Data Use and Access Bill: Clubcard culture in Government

The Bill was laid in Parliament one day with the press release supposedly embargoed for 00:01 that night, but the Bill text was posted by Parliament at 6pm. There is no better illustration of the stupid games that Governments (of whatever colour) play around data secrecy and around the digital centre of government.

Much of the Bill text is identical to that first laid by Nadine Dorries in 2022 – three Prime Ministers ago. Her gifts to the Tory right remain in the Bill, such as the ability to reuse data for any "research" purpose without further thought, unless that purpose is "public health" (and only public health). "Change" has not come to the Bill, or to Ministers who are still using the same talking points the civil service wrote for Nadine.

The Bill is minor 'tweaks' to embed a culture of 'Clubcard spam' in the UK's data ecosystem, ensuring that what happens to your data is not entirely within your knowledge or control. Even where there are no changes to the substantive text of the Bill, the descriptions have changed radically, lines disappearing like "businesses gaining at the expense of consumers"[1] and "The Bill has been co-designed with industry, for industry"[2] but where the legislative text remains identical. We also echo specialist concerns of others.[3]

Many data abuses from the last decade will be legalised under this Bill – processing has to be "in the public interest" *only* if for "public health";[4] no other use has that constraint (see probing amendments to Clause 67)**.** Will Schedule 12 be applied to Palantir or large GP suppliers?

The Bill allows "legitimate interest" to be used to track you online (clause 70[5]), then "research" to identify how to most exploit the vulnerable (cl 67-68), and a "legitimate interest" to send junk mail and spam (cl 70 (4) (11)). That includes explicitly targeting the vulnerable[6] – victims of strokes or cognitive impairment – in pursuit of profit (as we have seen before[7]).

The most important clauses for health data are 66-68 and 119, which we deal with first before going clause by clause. (for those who've read this briefing three times now, the numbers change, the text is largely the same, except for the "Social Media Resarch" and "Missing from the Bill" section on the last page which has changed).

---

[1] https://twitter.com/peterkwells/status/1634896811747086339
[2] How the Bill was previously described in a King's Speech https://assets.publishing.service.gov.uk/media/6…7/The_King_s_Speech_ background_briefing_notes.pdf
[3] NAT, Genewatch, and others. Chris Pounder has also a long series of deep analyses on his site.
[4] It seems DeSIT has not *entirely* forgotten the recent pandemic. But why protecting the public from abuses in such an scenario doesn't apply to protecting them in every other scenario is unstated.
[5] The previously much hyped changes around "cookie banners".
[6] Data used for the purposes of public health has a "public interest" requirement in clause 67(1)(b)(3)(b), but anything that is not public health does not have that requirement in 67 (1)(b)(3)(a).
[7] e.g. https://pharmaceutical-journal.com/article/news/pharmacy2u-fined-130000-for-selling-patient-data and others: https://medconfidential.org/for-patients/major-health-data-breaches-and-scandals/

66-68: Eugenics as “research that can reasonably be described as scientific”?

Clauses 66-68 are the original Bill’s clause 1-3, unchanged apart from the renumbering. Biobank, now infamous for handing their data to racists, gave evidence last time (q85) in support of these clauses. cl67 (1) (b) (2) says that anyone who thinks they’re doing scientific research by definition is (including the eugenicists Biobank remains happy to have handed their data to).

cl 67 (1) (b) (3) a and b, if someone is doing public health work they have to do a public interest test, if they're not doing public health it’s a free for all. This was a give away by Nadine Dorries to the Tory right who didn’t want to allow more public health research in the original bill. Labour didn’t spot/care that it’s there.

There should be a drafting change to mean the public interest obligation applies to all in clause 67, and at the Despatch box it should be made clear that open access research carried out in line with ethical approval is what is meant by research. Of course, that’s what’s already meant by research, so the Bill doesn’t help anyone but racists. Is that the point?

The narrow definition of “identifiability” in the Bill means data that a company has access to in the course of their normal business can be reused if they deliberately ignore attention to details. This is likely to cause a high risk to every contract the NHS has, especially those in which data has previously been unmentioned due to the soon to be repealed protections of the Data Protection Act. Additionally, the proposal that the UK also moves into the US led Cross Border Privacy Regime means every such contract will now be even more ambiguous.

