

Data sharing for public service delivery: a roundtable discussion on the UK government's data protection consultation

Summary note of roundtable held on 12 October 2021, convened by the Open Data Institute and the Institute for Government.

Introduction

On 10 September 2021, the Department for Digital, Culture, Media and Sport (DCMS) published a consultation on data protection, '[Data: a new direction](#)', inviting responses until 19 November. DCMS encouraged civil society and other organisations to organise events around the consultation, to explore some of the issues raised and inform the process.

As part of this process, the Institute for Government (IfG) and the Open Data Institute (ODI) organised a roundtable discussion on public sector data sharing, a key theme of chapter 4 of the consultation. The roundtable brought together participants from government, civil society, think tanks, academia and the private sector. It was held under the [Chatham House Rule](#) – this document, produced by the ODI, is a non-attributable note that draws out some of the key points from the discussion. It reflects the discussion and does not necessarily reflect the views of either the ODI or the IfG.

The consultation is open until Friday 19 November 2021, and at the ODI we are preparing a response which we will also publish. You can read more about our engagement on [our project webpage](#), or contact the team on policy@theodi.org; we'll also be sharing updates on Twitter: [@ODIHQ](#).

Consultation summary

The reforms suggested in 'Data: a new direction' are designed 'to create an ambitious, pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of data'. The consultation is linked to [Mission 2 of the National Data Strategy](#), 'securing

a pro-growth and trusted data regime', as well as one of the [government's 10 Tech Priorities](#), to unlock the power of data.

Chapter 4 of the consultation is all about 'Delivering better public services'. The specific consultation questions in this chapter relate to:

- Whether the **Digital Economy Act 2017** – which provides a gateway for data sharing across the public sector – should be extended to help improve outcomes for businesses as well as individual citizens
- Clarifying that **private companies processing data on behalf of public bodies** can rely on the same lawful grounds for processing the data as the public body
- Clarifying that **public and private bodies can lawfully process health data** for reasons of 'substantial public interest' in health or other emergencies
- Introducing **compulsory transparency reporting on the use of algorithms** in decision-making for public authorities, government departments and government contractors using public data
- Either **introducing a legal definition of 'substantial public interest'** or adding to the list of situations which are **always deemed to be of 'substantial public interest'**, to support the use of sensitive personal data
- Clarify rules on **police collection and use of biometric data**, and standardise wording in legislation to allow more cross-sector working between **intelligence and law enforcement services**
- Considering whether any of the proposals in the chapter would **particularly impact people with protected characteristics**.

The roundtable discussion focused on one of the key themes from the chapter: data sharing across the public sector. It also touched on public sector considerations from some of the other chapters, particularly chapter 2 on 'reducing burdens on businesses and delivering better outcomes for people' (which recommends, for example, removing the requirement for organisations to have data protection officers and produce data protection impact assessments, and changing the threshold for reporting data breaches).

One sentence on government data sharing

At the start of the event, participants were asked to summarise their thoughts on data sharing in government in one sentence:

- 'Potentially hugely beneficial, if implemented well and trusted by its data subjects.'
- 'Data sharing across government is getting better, but government needs to get much better at being much more open and transparent with the public about what they want to do with data.'
- 'There is no such thing as government data'

- 'All the problems in government data sharing have been solved apart from some technical ones and the big one about the people that make decisions.'
- 'Government data sharing is based on a perverse attitude to risk and does not support automation.'
- 'I am hugely excited about the opportunities that the Digital Economy Act gives us in promoting the use of government held personal data across public sector.'
- 'I think that data sharing in government still feels like too much of an afterthought when it should be the default.'
- 'There's much more sharing that can be done in government both in and out of government.'
- 'Data sharing government is everything and nothing: everything, because politicians love to talk about it; nothing, because they rarely follow up on their promises.'
- 'Data is not a 'nice to have' and GDPR is not the problem: culture, legacy systems and poorly executed contracts with the private sector are a key barrier.'
- 'Data sharing requires proactive public engagement to get them on board.'
- 'It's a long, hard road; we've been trying to do it for 25 years; let's sort it out one step at a time and keep tackling the barriers.'
- 'It's something that holds great potential, but it's really hard to realise it to make it happen.'

