Australian Privacy Index 2016– Deloitte,2016

[11] Huge rise in hack attacks as cyber-criminals target small businesses – Feb 8, 2016

[12] 2016 Mobile AdBlocking Report – PageFair, May 30, 2016

[13] Why you should bet big on privacy – TechCrunch, May 17, 2016

[14] Trust as a Strategy – Digital Catapult Centre, May 9, 2016

Choices in the Dark

Richard Gomer, University of Southampton

Each security breach and perceived misuse of data undermines public confidence in the companies that collect, process and broker our personal data. We don’t read the small print or really understand what is happening to our personal information. Worse, research shows that even if we do read the small print, it often doesn't help to inform or even reassure[15]

Something is fundamentally wrong: Our world is not just increasingly complex and automated; it seems it is also increasingly unintelligible to citizens. It breeds mistrust and disempowers us in a way fundamentally incompatible with our hard-won notions of freedom and autonomy.

Richard Gomer
University of Southampton
Meaningful Consent in the Digital Economy Project

His work, and the work of the project, examines issues of consent and citizen empowerment with relation to digital technologies through the development of appropriate, meaningful interaction mechanisms and design. Originally a computer scientist, Richard's research now also spans psychology, behavioural economics and law. He dreams of a world where people are helped to understand technology and to know what's happening with their personal data.

> “We don’t read the small print or really understand what is happening to our personal information”

Even the old trope of the privacy 'paradox' is starting to crumble. Many researchers, industries and even regulators have long maintained that citizens don't protect their privacy because they just don't care, that privacy is dead and that we need to collectively get over it.

Instead, it seems like consumers are actually just making choices in the dark, with no insight into the extent to which their decisions today will impact the things that they care about at some point in the future.

This is a bigger question than 'just' privacy – although privacy is a useful concept – it's a question about how the complexity behind the services we engage with, mixed with the data they collect and process about our own social context and us might

[15] Marreiros, Helia, Gomer, Richard, Vlassopoulos, Michael, Tonin, Mirco and schraefel, mc (2016) Scared or naïve? An exploratory study on users perceptions of online privacy disclosures, IADIS International Journal on WWW/Internet,13, (2),1-16.

alter our lives in potentially unforeseen ways.

One thing that is increasingly clear, though, is that the uncertainty over what services are doing, and what the consequences of that might be, is a limiting factor in the adoption of new services and sources of value[16] Not only are the stakes higher than before but also many people feel that the companies themselves are fundamentally less trustworthy.

Consumer behaviour will increasingly be shaped by their misgivings about new digital services, rather than the opportunities, until the industry is able to start inspiring trust rather than eroding it.

The True Cost

Nathan Kinch, Head of Experience and Labs - Meeco

So, is there an economic motivator to inspire trust?

In a 2015 study[17] conducted by Meeco, the true cost to businesses and consumers of the current Ad Tech market was explored. The study found that over a period of one quarter, across two Google product lines and five industry sectors:

- 12.78 billion people were served online advertisements
- 0.018% of these were 'converted' into leads (not transactions)
- 12.5 billion ads were served to an uninterested audience
- The direct cost to brands resulting from this was $104.5 Million USD

The race to install Adblockers and the rapid decline in consumer trust around the use of personal data should come as no surprise.

The real question here; is this is a threat or an opportunity?

[16] Trust in Personal Data: A UK Review, Digital Catapult 2016
[17] Online Advertising: Booming or Broken, Meeco, Sep 2015

The Impact of Digital Identity

Rob Lawrence, Director – Innovate Identity

Enabling us to be in control of and to share our personal data has the potential to truly transform those costly and difficult to fulfil services. Knowing who is sharing their attributes at the outset of the service can change the way digital services are delivered and potentially remove costly back office processes, often put in place because the organisation does not know with confidence who we are.

Take, for example, an application process for a financial product. How many organisations have created an online process that mimics the paper process? Well, most really. How many organisations can accept our applications in real time? Close to none is the reality. There are always additional checks that have to take place, some of which often involve us submitting further information offline.

Rob Lawrence
Director – Innovate Identity

Rob is a thought leader in digital transformation and experienced senior leader with a proven history of taking new innovations to market. He built a new division at GBG plc and took to market the UK's first purpose built electronic identity verification service, growing revenue from zero to £11 million+ in 5 years. Rob advises clients on strategy, best practice in identity and compliance

> "How many organisations create online process that mimic paper processes?"

Why? Well, first of all the organisation doesn't know 'I am really who I say I am'. Second, when the organisation establishes who 'we' are, it is then required to check it is allowed to accept 'us' as a customer. Third, if lending or the provision of credit facilities is involved, the organisation has to establish the risk involved and that 'we' have the means to meet repayments. These processes are long-winded and expensive.

In the 15 years or so since Internet banking emerged, nothing much has changed. Identity checks are carried out by effectively mimicking face-to-face checks of government-issued documents, financial statements and utility bills online, by referencing document numbers and personal details and cross-checking these with many different data sources.

To compound these constraints, consumer credit checks have scarcely changed in two decades. This results in organisations being completely locked in to 3rd party services having built complex scoring models tuned for their business – probably just as they existed 20 years ago.

Even when there is a long-standing relationship in place, fraud mitigation and prevention checks are built in throughout the process because, at no stage, can organisations be sure 'who' they are dealing with.

"Even though I have been a customer of the bank for more than 40 years, my debit card still gets blocked from time-to-time"

So how can organisations establish with confidence 'who' we are, online? And if they were able to build a level of confidence and trust, can that trust be extended to additional information, such as our credit reports, rather than going to a data aggregator of all our financial history?

As for us, how can we trust organisations with our data? Can we be sure someone won't pretend to be 'you or I' in order to gain access to services or make payments in our name?

"A digital identity, trusted by all parties may be the answer"

Digital identities exist all around us. We use them every day; with our banks, our mobile phone companies, Google, Apple, Facebook, PayPal and Amazon. But the drawback is we have many digital identities and are generally unable to share them across organisations or eco-systems.

The root problem is trust. Trust in how it was created. Trust in how secure it is. If we can solve the issue of trust, only then can we begin to change these antiquated processes.

An Evolving Ecosystem

At the start of the decade, a number of countries in Europe focussed on building the trust infrastructure to enable the emergence of a single digital economy. The European Commission took a strategic approach to catalyse the development of an interoperable, Pan-European identity ecosystem, which, by extension, is leading to the growth of the Attribute Economy 2.0.

However, in order for the Attribute Economy 2.0 to flourish it needs to solve, at a global scale, the problem of establishing attribute based eligibility to either access, purchase or otherwise interact with services both on and offline.

In recent years, we have seen the emergence of digital identity schemes at national levels. In Norway and Sweden, it has been the banks that have taken the lead to create a digital identity scheme that subsequently became accepted by government. BankID in Sweden has 6.5 million active users in a population of 9.7 million.

In Germany and Estonia, it is the government that has introduced digital identities by effectively extending existing identity card schemes. In the United Kingdom, the government and the private sector have collaborated to design a federated digital identity scheme that is now live across a growing number of government services. Moves are underway to extend its use to the financial services sector.

For us, as individuals, there are clearly benefits in having a single digital identity that could be used with a wide range of government and private sector services. However, for organisations, there are difficult issues to be resolved before the benefits can be realised; such as how to maintain trust in the ecosystem? If something goes wrong who is liable? What is the commercial model?

Nevertheless, progress is slowly but surely being made and when rather than if its adoption grows, then we'll see this as a key step to unlocking the attribute economy.

“Public scepticism and lack of trust endanger digital business models”

Dr Claus D. Ulmer, SVP, Global Data Privacy Officer, Deutsche Telekom AG, Brussels November 2016

Digital Agenda

Dr. Rachel O’Connell, Founder & CEO – Trust Elevate

In 2010, the European Commission crafted the Digital Agenda, a strategy document that outlines one of the main objectives of the European Union, which is to develop a Single Digital Market in order to generate smart, sustainable and inclusive growth in Europe.

Critical to the operation of a digital single market is a secure identity layer, which enables citizens and businesses to be able to trust that their data is managed in accordance with the data protection legislation.

The document set a series of goals to be met by 2020, which included the development of interoperable electronic identity ecosystems. An identity ecosystem adds a layer of security, aimed at reducing identity theft and simplifying the user experience for various types of electronic transactions.

Dr. Rachel O’Connor
Founder & CEO
Trust Elevate

Dr Rachel O’Connell, is one of the preeminent authorities on electronic identification and age verification. Rachel’s PhD focused on online criminal activity and the implications for investigative strategies. She is the former chief safety officer of BEBO, one of the first mainstream social media platforms and speaks frequently at technology events on all issues related to online identity be it age verification or how large technology companies should engage more on child protection issues online.

Crucially, unlike other regions of the world, there is a long tradition of identity documents in Europe, for example the shape and size of identity cards were standardised[18] in 1985. During the UK Presidency of the EU in 2005, the office put forward a proposal for the EU-wide use of biometrics in national identity cards.

A decision was made to “agree common standards for security features and secure issuing procedures for ID cards”

A decision was made to “agree common standards for security features and secure issuing procedures for ID cards”, with detailed standards agreed as soon as possible thereafter.

[18] Standardisation of Identity Cards determined in 1985 by ISO/IEC 7810

Modern identity documents are smart cards including a difficult-to-forge embedded integrated circuit, which were standardised[19] in 1988. New technologies allow identity cards to contain biometric information, such as photographs, face, hand, iris measurements or fingerprints.

Various countries across Europe have rolled out national electronic identity systems. This includes the technical infrastructure to supports the mutual recognition of electronic identity cards, (eIDs) by different member states. This initiative was designed and developed under the auspices of the Secure idenTity across bOrders linKed project known as STORK.

