BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

THE DIGITAL ECONOMY BILL – PART 5
A few problems which need to be addressed

Government's poor history on data sharing and data security:

- Part 5 of the Bill will lead to greater data sharing across Government, despite a recent National Audit Office report[1] revealing that almost 9,000 data breaches across government departments occurred in 2014/15, only 14 were reported.
- The same report also revealed that the Cabinet Office conducted an internal review of data sharing across government which revealed that 'government's existing security structures and roles will not adequately support the next phases of our cyber security, workplace and digital strategies'.
- The strategy in Part 5 of the Bill is to improve the "wellbeing" of all in society with emphasis on helping the most vulnerable. Over the weekend it was revealed that due to DWP failing to inform HMRC an estimated 28,000 families with children who qualify for disability living allowance missed out on additional tax credit[2]. This one example alone shows that ill-considered and poorly executed data sharing often makes the vulnerable even more so.
- It was determined by the Supreme Court[3] earlier in the year that sharing personal information for the benefit of "wellbeing" failed to meet the high bar set by the Data Protection Act which says data use must be "vital".
- The Bill also intends that any personal information we share with government can then be shared with a broad range of other public bodies and private companies (gas and electricity firms initially) - citizens will not have any choice in whether their data is shared, accessed or used. They won't know when someone is looking or using their data and they won't have any say or opportunity to amend their data if there is an error.
- This sounds fine until you consider the recent HMRC issue with Concentrix[4] who had their contract with HMRC cancelled early due to withdrawing tax credits from hundreds of people who they wrongly determined were guilty of fraud and error of the tax credits system. Access to those people's personal information led to serious errors and data misuse.
- With these few examples taken from a much larger pot it is not at all clear how government departments will cope with the changes of proposed of increasing data sharing gateways which Part 5 of the Bill will enable.

Civil Registration Documents:

- Part 5 of the Bill will enable a fundamental change to how civil registration documents, birth, death, marriage, civil partnership will be handled by amending the existing Registration Service Act 1953.
- The documents will be digitised with a copy held by civil registration officials who will be able to disclose any information they hold to another registration official, or to a "specified public authority" either on an individual basis or in bulk.
- 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 to *"help parents access early years*

[1] https://www.nao.org.uk/wp-content/uploads/2016/09/Protecting-information-across-government.pdf
[2] https://www.theguardian.com/uk-news/2016/nov/25/tax-credit-error-costs-families-with-disabled-children-4400-a-year
[3] https://www.supremecourt.uk/cases/docs/uksc-2015-0216-judgment.pdf
[4] https://www.taxation.co.uk/Articles/2016/09/20/335376/concentrix-loses-tax-credit-checking-contract-hmrc

services". How this will be done is not explained or defined. Why this is deemed to be "clear or compelling" is also not outlined.

- Bulk sharing of data as we know from the Investigatory Powers Bill means a large data set (often centralised) which holds the personal information of tens, hundreds, thousands or even millions of people can establish a insecure honeypot of information.
- None of us will be told or even asked our permission for this data to be shared. We will often have no idea that a council official for example has requested the information.

Control of data – informed consent:

- Increasingly the method of data minimisation i.e., only accessing, using or requesting the minimum data required in order to prove identity or finalise an application. This is a security principal that ensures unnecessary data isn't shared as sharing of data whether we like it or not can leave data vulnerable.
- The proposals in Part 5 are the opposite to data minimisation.
- An individual's ability to control their personal information will cease as soon as it is acquired by government or by a council official. Under this Bill a Government Minister will decide how our data is shared, with whom and for what purpose.
- Under the General Data Protection Regulation (GDPR) which Government have confirmed the UK will implement by May 2018, an individual must give their informed consent when handing over access to their data.
- If the use of their data changes once it has been handed over, further consent must be sought. This Bill in its current form will not adhere to the GDPR.

Data Breach and notification:

- We will not be notified if our data is breached - This is a requirement of the GDPR.
- This Bill will fail to adhere to the GDPR

Codes of Practice:

- The Codes of Practice accompanying the Bill were not published at 2nd reading, it is unlikely that any Member of Parliament, other than those on the Public Bill Committee, will have read or even seen the codes, despite the codes allegedly being the key resource for how the proposals in the Bill will work.
- The Codes of Practice are still in draft form, with many blank spaces. This is not acceptable. It is clear, particularly in the area of civil registration that there is no coherent process behind the proposals.
- The Bill only requires those who will be sharing our data to have "regard to" the codes of practice.

Anonymisation and data security:

- 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.