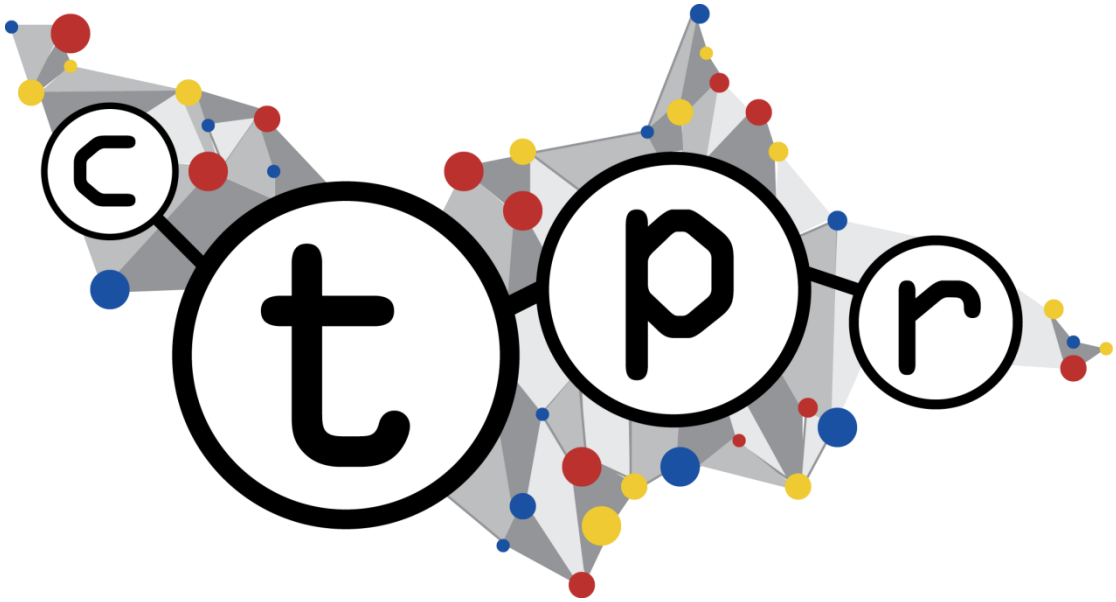

Centre for Technology Policy Research

MEMO NUMBER 2: NOVEMBER 2009

THE OBAMA EFFECT: THE US IT REVOLUTION AND THE UK

EXECUTIVE SUMMARY

This Memo, from the independent Centre for Technology Policy Research (CTPR), provides an analysis of some of the key IT developments in the US relating to President Obama's campaign to secure the presidency and subsequently, since taking office. It considers these developments in the context of how they have already impacted, or could further impact and influence, UK public sector IT and the smarter use of IT during electoral campaigns.

Our findings in this Memo include:

- Barack Obama made extensive, intelligent use of IT during his Presidential campaign and has continued to do so since taking office. IT expenditure is less significant as a percentage of GDP than in the UK, but the US federal government still spends over $75 billion annually on information technology.
- During his campaign, Barack Obama set out clear thoughts on changes to the policies and governance around IT that would follow should he become President.
- In many ways, the current US position is reminiscent of the late 1990's in the UK and the commitments and policies set out by Blair, with ambitious aspirations for how technology will enable the modernisation of government services.
- This is little surprise since in many ways the US has lifted some of the best of the UK's policies from the late 1990's, particularly in the area of online trust models. However, unlike the UK, Obama's team has focused as much on delivery, rather than on the belief that policy alone is a worthwhile outcome. The UK's failure was not so much in its lack of vision and objectives, but its inability to execute successfully in delivering against them.
- To balance this critical perspective however is a recognition that the US initiatives have re-awoken efforts around open government and smarter use of IT in the UK – but it remains to be seen whether this will any better sustained and delivered this time around than previously.
- There is a potential "Obama impact" on the coming UK election. The Conservatives studied Obama closely during his campaign to become President. Speeches over the past few years, such as those of George Osborne on open source and open government, are reminiscent of policies set out by Barack Obama during his Presidential campaign. What remains

less clear in the UK at present are the clear policies and changes that would follow a new administration taking office around the governance, architecture and procurement of more effective IT in the public sector.

- The real challenge will remain, whatever the flavour of government next elected, its ability to put into place an effective model of governance, architecture and procurement to enable the UK not only to emulate the US position, but to use it as a springboard to renew the UK's faith in, and best use of, IT in the design, delivery and operation of public services. This should be about more than just copying the US model since the US public sector IT supply marketplace is markedly different from that of the UK: the US has maintained an effective market with far greater competition when compared to the relatively small number of large players that dominate UK public sector IT supply.
- With its investment in skills, infrastructure and renewal, and the associated governance and investment through the recovery programme, the US has made clear commitments and investments that the UK has deliberately shunned (for example, the UK through initiatives such as "*Digital Britain*" has sought to tax the new digital economy whilst subsidising old economies such as the car industry and banking. This is in stark contrast to the forward-looking leadership of other countries such as the US, which have invested in new areas such as broadband as part of their economic programmes).
- Elsewhere, in specific technology policy areas such as its identity strategy, the UK seems to have lost its way. The opportunity and actual cost of the national ID cards programme has displaced the UK's original thought leadership in this important area. The UK's earlier vision for a federated, third-party identity model is one that Obama's America is now delivering. The UK needs to re-think its current approach in a far more integrated and comprehensive fashion if it is to get back on track, deliver effective online public services and remain internationally relevant and competitive.
- An underlying concern remains regarding why the UK has in the past originated good ideas in terms of IT policy, but lacked the ability to implement them – whilst the US has taken the best ideas from elsewhere (including the UK) and worked out both how to innovate around them and, so far at least, managed to deliver them.