The aim of the STORK project was to establish a European eID interoperability platform that allows citizens to establish new e-relations across borders, just by presenting their national eID. Cross-border user authentication for such e-relations was applied and tested by the project by means of five pilot projects that used existing government services in EU member states. As a result, eIDs are already available in some countries including Belgium, The Netherlands, Portugal and Denmark.

Belgium, where everyone above the age of 12 is issued an identity card, and from the age of 15 carrying this card at all times is mandatory. Since 2000, all newly issued Belgian identity cards are eID cards that can be used both in the public and private sector for identification and for the creation of legally-binding electronic signatures

The Netherlands. Dutch citizens from the age of 14 are required to be able to show a valid identity document upon request by a police officer or similar official. These identity documents are required when opening bank accounts and when taking up a position with a new employer

Portugal. All Portuguese citizens are required by law to obtain an Identity Card by six years of age. They are not required to carry it at all times but are obligated to present them to the lawful authorities if requested. From the electronic point of view, the cards have a contact chip, with digital certificates (for electronic authentication and signature purposes)

Denmark, where the National Health Insurance Card is issued to all citizens aged 12 and above. It is commonly referred to as an identity card despite the fact that it has no photo of the holder. The card states your name, address and the address of your doctor. It also carries the municipality that issued the card and the date from which the card is valid

Figure 4: Countries with available eIDs

[19] Embedded integrated circuit standardised 1988 by ISO/IEC 7816

International Standards and Interoperability

The STORK project developed internationally recognised standards that support the process of the interoperable technical architecture that supports the Pan-European identity ecosystem. Organisations that adhere to these standards when leveraging similar technical architectures will be in a position to adapt technology and policy innovation to meet specific business requirements for attribute checks.

It is expected that the next steps will involve additional service providers connecting to the platform, thereby increasing the number of cross-border services available to European users. The vision is that, for example, an EU citizen will be able to start a company, get a tax refund or obtain university papers without physical presence; all a citizen will need to access these services is to enter their national eID, and the STORK platform will obtain the required guarantee (authentication) from the relevant public body.

Electronic Identification and Signature - eIDAS

The eIDAS regulation was adopted in July 2014 to provide a predictable regulatory environment, together with mutual recognition of electronic identities[20] across Europe, enable secure and seamless electronic interactions between businesses, citizens and public authorities.

eIDAS create a European internal market for electronic trust services, namely electronic signatures, electronic seals, time stamps electronic delivery service and website authentication

This regulation ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.

Only by providing certainty on the legal validity of all these services, businesses and citizens will use the digital interactions as their natural way of interaction.

[20] Regulation (EU) No910/2014 on electronic identification and trust services for electronic transactions in the internal market, eIDAS, was adopted by the co-legislators on July 23, 2014

Creating a predictable legal framework is critical for the adoption by businesses and citizens of eIDs to safely access services, do transactions online and across border in just one click.

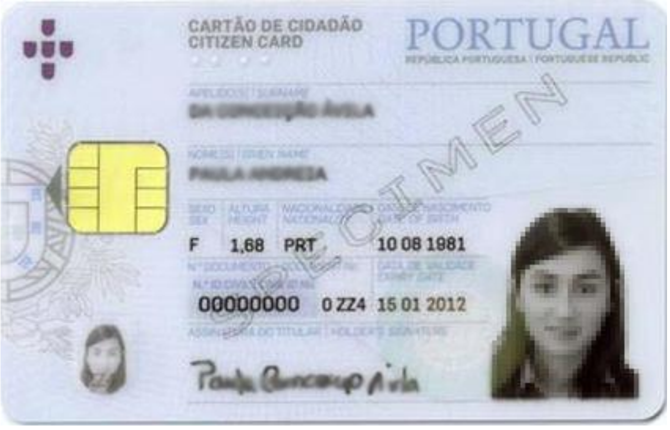


Figure 5: Portuguese eID

These methods provide higher security and more convenience for any online activity, such as submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, or setting up a business in another Member State. This is also fuelling massive rates of technology innovation in the identity sector. Innovations aiming to afford the same levels of security and convenience for customers wishing to transact with businesses, leading to commentators describing identity as the new oil of the Internet.

Use Case: UK Government Identity Ecosystem

One of the recent identity ecosystem developments was designed by the UK Government to enable citizens to transact with eGovernment services. In the UK, the Cabinet Office's Government Digital Services (GDS) team, in partnership with the private sector, has developed Gov.UK Verify (see Figure 6), which is an example of an identity ecosystem.

The purpose of Gov.UK Verify is to enable UK citizens to transact with UK eGovernment Services by enabling reliable and secure online identity verification of a citizen wishing to, for example, file a tax return or apply for benefits online. Similar initiatives are being developed around the world, for example, the USA NSTIC program. A UK citizen wishing to file a tax return or apply for a pension needs a convenient way to prove online that they are who they say they are, which is now possible via GOV.UK Verify.

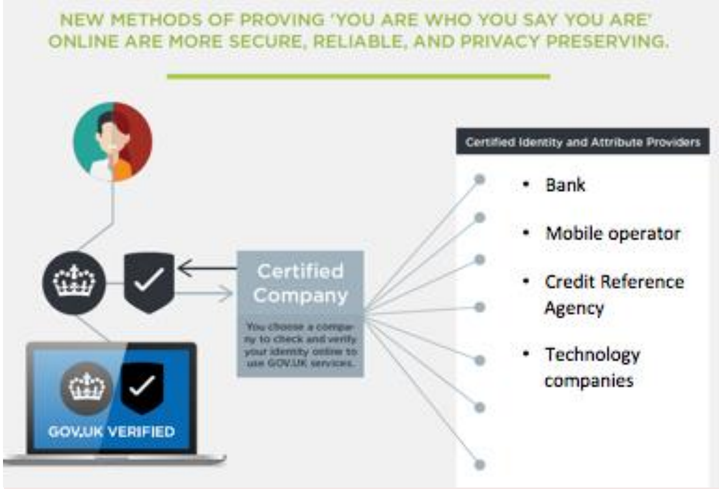

NEW METHODS OF PROVING 'YOU ARE WHO YOU SAY YOU ARE' ONLINE ARE MORE SECURE, RELIABLE, AND PRIVACY PRESERVING.
Certified Company
You choose a company to check and verify your identity online to use GOV.UK services.
GOV.UK VERIFIED
Certified Identity and Attribute Providers
Bank
Mobile operator
Credit Reference Agency
Technology companies

Figure 6: Gov.UK Verify

The relevant Government department requires certainty that a claim to a particular identity made by a citizen, or on behalf of a citizen, can be trusted to be the claimant's 'true'

In an identity ecosystem, a citizen chooses from a list of companies, known as identity providers and attribute providers (see Figure 6). These companies have been through rigorous checking mechanisms to assess the efficacy of their data handling and security processes and the quality of the data they provide before being certified.

Certified companies, which include banks, credit reference agencies, postal services and a range of new technology companies that provide innovative methods of identity verification are also required to comply with data protection laws and contractual obligations put in place to respect user rights and needs.

Each certified company has different ways of verifying a citizen's identity, for example, a citizen that has a bank account with Barclays Bank will go through a particular process that enables the bank to vouch for their identity. Other companies allow a citizen to scan a passport and run a facial recognition comparison between the photo in the document and a live selfie.

Innovation in the identity sector means the options for electronic identity verification are growing all the time. The technical platform that underpins Gov.UK Verify is an attribute exchange - an online gateway that operates according to specific sets of rules on transferring information about the user between identity providers and a Government department. Crucially, **it does not centrally store citizens' data** and the rule set hides the details of the identity provider chosen by the citizen from the Government department and vice versa. An identity ecosystem designed to conduct identity verification.

At this juncture, Gov.UK Verify is currently restricted to enabling citizens to access eGovernment services but there are plans to look at extending it to the commercial sectors. There are a number of business sectors, including banking, FinTech, insurance, and wealth management that would benefit from robust identity assurance schemes.

Attribute Checking

Regulated public-facing service providers such as gambling operators and banks carry the responsibility for verifying their customers' identities to lessen the risk of fraud, money laundering and identity theft. However, in instances where an individual wishes to, for example, purchase alcohol or view adult content, there is no legal requirement to know anything other than that the person is aged 18 years or over.

To date, both regulators and industry regarded the identity verification solutions provided by credit reference agencies as privacy invasive and therefore disproportionate in the context of the sale of some categories of age-restricted goods. Furthermore, banks and gambling operators enjoy large profit margins and can absorb the costs associated with identity verification. For retailers and online platform providers, which operate on a thin profit margin or small average revenue per user respectively, the cost of identity verification means expensive compliance costs.

Changing Regulatory Environment

In recognition that an attribute economy is emerging, the European Commission and the UK Government have proposed legislative changes (UK Digital Economy Bill and proposed EU's Audio Visual Media Services Directive (AVMSD)) designed to ensure that online businesses respect children's rights online. In particular, those in Article 17 of the UN Convention on the Rights of the Child (UNCRC), which states:

> *"States Parties recognize the important function performed by the mass media and … encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being ..."*

The European Commission recognises that children have particular needs and vulnerabilities on the Internet; however, the Internet also provides opportunities for children to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employability. The European Commission's "A European Strategy to deliver a Better Internet for our Children" proposes a series of actions to be undertaken by the Commission, member states and by the whole industry value chain. For example, the strategy proposes a series of actions grouped around the following main goals.

