Database State

A REPORT COMMISSIONED BY THE JOSEPH ROWNTREE REFORM TRUST LTD.

Ross Anderson
Ian Brown
Terri Dowty
Philip Inglesant
William Heath
Angela Sasse

Published by the Joseph Rowntree Reform Trust Ltd.
The Garden House, Water End, York, YO30 6WQ
www.jrrt.org.uk

Company registered in England No. 357963

ISBN 978-0-9548902-4-7

Contents

Foreword

In October 2007 Her Majesty's Revenue and Customs lost two discs containing a copy of the entire child benefit database. Suddenly issues of privacy and data security were on the front page of most newspapers and leading the TV news bulletins. The old line 'if you have nothing to hide, you have nothing to fear' was given a very public rebuttal. The millions of people affected by this data loss, who may have thought they had nothing to hide, were shown that they do have much to fear from the failures of the database state.

In the wake of the HMRC fiasco, and all the subsequent data losses that came to light in the months that followed, the Joseph Rowntree Reform Trust sponsored a meeting of academics and activists with an interest in privacy. These experts attempted to map Britain's database state, identifying the many public sector databases that collect personal information about us. The task proved to be too big for one seminar, highlighting the need for a more in-depth study of the 'Transformational Government' programme. The Trust, therefore, commissioned the Foundation for Information Policy Research to produce this report, which provides the most comprehensive map of Britain's database state currently available.

Of the 46 databases assessed in this report only six are given the green light. That is, only six are found to have a proper legal basis for any privacy intrusions and are proportionate and necessary in a democratic society. Nearly twice as many are almost certainly illegal under human rights or data protection law and should be scrapped or substantially redesigned, while the remaining 29 databases have significant problems and should be subject to an independent review.

We hope this report will help to highlight the scale of the problem we are facing and inform the ongoing debate about the sort of society we want to live in and how new information systems can help us get there.

David Shutt
Lord Shutt of Greetland

Chair of the Joseph Rowntree Reform Trust Ltd.

March 2009

About the Authors

Ross Anderson chairs the Foundation for Information Policy Research. He is Professor of Security Engineering at Cambridge University, a Fellow of the IET and the IMA, and a pioneer of the economics of information security.

Ian Brown is a senior research fellow at the Oxford Internet Institute, with a PhD in information security. He is a member of the Advisory Council and a former Director of the Foundation for Information Policy Research.

Terri Dowty is Director of Action on Rights for Children. She has many years' experience in education and children's human rights. She sits on the Advisory Council of the Foundation for Information Policy Research.

William Heath chairs Open Rights Group and two new start-ups: Mydex CIC and Ctrl-Shift Ltd. He founded the public-sector IT research business Kable, now part of Guardian News & Media. He also sits on the Advisory Council of the Foundation for Information Policy Research.

Philip Inglesant is a postdoctoral researcher at University College London specialising in the human aspects of information systems and e-government.

Angela Sasse is Professor of Human Centred Systems at University College London, specialising in how to design and implement novel technologies that are fit for purpose and that benefit individuals and society. She is also a member of the Advisory Council of the Foundation for Information Policy Research.

About the Joseph Rowntree Reform Trust Ltd.

The Joseph Rowntree Reform Trust Limited, founded in 1904 by the Liberal, Quaker philanthropist, Joseph Rowntree, was set up as a company which pays tax on its income and is therefore free to give grants for political and campaigning purposes, to promote democratic reform, civil liberties and social justice. It does so by funding campaigning organisations and individuals who have reform as their objective, and since it remains one of the very few sources of funds of any significance in the UK which can do this, it reserves its support for those projects which are ineligible for charitable funding. The Trust aims to correct imbalances of power, strengthening the hand of individuals, groups and organisations who are striving for reform. It rarely funds projects outside the UK, directing most of its resources towards campaigning activity in this country.

Acknowledgements

We received help from a number of people including John Suffolk, Paul Whitehouse, Paul Thornton, Richard Clayton, Douwe Korff, Ruth Kennedy, Eileen Munro, Philip Virgo and Nick Bohm. We are also grateful to Kable for making available to us their market intelligence publications and for input from their analysts Victor Almeida, Michael Larner, Philippe Martin and Stephen Roberts.

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.

Chapter 1. Introduction

It was the loss on 18 October 2007 of 25m child-benefit records that finally made the database state a mainstream issue. The Prime Minister and the Chancellor faced hard questions in the House. The Chairman of Her Majesty's Revenue and Customs (HMRC), Paul Gray, resigned.

The Prime Minister denied at the time that the HMRC failure was 'systemic'. But over the following months the list of public-sector bodies that owned up to losing people's personal details swelled to include the RAF, Navy, MoD, Home Office, police, NHS Trusts, GPs, DVLA, the Department for Work and Pensions, other Whitehall departments and local councils. Those affected include patients, taxpayers, welfare recipients, applicants for driving tests, students, teachers, job applicants, farm workers, prison staff and service personnel. The HMRC episode was anything but an isolated incident. Indeed, on 1 March 2009, the press reported that the Prime Minister's own medical records had been compromised.[1]

Computer security experts had warned for years that building ever-larger databases of personal information, to which ever more people have access, was not sustainable.[2] Information Commissioner Richard Thomas warned in 2004 that Britain was sleepwalking into a surveillance society.[3] In 2006, in a more ominous but less widely reported phrase, he reported that we had woken up in one.[4] He mentioned Britain's 4.2m CCTV cameras, numberplate recognition, Radio Frequency Identification (RFID) tags in shops, Oyster cards, loyalty cards and credit cards, phone tapping, call monitoring and Internet surveillance.

Privacy International now ranks Britain as the most invasive surveillance state and the worst at protecting individual privacy of any Western democracy. Civil servants are now being disciplined or sacked at the rate of one every working day for personal data breaches from HMRC, DWP and the Home Office alone.[5]

How did we get here?

The (conflicting) ambitions to make government 'joined-up' and to make every public service available online date back to the dotcom boom era. Government IT spending increased significantly after that boom ended, with the launch of projects such as the NHS National Programme for IT. But government found targets easier to set than to achieve. As IT projects continued to fall far short of expectations, government focussed – with the McCartney 2001 review, the formation of the Office of Government Commerce and its Gateway process – on project management, procurement and relations with suppliers.

The 2005 Transformational Government IT strategy[6] promised citizens choice and personalisation in their interactions with government. However, this was to be based on centralised databases and data sharing across traditional provider and departmental boundaries. At its heart lay not people, but great collections of data about people.

Meanwhile, two different faces of government were being joined up. One is the public services agenda, which formalises our social compassion. It speaks of customers and choice, cares for vulnerable children, provides health and education, keeps the streets clean and generally seeks to please. The other is the enforcing state, in constant conflict with those who break laws or ignore

regulations. It seeks to exercise coercive control and speaks of enemies, targets, suspects and criminals.

The database state appears to fuse these two together. Increasingly users who should feel like a citizen or customer – responsible and in control – feel instead like a suspect or recidivist: fingerprinted, scanned, and their numberplates recorded as they travel around the country. But, as the police themselves freely admit, policing depends on continued public perceptions of legitimacy and fairness.[7] Technologies such as DNA profiling, databases and even CCTV cannot be dissociated from ethical and social questions.

The database state can undermine people's desire to participate in desirable and socially responsible activities, from seeking confidential advice for teenage health issues to showing co-operative goodwill towards law enforcement. There is an example of the sort of problems that worry professionals in 'Stephen's story' in the box on the next page.

