Submission on Part 5 of the Digital Economy Bill: "Digital Government"

Dr Jerry Fishenden FIET CITP FBCS FRSA
Co-Chair, Cabinet Office Privacy and Consumer Advisory Group (PCAG). 5th October 2016.

Summary

The desire to make better use of data in order to improve public services for citizens and businesses is important. The use of technology offers the potential to empower and better assist some of the most disadvantaged in society, as well as improving the daily experience of public services for UK citizens and businesses alike.

Empowering citizens to have access to and control over their own personal data and how it is used will also help improve data quality: citizens will be able to see, correct and maintain their own records. Data needs to work for people and society: citizens need to be actively engaged in how their data is secured, accessed and used.

As the Information Commissioner's Office has commented:

> "*It is important that any provisions that may increase data sharing inspire confidence in those who will be affected. Our research shows that the public are concerned about who their data is shared with and reflect concerns that they have lost control over how their information is used. Even apparently well-meaning sharing of data such as GP patient records for research purposes can arouse strong opinions.*"[1]

The theme of trust is one that the BCS, the Chartered Institute for IT, also highlights:

> *"We need to change our approach to data, so that individuals have trust and control, and organisations have the freedom to integrate and use data safely."*[2]

Whilst there are welcome aspects of Part 5 of the Digital Economy Bill, such as making data breaches a criminal offence, its provisions also reduce current controls on data protection and security in order to facilitate what it refers to as "data sharing" – although the Bill contains no definition of this term. When it talks of "disclosing" personal data to gas and electricity suppliers for example (Para 30, p.29) it contains no details of what personal information might be disclosed or how. There is none of the legal or technical detail essential to ensure data security, the ethical use of data, and the necessary trust framework essential to protect the rights, privacy and security of citizens.

Part 5 seems to imply an approach to "data sharing" modelled on the era of filing cabinets and photocopiers when – quite literally – the only way to make data available to others was to send them a duplicate physical copy. Modern technology has already rendered the need for such literal "data sharing" obsolete: data can now be used without copying it to others and without compromising security and privacy.

In an increasingly digital economy, expanding the number of people and organisations with access to citizens' personal data – much of it sensitive, such as details of disabilities, relationships, income, welfare status and health – is likely to increase the risk of fraud, not reduce it. Such threats are at least as likely from insiders as from outside[3]. At the same time that the government is rightly investing heavily in cyber security, including the creation of the new National Cyber Security Centre (NCSC), Part 5 appears to weaken existing data protection and security controls. Doing so would also place it at odds with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA), which presumably take legal precedence over this Bill.

Part 5 does not make clear how proposals to "data share" comply with the government policy of citizens' data being under their own control (as set out for example in paragraph 3 of the UK

Government Technology Code of Practice[4]). Instead, it appears to weaken citizens' control over their personal data in order for public bodies and other organisations to "share" their data around. It thus appears out of step with the focus on user needs and better designed public services being undertaken by the Government Digital Service.

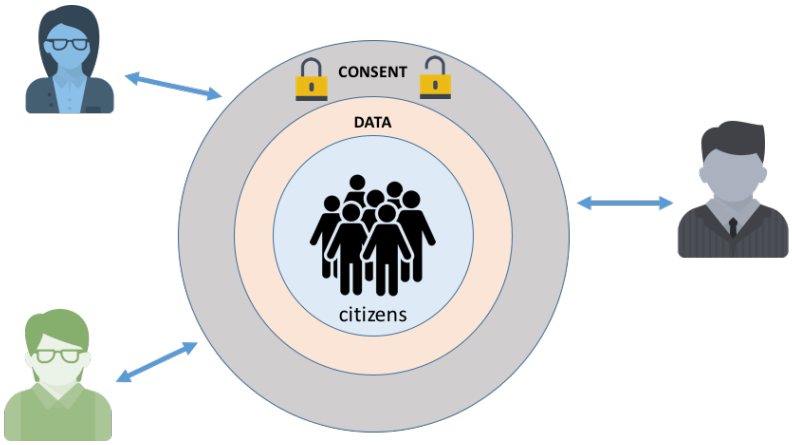

Figure 1: the current model – citizen consent is required to use their personal data, such consent usually being given when signing up to a specific service for a specific purpose. Citizen control over their own personal data is at the centre of the GDPR and DPA.

Weakening controls on the protection of their data is likely to undermine trust in government and make citizens less willing to share their personal data, challenging the move towards digital government – and also eroding the data insights needed to better inform policymaking and related statistical analyses. This is the type of organisation-centred, rather than citizen-centred, approach that characterised the failure of the top-down imposition of Care.data in the NHS[5].

