mydex

The Case for Personal Information Empowerment: The rise of the personal data store

Rather than owning and controlling their own personal data, people very often find that they have lost control of it.
The Economist Special Report: The Data Deluge,
25 February 2010

Wherever possible we believe that personal data should be controlled by individual citizens themselves.
Conservative Party Manifesto, 13 April 2010

The principle of commercial entities, acting as trusted intermediaries, exchanging assets on behalf of individuals, following a clear set of principles and legally binding contracts, could be applicable in a personal data ecosystem. This 'data vault' concept, an intermediary collecting user data and giving 3rd parties access to this data in line with individual users' specifications, is one potential solution that offers many theoretical advantages.
World Economic Forum: Rethinking Personal Data Project,
June 15 2010

The greatest impact of an increasing return wave comes long after the technology is first invented. It comes when the technology is democratised.
Matt Ridley in The Rational Optimist, 2010

Contents

Executive Summary

1. Our current approach to collecting and using personal data is dysfunctional. As individuals, we have lost control over our personal data, so much so that most of us see personal data management as a threat and a risk (identity theft), a hassle and a chore (red tape) and a source of frustration and irritation (organisations taking our data and losing it, abusing it by using it to spam us with junk messages, or handing it over to third parties who we don't know and have no control over).

Organisations are meanwhile discovering that the collection and use of personal data is:

- increasingly expensive, with high levels of waste from excessive duplication, error and inaccuracy, and guesswork
- corrosive to trust, turning off customers, which in turn undermines rather than strengthens relationships
- a brake on innovation and growth

2. A new personal information ecosystem is emerging. It is organised around individuals collecting, storing, managing, using and sharing their own personal data for their own purposes. Building on the technological revolutions of the last few decades (data warehousing, ubiquitous personal and mobile computing and internet connectivity, social networking) its core purpose is to help individuals manage personal data as a personal asset and resource which they can use to organise and manage their lives better.

3. The new personal information ecosystem will trigger and support a new wave of innovation and economic growth from a wide range of new services. These services will help individuals use their own personal information to research, make and implement better decisions in countless ways. They will help people when they lose their wallet, move home or buy a car, and help them manage their health or finances over long periods.

4. Many of the components of this new information ecosystem have emerged over the last ten years (e.g. online search, comparison sites, P2P product reviews, social networking, identity management, privacy-enhancing technologies). However, the catalyst around which the new ecosystem will crystallise is only beginning to emerge now: the Personal Data Store – a new type of personal information management service that helps individuals gather, store, update, correct, analyse and share their own data in ways that they can control.

5. Personal Data Stores represent a fundamental breakthrough in personal information management. They will:

- Give individuals the tools they need to realise the rapidly growing value of their own data in an increasingly online world.
- Unleash a new wave of economic growth around new types of information-driven personal services.
- Help organisations reduce the high levels of cost and waste inherent in their current organisation-centric approaches to the management of personal data, while helping them gain richer, more timely insight into their customers' needs and preferences.
- Help to create a climate of trust, leading to more information being used more responsibly, to add greater value for both organisations and their customers.
- Benefit society: the more confident and empowered individuals become in the management and use of their own personal data the more they will contribute positively to social, civic and economic affairs.

6. Organisations need to work with Personal Data Store providers such as Mydex to test, develop and prove Personal Data Store technologies, infrastructure, information sharing processes and mechanisms, legal and business models.

7. Governments and regulators need to pave the way for the new ecosystem by addressing online identity policy and being ready to work with structured authenticated data from verified individuals. This needs standards. It may need minor policy revisions. It does not need significant new legislation or major infrastructural investment.

1. Introduction: The tipping point

Over the last 50 years, the cost of computing – information processing – has fallen a billion-fold. The first hard drive was the size of a large cupboard and held a trifling amount of data by today's standards – just 5MB. By 1979 a hard drive capable of storing 250MB of data would fill a large supermarket trolley. By 2007, hard drives had reached the size of 1 TB (terabyte, i.e. 1,000 GB). Only two years later, the first hard drive with 2 TB of storage arrived: while it took 51 years to reach the first terabyte, it took just two years to reach the second. If the prices of motor cars had fallen as fast, you would be able to buy 4000 Rolls Royce Silver Shadows for just £1.

The rise of the computer (and everything it makes possible) has transformed our society: work, leisure, products, services – the economy itself. Within this transformation we can see some distinct phases.

In the first phase, before 2000, information processing power was embedded into products that were sold the normal way: personal computers, video games, cars, cookers, cameras, phones etc. This first phase will never end. Products will always get smarter, but the second phase took a new and different direction. Between 2000 and 2010 information-driven internet services exploded onto the stage: e-commerce (Amazon, e-Bay), search (Google), price comparison sites, blogging, social networking (Facebook) and so on. The big shift had begun: individuals were beginning to use information as a tool in their own hands, to pursue their own purposes.

The next phase is only just beginning. It takes the theme of information as a tool in the hands of the individual to a new level - and in a different direction. Up until now, even as the costs of gathering, storing and managing information continued to fall, the job of 'information management' remained a monopoly of big organisations. Organisations *managed* information. Individuals *accessed* it.

Today, individuals are becoming managers of their own personal information in their own right. As this White Paper shows, *that changes everything*.

2. Individuals as Information Managers

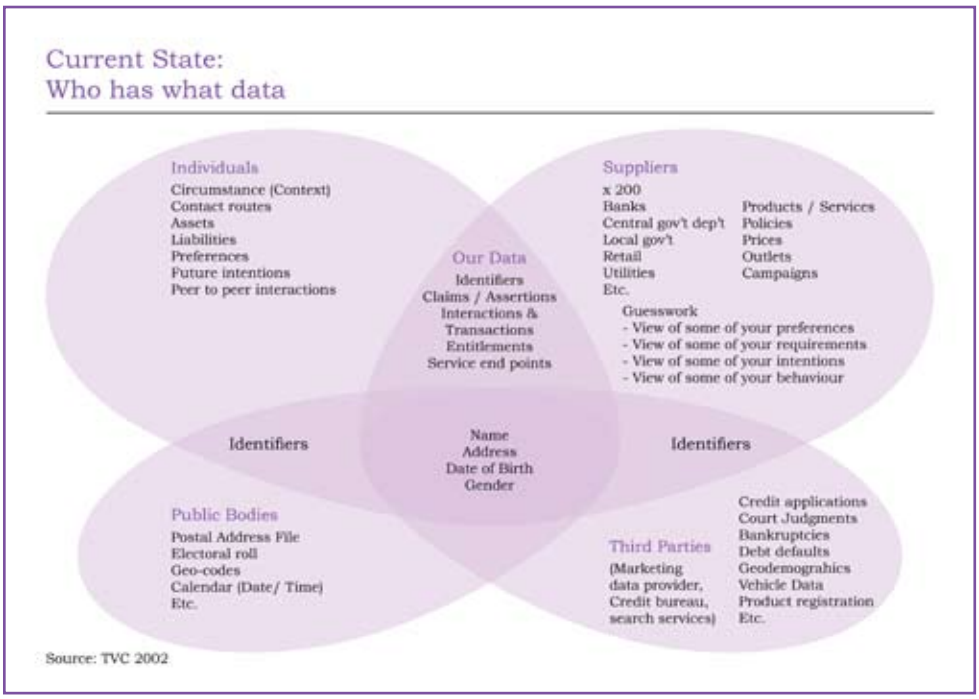
To organise and manage their daily lives in a modern economy/society every individual has to manage information, including:

- Keep, find and provide proofs and verifications such as driving licences, birth or marriage certificates, passport details, insurances.
- Keep records of transactions including orders, receipts, account statements, guarantees, booking references.
- Keep records of correspondence including letters, queries, complaints, and their responses.
- Inform other people or organisations of significant changes to personal details such as contact details or address.
- Make plans and arrangements and organise things; make sure that the right person, or thing, or piece of information is at the right place at the right time.
- As more and more services go online, we also need to remember a growing list of different user names, passwords, account numbers, reference numbers and so on. This is made unnecessarily complex as each service specifies its own, different, rules for how we should interact with it.
- Provide identity assurance, to convince other people and organisations that we are who we say we are.
- To manage 'life events' (such as moving home, buying a car, organising a holiday, getting married, changing schools etc) we have to bring all these things together, including being able to access the right information and advice to make the right decision in the first place.