Where are we at the beginning of 2009?

The spate of reviews commissioned post HMRC – O'Donnell, Poynter, IPCC, Burton, Thomas-Walport – have now all reported. Yet ministers remain intent on building increasingly intrusive personalised services around more large centralised databases with a strong element of data sharing. This supertanker will not be turned quickly .

Politically, the Government has started to send confusing signals. The Prime Minister now admits 'we cannot promise that every single item of information will always be safe'.[8] The Home Secretary told MPs the government fully believes in data minimisation[9], while the Transport Secretary claims that not to record everyone's communications data would be 'a licence to terrorists to kill people'.[10] The Transformational Government Minister ducked a question on data leaks by saying that "it is not in our security interests to confirm information regarding electronic attacks against Government IT systems".[11]

There is a sense in the senior civil service and among politicians that the personal data issue is now career-threatening and toxic. No-one who values their career wants to get involved with it. This is irresponsible and short-sighted. Like Chernobyl, the database state has been a disaster waiting to happen. When it goes wrong, some brave souls need to go in and sort it out while others plan better ways to manage things in the longer term.

The HMRC data loss was a wake-up call. But there is no sign of a change in course. Supertankers may take a long time to turn, but nobody has started to turn the wheel yet.

It is against this background that the Joseph Rowntree Reform Trust asked FIPR to undertake this work. The contribution of this report is mainly to map what there is: the following section describes the most important systems, what they do, how they share data and what risks they pose. The final chapter compares what Britain is doing with other countries, provides an analysis, and makes policy recommendations.

Stephen's story

Stephen is fourteen and lives with his mum in Nottingham. He is listed on all the big databases that every youngster is on nowadays: ContactPoint gives links to all the public services he has used; the NHS Care Record Service has his medical records; the National Pupil Database has his school attendance, disciplinary history and test results; he is on the Child Benefits Database, and also on the National Identity Register since he applied for a passport; the Government Gateway has a record of all his online interactions with public services; and the ITSO smartcard he uses for local bus services and discount rail fares has been tracking him ever since his mum refilled it with her bank card. His mother frets about all this – when she was a teenager in the 1980s, things like medical and school records were all kept on paper. And although the family has always kept its phone number ex-directory and always ticks the 'no information' box, they get ever more junk mail. More and more of it is for Stephen.

Like millions of children, he is on a few more databases besides. After an operation to remove a bone tumour, he needed an orthopaedic brace for two years, which brought him into the social care system. As his teachers could see from ContactPoint that he was known to social workers, they expected less of him, and he started doing less well at school. The social care system also led to his being scanned for ONSET, a Home Office system that tries to predict which children will become offenders. The Police National Database told ONSET that Stephen's father – who left home when he was two and whom he does not remember – had spent six months in prison for fraud, so the computer decided that Stephen was likely to offend. When he was with some other youths who got in a fight, the police treated him as a suspect rather than a witness, and he got cautioned for affray.

Ten years later, after he thought he had put all this behind him and completed an MSc in vehicle testing technology, Stephen finds that the government's new Extended Background Screening programme picked up his youthful indiscretion and he can not get the job he had hoped for at the Department of Transport. He tries to get jobs in the private sector, but the companies almost all find excuses to demand EBS checks. Two did not, but one of them picked up the fact that he had been treated for cancer; all cancer data is passed to cancer registries whether the patient likes it or not, and made available to all sorts of people and firms for research. Given the decline in the NHS since computerisation, most decent employers offer generous private health insurance – so they are not too keen to hire people who have had serious illnesses.

Chapter 2.
Survey of Public-Sector Databases

The UK public sector has accumulated an enormous number of databases. For example, the Serious and Organised Crime Agency alone inherited over 500 databases from its predecessor agencies, and hopes to consolidate these into 50–60 over the next five years.[12] Across government as a whole there are thousands of systems.

So the first problem is one of scope – what is the 'database state'?

A narrow view would be to consider only those systems that hold information on most citizens (tax, NHS records, driver licensing, ...). We have taken the broader view that we will cover those systems that will at some time or another hold identifiable personal information on at least a significant minority of citizens. We therefore include children's databases and pensions. We include criminal justice, as about a third of men will acquire a criminal record at some time in their lives.[13] We also cover systems that have been announced but not yet built, such as the National Identity Register and the proposed 'Interception Modernisation Programme' communications database.

In this chapter, we set out these systems by department. There are ever more information flows between departmental systems, and we describe the most important of these – the 'thick pipes' that carry large volumes of data, and the most sensitive flows – as we go along. We use a 'traffic light' system whereby each system is ranked red, amber or green. Our basic yardstick is the European Convention on Human Rights (ECHR), and our assessments look at each system on the basis not just of its likely privacy impact but also of its utility, effectiveness and other risks:

Traffic Light System

green – the underlying system appears basically sound, without any insuperable legal problem, although there may be aspects of governance and management that need improvement;

amber – the system demonstrates significant, worrying failings, and may fall foul of a legal challenge;

red – the system's failings are so significant, or its architecture so inappropriate, that we do not feel this system can be made ECHR-compliant without substantial redesign. Without that we do not feel it should continue, given the likelihood that it will have a negative impact on life in our society.

There will inevitably be omissions and errors in our report; government does not always go out of its way to provide accessible information on systems. There is now a project to catalogue the 'trillions' of pieces of information that the government holds on citizens, but this is admitted to be a 'huge problem' especially for public-facing departments such as health and pensions[14]. We welcome that project, and hope the results are eventually published; in the meantime, the rest of this chapter provides a first draft.

The final chapter, Chapter 3, will present a systematic analysis of the overall direction of policy, together with recommendations for change.

2.1 Department of Health

The Department of Health (DoH) has been central to the Transformational Government programme, with many other departments taking their lead from its 'National Programme for IT' (NPfIT). NPfIT started in February 2002 following a decision by Tony Blair to spend billions on replacing all NHS computer systems with new systems that would share information. Since April 2005, it has been run by an agency of the Department of Health called Connecting for Health (CfH), whose goal is "to bring modern computer systems into the NHS with the aim of improving patient care and services". NPfIT is in serious trouble with systems being delivered years late or not at all, inquiries by several parliamentary committees, and public concerns about the safety, privacy and functionality of a number of systems, which are summarised below.

As health is a devolved matter, the following relates principally to England. The other member countries of the UK have their own health service IT programmes, although these are all less ambitious than the English one and have not run into as many problems.

A report by the Health Committee[15] provides a snapshot of the project at mid-2007, while links to many documents and press reports have been collected online.[16] In what follows we describe the main systems that collect and disseminate personal health information about significant numbers of patients. We start with the national applications, colloquially known as the 'Spine'; the first three of these are operated by BT, the NHS's National Service Provider.[17] We then go on to other central applications and finally the applications run by each Local Service Provider; these are somewhat standardised but run by different contractors in different regions of England.

Population Demographics Service

The Population Demographics Service (PDS) is the NHS's new 'address book', and will eventually replace a number of older local and national systems for patient registration. It contains names, addresses, phone numbers and other basic information about 50m+ patients in England, which it maps to NHS numbers. It also stores information relevant to identifying a patient and accessing their core medical data, such as any password they have set up to deal with call centres, and whether they have consented to share certain types of information.[18] There are over half a million people with an NHS smartcard, and there's a concern that any of them could use this system to locate any NHS patient in England[19] – unless the patient has had the foresight to ask their GP to 'stop-note' them on the system. In addition, many modern systems automatically check patient details against PDS, with the result that its audit trail shows which doctors or other providers have dealt with a patient. This can be highly sensitive (e.g. mental health).

