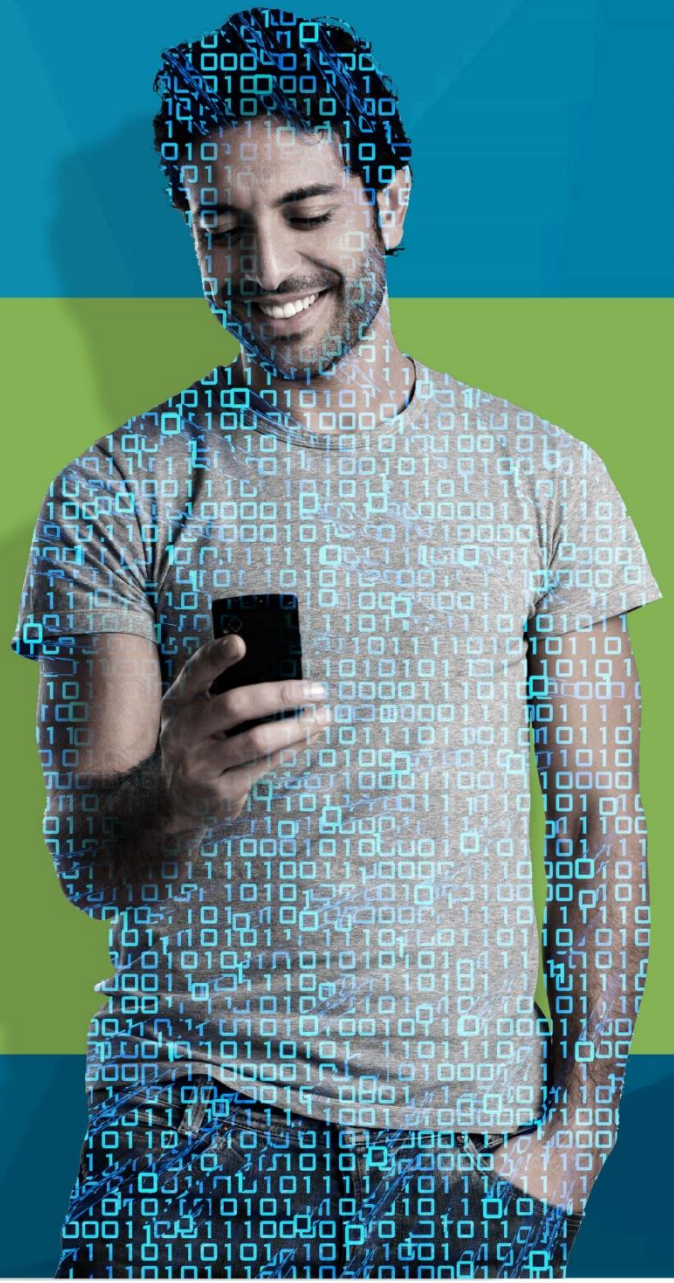
WHITEPAPER

UNDERSTANDING THE PERSONAL DATA ECONOMY

THE EMERGENCE OF A NEW DATA VALUE-EXCHANGE



MEF MOBILE ECOSYSTEM FORUM

JUNIPER RESEARCH

Contents

1. Foreword: What is the Personal Data Economy?

Simply, the personal data economy describes a powerful new idea: letting individuals take ownership of their information so they can share it with businesses on their terms.

Interest in the idea is growing for reasons of efficiency and ethics. The average individual has personal data stored in dozens of different locations. but it can be hard to access this information and then share it. Giving data back to individuals would solve this.

It would also address the concerns some people have about the way companies accrue data about them and, indeed, many companies would welcome this too. Data harvesting is expensive and can be ineffective; companies are looking for an alternative.

In theory, people in a user-centric data economy could store data about every aspect of their lives. For the first time, they could gather in one convenient digital location data such as:

- Basic ID
- Health information
- Financial information
- Buying history
- Social media history
- Photos and videos
- Travel history
- Biometrics (footsteps, heart rate etc)
- Education records

The companies driving the personal data economy (also known as the Internet of Me, the API of Me, M2B, self data, the personal information economy and more) offer a way for them to do so. These start-ups, futurologists, government agencies and major corporates are actively creating the market.

In this whitepaper, we will explore this disruptive new concept and look at its potential benefits, its technological foundations, revenue potential and business models, as well as look at some of the use cases and companies driving the personal data economy.

'I would like us to build a world in which I have control of my data… if you put together all the data from my wearable, my house, from companies like the credit card company and the banks, from all the social networks, I can give my computer a good view of my life. And I can use that. That information is more valuable to me than it is to the cloud.'

Tim Berners-Lee, speaking at IPExpo Europe/2014[i]

2. Introduction

The rise of the digital economy has brought untold benefits to billions of people. It is now possible to buy goods online and to have them delivered within 24 hours. Consumers are no longer obliged to queue to pay in a cheque or to file a tax return; these functions can be completed online. If an individual wishes to learn a language, they can do so in their own home via an app. Almost any song ever recorded can be accessed via a smartphone in a matter of seconds.

Of course, none of these services can happen without organisations gathering data about their customers and it is true that most people will willingly trade their data for useful and trusted services.

However the system is far from perfect. Some people are concerned about how much data they need to share. They worry about whether that data is passed on without their consent and if it can be stolen.

On the flipside, they can become frustrated when they actively want to share the information and the system prevents them from doing so. Consider, for example, how long it takes a person to retrieve and forward the results of a medical test.

The personal data economy offers a correction to this state of affairs.

For the moment, the personal data economy is embryonic. A small number of start-ups and government quangos are testing it, but the concept is gathering momentum. Venture Capital money is flowing into the space, while regulation, cost and the security risks of cloud data are pushing corporates towards it.

Individuals have the chance to take ownership of their own data. They can then choose to share it with trusted third parties. The data will then necessarily be richer than any stored by any of these third parties; it will be up to date and, of course, it will be private.

2.1 How This New Approach Can Improve the Status Quo

Individuals and companies can each benefit from a new consumer-centric approach to information in the following ways.

