**A Data Preference Service**

Data mining is the new junk calls.

The same way it used to be reasonable to cold call random phone numbers simply because you had (guessed) their phone number, organisations currently think that because they have the ability to use data on you to sell you stuff, they *can* do so. Both approaches make money.

In 2024, “Smarter data” projects seek to link supermarket spending data with DWP / DfE / NHS etc data, on to other data held by industry. The “Smarter Data Council” wants legislation to facilitate data sharing at population scale for benefits that are unclear. “Smarter Data Research” seeks to use those same links for research.

**It is not reasonable to require a citizen to dissent from the work of one umbrella organisation by going to all of its potential members.**

Both “legitimate interest” and “public task” are dissentable when the processing is not *necessary* for the performance of a requested service or a legal obligation – they are not absolute permissions for data sharing, “smart” or otherwise.

Modelled on the precedents of the Telephone Preference Service and the NHS National Data Opt Out, a new Data Preference Service should allow a person to opt out of any regulated data sharing across data controller boundaries, other than to provide them services they have requested:

> “I object to my data being used for purposes other than to provide the services I have requested.”

This would be a broad objection to data sharing. Individual services should either prominently highlight that they use the national service for internal use, or provide their own equivalent opt out for their own internal uses. As with the NHS precedent, responsible organisations would be clear that they voluntarily respect the DPS opt outs on internal uses, irresponsible organisations would continue to be irresponsible.

The filtering must be privacy preserving via a well defined simple interface[1]. The minimum viable service would not be complicated to build and run.

medConfidential
First draft – August 2024
coordinator@medConfidential.org

[1] Following the NHS Digital “MESH” model for the NHS NDOO, a data controller should provide a list of their own unique and random UUIDs for each person whose personal data it holds, and the service provides in response only the UUIDs who should remain in a shared dataset.