It should be of concern to all the mainstream political parties in the UK that the most visited Website of any UK political party is that run by the far right British

National Party (BNP), with more hits than all other parties put together[1]. Lessons can be learned from the Obama Presidential campaign about how to use technology to re-engage grass roots supporters.

It is important that all UK politicians and Parliamentary candidates engage more fully with technology and its potential – for both good or ill. IT is no longer an adjunct to UK politics, but an integral part of policymaking and public engagement. This is something Obama and his team understood, both during the Presidential campaign and on taking office.

As this Memo narrates, Obama's campaign team were able to achieve a strong and effective interplay between the online and offline world, with online supporters also being highly active on the ground when required. The two become mutually reinforcing of each other rather than being seen as separate campaign initiatives.

[1] http://www.telegraph.co.uk/news/uknews/1562960/BNP-website-is-the-most-popular-in-politics.html

CONTENTS

BACKGROUND

In the USA, President Barack Obama has initiated a new approach to the use of information technology (IT) in the public sector. This use predates his investiture as President and demonstrates a smart use of technology both as a campaign tool, and the extent to which technology policy needs to be thought through systematically in opposition in order to hit the ground running in office.

During his campaign to enter the Whitehouse, internet and web-based tools enabled Obama and his campaign team to attract a high number of financial donors and to energise an effective grass-roots volunteer base. The ease of use and awareness of social media such as Facebook opened up participation amongst those who had not previously been engaged in a Presidential campaign.

Following his election to office, Obama has moved swiftly to adopt new models of governance, architecture and procurement across public sector IT. This has involved putting into place new people, having policies (such as those around open data, and federated models of identity and authentication) ready to deliver, and driving the open source and open standards agenda not only at the policy level, but in terms of real-world implementation.

There are clear lessons here from which the UK needs to learn if it wishes to address the current shortcomings of IT in the design, delivery and operation of public services in the UK.

PRE-ELECTION UTILISATION AND VIEWS OF IT

During his campaigning, Barack Obama made repeated references to the need for openness, including in areas such as net neutrality, policies to encourage greater diversity in media ownership, an expansion of access to broadband, and the use of technological innovation to address concerns about the economy, health care, climate change, energy, and immigration[2].

Obama and his technology team were strong proponents of open-source, shared knowledge models, not just in theory for when they might take office but also in the ways they developed their own policies and developed their campaigning approach. Web sites, wikis and similar tools were all used to develop their thinking and plans. There was smart central management and utilisation of technology to drive active participation amongst a new network of volunteers at local level.

[2] http://www.prospect.org/cs/articles?article=obamas_plan_for_opensource_democracy

Obama formalised his Presidential intentions with the announcement of his *Technology Plan*[3] in October 2007, saying at its launch:

> *"Let us be the generation that reshapes our economy to compete in the digital age. Let's set high standards for our schools and give them the resources they need to succeed. Let's recruit a new army of teachers, and give them better pay and more support in exchange for more accountability. Let's make college more affordable, and let's invest in scientific research, and let's lay down broadband lines through the heart of inner cities and rural towns all across America"*

Five key objectives were set out in the plan, namely to:

- *ensure the full and free exchange of information among Americans through an open Internet and diverse media outlets*
- *create a transparent and connected democracy*
- *encourage the deployment of a modern communications infrastructure*
- *employ technology and innovation to solve our nation's most pressing problems, including reducing the costs of health care, encouraging the development of new clean energy sources, and improving public safety*
- *improve America's competitiveness*

Alongside the ambition to make more effective use of technology in the future of the USA, the plan also highlighted the need to safeguard the right to privacy, recognising the potential problem that the open information platforms of the 21st century can also tempt organisations to violate the privacy of citizens. It set out the need for sensible safeguards to protect privacy in this "*dynamic new world*". As President, Barack Obama committed in his plan to "*strengthen privacy protections for the digital age and will harness the power of technology to hold government and business accountable for violations of personal privacy.*"

Some of the most notable commitments came in the area considering how technology can help renew and re-empower democracy, including:

- *making government data available online in universally accessible formats to allow citizens to make use of that data to comment, derive value, and take action in their own communities. Greater access to environmental data, for example, will help citizens learn about pollution in their communities, provide information about local conditions back to government and empower people to protect themselves*

[3] http://obama.3cdn.net/780e0e91ccb6cdbf6e_6udymvin7.pdf

- *establishing pilot programs to open up government decision-making and involve the public in the work of agencies, not simply by soliciting opinions, but by tapping into the vast and distributed expertise of the American citizenry to help government make more informed decisions*
- *requiring appointees who lead Executive Branch departments and rulemaking agencies to conduct the significant business of the agency in public, so that any citizen can watch a live feed on the Internet as the agencies debate and deliberate the issues that affect American society. Ensuring that these proceedings are archived for all Americans to review, discuss and respond. Requiring appointees to employ all the technological tools available to allow citizens not just to observe, but also to participate and be heard in these meetings*
- *restoring the basic principle that government decisions should be based on the best-available, scientifically-valid evidence and not on the ideological predispositions of agency officials.*
- *lifting the veil from secret deals in Washington with a web site, a search engine, and other web tools that enable citizens easily to track online federal grants, contracts, earmarks, and lobbyist contacts with government officials*
- *giving the American public an opportunity to review and comment on the White House website for five days before signing any non-emergency legislation*
- *bringing democracy and policy deliberations directly to the people by requiring Cabinet officials to have periodic national online town hall meetings to answer questions and discuss issues before their agencies.*
- *employing technologies, including blogs, wikis and social networking tools, to modernize internal, cross-agency, and public communication and information sharing to improve government decision making*

