

It's ours

Why we, not government, must own our data

LIAM MAXWELL



THE AUTHOR

Liam Maxwell is a Councillor and the Lead Member for Policy and Performance at the Royal Borough of Windsor and Maidenhead, where his brief includes Information Technology. His background is as an IT Director in Fortune 500 and FTSE 100 business service companies. He is the author of *How the Internet took Obama back to the 1950s* (Centre for Policy Studies, 2008) and co-author, with Mark Thompson, of *Open Source, Open Standards: Reforming IT procurement in Government, a report for the Conservative Party, 2008*.

The aim of the Centre for Policy Studies is to develop and promote policies that provide freedom and encouragement for individuals to pursue the aspirations they have for themselves and their families, within the security and obligations of a stable and law-abiding nation. The views expressed in our publications are, however, the sole responsibility of the authors. Contributions are chosen for their value in informing public debate and should not be taken as representing a corporate view of the CPS or of its Directors. The CPS values its independence and does not carry on activities with the intention of affecting public support for any registered political party or for candidates at election, or to influence voters in a referendum.

ISBN 978-1-906996-00-0

© Centre for Policy Studies, June 2009

Printed by 4 Print, 138 Molesey Avenue, Surrey

CONTENTS

Summary

1. Introduction	1
2. The high cost of government IT	6
3. The absurd ambition of government IT	8
4. Another way	21
5. Conclusion	35

Appendix: A brief introduction to Service Oriented Architecture and Cloud Computing

“Political leaders will have to let go... of the idea that “we know best” – that people can’t be trusted to run their own lives and their own communities ... because if we get things right we can now move confidently into a new, post bureaucratic era... where true freedom of information makes possible a new world of responsibility, citizenship, choice and local control.”

David Cameron, Speech to Google Zeitgeist Conference,
October 2007.

SUMMARY

- Effective use of Information Technology (IT) can do much to improve public services. In particular, it has the potential to break the central monopoly over public services by giving individuals the ability to exercise real choice and control over schools, GPs, hospitals and other public services.
- In 2009/10, the UK Government will spend about £16.5 billion on IT, equivalent to 1.4% of GDP. However, much IT spending is currently wasted. Only 30% of projects succeed.
- A clear choice is emerging for the future of government IT:
 - **Either** to continue with the Transformational Government agenda. This relies on the State holding, in the words of the Treasury's adviser, a "deep truth about the citizen, based on their behaviour, experiences, beliefs, needs and rights", with huge centralised databases directing public services to the point of need (as judged by the State).
 - **Or** to abandon expensive and failing centralised IT projects and yield control of personal information to individual citizens. This is the approach that has been increasingly effective in the private sector.

- An example: the individual citizen could, if he or she so chose, use services such as HealthVault or Google Health to store their health records and to communicate with their GP or hospital. This would eliminate the need for the NHS database.
- These arrangements would be voluntary. The State would remain as the default holder of personal data. All those who either cannot or do not wish to opt out of central control would still have full access to public services.
- Nor would they apply to matters of national security, or law and order. So it is not proposed, for example, to allow criminals to control their police records.
- This approach requires all public services to use open data standards to ensure that data can be easily transferred from one data provider to another in the same way that customers can today transfer their accounts from one bank to another.
- The potential benefits of this approach are substantial. They include estimated savings on government IT expenditure of 50%; more flexibility; better public services; greater security and privacy over data; and far less intrusion by the State into the everyday lives of its citizens.
- This approach does not, in contrast to the Government's agenda, require huge investment in the creation of untested and largely unnecessary new technology.
- It would, however, reverse the Government's attempt to nationalise data by giving control back to those who should own it: us.

1. INTRODUCTION

The next Government will be faced with unprecedented pressure on public spending. One area for immediate review and reform will be the governance of public sector IT, where central and local government expenditure is estimated to be £16.5 billion in 2009/2010 – equivalent to 1.4% of GDP.¹

Despite this vast expense, much government IT simply does not work. A recent report has calculated that “only 30% of government IT projects succeed”.² It concluded that:

“The public are neither served nor protected by the increasingly complex and intrusive holdings of personal information invading every aspect of our lives.”

The returns on investments are disappointing. Government IT was meant to reduce cost, partly through increased use of online participation with the public. This has at times been

¹ Kable Direct, *Underlying Data*, July 2009.

² The Joseph Rowntree Reform Trust, *Database State*, 2009.

staggeringly unsuccessful. For example, as the LSE academic Patrick Dunleavy has demonstrated, when the DWP analysed its communications with customers, it found that the take-up was tiny.³ More than half of the “customer base” (51%) were able to access services online by mid 2008. But out of the 142 million contacts with the public, only 340,000 (about 0.25%) used the online services.⁴

Reform will not be easy. Existing IT programmes have a formidable institutional momentum. Yet there is some political will to abandon some of the larger projects such as ID Cards and the Interception Modernisation Programme. And, as the Shadow Chancellor George Osborne has already promised,⁵ large IT projects will have to be split into smaller and more manageable components in future. This should improve value for money for the taxpayer.

But far more can be done. Information technology can, if properly designed and implemented, do so much to improve the delivery of public services. The problem is that the way it is being used by government at the moment is hopelessly out of date, expensive and plain wrong.

It is not just a case of getting better value for money on projects that have already been commissioned. It is a question of completely recasting how the public sector uses IT. Currently, the government places itself, rather than its citizens, at the centre of IT design. The Labour Government talks of

³ Department for Work and Pensions, *Communicating with customers, Report by the Comptroller and Auditor General*, 2009.

⁴ P Dunleavy, Paper to the Identity and Privacy Conference, London School of Economics, 15 May 2009.

⁵ “When it comes to IT, Big is not Beautiful”, *The Times*, 3 February 2009.

'transformational government' and sees a need to acquire and share our personal data across departments in an attempt to improve the provision of public services.⁶ Its use of IT is based on the mistaken premise that a huge central dashboard can enable the state to direct services efficiently to points of need. For the government is seeking to take into public ownership as much of our personal information as it can. The old-style statist assumptions behind this approach are plain for all to see.