Key themes

The remainder of the roundtable discussion was split into two open talks:

- The current data protection framework: how well it's working, what the barriers are to data sharing, and the pandemic experience.
- Proposed reforms: what reforms could improve the delivery of public services, what difference the proposed reforms will make, and what safeguards might be necessary.

Several key themes emerged across the discussions, which are synthesised below.

The law is not the main challenge

Perhaps the strongest theme from the discussion was that the existing legislation was not the main challenge to data sharing in government – culture, a lack of guidance, and needing to get data basics right were all cited as bigger challenges. One participant summarised the discussion as: 'We've not touched on data protection as being the biggest barrier for sharing. It's more about the data, the skills, the technology, the processes, the culture. These are the broader issues we need to feed back into this consultation – a few tweaks to data protection are not going to fix some of the things we want to do.'

It was reported there had been a rumour that one minister wanted to suspend the General Data Protection Regulation (GDPR) during the pandemic – but the discussion suggested other actions would be more helpful in encouraging data sharing.

Challenge: The importance of organisational culture

Several participants suggested GDPR was often invoked by government organisations when they didn't want to share something: it was rare that the law actually stopped you doing so. A reluctance to share could also come from a fear of being exposed as a poor custodian of data holding poor-quality data. And sometimes, it is simply the case that people think that certain data transfers aren't allowed when actually there isn't a legal impediment.

Many parts of the government do not have an existing culture of data sharing between individual departments, and even within individual departments, different groups, programmes and teams have different cultures. It was argued that cultures interact with institutions and cultures are reinforced by structures, and there fundamental problems with incentives as part of those structures. For example, ministers and senior civil servants might express an interest in more data sharing, but the burdens and risks are concentrated at middle management level (grades 6 and 7), who have very little incentive to share (risky innovation leading to failure could harm their promotion prospects).

The lack of an existing culture of data sharing – and knowledge of data sharing – meant it was difficult to leverage existing mechanisms for sharing data even during the pandemic. One example was that [the Caldicott Principles](#), overseen by the [National Data Guardian](#) (who advises and challenges the Department of Health and Social Care), were often deployed to say 'no, you can't do this', when the seventh principle is 'The duty to share information for individual care is as important as the duty to protect patient confidentiality'. This also highlights that data governance is a live and evolving thing and may depend on context, but 'once somebody has said no in the data world, it is very hard to change that'.

One participant reported asking a secretary of state about improving the data their department holds. Their answer was: 'Well, it's a question of either doing that, or getting down the backlog, which do you want me to do?' when actually, the two are really intimately linked. Participants framed this challenge as: 'How do we shift a culture which still sees data as a nice-to-have, optional extra?'.

Challenge: The need for proper guidance, support and tools

Given this, guidance and support – rather than changes to legislation – were thought to be most useful for public sector data sharing. Having a more sophisticated understanding of

the Caldicott Principles, for example, allowed the 'rote sort of objections' that might be faced to be overcome.

The [National Audit Office \(NAO\) report](#) on the challenges of using data in government recommended providing guidance for people on the frontline as to what they can do and what they are allowed to share. The report also notes this 'fog of confusion' is a longstanding problem, and cites previous government recognition of it (for example, the [2008 Thomas and Walport review of data sharing](#)).

A lack of legal support was also cited, with some government organisations lacking sufficient legal skills to advise colleagues on data sharing. Upskilling these legal departments would therefore be helpful.

Participants observed that it can be really difficult for a public servant to have to make the decision on whether to share data or not – 'it's a really hard place to be and so support is really important'.

Challenge: The lack of data foundations

Pillar 1 of the National Data Strategy defines '[data foundations](#)' as 'data that is fit for purpose, recorded in standardised formats on modern, future-proof systems and held in a condition that means it is findable, accessible, interoperable and reusable'. Several participants felt that this – the need to 'fix the plumbing' of data in government – was a more significant barrier to data sharing than anything in legislation, or indeed any technical barriers.

It was argued that focusing attention on the legal framework is a 'distraction from the foundational work that is needed'. Examples given included:

- A lack of basic agreed definitions and standards across government; for example, nobody could agree how many judges had sat during the pandemic, with no standard for what a court is, or what constitutes a sitting day.
- There is no consistent standard for a citizen record across government ([the NAO found](#) 'more than 20 ways of identifying individuals and businesses across 10 departments and agencies, with no standard format for recording data such as name, address and date of birth').
- Public sector organisations having to buy back data from private sector providers.
- A reliance on legacy systems and technology.
- The difficulty in knowing who holds what data across government (a [recent ODI report](#) shows the range of different organisations involved).
- The poor quality of datasets, leading to concerns about automated decision making in particular: the [report by CDEI on algorithmic bias](#) said that poor data infrastructure

and quality was a serious impediment to the responsible use of data driven tools and that needs to be sorted out.