Another part of the plan included a commitment to "*bring government into the 21st Century*" and to use technology to reform government and improve the exchange of information between the federal government and citizens. Specifically Obama committed to:

- *appoint the nation's first Chief Technology Officer (CTO) to ensure that the government and all its agencies had the right infrastructure, policies and services for the 21st century. The CTO will ensure the safety of the USA's networks and lead an interagency effort, working with chief technology*

and chief information officers of each of the federal agencies, to ensure that they use best-in-class technologies and share best practices.

- *task the CTO to have a specific focus on transparency, by ensuring that each arm of the federal government makes its records open and accessible as the E-Government Act requires. The CTO will also focus on using new technologies to solicit and receive information back from citizens to improve the functioning of democratic government.*
- *task the CTO with ensuring the technological interoperability of key government functions. For example, the CTO will oversee the development of a national, interoperable wireless network for local, state and federal first responders as the 9/11 commission recommended. This will ensure that fire officials, police officers and EMTs from different jurisdictions have the ability to communicate with each other during a crisis and that there is no repeat of the failure to deliver critical public services that occurred in the aftermath of Hurricane Katrina.*
- *recognise that in the 21st century, our economic success will depend not only on economic analysis but also on technological sophistication and direct experience in this powerful engine of our economy. The government's economic policy-making organizations and councils will include individuals with backgrounds in our technology industry.*

Barack Obama's campaign to become President of the USA was notable for its smart use of modern IT which worked in concert with his grass-roots, ground-up and devolved campaign model. His programme took a simple approach to IT, taking maximum advantage of open source software and online social networking facilities such as *Facebook*. Indeed, Obama's campaign team included Chris Hughes, one of the three co-founders of *Facebook*. He helped establish the influential campaign website *my.barackobama.com*, which helped develop a social networking style online community for the Presidential campaign, *MyBo*. This enabled supporters to self-organise as they saw fit, and by March 2008 claimed more than half a million members and more than 8,000 affinity groups[4]. Already by October 2007, more than 280,000 people had created accounts on *barackobama.com*, with those users in turn creating over 6,500 grassroots volunteer groups and organising more than 13,000 off-line events using the site.

The campaign also made use of a smart distributed "*cold calling*" system that enabled volunteers to make calls efficiently from their own homes whilst still

[4] http://www.rollingstone.com/news/coverstory/obamamachineryofhope/page/3

working as part of a co-ordinated campaign of calls to supporters and potential supporters managed through an overall web-based system[5].

The system addressed issues of poor quality connections and bandwidth by enabling supporters to download schedules of calls and to work in semi-autonomous mode where necessary before later reconnecting and re-synchronising with the main campaign system.

FIGURE 1: MYBARACKOBAMA.COM

BusinessWeek reported that "*on the Web, Obama is the clear winner*"[6]. At a time when he was competing heavily with Hilary Clinton, *techPresident*, an impartial blog that tracked the 2008 Presidential candidates campaign use of technology, reported that he had more than three times the number of supporters on social networks *MySpace* and *Facebook* and his *YouTube* videos were experiencing more than 24 million plays a day in March (nearly three times more daily views than Hilary Clinton's). It is also widely reported that Obama's use of online fundraising was a major factor in him raising the significant amounts of revenue required to run his campaign, with around 80% of donations reported as having been raised online[7].

Obama's campaign team were able to achieve a strong and effective interplay between the online and offline world, with online supporters also being highly active on the ground when required. The two become mutually reinforcing of each other rather than being seen as separate campaign initiatives.

[5] http://blogs.zdnet.com/BTL/?p=9019
[6] http://www.businessweek.com/technology/content/mar2008/tc2008035_280573.htm
[7] http://www.businessweek.com/technology/content/mar2008/tc2008035_280573.htm

During his campaign, Obama also started to make clear some of the changes he would make if he were to become President around the effective governance of IT and its interplay with public policy. He called for a new powerful role to be created to help drive technology in government, a new cabinet-level Chief Information Officer and associated Chief Technology Officer who would be responsible for oversight of the federal government's use of technology.

Role in Economic Stimulus

The American Recovery and Reinvestment Bill of 2009 included $550bn of investments, including provisions to expand broadband services to the 40% of households in the US who currently do not have it, the computerisation of medical records for GP's and hospitals and to develop a smarter national electrical grid.

In total, some $37bn of IT network infrastructure spending was included. This followed an earlier comment from President Obama that it was unacceptable that the United States ranked only 15th in the world in broadband adoption[8].

Structure

President's Council of Advisors on Science and Technology (PCAST)

PCAST is an advisory group of scientists and engineers who advise the President and Vice President, helping to formulate policy in areas where an understanding of science, technology, and innovation is important. PCAST is co-chaired by John Holdren, Assistant to the President for Science and Technology and Director of the White House Office of Science and Technology Policy; Eric Lander, Director of the Broad Institute of MIT and Harvard and one of the principal leaders of the Human Genome Project; and Harold Varmus, President and CEO of Memorial Sloan-Kettering Cancer Center, former head of the National Institutes of Health and a Nobel laureate.