Control over our personal data is at the heart of the Labour Government's plans for improving delivery of public services. Information on how we live our lives is to be centralised so that the State can decide when and where to provide public services. It is a "we know best" approach, a panopticon, with government insight into every aspect of our lives. It relies on a structurally unsound monopoly, with poor security, little consent, enormous cost and a naïve belief that government knows best.

This is wrong. Future IT projects cannot be designed in the same way. We, the citizens, should control our own data, not the government. The recipient of public services should be at the centre of IT design, not as is currently, viewed as a passive end user of public services.⁷

⁶ For more details on transformational government, see J Kirby, *Who do they think we are? Government's hidden agenda to control our lives*, Centre for Policy Studies, 2007.

⁷ There has, it is fair to say, been much talk of 'citizen centric' design in government IT strategies. Little, if anything, has been done to ensure its effective delivery.

The growth of digital identity

For many people in the UK, the use of online digital identities has become a comfortable addition to our lives. They are content to use personal data profiles for online interactions with friends (Facebook, MySpace), jobs (Linked-in), personal finance and communicating (Hotmail, gmail, instant messaging and so on).⁸

More and more people are using these online services more and more frequently. They are clearly comfortable providing access to aspects of their personal data in exchange for efficient and swift delivery of specific services. They have public and private profiles (and shades in between). But they like to control their own data and who can see it.

Localism, user input and collaboration are driving innovation and change in the online world. But the government's all-seeing, all-knowing concept of centralised state control demonstrates that government has not understood or reacted to these major changes.

The recent Coroners and Justice Bill is a good example of Labour's approach. In the now infamous 152nd clause it sought to "remove barriers to effective data sharing to support improved public services and the fight against crime and terrorism", introducing a mechanism for data sharing right across the public sector. This was, explained Phil Booth, the Director of campaign group No2ID, nothing less than "a sneaky set of tactics attempting to extend the database state."

⁸ Of course, not everyone uses a computer, but the 70% that do are increasingly using IT in this way. However, it is important to recognise that the other 30% are often heavy users of public services. They must not be left out of the loop. The challenge is to ensure that, for both groups, services are delivered more effectively as a result of the improved IT design.

Thankfully the clause was removed at committee stage, but it was not an isolated move and it may come back in the report stage of the bill.⁹

At the same time, in the rest of our lives, technology is going in the other direction, enabling us to choose what data to store and share online. It is also best practice to minimise the amount of data acquired by service providers in the first place.

These are the principles on which government IT should be built. The potential benefits are huge. Giving control of personal data back to citizens will improve the quality and efficiency of public services, will be less expensive and will be far less intrusive.

⁹ “Straw bows to pressure over data sharing”, *The Observer*, 8 March 2009.

2. THE HIGH COST OF GOVERNMENT IT

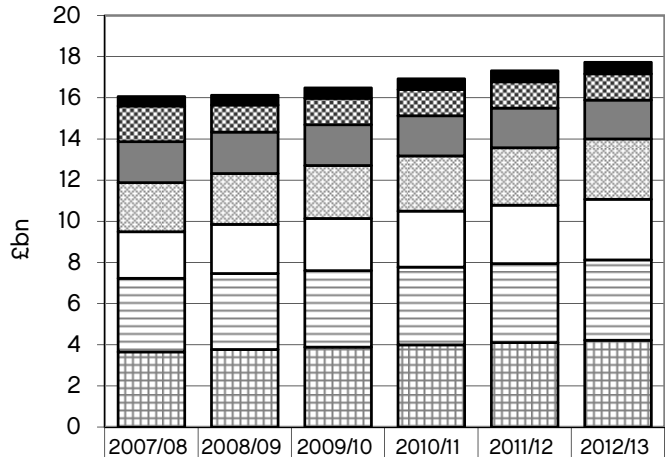
The high cost of government IT provision – £16.5 billion this year, and growing – is equivalent to £700 for every household in the country, or almost £300 for every man, woman and child. To put this in perspective, the State spends approximately 60% more every year on administrative IT than it does on drugs for the National Health Service.¹⁰

No other organisation spends anywhere as much on IT, even though they process similar amounts of data on each individual. For while central government spends £300 per person per year, Google, MSN and online banks spend between £10 and £60 per person per year.¹¹

¹⁰ Written Answer to Anne Minton MP by Andy Burnham MP (then Minister of State (Delivery and Quality), Department of Health), 21 June 2006.

¹¹ SOCITM, *Benchmarking the ICT service across the UK*, 2008.

Forecast of UK public sector expenditure on IT



■ Transport	0.46	0.48	0.51	0.53	0.54	0.56
▣ Justice	1.73	1.31	1.28	1.27	1.27	1.28
■ Defence	2.00	2.01	1.98	1.95	1.92	1.89
▣ Education	2.38	2.48	2.58	2.68	2.79	2.93
□ Health	2.27	2.38	2.53	2.72	2.84	2.95
▣ Central govt	3.58	3.69	3.72	3.78	3.84	3.90
▣ Local govt	3.65	3.77	3.89	4.00	4.11	4.23

Source: Kable, op. cit.

3. THE ABSURD AMBITION OF GOVERNMENT IT

The estimates on government IT spending indicate that central expenditure on IT is hugely wasteful. And one reason for this waste is that each large scale public sector IT system is effectively a monopoly purchaser.

Government IT delivery in the UK operates on the principle of outsourcing large projects to large contractors for very long contracts – contracts that are often worth hundreds and even thousands of millions of pounds over their lifetime. These programmes are usually specific to a department or function and therefore form their own IT “silos” of operation with a great deal of duplication of personal data between them. Examples of seven of these silos, with a collective cost of between £45 billion and £55 billion, include:

- Aspire (HMRC) aims to deliver “a modern and efficient revenue and customs operation” at a cost of £8.5 billion over a 10 year contract. The contract is divided between four outsource partners.