- Stimulate the production of creative and educational online content for children as well as promoting positive online experiences for young children scaling up awareness and empowerment, including teaching of digital literacy and online safety in all EU schools

- Create a safe environment for children through age-appropriate privacy settings, wider use of parental controls, age rating and content classification

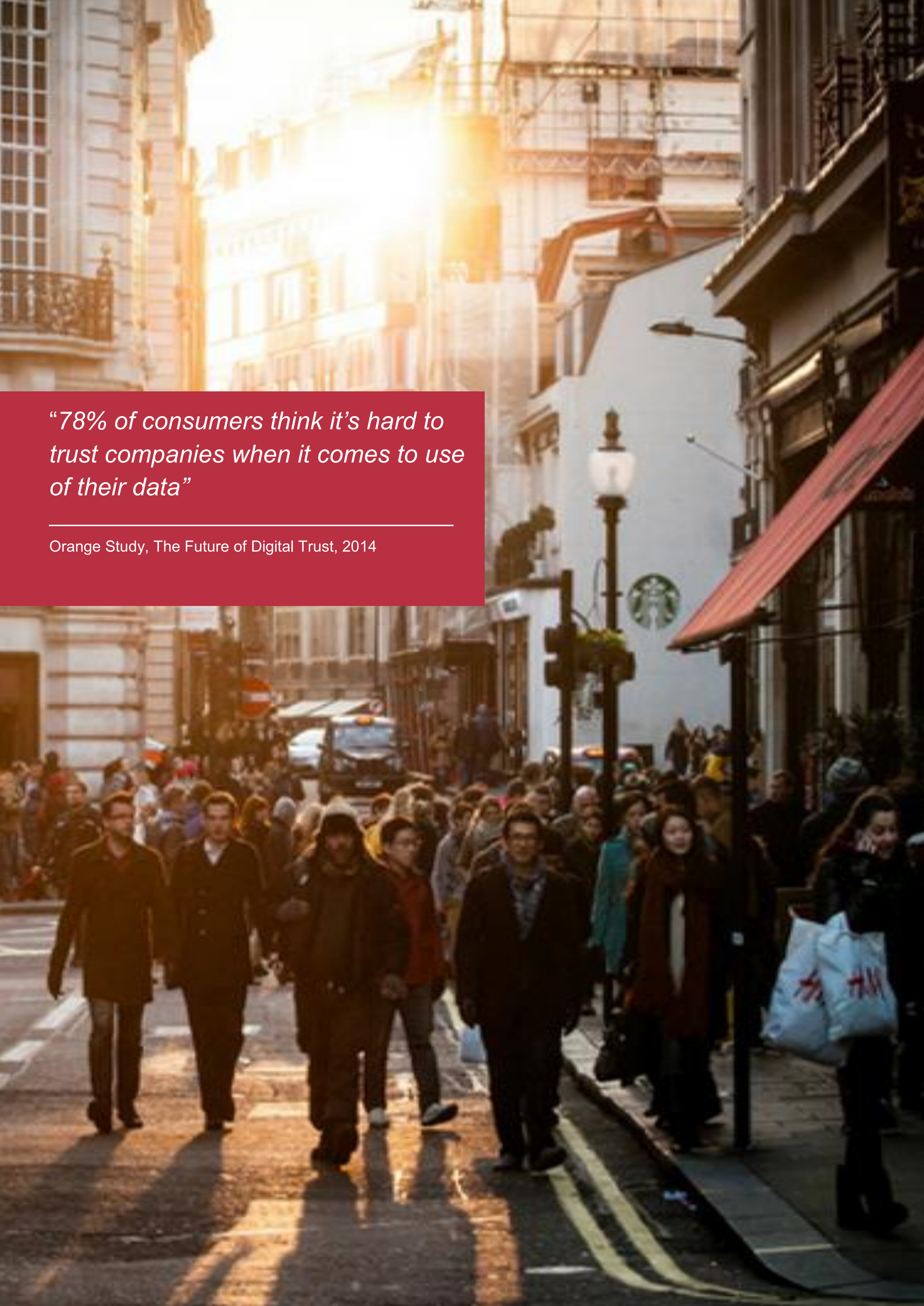
- Combat child sexual abuse material online and child sexual exploitation.

The evolving regulatory and policy environment dictates that the age band to which a user belongs is becoming increasingly significant in a range of instances. There is pressure mounting on online businesses to ensure that both age-restricted and age-rated online content, goods and services are only accessible and delivered to those for whom they are intended or legal towards.

Self- and Co-Regulatory Drivers

In June 2016, in a press release [21] about the updated Audio Visual Media Services Directive, the Commission announced that it intends to engage platform providers in a self-regulatory process to implement measures designed to better protect children online. Crucially, the Commission explicitly stated its intention to encourage online platforms to use technological innovation relating to secure eID, to conduct age checks to limit children's access to harmful content. The Commission has set a timeline for this dialogue and intends to issue sets of principles and guidance on more secure means to protect children online at the latest by 2017.

￼ [44]. [44].



“78% of consumers think it’s hard to trust companies when it comes to use of their data”

Orange Study, The Future of Digital Trust, 2014

Standards that Support Person-First Technologies

COEL

Joss Langford, Director - Coelition

In 2013, Coelition published ‘Data to Life’, the culmination of three years of research in partnership with Unilever. The findings set out a blueprint for how our everyday lives could be recorded in way that gave individuals access to fantastic new personal services without sacrificing control over their personal data.

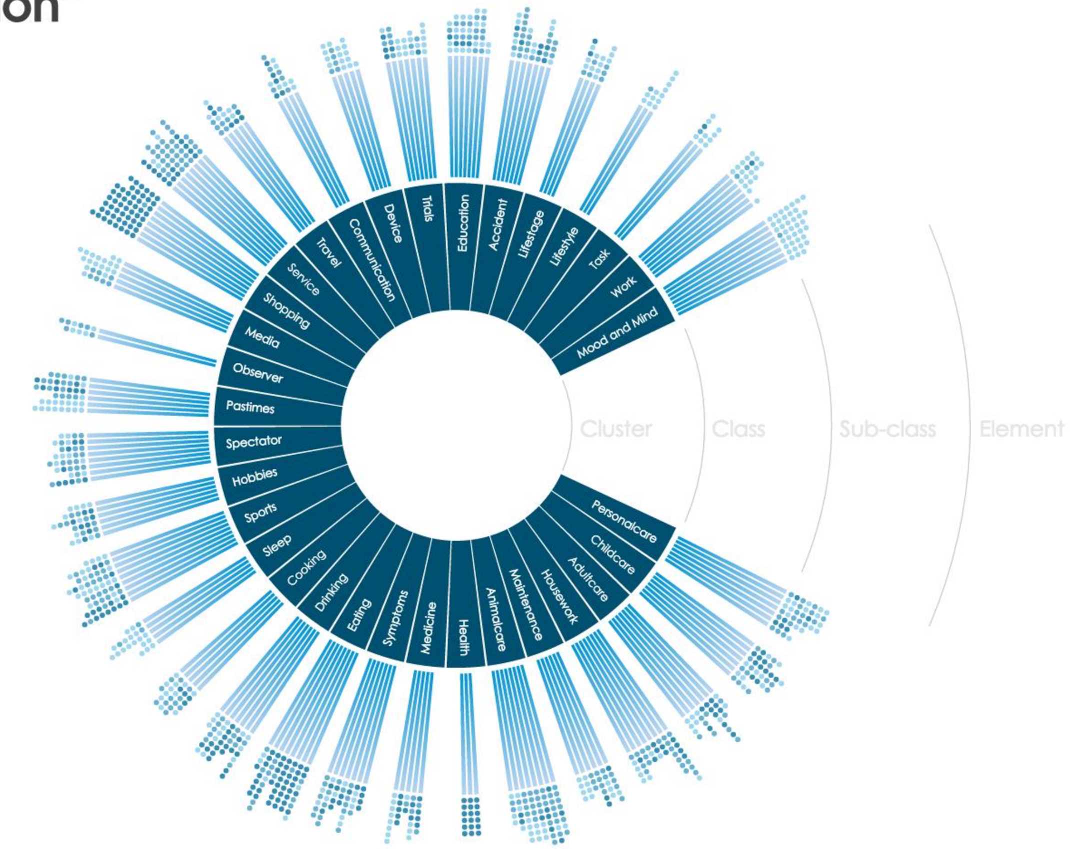
In the manifesto of the publication, one key tenet was to ‘humanise technology and knowledge rather than digitise life’.

Over the last 3 years, that blueprint has been developed into a global open standard with the support of Fujitsu resulting in COEL; the Classification Of Everyday Living.

Joss Langford
Director, Coelition

Joss Langford is co-founder of Coelition, a not-for-profit supporting the responsible use of behavioural data by organisations looking to grow brands and drive social change. He is also technical director of Activinsights using wearables to provide behavioural insights to healthcare professionals. Joss has senior management experience in blue chip, SME and start-up businesses. His expertise is reinforced with a proven track-record developing new ventures, brands and products.

Coelition



The standard provides both a coding scheme capable of recording any type of human behaviour and a data format to exchange information.

While the concept of data access is already part of data protection law in many countries, the pending General Data Protection Regulation (GDPR) brings forward the concept of portability. Not only must individuals have access to their data but also organisations are expected to provide that data in a meaningful, reusable form. The use of the COEL standard enables us to move beyond *system interoperability* to *data interoperability* where individuals can start to experience the power of collecting their own data from multiple facets of their lives.

Part of the friction we experience as we move from the analogue to the digital world is that we are still trying to work out which behaviours need to be private versus public.

