Big Brother Watch Written Evidence – Digital Economy Bill Part 5

October 2016

Introduction

- The intention behind Part 5 of the Digital Economy Bill; to improve data sharing across Government, is something we support. A well established and well defined data sharing scheme for Government is essential not just for Government to function in a data driven society, but in order to enable better public services, benefit the vulnerable and needy in society and help with research and statistics; it will be a critical part of every citizen's engagement with the State. Unfortunately Part 5 in its current form, we believe, will fail to establish a clear, well defined, efficient, principled and legal data sharing process.

- This submission will outline what we believe are the broad problems with the Bill as currently written. Rather than suggest amendments to the Bill, we request that Part 5 be removed from the Bill as a whole, to enable a coherent, properly defined, legally compliant piece of legislation to be drafted which will have the safeguards and longevity needed in this absolutely critical area.

- Data sharing will be one of the most important functions in a completely connected society; it should therefore be done properly. We fear that Part 5 will merely build a temporary solution which will fail to solve the profound problems, some of which have been highlighted by the National Audit Office and the Cabinet Office in recent weeks.

- Big Brother Watch were part of the Open Policy Making process which preceded the Bill. We are also members of the Privacy and Consumer Advisory Group (PCAG).

Concerns regarding definitions, transparency, safeguards and future data protection regulations:

- The Better Public Services factsheet published alongside the Bill says that Government are going to *"create a robust, clear and transparent framework with appropriate safeguards including a Code of Practice for sharing information with specified public authorities for clearly defined purposes".* Based on what has been laid before Parliament we do not believe this assertion to be supported.

- The Bill fails to define what information will be shared. No definition of data sharing is given.

- Part 5 indicates that the intention is to hand over or replicate data between departments. This approach is fast becoming outdated.

- Data sharing based on the old paper model of handing over all data rather than

relevant data is something which the Government Digital Service (GDS) has been actively working to move away from.

- The GOV.UK Verify Scheme (Verify) has been working for the past 5 or so years to establish a model of attribute exchange sharing, based on the Government not centrally storing data and ensuring that there is no "*unnecessary sharing of information*". Verify adheres to strong privacy principles and is based on the premise of asking the citizen for limited access to their data in order for a secure reusable identity verification process to be established.

- There is no mention of Verify in the Bill or in the supporting documents. We think this is cause for concern as it shows a lack of communication with experts working in Government on data sharing.

- No definition of the difference between personal and public data is given, indeed there appears to be general confusion as to what data will be considered personal or not. Clause 31(4) for example defines personal information as anything which *"relates to and identifies a particular person"* but offers an exception 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 names, addresses, bank details and energy usage can be shared under this legislation, data which under the Data Protection Act 1998 (DPA) is defined as *"personal information".*

- The phrase *"benefit"* as outlined in Clause 29 is not defined. This was a point of concern raised in the Chamber during 2nd Reading by Desmond Swayne MP. He asked *"is the purpose of Part 5 to claim rights of ownership over all data? The definition of benefit in clause 29 is so broad that I cannot think of a piece of information that would elude it. Can the Secretary of State name a piece of information that falls without that clause?"* no answer was given.

- Throughout Part 5 reference is made 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, potentially enabling data to be shared with anyone if they can be determined to be "*specified*".

- *"Specified persons"* are not named on the face of the Bill but are only listed in Annex B of the explanatory notes. It is far from clear who will be accessing, retaining and sharing data. The Bill therefore falls short of its very laudable aim to be clear and transparent.

- The Bill and its supporting documents fail to define any safeguards. The lack of detailed information, either on the face of the Bill or in any of the published supporting documents is of profound concern. We believe that the safeguards should have been defined prior to publication of the Bill and then written into the legislation on the face of it. We acknowledge that the Bill refers to codes of practice where the Government may intend for safeguards to be defined, but as they have not, to date, been published, the safeguards remain undefined and unavailable for scrutiny.

- No reference to permission, let alone informed consent from the citizen for the sharing of data is made in the Bill. Yet this is a critical element of the forthcoming changes to data protection. The General Data Protection Regulations (GDPR) will require citizens to be asked for their "*freely given, specific, informed and unambiguous*" consent before any personal data can be processed. In addition they must be able to withdraw their consent at any time and be informed if the purpose with which their data was given is to change. Part 5 fails to establish any of these points.

- There is no indication as to how long personal information will be held for once it has been acquired. It is not clear if the intention is for data to be held indefinitely by all departments. If this is not the case then further detail must be provided.

- No detail is given detailing where data will be stored or if data will ever be destroyed. If new data systems will be required in order to hold or destroy data, who will be responsible for their creation, oversight and review? If the intention is for data to be held in the cloud this needs to be made clear, particularly in relation to the profound and increasing concerns about data security, cybercrime, hacking, theft, loss and misuse.