- ID Cards (Home Office) are intended to create a national register of personal information at a cost of £10 billion. The contract will be divided between five major suppliers.
- National Programme for IT (Department of Health) is a series of centralised patient databases and infrastructure. Costs are estimated at between £12 billion and £20 billion. Suppliers are walking away from this project.
- ContactPoint (DCFS) will store details of every child under the age of 18 in the UK. Set up costs are £224 million with annual running costs of £41 million.
- Communications Data Bill (Home Office) will track every email sent or received, website visited by every UK resident at a cost estimated at £12 billion.
- E-Borders (Home Office) will log and screen 95% of all border crossings at a cost of £650 million.
- Libra (Ministry of Justice) will join up magistrates' courts at a cost of £500 million.

The Balkan Wars

As these large independent programmes are delivered, a “balkanisation effect” occurs to the personal data of citizens. More and more bits of personal information are being held by more and more different departments.¹² And while departments are supposed to be collaborating with each other, the reality on the ground is that turf wars are breaking out.

¹² This balkanisation has led in recent years to the drive for transformational government in which all the government systems are meant to be “talking to each other”.

Internal fighting is at its most fierce between the ID Cards scheme (which wants to use the National Identity Register Number as the primary index for population data) and the Government Gateway (which supports existing, separate departmental identifiers, such as National Insurance Number and Unique Taxpayer Reference number, rather than imposing a single number). These two major programmes are in turn competing with identity schemes from the NHS (NPfIT), DCSF (ContactPoint), DfT (biometric driving licence), the Home Office (IRIS, eBorders) and a host of law enforcement and local authority schemes.

Is big best?

The size of IT projects grows and grows. They are now so large that government must rely on only the very largest consultancies and outsourcing providers who, naturally, are able to secure long-term contracts at premium prices. As the table below shows, 60% of spending is concentrated in the hands of just nine firms.¹³

Supplier	Estimated public sector ICT revenues (£ million)
HP/EDS	2,235
BT	2,100
Fujitsu Services	1,200
Capgemini	900
IBM	650
Capita	646
Dell	645
Serco	580
CSC	400

¹³ Kable, op. cit.

This reliance on a handful of suppliers is peculiar to the UK. One study found that in the Netherlands, the top five IT suppliers have 20% of the government market. In the US, this figure is 48%. In the UK, it is 80%.¹⁴

The following table shows some of the IT projects agreed last year and details the extent of the commitments that are being made.¹⁵

SELECTED IT CONTRACTS AWARDED IN 2008

Client	Project	Supplier	Contact Value (£m)	ICT value (£m)	Length (years)
Home Office	Supply of e-borders immigration and government security systems	Trusted Borders	534	534	10
Communities and Local Government	Supply of command and control system	EADS	274	274	8
Learning & Skills Council	Supply of ICT services	Capgemini	162	162	5
Home Office	Visa Application centres	CSC	140	28	5
Cabinet Office	Flex - procurement of IT shared services	Fujitsu Services	61	61	5
Dept Finance & Personnel NI	Accounting services programme	BT	52	52	12
Transport for London	IT service delivery	CSC	74	74	2.5

¹⁴ See P Dunleavy and H Magretts, *Government IT Performance and the Power of the IT Industry: A Cross-National Analysis*, American Political Science Association, 2004.

¹⁵ Kable, op cit.

One of the many dangers of awarding these size of contracts is that, when things go wrong, they can drag on for years, at great expense. The National Audit Office recently reported on the National Offender Management Service's attempt to build a single offender management system for the prison and probation service. On this project, costs rose from an initial £234 million to £690 million. The NAO commented that the project was:¹⁶

“...hampered by poor management leading to a three year delay, a doubling in project costs and reductions in scope and benefits.. the core aim of the original project of a single shared database of offenders will not be met.”

Further, while placing major projects with a single supplier is often seen as desirable because risk is in theory ‘transferred’, the reality is that this rarely happens. Ultimately, if a government IT project becomes unviable, it is the procuring department that still bears the risk and the expense. And this happens, all too frequently. In a study of government IT procurement in seven countries, the UK had one of the highest “scrap rates” of all.¹⁷

Even where some suppliers have taken the financial hit, as in the case of the failing NHS computerisation programme, it is still the citizen who ends up enduring the resulting problems, be they delayed services or inefficient systems.¹⁸

¹⁶ National Audit Office, *The National Offender Management Information System*, 2009.

¹⁷ P Dunleavy and H Magretts, op. cit.

¹⁸ It is possible to avoid these problems. For example, the Thompson report, recently published by the Shadow Chancellor George Osborne called for a cap of £100 million on large government software projects.

An example of the implications of this “big is best approach” can be found in the comments of an IT manager in the NHS:¹⁹

“Inevitably, with the size of the programme, we’re bound to be up against the wall. For the next decade, not for the next year.”

Poor security

That this huge collection of data is insecure is well known. Last year, there was a serious loss of data every couple of days. Security breaches span a whole range of issues, from email errors, to loss or theft of computers, to inadequate website security, to the loss of removable electronic media. A wide range of reports have been issued aiming to identify and fix the problems, including the Poynter report on the HMRC breach, the Burton report on the Ministry of Defence breach, and Sir Gus O’Donnell’s report on data handling in government. However, despite these initiatives and reports, a recent survey of government departments by privacy experts Garlik found that:²⁰

“The biggest culprits of data breaches in recent times – HM Revenue and Customs (HMRC), Ministry of Justice (MoJ), Department of Health (DoH), and the Ministry of Defence (MoD) – all reported a lack of basic systems for managing personal data effectively.”

¹⁹ Comment by the Head of information management and technology planning for Connected for Health, reported at Silicon.com May 2007.

²⁰ Garlik, *Government data policies continue to fail Britons*, 2009.