Participants reported that the political focus on ‘data driven technology’ and artificial intelligence (AI) feels divorced from this foundational work; one often has to dangle the ‘shiny, shiny thing’ and promises of efficiency to get buy-in for the basic work, which still doesn’t get done. It has proven difficult to make the case for investment in this foundational work in business cases. Even if some standards issues were solved, how could this be retrofitted across the government? And while this would help interoperability across the government, interoperability isn’t a solution on its own. ‘If the government is really serious about tackling the challenges to sharing data, it needs to address these issues and not myopically focus on this [legislative data protection reform].’

It was highlighted that the government now has the [Data Standards Authority](#) setting standards across government and there are other helpful initiatives, like the [Data Ethics Framework](#) and [Data Quality Framework](#). All of this is aimed at making access and availability of government data much easier across the public sector – although perhaps not so much the private sector.

Challenge: The need for stronger incentives

As mentioned in ‘Culture’, above, incentives often work against data sharing rather than supporting it. Organisations like [ADR UK](#), which supports the use of administrative data for research, have found that one incentive is an information feedback loop – the improved data can feed into a department’s policies and decisions.

It may be a ‘false perception’ that we need to remove barriers to share more data; we may need to think about increasing incentives instead. Units across the government that facilitate data sharing may reinforce incentive structures and provide mechanisms to do things better.

The pandemic provided many incentives to share more data, more quickly: ‘we’ve got to do this, we will get past these barriers’.

Missed use of data as well as misuse of data

It was suggested that there is a perverse sense of risk when it comes to data in government: we hardly ever hear anyone talk about the risk of not sharing. This is a cultural problem – we can conclude this because we encounter the same issues when sharing data that is not sensitive personal data, and often not personal data at all, as we would when sharing sensitive personal data. Counterintuitively, one participant suggested it was often easier to share sensitive personal data because there is normally a system to control and

manage it; when it's not personal data, departments have often not prioritised the digitization and collection of the data, or understood the data-supply chain process, etc.

Two different experiences of the introduction of the [Digital Economy Act](#) highlighted this challenge. One participant said their experience was that data sharing had gone backwards – a lot of organisations considered it as a chance to review everything they'd done and think 'we shouldn't be doing that' rather than anyone saying 'let's do that better'. Another disagreed that data sharing had gone backwards, but found that, with [GDPR](#) coming into force at a similar time, government departments were saying 'we've got to give priority to ensuring compliance with GDPR, otherwise we're going to face a massive fine from the Information Commissioner's Office (ICO)' – even though the codes in the Digital Economy Act were written with GDPR in mind.

One participant said it 'almost felt like data protection had been too successful in scaring people not to allow data sharing'. Nonetheless, some felt the conversation was moving away from a completely defensive stance – even if they still had to keep making the point, the conversation was easier. Organisations like ADR UK have started to talk about the missed use of data, as well as the misuse of data all the time, because it is important to get the balance right – 'and it is a balance'. There are precedents now, particularly in health, which can help build the confidence in government departments around why data sharing is a good thing (again, the key barriers are 'people not knowing, not having a precedent, on how to use the Digital Economy Act'). Different risk appetites across the government can still be a problem – one department saying no can stop linkages across departments. Australia was also given as an example, with a default open accreditation model that some are trying to push as a model across the UK government: 'give us a reason why you're not sharing your data on this.'

Problems with government data sharing are often problems with government

Problems of culture and incentives were seen as going beyond just data and into the wiring of the government itself, affecting all kinds of cross-departmental collaboration. One participant felt this had improved in the last few years, but the whole system is set up to encourage departments to pursue their own interests and objectives, with the Cabinet Office and Number 10 banging heads together as necessary. There are exciting data projects, as shown at the [IfG's Data Bites](#); some of the projects through the [Shared Outcomes Fund](#) are really impressive – but frustration was expressed that the fund was only £200m, as this was considered a marginal amount. One participant commented: 'You have to address some of those real structural problems within the way government is set up.'