- Additionally no information has been provided outlining what mechanisms departments will adhere to in order to maintain the protection of data. This is of concern in light of the recent National Audit Office (NAO) report "Protecting information across government" which revealed that *"The centre of government has few mechanisms for understanding whether the procedures departments are putting in place to assure their information are adequate….this will become increasingly challenging as more information is shared across government, as the protecting information arrangements of the weakest organisations could expose other departments."*

- The same report revealed a wealth of problems with how government departments consider, protect and handle data. In particular it reports that in March 2016 after an internal review the Cabinet Office found that '*the government's existing security structures and roles will not adequately support the next phases of cyber security, workplace and digital strategies.'* The NAO report states that this is *"an assessment which the evidence of our work supports."*

- In light of this, the lack of any reference to cybersecurity in the Bill is of serious concern. No reference to encryption is made in the Bill or in the supporting documents despite the fact that encryption, whilst controversial, is seen as a necessity for protecting and maintaining security of data.

- Anonymisation is not referred to anywhere in the Bill or in the supporting documents. The closest the Bill comes is the vague assurance that "*if the information identifies a particular person"* it will be *"processed"* so 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 is provided to show how this will

be achieved. Furthermore *"reasonably likely"* offers no substantial reassurance that sensitive personal information will not be revealed.

- The intention for the Bill to establish *"permissive gateways"* is welcome. We acknowledge that regulation can make the data sharing process complex and tiresome, however we don't support the establishment of any permissive gateway where the necessary and vital safeguards are not in place.

- The intention of the Bill to establish a new criminal offence for the unlawful disclosure of data, Clause 33(5), is the one clear safeguard provided. This is something we have long campaigned for and we welcome the Government's determination to see this through.

- The Bill refers to adhering to the current Data Protection Act 1998 (DPA) and the Regulation of Investigatory Powers Act 2000 (RIPA). Both pieces of law are soon to expire. RIPA will mostly be replaced by the Investigatory Powers Bill (IP Bill) by the end of this year and the DPA will be replaced with the GDPR by the end of May 2018.

- Part 5 fails to show how the legislation will adhere to the GDPR. There are many areas where we fear the legislation won't abide by to the GDPR, for example the GDPR states that processing of data should only happen if there is no alternative way. Whilst the intention expressed during the OPM process was that data sharing was not to be the only solution, the legislation doesn't seem to have maintained that view and appears to be establishing processing of data as the norm rather than the exception. The failure to address the work of Verify is a key example of this.

Concerns regarding Chapter 1: Public Service Delivery

- The detail regarding the broad intentions for data sharing and public service delivery is only made clear on the accompanying factsheets where it is outlined that *"the state will share identified data on property characteristics to flag identified persons"* who are entitled to assistance with their energy bills.

- Using this definition, we have concerns that the Bill's intention to use data sharing as a means of flagging people based on their behaviour such as energy usage or financial situation runs the risk of falling foul of the new data protection regulations. Regulations which will prohibit the use of data to monitor the behaviour of people in a way which could be seen as profiling.

- The *"objective"* in the Bill for the sharing of data in relation to public service delivery is defined as being for the *"well-being"* of citizens and in order to *"improve"* public service delivery. The term *"well-being"* was heavily criticised by the Supreme Court in its ruling on the Scottish Parliament's controversial Named Person Scheme earlier this year. It was determined that *"well-being"* does not match the high bar set by the DPA which says data use must be *"vital".*

- The process of data sharing in the Named Person Scheme was deemed to 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.

- We draw your attention to this ruling as although it is not stated on the face of the Bill the supporting factsheet indicates further uses for personal data under Chapter 1, including sharing data to enable the retuning of televisions or in order to assist the Troubled Families Programme.

- Our concern is that if sensitive personal data will be shared across departments with the objective of *"well being"* in order to *"identify families in need"* the legislation may find itself falling foul of the law in the same way as the Named Person Scheme.

Concerns regarding Chapter 2: Civil Registration

- Changes to civil registration documents are only referenced in the Bill's explanatory notes. No detail about the digitisation of these documents is outlined on the face of the Bill.

- Clause 38 outlines the process of disclosure. There is no mention of consent from the citizen. We are concerned that the decision to disclose information solely resides with an official which will breach the GDPR.

- There is no mention of how individuals, either those sharing the data or those receiving it, will be asked to verify who they are in order to ensure that each party is dealing with a trusted and authorised individual. We see this as a fundamental flaw because rather than reducing fraud and identity theft this approach could in fact increase it.

- The little we know about the purpose behind Chapter 2 comes from the Better Use of Data in Government consultation. The documents behind the consultation stated that digitising civil registration documents will *"enable public authorities to fulfil their functions"* (functions are not defined), would *"reduce the demands placed on citizens to provide hard copy certificates"* and will reduce fraud by *"protecting the public against identity theft by sharing information electronically."*

- The Better Public Services factsheet accompanying the Bill outlines the intention for Civil Registration documents to be shared in bulk when there is a *"clear and compelling need"*.
  The clear and compelling need is not defined anywhere. The example given in the Better Use of Data in Government consultation of sharing birth certificates in order to *"help parents access early years' services"* is frankly far from compelling. Furthermore "*clear and compelling"* is a much lower threshold than "*necessary and proportionate*" which is recommended by the DPA and in the IP Bill when referring to the acquisition, retention and sharing of bulk data.