Basic principles of data minimisation and storage are not common currency in the public sector.²¹ The Information Commissioner has expressed concern about this many times. Perhaps the situation is best illustrated in the evidence the representative of the UK Computing Research Committee gave to the House of Lords Surveillance Committee:²²

“The people who are handling the amounts of data , because they are in contact with them every day are utterly blasé about the risks associated with the data... and have no understanding about the impact of disclosure or leaking... has on the lives of individuals... That is something that has to change.”

It is not designed for citizens

Government IT systems are flawed for another reason: they are designed to operate for the provider (the government), not to meet the needs of the users of public services. This again is out-moded and flies in the face of current best practice.

A recent Oxford Internet Institute report showed that citizens found the design of almost all public service delivery sites unsatisfactory in their current limited provision (with the notable exception of the DVLA Vehicle Excise renewal service).²³

Putting the citizen, and not the government, at the centre of IT design can have startling results. For example, home healthcare for the elderly is currently a huge paper-chasing exercise for care and medical workers, not to mention their administrators.

²¹ Ibid.

²² Professor Angela Sasse, House of Lords Surveillance Committee, op cit.

²³ Margretts, op. cit.

Yet in Sweden, personalised data access has been remarkably successful and has shown that it can transform third-age healthcare services.²⁴

But in the UK, the Government is still trying to offer a one-way “Web 1.0” service to citizens. This approach is awkward and unwieldy – to the point where capability is reduced. As Patrick Dunleavy has explained:²⁵

“People go where they want to go – they traditionally go to high streets and not to government offices. On the Internet they will go where their interests and business take them – government is either there (looking good, looking similar) or it’s nowhere in sight. When they get there, they do what they want to do, or they leave.”

An absence of consent

There is a lack of consent between the state and the citizen in terms of the information that is held on each of us. There is, for example, no method of a citizen tracking what data is held about them. As the Joseph Rowntree report states:²⁶

“The emphasis on data capture, form-filling, mechanical assessment and profiling damages professional responsibility and alienates the citizen from the state.”

²⁴ VINNOVA (Swedish Innovation Agency), *OLD@HOME: Technical Support for Mobile Close Care*, 2006.

²⁵ P Dunleavy, Paper to the Identity and Privacy Conference, LSE, 15 May 2009.

²⁶ Joseph Rowntree Foundation, op cit.

People are right not to trust the government in terms of its capacity for looking after the information it holds on us, for a number of reasons including:

- **Trust.** Government can not be trusted to handle the current data load. Examples of loss are commonplace – HMRC, drivers' information, laptops left on trains and so on. The competence of central government departments is rightly doubted: at least two thirds of the population do not trust the government with their personal data.²⁷
- **Stealth.** The ID card scheme is remorselessly approaching deployment in the UK without the support of a wide range of the population.
- **Permission.** In the private sector the marketing of personal data is relatively strictly regulated. Consent is required. Yet information acquired for one purpose in the public sector may be used for another entirely different purpose.
- **Inaccuracy.** The information that is stored on people is often inaccurate – major Government departments (particularly HMRC, MoJ, DoH and MoD) have failed to put in place basic data protection and error correction policies, despite hundreds of public data breaches over the last 12 months.²⁸
- **Accountability.** No one can know how much or what information on them is held by the government. And when things go wrong (such as when our personal data is misused or lost), no one is held to account.

²⁷ Joseph Rowntree Foundation, op cit.

²⁸ Garlik op cit.

A new, more sustainable and accountable model – genuinely centred on our needs as citizens – is required.

The naïve but terrifying idealism behind Transformational Government

The Government's approach to IT in the public sector is based around the ideal of a benign state with perfect databases. A state that requires, according to the man behind the idea of Transformational Government, Sir David Varney.²⁹

“...a ‘deep truth’ about the citizen based on their behaviour, experiences beliefs needs and rights.”

The former Minister Tom Watson MP refers to this as:³⁰

“...an enabling state moderating collaborative activity for the common good.”

There are numerous worrying assumptions underlying this approach, including: that the state is able to handle this data effectively (all the evidence to date suggests that it isn't); that the state is able to analyse and use the data to improve public services (again, there is no evidence that this has ever been achieved); that the state should have ownership of all aspects of our personal data (why should they?); and, most importantly of all, that the state should be using all this information to interfere more and more in our everyday lives.

²⁹ HM Treasury, *Service Transformation: a better service for citizens and businesses, a better deal for the taxpayer*, 2006.

³⁰ Tom Watson MP, Cabinet Office Minister for Transformational Government, Tower 08 Speech, 10 March 2008.

For our personal information is being nationalised. Examples of how this is happening include:

- The National Identity Register (the core of the ID Cards system).
- The new ContactPoint system from the DCFS.
- The National Pupil Database.
- The NHS Detailed care record.
- The Customer Information System of the Department for Work and Pensions.
- The system to collect a standard identity on each student before they leave school.³¹

One of the aims of Transformational Government is to record every interaction that we have with the state. This information will then be used – it is supposed – to model the public service provided by the state from its analysis of that data.

We, the passive recipients of services, will then have to accept this centralised, targeted public service provision. The assumption underlying this model is that the massive quantities of our personal data collected centrally will enable government to target allocation with ever increasing accuracy.

³¹ Although denied in March 2008 by Bill Rammell MP (a Minister at the then Department of Innovation, Universities and Skills) documents leaked in January 2008 indicated that the Home Office has plans for such a scheme which will join up with the identity card scheme and which a student is expected to have in order to get a student loan. See *The Guardian* 24 January 2008.

Some of the dangers of this approach have been identified by the Information Commissioner's Office. It has, for example, criticised the Government's ONSET programme (which tries to identify children who, it is claimed, "grow up into one of the 20% of adults who are believed to commit 80% of the crime");³²

"This runs the real risk that children are stigmatised from an early age and however well behaved... will be treated with suspicion."

This Brave New World of government by all-knowing databases and remote control relies on the unlikely presumption that the centre knows best. Indeed, it goes even further. It assumes, in the words of a Cabinet Office report, that it will irreversibly perpetuate this concept:³³

"The goal should be to have made the key changes, to have embedded the new cultures, and to have made the process irreversible, by 2011."