In April 2007, the President announced[9] the members of PCAST, which included a broad mix from private and public sectors, with the inclusion of Eric Schmidt (Chairman and CEO of Google) and Craig Mundie (Chief Research and Strategy Officer at Microsoft) attracting most comment. The inclusion of both has been

[8] http://blogs.zdnet.com/BTL/?p=11115
[9] http://www.whitehouse.gov/the_press_office/President-Obama-Announces-Members-of-Science-and-Technology-Advisory-Council/

interpreted as an effort to maintain balance between two of America's most competitive and influential large technology corporations.

CIO

The Federal CIO establishes and oversees the government's IT enterprise architecture to ensure system interoperability and information sharing, as well as maintaining information security and privacy. Vivek Kundra, previously the District of Columbia's Chief Technology Officer, was appointed by President Obama as the first Federal Chief Information Officer, a position that Obama had committed to create during his Presidential campaign.

Kundra has set out a five point plan[10] which encompasses:

1. Open and transparent government.
2. Lowering the cost of government.
3. Cyber-security.
4. Participatory democracy.
5. Innovation.

CTO

Aneesh Chopra, previously the Secretary of Technology for the Commonwealth of Virginia, was appointed to the position of Chief Technology Officer, working with the CIO. President Obama has described his vision for the role:

> *"As Chief Technology Officer, Chopra's job will be to promote technological innovation to help the country meet its goals such as job creation, reducing health care costs, and protecting the homeland. Together with Chief Information Officer Vivek Kundra, their jobs are to make the government more effective, efficient, and transparent.[11]"*

CYBERSECURITY STRATEGY

The problem of protecting the USA's digital infrastructure was given early and high profile attention by President Obama's administration. In February 2009 a rapid 60 day review was started to examine all aspects of the plans, programmes and activities of the USA's cybersecurity efforts. President Obama directed the National Security Council (NSC) and Homeland Security Council to

> *"… conduct a 60-day review of the plans, programs, and activities underway throughout government that address our communications and information infrastructure (i.e., "cyberspace"), in order to develop a strategic framework to*

[10] http://www.govtech.com/gt/653151
[11] http://www.whitehouse.gov/the_press_office/Weekly-Address-President-Obama-Discusses-Efforts-to-Reform-Spending/

ensure that the U.S. government's initiatives in this area are appropriately integrated, resourced, and coordinated."[12]

The review was led by Melissa Hathway, who was appointed as acting senior director for cyberspace and who had previously worked in the Bush administration[13].

In presenting the report, President Obama put the scale of the problem in context by pointing out that cyber crime was estimated to have cost the USA more than $8bn over the previous two years. Worldwide it was estimated that cyber criminals had stolen intellectual property from organisations worth up to $1 trillion[14].

The report sets out a range of findings that President Obama has indicated will be acted upon including the initiation of a cybersecurity office and the development of a comprehensive strategy for cybersecurity which spans both government agencies and the private sector. He also wants to see a better mechanism and structure put into place for responding to cybersecurity incidents when they happen. The programme will be backed-up with more research and development into the issue and a national campaign to drive much higher awareness of cybersecurity issues and their mitigations.

Specifically, the five areas of main focus identified by the report are:

- ***Leading from the Top:*** a strengthening of cybersecurity leadership for the United States through (1) the establishment of a Presidential cybersecurity policy official and supporting structures; (2) reviewing laws and policies; and (3) strengthening cybersecurity leadership and accountability at federal, state, local, and tribal levels.
- ***Building Capacity for a Digital Nation:*** a national dialogue on cybersecurity to increase public awareness of the threats and risks and how to reduce them, including increased education efforts at all levels to ensure a technologically advanced workforce in cybersecurity. It also identifies the need to expand and improve the federal information technology workforce and for the Federal government to facilitate programmes and information sharing on cybersecurity threats, vulnerabilities, and effective practices across all levels of government and industry.

[12] http://www.whitehouse.gov/the_press_office/Cybersecurity-event-fact-sheet-and-expected-attendees/
[13] http://www.forbes.com/feeds/afx/2009/02/09/afx6029719.html
[14] http://news.bbc.co.uk/1/hi/world/americas/8073654.stm

- ***Sharing Responsibility for Cybersecurity:*** sets out the need for improving and expanding partnerships between the Federal government and both the private sector and key US allies.
- ***Creating Effective Information Sharing and Incident Response:*** emphasises that the USA needs a comprehensive framework to facilitate co-ordinated responses by government, the private sector, and allies to a significant cyber incident.
- ***Encouraging Innovation:*** looks at ways for the USA to harness the benefits of innovation to address cybersecurity concerns, including work with the private sector to define performance and security objectives for future infrastructure, linking research and development to infrastructure development and expanding co-ordination of government, industry, and academic research efforts. It also addresses supply chain security and national security and emergency preparedness telecommunications efforts.[15]

Cybersecurity Co-Ordinator

The cybersecurity co-ordinator was announced as part of the package of cybersecurity measures. The role is responsible for orchestrating and integrating all cybersecurity policies for the US government. The co-ordinator is a member of the National Security Council, reporting both to the national security adviser and to the White House's senior economic adviser. The role has direct access to the President on cybersecurity matters *and* sufficient authority to drive the required changes across government agencies.