Another participant added that when data is shared within industry, it's covered by contract: it is clear who is paying and who is the customer. The government is very bad at dealing with other parts of the government as a customer for a data service. There's a lack of investment in interoperability.

Participants felt that the government remains very siloed, with a lack of incentives to cooperate across the siloes – 'nobody ever lost their job for not taking a risk'.

Learning carefully from pandemic experience

The pandemic clearly changed some of the incentives around data sharing and removed existing barriers. 'After Covid, if we cannot find an argument now for greater data sharing, I don't think we ever will.' There is obviously much that we can learn from.

But there was also some concern that 'hard cases make bad law'. There may be a danger in assuming the public will continue to tolerate what they accepted during a pandemic. Should we allow the unprecedented circumstances of the pandemic to drive what we think good looks like? This may be a particular concern, since there was an absence of 'what does the public think about this?', especially when it came to commercial reuse of data held by the public sector.

Transparency is necessary but not sufficient

The public cannot see who is making decisions about data, or the factors that those decision-makers are weighing when making those decisions. Transparency is therefore vitally important. But proper involvement and engagement in decisions about how data is used, and robust mechanisms for redress when something goes awry, are also essential. 'Transparency means nothing unless there's something behind it'.

One participant felt that the consultation had really got this wrong: it is not just about making it easier for people to understand how automated decisions affect them, but providing meaningful access to meaningful redress and helping people to understand how they can challenge unfair use. 'If we were talking about strengthening anything it ought to be that.' This could also help to drive good and better practice: it becomes a virtuous cycle of people knowing what things people object to, which helps them guide policy and design for different systems in the future.

Another participant framed the three key prongs as transparency, control and redress: the ability to have some understanding of what's happening with your data; the ability, ideally, to make some choices about that; and knowing that there's a single point of contact and a clear person who's responsible when things go wrong. People may not always make those choices (for example, switching energy supplier under [Smart Data schemes](#)), but they value

having them and the ability to make that choice is ‘hugely significant’ in getting people to engage. ‘People really don’t like feeling stuff is being done to them’, and dislike ‘black-box decision-making’ which feels like it lacks accountability. All of this is particularly acute with automation in the public sector, which is ‘a monopoly’ and requires regulation. ‘If you automate a system that takes humans out of the loop entirely, you need a replacement way of ensuring transparency’, and an individual needs escalation paths (in a suitable timescale) if they are affected by an automated decision.

For all the support of public engagement, it was regarded as a salutary example that even where a more developed ecosystem for supporting those conversations, like in health, exists, things can go wrong: anyone paying attention to [Understanding Patient Data](#) or the [National Data Guardian](#) would not have proceeded with [General Practice Data for Planning and Research \(GPDPR\)](#), an attempt to link patient records. Having this infrastructure that you then don’t listen to might contribute to cultural problems and nervousness about data sharing.

The ‘public good’ and ‘public interest’ may be too generic to guide good decision making in individual departments. It may be too easy to construe the public interest as synonymous with economic benefit. And while most discussions are framed around privacy, or privacy versus openness, and not around other rights, conversations can be difficult and we don’t think about promoting a range of other interests and goals. Discussing the public good in an honest way – ‘we need to do this to achieve this outcome’ – could also be helpful. It might be helpful to show the public what they get in return for sharing their data – this is why people share their data with tech and social media giants.

The role of politicians was discussed: ‘No matter how many frameworks and mechanisms there are at the official level, all of that can be trashed in a second by a ministerial comment that’s misplaced.’ Sharing contact-tracing data with the police, for example, was considered ‘catastrophic’. The reason for these missteps is that ‘there’s no political strategy underlying it – it’s very much made up as we go along’. There is a role for civil society in helping politicians develop a strategy and consistent set of principles for what they think the right circumstances and conditions are for the government to be making use of people’s data. Another participant answered that while ministers can be unpredictable and ‘throw spanners into the works’, we might not be so concerned if there were underlying public trust in the first place. It is interesting to note that [according to polling](#), the [Office for National Statistics](#) is very trusted as a data organisation, but relatively few people knew what it was. ‘Maybe there’s something in the fact that one of our most trusted institutions is also not very well known by the public.’

