BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

The Digital Economy Bill Part 5 Digital Government
Big Brother Watch 2nd Reading Briefing - September 2016

Introduction

In advance of 2nd Reading of the Digital Economy Bill this briefing outlines concerns relating to Part 5 of the Bill.

Part 5 of the Bill intends to change the nature of data sharing across Government. However it fails to provide any clarity as to why this needs to be done, how it will be achieved or what safeguards will be put in place to ensure the security and privacy of citizen's personal information.

The Bill was published on the 5th July 2016 together with explanatory notes and factsheets, but we are still awaiting publication of the promised codes of practice and the technical explanation behind the Bill. We draw your attention to this as without these further publications it is almost impossible to determine and subsequently debate, exactly what Part 5 of the Bill will do, how it will work and what safeguards will be put in place.

The publication of this legislation followed a Cabinet Office consultation on better use of data in Government. The consultation met with a great deal of concern about definitions and intentions from a broad spectrum of data protection experts including most notably the Information Commissioners Office. Much of the concern stems from the failure to define what is "data" and what is "data sharing".

Value of data

Data is often described as the "new oil" and public data has proven itself to be enormously beneficial in society. But alongside public data, individuals have all begun to generate huge amounts of private data. In fact we are all becoming digital by default and our personal data is now a critical element of who we are, in a way people have never fully experienced before.

The intelligent use of data can create beneficial outcomes for society, but it is important that before we adopt any new data sharing policy, consideration to the risks as well as the benefits of accessing and using data are addressed.

Unfortunately there is often a lack of differentiation made between what constitutes public and personal data.

For data sharing to benefit society, but also for individuals to have control and protection over their data, there needs to be clarity about what the distinction between these two very different types of data is. Without that distinction and without due consideration to it, our inherent right to privacy which we all had before the digitisation of data is likely to become obsolete.

Data protection law is leading the way in exploring these issues. The law is changing in order to ensure that data can be used safely and securely, that society can benefit from greater access and analysis of data, and that the rights of the citizen to protection of their personal data and awareness of how their data will be used is not considered as an afterthought, but is determined from the start.

Data protection

Our data is currently protected by the Data Protection Act 1998 (DPA). The Act will be replaced by the General Data Protection Regulations (GDPR) in May 2018.

The GDPR will place far greater emphasis on informed consent from individuals to what, how and why their data is being requested, used and potentially shared. It will place new and very necessary restrictions on how data is handled, used, shared and what rules must be adhered to should their data be misused, breached, hacked or subject to cyber-crime.

These regulations will be critical in ensuring that as we move further into a data driven society, protection for all data, whether personal or public, will be built into our everyday lives.

We draw your attention to these changes as they will have an impact on the proposals outlined in Part 5 of the Bill. In fact it is very unclear why Part 5 is required at all given that the GDPR will be the legal arbiter of what is, and is not, permissible when planning to access or share data in the future.

Overview of the Bill

Part 5 is broken down into 7 chapters.

Chapter 1: Public Service Delivery

Outlines ways the sharing of data might be able to improve public service delivery. The legislation refers to the sharing of data with

1. Gas and electricity suppliers
2. Revenue and Customs

The supplementary factsheet provides "examples" of schemes which the Government would use data sharing to support but these are not outlined on the face of the Bill.

1. Troubled families programme
2. TV re-tuning assistance
3. Fuel poverty

Chapter 2: Civil Registration

A fundamental change to how civil registration documents, birth, death, marriage, civil partnership certificates will be handled by amending the existing Registration Service Act 1953.
Civil registration officials will now be able to disclose any information they hold to another registration official, or to a "specified public authority".

Chapter 3: Debt Owed to the Public Sector

A permissive gateway will be created to enable data to be more easily shared for the purposes of tracking down who is in debt to a person or to the Crown.
According to the Explanatory Notes, this will enable:

- Identifying and collecting debt
- Bringing civil proceedings
- Taking administrative action as a result of the debt

According to the factsheet

- Data sharing will "help the government to make informed decisions about a customer's individual circumstances and their ability to pay."

This Chapter deals with debt across the public sector so we think it fair to assume that the legislation will involve and impact HMRC. With this in mind it is worth noting clause 41 subsection(3) and clause 43 subsection(2) both of which exclude HMRC from any of the restrictions or guidance to when data can and cannot be shared.

It is made clear that any information disclosed to HMRC "may be used" "for purposes other than those for which it was disclosed with the consent of the Commissioners for HMRC (which may be general or specific)."