2.1.1 Individuals

i. Their Data will be Safer

Most cyber attacks are financially motivated. Criminals want to steal thousands, or even millions, of details in one attack. When data is stored by individuals, hackers could, in theory, still try to steal it, but it would be the digital equivalent of spear-fishing, therefore less worthwhile.

ii. Their Data will be More Accurate

Most people do not meticulously update their online accounts when their details change; this means a huge number of records are flawed. When individuals keep their own records, this problem is solved.

iii. Their Data will be Wide-ranging

The organisations with which consumers interact online only have access to siloed information about them: a bank has access to financial information; a healthcare provider, to medical records; a retailer, to transaction histories. While this is reassuring in that most individuals would be reluctant for an organisation to know everything about them, it also means these organisations lack the broader insights to make truly informed judgements. Self-management of data puts a broad range of information in one place.

iv. Their Data will be Easier to Share

When information is siloed, none of the datasets held by organisations can easily 'talk' to other datasets. So if a consumer's insurer wants to view that individual's medical records, it cannot just ask permission and retrieve that data. In such scenarios, the transfer process is long, expensive and tortuous. Personal data management can make it simple and fast.

The sum total of all these pain points is that online life can be complicated and inefficient. Research by email specialist Dashlane in 2015 said the average UK consumer has 118 online accounts and that this could almost double up to 207 accounts by the end of the decade.[ii]

For every one of those accounts there are passwords to remember and details to keep up to date. Many believe this is untenable.

2.1.2 Companies

i. Data Management will be Cheaper

It is expensive to buy and run servers, not to mention securing them. Moreover, the cost of an attack is soaring. On average, says IBM, the average cost of a breach is $4 million per incident, up 29% since 2013. When people own their data, the need to build large data sets is reduced.

ii. Regulation will be Lighter

Regulators are looking at ways to protect consumers. In Europe, for example, GDPR (General Data Protection Regulation) legislation has been released and comes into force in 2018. It sets new laws around the security and transparency of data, which will add to the overall cost of keeping information about users (see section 5.1). Companies should see these regulations as a chance to re-think their data gathering. The personal data economy could help them address regulation.

iii. Trust will Improve

If data is exposed and customers suffer as a result, then affected companies may well receive a backlash. Existing customers (and potential new customers) might be concerned for the safety of their own data and migrate to alternative service providers. There may also be a negative impact on brand values.

The personal data economy offers companies a chance to be proactive about trust. By returning ownership of information back to their customers, they could achieve a boost to their brand.

iv. Companies can Focus on Core Business

In the ‘analogue’ days, shoe retailers sold shoes. Now they are expected to be digital security specialists. Many organisations are uncomfortable with these new required skill sets.

v. Companies can Offer New Trusted Services

Any company that lets individuals take back ownership of their data could use this as the basis for new customer relationships. They could build products and services that access customer data with full permission. An obvious example would be a health-related company launching an app that could capture fitness tracker information.

Case Study

2.2 Data Gathering, Trust & Security: What Customers Think

2.2.1 Four in Ten are 'Reluctant Sharers'

Multiple surveys and reports have revealed how consumers feel compromised by the need to constantly share data. The Mobile Ecosystem Forum's 4th Global Consumer Trust Report 2016, found 41% of mobile users identified themselves as 'reluctant sharers' of their personal data.[iii]

It also revealed that almost half (47%) said they would pay extra for apps which guaranteed the data collected would not be shared with third parties, while more than 1 in 6 (17%) were willing to pay a premium to ensure their data is protected.

2.2.2 An Explosion of Ad Blockers

Meanwhile, consumers are fighting back. The rise of ad blocking is an expression of this resistance. Installation of ad blocking software on mobile devices jumped 90% in 2015 to 419 million devices, according to PageFair.[iv]

2.2.3 Most Consumers will Share Data if there is Trust

Nevertheless, the reality is that consumers will, and do, trade their data for services. Microsoft's 2015 Consumer Data Value Exchange Study found that 56% of consumers believe that brands collect personal information from them without their explicit consent.[v] Yet 29% are willing to exchange their data for services that help them discover new ideas, content and products, or for more streamlined processes.

GfK's research is even more emphatic. It says 77% of people would provide companies with more information if they were sure the companies would not share it without permission. Meanwhile 71% would share if it saved money and 63% if it saved time.[vi]

2.2.4 Four Types of Data Sharers

Research by Columbia Business School's Center on Global Brand Leadership came to a similar conclusion. Its 2015 report *What Is the Future of Data Sharing? Consumer Mindsets and the Power of Brands*[vii] quizzed 8,000 consumers from the US, UK, Canada, France, and India.

It found more than 75% of consumers are more willing to share PII (Personally Identifiable Information) with brands that they trust, than those they do not know.

It also highlighted 4 types when it comes to data sharing:

- Defenders (43%) – most likely to guard their personal information
- Savvy and in control (24%) – willing to exchange personal information for perks
- Resigned (23%) – think data collection is inevitable
- Happy go lucky (10%) – content to share personal data with marketers

3. Commercial Potential: A 'Trillion Dollar' Personal Data Economy?

It is easy to understand the ethical dimension of the personal data economy. For reasons already explained, people are craving more privacy, less surveillance and greater security in their digital lives. However, ethics alone are unlikely to make the idea flourish. A more plausible motivation is money.

Experts believe the impetus must come from brands, utilities, government and other enterprises. If they can use the personal data revolution to make money, save money or make things happen faster (which equals money), then the market is more likely to experience strong growth.

Multiple research studies suggest companies could unlock huge value from a more honest and transparent sharing of data with customers, but how much?

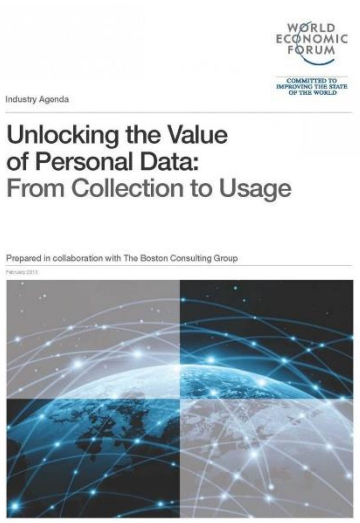
UK consultancy Ctrl Shift estimates a market opportunity for the PIMS market in the UK alone of £16.5 billion ($20.68 billion); data and life management services worth £11.5 billion ($14.42 billion) and decision support services worth £5 billion ($6.27 billion). This would account of around 1.2% of the UK economy.[viii]

Another approach is to look at the worth of the 'data driven marketing' industry; the earnings of data brokerage companies that collate information about people and sell it to brands.

According to the Data Driven Marketing Institute, the data brokerage industry generated $156 billion in 2012, approximately $60 per every one of the world's 2.5 billion Internet users.[ix] By the end of 2016, Juniper Research estimates that global Internet users will approach 3.5 billion, implying that, even if the value per user remained flat at $60, then the value of the data market would be $210 billion this year.