Open Government Initiative

President Obama issued an Open Government Initiative memorandum in January 2009, committing his administration to "*unprecedented levels of openness in Government*". The memo set out three key principles that would underpin the workings of government:

- ***Transparency*** *– to enable greater accountability, efficiency, and economic opportunity by making government data and operations more open.*
- ***Participation*** *– to create early and effective opportunities to drive greater and more diverse expertise into government decision making.*

[15] http://www.whitehouse.gov/the_press_office/Cybersecurity-event-fact-sheet-and-expected-attendees/

- ***Collaboration*** *– to generate new ideas for solving problems by fostering co-operation across government departments, across levels of government, and with the public.*

The memo tasked the Chief Technology Officer, together with the Office of Management and Budget and the General Services Administration, with creating recommendations for a directive on open government within 120 days. Part of the goal is to "*experiment with mechanisms for effective citizen participation in order to complement the know-how of government employees with the expertise and intelligence of the American people*".

Sites such as http://www.recovery.gov/Pages/home.aspx help deliver on the commitment to transparency through the smart use of IT.

Delivery of the administration's commitment to open source was also demonstrated eloquently in October 2009, when the Whitehouse website site, at http://whitehouse.gov, was moved from a proprietary to an open source platform.

DATA.GOV

Data.gov was set up by the Obama administration to increase public access to computer readable government data. Data.gov:

> *"…increases the ability of the public to easily find, download, and use datasets that are generated and held by the Federal Government. Data.gov provides descriptions of the Federal datasets (metadata), information about how to access the datasets, and tools that leverage government datasets."*

The use of these open Federal datasets will enable organisations to build value-added applications, conduct analyses, and perform research in a more effective way than was possible when government data only existed in documentation form (such as in PDF documents).

FEDERAL IT DASHBOARD

The Federal IT Dashboard (at http://it.usaspending.gov/), provides online details of Federal information technology investments. Users are also able to track the progress of investments over time. The IT Dashboard displays data received from agency reports to the Office of Management and Budget (OMB), including information on over 7,000 Federal IT investments and detailed data for nearly 800 of investments classified as "major." Agency CIOs are responsible for evaluating and updating select data on a monthly basis.

IDENTITY AND AUTHENTICATION

The issue of digital identity is a key component in providing effective online government services. President Obama's memorandum aims to make it easy for individuals to register and participate in government websites without the costly overhead and inconvenience of creating yet more new usernames and passwords. Citizens are also keen to better control how much or how little personal information is shared with the government.

As part of its open government initiative, in September 2009 ten industry leaders (Yahoo!, PayPal, Google, Equifax, AOL, VeriSign, Acxiom, Citi, Privo and Wave Systems) announced their support for the first pilot programmes designed for the American public to engage in open government (being defined as government that is "*transparent, participatory, and collaborative*")[16].

The pilot programmes are being run by several government organisations, including the Center for Information Technology (CIT), the National Institutes of Health (NIH), the U.S. Department of Health and Human Services (HHS), and some other related agencies. In order to participate in the programme, the companies are certified under open trust frameworks based on a collaboration between the OpenID Foundation (OIDF) and the Information Card Foundation (ICF), in line with the federal government's Trust Framework Provider Adoption Process.

The new approach to identification and authentication is aimed at enabling citizens to use online services more effectively and to be able to customise their experience on government websites without revealing any personally identifiable information (including passwords). The approach being taken builds on recent advances in the private sector for protecting online privacy and security, in particular the use of pseudononymous identities where appropriate.

Tackling the online, digital identity issue is an important pre-cursor of delivering more intelligent and interactive online services, rather than the more traditional approach of government using the web largely as a static publishing tool.

Security, privacy, and reliability requirements are documented in the ICAM Trust Framework Adoption Process (TFAP), published on the IDManagement.gov website. The adoption of third party digital identities, using strong privacy and security layers, is an effective way of quickly scaling US government online services in a more personalised and effective way.

[16] http://informationcard.net/blog/open-identity-initiative-2009-09-09

APPS.GOV

In September 2009, Vivek Kundra announced on his blog[17] the new government application store, apps.gov, which provides an online facility for federal agencies to browse and purchase cloud-based IT services, for productivity, collaboration, and efficiency. The intention is that "*rapid access to innovative IT solutions [will enable] agencies [to] spend less time and taxpayer dollars on procedural items and focus more on using technology to achieve their missions*".

FORGE.MIL AND OTHER DEVELOPMENTS

Whilst security considerations can potentially constrain the adoption of a fully open source approach to information systems and their development, the principles can be applied to good effect in non-security critical areas and within the firewall, provided the community is carefully managed. The US Department of Defense (DoD) and the Department of Homeland Security have made great advances in adopting the advantages of community development in reducing the cost of development, promoting re-use and innovation.

Three programmes in particular stand out:

- **CRADA**
  - The Defense Information Systems Agency has established a Co-operative Research and Development Agreement (CRADA) with the Open Source Software Institute (OSSI). The agreement will pave the way for collaboration and partnerships between the federal government, non-profit organizations, academia, and industry to research and develop cutting-edge software for users in DoD, governments at all levels, and the public.
  - The CRADA focuses on release of an open source version of DISA's internally developed Corporate Management Information System. CMIS is a Web-based federal workforce management and administrative software suite with nearly 50 applications and tools to manage human resources, training, security, acquisition and related functions for more than 16,000 DISA users worldwide
- **Forge.mil**
  - Forge.mil is a family of services provided to support the DoD's technology development community. The system currently enables the collaborative development and use of open source and DoD community source software. These initial software development capabilities are growing to support the full system life-cycle and enable continuous collaboration among all stakeholders including developers, testers, certifiers, operators, and users.