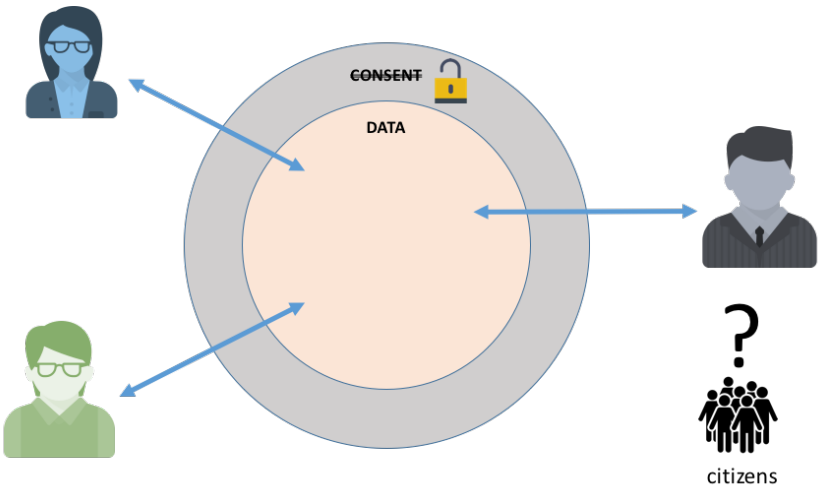

Figure 2: Part 5 of the Digital Economy Bill proposes letting organisations share and access data without the citizens' consent or involvement, moving away from the established model that places the citizen, their consent and their data, at the centre.

The recent National Audit Office (NAO) report "Protecting information across government"[6] has revealed the prevalence of weak controls on the protection and management of personal information in government. Any continuation of the existing poor information management identified by the NAO, or the further weakening of cyber security and data protection implied by Part 5, is likely to create negative economic and social impacts.

This is an important time to be strengthening cyber security and the minimisation and protection of data, especially since the UK is world leading in terms of the proportion of its GDP dependent upon

the digital economy[7]. Part 5 also only considers the role of individuals and organisations and overlooks entirely the growth in the so-called Internet of Things[8] – the increasing number of devices and sensors around us (and physically on us in the form of wearable devices), transmitting, receiving and analysing a wealth of personal data. This presents a significant shift in the nature and growth of data, yet Part 5 makes no provisions for how the IoT will be incorporated securely within its proposals for "Digital Government", despite its relevance and importance for the future of better public services.

Conclusion

It is important that modern technology is used well to improve our public services, to reduce cybercrime and fraud, and to enable better-informed policymaking through access to more accurate and timely data – particularly to assist the most vulnerable in society. It is also essential that citizens can have trust in the system, and that their data will not be misused or abused.

The government policy of letting citizens have access to and control over their own personal data is contradicted by Part 5. It's unlikely that it will produce the policy outcomes intended and could well cause unintended outcomes, including a loss of citizen trust in government's use of personal data, and potentially the loss and/or disclosure of citizens' sensitive personal information.

There are already effective and secure ways of enabling government to make better use of data – from improving the design of public services to technical measures to protect personal data – whilst still enabling such data to inform decision-making. Part 5 appears out of touch with the state of current digital practice. This is in part because it relies upon the well-meaning but poorly executed consultation that preceded it over the prior two years. It's notable that the consultation itself concluded that

> *"There remain some areas, particularly around safeguards that will need to be in place where data is to be shared, where further and wider consultation is required, as consensus could not be achieved. Government would wish to consult further on the full range of policy proposals before deciding which to take forward and in what exact form."*[9]

This "further and wider consultation" has not yet taken place and is reflected in the shortcomings of Part 5.

It is worth making time to get this right – the NHS Care.data programme set back patient-led innovation because it was not patient-led but imposed without consent and largely without patients' knowledge. It's essential that the same mistake is not made by rushing through into law a form of "data sharing" that seeks to implement a similar model across the public sector on a much larger scale.

The absence of any Codes of Practice makes the nature of the "data sharing" proposed and the safeguards outlined in the Bill impossible to assess. If Part 5 is required – for example, to put into law provisions such as making data breaches a criminal offence – it will need to be substantially revised to be significantly more precise, putting into law the legal and technical detail currently absent.

Additional analysis

This section provides additional detail behind the summary provided in the first three pages of this submission. It concludes with a few recommendations.

Context

Cybercrime is on the rise[10]. Citizens are increasingly the victims of fraud and much fraud is attributable to insiders gaining unauthorised or privileged access to information[11]. The larger the pool of people able to access and use personal data, the greater the risk and hence the more likely it is to be compromised and misused.

Moving to "Digital Government" requires the implementation of best practice in designing systems and services around citizens' needs, and the way in which best practice cyber security protection is established around those systems – and in particular personal data within those systems.

Analysis

Part 5 of the Digital Economy Bill makes inadequate distinction between public (open) and private (personal) data. Yet this is an essential distinction, with public and private data requiring very different security and accountability mechanisms. It reflects the shortcomings in the prior consultation exercise[12], which similarly lacked a clear distinction, and which saw the independent quality assurance group and the government's own Privacy and Consumer Advisory Group (PCAG)[13] side-lined due to an apparent rush to include the data sharing recommendations within the Digital Economy Bill – with a civil servant involved commenting in an email that "this next part of the process is not as open as we have strived to be"[14].

Public / Open Data

In terms of using data to facilitate improved search and statistics to inform better decision-making, there is inadequate distinction between public and private data.