Indeed, the worth of that data could go significantly higher. The World Economic Forum suggests: 'It's reasonable to project that individual data will soon be worth over $100 per Internet user within just 10 years (by 2024).[x]

Figure 1: World Economic Forum Report



Source: World Economic Forum

This assumes that the only way the personal data economy can create value is by helping individuals to trade it. However, its broader impact could be to introduce efficient new business practices across every kind of organisation that deals with people.

For example, in the healthcare space, billions are spent every year on capturing, storing and sharing medical data. BCG (Boston Consulting Group) says that replacing siloed data with complete data held by individuals could 'reduce duplicate lab testing and imaging, fraud, and inefficiencies as well as improving care coordination and treatment.'[xi] It suggests that the savings could reach $700 billion in the US, or about 30% of the current annual bill.

3.1 A Brief History of the Personal Data Economy

a) 2005-2011 – The Attention Trust & the Locker Project

The idea of transferring stewardship of data back to the individual can be dated back to 2005, when a group of US programmers launched the Attention Trust; free open source software that let people record information about the websites they visited and then share it.

The AttentionTrust was succeeded by the Locker Project in 2011. It used APIs (Application Programming Interfaces) to pull in tweets, updates, pictures, check-ins, transactions and so on, into a single repository (on the desktop). In theory, developers could build apps on top of the service and, with permission from users, analyse the data to deliver better products and services.

Both the AttentionTrust and the Locker Project were ahead of their time, but they did popularise the concept. In 2012, the digital thinker Doc Searls caught the mood in his book *The Intention Economy*.[xii]

b) 2012: The Ideas of Doc Searls – the Intention Economy, Vendor Relationship Management & Intent Casting

Searls' main insight was that the digital era had tilted the balance of power massively away from customers and in favour of suppliers. This imbalance was expressed not just in the data, but also in the legal agreements. Searls said that in one-to-one business relationships, the 2 parties typically create an agreement that suits them both. However, in a market of one entity serving millions of customers, this cannot work. The net result is 'adhesion' contracts running to million of words that load all the power in favour of the enterprise.

Searls proposed a re-balance. He suggested that giving customers control of data would let them release their information to trusted third parties. Rather than having an 'attention' economy in which organisations profile customers and try to guess what they want, customers would be able to notify companies of their 'intentions'.

He stated that customers should be able to say: 'This is my personal data place, where we store personal data that is useful to us in market interactions and also our preferences and policies, terms and services. For example, "don't stalk me" or "give me back my data when I'm done with it." Here are the things you can look at, here are the things you can't.' Searls called this VRM (vendor relationship management), the flipside of CRM (customer relationship management), where companies collate data about customers. He even started a ProjectVRM initiative with Harvard University to track activity in the space.

Searls continues to be a leading light in the personal data economy, though his ideas remain mostly theoretical. However, he did allude accurately to the work needed to make it real: 'Customers need to have signalling that's fully respected and respectable. It's going to take apps, it's going to take protocols, it's going to take some new inventions and some new concepts.' This was a prescient observation; in 2012, those factors didn't exist, now they are closer.

4. The Personal Data Economy: Why Now is the Time

For an individual to own their information, they need 4 things:

- Storage space
- Bandwidth
- An easy way to organise it
- A consistent way to share it

Today, people have storage space and bandwidth thanks to smartphones with affordable data plans. They can use services like Dropbox and Google Drive, sometimes for free.

However, consumers need intermediaries to help them organise their data and share it with trusted third parties. Various organisations have emerged to do this including start-ups calling themselves PIMS (Personal Information Management Services), government, telcos and more.

4.1 PIMS (Personal Information Management Services)

PIMS offer a digital platform or app that enable people to accrue and trade data about themselves. Enterprises can link to these apps with protocols/APIs that access the data and pull out what they need.

Some estimates suggest that there are currently up to 700 PIMS,[xiii] but most of these are in development or are research projects. In terms of operational entities, only a select few have built viable platforms and gathered significant funding. The following 3 profiles focus on companies with 3 distinct approaches and business models.

4.1.1 Digi.me

UK-based Digi.me is one of the most visible of all the PIMS. The company raised £4.2 million ($6.1 million) in Series A funding in 2016, led by global re-insurer Swiss Re. Shortly after, Digi.me added a further £1.1 million ($1.34 million) from the Omidyar Network, an impact investment firm created by eBay founder Pierre Omidyar.

Digi.me offers an app that gathers a user's data in one place and lets enterprises build compatible apps (or bots) that can interrogate that data. Crucially, all the data sharing happens on the device. As Digi.me says, its service brings the processing to the data, not the other way round.

This ensures that neither Digi.me nor the enterprise ever see the customer's information; the individual is free to give a third party access should he/she wish.

Digi.me understands that this is a big idea, possibly too big for the average customer to grasp in one go, and is therefore taking a step by step approach. Thus, the first version of its app is designed purely to give users a better way to organise their social media accounts.

Figure 2: Digi.me App Snapshot

Source: Digi.me

The company argues that people will download the app because it offers universal search across their social media content and that, in the longer term, it can become the home for all kinds of personal data. For example, a user would simply log into his/her banking app from inside Digi.me to capture financial data, or could connect a health wearable or allow the app to record their location history. Thereafter, users could expose their data to brands and utilities in return for faster, better and more personalised services. The company is now working on projects with businesses in the health, finance, FMCG (Fast Moving Consumer Goods) and telco sectors.

The app is available on the main app stores and a desktop version has been pre-loaded by Lenovo and Toshiba. At the time of writing it has 400,000 users.

4.1.2 Meeco

Australian/UK company Meeco was launched with a mission to champion consumer rights. It offers an app that lets people curate a huge amount of information about themselves. Its 'life tiles' gather basic profile information, contacts, browsing habits, favourite brands and so on.

Figure 3: Meeco App Snapshot

Source: Meeco

Users can then share some, or all, of this information with other Meeco-using contacts or organisations. This could be something as simple as sharing a tile dedicated to a user's child with grandparents.

Other use cases are more practical. If a person's address changes they can update it once and then share it with every person or organisation. Meeco also has a privacy/security dimension. It offers plug-ins that prevent cookies from tracking activity when users are online.

The app includes the ability to do 'intentcasting' via a My Intentions section. Here, users can list the products and services they would like to purchase. The facility is anonymised, but the wishlist is open to any brand that wants to make an offer.

Finally, the app features My Insights, where Meeco crunches all data from across the app to reveal charts and graphs. The idea is that users can analyse these charts to understand themselves better.