- The concerns raised during the OPM process about these new powers outlined a fear that a citizen database would be established. This was a key concern during the contentious ID Card debate. The "Better Use of Data in Government" consultation stated that this won't be the case, because *"systems of civil registration in Scotland and Northern Ireland are separate and different…..so in many instances there is not*

a complete set of registered life events that could be linked." We are not convinced that this response addresses the concern that centralised databases will not be created.

- The creation of any database with citizen data which can be linked by a permissive gateway must be approached with caution. The recent Office of Personnel Management data breach in the USA, which exposed the personal information of millions of US Government workers, should be considered as a warning that centralised databases of personal information are a honeypot for criminals, hackers and large scale data errors.

Concerns regarding Chapter 3: Debt Owed to the Public Sector and Chapter 4: Fraud Against the Public Sector.

- During the OPM it was agreed that more robust evidence would be presented on the areas of fraud, error and debt. This was agreed in order to establish the scale of what problems, if any, existed, and what value might come from using data sharing to solve them. That evidence was not presented to the OPM.

Concerns regarding Chapter 5: Sharing for Research Purposes.

- Far greater detail is required about the sharing of data for research purposes which are in the public interest. No definition of "*public interest*" is given.

- Without definition or detail outlining the circumstances in which data could be shared, the legislation makes the sharing of personal identifiable data for spurious reasons a possibility. This concern is not fanciful. The Office of National Statistics Big Data Project 2015 proposed using sensitive data for non-essential statistical research, such as taking people's names to determine their ethnic origin. We would argue that use of personal data for such purposes is far from essential and in that instance could have been used to profile people.

Critical points from the National Audit Office "Protecting information across government" report.

- We draw the Committee's attention to the NAO's "Protecting information across government" report which outlines in detail the current failings of the data sharing infrastructure within government.

- We acknowledge that Part 5 may be seen as a solution to many of these problems. However the concerns outlined in this submission, when read alongside the problems outlined in the report, reveal that the proposed legislation will do little to solve the inherent flaws of attempting to share data.

- Key findings of the report:
    - Between 2014 and 2015 the 17 largest government departments recorded 8,995 data breaches. Most of which were not reported to the ICO simply because they are currently not required to, this is likely to change under the GDPR.

- The department with the largest number of breaches was the Department of Health. However this figure appears to be based on the fact that they are the only department which insists on the reporting breaches. It is no wonder that this was found to be the case as not only is health data considered to be of particular sensitivity, but the disaster which was the care.data scheme revealed to many within the department that the need to take data seriously is of profound importance. We have been led to understand that the long term intention of the legislation may involve the sharing of health and medical data between departments. Whilst this has not been publicly stated we are led to believe from direct conversations with the team behind the legislation that there is a desire for this to be the case in due course.

- The Cabinet Office "*does not provide a single set of governance standards or departments to follow, and does not collate or act upon identified weaknesses."*

- *"Central governance of security, which includes overseeing the protection of information is unclear."*

Conclusion

- Big Brother Watch welcomes the intention behind Part 5 but whilst the intention is good the execution has been poor.

- At present Part 5 doesn't properly tackle any of the problems which need to be overcome in order to allow data sharing to take place effectively and securely. Not only does it stray from current data protection law, it would be completely incompatible with incoming regulations.

- If we are all to be digital by default the engagement we will have with our data is going to change. It is short sighted of government not to put the citizen at the heart of this process. Data protection law is moving towards giving more control of data to the citizen and government policy should mirror this approach. This would have the advantage of enabling strong, secure and citizen focused data sharing principles to be established for the long term. It would also allow citizens, staff, departments, authorities and government to have clarity of purpose and security of method.

- The oblique nature of the drafting of the legislation makes the codes of practice critical. That the Bill was laid before Parliament without them (and at the time of writing they have still not been published) is of profound concern, particularly as we know no agreement was reached on safeguards during the OPM process. The failure to publish the necessary documents and provide detail of the vital safeguards makes the job of scrutinising the intention of the legislation impossible.

- In light of these concerns we believe the Committee should recommend the removal of Part 5 rather than attempting to amend it. By doing this the remainder of the Bill can progress whilst focused work can take place to establish a new Bill

solely outlining data sharing. This will enable legislation to be drafted which is absolutely clear on definitions, clear on method, clear on safeguards, places the citizen at the heart of the approach and is legally compliant with current and future data protection laws.

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 participated in the Open Policy Making process which preceded the publication of the Bill. We are also a member of the Privacy and Consumer Advisory Group (PCAG) which advises the government on how to provide users with a simple, trusted and secure means of accessing public services. Part of the work we have been involved in in relation to PCAG is the Verify scheme.

We are responding to this consultation in a professional and public capacity.