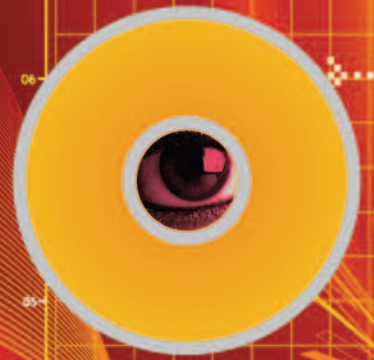# Database State

A REPORT COMMISSIONED BY THE JOSEPH ROWNTREE REFORM TRUST LTD.

Executive Summary and Recommendations

In recent years, the Government has built or extended many central databases that hold information on every aspect of our lives, from health and education to welfare, law–enforcement and tax. This 'Transformational Government' programme was supposed to make public services better or cheaper, but it has been repeatedly challenged by controversies over effectiveness, privacy, legality and cost.

Many question the consequences of giving increasing numbers of civil servants daily access to our personal information. Objections range from cost through efficiency to privacy. The emphasis on data capture, form-filling, mechanical assessment and profiling damages professional responsibility and alienates the citizen from the state. Over two-thirds of the population no longer trust the government with their personal data.

This report charts these databases, creating the most comprehensive map so far of what has become Britain's *Database State*.

All of these systems had a rationale and purpose. But this report shows how, in too many cases, the public are neither served nor protected by the increasingly complex and intrusive holdings of personal information invading every aspect of our lives.

The report assesses 46 databases across the major government departments, and finds that:

- A quarter of the public-sector databases reviewed are almost certainly illegal under human rights or data protection law; they should be scrapped or substantially redesigned. More than half have significant problems with privacy or effectiveness and could fall foul of a legal challenge.

- Fewer than 15% of the public databases assessed in this report are effective, proportionate and necessary, with a proper legal basis for any privacy intrusions. Even so, some of them still have operational problems.

- Britain is out of line with other developed countries, where records on sensitive matters like healthcare and social services are held locally. In Britain, data is increasingly centralised, and shared between health and social services, the police, schools, local government and the taxman.

- The benefits claimed for data sharing are often illusory. Sharing can harm the vulnerable, not least by leading to discrimination and stigmatisation.

- The UK public sector spends over £16 billion a year on IT. Over £100 billion in spending is planned for the next five years, and even the Government cannot provide an accurate figure for cost of its 'Transformational Government' programme. Yet only about 30% of government IT projects succeed.

The Database State – scrap it, fix it or keep it?

This report surveys the main government databases that keep information on all of us, or at least on a very substantial minority of us, and assesses them using a simple traffic-light system.

Red means that a database is almost certainly illegal under human rights or data protection law and should be scrapped or substantially redesigned. The collection and sharing of sensitive personal data may be disproportionate, or done without our consent, or without a proper legal basis; or there may be other major privacy or operational problems. Most of these systems already have a high public profile. One of them (the National DNA Database) has been condemned by the European Court of Human Rights, and both the Conservative Party and Liberal Democrats have promised to scrap many of the others.

The red systems are:

- the **National DNA Database**, which holds DNA profiles for approximately 4 million individuals, over half a million of whom are innocent (they have not been convicted, reprimanded, given a final warning or cautioned, and have no proceedings pending against them) – including more than 39,000 children;

- the **National Identity Register**, which will store biographical information, biometric data and administrative data linked to the use of an ID card;

- **ContactPoint**, which is a national index of all children in England. It will hold biographical and contact information for each child and record their relationship with public services, including a note on whether any 'sensitive service' is working with the child;

- the NHS **Detailed Care Record**, which will hold GP and hospital records in remote servers controlled by the government, but to which many care providers can add their own comments, wikipedia-style, without proper control or accountability; and the **Secondary Uses Service**, which holds summaries of hospital and other treatment in a central system to support NHS administration and research;

- the electronic **Common Assessment Framework**, which holds an assessment of a child's welfare needs. It can include sensitive and subjective information, and is too widely disseminated;

- **ONSET**, which is a Home Office system that gathers information from many sources and seeks to predict which children will offend in the future;

- the DWP's cross-departmental **data sharing** programme, which involves sharing large amounts of personal information with other government departments and the private sector;

- the Audit Commission's **National Fraud Initiative**, which collects sensitive information from many different sources and under the Serious and Organised Crime Act 2007 is absolved from any breaches of confidentiality;

- the **communications database** and other aspects of the Interception Modernisation Programme, which will hold everyone's communication traffic data such as itemised phone bills, email headers and mobile phone location history; and

- the **Prüm Framework**, which allows law enforcement information to be shared between EU Member States without proper data protection.

