CONSULTATION RESPONSE

Open Data Consultation
Transparency Team
Efficiency and Reform Group
Cabinet Office
1 Horse Guards Road
London SW1A 2HQ

DATE: - 2 November 2011
TO: - Transparency Team
RESPONSE BY: Georgina Nelson, Lawyer: Information
Rebecca Owen-Evans, Policy Adviser

Making Open Data Real

Introduction

Which? is a consumer champion. We work to make things better for consumers. Our advice helps them make informed decisions. Our campaigns make people's lives fairer, simpler and safer. Our services and products put consumers' needs first to bring them better value. We are an independent, not-for-profit consumer organisation with over 700,000 members - the largest consumer organisation in Europe. Independent of Government and industry, we are funded through the sale of Which? consumer magazines, online services and books.

Which? has over 50 years of experience in providing expert information and advice for all consumers and we will do all we can to help people make informed choices in key public services. We are pleased to comment on the proposals in the *Making Open Data Real* consultation. As a champion of choice, we broadly welcome the steps being taken by Government to open up public services.

We believe that Open Data has the potential to help raise the standard of public services, provide information to help users make the right choices for them and increase accountability.

Whilst there are differences between sectors that should be borne in mind, there are four key principles that should be considered across the board to make the open public services agenda a success:

Standards - Firstly, there must be an extent to which everyone should have access to a certain level of quality, regardless of whether they can, or want to, exercise choice. We need to be sure that we differentiate between factors that are non-negotiable and factors that are legitimate sources of diversity and choice.

Reality and Nature of Choice - Secondly, where there is diversity, we need to make sure that choice is a reality and that people are genuinely equipped to engage with it. For example, choice is less meaningful for many parents because geography limits the schools they can choose from. At the same time in health, many consumers do not want to choose or can feel that they don't have the ability to make effective choices.

Information and Enabling Choice – The release of data is a necessary, yet not sufficient condition, for achieving the objectives of the Open Data philosophy. Whilst supportive of transparency and openness, we have made the point in other markets that information by itself is rarely useful. Indeed, information wrongly used can actually make people's lives more difficult rather than easier. The key to making information powerful is to ensure that people are given the right information, at the right time in the right ways.

Protection and Redress - Finally, if services are to be opened up to new providers and to choice then people must be protected when things go wrong. This means that consumers need to have effective mechanisms, such as redress schemes, for dealing with their concerns and with failings in provisions. It also means empowering consumer representatives with the necessary tools to intervene on behalf of consumers.

As an experienced provider of information and advice, we consider that Government must embrace some key principles in order for the strategy to achieve its potential. We discuss some of these here, and would be pleased to engage further on this topic.

Transparency and accountability

Which? strongly supports the concept of an open and transparent government, and we believe that delivering Open Data can play a key role in ensuring that providers of public services are accountable to their users. It is just and fair that this data collected on behalf of the public in the provision of public services is made available to those users. We believe that this data, if provided and used correctly, can lead to more informed choices, improve public service standards and catalyse innovative tools to achieve these goals.

However, information on its own will not be enough. There will be a need for trusted third parties to aggregate and contextualise the information provided to ensure that it is genuinely useful. In our view, the presumptions of a 'right to data' and a 'presumption of publication' are

sensible and helpful. We will challenge institutions to release relevant data and we will do what we can to hold them to account where this does not happen. In this capacity, we are strongly supportive of the proposed 'right of challenge' against decisions not to publish data to an independent body.

A 'right to data'

There may be limitations to the information that members of the public or their representatives can currently access. So that all providers are equally accountable in the future, those companies using public money to provide public services should be covered by the Freedom of Information Act (FOIA).

We would be concerned about any proposals to weaken FOIA, as we believe that it will remain an essential tool to acquire specific information that could remain 'hidden' in a large dataset, or require the kind of highly specialised analysis which may be out of reach of an individual user.

A market for data

In providing a true market for data, it will be important to ensure that everyone involved in the process acts responsibly and in the public interest. Having multiple providers of the same information could be problematic if they provide conflicting advice, especially given the difficulty that many of us have in deciphering statistics. We know in health, for example, that people are keen for one provider that they can trust.[1] Data providers must demonstrate that they are unbiased, objective and credible. The role of an accreditation scheme, recognising adherence to minimum standards in this space should be explored.

Privacy

Privacy is a key concern for service users. While we understand that the intention of Open Data is that no personal data will be made available to a third party, we are aware of the fragility of certain anonymisation methods. An article in The Telegraph (4th February 2011) detailed the publication of a data set by the NHS where patients names and addresses were replaced with date of birth and postcode. Such levels of anonymisation are not sufficient, and we support the recommendations of Dr Kieron O'Hara as developed in 'A Report on Privacy and Transparency for the Cabinet Office'.

Our own research has highlighted that consumers have concerns about the uses of their personal data online - they feel they are losing control as to what purposes it is put to and to whom it is

[1] Which? research on information and choice in health, September 2010

passed [i]. When asked to think about the safety of their personal information in general, 42 per cent of consumers responded that they were most concerned about 'personal data being passed to unknown companies without my permission.'(the most popular response). As consumers will not consent to their data being made public via Open Data, it is critical that their information does not become 'personal data' by de-anonymsation methods as by the very nature of the open licence, it will be passed to unknown companies and this consumer fear will be realised.

If the public fail to trust public services providers to look after their information, it could have an adverse affect on their interaction with that public service, and with Government more generally. This is highlighted in recent research by Fair Warning:

- 54% have or would withhold information from clinicians if a hospital had a poor reputation for security;
- 38% have or would put off seeking treatment if a hospital had a poor reputation for security;
- 37 % would travel 30 miles or more to avoid being treated at a hospital they didn't trust, just so they could keep their sensitive information confidential.[ii]

Under the current Data Protection legislation framework, if one is to suffer a data breach at the hands of a data controller, the available routes for redress are taking that organisation to court and then proving quantifiable financial loss. This is not a likely route for a user of public services to take, considering the time and cost implications, and the improbable likelihood of being able to show financial loss.

If there is a risk of consumers being identified, then this would be a data breach - and we would like to see far easier, quicker and cheaper redress solutions (such as class actions, ombudsman schemes or mediation routes) or compensation mechanisms for individuals. There is also the question as to who would be answerable to the victim in such a scenario. Would the government accept liability for failing to anonymise sufficiently? This is particularly relevant considering there is likely to be no audit trail of those individuals or companies who access the data via data.gov.

Data Reliability

Related to the concerns of re-anonymsiation, is that of data accuracy. In our own research we found that 19% of those individuals who had requested to see a copy of their personal data held by a company (a subject access request) had found it to be inaccurate.[iii] To be useful, data has to be reliable - and if there is a belief by government that it isn't, then there should be a warning sign to accompany the data set when uploaded. We believe there should be a

framework of how to get the best value out of data, this could be links between data sets and metadata, explaining where the data came from, its quality and how it can be used. This additional information could accompany each data set when uploaded onto data.gov.

For further information, please do not hesitate to contact:

---

[i] 69% consumers are increasingly worried about the safety of their personal information held about them by organisations Which?, Data Breaches, 2562 GB respondents, July 2010,

[ii] Fair Warning, 'How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes', Nationwide survey of 1,000 respondents ,October 2011. Available at: http://www.fairwarningaudit.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf

[iii] Which? 'Money Omnibus 20: Data Breaches', March 2011