Part 5 provides no specific detail on the process of de-identifying personal data nor any reference to the known problems of achieving this successfully, although the earlier consultation stated that:

> "*Key criteria of the de-identification process (such as the removal of the identity information before it is supplied) will be set out in primary legislation and sets out that any new procedure can only be made by regulation if it adheres to those criteria.*" ("Better Use of Data – Consultation Paper", p.30[15])

Part 5 of the Bill contains no such criteria. Processes of de-identification will need to be about more than just removing personal identifiable information before disclosure however, also placing an obligation on the data owner to ensure no re-identification can be made using the data released in combination with other data. This is a much more complex issue than focusing on a single data set released in isolation and requires co-ordination and risk assessment across and between data sets.

As the Open Data Institute (ODI) has observed, "*open data remains frustratingly siloed*"[16]. Part 5 is opaque about the specifics of how this situation will be improved. Where genuinely public or open data, rather than a citizen's private data, is concerned such data should be automatically published, or (better) made directly accessible on the Internet via open system interfaces (more formally, application programming interfaces, or APIs). This requirement should be made obligatory for all publicly financed systems and contracts. Such interfaces would help provide a public good – an open resource for innovation for the wider UK economy. There should be no additional cost in doing this: the same interface can serve the Office for National Statistics (ONS) for example alongside everyone else.

However, Part 5 makes no specific reference to the approach to be used for open data, despite considerable work by the ODI and others in this area. It is also unclear whether legislation is required at all to stipulate requirements for the open technical standards, availability and transparency to be used across the public sector for ensuring consistent access to open data.

Private / Personal Data

Part 5 is built around a mechanism termed "data sharing" (elsewhere referenced as "disclosure") to achieve its purpose. Yet "data sharing" is not defined, legally or technically, within the Bill.

Does "data sharing" mean data duplication / copying / distribution, or data access, or alternatives such as attribute exchange / claim confirmation? These are all quite different things with their own distinct risk profiles. In the absence of any definition, or the Codes of Practice, the term is ambiguous at best, and potentially damaging – in terms of citizen trust, cyber security and data protection.

For example, there is a significant difference, and security risk, associated with: distributing (copying) personal information to third parties; granting them controlled and audited one-time access for the purpose of a specific transaction; or simply confirming e.g. "this person is in debt" or "not eligible for benefit X" without revealing any of their detailed personal data.

Part 5 appears to be based around out-dated concepts from the time of filing cabinets and photocopiers. As the simplified schematic below shows, it proposes that citizens' personal data is opened up and used by other people and organisations without the citizens' consent.

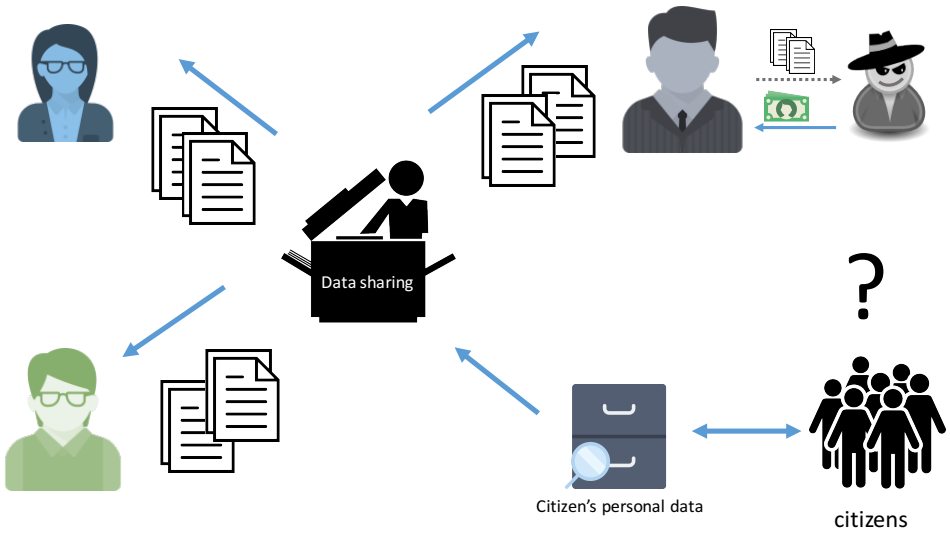

Figure 3: Part 5 of the Digital Economy Bill proposes an out-dated and insecure model of "data sharing"

Part 5 makes little mention of security or privacy nor how such "data sharing" will comply with the obligations of informed consent and the ability to revoke that consent. There is no explanation for example of how it will be possible for a citizen to revoke consent if data has been copied and passed onto third parties, particularly if this was done without their knowledge. Once digital data is no longer under the control of its original owner it will be difficult to know who has a copy and equally difficult for a citizen to revoke consent to access and use such data now held by third parties.

Part 5 also seems to assume that the utilisation of personal data is limited solely to people and organisations and ignores entirely the fact that an increasing amount of personal data is generated, stored, analysed and acted upon by devices and sensors – the so-called Internet of Things. Such devices and sensors, often combined with decision-making systems using machine learning[17], are increasingly ubiquitous, transmitting, receiving and analysing considerable quantities of personal

data. This represents a significant shift in the utilisation and volumes of personal data, yet Part 5 lacks any provisions relating to how this IoT of sensors and devices will be incorporated securely within its proposals for "Digital Government" alongside the more traditional human-arbitrated uses of personal data by organisations and individuals.