For many years, individuals have managed these tasks as best they could, without technology to store or share information or software to organise, automate or streamline processes. We've made do with pieces of paper, an old shoe box, the fridge door and what we can remember in our brains. Meanwhile, on the other side of the fence, organisations' information management capabilities have raced ahead as they've deployed huge, sophisticated data warehouses, ERP (Enterprise Resource Planning) systems, CRM (Customer Relationship Management) systems, analytics, and so on.

As a result the world of information management has become highly imbalanced. Figure 1 maps who currently deals in different aspects of personal data. Three groups of organisations are all involved intensively in the collection, management, use and sharing of personal data: organisations who transact with customers, public sector bodies dealing with things like the electoral roll, and third parties who collect, process and sell personal data. All of them do this in a highly organised, systematic, professional, technology-supported way. The fourth group – individuals themselves – are effectively disempowered. The way technology has evolved, organisations have become managers of our data. We lost have control.

Figure 1:
the main managers of personal data



Personal Data Stores redress the balance. They do two hugely important things:

1) They deploy modern technologies to help individuals gather, store, access, update and change, use and share their own personal information, for their own purposes, PDS's, use technologies as sophisticated and powerful as the biggest corporation.
2) They help individuals share this information in ways they can control – enabling them to choose what information they wish to share with who, for what purposes.

At first sight these two services – helping individuals store and manager their personal data more efficiently and effectively, and helping them share this data in ways they can control – don't seem that remarkable. Dig a little deeper however, and we will see that these capabilities:

- transform relationships between individuals and organisations to *both* sides' benefit.
- are the catalyst and organising epicentre of an entirely new business and service eco-system of personal information management services.

But first, let's stick to the basics.

3. What do Personal Data Stores do?

The first thing to remember is that Personal Data Stores are a service to the *individual*. With a Personal Data Store, the data sits on the side of the individual under the individual's control; data is collected and stored in the individual's own database to be managed and controlled by that individual for the individual's purposes.

This is a central, critical departure point. Personal Data Stores are first and foremost a 'person-centric' service. They are not designed or implemented with any organisation's interests or agenda in mind. They exist to serve the individual.

We have to stress this (again and again) because the prevailing mindset sees the organisation as the manager of personal information and therefore just assumes that anything to do with the management of personal information has to be designed to fit the organisation's agenda. The message of this White Paper is that *this assumption is not only groundless, it's also damaging*. As we'll show, it is precisely because Personal Data Stores are designed as services to the individual that organisations' best interests will be served by them (see below).

But first, how do Personal Data Stores work for individuals?

Data storage: The first thing Personal Data Stores do is help individuals store, access and use the information they need to manage their daily lives. Take something boring but essential such as an insurance policy. We need to keep a record of the policy number, the certificate, the terms of the policy, how to claim, the details of correspondence relating to a claim, and so on.

We need similar information relating to everyone we deal with: most of us don't know it (because we don't stop to think about it and make a list), but at any one time we have a commercial relationship with about 200 different suppliers, all of them generating some information which needs to be stored, accessed and used at some point in time. In real life what tends to happen is that a) this information gets scattered across many places (a filing cabinet here, an email there), and b) when we need it, we can't find it. Personal Data Stores create a single, secure, easy-to-access store for such information so that when we need it it's at our finger tips.

Personal Data Stores will therefore be a godsend when little disasters happen, such as losing a wallet. Wallets are jam-packed full of vital, useful, valuable information. Your wallet could include your credit cards, driving licence, passport, membership cards, loyalty scheme cards etc. With a Personal Data Store you simply retrieve a list of your current active cards, licence and passport details etc along with necessary contact points. Instead of having to phone a call centre for each organisation (waiting in frustrating queues for each one, giving the same painful

details again and again) the PDS can create one single message informing them of the fact that the card has been lost. It can then be sent securely, direct to their systems by-passing traditional call-centres, log-ins and passwords and so on. It can be done in a matter of minutes – a 'one-click' hassle free process rather than a bureaucratic nightmare.

In other words, Personal Data Stores are *convenient*. They help people do things they already have to do, only much easier and much better.

Figure 2:
Some of the challenges of personal information management

The challenge of personal information management:
Some of the ways individuals routinely use information in their lives

Gather	Provide identification	Set goals, targets	Anticipate
Store	Authorise	Set priorities	Scope
Authenticate	Give permission/s	Consider trade-offs	Plan
Verify		Manage trade-offs	Forecast
Share	Ask questions		Set budgets
Protect	Seek advice	Offer	Monitor variances
Transfer	Clarify	Negotiate	Report exceptions
Dispose		Make agreements	
Combine	Research possibilities	Mediate	Complain
Sort	Identify alternative options		Suggest
Manipulate	Create wish lists	Organize	Express opinions
Correlate	Identify preferences	Arrange	Argue
Anonymize	Identify constraints	Co-ordinate	Campaign
Personalize	Research pros and cons	Integrate	
Duplicate	Evaluate and weigh		Share notes
De-duplicate	options	Benchmark	Gossip
Audit	Identify risks	Monitor	Share experiences
Keep records	Evaluate risks	Check	Explain
Search for	Specify	Adjust	Interpret
Find	Stipulate	Assess	Reassure
Access			Celebrate/commiserate
Update	Choose	Learn	Joke
Correct	Express preference	Keep up to date	Tell stories
	Vote	Stay informed	

Data management: The second thing Personal Data Stores do is help us manage this information better. Figure 1 lists many of the common information processing activities we undertake every day of our lives. We do them so automatically we don't realise how many different processes there are, or how sophisticated and complex they can become. Personal Data Stores help us translate these information processing activities to an increasingly online digital world, giving us tools to undertake a wide range of information management tasks including: Gather, Store, Authenticate, Verify, Share, Protect, Transfer, Dispose, Combine, Sort, Manipulate, Correlate, Anonymise, Personalise, Duplicate, De-duplicate, Audit, Record, Provide identification, Authorise, Give permission/s.
(For more on some of these tasks, see below).

Data sharing: The third thing Personal Data Stores do is provide individuals with better, more sophisticated tools for information sharing. This can work in many different ways, so let's look at a few examples.

Currently, when conducting transactions online, the typical process goes something like this. We choose what we want to buy. Then, to complete the transaction we have to tick a box declaring that we have read and agreed to the organisation's terms and conditions, privacy policy etc. Ticking the box is a condition of completing the process so most of us simply tick without further ado – without really knowing what we are agreeing to (neatly illustrated by Gamestation's "Immortal Soul Clause", obediently ticked by 88% of customers. The 12% smart enough to read it and uncheck got a £5 gift voucher).

Personal Data Stores reverse the process. If the organisation wants to gain access to information in the individual's Personal Data Store, before it does anything else, the organisation has to tick the *individual's* terms and conditions. (For more detail, see the box: Information Sharing Agreements). This allows individuals to *specify what information they wish to share with which organisations, for what purposes under what terms and conditions*: what we call Selective Disclosure.

Selective Disclosure works in two main ways: bespoke and automatic. Bespoke information sharing happens on a one-on-one basis. It is negotiated individually for each new situation. For example, a charitable medical research foundation might want to access an individual's health records for research purposes. The individual may say "Yes, you can have access to this information for free on the condition that a) it is not passed on to anybody else and b) it remains anonymous – so no personally identifiable details travel with it". If it's a pharmaceutical company doing research however, the individual may set the same terms except charge a sum of money instead of handing it over free. (In practice, over time, many standard agreements will emerge allowing for many different such information sharing negotiations to take place quickly and easily.)

The second type of selective disclosure is an automatic 'subscribe to me' service. Here organisations subscribe to updates from specific fields within the individual's Personal Data Store. To gain access they have to sign the individual's terms and conditions. The individual can choose which organisation he or she wishes to accept or reject as a subscriber. Once the subscription is in place every time the individual changes the relevant field in his data store, the subscribing organisation is alerted to this fact.

Take the simple example of address change. Currently, if we move house, we have to remember all the organisations we have a relationship with, getting in touch with them via the processes they have dictated, wasting hours of time and hassle in call centre queues, putting in passwords and

usernames on web sites, and so on. With a fully populated Personal Data Store the list of current relationship is up-to-date and complete (because the store is used to manage the relationship), and the same updated information is shared with all these suppliers with just one click.

The other side of house moving coin is the organisations we forget to inform. This creates relationship management headaches for both the individual and the organisation, which now has to invest significant amounts of time and money simply trying to make sure its existing database is not out-of-date. With the 'subscribe to me' service, subscribing organisations benefit from getting the right information at the right time, not six months after the event.

These three functions of 'store', 'manage' and 'share' form the heart of the Personal Data Store. But they are just a beginning. Once they're in place, they become a foundation and spring-board for a host of additional, more sophisticated services.