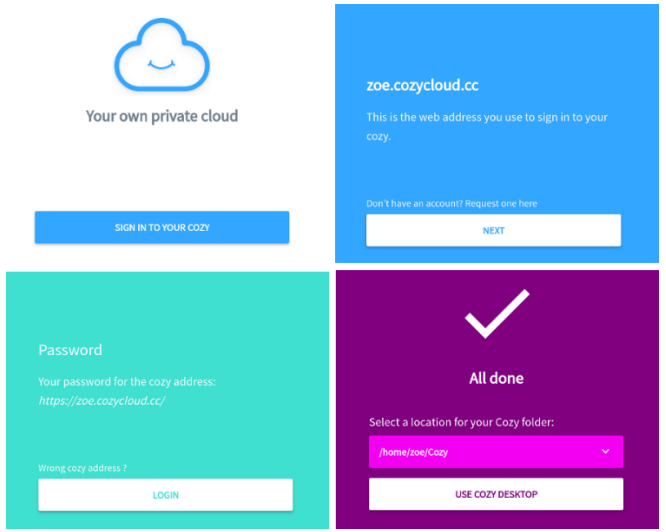
The company has been acquiring users via partner enterprises and developing brand allegiances via its Meeco Labs division. This helps organisations to examine how they can improve efficiencies by engaging with customer data.

4.1.3 Cozy Cloud

The French company was founded in 2012 and is a high-profile supporter of the personal data economy.

Specifically, Cozy Cloud offers what it calls 'an easy-to-use personal cloud solution', allowing customers to host their data on a personal server offered either by Cozy Cloud itself or by a trusted third party. Within this server, users can aggregate all their personal data (emails, calendar, files, contacts, IoT-generated data, third party data, such as bank accounts and bills).

Figure 4: Cozy Cloud App Snapshot



Source: Cozy.io

Users can then download applications that link to this data, available from a marketplace similar to the iOS and Android stores. Cozy has gathered several high profile brand supporters and €4 million (S4.37 million) in investment. Its partners include Gandi, OVH, La Poste, INRIA, EDF and Orange. It has worked closely with the French digital agency Fing on the MesInfos project (see below).

4.2 Personal Data Projects: Telcos, Social Networks, Government & Digital Agencies

PIMS are not the only entities exploring the power of personal data. Here are a selection of projects run by mobile operators, social networks, government and digital agencies.

4.2.1 Facebook Takes Heed

For the more idealistic proponents of personal data, the digital giants known as a GAFA (Google, Amazon, Facebook, Apple) can represent the 'enemy'. They are the firms that collect the most data from individuals and, it is argued, do little to explain what they then do with it. However, the truth is that (as of June 2016) 1.7 billion people worldwide use Facebook every month. It is likely that the vast majority of them would continue to do so, even without complete transparency over Facebook's use of their data.

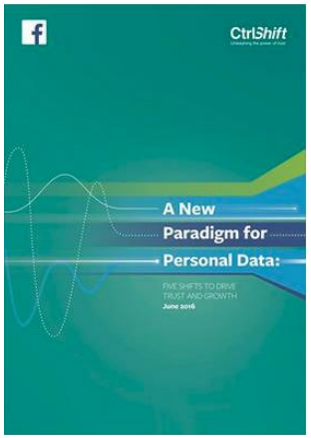
Facebook has emerged as a proponent of the idea of returning personal data to the person.

In 2016, it published a paper, *A New Paradigm for Personal Data*, drawing on the thoughts of 175 experts to explain its vision. In it, Stephen Deadman, Facebook's Global Deputy Chief Privacy Officer, argued that Facebook is better placed that regulators or security specialists to give people the tools to 'start becoming hubs for their data'.

He wrote: 'Too much of the debate (about personal data) has focused on risks and harms, at the expense of the opportunities and benefits. The debate also entrenches an assumption that only organisations can control data, ignoring the ability and potential of individuals to take a more active role, exercising agency, choice and control over their own data.' [xiv]

The paper focused on the potential of personal data and its mere existence reflects Facebook's desire to think carefully about data, privacy and security.

Figure 5: Facebook Report



Source: Facebook

4.2.2 Telecom Italia: My Data Store

Since 2014, Telecom Italia has been running a My Data Store project to investigate the personal data economy. It involves a few hundred citizens in Trento, northern Italy.

My Data Store itself is a secure, cloud-based digital space owned by the user. It is a repository for their personal information and also gives them the tools to share this data with third parties.

Data included in My Data Store includes:

- Location and movement (via GPS sensors, accelerometer, proximity records via Bluetooth etc)
- Data collected by mobile apps (eg games, chat, personal expenses manager)
- Biometrics from connected devices, wearables and sensors
- Social media and online behaviour

The My Data Store architecture lets developers build certified and trusted applications that can link to it via APIs. Users, meanwhile, can set their preference based on the data type, time duration, anonymisation level and so on.

Apps built for the project included; SecondNose, which aggregated sensor data from the participants to assess air quality and Personal Money Manager, which examined financial data to make recommendations.

4.2.3 Fing: MesInfos

In 2013, France's MesInfos project brought together 300 customers with large companies including Banque Postale, Credit Cooperatif, Google Takeout, Orange, Société Générale (bank account data), Intermarché (retail purchase data) and AXA (insurance contracts).

It wanted to explore how companies and public agencies could share personal data back to customers for their own use. In this sense, it was similar to the UK government's midata initiative (see section 4.2.5), although in this instance the national government played no part in it. Instead, it was run by a Paris-based think tank, Fing (Next Generation Internet Foundation).

'The quality of personalisation is still lousy online, and consumers are more fickle than they've ever been. I think sharing data will give some brands the opportunity to build more trust and loyalty.'
Daniel Kaplan, CEO of Fing (Next Generation Internet Foundation)[xv]

The project selected French start-up Cozy Cloud (see above) to provide a 'personal cloud' for users to host their data and through which to interact with the aforementioned brands. At time of writing, ithe service is still in pilot mode; no end date has been specified.

Data holders provided 40 different types of data divided into 2 categories: transactional (cash register receipts, geolocation data, call logs, bank statements etc) and profile (identity information, household data, vehicles, contracts/policies, income etc). 5 million data items were transferred across the project.

Through the Cozy Cloud platform, users could download a third party app to their personal cloud, which would then access their data. In each case the system would reveal which datasets were to be accessed and why. The testers could also choose to uninstall applications at any time.