Although registers always existed, they used to be available only to a small number of administrative staff; building registration into many systems and making data available to many people (including patients themselves) puts the model under severe strain. Perhaps one might recast PDS as a simple authentication system, but it is not even clear that identifying all patients at all times is prudent: some patients (e.g. of genito-urinary medicine clinics) may have good reason to seek care under false names, and many others are unable to participate in authentication protocols (being drunk, demented or unconscious). It is also significant that much of the information about children that appears on ContactPoint, and to whose sharing many people strongly object, is also available via PDS. Fresh thinking is clearly needed. *We therefore rate PDS as Privacy impact:* **amber**.

Summary Care Record

The Summary Care Record (SCR), also known as the Personal Spine Information Service (PSIS), will 'initially' hold information such as allergies and current prescriptions that might be of use in unplanned care, although some in the Department appear to want to develop it into a full electronic health record that will be available nationally. It is also planned that SCR data will be viewable by patients using the HealthSpace web portal (which raises issues of coerced access, particularly by women and children). The English project is stalled following pilots in Bolton and elsewhere. These pilots were run on an opt-out basis, with patients given very cursory notification of what was planned; doctors argued that patients should have to opt in and this controversy spread to the media. There has also been controversy about possible police access to the SCR. In Scotland, where the SCR project has been completed, there has already been an abuse case: several celebrities had their records accessed by a doctor who is now facing charges[20], and just as this report was about to go to press, there were further reports that both the Prime Minister and the First Minister of Scotland had had their records compromised.[21]

The Department of Health is moving to a 'consent-to-view' model in which the data will be collected anyway, but made available to clinicians treating a patient if they claim the patient has consented. This is quite the wrong way round: SCR data will be widely available to administrators and civil servants, even where the patient prevents clinicians involved in her care from seeing it. (It is also the model used in the Scottish system). Although the SCR may bring benefits to some patients, it has been blighted by uncertainty over the Department's intentions; the Health Committee commented on the Department's lack of clarity about the record's contents and about consent arrangements, and that the French system worked better. Many clinicians agree and argue that the SCR should be turned into a proper, purpose-designed emergency medical record.

If the SCR collects everyone's health data and makes it available to administrative staff regardless of consent, then it will be unlawful and must be classified red. However, there have been claims that patients wishing to opt out completely will be able to have their records deleted. This system is currently on the borderline, but we propose to give the department the benefit of the doubt for now, and therefore formally assess the SCR as *Privacy impact:* **amber**.

Secondary Uses Service

The Secondary Uses Service (SUS) archives summaries of episodes of secondary care, and is set to acquire significant data from primary care too. By April 2009, "all providers of NHS care will be submitting data to SUS and accessing these data through SUS".[22] Clinical data is harvested from a wide range of electronic and paper sources, including summary and detailed care records; the move to electronic records is seen as a major opportunity to expand its scope and usefulness.[23]

The system's main use is administration – from payments and cost control through tracking compliance with performance targets and from resource planning to answering parliamentary questions.

Its secondary use is to support research, and it is anticipated that the much greater volume and detail of clinical data in the system will enable it to serve many more purposes in medical research. As there is no effective opt-out from SUS, this has given rise to serious debate about confidentiality and consent. Data may be supplied in identifiable form if need be, or pseudonymised; but it is very hard to remove enough information from medical records that patients cannot be identified while still leaving enough for the records to be useful, so some risk of re-identification will usually remain.[24] Not all of the critics of SUS focus on privacy, however: personal control of data is a wider issue than that. The Catholic Bishops' Conference takes the view that religious women should have the ability to prevent their medical information being used for research on abortifacients or in stem cell work.[25]

European law requires that systems which store sensitive personal information such as medical records either have the free and informed consent of the data subject, or be based on specific legal provisions that are sufficiently narrow to make their effect foreseeable; such provisions must also be proportionate and necessary in a democratic society.[26] If they are to be used for research, this must moreover serve a 'substantial public interest' and be 'subject to the provision of suitable safeguards'; and they must be notified to the European Commission and the other EU Member States so that the latter can check if these conditions have been met.[27] This law is grounded in the European Convention on Human Rights and is codified in the Data Protection Directive. The EU's Article 29 Working Party has provided further guidance in the case of medical records, which specifically excludes the use of patient data for research without their consent.[28] It has also recently been elucidated by a judgement of the European Court of Justice, according to which health care staff not involved in the care of a patient must be unable to access that patient's electronic medical record: "What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place."[29]

For these reasons, the use of SUS in research without an effective opt-out contravenes the European Convention on Human Rights and European data-protection law. It is also considered morally unacceptable by millions of UK citizens. For these reasons alone, and quite apart from any privacy concerns about the use of SUS data in administration, we have no choice but to assess this system as *Privacy impact*: **red**.

Electronic Prescription Service

The Electronic Prescription Service (EPS) is already used for millions of prescriptions a year.[30] The problem with electronic prescribing is patient mobility: what if you don't take the prescription to your local chemist? In stage 1 of the project, prescriptions are uploaded from the GP to an EPS database kept on the Spine, and there is a barcode on the actual prescription which the pharmacy uses to download it.[31] In stage 2, the paper prescription will vanish: the patient will be able to turn up at any pharmacy and perhaps show them an ID card. The fact that prescription data is available centrally is not new; the NHSBSA Prescription Pricing Division has a database of all prescriptions written in England in the last five years, which are collected after the fact as pharmacies are paid.[32] But much greater functionality is being built into the new system and many more people have access to it. Stage 2 has not yet got the go-ahead, but assuming it does we would surely rate this as *Privacy impact*: **amber**. (If, as some stakeholders wish, EPS data were to be used for research without consent, this rating would turn to red.)

Out of Hours

Two systems support the care of GPs' patients outside normal surgery hours. NHS Direct (which is being rebranded as NHS Choices) has been going for 8 years and provides a nurse-based telephone triage system. Adastra[33] supports out-of-hours GP service contractors and has been operating for 13 years. Both have large amounts of data on millions of patients.[34] Curiously, although more information is collected centrally than may be necessary for patient care, and it may be retained for longer than strictly necessary, making it available to others for direct care appears to have been a low priority. GPs are upset that half the notifications they get of NHS Direct contacts with their patients arrive by fax. It had been agreed in 2000 to replace this with electronic messaging, to save time and errors, but the project fell victim to NPfIT. *Privacy impact:* **amber**.

Picture Archiving and Communications; Radiology Information

The Picture Archiving and Communications System (PACS) enables X-rays and other medical images to be stored remotely in digital form, and transmitted to where they are needed. A related system, the Radiology Information System (RIS), stores related data such as diagnostic opinions written by radiologists about PACS images. On the one hand, this enables images to be viewed in multiple providers (e.g. in hospital, and in follow-up care at a GP's surgery); on the other, it raises privacy concerns (as anyone can access your images, not just the consultants at the hospital treating you). The loss of network service or of a remote server may make images unavailable, interrupting operations. These systems link to more specialised databases (such as mammography) and specialised research databases (such as on cancer). The problem is that in many parts of the country a patient who refuses to have their image data held remotely cannot receive medical care involving imaging or radiotherapy. This is a clear violation of rights and leaves us with no choice but to assess PACS/RIS as: *Privacy impact:* **amber**.