Data collection, data hand-backs and personal profiles: Currently, when we buy something in a shop we are given a paper receipt which we are told to keep as proof of purchase but which most of us promptly throw away or lose. With a Personal Data Store the data can be 'squirted' from the retailer's system to the PDS in the form of a digital receipt. With a PDS, the individual can build a richer and richer transaction history – a profile – of his or her purchases receipt by receipt. In addition, organisations that have collected data about the individual for their own purposes can pass this data back to the individual.

Why should organisations do this? First, because individuals will ask for it (after all, transaction data is as much the individual's as the organisation's). Second, because if the customer can combine data from many different suppliers, the resulting picture of the customer's behaviours and preferences is much richer and much more accurate.

Take a simple example. Currently, Amazon has a detailed record of all the books I buy … from Amazon. But it doesn't know what books I buy from other book sellers. So, at best, it has a partial picture of my book purchases and when it uses this data to generate 'if you bought this you might want to buy that' recommendations, it invariably gets things wrong.

But if Amazon helped me build a picture of all my purchases (by combining its transactions with transactions from other booksellers) then the picture becomes much more accurate. Of course, it's up to the individual whether or not he or she wants to share this profile with Amazon. But if Amazon agrees to the individual's data sharing terms, there may mutual benefits. The customer gets better recommendations, and Amazon gets more sales. In fact, Amazon might even be prepared to pay for the right to access such personally-enriched data.

This gives the lie to the current organisation-centric quest for a 'single view' of the customer which, in reality, is nothing of the sort. It is just a single view of that particular organisation's dealings with the customer. In fact, the only entity capable of building a genuinely comprehensive 'single' view of customer is the customer – using his Personal Data Store.

In fact, as individuals build comprehensive pictures of their activities across aspects of their lives such as 'my money', 'my health', 'my home' and so on, *the data held by individuals in their personal data stores will grow to be richer, more rounded and comprehensive, more accurate and generally more valuable than any individual organisation's customer data.*

This has two implications:

- Looking forward, the critical 'master data' that's essential to the efficient management of customer/company relationships will shift from its current position as 'owned', controlled and managed by the organisation to 'owned', controlled and managed by the individual. The individual will become the primary data manager.
- The more this information accrues, the more it will fuel new 'added value services' that analyse and act upon it on behalf of the individual (see Personal Information Management Services below).

Verifications: One of the problems with the picture as painted so far is that the individual may get things wrong, or may lie. Enter PDS verification services.

Currently, if you want to make a significant purchase such as a car, the seller conducts many credit referencing and other checks 'behind your back' – to make sure that you are capable of paying for it, that you have a good credit history and so on. If you are negotiating with three different sellers at the same time, they each have to organise their own checks – thereby duplicating the process three times over.

With Personal Data Stores, the individual can store this data in his PDS *with the verification attached to it*, so that when he or she sends his details to the car seller it arrives already verified: 'these are my credit scores as defined by Experian, Acxiom, etc'. Any information which requires verification by a third party – driving licence endorsements, passport, educational qualifications, employment history, testimonials, insurances, transaction receipts etc – can be treated in the same way.

In this way, it becomes cheaper and safer rather than more expensive and risky for organisations to use data from the individual's PDS. The PDS helps streamline the process of doing business.

Identity assurance: As part of the same process of interacting and transacting, organisations in both the private and public sector need to be confident that the person they are dealing with is who they say they are. Usually, this assurance is given by an agreed 'gold standard' piece of identification such as a passport, or bank account. Personal Data Stores can help streamline these identity assurance processes by linking verifications to such data.

But Personal Data Stores can take identity assurance much further. With a PDS, the individual can provide a wide range of identifiers in addition to traditional 'gold standard' pieces of identity assurance. For example, as well as the passport/driving licence, individuals could also provide evidence that they have banked with this bank for 15 years, using this address for six years and received home delivery groceries and Amazon shipments at this address for five years and have been a member of the following online communities for three years, and so on. The greater the combination of different such data sources, the harder it is for fraudsters to succeed.

Privacy management: Much of the current debate about privacy is misconceived because it is based on organisation-centric assumptions: about what 'privacy policies' organisations should or should not confer on individuals whose data they collect. Personal Data Stores transform this debate by recognising *privacy as a personal setting*: where the individual is empowered to choose what information he or she wishes to share with what other party, for what purposes, in what context. It recognises the contextual, contingent nature of all privacy concerns.

An innovation agenda

Just this short list of core PDS functions – data storage, management, sharing, verification, identity assurance, privacy management – shows how and why Personal Data Stores are set to become a pivotal, foundational information utility of the 21st century.

Personal Data Stores will become informational equivalents of electricity supply or the plastic payment card for the 20th century consumer: rather boring and rather taken for granted but absolutely essential; simply used naturally and unthinkingly as an automatic aid to everyday living; only really noticed with howls of anguish and frustration when something goes wrong. Utilities like this work because they make life easier for everyone and because they make new things possible. They are 'platform' services. They create a platform for everyone and everything else to walk on. The more taken for granted they are, the more successful they are.

Like electricity supply and payment cards, they also create significant behind-the-scenes technical and eco-system challenges. We pay by plastic cards because it is easy and convenient. But behind each payment there is a hugely sophisticated system of highly secure data 'handshakes' taking place across a complete eco-system of supporting players: credit card issuers, merchant acquirers, retailers etc. Behind-the-scenes complexity and robustness march hand-in-hand with the simplest possible user interface.

Personal Data Stores are no different. To achieve their essential utility status they will need to surmount many challenges including:

- Exemplary data security, both in data storage and data sharing. Individuals have to be confident that the data in the PDS is safe and will not be compromised.
- Absolute ease of use. The biggest selling point of the PDS is convenience. If it fails to deliver easy intuitive help in day-to-day chores it won't succeed.
- Easy population of the data store, with equally easy access and use – to correct, update, link, share etc. (e.g. automatic capture of electronic receipts and other transaction records).
- Easy-to-use and understand data sharing agreements, protocols and processes. For example, 'subscribe to me' services require relatively new technologies such as information cards to bypass clunky first-generation password + cookie user access to organisation's information systems online.
- The development of technical, legal and other standards to support data sharing and data sharing agreements.
- The ability for data fields in Personal Data Stores to talk to data fields in organisations' databases without confusion or error. This requires the development of sophisticated data architectures.
- The ability to easily gather and share bespoke 'bundles' of data from the data store (for example, driving licence, insurance, identity assurance and financial information for the purposes of buying or hiring a car). Depending on the task at hand this might involve working with a range of different types of personal data including:
    - data that identifies me' (e.g. my name, address etc)
    - 'data conferred by other parties' (e.g. my passport number, my credit reference rating)
    - 'information gathered by me' (e.g. search and research results)
    - 'data generated by my dealings with other parties' (e.g. transaction and interaction records)
    - 'information created by me' (my plans, my preferences)

- ‘information about me’ (‘mash ups’ of information created by me, conferred by other parties, and gathered by me about my financial circumstances, my health, my skills and learning, etc)
- The ability to analyse data in the store to identify trends, glean insights etc
- Enabling discovery of information by external parties who can access to specific data in individuals’ personal data stores on a permission only basis (e.g. seeing a purchasing or behaviour profile on either an anonymised or personally identifiable basis).

Person-centric information sharing agreements mark a new stage in both information management and in the relationship between individuals and organisations.

Some of the key attributes of information sharing agreements are:

- They are practically oriented and specific, focusing on a specific problem or information sharing need.
- They release a genuinely new class of information – ‘volunteered personal information’ (VPI) that previously only the individual knew, could see, or had access to.
- They give individuals the confidence to share information they would have previously withheld – because now they know appropriate safeguards are in place.
- They are – *have* to be – user-friendly, based on a small number of standards, well explained and understood agreements covering the main information-sharing scenarios individuals are likely to encounter.
- They are machine readable, so their generation and consumption can be automated, including their comparison to a baseline set that are pre-approved by the individual – thereby helping the individual determine differences, extensions, etc.
- They operate above the level of all global privacy regulations, offering individuals and organisations a release from country-to-country regulation differences, arbitrage, etc.
- The deployment of these agreements within a broader trust framework (which explains standards, inter-operability, how liability is handled etc) will create a secure, efficient and workable foundation for rich, mass scale information sharing between individuals and organisation. This is the information needed to fuel the rise of personal information management services.

4. A New Personal Information Management Ecosystem

Personal Data Stores' first use will be as an information utility helping individuals manage daily informational chores, including their dealings with suppliers, public services etc. But as a platform, they also provide a secure foundation for a host of new types of service. Let's take just two examples.

