medConfidential Briefing on the Data Protection and Digital Information Bill: Profiting off a culture of 'Clubcard spam'

Far from "cementing post-Brexit Britain's position as a science and tech superpower",[1] the Data Protection and Digital Information Bill is more a set of 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**.

The 2023 Bill allows "legitimate interest" to be used to track you online (clause 79[2]), then "research" to identify how to most exploit the vulnerable (clause 2), and a "legitimate interest" to send junk mail and spam (clause 5 (4) (9)). That includes explicitly targeting the vulnerable[3] – victims of strokes or cognitive impairment – in pursuit of profit (as we have seen before[4]).

Many recent health data abuses will be legalised under this Bill – processing has to be "in the public interest" *only* if for "public health";[5] no other use has that constraint.

One does not "strengthen" protections and safeguards by removing them, or watering them down;[6] one does not "help British businesses trade abroad" by putting adequacy at risk;[7] nor does one inspire "confidence" or create certainty by handing the Secretary of State an arsenal of Henry VIII powers.[8]

It's 2023, not 1522 – and people are not dumb about data; they can tell when things are being made worse for them, even when Ministers fly the banner of 'better for business'. Cock-up[9] after cock-up,[10] broken algorithms,[11] giant data grabs,[12] getting into bed with 'data mercenaries',[13] and other harebrained schemes,[14] the citizens to whose personal data this Bill relates will no longer accept "Just trust us", being increasingly well-attuned to the "creepy line".

On process, we are concerned about the introduction of significant amendments to the Bill at a point when it is too late to remove them, just as happened with what is now sections 191-194 of the Data Protection Act 2018, which – though the Government argued their necessity – *remain entirely unused*. Given the reintroduction of this Bill, and the small amendments that were made, there should be no need for late-introduction of new clauses.

---

[1] As described by former Secretary of State, Nadine Dorries, in her (pre)announcement of the first Bill in June, and repeatedly since then under the current government.
[2] The much hyped changes around "cookie banners".
[3] Data used for the purposes of public health has a "public interest" requirement in clause 2(4)(b), but anything that is not public health does not have that requirement in 2(4)(a).
[4] 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/
[5] 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.
[6] e.g. on Article 22: https://twitter.com/jennifercobbe/status/1549098376821628933
[7] https://techmonitor.ai/policy/privacy-and-data-protection/uk-data-protection-digital-information-bill
[8] cf. criticism as noted in 'What the Bill doesn't do': https://www.mishcon.com/news/the-data-protection-and-digital-information-bill-an-initial-view and https://www.mishcon.com/news/the-new-data-protection-reform-bill-same-as-the-old-bill
[9] https://twitter.com/EinsteinsAttic/status/1297640499583619072
[10] https://twitter.com/medConfidential/status/1357037423172141061
[11] Everything that went wrong with the botched A-Level algorithm wired.co.uk/article/alevel-exam-algorithm
[12] https://medconfidential.org/whats-the-story/
[13] https://opendemocracy.net/en/ournhs/we-must-be-told-what-cummings-and-palantir-are-doing-nhs-data/
[14] https://www.thebureauinvestigates.com/stories/2021-04-19/home-office-algorithm-sham-marriages

Interactions of Clauses 1, 2, 3, 22 and 79 – enabling the culture of 'Clubcard spam'

While some broad rationales are given in the Bill's impact assessment,[15] and nearly a year on from initial publication, we have seen no assessment of the *interactions* of clauses 1, 2, 3, 22, and 79 *together, in practice*.

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.
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[16] for data sharing makes this even more concerning.

Clause by Clause

Clause 1: Scope of the Bill and Defining personal data, again

What is and is not personal data was a major point of contention in DPA 2018, and it is a credit to the Government that the topic made it into clause 1.

We would, however, like to probe the details of what this means:

1) This being clause 1, and given the desire of this Government that Regulators and the Judiciary do only what Parliament intended, can the Government explicitly confirm that personal data that is pseudonymised (in part, but in which other indirect identifiers are unaltered) will remain personal data after this clause is passed?

2) Can the Government also confirm that if an assessment is made that some data is not personal data, and that assessment is later shown to be incorrect, then the data will have been personal data at all times and should be treated as such by controllers, processors, and the (then) Information Commission?

---

[15] 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
[16] https://amberhawk.typepad.com/amberhawk/2022/08/dpdi-bill-removes-public-interest-test-in-push-to-legitimise-general-public-sector-data-sharing.html

Clauses 2 & 3: Purpose limitations removed

While there are specific safeguards for ethical scientific research, there are no bars to reuse from less ethical projects that often appear as “research and development” or “market research”.

Probing amendment:

Insert into Clause 3 (3) (7) as new item (c):

(c) the data subject has been given the opportunity to express dissent and has not done so, and

Explanation: To make clear that when the purpose limitations are changed, that does not reduce or weaken the obligations around dissent.

Clauses 7-10: Increasing fees[17] and reducing the rights of data subjects

Following the pattern of the “Bill of Rights Bill”, these clauses reduce the access to rights of data subjects by erecting barriers and fees to access at the discretion of the data controller. Truly a Clubcard culture for data.

Clause 11: Automated decision making

Automated decision making,[18] especially about health, must recognise bias and the removal of rights for culture of clubcard spam will cause harm when those decisions are about health.