One participant said that their organisation talked to the public, citizen assembly-style, about what they were planning to do with data about them, and said that the public were ‘extraordinarily positive’ about that process. ‘I think there are much higher reservoirs of

goodwill among the public towards appropriate data sharing, particularly when people can see clearly the data sharing is in the interest of the public and themselves.'. It must be a dialogue: what good looks like and why good is good for the public. Government polling has shown that while people might be uncomfortable with AI replacing doctors, there was much support for AI being used to complement their decision making. (Although one participant shared a report [from the Center for the Governance of Change](#) that found a majority of Europeans would be comfortable replacing parliamentarians with algorithms.)

Trust is something that has to be unpacked – 'it's not black and white, you just can't put a factual thing in there'. Participants mentioned the [work](#) of [Onora O'Neill](#), which focuses on trustworthiness – the sorts of things that need to be in place, like transparency, redress, and engagement – rather than a narrow focus on trust alone.

Considerations around legislation

One participant asked: 'From all the things we've talked about, what actually goes into legislation?'.

One concern raised about legislation was that 'we need to be careful about not implementing legislation or regulation to fix yesterday's problem, and particularly in the world of algorithms': 'perhaps we need to be a bit more forward looking in terms of legislation than the government has historically been in the data space'. There was also a danger that if reforms 'are seen as being part of a culture war or leading to the greater politicisation of bodies like the ICO' it could 'harm and undermine public trust in data sharing and actually defeat the purpose for which we're seeking these reforms.'

Legal reforms may not be enough to implement desired changes. One participant found that there was a lack of confidence among local authorities in using the Digital Economy Act and had to seek a legal opinion to assure data officers they could use the sharing gateway they were building. How could any reforms be properly embedded, making sure that people understand what they mean for them, and provide them with the tools that they need to harness them?

Any changes should aim to simplify regulations, not complicate them. A lot of departments wary of data sharing are often looking for a reason 'to kick it into the long grass' because they know it's going to be complicated. The more complex the legislation, the easier it is to do that. Others want to do the right thing, but it's all just too complex. As well as any legislation, DCMS writing plain English summaries of what is allowed and what isn't 'would be really valuable'.

Strengthening redress – as per the section above – was felt to be one area that could go into legislation. Few of the real barriers are things that legislation is actually equipped to solve.

Other points raised

There was some discussion about:

- **Public and private.** The private sector being no better at sharing data than the public sector – ‘in fact, it’s possibly a lot worse’. The cultures discussed extend beyond government. Sometimes the private sector fundamentally misunderstands some of the requirements for sharing government data ethically and responsibly.
- **Health and non-health.** The distinction between health and non-health data, which ‘just tripped off all of our tongues before the pandemic’, is really being called into question. What exactly is health data? A lot of things that are classified as non-health data actually have very relevant health applications. That needs some rethinking.
- **Infrastructure and technical challenges.** At the start of the pandemic, ‘every agency and department stood up an ad hoc platform or multiple ad hoc platforms’. We shouldn’t underestimate the technical challenges for data sharing. There are still some technical barriers. But the Integrated Data Service and more discussion about interoperability are encouraging. There was some discussion around how solvable technical barriers are – some thought ‘almost always’, if you go to market for the right solutions and skills that don’t exist within the government, but some of these skills can be quite scarce (and we returned to whether the private sector was better than the government at this).
- **Data protection officers.** There was some worry about the proposal to remove the requirement for data protection officers, ‘because doing data governance is really hard. It takes a while to get that balance right between the carrot and the stick in an organisation, and to be able to talk to senior executives’ about data issues.
- **Digital resignation** Defined as ‘where people just give away their personal data, because they don’t feel like they’ve got any other alternative’. Can the consultation address that in some way?
- **A government perspective.** Government representatives noted that while public servants were generally able to find ways to share data – particularly health data – that were necessary and proportionate, there were some occasions which created more difficulty as to whether something would be permissible or not. The changes to the Digital Economy Act were described as minor changes to allow access to government health data and improve the services that government provides to businesses. In general, the emphasis throughout the consultation is less about changing the law, and more about trying to bring it into one place, providing greater

clarity for government departments and other organisations about how those provisions work.

- **The importance of dialogue and deliberation.** 'I think this conversation is proof that sophisticated conversations about data sharing and data take place across government as well as between government and stakeholders.'