Choose and Book

This system processes 30–40% of secondary care referrals in England.[35] Referral letters contain personal health information, so there is a facility for sensitive content to be so marked with the result that only the referring clinician, the staff of the service booked to, and that patient, will be able to see details of the appointment or the referral letter.[36] It is not clear why all referrals are not simply treated as sensitive. It is also not clear why referrals need to be centralised at all. For that reason the system should be assessed as *Privacy impact:* **amber**.

Detailed Care Record

The Detailed Care Record (DCR), or Local Details Record, is the centrepiece of NPfIT. It is in essence a multi-contributor record, to which GPs, hospitals, nurses, social workers and others can all contribute. It is supposed to replace traditional systems in which patient records were kept on local systems in the provider (GP surgery or hospital). As a halfway house, both hospital systems and GP systems are being replaced with 'hosted' systems. This means that both the records and the supporting software are moved to remote server facilities. This has major implications for professional control of data and also of system functionality. Perhaps 30% of GP systems are already hosted, although many surgeries are resisting the move. These recalcitrant surgeries have been provided with a tool, GP2GP links, to enable records to be transferred as patients move; it has the vulnerability that staff at any surgery so equipped can pull the record of any patient at any other such surgery, without effective access-control or consent mechanisms. The deployment of NPfIT systems in acute hospitals has also not gone well, with the flagship 'Lorenzo' system years late and not working at all well enough.[37]

Quite apart from specific design and delivery failures, the multi-contributor record raises deep and serious questions. It is already deployed in a few early adopter areas, but many clinicians believe it to be unsatisfactory. First, there is a safety problem: if many different health professionals can write to a record, but none of them is responsible for curating it and maintaining its quality, it can rapidly become a mess. This is the wikipedia model of uncontrolled collective authorship, and it appears reckless for the NHS to embrace it for medical records just as wikipedia is moving to a more controlled model. Second, there are serious privacy issues: it has been reported that making GP records available to social workers has eroded trust in GPs and made low-income single mothers less likely to seek treatment for post-natal depression.[38] Putting everything into one pot not only makes privacy compromises more likely (more users have access to a larger set of data) but also precludes careful consideration of context-specific information flows. It also becomes less clear who is the 'controller' of the data. Given that the whole data protection system hinges on the duties of the controller, and that patients mostly trust their doctors but distrust ministers and officials, any move to make the Secretary of State the data controller rather than the doctor undermines both legal protection and trust.

There is thus a developing consensus among practitioners that for safety, privacy and system engineering reasons, we need to go back from the shared-record model to the traditional model of provider-specific records plus a messaging framework that will enable data to be passed from one provider to another when this is appropriate. For these reasons the DCR must be assessed as *Privacy impact:* **red**.

National Childhood Obesity Database

The National Childhood Obesity Database (NCOD)[39] contains the results of height and weight measurements taken from school pupils in Year 1 (age 5–6) and Year 6 (10–11) since 2005. Parents can refuse to have their children weighed and measured, but currently around 80% of children participate. The database is the largest of its kind in the world. Its aim is to provide local-level data to evaluate interventions and monitor government progress towards the target, set in 2004, to halt the rise in obesity among children under 11 by 2010.[40]

Children's measurements are entered on to a spreadsheet and submitted to the Primary Care Trust, which then uploads the data to UNIFY, a Department of Health performance management system. Each child's body mass index is calculated and the numbers of children who are of normal weight, overweight or obese are stored as aggregate information on the basis of school, age and sex. Individual pupils' names and dates of birth are not held on NCOD, and the related postcode is that of the school. However, the PCT may retain individual information, including the postcode of residence. The biggest objection to this project, though, is whether it's needed at all. Statistical samples of children, both nationwide and where interventions are being tried, should surely be enough. Therefore we assess its *Privacy impact:* **amber**.

2.2 Department for Children, Schools and Families

This department operates or supervises a number of databases for purposes ranging from school administration through child welfare to child protection. (FIPR wrote a detailed report on children's databases for the Information Commissioner in 2006[41]; the overall picture has not changed substantially since then, although some systems have been tweaked or renamed.)

National Pupil Database

The National Pupil Database (NPD) has been in existence since 2000. It 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. It is principally used for statistical and research purposes, but is increasingly being used as a data source for some of the other systems described below.

Pupil data is collected via a termly school census, and the data required are specified by the Secretary of State in regulations. The current dataset includes: 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.[42] An annual 'Early Years' census collects data on pre-school children.[43] The NPD also holds details of key stage and public examination results. As there are legal concerns about maintaining sensitive information on children without an effective opt-out, and as the scope of this database increases year on year, we rate this as *Privacy impact:* **amber**.

ContactPoint

ContactPoint is a national index of all children in England. Together with eCAF (which we describe next) it provides a nationally standardised data collection system intended to facilitate the sharing of information about children and their families between agencies. These systems are central to the Government's 'Every Child Matters' agenda[44] because they provide a single point of reference that enables agencies to monitor children and co-ordinate intervention if they believe a child is not making good progress.[45]

ContactPoint will hold each child's name, address, gender and date of birth, contact details for parents, and information on the child's education provider and primary health care team. It is intended to enable practitioners to see who else is working with a child, and it will list the contact details for practitioners in any service with which the child is involved, together with any case record number by which the child is known to individual agencies. There will also be an indication of whether an in-depth assessment has been carried out under the Common Assessment Framework (CAF) and if so whether it is available for viewing.[46] Details of 'sensitive' services such as mental or sexual health, or substance abuse agencies, will not normally appear on the index. Instead, a note that an "unspecified sensitive service" is working with the child will be added (consent will be asked for this but consent procedures are unsatisfactory). There will be a facility to 'shield' the records of especially vulnerable children, such as those who are the subject of hostile fostering or adoption; families in witness protection; those escaping domestic violence; and the children of public figures. Shielding will be left to local authorities, many of which are unsure about how to do this. (They are aware of children on the child protection register, but have no easy access to data on celebrities or armed service families.)

ContactPoint will initially be populated from existing national data sources: the National Pupil Database; NHS patient records; the HMRC Child Benefit database; and the Office for National

Statistics births register. The system will be deployed gradually to local authorities over a period of several months and they will be responsible for checking the accuracy of each child's entry and supplementing it with data from local sources.

Implementation has repeatedly been delayed by security concerns. A government-commissioned security report from Deloitte, of which only the executive summary was published in February 2008, said:

"It should be noted that risk can only be managed, not eliminated, and therefore there will always be a risk of data security incidents occurring." [47]

At the time of writing, the Government proposes to begin deployment in 2009. Because of the privacy concerns and the legal issues with maintaining sensitive data with no effective opt-out, and because the security is inadequate (having been designed as an afterthought), and because it provides a mechanism for registering all children that complements the National Identity Register, we rate this as *Privacy impact:* **red**.

Common Assessment Framework and eCAF

Work is under way to develop a second national database to hold the records of all children who have been assessed under the Common Assessment Framework (CAF). The CAF is a standardised personal profiling tool developed for use by all agencies, except social services, when a practitioner believes that a child needs extra services over and above 'universal' education and health care, or if it is thought that the child is not making progress towards a set of five outcomes laid down by the Government (that children should "be healthy, stay safe, enjoy and achieve, make a positive contribution and achieve economic wellbeing"). CAF goes beyond recording factual information to include practitioners' judgements on how the child is developing in his/her family. It often includes extensive data on family members, including value judgments about parents and other family members. Although CAF can be done on paper, it's being supplanted by eCAF, a database that the Government plans to make available from the autumn of 2009, and which will make practitioners fill in all the fields (rather than just skipping the questions that are irrelevant or for which they don't really know the answer).