Reinventing marketing: Current marketing communication systems work by guesswork. Sellers don't know who is interested in what service at what time, so they have to make either an educated guess or simply spam people with messages on the off-chance that a certain percentage of these messages will be picked up. These processes are wasteful to sellers and irritating and/or intrusive to buyers.

Personal Data Stores will help buyers express and communicate their preferences and specifications to the marketplace, thereby helping sellers communicate with the right people about the right things at the right time. This will turn a currently wasteful and often adversarial process into an efficient, win-win 'handshake' instead.

Added value services: Once the core data functionality is in place countless new data-informed services become possible. Imagine a new person-centric car buying service for example. It starts off with specification-building. This spec-building service combines a number of different types of data including: my plans and preferences (what I intend to use the vehicle for, what my likes and dislikes are including brand, features, trimmings etc); my budget (including whether I can pay for it, my credit scores etc); my previous car usage (mileage, trade-in value, length of ownership, service history etc).

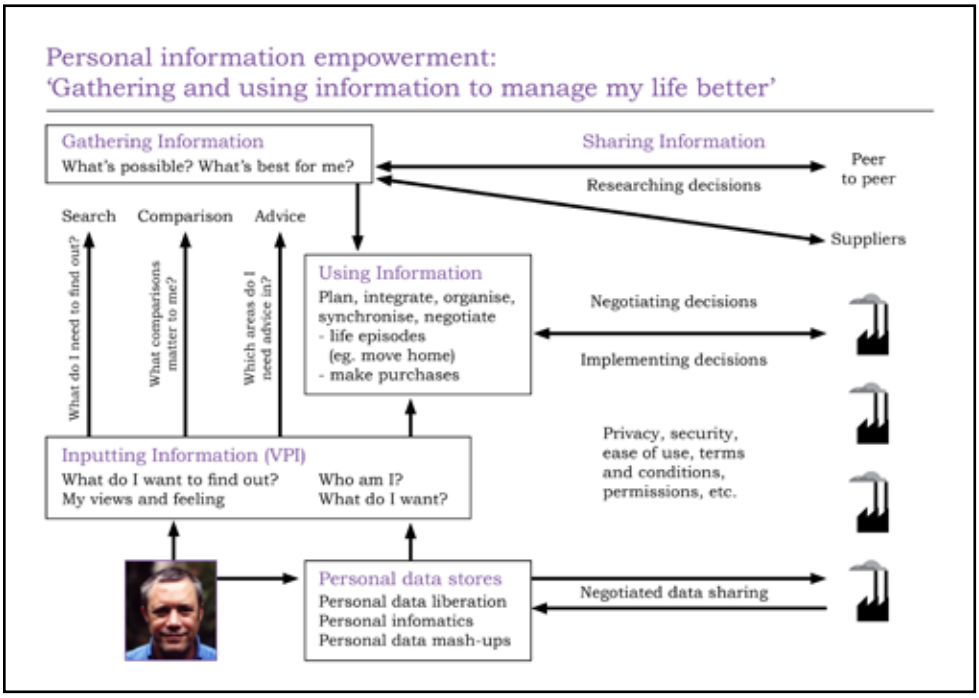
With data such as this, the service helps the buyer build an 'ideal' specification including potential trade-offs and compromises. The service then takes the spec to market (probably anonymously but with supporting verifications to reassure sellers that this is a real buyer with good money to spend). Sellers provide offers matched to the specification, which the buyer then considers. The buyer then either tweaks the spec for a second round or makes a purchase decision, at which point he or she can use the PDS to share the data needed to complete the buying process.

Over the years, individuals have to manage countless different 'life events' and episodes, such as moving home, buying a car, organising a holiday, getting married, getting divorced, having a child, changing schools, etc. They also have to manage a whole series of ongoing life management processes such as 'my money', 'my health', 'my communications infrastructure', 'my home', and so on. Each one involves intensive bursts of finding, sifting, sorting and providing a wide range of different types of information.

With Personal Data Stores as a foundation, countless specialist Personal Information Management Services will be able to enrich, streamline and enhance these processes both for the individuals they are working for, and these individuals' suppliers: we are talking about the evolution of a new and different commercial and public service eco-system driven by enriched, permission-based exchanges of personal data.

What will these new personal information ecosystem look like? Figure 3 draws an outline map.

Figure 3:
The emerging personal information management ecosystem – focused on helping individuals manage data better



At the top of the figure lies the infrastructure that was developed largely in the first decade of the 21st century: specialist services offering online search, comparisons, peer-to-peer information sharing such as product reviews and word of mouth recommendations, plus broader social media/ networking services.

At the bottom of the map lies the new foundation-stone around which the ecosystem will crystallise: the Personal Data Store. It does all the things we have talked about in this White Paper including information sharing with suppliers and potential suppliers. More generally it opens up a new data source: Volunteered Personal Information.

Before VPI there were only really two types of customer data used in commerce: 'market research' which was statistical and anonymised, and transaction/interaction data which was granular and personally identifiable (but which was also a partial snapshot, not in context and quick to go out-of-date).

VPI represents a third and potentially bigger and more valuable form of personal/customer data – encompassing:

- 'who I am' (my identity data, my circumstances and lifestyle)
- 'what I want' (things I want to do or buy, plans, projects)
- 'what I want to find out' (questions I want answered, advice I need)
- 'my views and feelings' based on my experiences, which inform my own decisions and can be shared with other people.

Using VPI and Personal Data Stores, a wide range of specialist Added Value Services help individuals gather, use and share the information they need to manage aspects of their life better (from 'my lost wallet' though 'buy a new car' to 'manage my personal finances'). These Added Value Services (see the middle of Figure 2) link in with the top layer of search, comparison, advice and social networking – so that they become increasingly driven by information generated by Personal Data Stores, and in turn, become a source of new information for PDS.

Meanwhile, these Added Value Services interact with organisations (both public and private sector) for and on behalf of the individual, helping to match both sides requirements, reduce transaction costs, and enrich outcomes – using rich, accurate information from individuals Personal Data Stores to make sure the right services/information get delivered to the right individuals in the right ways at the right times.

This new eco-system is both disruptive and highly productive. It's disruptive because it changes many established ways in which individuals and organisations interact. It will force a rethink of many marketing, advertising, retailing, CRM and customer service/service delivery processes.

At the same time, it creates the conditions for an explosion of innovation and new services delivering the 'double whammy' of reduced costs (for both sides, including time/hassle costs as well as money costs) plus new dimensions and forms of value – helping both individuals and suppliers get more value from their markets.

5. What's in it for individuals?

Personal Data Stores bring to individuals the information management benefits that organisations have enjoyed for years. These include the ability to:

- gather and analyse data to gain and act on new understandings and insights
- streamline and automate processes to save time and money
- organise and synchronise activities to move faster and become more coordinated and responsive

Personal Data Stores will transfer these benefits to individuals in the form of:

Convenience: saved time, reduced stress and hassle in daily 'life management' projects, tasks and chores.

New benefits and forms of value: The information generated by personal data stores make it much easier and cheaper for organisations to deliver more relevant, personalised and even customised services to their customers: exactly the right value at the right time and the right place. At the same time, because the information volunteered by individuals via Personal Data Stores is potentially so valuable, many organisations will be prepared to pay (in cash or in kind) for access to this data. Personal Data Stores could become a small but welcome income stream for individuals.

Insight: Personal Data Stores will help individuals gather and analyse personal data to reveal and crystallise important insights about their own lives. Organisations have already been through this process of discovery: using data to discover things about their own activities and 'habits' that they weren't aware of before. This agenda - of using personal data to generate new insights about their own lives leading to better decisions - is a potentially significant growth industry in its own right.

The emotional benefits of empowerment: There is now extensive evidence from psychological research that feeling 'not in control' generates feelings of vulnerability, anxiety and depression. On the other hand, feeling 'in control' – empowered – makes people feel more confident and positive. New research is beginning to indicate that these general observations apply just as much to personal data as any other aspect of individuals' lives.

Recent consumer research in the US and China, for example, finds consumers citing four emotional benefits of information empowerment: a feeling of being in control, a sense of being smarter, help in 'beating the system', and positive 'challenges to my beliefs'. There are some psychological costs too – feeling overwhelmed, uninformed, confused or frustrated – but the benefits far outweigh the costs.[i]

Intriguing research from the BCS (the Chartered Institute of IT in the UK) suggests these psychological benefits are biggest amongst those who currently feel most disempowered. The research finds that access to and use of IT increases individuals' sense of freedom and control, which has a positive impact on well-being and happiness – and that these benefits are most marked among women especially on lower incomes or with fewer educational qualifications.[ii] This is a new area which is crying out for more research.