There is no reference to identity – how officials or citizens or organisations or devices and sensors will be able to prove who they are and their entitlement to access specific personal data. Without this, it is impossible to share data securely since it will not be possible to know with whom (or what) data is being shared and whether they are an appropriate person or organisation (or device) to have access to that data. Security audits of who has accessed which data, when and why requires a trusted identity framework to ensure details of who has been granted access to data is accurately recorded. It will also presumably be mandatory to implement good practice security measures such as protective monitoring – preventing in real time inappropriate attempts at data access and flagging such attempts to enable immediate mitigating action to be taken.

An example of the type of improved public service that Part 5 aims to deliver was included with the preceding "Better Use of Data in Government" consultation[18] as follows:

Example of how information could be shared on a case-by-case basis

A couple have recently had a new baby daughter. Following registering the birth of their daughter they applied for Child Benefit. They were really pleased to find out that they no longer had to send their child's birth certificate to HMRC as a new digital service would match their daughter's birth records against birth information held by the General Register Office. The whole experience was far better than their previous experience of claiming Child Benefit when they had to purchase a new birth certificate to send to HMRC in the post to replace a lost certificate. As a result they had to wait a number of weeks before receiving their entitlement letter and birth certificate. This time the process of claiming Child Benefit was straightforward, secure and hassle free.

Figure 4: Example use case from the "Better use of data in Government" consultation

However, whilst admirable in its intent to simplify and streamline a service, this example raises many questions that neither the consultation nor the Bill address. Some of these are illustrated in this annotated version of this same scenario:

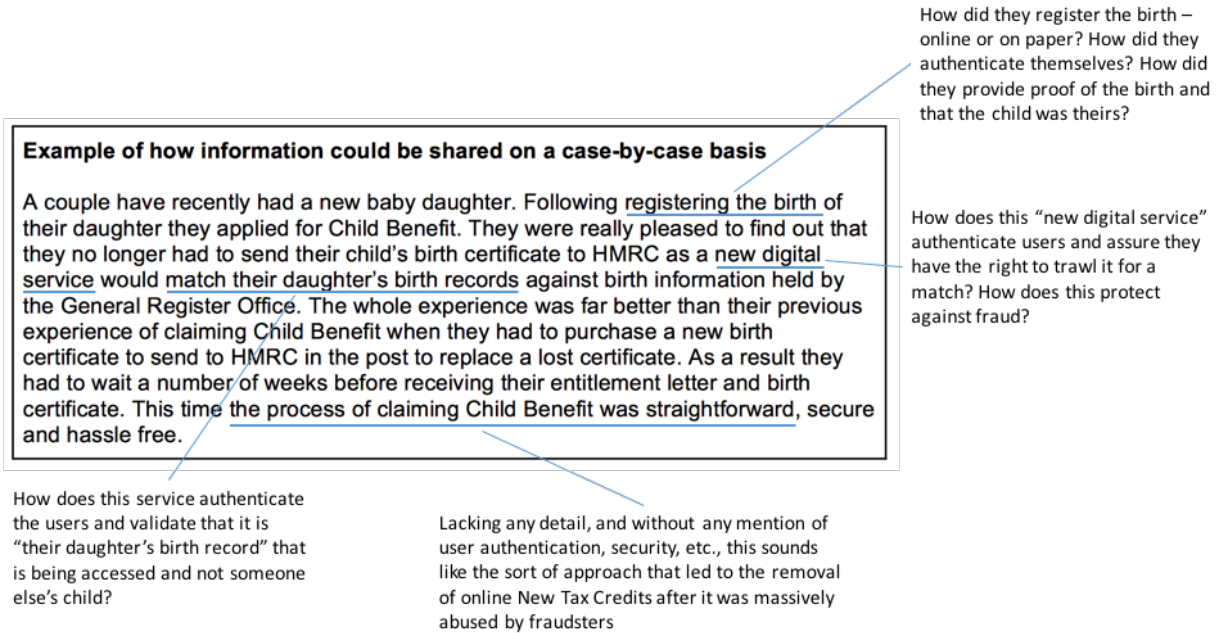

Figure 5: Illustrative lack of detail about how "data sharing" will work

As the annotated Figure outlines, to deliver a service like this will require a combination of both knowing who is online (strong identity verification of citizens, officials and third parties) as well as ensuring they have the right to act in the capacity they claim (e.g. that they are the parent of a given child, or that they are a member of a government organisation with the right to access the data concerned). "Data sharing" alone (however that is defined) will not solve the problem of how to deliver better services, and in the absence of the Codes of Practice it is unknown how the Bill intends services to operate.

Without any technical detail it is impossible to assess the data sharing mechanisms and controls, nor the provisions that will enable citizens to provide or withdraw consent. It's hard to see how Parliament can review and comment on Part 5 of the Bill in its current state, or validate its compliance with the DPA or GDPR. Some of the important questions that remain unanswered include:

