Science and Technology Committee

House of Commons London SW1P 3JA
Tel 020 7219 3580 Fax 020 7219 3796
http://www.parliament.uk/science

From Andrew Miller MP, Chair

Rt Hon Francis Maude MP
Minister for the Cabinet Office & Paymaster General
House of Commons
London
SW1A 0AA

9 July 2013

Thank you for giving evidence to the Science and Technology Select Committee on 17 June 2013. The session, and its predecessor where we took evidence from a range of expert witnesses, gave us the opportunity to explore the early stages of the Digital by Default strategy. We will be publishing the oral and written evidence we received in addition to this correspondence.

The Committee intends to continue scrutinising the Government's work as services go online under the Digital by Default strategy and may consider a full inquiry in the future. Before the first exemplar digital services go live, we request that the Government responds to the following points.

1. ***Cost***

   During the evidence session, you stated that the Government finds it hard to know with certainty what savings have been made from moving transactions online, partly because data in Government is "not good". This is surprising because a key justification of the strategy is savings to the taxpayer. It is not evident to the Committee that the Government has a handle on measuring these savings. We welcome your message that savings are being made but urge the Government to be clearer about the detail of both savings being made as services become Digital by Default, as well as the costs of designing, or redesigning, the services.

2. ***Security***

   The Committee heard from Dr. Martyn Thomas, Vice-President of the Royal Academy of Engineering and Chair of the IT Policy Panel of the Institution of Engineering and Technology, that the Government does not keep up with privacy-enhancing technologies and uses "old, unpatched and non-updated software" (see attached extract from the transcript). We are concerned that inadequacies in Government software may lead to security vulnerabilities. The Committee would like to know whether the Government is

confident that software developed meets the highest engineering standards.

Dr. Martyn also suggested that the Government could be importing the security vulnerabilities of authorised ID assurance providers into their online services. The Committee is concerned that sensitive personally identifiable data could be compromised and be the subject of unauthorised use.

You told the Committee that the Government has an obligation to protect people's data sensibly and effectively. It appears that the public are unable to ascertain whether online Government services are developed adequately to withstand cyber attacks. The Committee suggests that the Government should be clearer with the public about this.

3. ***Awareness and uptake***

The Committee considers it important that all Government online services cater for citizens with basic functional literacy, following the example of GOV.UK.

The Committee queries your assertion that if the Government can get 20% of the population to transact online, it can achieve 80% participation. The Committee would like the evidence behind this figure to be brought to our attention.

There appears to be low public awareness of the Digital by Default strategy. You suggested "word of mouth and a good user experience" is the best way to promote the strategy. Has the Government evaluated the effectiveness of these public awareness techniques?

4. ***ID assurance***

The Committee welcomes the draft identity assurance principles published on 17 June 2013. The evidence we received suggests that the principles are satisfactory. The Committee strongly supports principles 5 and 8 which state that the citizen can choose when to update his or her records and also the appointment of an independent arbiter who can resolve complaints or problems. The Committee considers these principles vital in increasing and maintaining public trust when transacting with online Government services.

The Committee suggests a ninth principle stating that if a dispute arises concerning a citizen's online dataset, that the citizen should be initially presumed correct and that the citizen has the right to instant correction if a mistake has been made.

5. Data accuracy and public confidence

You undertook to reflect on my observations about the default position being that citizen's version of their data be regarded as correct. I would be happy to discuss this further with you as I have some clear ideas as to how we can move this forward.

We would be grateful if you could respond to these key points by October 2013. In addition, we wish to be kept informed about any further developments in Digital by Default strategy.

Yours sincerely,

Andrew Miller
Chair

HOUSE OF COMMONS

ORAL EVIDENCE

TAKEN BEFORE THE

SCIENCE AND TECHNOLOGY COMMITTEE

DIGITAL BY DEFAULT

WEDNESDAY 5 JUNE 2013

DR MARTYN THOMAS CBE, FREng, WILLIAM HEATH and KEVIN SELLER

TONY NEATE and CLIVE RICHARDSON

Evidence heard in Public Questions 1 - 69

Q4 Chair: You say "if it is done properly" and "it depends on how it is done". What evidence is there that digital by default will work? In other words, is there the competence to deliver the answer to your caveats "if it is done properly" and so on?