This is the opposite of the participatory, devolved and user centric digital culture that is commonplace across the globalised economy. The Government is swimming against the very currents that make the current digital age so successful.

The aim to find out "a deep truth" about each citizen is fundamentally flawed, both philosophically and in practice. Data collection is inaccurate and insecure. Government IT is extraordinarily expensive, over-reliant on a small number of powerful contractors and has a long record of failure. Yet it is on

³² Information Commissioner's Office, Evidence to Lords Surveillance Committee, 2009

³³ Cabinet Office, *Transformational Government enabled by technology*, 2005.

these foundations that the Government is planning to transform the public services.

This is clearly absurd. There is, fortunately, an alternative.

4. ANOTHER WAY

The world is being transformed by technology. The majority of the population now use online services to shop, to bank, and to communicate with friends, colleagues and family.

This has been such a rapid change in large part because the user of the services, not the provider, has been placed at the centre of systems design. Service providers are quickly adapting and responding to their users and their needs, modelling their services around them and responding quickly to user feedback.

A similar transformation is now needed in public service design and the associated role of information technology. This will involve changing the design and the structure of people's interaction with government services. The old structures of centralised state control model must go. This will lead to public services that are more effective, more locally accountable and delivered at a much reduced administrative cost. At the same time, government can then focus resources most effectively on those who are not digitally connected or who prefer not to be.

User-driven online communities illustrate how this could be achieved. Take an example such as the successful Patient Opinion, which uses patient feedback in order to improve NHS services. This is just one small example of how Web 2.0 ideas could really help to make patient (or parent) choice meaningful.

Data storage

Operational government IT systems are often complex, and interoperability is not common. In fact, because of the way that government procures IT, systems regularly function as silos of information and application.

In a well-designed inter-operable IT architecture, however, core data can be accessed by different applications because there is a data transfer layer which enables this: in current IT parlance, what is known as a services or message bus enables different systems to communicate with each other.

The Internet itself and many of the innovative websites that we use now on a daily basis illustrate the way in which properly designed technical architectures can enable us to draw information and services from multiple sources and to enjoy choice in which providers we select.

We need the same dynamics to be applied to public sector IT.

The government's approach to IT governance, architecture and procurement locks in the current vendor to provide the services. It also locks in the data storage infrastructure. And, as discussed above, data on people is often unnecessarily duplicated across public service delivery functions and organisations. Once one has accepted the provision of national defence, law and order and tax collection, the main role of government is the facilitation of public services. This may need

to use data provided by citizens (and may require it to be provided in order to deliver some services). But it should not be a core competence of government to store and manage our data. In fact it may be counter-productive if it tries to do so.

Compare this to what happens in the commercial sector. When a consumer changes their address at Amazon, their bookseller, their CD retailer and the vast array of their carefully selected partner companies (thousands) all have access to that change. Our needs as a user are reflected both in the business processes behind Amazon's systems and in the technical architecture that delivers those business services. User design, business design and technology design work together to deliver a high quality service to the consumer.

Such systems work well because we choose whether to grant them access to our data. We have for example a data profile with the ordering system and we remain responsible for updating it. If we don't update it and move or change our credit card details, we don't get the book.

The way that Amazon can do this is through using the data access model – the partners that are allowed access integrate the data access process in their own procurement and provisioning processes. Data is held in appropriate systems but when the user provides consent they can control the ways in which it is brought together – in ways mutually beneficial to them and the service provider.

The crucial distinction is that *access* does not equal *control*. Although we may choose to give Amazon and its thousands of partners *access* to our data we do not grant them *control* of our data. Because it remains *our* personal data. Amazon is happy

for the person who makes the changes to personal data to be the person that knows about that person best – us.

Our data under our control.

Allowing IT diversity

Allowing citizens to control their own data also enables a far more flexible approach to IT design. Referring to these as “gateways”, the Thompson report explained that:³⁴

“.....open gateways hold out the prospect of rapid development of sustainable point-systems which meet particular needs in government rapidly and at low cost.

For example, a manager in a local social security office working with her staff might envisage ways of re-organising the work of the office if information in the central computer systems could be presented in a different way. If the software proved useful it would be a simple matter for other offices to use it too.”

Indeed the evolution of open source developments and applications in schools, in hospitals and in other public service delivery units is possible through the implementation of open standards driven by personal ownership of data.

The best applications will be those that are created by those who are delivering public services. The individual GP practice, the school, the benefits office – all of these will be able to adapt

³⁴ M Thompson et al, *Open Source, Open Standards: Reforming IT procurement in Government*, Conservative Party 2008.

IT to their own needs. Government processes will become easier to navigate, smoother and more efficient. But crucially they will also be able to evolve to meet change. Incremental changes over time can be implemented in many local, relatively low-risk environments.

Contrast this to the high-risk, “one size fits all” monolithic approach proposed by the central enabling state. In the latter case, change has to be revolutionary and has to involve massive, game-changing shifts. The world of the internet, of twenty first century citizenship favours the former. Evolution beats revolution.

It works elsewhere

That this approach can deliver significant changes to the effectiveness and cost effectiveness of public services is recognised elsewhere. Take for example the health care system in the US:³⁵

“The first US national health care information technology coordinator estimates that if the current rate of interoperable electronic health record (EHR) adoption is sustained through 2014, it would create a launch pad for quality gain and health care spending reduction in excess of 50 percent in the subsequent decade.”

³⁵ A Milstein, “Health Information Technology is a Vehicle, not a Destination”, *Health Affairs*, February 2007.

One of the critical changes required to make this happen is ensuring that the health providers cede “control of clinical information to patients.”³⁶

Another example is the old@home programme in Sweden. In this case, personal health records are controlled by the patients. But they grant access to carers, health workers, close relatives and so on as the role requires. This has enabled flexible delivery of healthcare services to a vulnerable and high-maintenance cohort of patients. Its success has been based on:³⁷

- “a virtual health record (VHR) with different views for general practitioner, district nurse and home help service,
- a virtual care plan (VCP) for district nurse, home help service, patients and relatives as part of the VHR,
- a web portal with intuitive information access for patients and relatives (WPR), and
- an integration platform based on a service oriented ...architecture.”