Clauses 15-18: Records of processing and DPIAs

Article 30 Records of Processing Activities (ROPAs) are to be replaced by a lesser requirement to have a "Record of Processing of Personal Data" (clause 15). At clause 17, Data Protection Impact Assessments (DPIAs) will become Assessments of High Risk Processing - again, much leaner and less prescriptive than the existing requirements. Added to this, in the context of DPIAs, at clause 18 controllers will no longer be required, under Article 36 UK GDPR, to consult the Information Commissioner's Office on certain high risk DPIAs – instead, they will merely be permitted to do so.

Given past issues with unpublished and inadequate DPIAs, weakening the process is foolhardy. The NHS will have to add them back via contracts and other paperwork, which will involve amending a lot of agreements.

[17] https://twitter.com/jennifercobbe/status/1549096589146423300
[18] Others will write far more on this topic, and we have little meaningful to add.

Clause 22: 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 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.

1) **Probing amendment 1: Respect dissent:**

   Insert into Clause (22) (2) (1) after "data", ", where the data subject has been given the opportunity to express dissent"

   Explanation: To make clear that when the purpose limitations are changed, that does not reduce or weaken the obligations around dissent.

2) **Probing amendment: What happens in the case that this clause is breached?**

   "22 (2) (84B) (2): Processing of personal data for RAS purposes must be carried out in a manner which does not permit the identification of a living individual."

   Explanation: To ensure that if the safeguards are breached, the ability to process data in this way does not still apply.

3) **Probing amendment: What happens in the case of explicit dissent by data subjects?**

   Insert into 22 (84C) as:

   > "(6) The requirement is not satisfied unless applicable dissents by the data subject are respected."

   Explanation: To ensure existing patient dissents are respected and cannot be ignored.

Clause 30: Everyone gets to write their own Codes of Practice

While Codes of Practice on particular topics are welcome, that this Bill says "The Commissioner **must encourage** expert public bodies to produce codes of conduct" is 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.

Clauses 46-60: Identity

We address Part 2 of the Bill in a separate, Part-specific briefing.

Clauses 61-77: Is GP Data 'Smart Data'?

Noting the scope of clause 99, general practices would appear to meet the definition of "trader" in clause 61(2). Do the 'Smart Data' provisions apply to NHS contractors? Do they apply to care homes?

Clause 92: Relating to the Digital Economy Act

It is welcome that none of the hairbrained data schemes around the DEA were in a fit state to make it into the Bill. The clause to add businesses into scope of the DEA in the same way as it already covers people is entirely sensible and unobjectionable.

However, even after the 8 month delay in the text of this clause, we remain very concerned about other surprises being snuck into the Bill part way through the process.

We have asked the Cabinet Office for a list of the subgroups that have been looking at possible extensions to the Digital Economy Act, but CO refused that request,[19] despite admitting in published minutes that they exist.

The recent consultation on "identity verification" powers under the DEA was a complete shambles.[20] (note, that identity consultation is entirely different to the identity powers in this Bill).

Rather than using DEA powers (or this Bill), the wider government response to future pandemics or similar emergencies should be dealt with in the DHSC review of COPI and sit under the Chief Medical Officer's authority. In short, as the NHS and health system were able to respond under COPI acting under the CMO's authority, that authority should extend to the rest of government too (since the CMO is the principal health advisor to the Prime Minister and a civil service permanent secretary in the Department of Health). Any changes in this Bill would be premature and pre-empt the specific primary legislation that is expected to be drafted and discussed in due course.

Clause 99: Information Standards for Health and Social Care

We welcome clause 251ZC, but note that 251ZE seems to imply that DHSC and NHS England will have the powers to take over the information infrastructure of Social Care. This is a major policy shift that seems unusual to sneak through in clause 99 of an unrelated Bill.

[19] https://www.whatdotheyknow.com/request/subgroups_of_the_dea_review_boar#incoming-2072525
[20] https://medconfidential.org/wp-content/uploads/2023/02/DEA-identity-consultation-response.pdf

Clauses 104-106[21]: Revocation of sections of the Protection of Freedoms Act

Noting the use of this Bill to revoke sections of the Protection of Freedoms Act 2012, and as members of the Independent Advisory Group to the National Police Chiefs' Council on Automatic Number Plate Recognition (ANPR IAG), we support an amendment which will place ANPR on a statutory footing.

DeSIT/ICO may wish to clarify the future of oversight of biometric materials (104) which aren't just for forensic use, as most biometric databases (106) are certainly becoming wider than just forensics (such GOV.UK One Login, NHS Login, etc). DeSIT should also be aware, in a way that is likely to be more meaningful to them than it was to DCMS, that the definition in 106(13) means this covers whole genome sequencing database, which has a whole can of worms may be better entirely excluded.

DeSIT may wish to consider stating that, in the new Information Commission, there is expected to be a commissioner responsible Surveillance Cameras replacing functions of the existing external commissioner(s). How that works in practice will be up to the next Information Commission, but someone will have to take on responsibility for the Codes of Practice, and it makes sense for that to be the Information Commission, with a nominated expert.

medConfidential
March 2023
coordinator@medConfidential.org

Postscript:

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.

[21] It is only after clause 100 where the clause numbers in the 2023 Bill diverge from the 2022 version.