- what precisely, legally and technically, does "data sharing" mean?
- how will a civil servant, or an employee in a private sector organisation, identify themselves as a person with a legitimate interest in a citizen's personal data (and with an appropriate level of clearance where required)?
- how will their access be monitored and how will it be audited – and will this be real-time protection or retrospective? (particularly important if someone is accessing an at risk individual's personal data)
- will civil servants be able to trawl all records or only the specific one related to the service on which they are currently working, and how will such mapping / matching happen and be applied?
- how will data be "shared"? Will it be copied to their system, will they get access to the full record, will they view the record on the system where it is currently retained, or will the system simply confirm attributes – e.g. "this parent has a child and is eligible for child benefit", without disclosing any details about the child or their data?
- how will data be secured, what levels of protection are being applied to data at rest and in motion? What levels of granularity are being applied to access controls to ensure more sensitive data is not disclosed without appropriate authority?
- how does the civil servant prove they are authorised to carry out their activities and are not participating in a potential or actual fraud and merely "fishing" for data?
- how does a citizen initiating a service, such as a claim for child benefit, prove who they are and, in the case of child benefit, prove that the child that they are asserting is theirs *is* theirs?
- how is the data of those most at risk or vulnerable going to be "shared" whilst ensuring preservation of security and without tell-tale flags that in turn reveal that a sensitive record has been "hidden"?

Without addressing this level of detail, Part 5 of the Bill has the potential to facilitate more widespread and automated fraud and the compromising of potentially at risk people, such as vulnerable children.

Part 5 of the DE Bill seems to define its own non-standard definition of "personal information" rather than simply referencing the DPA and GDPR. This is Section 32, 4:

- *"For the purposes of this Chapter information is "personal information" if—*
  - *it relates to and identifies a particular person (including a body corporate), but*
  - *it is not information about the internal administrative arrangements of a specified person or a person to whom information may be disclosed under section 30."*

The arbiter of what is, and is not, personal information is the DPA – any attempt to redefine what is "personal data" within this Bill is presumably likely to be ruled invalid. Part 5 also appears at odds with the DPA when discussing civil registration documents. These will be shared in "bulk" to "improve service delivery" "where there is a clear and compelling need" according to the Bill. However, "clear and compelling" remains a lower test than the DPA's "necessary and proportionate" and is likely to be challenged. Also, the use of bulk data runs counter to Centre for the Protection of National Infrastructure (CPNI) guidance, which warns of the risks associated with bulk data, particularly from hostile foreign intelligence services.

Part 5 states with regard to civil registration documents:

> *"A civil registration official may disclose information under this section only if the official is satisfied that the authority or civil registration official to whom it is disclosed (the "recipient") requires the information to enable the recipient to exercise one or more of the recipient's functions." (page 36, paragraph 38(2)(2))*

This suggests that consent is to be moved away from citizens to officials leaving officials to decide when they can share personal data even if the data was not provided by the citizen for that purpose.

This raises a notable characteristic of the Bill – its apparent intent to move the control of personal data away from citizens to officials. It proposes that the decision on what to share and with whom will be determined by "regulations made by the appropriate national authority" (see e.g. Section 29, Para 2, Page 28) where the "national authority" "means the relevant Minister" (see e.g. Section 37, Para 1, Page 34). Consent to use personal data is thus moved away from the citizen to the Minister – in practice, effectively the Minister's officials.

The Bill leaves Ministers free to choose which organisations are to be involved in more widespread data sharing but provides no detail regarding the nature of the data to be shared, the justification or the purpose for doing so. It is not clear how this organisation-centric model complies with the GDPR or DPA (which require user consent), or how this requirement in the Bill aligns with the policy intent to ensure that citizens are placed at the centre of ownership and management of their own data.

On data sharing for research purposes (Chapter 5 of Part 5), it's unclear how this relates to say Article 89 of the GDPR safeguards. Is the intent of Part 5 of the DE Bill to establish an alternative data protection and sharing regime? This could be a potential issue if the UK needs to prove "adequacy" in its Brexit negotiations. As the GDPR takes precedence, is Part 5 of the DE Bill even required given the GDPR sets out when and how data may be accessed? There is no justification or evidence provided as to why there is a need to place organisations and officials in charge of deciding what to do with citizens' data rather than enabling the citizen to be an active part of the use of their data together with an appropriate consent model.

Even after Brexit, the UK will presumably need to remain broadly in compliance with the GDPR if it is to host European citizens' data. Whilst there are "flexibilities" around GDPR, in terms of its precise implementation, its intent is well-aligned with stated policy – to improve citizen control over their own data and ensure secure data in an age of increasing cyber threats – and the working assumption here is that it will broadly be adopted "as is". Some potential conflicts with the GDPR are provided in Table 1.

GDPR requirement	**Part 5**
1. Data must not be used to monitor the behaviour of people in a way which could be seen as profiling.	Part 5 of the DE Bill wants to share data in order to "flag identified persons" entitled to receive assistance. This appears to be profiling, in conflict with the GDPR. Also, there is no mention of the emphasis that should be given to data minimisation.