Unlike ContactPoint, eCAF only covers children who are child-welfare cases, and they can opt out in theory. However, few will be really free to opt out in practice, and the system collects far too much data, much of it subjective, on dubious legal grounds. The data are also too widely disseminated and likely to lead to stigmatisation of young people. Therefore we have no choice but to rate this as *Privacy impact*: **red**.

Integrated Children's System

The Integrated Children's System (ICS) is an electronic case-management system for social care records. It has a series of forms for social workers to record information about children with whom they are working. Although ICS is being implemented locally, with each council buying software from one of a handful of suppliers, the overall programme is directed by DCSF[49], who specify connectivity and other functionality.

There have been repeated delays with ICS, which has also attracted a lot of criticism from social workers. In February 2008, a government taskforce report said:

"local authority staff believe that the Integrated Children's System (ICS) moves the focus of activity towards compliance with the expectations and needs of a standardised system, which appear to be chiefly related to data capture, and away from using effective professional approaches and analysis related to meeting the needs of the client family and child."[50]

The DCSF declined to publish an academic report on ICS that it had commissioned which questioned whether the system was fit for purpose, instead attributing difficulties to social workers' resistance to change. Concern about ICS has increased following the recent murder of Baby P in Haringey who was the subject of a child protection order[51] – were social workers following 'the system' at the expense of common sense? (Indeed, Ofsted rated Haringey as 'good' even after this baby's death; the inspectors relied on the data rather than doing a proper inspection.[52]) Unlike ContactPoint, this system is restricted to children who have come into contact with social work, and it's maintained locally. But the concerns about its effectiveness and intrusiveness compel us to rate it as *Privacy impact:* **amber**.

Wiring Up Youth Justice

Youth Justice Information Systems are undergoing a radical overhaul in a Youth Justice Board (YJB) programme called *Wiring Up Youth Justice*[53] that is due to be completed by 2010. WUYJ is funded by the National Offender Management Service (NOMS). Since 2000, fragmented local systems developed by local authority Youth Offending Teams (YOTs) without an overarching national strategy have placed increasing stress on the youth justice system. The priority is to join up information systems across youth justice and ensure compatibility with other criminal justice systems, ContactPoint and local authority children's services.

The YJB is responsible for all children in the 'secure estate', such as young offenders' institutions. YOTs are responsible for those who receive non-custodial sentences, and they also run prevention programmes for children aged 8–13 assessed as likely to commit criminal offences.

YOIS/RAISE/UMIS

Two-thirds of Youth Offending Teams use Social Software's Youth Offender Information System (YOIS) system[54] to record information and hold case notes on work with young offenders, the remainder use Careworks' RAISE[55]. Both systems support the ASSET system developed by the YJB. RAISE holds information both about offenders and about those thought likely to offend. The Universal Monitoring & Evaluation Information System, UMIS, is the most popular system for preventive work in YOTs that do not use RAISE. It records detailed information on children who have been referred to the Youth Offending Team because they are thought likely to commit criminal offences. They may, for example, have been identified in a YOT exercise called 'ID50' which seeks out the 50 children in the local area aged 8–13 who are considered most likely to become offenders. It also stores ONSET data. As the main objections to these systems concern the stigmatising information held in ASSET and ONSET, we will rate those systems rather than the YOIS, RAISE and UMIS systems that front-end them.

ASSET

The ASSET Young Offender Assessment Profile[56] is a profiling tool used to assess offenders and prepare pre-sentence reports for the courts. It explores every area of the child's development – health, environment and attitudes – and calculates the likelihood of re-offending by allocating scores to the various risk-assessment categories. The YJB has recently announced that sentencing

recommendations as to the length and intensity of community punishments will in future be based on ASSET scores.[57] A child's ASSET profile remains on the YOIS or RAISE system unless s/he is given a custodial sentence, when it will be moved to the YJB's eASSET Sentence Management System.[58] Because of the intrusive nature of such assessments and the shaky evidence base for them, we rate ASSET as *Privacy impact:* **amber**.

ONSET

All children referred to a Youth Offending Team as potential offenders are assessed using the ONSET profiling tool.[59] The assessment will be stored on RAISE or a similar system. ONSET examines a wide range of factors in the child's life and looks for signs of social exclusion such as being a victim of bullying, living in poor housing or having a low family income. Unless the ONSET indicates that the child is at low risk of committing crimes, s/he will be referred to a preventive scheme such as a Youth Inclusion Programme (YIP), or a Youth Inclusion and Support Panel (YISP). Children may be stigmatised by ONSET; for example, if they come to the attention of the police they may be more likely to be treated as suspects rather than as victims or witnesses.[60] Because it may have such effects on unconvicted children, we believe that ONSET contravenes the European Convention on Human Rights and rate it as *Privacy impact:* **red**.

2.3 Department for Innovation, Universities and Skills

Managing Information Across Partners

Managing Information Across Partners (MIAP) is a new initiative led by the Department for Innovation, Universities and Skills (DIUS) in partnership with education and training bodies. It is operated by the Learning and Skills Council. MIAP will create a lifelong, online record of each person's education and training from the age of 14 and maintain a register of learning provision.[61] The rationale is to provide higher and further education institutions with streamlined access to people's educational records, with data being made available to educators, careers services and government agencies. However, students who opt out of sharing their data *"will have to complete additional paperwork and provide evidence of their participation and achievement information each time they ... apply for a new job"*[62], so presumably employers will have access too.

It is being introduced in stages. The first stage was an online UK Register of Learning Providers, launched in 2005; the second stage is the Learner Registration Service (LRS), which allocates a 10-digit, Unique Learner Number (ULN) for everyone over the age of 14 in education or training. This began in May 2008, when data from the National Pupil Database was loaded into LRS, resulting in the allocation of 1.6m ULNs. School census information will continue to be the primary means of allocation. Other learners will receive ULNs when they reach 14 or apply for courses.

The third stage will be an online 'Learner Record', holding details of all qualifications and learning achievements. There will be two versions: one containing full details, and a restricted version listing only successful achievements. The former will be available to the data subject while the latter will be available to "all other users with the right of access". Organisations will get access by signing a data sharing agreement.[63] Pilots of the Learner Record have now been completed and the Government envisages launching the scheme in 2009. The final stage will be the 'Learner Plan': a system to facilitate information sharing about each learner, and to create a more detailed record of education, assessments and achievements. Pilots are under way, and will be completed during 2009.

The available information about MIAP stresses that each learner will be in control of their own record and can opt out of having their information shared. They cannot opt out of being allocated a Unique Learner Number. It is too early to assess how MIAP will work in practice. It is also important to consider what the long-term effects will be on those who have patchy records, perhaps because of time spent out of the country. However, although the privacy compromise may only be moderate, we are not convinced that this 'me-too' database will bring significant benefits. For example, those of us who are educators see no use for it. Therefore we rate MIAP as *Privacy impact:* **amber**.

2.4 Home Office

The Home Office recently published a Review of Criminality Information by Sir Ian Magee, which provides a useful analysis of many of the information resources used primarily in law enforcement.[64] In this section we provide an overview of the main existing systems, and then of two proposed systems – the National Identity Register and the Communications Database.

