Creating an evidence base for data processing by Government

As Minister for the Cabinet Office, Matthew Hancock, (now Secretary of State DCMS) spoke about the public use of data in this way: “Citizens should know how data about them is used in the same way taxpayers should know how taxpayers’ money is spent.”

The debate around the use of personal data by Government is marred with fear and institutional denial. Citizens are afraid how information could be used against them (with good reason: e.g. care.data); civil servants are afraid to use data to (actually) help citizens (with good reason: the press), and processes are dysfunctional on all sides (e.g. ATOS/PIP) mostly through a lack of accurate and impartial information on how data is used.

The best way for a citizen to understand how their data will be used next month, is to see how it was used last month (or, for citizens who have just undergone a significant change in circumstances, publishing information on how data on those who went through that change previously is used). Such information must also be accurate, and trustworthy - the recent case where PHE admitted handing patient data to a tobacco company being a case where statements by a public body turned out to be neither of those things.[1]

The Data Protection Bill allows the Government to, by statute, provide information to the citizen when interacting digitally with public services. There is already a requirement digital services to do so in the Digital Service Standards published by the Government Digital Service, but it is not widely implemented. (It says “Your obligations include:… - making sure users of transactional services have access to data held about them - the service should clearly communicate how data will be used”).

When data projects go wrong - as they often do - there is also a price paid in concern and distress by citizens. A significant percentage of an MP’s casework is from public bodies mishandling data processing - the consequence of a public body making a decision where the evidence a citizen believes they provided is entirely divergent from the stated intent of Parliament. Often, that decision is opaque and unclear, which causes additional distress.

Accountability to a citizen of how data is used is the only way to give the citizen information about how a decision was made - and what data was not considered - to give insight into what happened. Absent evidence, systematic failure (and consequent cost) can not be addressed.

Brexit brings with it the need for many new data processing systems - a possible reason for the complete lack of safeguards in the ‘Framework on Data Processing by Government’ (clauses 185-188). Absent transparency on data flows, it is likely that businesses and citizens will find themselves in kafka-esque situations with these new Brexit systems, just as they regularly do with existing data processing systems, especially those involving the Home Office where processing decisions are also subject to changing political priorities..

---

[1] www.telegraph.co.uk/news/2018/01/15/health-officials-accused-failing-carry-basic-checks-data-cancer/

Probing Amendment:

Into the Code of Practice on Data Sharing

Insert as:

> “122 (b) Where data is derived from an interaction with a digital service of a public authority, the Code shall require that service to allow the data subject to see, on future uses of the service, the reasons for which data was shared, used, processed, or accessed, for purposes other than under Parts 3 & 4 of this Bill”

Explanation: *In line with the statements of Ministers, the Framework should citizens should be able to see how public bodies process their data.*

Extra note: this is probably not the right place for it to go into the Bill - since it is wider than just data sharing - although the likelihood is that Government will not want this to be statutory, but put in a Code of Practice somewhere (which is likely the right outcome).

medConfidential