2. "Data held by public authorities should only be disclosed when a written, reasoned and occasional request has been made and **should not be shared as a filing system in a way that could lead to the interconnection of filing**".	The general purpose of Part 5 of the DE Bill does not appear well aligned to the GDPR. It seems to default to the ability for organisations to share data without consent where the organisation, not the individual, makes the decision alone, and effectively seems to be proposing an approach analogous to a public sector wide file sharing system (the "data sharing" it proposes) – apparently in conflict with the GDPR.
3. Pseudonymised data should be considered identifiable information. Also, Recital 26 states that "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."	Recital 26 raises the question of how well personal data can truly be anonymised – there is a body of research / evidence about the problems associated with truly anonymising data and hence the potential for re-identification. Such difficulties suggest that in practice the GDPR will apply where data can be, or proves to be, re-identifiable even if an organisation intends or believes the data to have been anonymised? **De-identified data is not necessarily anonymised data**: where are the de-identification regulations / frameworks? If any exist, they do not seem to be referenced in Part 5.
4. People should be aware of the risks, rules, safeguards and rights in relation to the processing of their personal data.	If data is shared beyond the organisation or individual to whom it was originally provided and without their consent or knowledge, it is unclear how citizens will be updated on the additional risks inherent in opening up their data to additional organisations and people.
5. The **exact purpose** for the need of the data should be explained at the point the data is requested.	Part 5 appears to cut across the GDPR since it proposes to "data share" or "disclose" data meaning that it is, in such circumstances, no longer being used for the **exact purpose** for which it was originally requested and provided. "Data sharing" implies uses of the data other than that for which they were originally supplied.
6. Processing should only happen if there is no alternative way.	There already exist other ways that the objectives of making better use of data can be achieved without copying it around more organisations.
7. Data is only lawfully processed if consent has been given by the individual. The GDPR also gives data subjects **the right to withdraw consent at any time** and "it shall be as easy to withdraw consent as to give it." Controllers must inform data subjects of the right to withdraw before consent is given. Once consent is withdrawn, data subjects have the right to have their personal data erased and no longer used for processing.	In the context of "data sharing" (undefined), the consent issues becomes problematic: for example, how will consent be withdrawn if data have been widely "shared" and dispersed across multiple organisations over whom the original data controller has no jurisdiction?
8. The data controller should be able to **prove that consent has been given** (an automatically completed tick box is not considered consent)	Part 5 appears to be proposing a system of data sharing in which consent is not explicitly provided, but is determined by the decisions of "specified persons" rather than the citizen. This appears to place it in direct conflict with the GDPR.

Table 1: Part 5 – sample issues with relation to the GDPR

Alternative approach

Examples have been given above of some of the issues with Part 5 of the Digital Economy Bill. However, the need to modernise and move government and public services into the digital age is well understood and recognised. It is not the policy objective at fault, but the approach proposed in Part 5.

An alternative approach would be to consider developing Codes of Practice showing how for example the GDPR and / or DPA could enable the desired outcomes of Part 5 to be achieved, but without any of the security and privacy weaknesses. The basis of a DPA compliant approach that preserves data security and which places the citizen in control could, for example, potentially be achieved using the government Verify identity assurance system[19] combined with attribute exchange.

"Attribute exchange" is admittedly a dry technical phrase. But it's an important example of how the benefits of making decisions based on personal data can be achieved without the downside of weakening the protection of that data. It essentially involves the confirmation of circumstances (such as "This person is over 16") or the disclosure of a limited data set specific to a specific transaction (such as "This person lives at Flat 6 New Field Estate") with the full knowledge and active consent of the citizen concerned. Note that in the case of age verification ("This person is over 16") it does not even involve disclosing the full birth date of a person, further protecting their personal data.

This approach is not new: the Government Digital Service (GDS) has already undertaken work using the government's Verify identity assurance scheme together with attribute exchange in a series of pilots, including with local government[20]. They have also been working on public registers of open data to remove duplication and improve consistency across government of standard data such as addresses[21].

A highly simplified schematic is shown below of how a trusted identity assurance framework can be used with attribute exchange and active citizen consent to achieve the outcomes of improving public services in compliance with the DPA and GDPR.

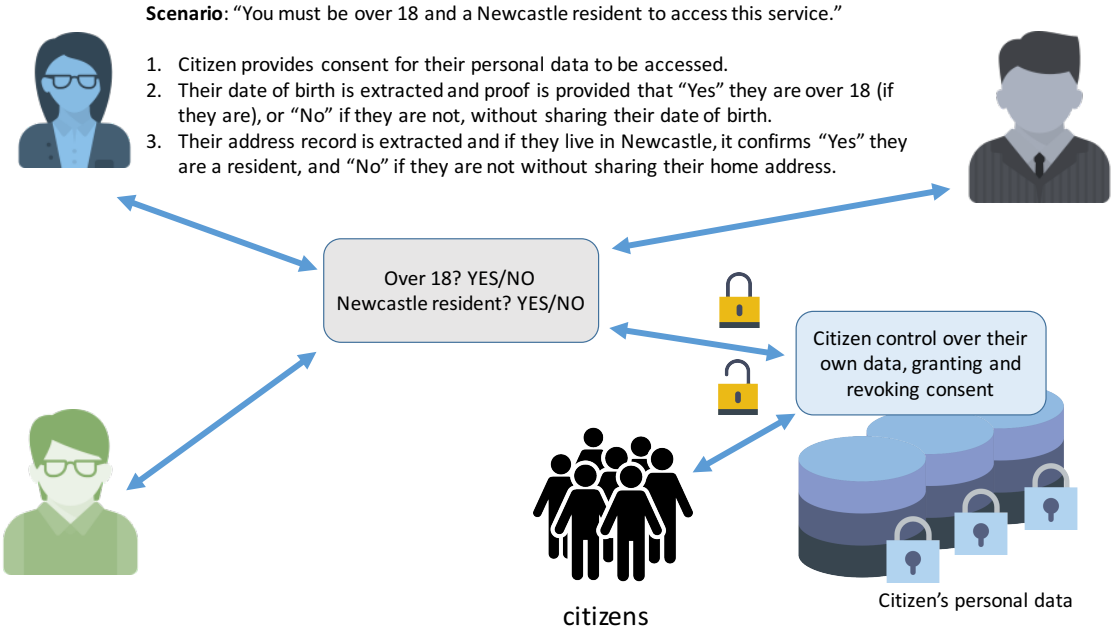

Figure 6: Secure use of personal data preventing unnecessary disclosure and placing the citizen in control