6. What's in it for organisations?

Our current *organisation-centric* approach to the management of personal information has brought significant benefits to organisations including access to new insights leading to better innovation, the ability to use customer information to improve customer service and to target more relevant communications. However, it is also has many intrinsic flaws and over time diminishing returns have set in.

The central flaw is that organisation-centric approaches can never ensure that the data in question is accurate, complete or up-to-date.

Data accuracy and quality: Most of the personal information collected by organisations takes the form of a snapshot that gets frozen into the organisation's database when it is captured … while the individual's life moves on. Because there is no automatic process for data synchronisation, no sooner has the organisation captured the data than its accuracy starts decaying.

This generates *endemic* waste on two fronts:

- organisations have to invest significant amounts of time and money simply trying to keep their data correct, up-to-date and accurate.
- they end up making decisions and taking actions on basis of out-of-date, inaccurate data thereby investing time, money and energy doing the wrong things at the wrong times – often unwittingly putting customers' backs up in the process.

Data completeness: By definition, the data organisations collect about individuals is partial and incomplete. For example, many organisations are currently struggling to create 'a single view' of the customer. As we saw with the Amazon example, the current interpretation of the phrase 'single customer view' is restricted to *the organisation's* view of that customer's dealings with *that particular organisation*. This rarely creates an accurate picture of what the customer is doing within the marketplace as a whole. Inthis way, inaccuracy, and therefore waste, *built into the way the system operates*.

Data richness: Today, an avalanche of new digital data is becoming available as new digital processes capture data that previously 'evaporated' as soon as it was generated. Examples include the barcode scanning and loyalty card data that was previously lost at the store check-out. Data-rich digital payment mechanisms which capture information about who spent what, when and where, are progressively replacing the previously data-free, anonymous payment mechanism of cash.

Online search is generating a moving picture of what we want to buy and what we are interested in. Geo-location-data is transforming mobile telephony and services. Web analytics are transforming our understanding and design of Internet services. Smart meters are set to transform energy markets. And so on.

Organisations are racing to capture or scrape this cornucopia of new digital information. Yet in doing so they are hitting two insurmountable problems. First, this new digital data 'landgrab' is undermining trust. Second, the commercial value of the data is being exaggerated. Virtually all of this data sits in just one dimension – of transaction and interaction data. It simply fails to touch other aspects of individuals' lives including:

- Their future plans and intentions (that remain largely inside individuals' heads)
- The context in which the data-generating actions are taking place
- What the individual's reasons, purposes, goals or preferences are

The net effect is that even as organisations struggle with information overload – unable to cope with all the new information that's becoming available – they find themselves hamstrung by lack of information about 'what really matters'.

Data costs: The siloed nature of organisation-centric data capture and use creates *wasteful duplication* for both organisations and customers.

In the UK, the average customer/citizen has around 200 relationships with different types of organisation across every aspect of his or her life (money, health, home, work, transport and travel, communications, holidays, hobbies etc). Each one of these organisations has its own processes and mechanisms to keep customer records up to date, check that names, addresses, billing and other details are correct, and so on. But often each organisation is checking and handling exactly the same piece of information. The result is wasteful duplication on a vast scale as the same bits of information are collected, checked and processed, in parallel, by different organisations. In this way, society's costs of managing personal information are being multiplied many times over.

To illustrate just how high these duplication costs are becoming, consider this simple model:

- *Basic data management tasks: average $5 per customer per organisation, across*
- *Multiplied by 200 (for each individual/organisation relationship) = $1000.*
- *Multiplied by 41 million (UK adult population)*
  = £41,000,000,000 or £41bn.

This is just an annual cost. If we assume that the average customer spends three years with each organisation (for many organisations it's longer than that), then the total cost to organisations of handling their customers' data over the course of the relationship is closer to $210bn. For the US, with a population of 305 million, the total cost is just short of $1 trillion ($915bn).

These costs have remained largely invisible and uncounted because every organisation is interested only in its own costs of data management: it is not aware of, or interested in, other organisations' duplicated costs.

They are also a dramatic underestimate of the total cost to society. They ignore all the costs (especially time costs) that millions of individuals incur duplicating the same processes in their own lives as they manage their relationships with these different organisations. For example, if they move home, they have to tell each supplier separately, having to repeat the process of informing suppliers of the new situation 200 times over.

With Personal Data Stores, much of this duplication would be eliminated … with huge benefits for organisations, individuals and society as a whole).

To underline the scale of the waste produced by our current practices, consider how much time and money is spent by organisations developing their own bespoke privacy policies, terms and conditions and so on. This is a job creation scheme for expensive lawyers yet ironically lawyers whose input is close to worthless. For example, recently a judge in a US Court of Law dismissed Blockbuster's online terms and conditions as 'illusory' and 'unenforceable' because Blockbuster reserved itself the right to unilaterally changes these terms any time it liked[iii]. It's not at all clear that companies could enforce the terms of these contracts in a court of law.

The Personal Data Store approach of creating common, standard agreements between individuals and organisations would eliminate high proportions of these costs (not all, but a high proportion) while also building trust between the two sides.

Figure 4:
Costs of handling personal data: UK example

Costs of handling personal data: UK example

Cost to handle one customer's data per annum	$5
Cost for 200 different organisations to each handle this one customer's data	$1,000
These costs duplicated for individual (say, 70 million)	$70,000,000,000
Costs of handling customer data over average customer life time of three years	$210,000,000,000

Customer trust: Under our current organisation-centric approach to the management of personal data, personal data is seen as a corporate asset, the purpose of which is to enrich the corporation concerned. Profiting from personal data takes many forms: selling lists of names and addresses to direct marketers; credit referencing bureaux and agencies collecting and reselling personal data; organisations such as Google and Facebook making money (or trying to make money) by selling user 'eyeballs' to advertisers.

This corporate 'value extraction' mentality undermines trust, as individuals feel their own data is being taken and used by other parties for these parties' purposes, with no benefit (and sometimes positive harm) to the individual concerned. This is an intractable issue under our current system because it relates to underlying purposes: whose purpose is being served – the organisation collecting the data or the individual whose data it is?

Government and public sector approaches to personal data collection and management are also undermining trust. Governments are keen to offer citizens 'joined up public services'. These would draw on data about individuals to be collected from many different sourcesand then combined (often without the individual's knowledge or permission). At the same time, Governments are collecting personal data for a very different purpose: national security. Governments' failure to keep these two purposes separate is a source of growing public concern: when the two purposes of public service and national security collide national security always prevails. This means Government's attempts to gather more data on their citizens inevitably trigger concerns about civil liberties.

For many years the scale of this problem has been masked by customer/citizen ignorance. Because individuals were not aware of how their data was being treated, there wasn't a problem. The more informed individuals become, the angrier they get (this is confirmed by Mydex's own research). For both the private and public sectors there is a 'time bomb' factor here: the real effects of today's practices cannot be judged solely in terms of today's reactions to them. The possibility/likelihood of a future backlash also needs to be taken into account.

On this score, examples of Government organisations losing customer data, or of organisations such as Facebook introducing and then withdrawing privacy eroding data policies, are helping inform individuals about the issues at stake… and fuelling the backlash.

Intrusiveness and threats to privacy: Under the current status quo, organisations struggling with their pitfalls of data inaccuracy, data incompleteness and data poverty have only one option: to fill the holes in their data by trying to acquire even more data. The more they do this,

however, the more intrusive and invasive their data gathering activities becomes. They are damned if they do and damned if they don't.

If they don't try to fill their data holes they have to accept the wastes of guesswork, error and inaccuracy. If they do try to fill their data holes, they further undermine trust. In fact, many organisations wishing to use personal information to build closer relationships with their customers have unintentionally ended up undermining these relationships, driving their customers away. For example, over 50% of customers of many large UK organisations such as banks and utilities have opted out of receiving online communications from them. What should be a rich source of new win-wins (access to ever more detailed information) is turning adversarial instead.

Compliance risk: The less trusted organisations are with personal data, the more Governments try to solve the burden by adding new layers of regulation. The more regulation there is the greater the costs of compliance, and the risks of non-compliance.

In the world of personal data, compliance costs and risks are now a massive burden in their own right. Yet they are also a classic example of shutting the stable door after the horse has bolted. Both compliance costs and risks would be significantly reduced if trusted processes were built into the data sharing and storage process right from the very start. This is what Personal Data Stores do.