Several Home Office databases are controlled via arm's-length agencies. The National Policing Improvement Agency is a non-departmental public body sponsored and funded by the Home Office and managed by a Board containing representatives from the Association of Chief Police Officers, Association of Police Authorities, the Metropolitan Police Service and the Home Office along with the agency's Chair, Chief Executive and two independent members. One of its key roles is to manage the following databases on behalf of police forces across the UK.[65]

Police National Computer, INI, and Police National Database

The Police National Computer (PNC) holds comprehensive details of citizens, vehicles, criminal offences and property and is continuously accessible over a secure network by criminal justice agencies and all UK police forces.[66] It includes applications such as the identification of suspects using a physical description and personal features; searches for vehicles by registration, postcode and colour details; searches for items such as firearms, trailers, plants and animals; and tools to link crimes with similar characteristics. A National Firearms Register was added after the Dunblane massacre, recording all individuals who own firearms and shotguns – and those who have had a certificate refused or revoked. This was a classic public-sector IT disaster and is still not satisfactory twelve years later.[68]

The PNC has grown dramatically in size and capability since it was introduced in 1974 as a stolen vehicles database. During 2007 around 170m transactions took place, increasing at roughly 10% each year. Work is continuing on mobile access. There are also linked systems, such as ViSOR (originally the Violent and Sexual Offenders Register) which is used to register, risk assess and manage more than 50,000 individuals convicted of sex offences or jailed for more than 12 months for violence, and other individuals who pose a serious threat to the public (such as those convicted outside the UK of sexual offences). ViSOR is managed within the Multi-Agency Public Protection Arrangements (MAPPA) and used jointly by police, probation and prison staff.[69]

By 2010 the PNC will be linked to the Schengen Information System II, allowing data to be shared with police organisations across Europe. Sirene UK is the Home Office-funded project to set up this connection.[70] SIS II holds information on wanted and missing persons, stolen vehicles, trailers, firearms, identity documents and registered banknotes. A central server in Strasbourg will send and receive data from national servers in each Member State. PNC checks on a person or object

will search both databases.[71] An SIS 'sister database', the Visa Information System, will hold biometric data on the 20m annual EU visa applicants. Under the EU's 'principle of availability', information held by police in one member state must be available to law enforcement agencies throughout Europe. The Schengen Convention set up a Joint Supervisory Authority to oversee SIS data protection issues.[72]

The NPIA IMPACT Programme is developing a capability for police forces to access softer intelligence information across local and national systems.[73] Soft intelligence includes opinion, hearsay, tips from informants and even malicious accusations; letting such things leak from the world of intelligence into that of routine police operations is dangerous, and some intelligence officers think it a mistake. The IMPACT Nominal Index (INI) allows forces to find out whether information is held on any individual by other forces in the areas of intelligence, crime, custody, child protection, domestic violence and firearms licence refusals and revocations. By March 2008 the INI held around 62m records on an unknown number of individuals, with around 36,000 searches conducted in March 2008. Roughly 11% of searches led to requests for access to data. INI is also used in the Disclosure Service and vetting process managed by the Criminal Records Bureau.[74]

The INI is an interim system. It will be superseded by the Police National Database, an extensive store of police intelligence and other operational information linked to the PNC. The PND will hold detailed information on people (including suspects, victims and witnesses), objects, locations and events. Forces will be able to share text, images, files, maps, video and audio. Interfaces are planned with other police systems and external systems such as DVLA's. A contract to build the system was to be signed by the end of 2008, with deployment in 2010 – at which point the government will decide whether the PND should subsume or link to the PNC. The IMPACT Programme is developing a code of connection to allow access to law enforcement agencies other than UK police forces – for example, Europol. [75]

The Management of Police Information (MoPI) project is standardising information management throughout the police via a statutory Code of Practice[76] and associated guidance. Initial and highly controversial guidance was that information on certain serious offences should be retained until the subject reached the age of 100 years. A review is ongoing and PNC retention periods are being challenged at the Information Tribunal. For example, one of the cases concerned retention of a record of a 13-year old girl who was cautioned (not convicted) over a fight in a school playground. The police argue the record should be kept until the girl – now a grown woman – is 100 years old; even the Information Commissioner regards this as excessive. There have also been considerable concerns over the sharing of information on sensitive matters such as race, disability and sexuality.[77] Although the PNC is an established and accepted system, such concerns about the direction of its evolution, about the vastly greater functionality of the PND and about the loss of the distinction between evidence and intelligence lead us to rate it as *Privacy impact:* **amber**.

National DNA Database

The National DNA Database (NDNAD) holds DNA profiles taken from crime scenes, suspects and witnesses. Accredited laboratories create profiles by filtering and analyzing samples taken from swabs.[78] As of 31 March 2007 there were 4,428,376 subject samples records held on the National DNA Database, representing 3,874,500 individuals.[79]

The Police and Criminal Evidence Act 1984 let police retain DNA taken from those charged with an offence. Samples taken from those who were not subsequently convicted should have been

destroyed; but the Audit Commission found in 2000 that 50,000 samples were being illegally retained. The House of Lords subsequently allowed illegally held DNA to be used in evidence.[80] The Criminal Justice and Police Act 2001 retrospectively allowed sample retention. The Criminal Justice Act 2003 allowed samples to be taken from anyone arrested for a recordable offence and detained at a police station. (Recordable offences include begging, being drunk and disorderly and taking part in an illegal demonstration.)

Over half a million innocent people (people not convicted, reprimanded, given a final warning or cautioned, and with no proceedings pending against them) – including over 39,000 children – are now on the database.[81] Profiles are held on nearly four in ten black Englishmen under the age of 35.[82] Scotland had meanwhile taken a different path; there the records of people acquitted or not charged are deleted; and DNA sample and data retention policies vary widely across Europe, with the regime in England and Wales being the most aggressive.[83] Yet there is serious doubt about its effectiveness: doubling the number of people on the database from about 2m to about 4m has not increased the proportion of crimes solved using DNA, which remains steady at about 1 in 300. Indeed, in 2007 the number actually fell slightly.[84] Finally, in December 2008, the European Court of Human Rights found that keeping the DNA of innocent people contravened the European Convention on Human Rights (ECHR).[85] So the database is excessive and we have to rate it as *Privacy impact:* **red**.

National Fingerprint Database

The National Fingerprint Database (IDENT1) allows the police forces of England, Scotland and Wales to compare records of 7.5m individuals against palm prints and marks taken from suspects and crime scenes.[86] Every person arrested in Britain has fingerprints and palm prints entered onto the database, and also the Police National Computer or Scottish Criminal History System arrest record. (Mugshots and DNA are also both collected at this point). Around 36,000 fingerprint sets are being added each month.

443 Livescan devices and 200 Lantern hand-held units allow prints to be taken in police custody suites. The Home Office is funding the deployment of mobile fingerprint devices, which will enable patrolling officers to identify individuals on the street.[87] Since May 2008 the system has also been cross-checking fingerprints from up to 8,500 visa applicants each day.[88]

IDENT1 is a managed service provided by Northrop Grumman Information Technology under contract until 2013. The National Policing Improvement Agency is working with the government's biometrics programme to further support identification where required – for instance, by matching fingerprints held under the National Identity Scheme, and developing facial recognition standards.[89] But fingerprints are an accepted part of criminal justice record-keeping and (unlike with DNA) the fingerprints of acquitted people are deleted. We rate the IDENT1 system itself as *Privacy impact:* **green**.