Dr Thomas: There are services that have been working for some time digitally such as, for example, renewing vehicle excise duty online, which seems to work very effectively. Therefore, there is some evidence that it can work effectively. There is also clear evidence that, if it is not done competently, it will not work effectively. For example, if you were to attempt to apply online for disability living allowance, you would immediately meet a page that said you must not be using a Macintosh, UNIX, any of the up-to-date versions of Internet Explorer, Windows Vista, or any of the other modern browsers like Chrome or Firefox; in other words, if you want to apply online for disability living allowance, you have to use old, unpatched and non-updated software that is full of security vulnerabilities. There is a counter-example.

Q5 Chair: Mr Heath, you and I have spoken before about things that have gone wrong in the moves towards digital delivery. Since public services started appearing online about 13 years ago, have the Government improved their understanding of the use of the internet and kept abreast of technological advances, or are there still weaknesses in the system?

William Heath: Both things are true: it has improved and there are still weaknesses. There are definite examples of good practice. The whole move towards open data, transparency, making available structured data, and the power of information agenda, which started under the last Administration and continued under this one, is very powerful and strong. For me, the big missing ingredient is a similar agenda about personal information. The power of information and open data is about stats, numbers, money, organisational structures and legislation. What is not yet on the right track, but there is progress, is understanding the real role and power of personal information and data. The idea of personal control over personal data is an idea whose time has come; it is not just a liberty, human rights, Lib Dem idea; it was in the Labour and Conservative manifestos. There is broad agreement and support for the notion that personal control over personal data is a big step forward, and we are now at the stage of working out just how that should happen.

Kevin Seller: As to "if it is done properly", William makes a good point. There are still at least 7 million people who are not online, and it is estimated that about 16 million probably could not complete a complex online journey. I think that is where the Post Office comes in. We have always been about universal access to service. Traditionally, we have always been about access to Government services. Even today, we still carry out a number of Government services. Typically, if customers have something from Government and don't know where else to go, they come to us. I would see that happening both as people start to move online and in the online world. We still get people coming to our website to find out about passports, car tax and so on, so we are associated with Government journeys, and in the future we have a big responsibility to make sure that for those who are not online the Post Office is there to help them and get them through that experience.

Dr Thomas: Things are getting better slowly, but the Government still have a lot to learn about the real science that underpins the dependable development of software. The Government do not appear to understand how easy it is to de-anonymise supposedly anonymous data, for example. Consequently, they keep announcing policies that are clearly going to become unravelled as a result because it will be possible to—

Q6 Chair: Can you give an example?

Dr Thomas: I give the example of the release of medical records. The general principle is that, if the information started off as personally identifiable data and post-anonymisation it still contains enough information to be of any use to anybody, by matching it against other existing datasets you can find out who the people are. That has been demonstrated time and time again. Therefore, the notion of useful anonymised personal data is an oxymoron. The idea of releasing personal data about citizens in the country ought to be off the agenda. I do not believe that the Government have kept up with the advances in privacy-enhancing technologies and different ways of doing identification and the strengths and weaknesses. In particular, from a technology point of view, there is a constant assumption that you can get stuff good enough by testing it and if, for some reason, there are faults in software it means you have not tested it enough, when heroic amounts of testing won't give you a high degree of confidence that things are correct or have the properties you expect.

Q23 Stephen Mosley: Your answers were very full, and a lot of them were, "If the Government do this, this is what they should do." The Government have produced good practice guides that they are asking potential suppliers to comply with. Have you had an opportunity to look at those good practice guides, and are they what you would describe as good practice?

William Heath: Do you mean the identity and privacy principles?

Stephen Mosley: Yes.

William Heath: We think the identity and privacy principles are excellent. They are currently in draft. We believe they are moving from draft to a published form; we would welcome that and are very happy to be held to that standard.

Dr Thomas: The good practice guides are good in what they actually say, but as an ordinary user of the service you cannot tell whether somebody has implemented a system according to the good practice guide, so it leaves you with a degree of uncertainty. I very much doubt that the identity providers will be willing to carry any liability if it turns out that they have security vulnerabilities in the ID verification that they are providing, simply because that liability could be extremely large if they had to notify all the users and compensate them for any damage caused by unauthorised release of their personal data as a consequence of those security vulnerabilities. It is not clear that, in the implementation, you will end up with something that is strong enough. From the point of view of the Government service, you end up importing all the security vulnerabilities of all the people you allow to become authenticated as identity providers. For each individual, it is only the ones they have chosen to use that put them at risk, but for the service, if any of them is compromised, it will damage the reputation of that service.

Kevin Seller: They are in draft, as William says. Our initial view is that they look okay to us, but the key to this is how it will impact on the customer. In the Post Office we are always trying to make sure we focus on the customer impact and how the customer feels when they have to go through this experience.