4.2.4 MyData Finland

In Finland, as elsewhere, government agencies hold information which citizens, enterprises and researchers are entitled to use. In reality, such data is not easily accessible and rarely interoperable. The Finnish Open Data Programme was founded to address this, so it launched the MyData project on personal information. This started in 2013 with a mission to 'help individual people manage and reuse their personal data currently controlled by companies and governments'.

The project has 3 components:

- MyData Infrastructure – a technical architecture defining the way the data should be organised and shared;
- MyData services – case studies of real usage;
- MyData Alliance – a network for company collaboration.

It also has 3 guiding principles:

- Human centric control and privacy: Individuals have the right and practical means to manage their data and privacy.
- Usable data: Personal data should be technically easy to access and use; data from closed silos must be reusable so that individuals can manage their lives. The providers of these services can create new business models and economic growth.
- Open business environment: The MyData infrastructure should improve interoperability, make it easier for companies to comply with data protection regulations and let individuals avoid proprietary data lock-ins.

Early case studies included the web portal minunterveyteni.fi, which is used in the City of Hämeenlinna to give patients access to their electronic medical record. The aim is to let the patients self-evaluate the symptoms based on the combined data. Ilona Rönkkö, Project Manager, Health Services, City of Hämeenlinna, said: 'Healthcare has long been based on closed data and, in the end, the amount of data provided by electronic patient record is scant. This pilot encourages us to see and develop options that take into account what we really know about peoples' health. This kind of involvement is known also to improve patient's commitment to the care.'[xvi]

4.2.5 midata UK

midata

In 2011, the UK government embarked on a partnership with 26 companies and regulatory bodies to explore the power of personal data. The idea was to help these entities release back the data they hold about their customers in a safe and portable format. Companies included British Gas, EDF Energy, Google, Lloyds Banking Group, Mastercard, RBS, Three and Visa among others.

The aims of the midata were as follows:

- To let individuals gain insights into their own behaviour;
- To allow individuals to make better choices of products and services;
- To allow individuals to manage their lives more efficiently.

Edward Davey, Consumer Affairs minister at the time, said: 'This is the way the world is going and the UK is currently leading the charge. We see a real opportunity here (but) we need to develop a platform upon which the innovation and services that drive growth can be built. midata aims to do just that.'[xvii]

Over the course of the project, the partners agreed a format and then made .csv midata files available from their online sites. Customers could download the file and then share it with third parties as requested.

It took until 2015 for the first commercial services to make use of midata, which centred on price comparison for financial services and energy.

i. Energy: the Voltz App

Voltz

The UK energy market is highly competitive, with a large number of service providers each offering numerous energy tariffs to consumers. To help them navigate this complexity, Voltz launched a free comparison app. Voltz requires access to customer accounts to make the best recommendations and it uses midata to do this.

App users can select their current provider's name and then give permission for Voltz to retrieve their data through the midata system. Armed with this information, Voltz can then make a correct assessment of whether the user should switch and, if so, which competitor has the most suitable and competitive product.

ii. Current Accounts: Gocompare

Gocompare is a very popular shopping comparison site. While it can make the best recommendations when it has the correct information, expecting users to enter that information is an obvious friction point.

In 2015 Gocompare added a blue 'search using midata' button for people looking for a better bank account; a click on this uploads the .csv file. Gocompare can then produce an account comparison showing how much a user could earn, or lose, by switching to another current account. It also gives the individual insights into their financial behaviour.

'Consumers are acutely aware that the information a company holds about them has a value to that brand. The perceived value that consumers place on their data can change, (so) companies must consider not only how they convey what the customer gets in return for this data exchange, but precisely how the data is being used, and where in order to build that essential trust.'
Daniel Gurrola, VP of Business Vision, Orange[xviii]

Case Study

4.2.6 The Orange Data Privacy Charter

In 2013, Orange showed the desire for mobile operators to regain consumer trust by doing more to protect personal data. It revealed the Orange Personal Data Charter, containing a series of commitments to safeguard personal data and respect privacy.

Its 4 commitments pledged:

- Security of customers' personal data through its reliable processing and secure storage
- Control for customers over their own personal data and how it is used, including a personal dashboard
- Transparency in terms of the handling of data for its customers and users at all stages throughout our relationship
- Support for all its customers and users to help them protect their privacy and manage their personal data better.

5. Regulation & Compliance

All over the world governments are looking closely at the digital economy. They are scrutinising existing rules and acting to improve transparency and user control. It is possible to see this as a problem, more interference, more red tape

It is equally valid to view regulation as a reason to revisit data strategy. Many companies are choosing to do this; they see the personal data idea as a means to meeting compliance demands while starting a new relationship with customers.

This could encourage more customer engagement; many studies show that people will share more when they trust the third party (see section 7.8).

It is also true that the regulators themselves are keen to drive innovation, not stifle it. Elizabeth Denham, UK Information Commissioner, said in her maiden speech in September 2016:

'I do not believe data protection law is standing in the way of your success. It's not privacy or innovation – it's privacy and innovation. The personal information economy can be a win win situation for everyone. Get it right, and consumers and business benefits.'[xix]

5.1 GDPR (General Data Protection Regulation)

GDPR takes effect in May 2018 and will, unlike previous legislation, affect companies of all sizes, in all regions and in all industries across Europe, as well as any foreign company processing data of EU residents. Organisations found to be in breach of GDPR can be fined up to 4% of annual global turnover or €20 million ($21.8 million), whichever is greater.

The main provisions of the new regulation are as follows:

5.1.1 Consent

Companies will have to be more transparent about how they gather data, the nature of that data and how it will be used. Indeed, consent must be 'clear and distinguishable' from other terms and conditions. It must be as easy to withdraw consent as it is to give it.

5.1.2 Breach Notification

Where tthere is a data breach that is likely cause a risk to individuals, companies must notify their customers within 72 hours.

5.1.3 Right to Access

Data subjects will have the ability to find out how their personal data is being processed, where and for what purpose. They can even demand a copy of their personal data, free of charge, in an electronic format.

5.1.4 Right to be Forgotten

Individuals must be able to erase their personal data and thereby prevent its further dissemination. This could be because they wish to withdraw consent or it could equally be because the data is no longer relevant.

5.1.5 Data Portability

People must be able to take their data with them and move it if they wish to another 'controller'.

5.1.6 Privacy by Design

Essentially this means building in privacy controls rather than bolting them on later.

5.1.7 EU Payment Services Directive 2

This new EU regulation will bring personal data economy ideas to the financial services space from 2017. It will compel banks to open up their platforms to third parties (with customer permission). This is called Access to Accounts (XS2A). It will encourage new services to launch that can help people manage their financial affairs more efficiently.