[17] http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud/

- **The Open Source Hardening Project**
  - The Open Source Hardening Project is an initiative of the United States Department of Homeland Security, created to improve the security of open source code. As the infrastructure of the internet, financial institutions and many other critical systems in the U.S. run on open source software, the security of these applications is crucial.

Participants in the project were given grants from Homeland Security: Stanford University ($841,276), Coverity ($297,000) and Symantec ($100,000). Stanford and Coverity collaboratively developed Prevent, an automated system for scanning submissions from open source programmers to popular projects. Vulnerabilities found are documented in a database for the development community. Coverity employs a rating system called the "Scan Ladder" to rank projects on a progressive track to security certification. Symantec's role is to test out Scan in the proprietary software that they work with and to provide security expertise.

UK IMPLICATIONS

The UK has followed developments under President Obama and already started to emulate aspects of them in its own programmes. Recent UK initiatives around cybersecurity, open government data and open source have all taken their strategy lead from the USA.

The current UK government has however not extended to encompassing the role of IT as an area for infrastructural investment as part of its recovery programme. Indeed, to the contrary, new technology developments have seen the introduction of new taxes, as recommended by the *Digital Britain* report. It is more traditional industries, such as the car industry and banking, which have been the major recipients of UK state investment. As President Obama's recovery programme makes clear however, there is a case to be made for investment in those areas that will impact the UK's future competitiveness and effectiveness, rather than solely in more traditional areas.

Some specific aspects of the Obama approach to technology that have already been shadowed in the UK, or which need to be revisited by the UK, include the following.

GOVERNANCE

Current governance of IT in the UK is based around loose co-operation between departments and other public sector organisations. This has been formalised in

the CIO Council and the CTO Council, both of which have representatives from across the public sector, although not definitive representation.

In the earliest days of the initial e-Envoy role (which has since transformed into the Cabinet Office HMG CIO position), there was a direct reporting line into the Prime Minister and close co-ordination between the Office of the e-Envoy and the Prime Minister's office. The role has since been de-emphasised, with the central CIO role now several tiers down from the senior levels of the civil service and controlling a small fraction of under 1% of overall public sector IT expenditure.

The centre currently has no real power and little apparent influence with the business owners of Whitehall, such as Permanent Secretaries and Ministers. It often instead focuses on highly technical topics, such as the nature of desktop clients or data centre provision rather than on developing a vision and strategy for cross-government exploitation of technological capabilities in the renewal of the UK's public services. There is a danger of increasing misalignment and marginalisation of IT in public services if work continues to focus on technical solutions without an engagement with the business re-design and delivery of public services and a clear understanding of the capabilities required of IT in delivering against political, rather than technical, imperatives.

Further back in time, in the 1990's, there existed a Central IT Unit (CITU) which developed a range of far-reaching policies, some of which have more recently been picked up and adopted by President Obama's team. However, that unit, whilst at the forefront of vision and strategy, lacked any significant implementation and delivery capability. It should be acknowledged that the unit, and its immediate successor, the Office of the e-Envoy, helped develop some innovative thinking and policies. But they lacked the ability to implement them.

Effective reform of the current model will involve ensuring that policy is not only developed as well as it once was, but that sufficient authority is in place to drive the delivery of those policies across Whitehall. This could include making Permanent Secretaries, and their Boards, accountable to any such new unit, in terms of how well implementation is proceeding, and in ensuring that technology helps become an integral part of Whitehall business plans.

Whatever the precise governance mechanism to be adopted – whether that is to emulate the empowered CIO and CTO model of the US – the future of IT in the public sector will depend upon revising the current model into one that is more effective and better integrated into the business of the public sector.

The UK has no real equivalent of the President's Council of Advisors on Science and Technology (PCAST). While there does exist the community of Chief Scientific Advisors under the Chair of the Government's Chief Scientist, there is no real focus by this group on independent *technology* and *technology policy* advice. There is a clear case for establishing a Chief Technology Advisory group that could help provide relevant inputs during the formulation of policy as well as in ensuring that it is better utilised in the design, delivery and operation of public services. To be effective, as in the US, any such advice would need to have access at the highest levels, working with the Prime Minister's office and government Ministers.

CYBERSECURITY

In July 2009, the Cabinet Office published the first Cyber Security Strategy[18] for the UK alongside the first annual update of the National Security Strategy. Amongst its other recommendations, the Cyber Security Strategy set out the need for two new organisations, both of which are intended to be fully operational by the end of March 2010:

- an Office of Cyber Security (OCS) to provide strategic leadership for and coherence across Government. The OCS will establish and oversee a cross-government programme to address priority areas in pursuit of the UK's strategic cyber security objectives
- a Cyber Security Operations Centre (CSOC) that will bring together existing functions: to actively monitor the health of cyber space and co-ordinate incident response; to enable better understanding of attacks against UK networks and users; and to provide better advice and information about the risks to business and the public[19]

The strategy set out the need for Government, organisations across all sectors, international partners, civil liberties groups and the public to work together to help reduce the risks posed by cyber security issues by improving knowledge, capabilities and decision-making.

The strategy also establishes a cross-government programme to provide additional funding for the development of innovative future technologies to protect UK networks and developing and promote the growth of relevant skills. It identifies a range of areas to be covered including:

[18] http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf
[19] http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

- Safe Secure & Resilient Systems
- Policy, Doctrine, Legal & Regulatory issues
- Awareness & Culture Change
- Skills & Education
- Technical Capabilities & Research and Development
- Exploitation
- International Engagement
- Governance, Roles & Responsibilities

DATA.GOV.UK

The USA's data.gov initiative has been emulated by the Cabinet Office through data.gov.uk and is currently being consulted with interested developers prior to going live. The site claims to have over 1,000 existing data sets, drawn together from 7 departments. This is an important step in helping open up public data in more effective and useful ways than has been possible in the past.