Amber means that a database has significant problems, and may be unlawful. Depending on the circumstances, it may need to be shrunk, or split, or individuals may have to be given a right to opt out. An incoming government should order an independent assessment of each system to identify and prioritise necessary changes.

There are 29 amber databases including:

- the **NHS Summary Care Record**, which will 'initially' hold information such as allergies and current prescriptions, although some in the Department of Health appear to want to develop it into a full electronic health record that will be available nationally. In Scotland, where the SCR project has been completed, there has already been an abuse case in which celebrities had their records accessed by a doctor who is now facing charges. The Prime Minister's own medical records were reported compromised. There is some doubt about whether patients will be able to opt out effectively from this system, and if they cannot, it will be downgraded to red;

- the **National Childhood Obesity Database**, which is the largest of its kind in the world, containing the results of height and weight measurements taken from school pupils in Year 1 (age 5–6) and Year 6 (10–11) since 2005. This database is simply unnecessary;

- the **National Pupil Database**, which holds data on every pupil in a state-maintained school and on younger children in nurseries or childcare if their places are funded by the local authority, including: name; age; address; ethnicity; special educational needs information; 'gifted and talented' indicators; free school meal entitlement; whether the child is in care; mode of travel to school; behaviour and attendance data. It is planned to share this data with social workers, police and others;

- **Automatic Number Plate Recognition** systems, which are operated by multiple agencies - the Highways Agency, local authorities, police forces and private firms – and will read 50m plates covering 10m drivers each day;

- the **Schengen Information System**, a European police database that lists suspects, people to be denied entry to Europe, and people to be kept under surveillance. It is due to be replaced with an updated SIS-II which will also store biometric data such as fingerprints; and

- the **Customer Information System** of the Department for Work and Pensions which describes it as "one of the largest databases in Europe". It makes 85 million records available to 80,000 DWP staff, 60,000 staff from other government departments, and 445 local authorities – whose staff are already abusing their access to it.

Green means that a database is broadly in line with the law. Its privacy intrusions (if any) have a proper legal basis and are proportionate and necessary in a democratic society. Some of these databases have operational problems, not least due to the recent cavalier attitude toward both privacy and operational security, but these could be fixed once transparency, accountability and proper risk management are restored.

- Green databases include the police **National Fingerprint Database** and the **TV Licensing** database.

Six years into the Transformational Government programme, the number of green databases is now shockingly low. Of the 46 databases assessed in this report, only six are given a green light.

So what do we do?

Based on a comprehensive analysis of Britain's database state, the report makes the following recommendations for how data should be collected, held and managed by government.

- The databases that this report has rated as 'Red' should be scrapped or redesigned immediately. 'Amber' databases should be subject to an independent review to assess their privacy impact and any benefit to society they may have.

- Sensitive personal information should normally only be collected and shared with the subject's consent – and where practical people should opt in rather than opting out.

- Government should compel the provision or sharing of sensitive personal data only for strictly defined purposes, and in almost all cases, sensitive data should be kept on local rather than national systems.

- Individuals should be able to enforce their privacy in court on human-rights grounds without being liable for costs – the state has massive resources to contest cases while the individual does not.

- Citizens should have the right to access most public services anonymously. We have been moving from a world in which departments had to take a positive decision to collect data, to one where they have to take a positive decision not to. This needs to be challenged.

The report also makes a further set of recommendations on how government should go about developing and building IT systems more effectively in the future.

- The procurement and development of new database systems should be subject to much greater public scrutiny and openness.

- Civil servant recruitment and training should aim at selecting and developing those with the ability to manage complex systems.

- The threshold for referring IT projects to complex OJEU procurement procedures should be raised to £10m from the current limit of only £130,000 – this will favour medium-sized systems rather than unmanageable large projects.

- The government should make its Chief Information Officer a Permanent Secretary reporting to a senior cabinet minister.

- There should never again be a government IT project – merely projects for business change that may be supported by IT. Computer companies must never again drive policy.

Database State was written by a team from the Foundation for Information Policy Research that included some of Britain's foremost experts in information systems and human rights.