Both of these examples show that putting citizens in control of their data gives the providers of public services the flexibility they need to transform their services.

³⁶ Ibid.

³⁷ OLD@HOME, op. cit.

Service Oriented Architecture

It is now possible to develop a better model for modern government IT. This involves using Service Oriented Architecture (SOA) to enable government IT systems, software, devices and services to integrate and talk to each other.³⁸

This, it must be stressed, is not a new concept in the private sector where its use enables great agility and cost-effectiveness, and the most effective European governments use this approach.

Consider for example the Austrian Government where the provision of public services over the internet is seen as “best in class”.³⁹ There, eGovernment applications are made using Online Application Modules which are “a software tool for the efficient and secure creation of government applications .. interoperability is guaranteed by the use of standard interfaces and tools.”⁴⁰ The Austrian approach has created effective e-government by ensuring departments work together using a common service oriented architecture.

The UK Government has been working to develop a cross-government enterprise architecture (xGEA) which sounds similar but does not in its current published form even mention SOA, the internet or the Web. It has been designed in-house by civil

³⁸ See the Appendix for an extended explanation of SOA.

³⁹ Capgemini Survey for the European Union, *Online Availability of Public Services: How Is Europe Progressing?*, 2006.

⁴⁰ I Goetzl, T Greeching and G Fisher, “eGovernment in Austria and Vienna: Progress by vertical co-operation” in A Shark and S Torporkoff, *Beyond eGovernment and e_Democracy: A Global Perspective*, Booksurge Publishing, 2008.

servants. Respected technical authors see it as an idea, little more, and one still rooted in the old world of provider-centric design.

Government processes and systems should become simpler – the layers of complexity need to be stripped out and replaced by a simpler architecture based on common “building blocks” and connectivity.

Cloud Computing

Cloud Computing is a similar approach to SOA which is rapidly taking root in the commercial sector. This is an infrastructure platform based not in a government server room, but within the internet cloud. Large corporate companies such as IBM, Microsoft, Amazon, and Yahoo are building huge new data centres which host customers’ applications online – “in the cloud”.

Cloud computing (dynamically scalable IT resources provided as a service over the Internet) provides a simple and effective platform for users to access the computing services they need. It also enables a diversity of application “building blocks”, hence the element of choice and consent that will help both drive and underpin citizen-centric public services. Importantly, cloud computing is also supported in open source products such as Ubuntu, further underpinning the Thompson report’s call to open up public sector IT procurement to the increased use of open source and the greater involvement of small and medium-sized UK businesses.

The combination of these two approaches brings more efficient business processes and simplifies the IT services to support them – but crucially this change will enable effective data control by citizens; and choice over where to hold that data.

Cloud computing systems, provided by third parties other than government, will enable us to choose where to store our personal information (such as our medical records). It will also allow us to choose with whom we want to share our details. This is increasingly mainstream. Microsoft HealthVault and Google Health are thriving, growing businesses, showing how future public services IT might be better designed.

The advantages of this are immense. Above all, government departments will no longer need to procure and own all the IT infrastructure itself, or to pay an outsourced company to do so on its behalf (as it does at the moment). For example, if services such as HealthVault had already existed, there would be no need whatsoever for the UK Government to spend anything like £12 billion building its own centralised medical records system. The market is now providing the IT systems needed for government, systems which are better centred on the needs of us, as public service users, rather than on government as a fumbling middleman, and which are far cheaper to run.

This system already works with retail banks – HSBC's well-respected FirstDirect has long led the way in the United Kingdom. So why not with other non-financial information?

Even if one takes the line that the private sector *per se* may not be better than the state at keeping data safe, the data would be likely to more widely distributed. People would be unlikely to store all their information with one provider, and so would be less compromised if the data went missing. By dispersing the data, the risk of serious damage would be minimised.

In addition, in the private sector there is choice. Users can move their data from one provider to another if they do not like the way it operates – in the same way they can move banks. And

government can ensure that the governance models around such commercially offered systems meet the high standards that need to be applied to public services and citizens' personal information. Indeed this appears to be the route anticipated by the respected Ontario Information Commissioner Ann Cavoukian in her description of how cloud computing should conserve privacy.⁴¹

Government Relationship Management

This approach is supported by the growing importance of Vendor Relationship Management (VRM). Since its adoption as a core project of the Berkman Center for Internet and Society at Harvard University, VRM has come onto the agenda of large public and private organisations which recognise the benefits of providing their customers with the tools to complement and contribute to their data “with their consent, for their benefit”.

VRM users store their data where they want and issue consent for access. In government, this approach has been tried successfully in Sweden where the Government Agency for Innovation Systems has piloted the “e-Me” programme – where schools, authorities and companies are required to work with the students' own data.⁴²

However, it is in North America and in the provision of health services where VRM is making strongest progress. The use of personal medical record systems in particular is starting to transform the way medical service providers interact with their

⁴¹ A Cavoukian, *Privacy in the clouds – A White Paper on Privacy and Digital Identity: Implications for the Internet*, September 2008.

⁴² M Siosteen and L Albinsson, “Innovation and Research in Public E-Services and Administrations”, in Shark and Toporkoff, op. cit.

patients. CVS, a large American pharmacy chain, has signed up with Google Health to provide personalized data storage for patients medical histories.⁴³ In concert with other pharmacies this now serves a 100 million strong customer base.

Because users own their data, they can start to generate information from it using tools – for example, a graphing feature helps patients visualise their medical test information.