However, the UK still needs to overcome some significant obstacles to making public data truly open, such as the fact that some data is still heavily protected and only available at a fee. One example is Ordnance Survey data, another the use of postcodes. A review of policy is required so that public data like this is made freely available so that innovators can utilise and build upon it, rather than maintaining and protecting taxpayer-funded functions that then try to monopolise public data.

IDENTITY AND AUTHENTICATION

The UK track record in tackling digital identity for online public services started positively, but appears to have stalled for some years. There is a certain irony in the fact that the UK policies developed for trust frameworks have now been taken by the Obama administration to form the basis for their own trust framework. The UK was an innovator in its approach to federated identity and trust frameworks, and indeed in the use of open standards, a leadership position later lost through the focus on the development of a single national identity card. Whilst there has been much debate about the cost of the national identity card programme, the opportunity cost to the UK has been little considered, although it seems increasingly likely that the UK may now need to return to the policies it originally established and which the Whitehouse has shown remain highly relevant.

By 2002, the UK had developed a strong identity verification and trust framework built around the principles of being able to use third party identities and the

delivery of online public services through intermediaries. This work was built on an earlier document, the "*e-Government Authentication Framework*" of 2000. In that earlier document are contained the underlying policies that have recently been adopted by the Obama administration, some nine years later. For example, the 2000 paper includes key principles such as:

> *"For most electronic transactions, government will accept authentication provided by accredited third parties, which will register individuals and organisations and issue them with credentials enabling them to authenticate themselves in subsequent transactions."*

Also:

> *"The Framework provides for those cases where anonymous or psuedonymous access is also acceptable."*

And:

> *"Government will encourage the provision of authentication services by a variety of bodies, including local authorities and the private sector, and will seek to make use of these services wherever possible … The Modernising Government white paper makes clear government's intention to work in partnership with local authorities, the voluntary sector, and with third-party delivery channels such as the Post Office and private sector companies. Where third-party service providers are conducting transactions on government's behalf, they will be required to authenticate the citizens and businesses they deal with to the same standards as government itself would. Government will in turn accept transaction data from those service providers, who will certify that they have carried out the authentication transaction to the agreed standard."*

The leading work in this area was to lay the basis for the implementation of the UK Government Gateway, the UK's online and authentication service. In its original incarnation the Gateway implemented full support for federated identities from third parties, including those issued by the likes of Royal Mail, Barclaycard and the British Chambers of Commerce. However, as those third party credentials were all based on digital certificates, and that market never commercially thrived, within a fairly short space of time the Government Gateway effectively became the default monopoly issuer of userIDs and passwords for use with online government services.

Attempts by the Government Gateway team to encourage the federated identity model through partnerships with banks and others were effectively undermined by the increasing focus on the national ID cards programme and the flawed

concept of a single citizen identity, owned, issued and controlled by the government.

As the recent work in the US has shown, there are more effective and powerful models of online identification and authentication, specifically in the area of online public services. Indeed, this was once well understood in the UK. It is to be hoped that the UK can now refocus on its original ideas, re-import the subsequent refinement of those ideas from the US and enable its online services to be taken to the next level – in a way that after all truly reflects the desire for a citizen-centric approach with appropriate privacy and security safeguards.

App Store

The app store model has been mentioned by the UK central CIO as something the UK will probably look to follow. It is in some senses a larger-scale version of the type of initiative that the Shared Learning Group (SLG) in local government has been trying to achieve over the past 5 or so years – enabling the more effective sharing and re-use of software, and experiences with IT, across the public sector. The concept and vision is again an area in which the UK took an initial lead, but was never able to deliver effectively at scale.

Forge.mil.uk

The US has started to invest in the development of open source software in the military arena. Given that the UK military and intelligence communities spend a large amount of money on software of all kinds, ranging from standard desktop applications through to bespoke safety critical applications, an examination of the potential role of open source software is also likely in the UK.

Like the US DoD, the UK MOD could take advantage of the open source approach to accelerate software development, improve cross project collaboration, software re-use and improve negotiating positions with existing vendors. Whilst the MOD may not be ready to embrace open source as radically as US DoD has, there are a number of potential candidate projects where it might be evaluated more formally, including:

- the development of a forge.mil.uk
- Urgent Operational Requirements
- Defence Equipment & Support MIS
- Records Management
- Royal Navy deployed applications

Broader Learnings

Historically there has been no lack of ambition to improve the UK's public services through the more effective use of IT. The e-government policy papers of the last Conservative administration and the policies of the subsequent Blair government after the Labour victory of 1997 set out aspirations to improve public services through the use of technology that remain as relevant today as they were at the time.

The Modernising Government report of 1999[20] for example set out three aims:

- *Ensuring that policy making is more joined up and strategic*
- *Making sure that public service users, not providers, are the focus, by matching services more closely to people's lives*
- *Delivering public services that are high quality and efficient*

It is unlikely that anyone would argue with such aims. But between the vision and the reality fell the shadow. In terms of IT, the report specifically mentioned the ambition to:

- *develop an IT strategy for Government which will establish cross-government co-ordination machinery and frameworks on such issues as use of digital signatures and smart cards, websites and call centres*
- *benchmark progress against targets for electronic services*

And in particular one of the five key commitments was to:

- ***Information age government:** we will use new technology to meet the needs of citizens and business, and not trail behind technological developments*

These aspirations were later backed up by a much more detailed set of plans around IT specifically.