Baby blood spot tests are retained long beyond the 5 years parents may have given consent for, with no recourse or redress to prevent data being used for purposes they did not expect, such as “research” by Chinese military-linked firms, because, "scientific research only uses anonymised data". This Bill legalises such retention, transfers, and broad uses. Around the collapse of 23andMe, the US has issued an Executive Order limiting who can buy genomic data on US persons, but there are no protections in the UK, which benefits biobank and Our Future Health who will sell what they have to anyone who’ll pay them money.

Formally in official data usage registers, or more comprehensibly at TheySoldItAnyway.com, NHS England policy is that when data is deemed “anonymous” in NHS England’s view, the choice of patients to dissent from those uses is entirely ignored. The Bill makes that data open to even more misuse, as if you know an individual had a kidney removed in a particular week in 2021, you can use that one key and the pseudonym to unlock and read their entire medical history.

Clause 119 (Schedule 12) are powers to censure NHS IT providers for not doing exactly what NHS England wants. The words are *entirely* unchanged[8] from the last Government which wrote them to provide a legal basis for talking about the commercial priorities of one particular IT supplier. The new Government has been proactive saying this Bill does many new things that aren’t there; why?

[8] The words are unchanged, but there are visual changes to whitespace and font, as if the generation system changed in the intervening years. The new PDF is nicer.

While this Bill may move many dodgy uses of data outside of the data protection regime via "anonymisation" (ie outwith the ICO responsibility), it will not, and can not, move political responsibility for abuses of NHS data away from Ministers and Government. Ministers will remain accountable to the House for the actions of data DHSC and associated public bodies collect and share, only now it will be at higher risk of scandal with reduced punishments for misuse, especially around medical records. NHS England's continuing claims of "pseudonymisation" being a panacea for ignoring patient dissent while the data also remains personal data demonstrate that the policy legacy is incoherent.

Rest of the Bill:

Part 1 – "Smart data" powers have sensibly been renamed, but there continues to be no requirement or provision for data subjects to easily exercise their right to object to unnecessary processing under those clauses. The "financial interfaces" powers continue to be open to abuses by creepy landlords who want to snoop on their tenants – the only thing that has changed since our earlier briefing on the topic is the clause number: now cl14-17.

Part II – Identity

While the Bill repeatedly refers to "Digital Verification Services" and "DVS", it is notable that the current 'beta' version of the Framework itself (still[9]) makes *not a single mention of either term*. In itself, this is only a minor point – but it is indicative of the far wider and deeper problems past Governments have had over decades in (not) defining important terms or key concepts consistently; or at all. We have seen no evidence this has changed, but these two short questions (requiring long answers) may show that Change has come to Identity policy:

- **Will Ministers confirm in writing that and how the current Home Office use of the framework is compliant with Part II of the Bill as currently written.** (ie have they fixed the problems we outlined at length in 2022)

- **Will Ministers confirm in writing how these Digital Verification Services to be managed by DSIT will interoperate with the digital Identity Verification services being offered by DSIT within the Gov.UK Login programme?**

Clause 85: Dissent

Research is vital and necessary, but a data subject has a moral and legal right to dissent from their data being used for unnecessary purposes – which includes research, especially research to which they have an objection. In the NHS and research with health data, that dissent is the National Data Opt-Out. ***How is a patient's / constituent's / data subject's lawful and moral right to dissent enshrined in this clause?***

The inability to object to data being used for statistical purposes is balanced by the narrowness of those purposes. The Bill however appears to create a loophole where data

[9] We mentioned this to DCMS when the Bill first came out in 2022, they've not fixed it.

can be *required* for statistics without dissent being respected, and then *re-used* for research purposes – purposes that would have had to respect dissent if the data had been collected directly. Allowing data to be processed by 'piggybacking' the reputation of and confidence in the statistical system and its vital purposes is a recipe for collapsing public trust.

Question: What happens in the case that this clause is breached?

> "85 (2) (84B) (1) (b): Processing of personal data for RAS purposes must be carried out in a manner which does not permit the identification of a living individual."

This is a simple question for Ministers that we'd like in Hansard.

Clause 29, 82–83 & 92 : Everyone gets to write their own Codes

While Codes of Practice on particular topics are welcome, this Bill says "The Commissioner **must encourage** expert public bodies to produce codes of conduct" remains a gift to special interests and the most committed lobbyists to undermine the safeguards of the Bill, especially given the loopholes of data reuse. Of course, those bodies will be lobbied to write their own codes of conduct anyway, and the Commissioner should address them solely on their content.