The result is a system that empowers the citizen whilst enabling officials and organisations to confirm the information they need – such as how much a citizen earns, how long they have been at their current address, if they hold a valid driving licence, if they are registered disabled, etc. – in order to make a correct decision or determine an outcome. Personal data is not copied around, as in the days of typing pools, carbon paper and filing cabinets, but kept secure, improving resilience against insider or external compromise. Citizens are able to provide consent, and withdraw it as they wish, enabling compliance with the DPA and GDPR.

To avoid social exclusion for those unwilling or unable to use such digital services, successful implementation must support intermediaries – people that can be granted permission to act on behalf of others. This could include the ability for a citizen to authorise anyone from accountants to carers to those with power of attorney to act on their behalf. The Bill makes no mention of support for intermediaries and their role in improving the use of data: it is unclear what the policy or

strategy is towards the empowerment of intermediaries[22]. Yet without such support for citizen-authorised delegated authority, any system will find it difficult to enable better use of data without also causing social exclusion.

Another challenging aspect yet to be resolved is the trust framework and identity scheme to be used across organisations – how, for example, someone from DWP proves they are from DWP and that they are entitled to be querying personal data held by another organisation. No such cross-government or inter-organisation identity model currently exists – a pre-requisite for any secure access to and use of personal data.

Recommendations

The absence of the Codes of Practice makes the nature of the "data sharing" proposed and the safeguards outlined in the Bill impossible to assess. Their absence is unusual since presumably such Codes would have needed to be drafted in conjunction with the Bill to test and validate its provisions and safeguards.

If Part 5 is to be retained for specific legal or technical reasons, such as making data breaches a criminal offence, it needs to be substantially re-drafted under expert supervision to put precise legal and technical detail into law to ensure (a) an improved approach to the use and protection of personal data and to bring it into alignment with best cyber security practice and (b) to ensure it implements an effective and consistent approach to the use and availability of open data.

Note

This is a personal submission, made from a technologist's – not a lawyer's – perspective. It should not be taken to reflect the opinions of any of my clients or employers – past, present and indeed future.

Glossary of Terms

API	Application Programming Interface – the interface on a computer system that enables it to talk to other systems
Attribute	An element of data regarding a person or object. For example, "Name" or "Date of Birth".
Attribute Exchange (AE)	Confirmation of a specific attribute or attributes. For example, details of someone's residential address might be confirmed by a local authority to a bank. Typically AE incorporates processes to ensure minimal data disclosure: for example, rather than releasing someone's full date of birth, an organisation would be able to confirm to another whether someone is over 18, over 65 etc.
Brexit	Brexit means Brexit
Care.data	The cancelled programme to share sensitive NHS patient data, including with commercial entities and without the patients' explicit consent
CPNI	Centre for the Protection of National Infrastructure
CTO	Chief Technology Officer
De-identification	The processes used to prevent a person's identity from being connected with or associated with data or information
DPA	Data Protection Act
DWP	Department for Work and Pensions
GDPR	The General Data Protection Regulation
GDS	The Government Digital Service
IT	Information Technology
NAO	National Audit Office
NCSC	National Cyber Security Centre
ODI	Open Data Institute
ONS	Office of National Statistics
Part 5	Part 5 of the Digital Economy Bill, relating to "Digital Government"
PCAG	The Privacy and Consumer Advisory Group, established by the Minister for the Cabinet Office in 2011 to review and advise on all aspects of technology-related policy impacting on citizen privacy and security
"the Bill"	The Digital Economy Bill 2016
Verify	The Government Digital Service identity verification scheme, enabling citizens to prove their identity online in order to access digital services

Further Reading

- "The problem with data sharing." Jerry Fishenden, May 2016. Source: https://ntouk.wordpress.com/2016/05/09/the-problem-with-data-sharing/
- "Online Government: SSO and Data Sharing". February 2007. An animated overview of how to use U-Prove for secure authentication and data sharing in an e-government setting. Presented at the 8th Annual Privacy and Security conference in Canada. Source: http://www.credentica.com/presentations.html
- Problems with the fraud associated with putting New Tax Credits online – see for example "Online tax credit system closed" 2 December 2005, BBC (source: http://news.bbc.co.uk/1/hi/business/4493008.stm) and "HM Revenue & Customs 2005-06 Accounts: The Comptroller and Auditor General's Standard Report" 11 July 2006, National Audit Office (source: https://www.nao.org.uk/press-releases/hm-revenue-customs-2005-06-accounts-the-comptroller-and-auditor-generals-standard-report-2/)

Acknowledgements

Some of the Figures in this submission incorporate icons licensed under the Creative Commons and in compliance with their licensing terms I wish to acknowledge the iconography of Freepik (http://www.flaticon.com/authors/freepik), Madebyoliver (http://www.flaticon.com/authors/madebyoliver) and the OSA Icon Library (http://www.opensecurityarchitecture.org/cms/library/icon-library).