And hospitals, such as the well-respected Mayo clinic in Rochester, Minnesota, are now offering personal medical records data services (through Microsoft's HealthVault). This programme allows patients to store medical information electronically, and to receive individual guidance based on it from physicians and healthcare staff.⁴⁴

The great advantages of this approach is that it is far cheaper for government; and that it returns data control to the people who can maintain it most effectively: us, the citizens. It also means that the citizens can do more with the data and use it more effectively. Citizens or their nominated carers can define and manage their own care plans to fit their scheduling requirements. Users can control their career search for jobs online making best use of government and private sector resources. Third sector organisations can provide public services in a flexible and cost effective manner by more closely matching their resources to their customers needs. The opportunity for the more effective spending of personal care budgets to provide a less expensive and more effective outcome is compelling.

⁴³ www.techcrunch.com/2009/04/06/cvs-signs-on-with-google-health-to-offer-comprehensive-pharmacy-history/

⁴⁴ See *The Seattle Post-Intelligencer*, 22 April 2009.

This approach would work in the provision of all public services data from education through health, career management and delivery of benefits. The features of a Government Relationship Management approach would include:

- Open data standards and the integration of government IT into a more sustainable and open approach.
- Data should be held by a third party chosen and trusted by the citizen, not the government.
- Government systems should have *access* to the data where it is needed for delivery of public services but the *control* of the data should be the citizens' – it is their data.
- Data provision should be provided by the data hosts who can provide such services more effectively and cheaply than the government.

The role of government will be limited to ensuring the existence of an appropriate governance, compliance and regulatory model. Provided that data infrastructure providers meet such requirements, they should be able to offer this service to the public. Citizens will then be free to choose which provider or providers host their data. At any time a citizen is free to change to another approved service provider.

Underlying principles

Several underlying principles and aspirations support these proposals. These include:

- **Open Standards.** Information must be properly structured, enabling common interaction through open data standards, including data formats and systems interfaces and protocols.

- **Effective Security.** Security and privacy will be enhanced. The decentralisation of data necessarily reduces the risk of a single, massive, data loss. The requirement to have open data standards will ensure data is held securely. Allowing public service systems access to citizen data in a clearly defined and accountable manner will ensure more effective security of data and data processing and enhanced citizen privacy.
- **Access does not equal control.** The citizen is identified as the user of the services and can interact on their own terms. Systems will necessarily be designed to work for the citizen. Systems that do not cater to the citizen will fail much more quickly and openly than current inadequate systems and processes.
- **Government can't keep up.** The idealised benign state, with the perfect database that can provide the services that government thinks the people need, is gone.
- **Trust is restored through ownership.** Consent is enshrined in the ability for the citizen to allow access to data in order to receive public services.
- **Cost is reduced – markedly.** The Thompson report suggested that the use of open procurement would enable a reduction of £600 million per year. The introduction of a more user centric, secure cloud-based infrastructure would enable hosting and management costs to be further reduced. In the medium term a sustainable reduction of the £16.5 billion spending in IT by 50% would be a realistic goal.⁴⁵

⁴⁵ All estimates on potential savings are necessarily vague. However, major savings will come from the reduction in data duplication; a reversion to single point data for users; and the ability to broaden the supplier base.

An additional beneficial side-effect of these proposals is that it would reduce the heavy dependence on the huge IT consultancies. Instead, they would be likely to favour smaller, more innovative and responsive SMEs (the majority of whom are excluded by the size of current government IT contracts).

Access for all

The 30% of the population that does not go online includes a high proportion of people in low income groups, the elderly and those on means tested benefits.⁴⁶ Some of the people that are most in receipt of public services can have “unstructured lifestyles”. The idea of an online profile would be alien to them.

Equally, there are a sizeable number of people who may remain comfortable with the government holding their personal core data. It is important therefore, that the proposals to liberate our data from central government are voluntary.

If you want the government to hold your data, fine. Therefore one of the providers, the default provider at the start of this programme, should be a government data hosting agency. This must allow access to services for those who prefer to make use of the more traditional forms of communication. The proportion using this approach will diminish, but it will always be with us.

However, by imposing the requirement that people can, if they wish, host data with a trusted VRM provider rather than the sole government supplier, the IT used to deliver public services will have to utilise open data standards. This will, of course, also lead to a less costly, more agile and more effective provision of IT and of public services.

⁴⁶ Magretts, op. cit.

5. CONCLUSION

Ever greater centralisation runs counter to the current movement towards accountable, consent-based, user-driven data administration and storage. It runs counter to public sentiment, which believes local services with local accountability are preferable to centrally imposed targets.

The use of more effective choice in data storage provides not just a cost saving measure in itself, it provides a route for a more strategic change in the way IT governance works in the public sector. If the costs of storing information by Government is of several orders of magnitude greater than the industry then the case for privatisation of this service is compelling.

A competitive market for data storage and management can be expected to emerge. Certainly it will be important for different providers to be able to talk to each other – but this is now standard practice (commonly referred as “open documented interfaces and protocols which enable systems to interoperate with the data”). Competitive forces will encourage data security and respect for privacy.

The ability for the dynamics of the marketplace to operate in the provision of IT and data services will lead not just to competitive providers of data storage. It will also introduce:

- effective accountability – providers will be accountable to citizens who can change provider easily;
- the dissection of huge projects into manageable modules;
- effective competition and control in the procurement of government IT services;
- leaner and more cost effective ways of delivering public services, often with better outcomes.

Developing the ideas set out in this paper will enable the introduction of effective management and cost control of government IT. And it will allow the citizen to claim their digital identity back. Citizen data under citizen control.

After all, it is our data. Not the state's.

APPENDIX: A BRIEF INTRODUCTION TO SERVICE ORIENTED ARCHITECTURE AND CLOUD COMPUTING

Service Oriented Architecture (SOA)

The concept of creating an architecture of individual technology components with defined interfaces is referred to as a Service Oriented Architecture (SOA) and is the basis of most IT delivery in large enterprises. This definition is from Wikipedia:

“... service-oriented architecture (SOA) provides methods for systems development and integration where systems group functionality around business processes and package these as interoperable services. An SOA infrastructure allows different applications to exchange data with one another as they participate in business processes. Service-orientation aims at a loose coupling of services with operating systems, programming languages and other technologies which underlie applications. SOA separates functions into distinct units, or services, which developers make accessible over a network in

order that users can combine and reuse them in the production of business applications. These services communicate with each other by passing data from one service to another, or by coordinating an activity between two or more services.”