5.1.8 The US/EU Privacy Shield

In July 2016, new rules around the sharing of Europeans' personal data by US companies came into force. The Privacy Shield agreement aims to provide EU consumers with information on what data is moved to US servers and how they can make complaints if they feel rules have been broken.

The Privacy Shield replaces the previous Safe Harbor framework, which relied on organisations merely stating that they complied with EU rules. The new system has a dedicated US ombudsman to handle complaints. Companies signing up to the Shield must abide by guidelines such as deleting personal data when it is no longer necessary.

5.1.9 The Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS)

This EU regulation, often referred to as simply 'eIDAS', intends to create a regulatory environment whereby public services in any EU member state must accept citizens and businesses native electronic identification schemes. The goal is to reduce both the time and friction when it comes to digital transactions cross-country.

Should the EU succeed in pushing this directive at a national level, promoting mass adoption within the EU borders, the systems, protocols and stardards would arguably become the gold standard of identification.

5.2 Global Data Protection Laws

It is clearly beyond the scope of this White Paper to describe data protection laws across the world. Broadly, it is fair to say that most countries do not have definitive agreements in place. Often, rules vary by region or state. However, many nations are working on new frameworks.

5.2.1 Brazil: Data Protection Bill

The current version of the Personal Data Protection Bill is fairly reflective of most regulation. Thus, companies need a user's consent to collect their personal information. They must also keep a record of the date and time of the application's use from a particular IP address for at least 6 months. Access to the data must be strictly controlled and encryption or equivalent protection measures must be in place.

Now, the Brazilian Congress is considering a new bill governing the use of personal information. It is based around the following principles:

- Data must be used for legitimate, specific and explicit purposes, which are clearly indicated to the user.
- Data must be transparent, with clear, adequate and easily accessible information relating to the use of data available to the user.
- There are new definitions for 'sensitive' and 'anonymised' data, which provide more clarity around the transfer of data out of Brazil.

5.2.2 South Africa: PoPI Act

In South Africa, the PoPI (Protection of Personal Information) Act was signed by the country's president in November 2013, but it has yet to come into force. Under the terms of the Act, which was largely based on the European Data Protection Directive, personal information:

- Must be processed lawfully, in a manner that is not excessive in relation to the purpose for which it is processed; in a manner that does not infringe the privacy of the data subject; and either with the consent of the subject or, if otherwise justifiable, to protect the legitimate interests of the data subject.
- Must be collected for a specific, explicitly defined and lawful purpose, with the data subject made aware of the purpose of collection of the personal information collected.
- Must be stored securely, with the responsible party maintaining the documentation of all processing operations under its responsibility and taking reasonably practicable steps to ensure that the data subject is aware that its personal information is being collected, who is collecting it and for what purpose it is being collected.

The Act also grants individuals rights with regard to establishing whether a third party holds their personal information and, if so, to request access to that information (and where necessary, the correction, destruction or deletion of that information).

There are suggestions that the delay in implementing PoPI arises from concerns that it may no longer meet the requirements of EU laws following the forthcoming introduction of GDPR.

6. Can Personal Ownership of Data Help Solve the Identity Puzzle?

In the digital world, the issue of 'who you are' is hugely important. Every organisation wants to be sure you are who you say you are, from the eRetailer to the tax office to the bank. There are two main issues with this. First, it is very easy for fraudsters to exploit the system when all that is required is an email address or password. Secondly, when the burden of proof is higher, this can be highly problematic for users.

These users might have to supply passport numbers, bank account details, letters from employers and so on. This information is hard to access and time-consuming to enter, particularly when, given the continuing digital migration, consumers have to re-enter the same information for a multiplicity of services. Furthermore, with that information now being stored by numerous online providers, it increases the risk (and the consumer's perception of the risk) that the data will be exposed and potentially misused.

Finally, this process is unsubtle. If an organisation only needs to know your age, why does it need to ask about anything else?

One partial solution to this quandary is being supplied by Facebook, Google, LinkedIn, GSMA and others, in a mechanism called federated identification, whose ultimate goal is to enable users of one domain to securely access data or systems of another domain seamlessly. They all offer log in services for identification. However, what they know about people is still limited, while there is concern about assigning these companies such an important role.

Giving individuals control over their own data, and thereby their various proofs of identity, offers potential solutions to these problems.

6.1 Government Initiatives: Verify

The UK government's Verify scheme asks citizens to assign their identities via authorised providers, Digidentity, Experian, the Post Office, Verizon, Barclays, GB Group, Morpho and PayPal. People supply information and answer questions to prove who they are. They are then sent an OTP (One Time Password) to their phone for final authentication.

Thereafter, when they use a government service, they can sign in through their ID provider and enter another OTP to complete the process, substantially reducing the time and effort required.

In the case of Verify, the UK government says its providers are required to meet strict privacy and security requirements.

Such schemes are likely to proliferate, given its applicability across a raft of organisations both to reduce dependency upon lengthy forms and intrusive questions and to accelerate administrative processes.

6.2 Start-ups: MyPinPad, Iproov, ShoCard, SITA

A growing group of new companies are building their own solutions to the identity problem. The UK's MyPinPad, for example, has designed a solution which creates an OOB (out of band) issuer domain challenge to authenticate cardholders. Instead of a webpage for password entry, consumers are directed back to mobile banking applications for authentication. Another UK firm, Iproov, uses machine learning technology to check that the user's face corresponds to the face they originally enrolled.

In the US, blockchain start-ups ShoCard and SITA offer identity solutions for the travel sector.

These companies argue that their ID products can work across a range of scenarios, both digital and 'real world'. Financial services is leading the way, but it could apply to anything from plumbers making home visits, to people selling on eBay or customers wishing to prove their age at nightclubs and so on.

6.3 Mobile Operators: Mobile Connect

The world's telcos possess important information about their customers: name, address, gender, location and so on. All of it is linked to the consumer's mobile number, so could the mobile number become a trusted source of identity? Operators think so. They created the Mobile Connect service to let customers log in to third party sites using their mobile number.

The system asks the user to enter the number, combined with a PIN for more secure use cases, to access online services anywhere they see the Mobile Connect logo. Importantly, there is no exchange of information. For example, an organisation might 'ask' Mobile Connect whether a person is over 18. The system would provide a reliable yes/no answer without sending the data.

In February 2016, the GSMA announced that Mobile Connect was now available to 2 billion consumers via 34 operators in 21 countries.