REFERENCES

[1] "The Information Commissioner's response to the Cabinet Office's consultation on better use of data". Paragraph 6. 27 April 2016. Source: https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1624084/ico-response-to-cabinet-office-consultation-better-use-of-data-20160421.pdf.

[2] "IT Now: The Magazine for the IT Profession". September 2016, page 7.

[3] "One third of enterprises suffered an insider breach in the past 12 months." 30 September 2016, eSecurity Planet. Source: http://www.esecurityplanet.com/network-security/one-third-of-enterprises-have-suffered-an-insider-breach-in-the-past-12-months.html
[4] "Technology Code of Practice". Updated 2 September 2016. Source: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
[5] See e.g. "Care.data: how did it go so wrong" BBC News, 19 February 2014. Source: http://www.bbc.co.uk/news/health-26259101 ; "Care.data is in chaos. It breaks my heart" Ben Goldacre, 28 February 2014, The Guardian. Source: https://www.theguardian.com/commentisfree/2014/feb/28/care-data-is-in-chaos
[6] "Protecting information across government". National Audit Office, HC 625. Session 2016-17. 14 September 2016.
[7] "UK's digital economy is world leading in terms of proportion of GDP". TechUK, 1 May 2015. Source: https://www.techuk.org/insights/news/item/4075-uk-s-digital-economy-is-world-leading-in-terms-of-proportion-of-gdp
[8] Internet of things. Wikipedia: https://en.wikipedia.org/wiki/Internet_of_things
[9] "Conclusions of civil society and public sector policy discussions on data use in government" undated (~April 2016?) source: http://datasharing.org.uk/conclusions/
[10] Numerous examples – see for example "Cybercrime figures prompt police call for awareness campaign" (The Guardian, July 2016) at https://www.theguardian.com/uk-news/2016/jul/21/crime-rate-online-offences-cybercrime-ons-figures ; "Cyber crime cost UK businesses more than £1bn in the past year" (Computer Weekly, June 2016) at http://www.computerweekly.com/news/450298242/Cyber-crime-cost-UK-business-more-than-1bn-in-the-past-year ; "Crime soars 107% as cyber offences included for the first time" (The Telegraph, October 2015) at http://www.telegraph.co.uk/news/uknews/crime/11932670/Cyber-crime-fuels-70-jump-in-crime-levels.html.
[11] Numerous examples – see for example "The threat is coming from inside the network: insider threats outrank external attacks" (Security Intelligence, June 2015) at https://securityintelligence.com/the-threat-is-coming-from-inside-the-network/ ; "Malicious insiders the fastest growing threat to cyber security, warns report" (Computing, January 2016) at http://www.computing.co.uk/ctg/news/2442565/malicious-insiders-the-fastest-growing-threat-to-cyber-security-warns-report ; "Half of UK's firms ill-equipped to tackle malicious insiders" (IT Pro Portal, August 2016) at http://www.itproportal.com/2016/08/18/half-of-uks-firms-ill-equpped-to-tackle-malicious-insiders/ ; "Non-police orgs merrily accessed PNC without authority, says HMIC" (The Register, May 2016) at http://www.theregister.co.uk/2016/05/12/hmic_inspection_reveals_non_police_organisations_accessing_police_national_computer/.
[12] See https://www.gov.uk/government/consultations/better-use-of-data-in-government.
[13] HM Government's Privacy and Consumer Advisory Group, see https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group
[14] e-mail to the independent quality assurance group. Dated 5 July 2016.
[15] "Better use of data in government – consultation." Source: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/503905/29-02-16_Data_Legislation_Proposals_-_Con_Doc_-_final__3_.pdf.
[16] "One year on from the general election: what does the UK data landscape look like?" Open Data Institute, May 2016. Source: http://theodi.org/news/one-year-on-general-election-uk-data-landscape
[17] Machine learning. Wikipedia: https://en.wikipedia.org/wiki/Machine_learning
[18] See https://www.gov.uk/government/consultations/better-use-of-data-in-government
[19] See GOV.UK Verify
[20] See for example "Attribute Exchange will enable government Verify plans" November 5 2014 CIO UK (source: http://www.cio.co.uk/it-security/attribute-exchange-set-increase-identity-security-for-cios-3583812/) and "Verify, attribute exchange and blue badges" Warwickshire County Council 3 March 2016 (source: http://istanduk.org/wp-content/uploads/2016/04/LCIO-Council-160303-with-screen-shots.pdf).
[21] "Registers: authoritative lists you can trust" GDS 1 September 2015 (source: https://gds.blog.gov.uk/2015/09/01/registers-authoritative-lists-you-can-trust/)
[22] There was substantial earlier work on intermediaries precisely to address these issues – see for example "Channels framework. Delivering government services in the new economy" Cabinet Office 30 September 2002 (source: https://ntouk.files.wordpress.com/2015/06/channels_framework_2002-09-30.pdf)