The rituals and conventions of everyday living provide us with tools to shield intimate behaviours such as hygiene, sex, sleeping, eating and family conversations.
However, we increasingly have agents such as Smart TVs listening to every living room conversation, or devices monitoring our sleep and increasingly Internet of Things (IoT) devices that are part of our deeper personal lives.

The COEL model gives us the tools to record any of these behaviours so that we can build life-management that really understands life. Whilst understanding these behaviours may well lead to advances in treatment, health and wellbeing, we must also be working on the ethical standards and the moral rights of the individuals that bring the digital into everyday living.

Clear, Meaningful and Unambiguous Consent

Nathan Kinch, Head of Experience and Labs - Meeco

As previously highlighted by Dr. Rachel O'Connell, the mechanism through which an organisation acquires the explicit consent to use personal information requires re-imagining. This is not just the result of the GDPR or other evolving regulatory frameworks, but also a direct result of consumer sentiment and behaviour.

These methods of consent will have a direct impact on customer experience, business capability, and technology. As a result, standards are being developed to support organisations throughout this process of change, and also reduce the potential unnecessary impact of cognitive load imparted on customers.

Proof of Consent and policy transparency enables people to track their own information at scale. Standardise this and billions in compliance costs will be saved. People will also have choice – a notion today we are all too unfamilair with.

Mark Lizar's contribution shows how trust can increase with layered policy notices. These insights are based on his work with Consent Receipts and the Open Consent Notice Framework, which aim to provide dynamic privacy and notice capabilities along with common tools for data control.

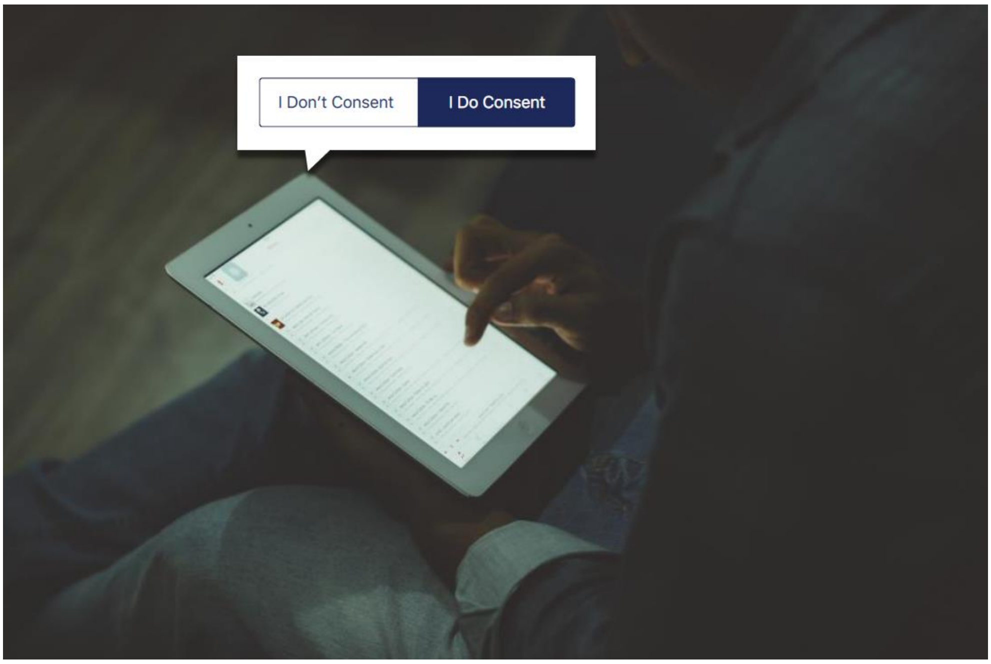


Figure 8: Consent and acknowledgement

Open Consent (OC)

Mark Lizar, Director – Open Consent Group

Open Consent provides a standards approach to consent and privacy notice engineering. It addresses the critical issue of people not being able to track the processing, disclosure and collection of personal data and use, so that once people track their personal information they can also control its flow.

Open Consent, as opposed to closed consent, is intended to dramatically reduce the costs of privacy compliance in the EU single market.

Research indicates that compliance costs within the UK will range from £150 to £300 million a year[22], not including the additional 17-23% increase of those costs due to Brexit[23]. As a result the rest of the world will need to demonstrate compliance with the UK and the EU, as the UK will become a separate regulatory market.

Mark Lizar
Director, Open Consent Group

Mark is the founder of the Open Consent Group which is a leading privacy engineering company delivering products and services. Mark is also the editor of the consent receipt specification at the Kantara Initiative, as well as the chair of the Consent WG at Digital Catapult currently leading a 1 year workshop series on Real Consent.

The Open Consent Group is working on a suite of tools for enhancing and harmonising existing policies and practices in order to help companies exceed compliance requirements. Integrating these tools into existing consent architectures will enable people to have streamlined consent experiences. Most importantly, people will be supported with standard consent based data controls, allowing them to self-authorise the flow of personal data after consent has been provided.

Consent Receipts

To go beyond compliance by empowering customers and citizens, the Consent Receipt v.1[24] is the perfect vehicle. Consent receipts, also known as a reverse cookie, are a standards-based specification published on February 17th 2017. It is

[22] What will it cost to become EU data law compliant? – My Customer, September 2. 2015

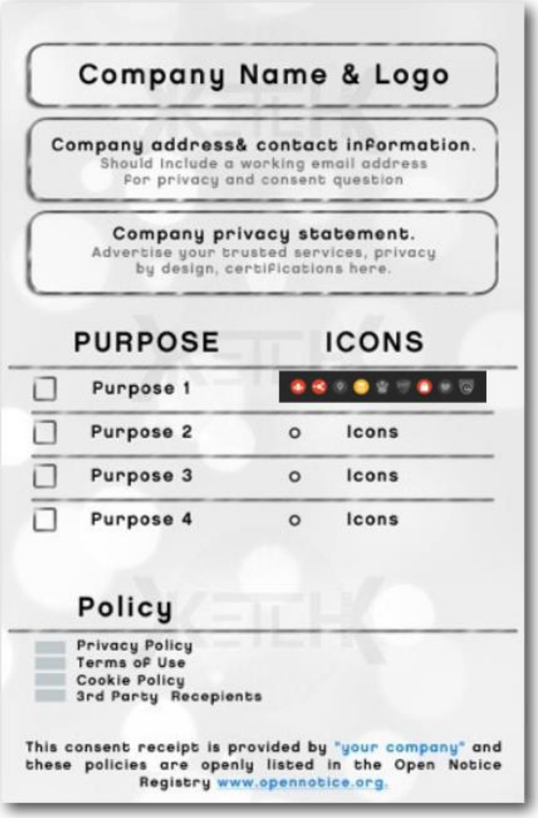
[23] Microsoft: We're hiking UK cloud prices 22%. Stop whining – it's the Brexit – The Register, October 24, 2016

[24] Consent Receipt Specification formal notice, January 8, 2017

developed at the Kantara Initiative, a non-profit organization that develops consensus based facilities and workgroups and is leading work in the field of consent receipt specifications. A machine-readable consent receipt makes it possible for people to track consent and information sharing by making a record that can also be used as proof of consent. This approach helps standardise and make machine-readable privacy policies, layered privacy notices and consent transactions.

Consent, as a legal mechanism, promises to provide the ability for people to change their own services and manage the use of digital identity, providing an attractive approach to single data market, especially in the EU where “GDP gains are estimated up to 8 Billion euros per year” (up to 0.06% of GDP, which is on par with the gains of recent free trade agreements)[25]

Having an open system of consent not only enables the single market but also provides the path for personal data management, contextual experience creation at a much lower cost through consent data.



Company Name & Logo

Company address& contact information.
Should include a working email address
For privacy and consent question

Company privacy statement.
Advertise your trusted services, privacy
by design, certifications here.

PURPOSE	ICONS
□ Purpose 1	● ● ● ● ● ● ● ● ●
□ Purpose 2	○ Icons
□ Purpose 3	○ Icons
□ Purpose 4	○ Icons

Policy

- Privacy Policy
- Terms of Use
- Cookie Policy
- 3rd Party Recepients

This consent receipt is provided by "your company" and these policies are openly listed in the Open Notice Registry www.opennotice.org.

Figure 9: Consent Receipt

Our Experience as ‘Users’

Nathan Kinch, Head of Experience and Labs - Meeco

“Your personal information will be used to optimise your experience,” is a phrase we’re all too familiar with. However, as we now know, this type of ‘consent message’ isn’t clear, meaningful and unambiguous, and won’t come close to meeting the requirements of the GDPR.

[25] Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States - December 2016

In reality, this statement could perhaps be translated to something like, “We are going to use your information to figure out how we can most effectively up-sell, cross-sell and get you to refer your friends, family and colleagues to our product or service.” This isn't inherently bad; it’s just more closely aligned to the truth.

Although we constantly hear about ‘deeply personalised’ experiences, our current reality as ‘users’ of digital products and services is that our experience is rarely personalised - regardless of how our personal information is used. This, however, is changing rapidly.

With advancements in the fields of machine learning and artificial intelligence, as well as our growing love affair with conversation User Interfaces[26] (UI), our day-to-day digital product experiences will become increasingly personalised.

However, in order to personalise a digital product or service, personal data that is accurate, in context, real-time, and ideally matched with intent, becomes a key component of fulfilling the experience. To do this, new user experiences that support informed consent models must emerge. The model of 'capture all the data and figure out what to do with it’ is now under threat.

Moving to this new model is by no means easy, but the value of a superior user experience, both to the humans using a product or service, and the organisations providing that offering, is significant. We know this, yet we now have to work towards delivering the greatest possible experiences, whilst deeply respecting the privacy and agency of our customers if we are to realise this value.