While we do not propose amending this clause, it does show how the culture of the Commission will be different after this Bill is passed.

Note, that the title of section 83 is "Law enforcement processing and codes of conduct", it is unclear which, if any, of those rules is limited to law enforcement processing. This may be a drafting error from the eternal tweaking of versions of the Bill. The changes does not appear to be limited to law enforcement part of the Data Protection Act, and NPCC should not be writing data protection rules for police forces (they write the guidance on the rules; the ICO remains the regulator).

Interactions of Clauses 1, 66-68 & 85 – enabling the culture of 'Clubcard spam'

While some broad rationales were given in the Bill's impact assessment,[10] and over two years on from initial publication, we have seen no assessment of the *interactions* of clauses 1, 66-68, 85 *together, in practice* (the numbers change, the interactions stay the same).

Would they, for example, allow personal data provided for a specified purpose to be 'laundered' through (e.g. market) "research", and thereby made available for processing activities which, had they been conducted directly, would have been dissentable (or simply unacceptable)? The expansion of "legitimate interests" suggests so.

It is loopholes and 'back doors' like this to which people strongly object; possibly lawful, but publicly unacceptable, secretive uses which have caused multiple government data programmes to blow up, with consequent serious losses of public trust and confidence.

---

[10] e.g. paras 35(a) & (b): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091814/Data_Protection_and_Digital_Information_Bill_Impact_Assessment.pdf

While the majority of researchers are legitimate, the use of “research” as a figleaf is a reputational risk for legitimate research from nefarious activities who want to get the type of personal benefits that come from a clubcard culture. The public will see the spam, and see the junk mail, and be told “this is from research”.

The explicit removal of the “public interest” test[11] for data sharing makes this even more concerning.

Social Media Research

Not all social media is public. Different networks work differently, and it is possible on (e.g. facebook) to have two consecutive posts from the same person one of which is in a very narrow limited group discussing sensitive health information, and another on an entirely different topic posted more widely. The data subject’s intent must factor into decisions about sharing.

When access to data for research is granted, researchers must not be able to receive the most sensitive updates people write for their closest confidants, next to public posts which are immediately findable via search engines. Will individuals be able to object to the unnecessary processing that is bona fide research? Will research projects be disclosed to those who form part of the dataset upon which that research is done? Will the findings of that research be available to everyone, or will special-interest funded briefing papers only be available to those who the special-interests choose?

These problems are solvable, but there must be a recognition from Parliament that these issues need to be addressed reflecting the sometimes unique designs of each platform, rather than adopting the extremist positions held by some lobbyists that because a teenager may be involved then Mark Zuckerberg or Elon Musk should have full parental obligations to share it with anyone.

With all the focus outwith the Bill on data sharing around Government, and from the commercial sector to Government, perhaps there should be a wider discussion about simpler methods of objecting to processing which are more widely respected.

Missing from the Bill

Speaking on Radio4, Stephen Kinnock said the Bill would provide a “cast iron guarantee” on who could access patient data. Which bit of which clause was he talking about? Because it’s not in the Bill.

We're sure Ministers believed "the government was "absolutely committed" to protecting patient data" when they said it, but that’s only what they say, and what they have done is nothing at all, besides say they will make the single patient record and medical notes

[11] About DPDI but text remains: https://amberhawk.typepad.com/amberhawk/2022/08/dpdi-bill-removes-public-interest-test-in-push- to-legitimise-general-public-sector-data-sharing.html

available to anyone in any place that shows the NHS logo, with no way to find out when and where they were accessed.

We therefore would seek confirmation from Government that despite this Bill being over two years old, no additional powers are going to be snuck in during Committee stage when it's too late for meaningful scrutiny.

We welcome that the Bill does not abolish the Biometrics and Surveillance Camera Commissioner post(s). With the expanding use of surveillance cameras in the emergency services and hospitals, the new Government should commit NHS public bodies to following the Surveillance Camera Commissioner's Code of Practice. The previous Government refused.

AI and Data Trusts are not in the Bill, and *nor should they be:* There is no legal or written standard on the core features of a data trust. This means there is little oversight of what guarantees their trustworthiness and ample room for diverging practices and standards. Similar, while there is a lot of good work going on about AI accountability (and work of other kinds), none of it is ready for the statute book (and none of which remains ready years after we first wrote these words).

medConfidential
October 2024