National ANPR Data Centre

Automatic Number Plate Recognition systems use optical character recognition to read a vehicle number plate from an image produced by dedicated cameras or modified CCTV cameras. They have been used for a number of years in strategic locations such as ports and the London financial districts, but are now being expanded across motorways, main roads, airports and town centres. Mobile cameras have been installed in patrol cars and in police helicopters that can read plates from a distance of 600 metres. The cameras are operated by multiple agencies – the Highways Agency, local authorities, police forces and private firms.

The NPIA manages a Back Office Facility (BOF II) that allows all UK police forces, HMIC, SCDCA, the Ministry of Defence, SPSA, HM Revenue and Customs and the Serious Organised Crime Agency to retrieve and analyse data.[90] Roadside cameras will read 50m plates covering 10m drivers each day, with data recorded for up to five years and a capacity of 18bn licence plate sightings in 2009. It is starting to provide the police with the capability to track suspect vehicles in real time. The police also operate mobile units that stop cars bearing the numbers of those that are reported as stolen, being driven without tax or insurance, or otherwise of interest. The ACPO ANPR strategy states that police forces should "fully and strategically exploit" the database.[91]

ANPR data is increasingly turning up as evidence in trials, and the ACPO policy document *NPR Strategy For The Police Service 2005/2008 – "Denying Criminals the Use of the Road"*[92] makes one of its goals clear from its title. Other goals include the seizure of untaxed and unlicensed vehicles, and making a national vehicle movements database part of the National Intelligence Model. ACPO also envisage data sharing with the private sector – for example, linking to garage forecourts so that the police can detect suspect vehicles being fuelled, while the operator is warned of vehicles from whose drivers he should demand advance payment.[93] There is also a proposal to introduce electronic vehicle identification by means of chips in number plates. The technology is ready but the Government has not yet decided to roll it out. Despite this reluctance to embrace the logical next step, ANPR data is already supplied to partners in local crime reduction initiatives (including private firms). This is a clear case of technology push; in the absence of evidence that the resulting privacy intrusion brings real crime-reduction gains, we have to rate ANPR as *Privacy impact:* **amber**.

UK Border Agency

Under Council Directive 2004/82/EC, air carriers are required to communicate Advanced Passenger Information regarding passengers to EU Member States' immigration authorities, and it is also passed to the USA by bilateral agreement. In the UK the data is processed by the UK Border Agency, which through its e-Borders Programme is developing a "joined-up modernised intelligence-led border control and security framework" including pre-boarding electronic checks of all persons flying to the UK. A trial project captured information on 10m inbound and outbound passengers. Data were matched against watch lists from immigration, law enforcement and customs, and used to deliver alerts to government agencies.[94]

The European Council is considering extending this requirement to other Passenger Name Record data, to land and sea travel, and to journeys within the EU. Each member state would set up a unit to carry out a risk assessment of passengers using this data, which could also be used for various purposes related to serious and 'other' offences.[95]

The UKvisas Biometrics Programme operates in 135 countries and covers the three-quarters of the world's population who need a visa to come to the UK. Over 2m fingerprint sets have been collected so far, with fingerprint matches against previously unsuccessful applicants (held in the Immigration and Asylum Fingerprint System) rapidly communicated to visa officers at diplomatic missions. Fingerprints recorded for use in biometric visas are also stored in IAFS.[96] Officers use an IT caseworking system called Proviso that sends information back daily to a Central Reference System database, which is accessible to government departments involved in immigration control, law enforcement and national security.[97] These systems appear to mix scaremongering 'war-on-terror' tactics with legitimate immigration control mechanisms, and with little evidence of effectiveness. Some calm reappraisal would not go amiss, and we rate them as *Privacy impact:* **amber**.

ID cards

The Identity Cards Act 2006 gives the UK government the power for the first time since the 1950s to introduce a national identity card and a supporting database, the National Identity Register. This system is run by the Identity and Passport Service (IPS), an executive agency of the Home Office; it will store biographical information (such as name, address, date and place of birth and gender), biometric data (facial image and fingerprints) and administrative data related to the issue and use of a card. Access may be required for many transactions, such as opening a bank account. As with the Population Demographics Service system already deployed in the NHS, the ID card will create an audit trail of a citizen's interaction with services that require its production. Intelligence agencies and to a large extent the police will have unrestricted access.

Some scheme data will be held digitally on ID cards or passports, and some in the National Identity Register. Originally this would have been a new system: the current plan appears to be distributing it across several existing government systems. Biographical data will be stored in a system based on the existing Department for Work and Pensions' Customer Information System. Biometric data will be held initially in the Immigration and Asylum Fingerprint System. Administrative data will be held in existing Identity and Passport Service systems. The systems will, of course, be linked.

While the Register will not contain other sensitive government-related information, a National Identity Number will make it easier to link together information held on individuals across other public-sector databases. This is worrying because in the UK, unlike other EU States with strong constitutional protection, there are few safeguards against excessive data exchanges. Indeed, the Government appears to be bent on removing such safeguards as do exist. Given the growing public opposition to ID cards, the constantly-changing rationale for their issuance, the lack of the compensating privacy controls found in civilised countries that do have ID cards, and the absence of any evidence that countries with them do better, we must rate this as *Privacy impact:* **red.**

The Communications Database

Most telephone companies and ISPs store records of customers' telephone calls and Internet communications for business purposes such as billing and fault diagnosis. Such 'communications data' includes subscriber information, records of numbers dialled, and the location of mobile phones. It may include headers of e-mails sent and received and information about websites accessed. Voice-over-IP operators such as Skype that operate centralised directory services are also able to log users and calls. The UK's intelligence agencies, 52 police forces, HM Revenue and Customs, prisons and 510 public authorities can all demand access to communications data. 519,260 such requests were made in 2007.[98] From 15 March 2009 ISPs and phone companies will be required to retain specified communications data for 12 months.[99]

The agencies have an Interception Modernisation Programme whose focus is a plan to centralise communications data in a government database, where it would be much more amenable to data mining for unusual patterns of behaviour. A typical application would be tracing the structures of individuals' friendships and communications patterns. In addition to this, it is planned to field Deep Packet Inspection (DPI) equipment that will look at the content of people's Internet communications in order to determine who is talking to them in cases where this is not evident from the source and destination of the data packets. For example, DPI boxes could record people's coordinates in Second Life, and their webmail inbox screens. It is most unlikely that the average citizen will agree with the intelligence agencies' argument that this is 'traffic data'; an attempt to define full URLs as traffic data was defeated during the passage of the Regulation of Investigatory Powers Bill.

The Government trailed the idea of taking powers to do all this in primary legislation; the story now is that there will be a consultation in March 2009. Meanwhile we understand that the construction of a prototype of the database is under way.

The fact that communications data is currently kept in separate locations under the control of telephone companies and ISPs provides a practical safeguard against abuse; agencies have to serve notices on these companies to retrieve specific data. They must also cover the costs of doing so, which provides an incentive for officials to consider the proportionality of requests. The Information Commissioner's Office has commented that the plans are "a step too far for the British way of life" and that:

"[B]efore major new databases are launched careful consideration must be given to the impact on individuals' liberties and on society as a whole. Sadly, there have been too many developments where there has not been sufficient openness, transparency or public debate."[100]

Given this assessment, the public opposition, the huge cost of the exercise, and the intent to reduce the costs of surveillance to the point that instead of being able to watch anybody the intelligence services would be able to watch everybody, we have no choice but to rate this as *Privacy impact:* **red**.