Chapter 4: Fraud against the Public Sector
A permissive gateway will be created to enable data to be shared to enable action to be taken in addressing fraud against public sector bodies.

Personal information will be accessed, shared and used to:

- Prevent fraud
- Detect fraud
- Investigate fraud
- Prosecute fraud
- Bring civil proceedings as a result of fraud
- Take administrative action as a result of fraud

Chapter 5: Sharing for Research Purposes
Public authorities will be able to share any information they hold, including personal information for the purpose of research in the public interest.

Chapter 6: Her Majesty's Revenue and Customs
Permits HMRC to share "non-identifiable" data if it is in the "public interest".

Chapter 7: Statistics
Permits any public authority, including HMRC, to share data with the Statistics Board (UK Statistics Authority), if the information is required for one or more of the Board's functions.

Concerns with the Bill

Transparency
The factsheet published alongside the Bill says DCMS are going to *"create a robust, clear and transparent framework….for sharing information with specified public authorities for clearly defined purposes."* Unfortunately the Bill doesn't outline what that framework is or what the *"clearly defined purposes are".*

The Bill refers to a *"specified person"* working in or for a public authority who may disclose information for the *"purpose of a specified objective".* This is an exceptionally broad definition: it potentially enables data to be shared with anyone if they can be determined to be *"specified"*. The specified persons are not named on the face of the Bill but are only listed in Annex B of the Explanatory Notes. We are told they will be determined by regulation. Transparency about who will be accessing, retaining and sharing data is far from clear.

No detail is provided regarding the safeguards that will be in place for data sharing.

People are mostly comfortable with data sharing when the social purpose is made clear and when strong safeguards are in place. The Bill alludes to strong safeguards but offers no real detail as to what they will be. Without detail about exactly how their personal data will be protected how are the public to trust the public sector with their data?

We only learn of changes to civil registration documents in the Explanatory Notes. No detail about the digitisation of these documents is outlined on the face of the Bill.

Definitions
Personal information is not clearly defined in the Bill. It is not clear if data will be personal data or non-identifiable personal data. In fact there is confusion as to when data is considered personal or not.

Clause 31, subsection 4 is particularly confusing. It offers a definition which says personal information is anything which *"relates to and identifies a particular person"* but then offers an exception to that definition which appears to indicate that any information given to a gas and electricity supplier can be shared and is therefore not defined as personal information – if that is the case then information such as your name, address, bank details and energy usage can be shared according to this legislation. However this information is defined by the DPA as "personal information" so Part 5 would appear to be in direct conflict with the DPA, despite claims that it clearly adheres to it

We are told data cannot be shared if permission has not been given, but there is no indication as to what data will be shared or how citizens will be asked for consent for their personal data to be shared more widely.

The term "well being" is referred to in the Bill as an "objective" for why data should be shared, particularly in relation to public service delivery. The term "well being" was heavily criticised by the Supreme Court in its ruling on the Scottish Parliament's Named Person Scheme. It was determined that "well being" does not match the high bar set by the Data Protection Act which says data use must be "vital".

No definition of "public interest" is given.

With regard to sharing data for research purposes in the public interest far greater detail is required. We raise concern about this as we are conscious that without clear definition personal identifiable data could be shared for spurious reasons. For example we are aware that the Office for National Statistics previously proposed using sensitive data for non-essential statistical research as outlined in the Big Data Project 2015[1]. This project proposed taking people's names to determine their ethnic origin, intentions to use private smart meter data to determine when a house is unoccupied and using location data from mobile phones to inform on population behaviour.

[1] Office for National Statistics, *The ONS Big Data Project:*
http://www.ons.gov.uk/aboutus/whatwedo/programmesandprojects/theonsbigdataproject

Broad safeguards:
The Bill and the supporting document fail to outline:

- Where data will be held, if new data systems will need to be built and if so who will be responsible for their creation, oversight and review.
- What security will be applied to the systems to ensure that the systems are protected from cyber-crime, cyber-theft, hacking, misuse, or malware.
- Whether Government or private companies will hold the data
- How long data will be held for
- How data will be destroyed, or if indeed data will be destroyed

No mention of encryption is made in the Bill or in the supporting documents despite the fact that encryption is a necessity for protecting and maintaining security of data.

Anonymisation is not referred to anywhere in the Bill or in the supporting documents. We are simply told that *"if the information identifies a particular person"* it will be *"processed"* so that *"the person's identity is not specified in the information, and it is not reasonably likely that the person's identity will be deduced"* either from the information itself or if it is combined with other information.
No information as to how this will be achieved is provided. Furthermore "reasonably likely" offers no reassurance that sensitive personal information will not be revealed.

