BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Better Use of Data - Big Brother Watch Response

April 2016

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group that was founded in 2009. We have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Specific to this inquiry we have produced research into breaches of data protection in local government, police forces and the NHS. We have also submitted written evidence on the threats to personal data to the Science and Technology Select Committee and the care.data programme to the Health Select Committee as well as giving oral evidence on the subject to a number of committees.

Big Brother Watch participated in the Open Policy Making process that preceded these proposals.

Response:

Big Brother Watch has profound concerns with the consultation document. Answering the specific questions posed is difficult until the broader issues are resolved. We therefore have chosen to address these broad concerns at this stage.

The consultation states in paragraph 13 that "*A complex patchwork of data sharing laws has grown over time*." It goes on to say that "*we need to go further and update the legal regime to provide simple and flexible legal gateways to improve public sector access to information*." However, we believe that the broad range of proposals outlined in the consultation document will not fulfil that brief and indeed, will, without careful consideration, extend the "complex patchwork" even further.

Whilst data sharing is presented as a benefit or a solution, many of the benefits given as examples in the document could be achieved through organisational restructuring and improved communications between departments, rather than installing a complex web of data sharing powers.

Definitions

Our overarching concern is that there is no definition of what is meant by "*data sharing*", what is meant by "*public data*" or what is meant by "*private data*".

It is unclear if data sharing means for information to be copied from one system to another, or if it will be held in one system and be made available to people requesting access. It is also unclear that if it is held in a database whether the entire database would be available or just certain parts of it. These are basic questions of which there appears to be no answer.

For every explanation of the problem in the document, no solid solution is given. A hotchpotch of ideas has been published. They all sound very interesting but rarely if ever detail what the proposed solution will be, how it will work and what the technical capability will be required to ensure its smooth running.

It may have been more beneficial to have published one clearly defined idea with the intention of developing it further before endorsing it as a blueprint for data sharing as a whole across government departments.

Data Protections, risk analysis and security provisions

The UK is on the brink of becoming digital by default. Over the next 20 years all citizens will be required to have a digital profile. Data protections, privacy protections, data control and informed consent will all become fundamental to ensure the smooth working of a digital data driven society. However the consultation document gives no indication that those future necessities have been adequately considered. The concepts of privacy and security by design appear to have been added as a tick box exercise under the key protective principles, rather than as a beneficial philosophy that underpins the process in a meaningful way.

The document does acknowledge some concern in this area but it does not provide a coherent outline of a solution. For example the *Risks of Data Sharing* section acknowledges that sharing personal information can potentially be dangerous but there is no detailed analysis of the risks or plans to ensure they don't become realities. The perceived benefits of having a digital birth certificate for ease of claiming benefits is also outlined, but again there is no attempt to explain how this data would be protected from hacking, loss, breach or the myriad of other cybercrime concerns. We are instructed that digital certification will help reduce fraud but there is no acknowledgement that storing this information could also present dangers to personal information. It could be argued that without clear definitions and without a clear approach to how all individuals; the public, the official, the researcher etc., will identify themselves, the risk of fraud or identity theft is potentially enormous.

The lack of specific detail on security arrangements to protect the personal data during acquisition, retention and during transit for sharing purposes is also a very serious omission. Detailed information outlining proposals for encryption and whether or not systems of access controls and user authentication will be put in place would have been instructive.

We welcome the references to key protective principles, Trusted Third Party models and privacy impact assessments but note that these are mentioned or suggested as possible privacy/security methods rather than clearly adopted or described as a basic structure to the proposed powers.

Strategy

It is unclear why a single implementation framework hasn't been suggested instead of the wide range of different approaches found in the document. This risks adding an unnecessary layer of complication to the scheme.

Of all the proposals outlined, those for fraud and debt appear to be the most coherent in terms of strategy. As a starting point the proposal for a pilot phase to ascertain what benefits could be established or indeed gained is sensible. It is also sensible for any permanent scheme to only be implemented after the results of the pilot phase have been analysed, and for an open, public review to take place.

These ideas are a good start, but frankly we would have hoped that two years on from the creation of the OPM these ideas would have been adopted more widely and would have been used as a backbone of privacy and security by design across all proposals in the scheme.

Data awareness

Increasingly, due to greater engagement with new data driven and connected technologies, people will begin to acknowledge and care about who holds their data, for what reason and for how long. The introduction of the General Data Protection Regulations (GDPR) will emphasise that controls on data will have to become more explicit. It is likely that what is outlined in paragraph 8 of the Government's Technology Code of Practice, that "*Users should have access to, and control over, their own personal data*" will be the method for all data access in the future.

The GDPR will make it necessary for all citizens to be told exactly what is happening at the point of collection as well as in the future, with their personal information. This includes who will subsequently have access to it and who it may be shared with, additionally the need for explicit informed consent to be given will be emphasised.

It should never be assumed that if a citizen gives permission for data to be used for one purpose that they give carte blanche for it to be used for <u>any</u> other purpose, even if the purposes stem from the same department which they have provided the data to.

An example of what can happen if proposals for data sharing are not properly communicated beforehand is the well-publicised failure of the care.data programme.

NHS England's awareness campaign was widely criticised as ineffective and a key piece of information; precisely who the medical records of citizens would be shared with was not made clear to the public. As a result of this the scheme was put on hold.

If the Government wants to avoid similar issues it must be upfront and clear with citizens about the need for certain information and what it will be used for.

It should be remembered that the burden of proving need for data will be with the Government, not the individual.

Codes of Practice

We are informed that two Codes of Practice will be drafted, one to cover the proposals on research and statistics and the other "*to cover the other provisions*". However these have not been published.

It is worrying that such important and fundamental elements such as "*principles for the use of the power*" and "*additional safeguards*" are not outlined in anyway in the consultation document.

Furthermore that they are to be buried in a yet to be written and published Code of Practice rather than on the face of any future legislation is of great concern.

The consultation promises that transparency will be "*a key principle that will apply to each of the Codes*". This is undermined by the fact that neither has been published as part of the consultation.

Future legislation

Based on what has been presented in the consultation document we have serious doubts that the proposals are even close to being drafted as future legislation.

We would recommend at the very minimum, a more considered approach. An approach which outlines definitions, gives clarity of the purpose, provides a clear structure as to how the scheme would work technically and outlines how security of data, privacy of data and individual control of data will be achieved.

Ultimately if the problems which the scheme intends to solve, can be solved without the need for data acquisition, retention and sharing, we would recommend that effort is put into addressing those methods rather than seeing promises of big data sharing as the only solution.