



# Response to National Data Strategy open call for evidence July 2019

## Contents

INTRODUCTION	1
KEY CONCERNS	1
PERSONAL DATA AND PRIVACY	2
PERSONAL DATA AND COMPETITION	3
PROCUREMENT, OPEN SOURCE AND OPEN STANDARDS	3
OPEN DATA	4
THE PUBLIC DOMAIN	5
INTELLECTUAL PROPERTY POLICIES	6

## 1. INTRODUCTION

- 1.1. Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.
- 1.2. We have responded to government consultations and data policy work for many years. Recent highlights include work on data protection enforcement, including challenges to online behavioural advertising practices, currently being investigated by the Information Commissioner. We have raised concerns about the lack of privacy protections relating to online age verification.
- 1.3. We contributed to the Cabinet Office's consultation policy processes that resulted in the Digital Economy Act's provisions for data sharing. We worked as a consultant to Barcelona City Council as they designed their city's data policies.
- 1.4. We have also campaigned against ID Cards in the UK, because of the data sharing potential, and consulted on the potential for better data practices following the JRRRT's Database State report. In Scotland, we have campaigned successfully for better data practices relating to government and online identity projects.
- 1.5. In this brief response to a vast question, we highlight the need for a multi-stakeholder approach, collaborative policy making and means to bring the public along with changes, starting with a rights-based approach to the use of data. We therefore are very pleased that the consultation states that "[t]his is a broad, wide-reaching remit and we will be in a continual process of engagement throughout the Strategy development to ensure that views across society, economy and government are taken into account." We would however like greater clarity about the methodology and depth of engagement.
- 1.6. There are many aspects of government data policy where the promise of digital access to the wealth of government information, contemporary and historic, documentary, photographic and otherwise, has simply not been met. We would advocate for a thorough review to deliver the full benefits of a digital future.

## 2. KEY CONCERNS

- 2.1. Many attempts at government data policy have come undone as a result of poor consideration of the public impacts. As a result, policies have been abandoned in the face of public protest. Obvious examples of these mistakes include use of health data for commercial research, clauses for unrestricted data sharing, and ID Cards.

- 2.2. Some of the underlying problems may include issues with service procurement, and failure to understand the value and impact of data itself. In our view, competencies to understand the strategic concerns are of increasing importance. Challenges relating to machine learning and use of government data for commercial ends are one example of this. It is critical that government does not simply transfer the value to the private sector, and that as much as possible, learnings and information are placed in the public domain.
- 2.3. Dealing with these kinds of challenge require an open process that involves as many stakeholders as possible in data policy. Therefore our primary call is that government attempts to evolve open policy making processes that cover issues including data sharing; use of data for service delivery; commercial application of data; and use of data for transparency purposes.
- 2.4. Government is engaged in a number of processes like this. The Cabinet Office ran a very good process around data sharing<sup>1</sup> in the lead up to the DEA 2017, albeit we remain concerned that proposals were widened, including the use of civil registration records were added very late.<sup>23</sup> The Home Office are currently using a similar process to understand the ethical, practical and legal considerations of changes to police use of evidence and criminal records in national police databases. Detailed discussion at the design stage of policies with people who may be concerned or have particular needs to be addressed seems only sensible. This strategy is an opportunity to bring in expertise in open policy design processes, especially where the strategy is particularly ambitious or potentially controversial.
- 2.5. The leading practitioners in this field in the UK are Involve. We would urge that DCMS talks to Involve about practical steps DCMS could take in designing the next steps of this strategy development.<sup>4</sup>
- 2.6. In the following sections, we offer some general observations about previous problems that have surfaced, in order to demonstrate the challenges the strategy will have to address.

### 3. PERSONAL DATA AND PRIVACY

- 3.1. Government often sees benefits or potential uses for personal data that it holds, and assumes that it should be able to do what it seeks fit, not least because it is easy to conflate government purpose with public benefit.