Safeguards regarding Civil Registration documents
It is claimed that digitising Civil Registration documents will reduce fraud. How this will be achieved is not defined. No explanation is given as to how either the individual who the certificate refers to or the specified person sharing or receiving the registration data will have to prove they are who they say they are. The risk of digital fraud is therefore a concern. Removing paper fraud and in turn increasing the risk of digital fraud is nonsensical.

Government wants Civil Registration documents to be shared in bulk when there is a *"clear and compelling need"*. That need is not defined in the Bill or in the associated documents. The only example given is the bulk sharing of birth data – in this case birth certificates – to *"help parents access early years services"*. How this will be done is not explained or defined. Why this is deemed to be "clear or compelling" is also not outlined. Our view is that the risks associated with sharing personal information in bulk outweigh any potential improvements to service delivery.

Profiling
Under the imminent GDPR, data must not be used to monitor the behaviour of people in a way which could be seen as profiling. However the accompanying factsheet on the Bill says *"the state will share identified data on property characteristics to flag identified persons"* who are entitled to assistance with their energy bills. We are concerned that using data to flag or identify people is quite simply profiling people and that Part 5 will therefore be in conflict with the GDPR.

The Troubled Families Programme as outlined in the explanatory notes of the Bill rather than on the face of the Bill, appears to have similarities with the aforementioned Named Person Scheme in that sensitive personal data will be shared across departments and organisations in order to *"identify families in need".*

It should be noted that the Supreme Court found that the data sharing element of the Named Person Scheme would breach the right to privacy and family life as defined by Article 8 of the Human Rights Act 1998 (HRA), and would lower the standards required by Principle 1 of the DPA.

As data must not be shared if it contravenes the DPA and Part 1 of the Regulation of Investigatory Powers Act 2000 (which is also set to change under the Investigatory Powers Bill by the end of 2016) the legislation will be out of date before it becomes law.

Regarding Chapter 3 "Debt owed to the Public Sector", the intention to allow data sharing to enable Government to make informed decisions about a customer's individual circumstances and their ability to pay needs to be explained. It is not clear what this process will involve. Nor is it clear whether a citizen will be asked directly about their ability to pay or whether an assessment will be made based on shared data that the citizen has no awareness of let alone has provided consent for?

Codes of practice
The codes of practice were not published alongside the Bill nor have they been published ahead of 2nd reading.

Without the codes of practice much of the workings of the Bill are unclear and many questions are unanswered.

Why the promised codes of practice will only be for those who disclose the information not those who receive it will also need to be answered.

Rights of the citizen
No information has been published outlining consent, choice or even how basic information regarding the new data sharing model will be explained to the general public. This will breach the requirements in the GDPR.

No detail is given as to whether citizens will be asked for their informed and implicit consent before their or their child's registration document is shared? Again this will breach the GDPR.

Health and medical data
There is no specific reference to whether health and medical data is to be included or excluded. As many questions remain over data sharing within the NHS particularly in light of the now defunct care.data scheme and the ongoing attempts to resolve the big questions, clarity on whether the NHS will be involved in this new legislation is critical.

Conclusion

We are deeply concerned by the profound lack of detail in Part 5.

We are also dismayed that Members of Parliament are being asked to debate this part of the Bill with very basic and in many cases vague information.

The failure of the Government to publish the codes of practice or technical information relevant to Part 5 makes the job of understanding the intention of these proposals, let alone scrutinising them, impossible. The Bill is effectively incomplete without this information and should not have been placed before Parliament let alone have reached 2nd Reading without all the detail being provided.

We strongly call for Parliament to halt the progress of the Bill until Part 5 is removed.

Data sharing is a critical and necessary part of all of our futures, to present legislation which is cobbled together, lacks clarity and fails to provide any detail let's down the departments wishing for reassurance and guidance about how data can and should be shared lawfully and safely, but also fails the citizens of the United Kingdom.

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group founded in 2009. We produce unique research which exposes the erosion of civil liberties in the UK, looks at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

We were part of the Cabinet Office's open policy making process.
We also submitted to the "Better Use of Data in Government" consultation (our submission can be found here https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/09/Big-Brother-Watch-Response-to-Better-Use-of-Data-April-2016.pdf) The concerns we outlined in that document and which we made during the open policy making process have been raised in this briefing and remain relevant to the current legislation.