To realise this value, new exchanges, where a person grants their explicit consent, or permissions their personal information directly to an organisation in return for a personalised experience and/or some form of agreed value, will occur on equal terms.

[26] The killer feature of messaging no one’s talking about - Inside Intercom, September 2016

Just as businesses have created value via B2B models, exchanging data in a standardised format via APIs, or the 'API-of-Me' will form a key part of the value chain. Through this, we're moving into a world where individuals will have the ability to bring their identity and consent into a product or service experience with an organisation of their choosing. In this context, forward thinking organisations are already asking questions like:

- How might we make it easier for a person to understand what information we'd like to use and why?
- How can we reduce the amount of personal information we have to use to fulfil our value proposition?
- What information could we give back to our customers so that they might be able to re-use to make their experience with us or our partners faster, simpler and more valuable?
- If we build a trusted relationship with our customers, and they choose to grant us access to new information about themselves, what new value can we create for them?
- When does identity actually become necessary? How might we decrease this necessity so that we may preserve our customer's privacy?
- What effect does a dynamic consent experience have on the cognitive load of our customers? How might we reduce that impact?

Each of these questions, along with the long list of additional questions they in turn trigger, present both challenge and opportunity.

As designers of products and services, the market forces referenced above must be considered. The way we approach personal data has now changed forever. Our approach to user experience design can't be different. It has to change. Privacy by Design[27] must become a foundational principle - something that is considered and constantly referenced as we execute our research and design processes.

To further highlight some of the emerging user experience design considerations James Harvey, Head of Design at Yoti, contributed the following case study that highlights their approach to helping people create a digital identity through seamless on-boarding processes.

[27] Privacy by Design, Information Commissioner's Office, UK

Case Study: User Experience in the Attribute Economy 2.0

What if we could mitigate the effects of cognitive load during the sign up process? And what if we could do this by giving people the feeling of control? Better yet, what if we could do all this do this by asking people to provide an asset they will never forget, that they own, and that is unique to all of us?

So often sign-up processes involve forms and questions to confirm who we are. The problem with this is that friction increases as we're asked to answer questions we've previously answered.

This puts a huge impact on our cognitive processing. It also raises questions of how we prove who we really are and who actually controls the data we provide. If we can't remember this information, or if we get the questions wrong, we're no longer the ones in control.

When it comes to our identity… surely we know who we are?

Our focus at Yoti was to simplify sign-up and enable a person to use data that is unique to them.

Using biometrics together with the individual's mobile device, Yoti has designed an experience that significantly reduces the impact of cognitive load on a user at the point of sign up.

Rather than presenting a long form, memorable word options and 'alpha-forgettable' passwords Yoti's person-first solution simply asks for what is necessary to create a unique account; a 'selfie' and associated mobile number.

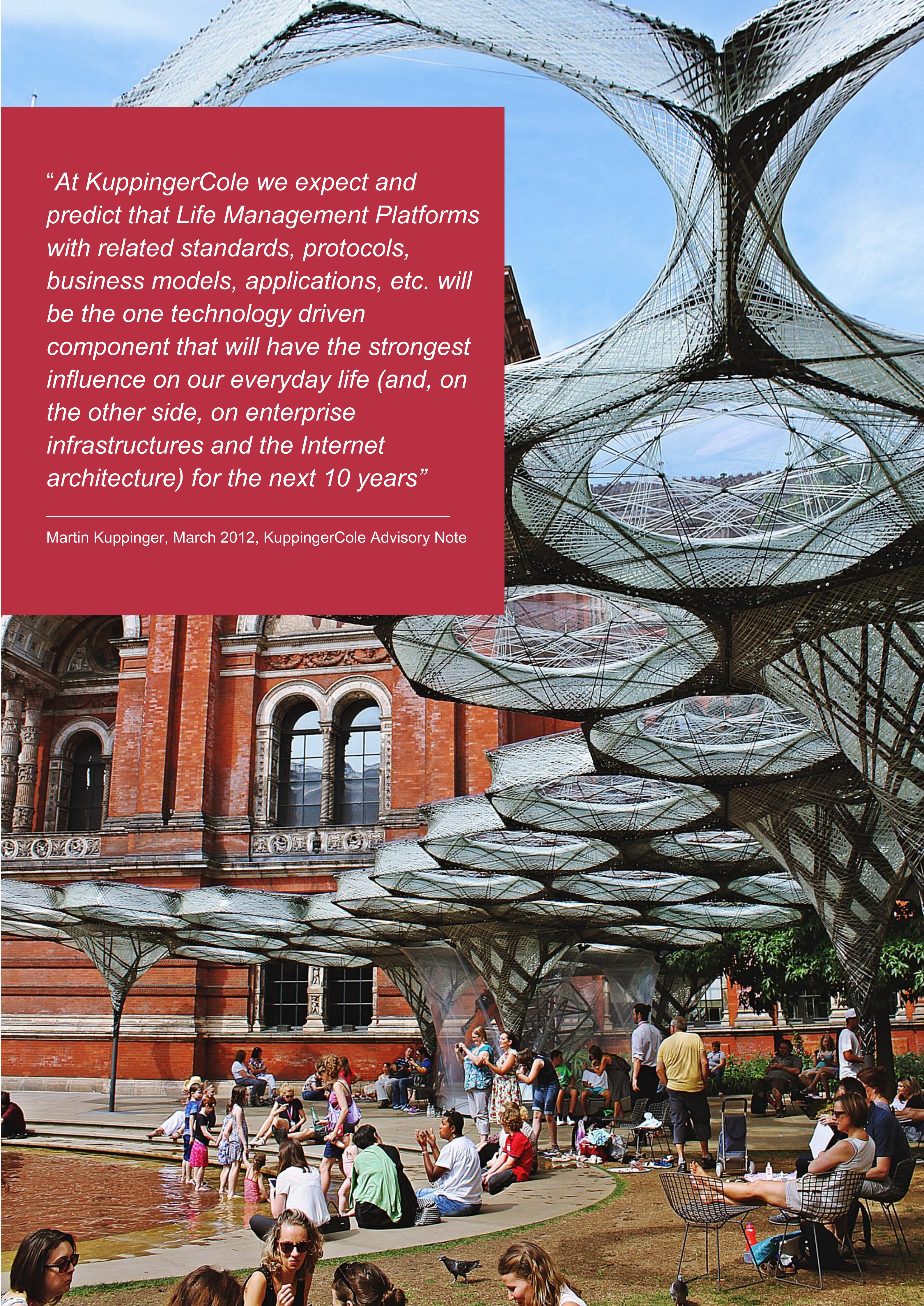
This solution allows customers to be themselves and evidence they're a real person. It does not require them in the first instance to provide additional information they might deem too personal before understanding the full benefit of the product. It gives them the opportunity to try the product with limited effort, within an environment of their control.

This increases the likelihood of someone completing their journey by removing the common obstacles faced.

The key to this approach: Design for people first, not their data.

James Harvey
Head of UX and Design, Yoti

James is Head of UX and Design at Yoti, leading a team designing native and web apps with privacy and consent at the forefront of the user experience. Yoti's mission is to give people back full control over their data.
Prior to this James was Head of Design at JustGiving where he was responsible for a team of visual and UX designers and notably the full re-design, re-brand, delivery and launch of all JustGivings new native and web app products and services



“At KuppingerCole we expect and predict that Life Management Platforms with related standards, protocols, business models, applications, etc. will be the one technology driven component that will have the strongest influence on our everyday life (and, on the other side, on enterprise infrastructures and the Internet architecture) for the next 10 years”

Martin Kuppinger, March 2012, KuppingerCole Advisory Note

Enabling Technologies

Joerg Resch, Managing Director – KuppingerCole

In 2012, German research and analyst firm KuppingerCole introduced the world to the concept of Life Management Platforms[28]; an enabling technology that extended far beyond a simple ‘Personal Data Store’ (PDS) and gave individuals full control over the utilisation of their data within the context of their lives.

The challenge of Life Management Platforms (LMP) is to balance the need for a high level of security and privacy, required for the storage and processing of sensitive personal information, with a user experience that is good enough to enable a broad impact on the way individuals interact with their banks, insurance providers, government, schools, retailers and medical institutions.

Joerg Resch
Managing Director
KuppingerCole

Joerg has over 15 years of experience in Identity Management projects and their implementation in both SMEs and large corporations. For a number of years, he owned different leadership positions in software product development and published many technical articles on a wide range of IM-related subjects.
Since 2004 he is Co-Founder and Managing Director of KuppingerCole.

An infrastructure providing the foundations for a trusted exchange of validated data has to be vendor agnostic, decentralised and standards based. Back in 2012, when we published our first research on LMP, the standards landscape supporting the concept wasn’t there yet. This is different today. Much progress has been made in the past four years including the User Managed Access (UMA) open standard, together with OpenID Connect and OAuth. These standards and emerging protocols provide the necessary ingredients for Life Management Platforms to deliver on the promise of user centricity and control.