The benefits deriving from implementing SOA are as follows:

- **Vendor neutrality.** An SOA is based on a set of open standards that have been widely embraced by the vendor community. They facilitate interoperability between applications and systems and enable procurement officials to select the particular vendor that best meets their needs.
- **Speed.** Applications built on SOA principles have well-defined and interoperable interfaces. Adding new functionality requires less system integration and can be delivered more quickly than with previous architectural approaches.
- **Cost.** The complexity of building distributed applications is reduced by using well-defined interfaces based on open standards. This improves developer productivity and reduces systems integration costs as each component can be developed independently of others.
- **Flexibility.** An SOA hides or abstracts the underlying physical complexity of the IT infrastructure. Once an SOA has been implemented, IT organizations can add or remove capacity to meet changing demands without having to re-write the applications.
- **Extensibility.** An SOA is generally based on the same open standards used in the Internet. This makes it much easier to connect customers and partners to services running on the government infrastructure.

Cloud Computing

The following definition is from Wikipedia:

“Cloud computing is Internet (“cloud”) based development and use of computer technology... whereby dynamically scalable... resources are provided as a service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure “in the cloud” that supports them... As customers generally do not own the infrastructure, they merely access or rent, they can avoid capital expenditure and consume resources as a service, paying instead for what they use. Many cloud-computing offerings have adopted the utility computing model, which is analogous to how traditional utilities like electricity are consumed, while others are billed on a subscription basis.

Sharing “perishable and intangible” computing power among multiple tenants can improve utilization rates, as servers are not left idle, which can reduce costs significantly while increasing the speed of application development. A side effect of this approach is that “computer capacity rises dramatically” as customers do not have to engineer for peak loads. Adoption has been enabled by “increased high-speed bandwidth” which makes it possible to receive the same response times from centralized infrastructure at other sites ... An often-quoted example is Google Apps, which provides common business applications online that are accessed from a web browser, while the software and data are stored on Google servers.”



BECOME AN ASSOCIATE OF THE CENTRE FOR POLICY STUDIES

For 35 years, the Centre for Policy Studies has stood for freedom. We trust people to make decisions about their lives. We believe this not just because freedom breeds prosperity, but because it is right. People should be free to live as they choose, to spend their money as they wish. The State should be their servant, not their master.

The Centre for Policy Studies is independent from all political parties and pressure groups. We consistently advocate a distinctive case for smaller, less intrusive government, with greater freedom and responsibility for individuals, families, business and the voluntary sector.

Through our Associate Membership scheme, we welcome supporters who want to be involved in our work. Associate Membership is available for £100 a year and will entitle you to:

- all CPS publications produced in a 12-month period
- invitations to lectures and conferences
- advance notice by e-mail of our publications, briefing papers and invitations to special events

For more details, please write or telephone to: The Secretary, Centre for Policy Studies, 57 Tufton Street, London SW1P 3QL.

www.cps.org.uk



SOME RECENT PUBLICATIONS

What's wrong with 50p? by Jill Kirby and Iain Griffiths

"50p tax 'unfair, complex and damaging' to economy" – headline
in *The Daily Telegraph*

Re-empower the Bank of England by Sir Martin Jacomb

"In a paper for the Centre for Policy Studies, the former Bank director argues the Tories are pulling their punches: the FSA should be transformed into a mere subsidiary of the Bank of England" – Lombard, *The Financial Times*.

The Phoney War on Drugs by Kathy Gyngell

"Think-tank slams Government's liberal approach to drug abuse"
– headline in *The Western Mail*

The Myth of Inflation Targeting: the worst policy mistake of our generation by Maurice Saatchi

"Blame this crisis on the myth of inflation" – headline in *The Times*

The Stock Market under Labour: the legacy of Gordon Brown by John Littlewood

"Labour's claim to be the best party for the City was called into question yesterday as research revealed that the FTSE 100 has underperformed every main stock market except Japan's since it came to power in 1997" – *The Times*

Save 100,000 homes from repossession by Natalie Elphicke

"Repossession plans not enough" – *BBC Online*



Step off the Gas: Why over-dependence on gas is bad for the UK by Tony Lodge

“Dire consequences of relying on imported gas” – headline in
The Sunday Times

Ticking the right boxes: why multiple tests are a better and cheaper alternative to SATs by Tom Burkard

“The report comes amid continuing controversy about the role of national curriculum tests” – *The Times*

Freedom for Public Services by William Mason & Jonathan McMahon

“Labour handed £15 billion job cut plan” – *News of the World*

The Price of Irresponsibility by Brooks Newmark MP

“The Great Debt Lie” – headline in *The Daily Mail*

From Boom to Bust: a plain guide to the causes and implications of the banking crisis by Howard Flight

“Every Cabinet member, indeed every MP and PPC should memorise and then understand Howard Flight’s Pointmaker” –
Conservativehome.com

The New Good Council Guide by Stephen Greenhalgh

“I have seen the Conservative future and it works” – op-ed
headline in *The Sunday Telegraph*

The 2009 Lexicon: a guide to contemporary Newspeak

“The much-praised 2009 Lexicon from the Centre for Policy Studies contains some hitherto-overlooked gems of interest to business readers” – *The Mail on Sunday*

The UK Government spends the equivalent to 1.4% of GDP – £16 billion this year – on its IT projects. Most of this money is wasted: only 30% of projects succeed.

It is time to abandon expensive, failing and intrusive IT projects and to reverse the Government's attempt to nationalise data. Control over the information that the government holds on us should be given back to those who should own it: us

This approach is common in the private sector. Its potential benefits include improved public services; estimated savings on government IT expenditure of 50%; greater security and privacy over data; and far less intrusion by the State into the everyday lives of its citizens.

Price £10.00