---

<sup>1</sup> <https://www.openrightsgroup.org/blog/2014/update-on-data-sharing-policy-process>

<sup>2</sup> <https://www.openrightsgroup.org/blog/2016/overview-of-the-digital-economy-bill-2016>

<sup>3</sup>

<https://www.openrightsgroup.org/blog/2017/lords-committee-slams-data-sharing-powers-in-digital-economy-bill>

<sup>4</sup> <https://www.involve.org.uk>

- 3.2. Government has also seen fit to grant itself exemptions to providing citizens with data protection rights, for instance granting itself a blanket exemption for immigration-related data. Regarding NHS Care.Data, government did not believe that data subjects needed to grant permission for the use of their data, eventually settling on broad brush attempts to inform people of their right to opt out.<sup>5</sup> Immigration exemption is now subject to a legal challenge, which we are part of. CareData collapsed as a result of concerns centred on consent.
- 3.3. The result of this approach is that it appears to many that double standards exist. Privacy rights are eroded or removed when convenient for the government. Ultimately, this undermines trust in government.
- 3.4. The power of government to discriminate, make arbitrary decisions and otherwise adversely impact UK citizens and residents is amplified as more use of data is made. Thus greater rights and care, not less, needs to be the standard applied by the new strategy. The strategy should address current deficiencies, including those introduced by the recent Data Protection changes.
- 3.5. The strategy should build on data protection principles. There is a great deal of scope to use concepts of fair processing, consent and transparency, alongside evolving ideas of accountability for machine decision-making. These can take government along way towards dealing with the emerging challenges of discrimination, exclusion and opaqueness from AI, machine learning and automated decision-making.

#### 4. PERSONAL DATA AND COMPETITION

- 4.1. The reuse of personal data can be of immense benefits for competition, where individuals choose to use their data in different contexts. Open Banking is a good example of how this can take place, and also of the problems that can emerge. Government should look closely at how this evolves to understand the risks and benefits of transfers of personal information.
- 4.2. These possibilities were understood by the 2010-15 government which attempted to open up access to personal data for market comparison. These efforts were in our view premature, as the full suite of GDPR rights are needed to give consumers both rights to their data and protection from abuse.
- 4.3. GDPR envisages that users can gain access to their information and reuse it. This should lead to price comparison and other tools for better market leverage by consumers. Nevertheless, there are significant risks that data transfers could be abused. Government and the ICO will need to work together to make sure that access to data gives good results, rather than leading to malpractice.

---

<sup>5</sup> <https://www.england.nhs.uk/2013/10/care-data/>; <https://en.wikipedia.org/wiki/Care.data>

4.4. One of the main challenges inhibiting the digital economy today is not data portability, but a lack of interoperability. Several countries around the world, such as the German Bundestag, have been considering mandating interoperability requirements for certain key products. This will require careful thought, but in general the promotion of interoperability requirements should be seriously explored, and would be likely to unlock value from data infrastructures without requiring large quantities of data to be shared..

## 5. PROCUREMENT, INTEROPERABILITY, OPEN SOURCE AND OPEN STANDARDS

5.1. Government must also evolve a skepticism about the appropriateness of commercial techniques for social policy. They are not always a good fit. Customers are not the same as citizens, with rights and social expectations. Citizens cannot be chosen or excluded, or opportunities missed, in the way that companies can select their chosen market and products.

5.2. GDS and the Cabinet Office were making progress with problems of procurement. Government must have its own expertise to deal with contracts and procurement. A future data strategy must address concerns about procurement strategies.

5.3. Open Source, Open Standards and competitive tendering remain critical for government to retain leverage over the private sector. Interoperability of products is enhanced by an open standards approach. Co-operation between governments to build open technologies is critical. Learning from other governments is very important.

5.4. In relation to this, Barcelona's attempts to build smart city capabilities that are ethical are a particularly useful example of the relationship between data policies and procurement<sup>6</sup>.

## 6. OPEN DATA

6.1. Data of course gains its value through usage. While this should not lead us to a conclusion that data may be used no matter what, it gives us the insight that some kinds of non-personal data are often better released for permissionless innovation. Government has started on that process, but can go much further. However it is unclear to us at this point what the means will be for government to identify information and data that should be released.