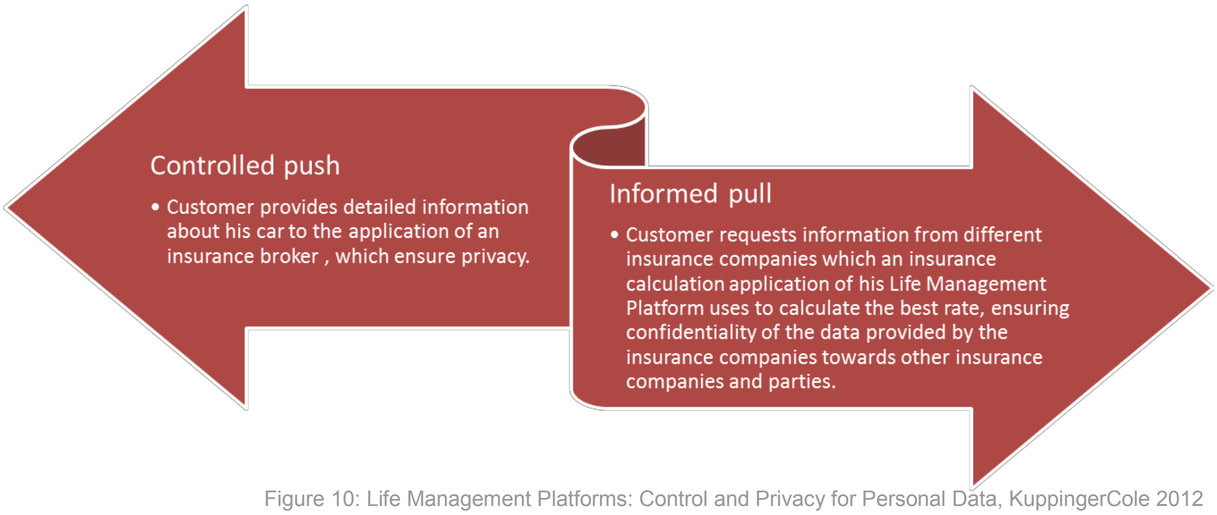
Additionally, the emergence of Distributed Ledger Technologies (DLT), the most commonly known of which is the ‘Blockchain’, will further add value to the concept of Life Management Platforms in enabling validation of personal data transactions. This transparency and verification contributes to building trust.

[28] Advisory Note: Life Management Platforms: Control and Privacy for Personal Data - 70608, March 2012

As these solutions begin to scale and mature, they will become the rails on which trust based solutions are developed, eventually becoming mainstream.

The concepts behind Life Management Platforms are increasingly becoming top priorities in many industries. These initiatives may be broadly referred to as ‘Consumer Identity Management’ or from the perspective of the individual as ‘Self-Sovereign Identity’.

Identity and trust are both key requirements and enablers of the Attribute Economy. They are essential for regulated financial services requirements such as customer on-boarding or ‘Know Your Customer’ (KYC) processes. KYC forms part of the legal requirement for financial institutions to comply with Anti-Money Laundering requirements in order to provide traceability to the source of a customer’s wealth.



Controlled push

- Customer provides detailed information about his car to the application of an insurance broker , which ensure privacy.

Informed pull

- Customer requests information from different insurance companies which an insurance calculation application of his Life Management Platform uses to calculate the best rate, ensuring confidentiality of the data provided by the insurance companies towards other insurance companies and parties.

Figure 10: Life Management Platforms: Control and Privacy for Personal Data, KuppingerCole 2012

Life Management Platforms offer the solution to balance the privacy needs of individuals, and the regulatory requirements of service providers. This is the mechanism for information to be both pushed (with consent) and pulled (with permission) to provide a trusted and secure exchange of attributes.

These all are different approaches to the same concept of a value driven and privacy compliant interaction between humans and organisations. These are the requirements that will make innovations like Internet of Things, machine learning and wearable computing a mutual success for participating stakeholders.

Enabling Technologies in Market

Nathan Kinch, Head of Experience and Labs - Meeco

Thought leadership, such as that from KuppingerCole, contributed to the architecture and capabilities of Meeco.

Meeco is a multi-award winning Life Management Platform, first launched in 2014 with a range of basic services that have since extended to deliver the capabilities referenced throughout this paper.

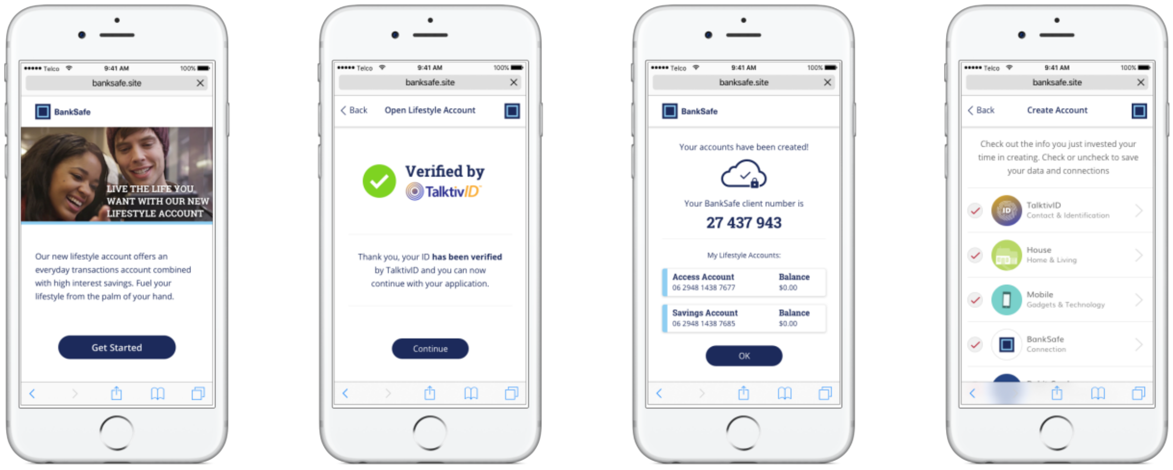
Meeco gives people the ability to take control and make use of personal information from all parts of their life. In simple terms, people can control and connect their digital lives, share their digital life with people and organisations of their choosing, and in the process, create new assets, new experiences and new outcomes.

To assist organisations in preparing for the Attribute Economy 2.0, Meeco is proving unique innovation around customer on-boarding and know-your-customer (KYC) capability through provisioning the API-of-Me. This enables individuals across diverse life roles such as citizen, customer, student, patient and employee to bring their identity and permission-based access to organisations, so that the right products, services and experiences can be seamlessly consumed.

This is resulting in a range of mutual benefits, including new value chains for enterprise and tailored outcomes for customers. Additionally, the direct relationship between the enterprise and the customer builds a private channel for on-going permission marketing.

An example of this innovation can be seen in the following figure, where an existing trusted and verified Digital Identity credential is used in place of traditional manual data entry to significantly reduce the time it takes for a person to prove who they are, and complete the application process for a new bank account.

By enabling the bank to ask for, consume, and make effective use of their prospective customers’ identity credentials and personal data, some of the existing on-boarding challenges are well on their way to being solved.



Our new lifestyle account offers an everyday transactions account combined with high interest savings. Fuel your lifestyle from the palm of your hand.

Thank you, your ID **has been verified** by TalktivID and you can now continue with your application.

Your accounts have been created!

Your BankSafe client number is

27 437 943

My Lifestyle Accounts:

Access Account 06 2948 1438 7677	**Balance** $0.00
Savings Account 06 2948 1438 7685	**Balance** $0.00

Check out the info you just invested your time in creating. Check or uncheck to save your data and connections

*Open a bank account and
get your data back in one minute

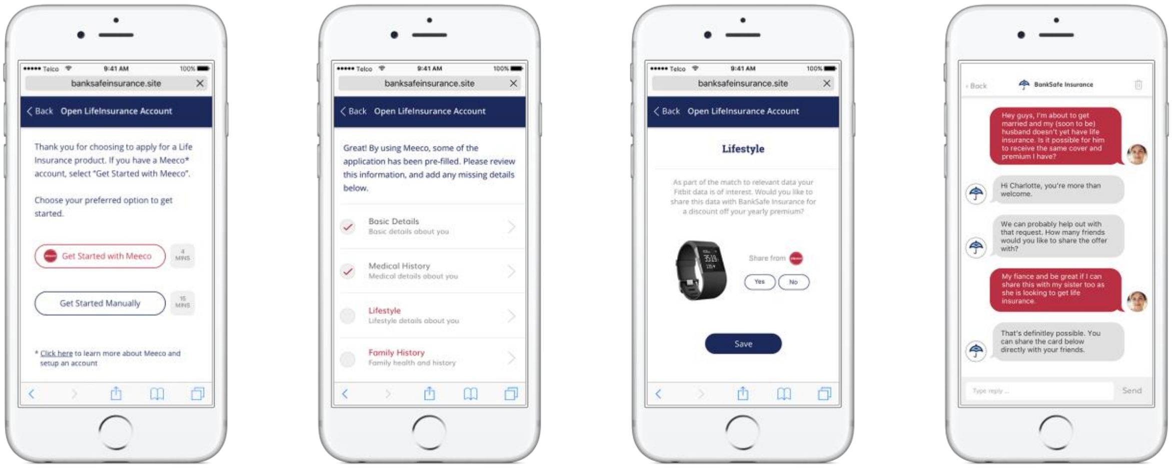
Powered by Meeco™
customer journey

©Meeco 2016
Meeco is part of the Meeco Planet Pty Ltd group of companies

Figure 11: Powered by Meeco^{TM} Bank Account Opening

Additionally, Meeco enables the bank to give the new credentials and personal data to their customer. The customer can choose to then save this information, creating a Meeco data wallet in the process. Customers are free to re-use this information on their terms in future transactions, and daily situations. The bank now has a direct ‘pipe’ where the data can be shared, edited and updated with shared access.

The next use-case included is focussed on enabling consumer insurance applications. In this example, the prospective customer of an insurance provider re-uses data they already have within their Meeco account to make the process of applying for an insurance product simpler, faster and more accurate.



Thank you for choosing to apply for a Life Insurance product. If you have a Meeco* account, select "Get Started with Meeco".

Choose your preferred option to get started.

* Click here to learn more about Meeco and setup an account

Great! By using Meeco, some of the application has been pre-filled. Please review this information, and add any missing details below.