However these worthy aspirations have largely remained unfulfilled. Despite a clear focus on needing to address successful delivery as much as vision:

- Within Whitehall [*there will be*] **a new focus on delivery –** asking every Permanent Secretary to ensure that their Department has the capacity to drive through achievement of the key government targets and to take a personal responsibility for ensuring that this happens. Bringing **more**

[20] http://archive.cabinetoffice.gov.uk/moderngov/download/modgov.pdf

people in from outside and bringing able, younger people up the ladder more quickly

It is of course early days for the Obama administration. It is possible that they too will find themselves unable to deliver the ambitious vision they have set for themselves. However, there remains a fundamental underlying question that the UK must address if it is to make more headway in the future and not merely repeat its previous failures. Why, specifically, does the UK often have the right ideas but lack the ability to implement them? Whilst the USA is able to take the best ideas from elsewhere (including the UK, as this Memo has indicated) and work out how to innovate around *and* apparently deliver them too.

There is little in the former Conservative and Blair vision documents to fault, except perhaps a tendency to focus too much on tactical technologies of the time ("*smartcards*" for example) rather than the underlying technology *policies* and *principles*. This reinforces the point that technology strategy needs to be about the provision of *services* and *capabilities*, not technology for its own sake. It would not be unrealistic to take some of these earlier documents, revise them to make them more strategic in the use of technology policy and then republish them in largely the same form with a current or future Prime Minister's image airbrushed in place of the then incumbent.

What remains lacking however is a clear mechanism both for reviewing the original aspirations to make them more cohesive and, more significantly, a clear mechanism to ensure they are effectively *delivered* this time around rather than remaining as historically interesting insights into the aspirations of a particular political party leadership at a particular moment in time.

RECOMMENDATIONS

Based on the overview set out in this Memo, the CTPR recommends several changes to the way that technology policy is considered by the various political parties ahead of, and following, the next general election. These include:

- The UK should develop a clear, consistent vision for the role of technology in the updating and renewal of the UK's public services. This needs to be driven by public service needs, with technology policy focused on provision of the services and capabilities required, not technology for its own sake.
- The UK needs to put into place effective *implementation* and *delivery* mechanisms for its technology strategy. Reform of the current governance model needs to ensure not only the development of *policy* but also that sufficient authority is in place to ensure the *delivery* of those policies across Whitehall. This could include making Permanent Secretaries, and their Boards, directly accountable in terms of how well implementation is proceeding, and in ensuring that technology helps become an integral part of Whitehall business plans. This is likely to require an empowered, central CIO and CTO function/office with genuine authority drawn directly from the Prime Minister, Cabinet and Treasury
- The UK should consider establishing a Chief Technology Advisory group that can provide relevant expertise during the formulation of public policy as well as in ensuring that technology is better utilised in the design, delivery and operation of public services. To be effective, as in the US, any such advisory group would need to have access at the highest levels, working with the Prime Minister's office and government Ministers
- The UK should develop a twenty-first century identity strategy. It should refocus on its original ideas, re-import relevant developments from the US and enable its online services to be taken to the next level – in a way that truly reflects the desire for a citizen-centric approach with appropriate privacy and security safeguards. The UK was once an innovative world leader in its approach to topics such as identity and trust, a lead later lost through the focus on the development of a single state-owned national identity card.
- The main political parties need to ensure they have well researched plans for IT, learning from Obama and others, to ensure they not only have the right vision for the use of technology in the modernisation of the UK's public services, but also a clear set of changes they will implement

instantly on taking office – across the interlocking jigsaw pieces of governance, architecture and procurement. Without this, in another 13 years time we may well still be in the position of reviewing the public sector approach to IT and commenting "Nice idea, shame it was never delivered."

About the Centre for Technology Policy Research

The Centre for Technology Policy Research (CTPR) is an independent, non-partisan organisation that aims to ensure that IT is better understood across public, private and voluntary sector boundaries in order to provide mutually beneficial outcomes. We hope to help avoid the toxic outcomes often associated with ill-designed projects and programmes. We help to make this happen by improving the evidence base, dialogue and links between private, public and voluntary sectors and academia.

We do this by:

- remaining independent of any market interests
- using open source market intelligence to provide insightful reports and analysis
- providing rigorously independent and objective insight, analysis and guidance into the best applications of IT in public, private and voluntary sectors
- informing public understanding of the intersection of information technology and public policy through reports, and private and public interactions
- improving the opportunities for engagement for SMEs in UK public sector programmes

Technology is everywhere around us, but rarely planned for effectively at a policymaking level due to a lack of understanding of its impacts during the formulation of public policy. One of the aims of the CTPR is to help raise the level of understanding of information technology and technology policy as a lever of policymaking, rather than as purely an administrative and operational tool

The CTPR's website can be found at http://ctpr.org.

Every care is taken to use primary, verified open sources of information in the compilation of these Memos but CTPR Ltd makes no warranties, express or implied, in this publication.

CTPR MEMO NUMBER 2: NOVEMBER 2009. THE OBAMA EFFECT: THE US IT REVOLUTION AND THE UK

The Centre for Technology Policy Research (CTPR Ltd) is a limited liability company number 6992015 registered in England & Wales. The registered office is 788-790 Finchley Road, London NW11 7TJ, United Kingdom.