Lost opportunities: The biggest design flaw of all however is the one that's hardest to measure. It's the cost of lost opportunities – our inability to do things that we *should* be doing but aren't, because we have mistrust where there should be trust and privacy concerns where we should have rich information sharing.

These lost opportunities are not small. They are huge. In a modern economy, every individual should be an active creator and generator of information positively contributing to the development and delivery of goods and services, to efficient markets, and to the process of wealth creation. By treating individuals as passive 'subjects' of data gathering and 'targets' of communication, our current system turns this tap off – replaces it with a low trust, high cost system instead. In other words, it has become a break on both social progress and economic growth.

Personal Data Stores help address all of these problems:

- Data accuracy and quality: By subscribing to individuals' personal data stores, organisations will be able to receive real time updates of changes to individuals' details, such as address and contact details, at low cost.
- Data completeness: Personal data stores create a complete single view of the individual's activities in a particular area (e.g. '*all* my book purchases'). Over time, the data held in individuals' personal data stores will grow to be far more comprehensive than any of the data any individual organisation can collect.
- Data richness: Personal data stores don't only collect transaction and behavioural data – they form a much richer picture of the individual's life. This picture can be shared with organisations willing to accept individuals' terms and conditions for data sharing.
- Data costs: Personal data stores eliminate much of the wasteful duplication endemic to today's organisation-centric approach to data collection.
- Trust: Because personal data is shared on a selective disclosure basis, with the individual being able to choose what information to share with which organisation for what purposes, trust is built into the way the data sharing system works. Organisations are incentivised to act in trustworthy ways a) because they are now legally committed to doing so and b) because individuals now have the power to revoke information agreements, thereby threatening organisations with loss of access to an increasingly vital resource. The other side of the coin: more trust there is, the more willing individuals will become to share information, while remaining confident that their privacy is not being invaded.
- Compliance risk: Because increasing proportions of personal data are actually held by individuals and not companies, and is shared with individuals' explicit permission, compliance risk is reduced.
- Lost opportunities: As we've seen (see 4. A new Personal Information Management Ecosystem) Personal Data Stores make a completely new type of personal service – a new growth industry – possible.

In short, when individuals are empowered with their own personal data stores a new data sharing 'contract' between individuals and organisations can be established. Using this contract as a foundation, it is possible to:

- Restore trust for both sides
- Reduce costs for both sides
- Improve data accuracy, richness and quality for organisations, thereby leading to:
    - Less waste
    - Better data-based services
- Help make individuals' lives both easier and richer
- Spark innovation and economic growth via the development of new value-adding services

Personal data stores don't only offer a 'win' for individuals; they also offer a 'win' to organisations and society too.

7. What's in it for the economy?

Personal Data Stores could have a significant role to play in encouraging sustainable economic growth by:

- Reducing costs of existing economic activities
- Igniting a new wave of product and service innovation

Exactly why and how may need a little explanation.

The 20th century approach to wealth creation (via mass production, distribution and communication) created extraordinary amounts of new material wealth which we enjoy to this day. However, it has also done immense damage to natural ecosystems (e.g. well-known issues of resource depletion, pollution and climate change), and *much of this damage could be avoided if its modus operandi wasn't so wasteful*.

In particular, industrial age approaches to wealth creation generate three levels of waste.

1. The constraints of 'averaging': Industrial age production processes are driven by a quest for economies of scale that reduce unit costs. Economies of scale rely in turn on standardisation – 'averaging'. Without standardisation, organisations get sucked into endless variations which multiply costs and complexity. But averaging breeds its own forms of waste. The average of the numbers 1, 2 and 3 is '2' (1 + 2+ 3 = 6 divided by 3). In a world where real demand takes the form of demand for '1' and '2' and '3' averaged production delivers only '2'. This is cheaper and more 'efficient' but it over-serves demand by 1 in the case of '1', and under-serves demand by 1 in the case of '3'. Overall, it creates a wealth-dissipating misalignment of '2' out of 6.

2. The costs of push: To achieve economies of scale organisations have to invest vast sums up-front in productive capacity. They also have to produce in batches to achieve optimal economic order quantities. With these approaches to production, they are not organising production (or distribution, or communication) to fit the requirements of the market. Instead, they end up trying to organise the market to fit the requirements of their own internally generated quest for production 'efficiencies'. Once they have produced their batch, they simply have to sell it, otherwise they go out of business – so they end up pushing their products at consumers. This creates new layers of wastes – the costs of producing, storing and distributing stuff consumers don't really want to buy; the costs of pushing, promoting and advertising them, and so on.

3. The wastes of guesswork: 20th century communication technologies only allowed information to flow one way – 'top down' from organisations to individuals. Because there was no practical, scalable way for individuals to talk to organisations – to say 'this is me and this is what I

want' – organisations never really knew what demand looked like: who wanted how much of what, when and where. As a result, many decisions – including decisions about what to make, how much to make, where to distribute to, who to communicate with, how, when and where – were made using guesswork. This guesswork may have been informed by research, but it was nevertheless guesswork.

This guesswork was invariably wrong leading organisations to generate huge amounts of waste. For example, the direct marketing industry boasts about the accountability and measurability of its processes, and the fact that it targets individuals with relevant marketing messages. Except it doesn't. It makes guesses about who might be interested in what and uses data *to reduce the degrees of error inbuilt into these guesses* (propensity modelling). Result: marketing campaigns with response rates of around 2% or less – which means 98% waste.

Personal Data Stores are an essential piece of infrastructure for an entirely different information ecosystem where 'bottom up' flows of information from individuals to organisations mean that *organisations can address all three major causes of waste*.

The more organisations know who wants what when – information made possible by Personal Data Stores – the more they can progressively:

- reduce the costs of averaging in production, distribution and communication (really, three separate challenges rolled into one).
- reduce the costs of 'push' in production, distribution and communication (again, three separate challenges rolled into one).
- reduce the wastes of guesswork in production, distribution and communication (again, three separate challenges rolled into one).

This is a massive opportunity to reorient our entire economy around the needs of 'demand' rather than the dictates of 'supply'. It's much more than an opportunity to cut costs. It's an opportunity to turn *yesterday's waste into new wealth* – to divert resources that were previously waste into new wealth creating activities.

This is the second layer of the PDS's economic potential. As PDS's gain critical mass we expect an explosion of innovation – of new products, services and businesses – that a) help individuals use their data better (e.g. specialist personal data analytic, monitoring and decision-support services) and b) use this data as a key input into new types of personalised service. Because of the nature of the data, this opportunity is all-encompassing, spanning every industry and service sector including 'my home', 'my money', 'my health', etc.

In this sense, information generated by the Personal Data Store is like the energy generated by our electricity generation and distribution system – helping to drive all aspects of economic and personal life, while making countless new products and services possible.

In this way, *the net economic effect of personal information empowerment could be a new era of economic expansion – a new 'value explosion'* – as resources previously wasted on averaging, push and guesswork are progressively reinvested in innovative new 'person-centric' services.

8. What's in it for society?

Research by Mydex into individuals' attitudes towards how organisations gather and use personal data reveals high degrees of 'learned helplessness'. Cynicism, apathy, and mistrust prevail – along with sometimes shocking levels of ignorance. This is not a good foundation for the development of healthy, fair or democratic society. It is a cause of division and inequality. It is a source of frustration and conflict. It blocks progress.

Today's extreme imbalance of information management power is creating a 'race to the bottom' as organisations find it easier to take advantage of individuals' ignorance or apathy than to invest in providing a better service or a more informed customer base. Personal Data Stores are not a panacea. But they do provide one of the means by which urgent and pressing social dimensions of information policy can be tackled.

In particular they can help:

- redress imbalances of power that effectively exclude individuals from effective, active participation in economic and civic life (except as industrial age 'consumers' and 'employees')
- as a highly positive policy tool to tackle 'the digital divide'
- both public and private sectors to radically reduce economic waste and environmental damage (see Section 7)
- turn today's personal data 'race to the bottom' into a 'race to the top' as more active, informed and confident customers and citizens incentivise organisations to focus on improved service delivery and mutually beneficial information-sharing driven engagement
- create a more active confident citizenry thereby underpinning a healthy democracy
- turn a low-trust economic and social environment into a more creative, innovative high trust environment
- create an improved climate of trust in relationships between organisations, including public sector organisations and Governments, and citizens. This is important for democracy, stability and economic growth
- trigger a new spate of economic growth around the new industry of Personal Information Management Services

At a more fundamental level, Personal Data Stores are placing a new, peculiarly modern battle for human rights on the social agenda: the battle for *digital* human rights.