As part of the match to relevant data your Fitbit data is of interest. Would you like to share this data with BankSafe Insurance for a discount off your yearly premium?

Hey guys, I'm about to get married and my (soon to be) husband doesn't yet have life insurance. Is it possible for him to receive the same cover and premium I have?

Hi Charlotte, you're more than welcome.

We can probably help out with that request. How many friends would you like to share the offer with?

My fiance and be great if I can share this with my sister too as she is looking to get life insurance.

That's definitley possible. You can share the card below directly with your friends.

Powered by Meeco™
customer journey

©Meeco 2016
Meeco is part of the Meeco Planet Pty Ltd group of companies

Figure 12: Powered by Meeco^{TM} Life Insurance Application

After verifying their identity, the person is given a clear view of the information that's been requested to use, as well as the information they still need to enter to complete the application process. As they quickly enter the remaining information, it's recognised they have a Fitbit connected to their Meeco account.

The customer is offered a discount on their premium in exchange for sharing information as part of the application process. The person can choose to accept or decline this offer. When developing these use-cases, the primary protection of data and legal rights is maintained. The consequences of sharing are explicitly displayed including how the data will be used.

Directly following the experience, a connection is made between the insurance provider and their new customer. This then enables a secure and private chat channel where support can be offered, claims can be made, and new products can be acquired. More importantly all this is under the explicit control of the customer.

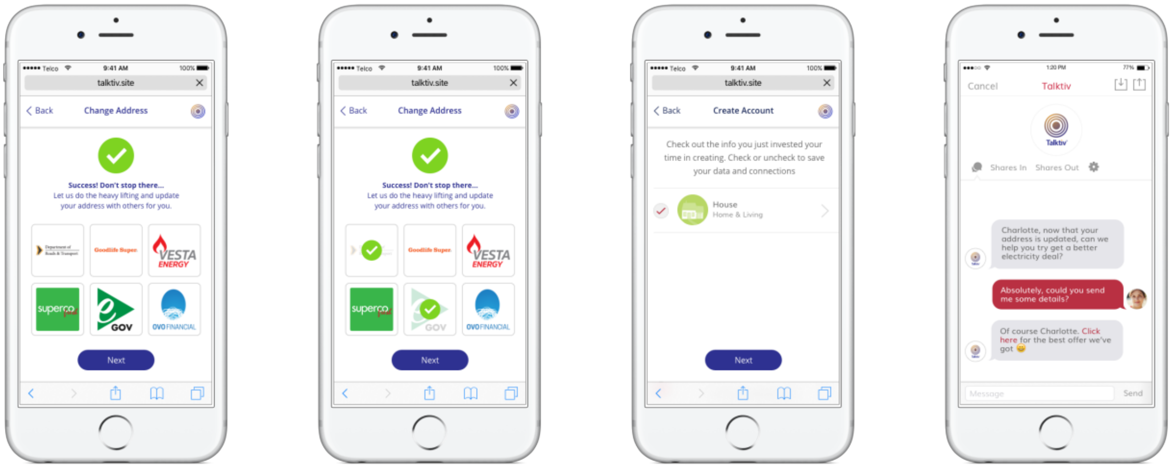
Examples like these are a core component of how the Attribute Economy 2.0 is emerging.

Person Controlled Permission

At Meeco’s core is a permission management tool, enabling identity credentials and personal information to be exchanged explicitly on the terms of the individual. This can be done with the people and organisations they trust through either ‘controlled push’, or ‘informed pull' interactions, as described by KuppingerCole.

Additionally, through the assertion of binary attributes (such as over 18 Y/N) or through a de-identified persona (pseudonym), Meeco supports progressive disclosure – the ability for personal information to be exchanged at an appropriate time, based on specific needs, with the explicit consent of the individual. Through this model, personal information is exposed as trust is earned. This model enhances privacy for the individual and reduces the risk for the organisation or institution of collecting and storing personal information.

Meeco also supports bi-directional and multi-directional permission-based data exchange - where an organisation may request information from an individual for a specific purpose in the context of the existing relationship. The individual may then explicitly consent to permission this information to the organisation, based on agreed terms, whilst also allowing the organisation to share that information with explicitly defined third parties for the purpose of achieving a specific outcome.



Success! Don't stop there...
Let us do the heavy lifting and update your address with others for you.

Check out the info you just invested your time in creating. Check or uncheck to save your data and connections

Charlotte, now that your address is updated, can we help you try get a better electricity deal?

Absolutely, could you send me some details?

Of course Charlotte. Click here for the best offer we've got 😀

Powered by Meeco™
customer journey

©Meeco 2016
Meeco is part of the Meeco Planet Pty Ltd group of companies

Figure 13: Powered by Meeco^{TM} Change of Address Service

A practical example of this is change of address. A customer of a Telco may update their address through a Powered by Meeco^{TM} service the Telco provides. The Telco may then offer to exchange that updated address with other organisations the customer already has an existing relationship with, thus creating value for their customer by saving them time, and relieving potential headaches many of us can empathise with. This enables the Telco to move from data seller to data custodian, offering a range of new privacy and trust-enhanced services.

Through this model, the individual can share data once, and grant explicit consent so that the data may be used to create value many times over.

In both the examples illustrated, certain requirements within the European General Data Protection Regulation (GDPR) and Payment Services Directive 2 (PSD2) are supported. As previously highlighted, this regulation is a key driver for organisations to improve their data acquisition and processing models, and provides a significant opportunity for innovation within the context of consent and permission-based interactions with customers.

Although much work is being done to enhance the value of consent and permission-based interactions for people and organisations, a model where individuals are in full control of their personal information, as well as the interactions that make use of their personal information, is yet to come to any level of 'meaningful' adoption.

This however, is the emerging market of Me-to-Any (Me2Any) and Any-to-Me (Any2Me), where individuals are the point of integration and the facilitator of their permission-based interactions with their peers, with industry and government. It is also the exact model that enabling technologies, such as Life Management Platforms, are beginning to make widely available.

Using Meeco for any of these Me2Any interactions, customers can explicitly permission the information they have within their control to a peer, a group, an organisation or a marketplace, for an appropriate exchange of value.

To enable seamless permission management Meeco uses a combination of policy rules that are API embedded. These determine the legal (governance) business model (value chain), and technology enablers that make up the API-of-Me.

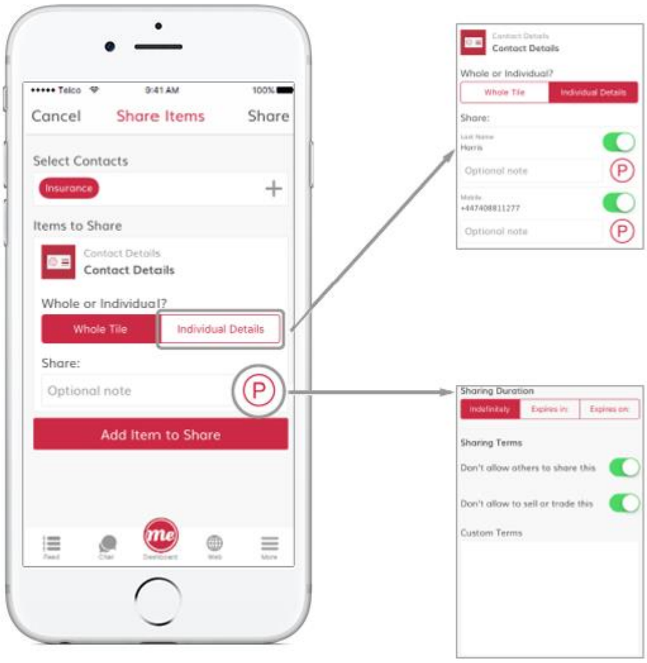


Figure 14: An example of person-first permission management through Meeco's Permission Management Tool

It is the combination of the legal, business and technology that provides increased agency and transparency in the sharing of personal data and granting of consent.

As seen in figure 14, the Meeco Permission Management Tool enables people to specify the following granularity of permission:

a) Duration of share:

- Until deleted
- For a set period of time in hours and minutes
- Until a set date

b) Terms of share:

- Data cannot be passed onto or shared with any third parties without the person's permission
- Data cannot be sold or traded without the person's permission

b) Custom Terms:

- A person can also include explicit terms that govern the purpose of the exchange and the use of that data once it has been shared.

The individual is also able to save and recall a set of default permissions to make similar permission-based exchanges a seamless experience.