6.4 How Blockchain Could Help: Sovrin

A big question mark over identity providers is how they can keep the information safe and immutable. Some believe blockchain provides the answer. Using a distributed ledger to store a person's many proofs of ID should be safer than locking it in one server. This is the argument put forward by ID specialist Evernym. In September it launched a free-to-use, open-source global identity network called Sovrin.

Evernym describes Sovrin as a 'self-sovereign identity platform that can give everyone a digital identity they fully own and control: no one can read it, use it, change it, or turn it off without the user's explicit consent.'[xx]

7. How Individuals & Companies Could Benefit from the Personal Data Economy

'Customers have to recover their digital sovereignty, own their digital footprint and consciously decide how they want to make use of their data.'
César Alierta, former Executive Chairman of Telefónica[xxi]

7.1 It Can Make Business More Efficient

For many in the personal data economy, this is the most important benefit of all. They argue that when companies realise they can make substantial cost reductions or time savings, they will have the motivation to embrace the idea.

On a very basic level, there is the simple benefit of keeping records up to date. An individual with a personal data app would keep that app up to date with all their profile changes, email, phone number, address, bank details and so on. He/she could elect to automate those updates with all approved third parties.

Other scenarios offer more radical improvements. A hypothetical example of this comes from Digi.me (see section 4.1.1) and centres on medical insurance on-boarding. At present, this is expensive and time-consuming. A medical claim would involve the insurer asking a claimant to fill out a form and then send it to the insurer, who would pass it on to a doctor for verification, who would in turn charge for his/her time. This process may take weeks.

If the insurance company could connect to a personal data app that already contained all the demographic and medical data, the form could be completed and transferred in seconds.

Meanwhile Meeco is building a 'signal' function that lets people create wish lists of products and services they can share with trusted brands.

7.2 It Can Help People Manage Their Lives

When information is spread across multiple silos it can be hard for individuals to organise their affairs. This is an obvious focus for the personal data economy and the best examples of it are in banking and personal finance.

Here, a number of companies have emerged to offer consumers the ability to see all their accounts in one place. Some will even analyse the transactional activity to offer advice and suggest changes.

Examples include Mint and Yodlee in the US, and OutBank and Numbrs in Germany. They work in slightly different ways. Apps like Mint ask for a user's bank account log in details and pass this data on to Yodlee, which 'scrapes' the account information and then saves it on servers. The apps then crunch the numbers and display them as easy-to-read charts and graphs.

OutBank and Numbrs are more sophisticated because they do not require a person's log in, using open banking APIs instead. Here, the app itself imports account information from virtually any bank and then tracks spending, sets budgets, creates alerts and projects future financial patterns.

This is possible because Germany has its own open banking protocol, FinTS (Financial Transaction Services), which is now supported by more than 2,000 banks.

In 2018, all banks in the EU will be compelled to open up their APIs as part of the new Payment Services Directive 2 legislation. This should result in a flood of new intermediaries like Numbrs and OutBank. The banking fraternity calls them AISPs (Account Information Service Providers). However, it should be noted that the banks themselves could become AISPs if they so wished.

7.3 It Can Give People Self-Knowledge & Personal Insight

There is a theory, espoused by many of the extant personal data ventures, that when people have a store of information about their behaviour, they can discover insights about themselves. Personal finance apps such as Numbrs (see above) certainly help people get a complete picture of their financial affairs.

Other companies focus on a more psychological type of insight. An app provided by UK-based Citizenme harvests social profiles and lets users answer quiz questions framed like a personality test. For users who wish to go further than simply taking the quiz, Citizenme offers the chance for them to share their profiles, privately, with brands for market research purposes.

7.4 It Can Help People Make Better Spending Decisions

The digital age has made it easy for people to switch between product and service providers. However, they only do this when it is easy and the information is available. This has led to the rise of powerful 'comparison' sites. The next phase of this market trend is, surely, analysing a customer's existing transactions and relationships to make personalised recommendations.

This can be best achieved when customers have access to their own data. The best examples of this come in markets where APIs have been opened up (German banking, for example, see section 7.2).

UK-based ctrlio specialises in mobile phone tariff comparisons. It analyses a person's last 3 online bills to calculate monthly usage. It tokenises the information and sends it to interested suppliers. It then haggles with the brands to derive the best discounts.

7.5 It Can Give People Control Over Terms & Conditions

When companies store vast troves of data about thousands of people, they do it on their terms. They have to do this; it would not make sense to negotiate every contract individually. In the personal data economy, however, individuals could in theory set their own terms and conditions. Companies could then agree or not to accept them.

This scenario is some way off. Nonetheless there are indications of it in the market already. MyPermissions, for example, lets users control access to their personal information on mobile devices and online. Its tools include a web browser plug-in that gives users real-time alerts whenever a new application connects. It also lets people control the data that apps are able to access.

7.6 It Can Be a Tool to Help Social Causes

Not all data gathering has to be for financial gain or personal enrichment. Sometimes it is possible to share data for good causes and the best example of this is in healthcare.

In the US, the non-profit organisation PatientsLke Me asks people to share their symptoms, treatment information and health outcomes on a collective database. It then turns this into millions of datapoints about diseases, aggregates it and organises it to reveal new insights. Over 400,000 people contribute, generating 35 million datapoints to date.[xxii]

PatientsLikeMe's insights even reversed conventional medical wisdom in one case. It reported in 2011 a challenge to the belief that lithium carbonate could slow the progression of a neurodegenerative disease, ALS. The results of its research were published in the journal, *Nature Biotechnology*.[xxiii]

At present PatientsLikeMe appears to work on the basis of manually entered answers from its members. However, it is easy to see how it could one day gather information through wearables/monitors and electronic medical records where available.

Figure 6: Wearables: A Future Data Source for PatientsLikeMe

Source: Fitbit Press Library

7.7 It Can Enable Deeper Relationships with Brands & Enterprises

Proponents of the personal data economy argue that once a person has engaged with a brand, it can lead to much richer relationships. Consider the example of insurance (see section 7.1). The thesis is this: an individual shares their data with an insurance company to speed up their claim. It all works quickly and with minimal friction. Now, the insurance company is in a position to re-define its relationship with its customer.

It could ask the policyholder to wear a monitor and link this to an app that reveals insights, and offers advice, on healthy living. It is important to state that this would not be done merely to reduce payouts or weed out high-risk customers. Instead, it could change the dynamic such that the insurer would be perceived as a healthcare partner, rather than a financial instrument of last resort.