9. Why now? Technology developments

Short answer: because the technology stars are aligned. Personal Data Stores and personal information empowerment in general were simply impossible ten years ago, when the Internet had not reached critical mass, when Google was just a tiny start up, when social media had never even been heard of. In just ten years, a huge amount of water has passed under the bridge.

The trend towards Personal Data Stores is now evident in countless ways already, most of them only suggestive of the future or displaying some flaws or failings. For example, it's now commonplace for e-commerce companies to provide customers access to 'My Account' facilities where they can update records, manage communication preferences, access transaction histories etc. Such facilities involve individuals as managers of their own information, but in an organisation-centric way – on the organisation's systems, in ways that require individuals to spend time and hassle logging into and jumping through the security and identity hoops of each different organisation. The next step is for such My Account information from all my suppliers to be held on an individuals own Personal Data Store so that I can manage them all together, from one place, in a time-efficient, safe, integrated way.

Another straw in the wild is the profiles individuals upload to services like Facebook. Here, they are creating a database about themselves, and selectively disclosing what information they want others to see. From the PDS perspective, the drawbacks of the Facebook approach are obvious: the data is held by Facebook, not the individual, and Facebook determines (and keeps changing) 'the privacy policy'. But it underlines the value of the data and educates the public into the concept of personal data management and sharing (including the pitfalls!)

Meanwhile in specialist industry sectors proto-personal data stores are being developed by many companies. Microsoft's Healthvault, for example, looks forward to a day when individuals manage their own personal health records.

This pace of change is accelerating and rapidly gaining critical mass.

Cloud Computing refers to when data and applications that are normally stored and operated either on personal computers or corporate servers are instead stored and operated on third party servers "in the cloud", i.e., accessible from any location or device over the Internet. This has many benefits in terms of cost savings, reduced complexity, simplified administration, and sharing of data across domains and applications. It is also a necessary step towards making information services less 'device-centric' and more 'person-centric'. Business Week predicts, for example, that cloud computing will trigger a proliferation of 'personal virtual assistant services', which are perfect vehicles for the generation of rich, structured volunteered information.[iv]

OpenID turns our current organization-centric approach to identity on its head. Currently, every organization assigns its own identifier to every individual it deals with, which means that individuals dealing with many different organizations have to remember to use the multiple different identifiers allocated to them. With OpenID, individuals have one, single identifier that they can 'carry' around with them wherever they go online so, for example, they no longer have to bother with multiple usernames and passwords. This is much more than a compelling consumer proposition. It makes the individual, not the organisation, the 'pivot point' of data sharing.

Information Cards (I-Cards) build on these technologies to make information sharing even easier. I-Cards are the digital equivalent of the cards you hold in your wallet: they contain information (from yourself, or from other websites) that you can use to prove your identity or share information about you. Instead of sitting in your wallet, however, I-Cards sit in a digital wallet which is accessible from all your devices. If a website accepts I-Cards for login, you just click their I-Card icon and then select the I-Card you want to use. One click and you are logged in: no typing usernames or passwords at all! Cards are always transmitted with strong encryption and disclose only the personal information needed for any particular transaction, so they protect both security and privacy. As the non-profit Information Card Foundation (ICF) explains, I-Cards "make routine Internet transactions—logins, form-filling, purchases, reference checking—as easy as swiping a credit card".[v] There is no pre-defined limit to the amount of information that can be shared in this way.

Relationship Cards: I-Cards can also be combined with XDI data sharing to create what are known as Relationship Cards (R-Cards). An R-Card is an I-Card that is shared in order to create an ongoing data sharing relationship. For example, you could use an R-Card to share your mailing address with a magazine site so that it was always delivered to your home no matter where you live. When you move house, you only need to update your mailing address once, and your R-Card will automatically send the updated address to each subscriber you have approved.

The Open Identity Exchange (OIX)[vi] is about trust at Internet scale. Open identity technologies like OpenID and Information Cards reduce the friction of using the Web, much like credit cards reduce the friction of paying for goods and services. However, they also introduce a new problem: who do you trust? How does a relying party know it can trust credentials from an identity service provider without knowing if that provider's security, privacy, and operational policies are strong enough to protect the relying party's interests? OIX is working on this, not just as a technology problem but also as a business, legal, and social problem.

XRI (often known as i-names) is a new type of Internet identifier that enables both people and machines to 'tag' pieces of information so that it can be located, described, and understood in a way that works across different domains and applications. For example, with a URL, the most common form of Web address today, you can only tell (at most) that it represents a file of a certain type (a Web page, a Word document, spreadsheet, a PDF file, an image, etc.) But with an XRI, you can determine if the address represents a person, a company, a concept, etc. If the XRI represents a file such as an Excel spreadsheet, it can tell you, for example, that it is the third version of a budget produced by a company's Human Resources department.

XDI is a new data sharing protocol based on XRIs that makes it possible to securely share, link and synchronise data between any two devices or applications anywhere on the Internet. A key feature of XDI is 'link contracts' that enable control over the authority, security, privacy and rights of shared data to be expressed in a standard machine-readable format. In the context of VPI, this means that we now have scalable, worldwide infrastructure for individuals to share their personal information on terms and conditions to which they agree, and these terms and conditions will always travel 'with' the data in a secure, auditable way.[vii]

Drawing on these developments, other bodies have emerged to advance work in particular areas. The Higgins Project for example, is using these technologies to develop 'Active Clients' that work on a person's computer browser or mobile device to provide a kind of dashboard for personal information and a place to manage "permissioning" - deciding who gets access to what slice of the user's data.[viii] The Kantara Initiative is developing standards for interoperability of data and services to ensure secure, identity-based, online interactions while preventing misuse of personal information. The goal: to make networks privacy protecting trustworthy environments. Kantara is also hosting the Information Sharing Work Group, which is working to develop a standard information sharing agreement that words as a tool – i.e. easy to understand and use – in the hands of the individual.[ix]

Separately and together, these new technologies and services are doing four things:

- They are making it much *easier* for individuals to share information.
- They are giving individuals greater *control* over what information they share – thereby increasing their trust and confidence in the process
- They are making it easy, and safe, to share large quantities of *structured* information, which can feed directly into organizations' systems thereby transforming the economics of information sharing.
- They are making these processes secure and auditable.

Looking forward, all known technology trends reinforce the potential – if not the actuality – of increased personal information empowerment. There are no current trends undermining or sapping its momentum.

10. Mydex's role

Mydex is just one of many services now pioneering the personal data store concept within this emerging ecosystem. Over time, separately and together, these services will become an industry sector in its own right: the subset of Personal Information Management Services (PIMS) helping individuals store and manage their personal data. Competition for users will be intense. Some of the key elements of Mydex are:

- Its use of state-of-the-art web-based technologies to enable highly efficient, secure, data storage and information-sharing
- Mydex services are being designed with the needs of the entire personal information management eco-system in mind:
    - mass-scale, efficient sharing of structured data
    - technology standards to underpin this data sharing
    - trust and compliance standards to oil the wheels of this data sharing
- Flexibility: the concept works equally well for a personal data store of one data field or 4000 data fields; it allows for one-off bespoke information sharing and mass-scale automated data sharing via 'subscribe to me' services (see above)
- Its design ethos: of placing the individual at the heart of the process as the point of information and service integration, and as the point of information origination.

Legal status: To reinforce its role as a service to the individual working for, and on behalf of, the individual, Mydex has been constituted as a Community Interest Company under UK Law. This means that:

- Mydex is legally required to pursue its *social purpose* of helping individuals realise the value of their personal data.
- Most profits made by the company have to be reinvested in pursuing this social purpose.
- The company's core assets are also legally 'asset locked' which means they can never be acquired by another entity not similarly asset-locked.

Individuals using the Mydex service can therefore remain confident that it is 'on their side' and 'working on their behalf' not only in spirit but also via the letter of law.

11. Summary

In this White Paper we have made four central arguments:

1. A new ecosystem of personal information management services (PIMS) is emerging. Its core function and purpose is to help individuals use modern information technologies to organise and manage their own lives better.

2. Personal Data Stores lie at the heart of this new ecosystem. Using PDS, individuals will gather, store and use huge amounts of rich, new, accurate, real-time information about who they are, how they live their lives, what they want, and so on.

3. By sharing this information with organisations individuals will become active partners in society's information management challenge: using their PDS individuals can and will help overcome the design flaws in the current personal data status quo.

4. Separately and together PIMS can a) rebuild trust in the collecting, sharing and using of personal data, b) help reduce costs and inefficiencies in our current economic system and c) inspire rich and ongoing innovation that ignites economic growth, both through the development of their own services and the new value offerings they make possible.