> “Data will eventually be collected on most everything, stored and analysed with recommendations sent back to users to enhance real-time decision making”

Silicon Valley Bank: The Quantified Self, 2014

The Attribute Economy 2.0 - A Human Opportunity

New Models of Value Are Emerging

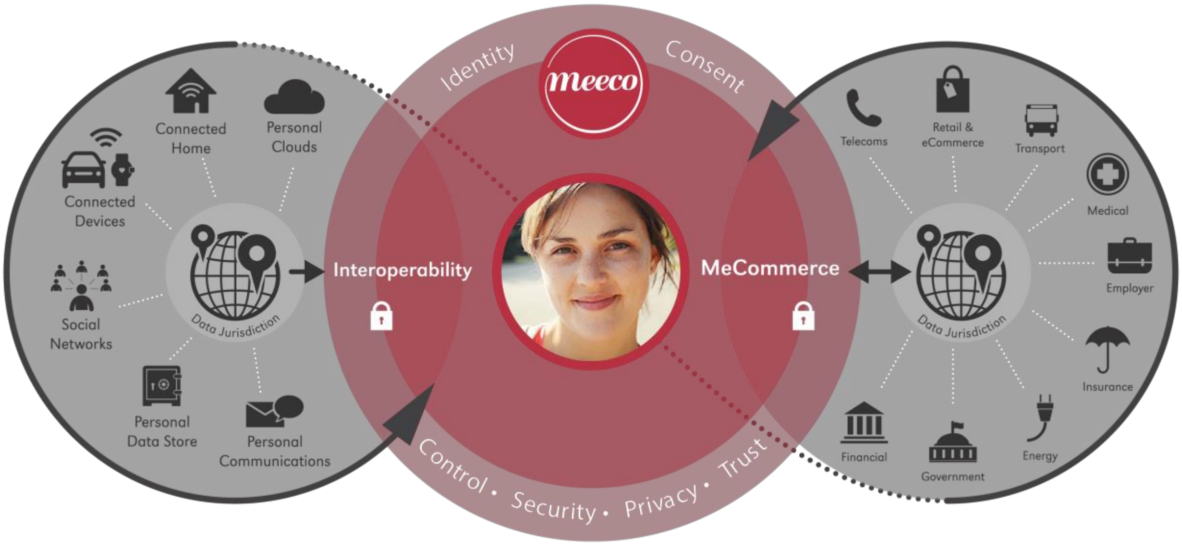


Figure 15: The MeEcosystem

The MeEcosystem: This diagram represents the point of a view of a person utilising Meeco as their Life Management Platform. On the left-hand side of the diagram are the things a person does or owns that creates data, and on the right-hand side are the people, organisations or 'things' a person may choose to share data with.

The centre of the diagram represents a trusted mechanism, controlled by the individual, that enables an individual to control secure transactions between themselves and the market.

When you consider the current model governing attribute exchange, where a company (an identity provider or data broker for illustrative purposes) will exchange a single attribute, or group of attributes that collectively represent a profile, with another company for a specific purpose, they charge a fee. This fee could range from a few cents to hundreds of dollars for lead generation. This occurs over and over again, meaning the revenue generated from our identity, or our 'digital profile' compounds over time. In simple terms, our personal data is traded as a commodity without our participation.

However, we are beginning to move towards a new model, like the one proposed by KuppingerCole, or the more recent model proposed by the Finnish Ministry of

Transport and Communications; MyData. In this model, people are in control of their personal data.

As Rob Laurence and Dr. Rachel O'Connell referenced, core to this model is some form of digital identity, enabling us to assert our right to participate. Or perhaps we choose to begin certain processes as a pseudonym, an anonymous persona, enabling us to browse and show interest without giving away who we actually are. We then have the ability to exchange various attributes, either individually or collectively, with people and organisations we trust. By doing so, we may never have to fill in a form again.

We may also be able to navigate the web with far less friction. We may even be able to express our intent to purchase an item or have an experience, push that to a market of potential vendors anonymously, and as we become more interested in a particular product or offer from a vendor, progressively disclose our information up to the point of transaction where we might reveal our true identity if required. This is the essence of the 'Intention Economy', popularised by renowned author and academic, Doc Searls.

In simple terms, this is our data becoming our commodity, traded by us to others when we perceive there is value in doing so. This is a model where we participate as equals.

Possibilities and the Impact on Financial Services

Think of the upcoming Payment Services Directive 2 (PSD2)[29]. This directive is changing the financial services landscape and empowering consumers with more flexibility than ever before. It's also set to introduce consumers to new AISPs (Account Information Service Providers) and PISPs (Payment Initiation Service Providers). Accenture predict that[30] (three out of every ten debit card payments will move to a PISP by 2020.

[29] Payment services (PSD 2) - Directive (EU) 2015/2366

[30] Consumers' reactions to AISP and PISP—the new PSD2-enabled services, Accenture 2016

Because of this, the land grab is already underway, with traditional providers, social media giants, FinTech innovators and Telcos now focused on this space.

Given this, imagine, as a consumer, having a single view of your digital life - everything from your connected devices, to your banking, car, and online behaviour. What might this view say about you? And more importantly, how could this make your life better?

Well, a simple view won't cut it. You need to extend that view with capabilities that create actual utility.

To do this, your Life Management Platform could act as an AISP. Simple tasks like account aggregation, account switching and account verification would become available at the click of a button. Creditworthiness and identity verification are also part of the offering. Then there's expense tracking. Tracking what you bought and when is great, but what if you could also start to understand why? This has never been possible because the information that gives context to the why isn't in consumer's control.

It soon will be.

So, here's the scenario. You receive a notification one morning on your phone. It tells you both your electricity and home loan have been switched. But there's a bonus; the net monthly saving is enough to fund switching your gym membership to your dream location - three-minute walk from home, and two minutes from your train stop. This'll save you 30 minutes of travel each day. Meaning your home with your partner earlier. To top all the good news off, the extra saving has been automatically invested into an ETF (exchange traded fund) via Acorns. This is going to earn you an extra 5 – 7% per year. And best yet, it's compounding.

Your morning is now looking pretty good. So, let's re-cap quickly.

1. Your data is in your control
2. Because of this, you've got a single view of your digital life, which absolutely doesn't mean all your data is in one place, nor have your created a honey pot

3. The combination of point 1 and 2 means your Life Management Platform can act on your behalf, and help make parts of life that used to take a lot of time a lot faster, simpler and better

4. You're now better off financially

5. You've re-claimed 30 minutes of your life 3 times per week

These are the types of outcomes Life Management Platforms, supported by regulation like the GDPR and PSD2, will help bring to market.

This is the power of The Attribute Economy 2.0.

“Our vision is to create a place for everyone on the planet to get equity and value in exchange for what they share”

Katryna Dow, The Meeco Manifesto, 2012

Conclusion

Katryna Dow, Founder & CEO, Meeco

Existing value chains are rapidly evolving to include not just organisations but also people and things. The Attribute Economy 2.0 is the manifestation of this evolution and with it comes the opportunity to create new economic and societal value.

Standards are emerging and regulation is evolving to support this shift. However, with any new opportunities, we also face new challenges.

We started collaboration on this paper towards the end of 2016. Our initial aim was to highlight the opportunities a transparent data economy will enable. Our research has validated what many of the expert co-authors have evidenced in this paper; that is the power that consent and permission have in building trust.

Many of us share the perspective that the incoming European regulation, such as GDPR or PSD2, could enable significant opportunities for business transformation and customer centricity.

However, as we enter 2017, we see an old challenge manifesting in new ways; the challenge of silos and silo thinking across industry sectors and organisational lines of operation.

Through our work in Meeco Labs, we see budgets and planning for compliance programs in preparation for GDPR. Whilst positively we see Privacy Officers hired, lawyers retained and programs scoped, we also see a concerning pattern emerging.

Disconnected businesses. Marketing and business executives that say the compliance changes are out of their scope and that their legal teams are working on the required changes, even though they personally stand to be prosecuted under the coming laws. Equally, we see large contracts being awarded to manage compliance, without the oversight or sponsorship of business-as-usual teams.

Tens of millions of euros are already being spent to manage processes, identify data and develop audit trails whilst digital transformation, customer centricity and brand value remain significant challenges for enterprises globally.

The way to unlock this new value is to collaborate between the compliance needs and the innovation thinking that will deliver new business models. Silo thinking will deliver a solution to only half of the problem. Now more than ever, organisations require portfolio thinking and multi-disciplinary teams to design lasting value.

The future is networked and powered by micro-transactions. Think eco-systems that both enable and depend on the participants served. In this new market we have observed three distinct eco-systems emerging;

1. Enterprise networks, linking customers across a portfolio of products and services together with orchestrating adjacent services resulting in a better customer experience
2. Walled-gardens like Apple, Google, Tesla that will create great value within their respective service offerings, whilst locking that value to the silo
3. Open networks that link horizontally and enable customers to participate across enterprise networks and walled gardens, providing the crucial link across networks through the use of their own permissioned data.

The key to enabling these networks will be the ways in which personal data can be accessed and used. The networks that provide transparency and require explicit contextual consent, together with designing for privacy will ultimately create the most value.

Whilst we are still in the very early stages of these networks developing, we can already see organisations demonstrating market differentiation by how they collect, use and share persona data.

The Attribute Economy 2.0 will enable tomorrow’s digital transformation. To play a pivotal role in this new world, the time to get started is now.

Contacts

Chicago
London
Berlin
Tel Aviv
Sydney

Berlin office opening April 2017

Global

Katryna Dow
Founder & CEO
Twitter: @katrynadow
LinkedIn: katrynadow

Australasia

Mike Page
Head of Platform Partners
Twitter: @MikePagesyd
LinkedIn: pagemike

Europe

Nathan Kinch
Head of Experience and Labs
Twitter: @NathanKinch
LinkedIn: nathan-kinch

UK

Commercial Director for Meeco Europe
Andy Lambros
Twitter: @ andydslambros
LinkedIn: andy-lambros

US

Todd Hoskins
Head of North America Operations
Twitter: @toddhoskins
LinkedIn: toddhoskins

Israel

Lionel Wolberger
Business and Technical Architect
Twitter: @lwolberg
LinkedIn: lwolberg

Enquiries: info@meeco.me

Meeco gives you the ability to save, sync and share your information with people and organisations you trust. Empowering people with the control and freedom to manage their digital lives since 2012. Experience Meeco

On behalf of our great authors, we ask attribution if you'd like to share or distribute this paper. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system without permission of the authors. To make this easy, simply email us at Meeco and we will secure the permission on your behalf.

The views expressed are those of certain participants in the discussion and do not necessarily reflect the views of all participants or of Meeco.

© Meeco Planet Pty Ltd 2017 - All rights reserved.
Meeco is a registered trademark.