6.2. Categories of non-personal data that should be 'open data' include: performance data; infrastructural data; and data created from research.

---

<sup>6</sup> <https://www.barcelona.cat/digitalstandards/en/init/0.1/index.html>

- 6.3. Some examples can be seen where the balance has not been struck correctly. One such is post code data, mapping to location. This data should be available as open data, in our view, as it is critical for many applications. It is a kind of core reference, infrastructural data, that enables further innovation. The case against rent-seeking by the Royal Mail is high, as Royal Mail's use of it is relatively limited compared to the broader uses by the public, business and industry. In our view this was not properly considered during the privatisation process. As a result a public asset has been or may have been privatised; there is some doubt about who now owns the information. At the very least, government needs a better process to identify 'infrastructural data' and ensure that as much as possible is released as open data.
- 6.4. Public-private contracts also pose problems for effective release of data. Securing the release of information of this kind requires government to build open data requirements into contracts. Data might need to be required through contracts so that it is both collected and released.
- 6.5. Open Data should be a core feature to understand government performance and planning. To do this effectively requires all stakeholders to be involved in a discussion about what data needs to be collected and published.
- 6.6. We are also concerned that the means by which predictive data are created also needs to be public. For instance, road traffic demand or climate predictions rely on algorithmic computations for their results. This appears to be the case for TfL for instance, whose traffic modelling is proprietary. Assumptions therefore are baked into information that informs policy decisions. It is easy for these to be misleading, if the assumptions are not spelt out. Thus it is highly problematic for such calculations to be provided by proprietary and non-transparent software.
- 6.7. Involving stakeholders in discussions about the data created, and the means by which this is done, and what transparency is necessary or desirable, should help create better policy results.

## 7. THE PUBLIC DOMAIN

- 7.1. Government is a great holder of historical data, documents and records. Many of these were not published under public licences. All historic material should be moved to the public domain, where this is legally feasible. This should include film, photography and publications. This would provide a resource for commercial reuse as well as personal and academic.
- 7.2. Care should be taken to ensure that digitisation does not re-privatise public domain material, by creating artificial barriers around digitised works. This has taken place in the context of academic digitisation, for instance through Google

Books programme. This is poor practice in our view, pushing the benefits of digitisation many years into the future.

- 7.3. Similar concerns arise around the future of personal historic records. There is a significant market in access to data of this kind, for instance through Ancestry.com ; however the data is fundamentally public domain. The greatest benefits accrue from digitisation and release of data. Care needs to be taken not to simply regard historic public records as a kind of cash cow, to be digitised privately in return for income to government, but rather something of broad public, academic and historic interest.
- 7.4. To the extent that the government commissions copyright works in the future, it should place these in the public domain, in the same manner as the USA.
- 7.5. Government also needs to be firmer in its support of moving academic research into the public domain, and ending the practice of commercially closed publication of academic research that is otherwise paid for by the public.
- 7.6. We would welcome a thorough discussion of these issues so that the governments' data policies support a thriving public domain, with the commercial, personal, academic and cultural benefits that could flow from it.

## 8. INTELLECTUAL PROPERTY POLICIES

9. Careful consideration of the restrictions that copyright, database right and other IP rights place on public outputs needs to be made. In general, these should be removed where government produces information for the public benefit. In some cases, IP is likely to be making unnecessary general restrictions. Government data policies should attempt to reduce this friction and look for opportunities to loosen IP to allow a wider benefit from data.
10. The review should in particular look at the Database Right. Evidence has never been found to show any positive impact of this IP right, yet it restricts the flow and ease of licencing of much factual data.
11. The review should also ensure that current IP law does not impede acts such as scanning, transcription and other literal copying by creating 'new' layers of copyright. Much confusion exists about where copyright may or may not apply new rights as a result of these acts. A new copyright should not be created for any act of copying, in our view.