12. Next steps

For these opportunities to be realised, lots of things have to happen.

First, we need to test, develop and prove Personal Data Store technologies, infrastructure, information sharing processes and mechanisms, business models to scale, on a global, real time basis. The time has come to experiment and innovate – to prepare for a new and different future.

As part of this, organisations need to design and introduce new information contracts with customers/citizens. Key elements of the new information contracts is a recognition that any personal data used by the organisation is the person's; that the person is the lead manager of his or her own personal data, and that the organisation's job is to use this data, with permission, to add value – for both sides.

To support this, Governments and regulators need to create a new policy environment supported if necessary by new regulations, that supports personal information empowerment and which encourages standards and protocols for trusted information sharing.

Individuals, for their part, need to avoid personal data defeatism (the feeling that 'the battle for control over my own data is already lost' – it's not), to realise the value of their own data and to use this data responsibly, for best effect.

One area government IT has made progress is with public data, with the "power of information" policy and the data.gov.uk portal, which recognises the value of 'unlocking' data held by the Government for reuse by added value service providers.

Next we need a comparably radical rethink on personal data. This starts with a return to the role of personal identifiers and intermediaries set out by UK officials a decade ago, and as recently adopted by the Obama Administration. This means:

- assume that access to on-line public services will be through a market or ecosystem of accredited third-party identifiers (issued for example by a range of existing online services, credit bureaux, or banks).
- drop the false notion that it's generally essential to know who people are.
- challenge the assumption that personal data is "owned" by service-providing departments to be shared at their convenience.
- instead, recognise that the individual is not only the rightful owner, but also the only technically feasible point of integration of exponentially growing volumes of personal data, and therefore the only possible place where "personalisation" can happen.
- recognise furthermore that structured, scalable personal data managed by individuals is set to become the source of immense new economic value, and that the individual is a rightful beneficiary.

This change in mindset includes a specific challenge to secret parts of government entrusted with keeping Britain safe. A safe society isn't the outcome of dysfunctional public services designed to aid surveillance. Britain has a far better chance of being secure with public services designed to work for individuals and front-line public servants, which respect human rights and dignity. When the data are cleaner, the relatively small number of exceptions stand out more clearly.

On-line identifiers need to work under the user's control, with minimal disclosure and revealing information only to justified parties. They need to be consistent and convenient (see Kim Cameron's "Laws of Identity").

In the short term the UK can copy the US administration: announce that future access to online services will be via third-party identifiers, and then provide for the emergence of a "trust framework" so a range of identifiers are accredited for suitable purposes. Many services can be accessed anonymously, and for many more all that is needed is a consistent user experience. It's not always necessary to identify people to check their entitlement. But sometimes individuals will need to invoke stronger

identification credentials online: for “Know Your Customer” processes or to meet the most stringent visa requirements for example.

- Government IT therefore needs to anticipate a world where individuals are equipped with
- highly evolved personal data stores
- the ability online to invoke strong authentication or verification (e.g. proof of qualifications, licences, credit, nationality or identity)
- selective disclosure, i.e. the ability to share the minimum necessary in a particular circumstance.

This doesn’t require major new procurement. It means:

- review each main service function to take into account the role of user-driven records for health, education, welfare, transport, or other areas such as the Census or the London Olympics
- quickly participate in at least two live prototypes of user-driven services across multiple organisations supported by independent online verification services
- where there is benefit, re-engineer the public services (health, education etc) users can drive new services.

Just as the existing “Power of Information” has created new APIs to allow structured public data out of government systems to create new value, so this “empowered citizen/customers” agenda will see new APIs that allow structured personal data in. This means public services can be driven and personalised by users, and new service packages created for them by third parties.

This “empowered citizen/customers” agenda might even reveal a revised role for the National ID Register as a voluntary service offering online verification as part of a trust framework, for the most demanding cases.

Bibliography

Cluetrain Manifesto, Rick Levine, Christopher Locke, Doc Searls, David Weinberger, Craig Newmark and Jake McKee. Basic Books; 10th Anniversary edition (2 July 2009)

Right Side Up, Alan Mitchell, Harper Business, 2001

The Data Deluge: The Economist, 25 February 2010

Liam Maxwell, 'It's ours — why we, not government, must own our data', Center for Policy Studies, Jun 2009.

Private Lives: A Peoples Enquiry into Personal Information, by Peter Bradwell, Demos 2010

Mydex: Research into users attitudes towards personal information sharing, 2010

ACMA (2009). Attitudes towards use of personal information online: Qualitative Research Report, ACMA.

Iain Henderson (2009). The Personal Data Eco-System, Kantara Initiative. Kantara

Initiative. (2009). "Information Sharing Workgroup." from http://kantarainitiative.org/confluence/display/infosharing/Home

Henderson Iain (2009). The Personal Data Eco-System, Kantara Initiative. Joshua Gomez, Travis Pinnick, et al. (2009). "Know Privacy."

Hazel, L. (2006). Trustguide: Final Report, October 2006. London, BT Group Chief Technology Office, Research & Venturing.

Mitchell Alan, Brandt Liz, et al. (Ctrl-Shift, 2009). The new Personal Communication Model: The Rise of Volunteered Personal Information

Landau Susan, Wilton Robin, et al. "Achieving Privacy in a Federated Identity Management System"

Wilton Robin (2009). "What's happened to PETs?" Information Security Technical Report14(3): 146-153 (p.6)

FIDIS and WP17 (2009). D17.4: Trust and Identification in the Light of Virtual Persons. Olivier David and Chiffelle Jaquet, FDIS: Future of Identity in the Information Society

Crofta Piotr (2007). Trust, Complexity and Control: Confidence in a Convergent World, John Wiley & Sons.

Louise, B. (2009). “Reflections on privacy, identity and consent in on-line services.” Information Security Technical Report 14(3): 119-123.

Allan A and Perkins E (2009). “Adaptive Access Control Emerges”, Gartner.

Bagdanovic, D. Crawford, C., Coles-Kemp, L., (2009). “The need for enhanced privacy and consent dialogues.” Information Security Technical Report 14(3): 167-172.

Whitley A. Edgar (2009). Informational Privacy, Consent and the ‘Control of Personal Data. EnCoRe Publication London School of Economics: 15.
Solove Daniel (2004). The digital person: technology and privacy in the information age, New York University Press.

Sachs, E. (2009). “Google OAuth & Federated Login Research.” Product Manager for the Google Security Team, from http://sites.google.com/site/oauthgoog/UXFedLogin/summary

Blakley Bob and Glazer Ian (2009). Privacy. Technology Thread: Policy, Privacy, Personalization: 31.

Norman Lewis. (2009). “Rethinking privacy and trust.” Battle of Ideas, from http://www.battleofideas.org.uk/index.php/2009/battles/3457/

Kantara Initiative (2009). User Managed Access.-Maler Eve (2009). “The design of everyday identity.” Online Information Review33(3): 443-457.

http://www.businessweek.com/globalbiz/content/jan2010/gb20100129_437053.htm - new EU privacy laws

References

i. Experience Brands and the New Engagement Model, Jack Morton Worldwide, 2010

ii. http://www.bcs.org/server.php?show=conWebDoc.35482

iii. Case 3:09-cv-00217-M, United States District Court for the Northern District of Texas Dallas Division, Cathryn Elaine Harris et al v Blockbuster Inc.

iv. How Cloud Computing Will Change Business, Business Week, June 4 2009

v. http://informationcard.net/quick-overview The Information Card Foundation is being supported by companies such as Deutsche Telekom, Equifax, Google, Intel, Microsoft, Novell, Oracle and Paypal.

vi. http://openidentityexchange.org/about

vii. http://www.xdi.org/modules/pages/

viii. http://wiki.eclipse.org/Personal_Data_Store_Overview

ix. Kantara has three working groups investigating different aspects of the new personal data sharing infrastructure. They are:

- The Information Sharing Agreements Working Group. http://kantarainitiative.org/confluence/display/infosharing/Home
- The User Managed Access Working Group, which is working to develop "specs that let an individual control the authorization of data sharing and service access made between online services on the individual's behalf, and to facilitate interoperable implementations of the specs." http://kantarainitiative.org/confluence/display/uma/Home
- The Identity Access Services Working Group. http://kantarainitiative.org/confluence/display/ias/Home;jsessionid=0EEA9940AEA836A0FF1850D0D8C57879

Contact:

Email: info@mydex.org

Visit: http://mydex.org
Follow us on twitter: twitter.com/mydexcic

Designed by Andrew Millar