7.8 It Can Give Any Company Access to Rich Data

An intriguing argument is that the personal data economy could break the monopoly of digital giants in 'Big Data'. At present companies like Apple, Facebook and Google have an advantage over other businesses by virtue of what they know about users. However, if every customer had their own personal data store, they could share it with any organisation. In theory this would mean that even the smallest company could know more about a potential customer than the biggest tech giant in the world.

7.9 It Can Let People Sell their Data to Brands

Much of the early discussion around the personal data economy was concerned with the 'economy' side of the equation. The argument ran: if companies want information about people because it is valuable, why shouldn't people sell it to them? The debate has grown broader since then.

Some companies are still exploring this commercial idea; the most visible being Datacoup and People.io. Datacoup is a US start-up that launched in 2014. The company's premise was that as companies buy anonymous aggregated data to better understand consumer behaviour, why not just buy it from the people themselves rather than from a data broker?

Its service tries to facilitate this. The Datacoup site invites visitors to set up an account and then link it to their personal services via APIs. Thus, people can connect to their debit/credit cards, Facebook, Twitter, LinkedIn, Foursquare, Google+, Youtube, Tumblr, Meetup and Instagram.

Thereafter, Datacoup builds a profile of data attributes such as gender, education, or monthly spending. These are given attribute a high, medium or low value determined by the demand from third parties for that attribute.

Datacoup is targeting brands, retailers, media agencies, wireless carriers, insurance companies and banks. People can see their data profiles and click a public link to share it with these potential purchasers. They can also see what information is bought, who is buying it and why it is of value. The data is all anonymised.At launch, the company was paying around $8 a month to its members.

In the UK, people.io has a similar vision. It launched in beta in January 2016, but with a more local flavour. It invites users to share information on the things they like, or by connecting data services. They can then receive rewards from brands in return for the data. The company started with a pilot involving retailers in its own area of East London.

8. The Personal Data Economy: Key Challenges

8.1 Customer Apathy

Individuals may feel restless about data intrusion, but is this enough to bring about change? Many studies have shown that they continue to use data-harvesting services, even those that have been shown to collect information without consent.

This is why proponents argue that trust and security may not be the best arguments for personal ownership of data. Instead, the arguments should centre on removing friction and getting more value.

8.2 Customer Confusion

Even if people warm to the idea of holding their own data, it will not be easy to explain how they can do so in practical terms. Are people ready for it? The approach of most companies to date is to start with something simpler. A place to better manage your photos, or your bank accounts, or your social media activity, is easy to comprehend. This builds understanding through trials and can be the springboard for more ambitious services in the long term.

8.3 Security Concerns

If people do not trust retailers, banks, social networks and other online companies with their data, why should they trust a start-up PIMS? The counter-argument from many PIMS is that the data storage becomes a conscious decision by the individual (the data owner). Whether this is local storage or a personal cloud, it should be the choice of the individual.

8.4 Interoperability

Let's imagine that a number of personal data services become popular. Will enterprises develop products that 'talk' to them if they each use their own proprietary tech? Probably not.

Whomever emerges to dominate the market must ensure their services are interoperable. Customers must be able to switch without losing their data, while enterprises must be able to reach millions of users across different services with just one protocol.

8.5 Identification

When individuals take ownership of intimate personal data and start sharing it with trusted brands, identity becomes crucial. Simply, any intermediary helping a person organise their personal data must be certain that person is who they say they are.

8.6 Making Money

Personal data economy will need solid business models to flourish. There are multiple options; some take a revenue share when customers trade data for services (Datacoup), some charge a fixed fee for any brand engagement with the app (Digi.me), while some charge the consumer a subscription (Cozy Cloud). The market will decide.

About Mobile Ecosystem Forum

The Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. It provides members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that drives inclusion for all and delivers trusted services that enrich the lives of consumers worldwide. Established in 2000 and headquartered in the UK, MEF has Regional Chapters across Africa, Asia, Europe, Middle East and Latin America.

MEF's Global Consumer Trust Initiative was established in 2012 to raise awareness of importance of building trust in mobile products and services. It helps establish industry best practice and provides practical tools built on the consumer's informed consent. The multi-stakeholder Working Group includes privacy, identity and security experts from MNOs, enterprises, app developers, start-ups and technology providers with legal counsel, product and business executives participating in the initiative.

This whitepaper is part of the working group's new programme **Building Trust in Personal Data** which takes a cross-ecosystem approach to accelerate the development of a data-driven economy and driving long-term sustainability through best practice and consumer choice.

For more information visit www.mobileecosystemforum.com

Endnotes

[i] https://www.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ownership

[ii] https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/

[iii] http://mobileecosystemforum.com/initiatives/consumer-trust/global-consumer-trust-report-2016/

[iv] https://pagefair.com/press-releases/mobile-adblocking-reaches-419-million-globally/

[v] https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/

[vi] http://www.cmo.com.au/article/544315/consumers_reject_brands_asking_too_much_personal_detail_finds_adma_report/

[vii] http://www8.gsb.columbia.edu/globalbrands/research/future-of-data-sharing

[viii] http://www.nesta.org.uk/sites/default/files/personal_information_management_services.pdf

[ix] https://thedma.org/news/dma-announces-groundbreaking-economic-study-on-value-of-data-at-dma2013/

[x] https://www.weforum.org/agenda/2014/09/whats-value-personal-data

[xi] https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/

[xii] https://cyber.harvard.edu/events/2012/05/searls

[xiii] https://cyber.harvard.edu/projectvrm/VRM_Development_Work

[xiv] https://www.facebook.com/anewdataparadigm/

[xv] http://mobileecosystemforum.com/2016/09/28/qa-daniel-kaplan-frances-mr-personal-data-economy/

[xvi] http://cht.oulu.fi/news/digital-health-revolution-drives-mydata-transformation

[xvii] https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment

[xviii] http://www.orange.com/en/content/download/25975/581985/version/9/file/Press+Release+-+Orange+Future+of+Digital+Trust+-+FINAL.pdf

[xix] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/transparency-trust-and-progressive-data-protection/

[xx] http://www.prnewswire.com/news-releases/sovrin-foundation-launches-first-dedicated-self-sovereign-identity-network-300336702.html

[xxi] https://www.business-solutions.telefonica.com/en/information-centre/news/c%C3%A9sar-alierta-presents-we-choose-it-all-telef%C3%B3nica-s-new-strategic-plan-to-be-an-onlife-telco-in-2020/

[xxii] https://www.patientslikeme.com/

[xxiii] https://www.patientslikeme.com/press/20110425/27-patientslikeme-social-network-refutes-published-clinical-trial-br-bri-nature-biotechnology-paper-details-breakthrough-in-real-world-outcomes-measurement-i-