2.5 Ministry of Justice

The criminal justice system does not have a unified electronic record system, partly due to system complexity and the number of departments and organisations involved. Between 2003–2008 the Home Office, Ministry of Justice and Attorney-General's Office spent £2bn on a Criminal Justice IT programme to modernise the IT infrastructure of the police, Crown Prosecution Service, magistrates' courts, crown court, prisons, the probation service and youth justice services. Targets were set in the Justice for All White Paper (2002) to reduce crime by 15% and further in high crime areas; improve the number of crimes for which the offender is brought to justice to 1.25m; and to boost public confidence by reducing fear of crime without compromising fairness.[101]

The Office for Criminal Justice Reform has now taken over these responsibilities, with IT systems focused on operational needs. Examples include Xhibit, which provides court hearing information; Link, an infrastructure for courts; the National Strategy for Police Information Systems (NSPIS) case preparation system; the Compass case management Service for the Crown Prosecution Service; secure e-mail for criminal justice staff including independent lawyers; Libra, equipment for magistrates' courts; Connect 42, equipment for the Crown Prosecution Service; and the Witness Management System.

National Offender Management Service

HM Prisons and the probation service are currently being merged into an executive agency, the National Offender Management Service (NOMS), to reduce overlap and improve efficiency.

The National Offender Information System (C-Nomis) is consolidating over 200 prison and probation service databases into a single offender information system. 80,000 users will be able to share information and manage offenders more efficiently. C-Nomis is under review due to cost over-runs; total costs are heading towards £950m. It will replace the existing Lids case management system across England and Wales by May 2010.

However, the Probation Service will now instead use an updated Offender Risk Assessment System (OASys), which provides practice analysis techniques, resource planning and management, performance evaluations and assessment monitoring. It also contains information on offenders moving within and between communities and prisons. The equivalent probation system is known as e-OASys and will be merged into the prison system. OASys is being linked to police and the courts.

The Offender Management National Infrastructure (Omni) is a common backbone for prison and probation services, managed by NOMS. NOMS is currently merging 43 data centres into three. There must be some concern that consolidating data into large systems to which many people need access may result in criminals obtaining access via careless or corrupt users so that they can target other criminals, and we assess this as *Privacy impact*: **amber**.

HM Court Service

The Libra Case Management System schedules hearings, handles case results, generates court orders and notices, manages fine accounts and fees and tracks enforcement action. The Bichard inquiry set a target that court results should be transferred directly to the PNC in 90% of cases. DVLA is being connected to courts and police forces across England and Wales. Vehicle notices are handled using the NSPIS Vehicle Procedures/Fixed Penalty Office application. The Penalty Notice Processing (PentIP) project is standardising management of disorder and road traffic offences. There are clearly some privacy issues with such systems but they appear secondary to the systems such as DVLA and PND which they feed, so we will not give them a separate assessment.

2.6 Treasury

The Treasury has responsibility for HMRC, formerly Inland Revenue and Customs & Excise, which merged to form HMRC from April 2005.

PAYE

The Pay-As-You-Earn tax-collection system has been running in its current form, known as Computerisation of PAYE (COP), since about 1988. This consists of 12 geographical databases holding records on around 35m taxpayers, organised by 1.5m PAYE schemes run by employers, pensions, etc. It is mainly concerned with taxpayers. The databases hold a record of PAYE payments, collected not via monthly returns but from employers' annual P14 and P35 submissions. Submissions from small firms (less than 50 employees) can be done on paper until 2009/10, but larger employers must now file electronically.[102] Currently there is no single PAYE account per taxpayer, and this is compounded by inconsistent working practices. Estimates for 2006–07 put likely underpayment at £880m and overpayment at £340m; there are said to be 13m discrepant records.[103]

A PAYE service redevelopment, Modernising PAYE Processes for Customers (MPPC), introduced online filing from 2004–5 and in its third phase will migrate to per-taxpayer records on nearly 40m taxpayers. It will be based on NIRS2 (see below). This record will hold all employment, pay, tax and pension information in one place.[104] It was supposed to be introduced in October 2008 but has been delayed. Once it is working, the current geographical constraints will be removed and taxpayer records will be available to HMRC staff in any location.[105] We will therefore assess the tax systems as a whole later under the 'National Insurance Recording System' subsection.

Self-Assessment Database

Self-assessment (SA) was introduced in 1996 and is the primary means of collecting tax on self-employed income and for taxpayers with complex affairs.[106] An individual registering to pay income tax using SA is automatically allocated a Unique Taxpayer Reference (UTR), which is the key to this data.[107] HMRC have a target that for 2007/08, 3m of all SA tax returns will be online, from a total of 8.6m (35%).[108] Registration and use of the online service is via the Government Gateway (see below).

Student Loans

Information from the Student Loans Company is checked against the SA data and the PAYE database.[109] This is a non-departmental body that works with HMRC, devolved administrations and local authorities to manage student support. At the end of 2007–08, there were 2.7m borrowers (in England), of which 1.7m were in repayment mode after students have left higher education.[110]

Tax Credits Database

Child and Working Tax Credits are the successor to Working Families Tax Credit and Disabled Person's Tax Credit, and were introduced in April 2003. The old system was notorious for overpayment, of the order of 10–14% by value[111]; the new credits are supposedly more resistant to claimant error and fraud, because there can be more cross checks with other data sources.[112] There is a policy of 'risk assessment' that weighs 23 different factors; all new claims are also checked with other databases for key entries such as names and addresses.[113]

However, there were serious computer problems with the new system (contracted to EDS), and in 2003–04 there were £1.93bn overpayments (of which £184m were blamed on software errors) and £464m underpayments.[114] The software is still described as "fragile".[115] In April 2008 there were 5.7m families in receipt of CTC or equivalent benefits, plus a further 0.4m receiving Working Tax Credit without Child Tax Credit.[116] Risk Intelligence and Analysis Teams (RIATs) in local offices use local intelligence and the HMRC data warehouse to investigate cases in which there appears to be "something wrong".[117] The data warehouse brings together information from the HMRC's own databases with third party information, for analysis and management information rather than for routine processing. It's worth noting that tax credits involve details of personal circumstances, not just income, and are thus more privacy-invasive than the rest of the tax systems.

National Database Frameworks

Supporting information for PAYE, Student Loans, Self Assessment, and Tax Credits is held on a number of national database 'Frameworks', which hold information in one place, for updating or viewing through other computer systems such as NIRS.[118] They are the Employments Framework (for employer data), the Citizen Identification Framework (taxpayer name and contact details), the Address Framework, (addresses), and the Primary and Secondary Tracing Frameworks (used for tracing cases where, for example, there is no NI number).

Child Benefits Database

The Child Benefits systems hold details of all families with a child under 16. They were the source of the two discs that caused embarrassment to the Government when they were lost in November 2007.[119] They contained a scan of the database, including the records of all UK children and their

parents – a total of 25m people along with addresses and bank account details. Following the data loss, it emerged that the problem was not an isolated operator error but a systemic failure of policy, culture and system design.

National Insurance Recording System

The National Insurance Recording System 2 (NIRS2) succeeded its predecessor NIRS in 1997 and has suffered from a number of failures[120]. It holds 65m individual contribution records and collects contributions, calculates contributory benefits, provides data to other government agencies, and pays age-related rebates to Occupational and Personal Pension schemes. A 1% sample from the NIRS2 dataset forms the Lifetime Labour Market Database used by National Statistics.[122]

The MPPC project is currently working on moving PAYE information from COP to NIRS2. Because of the centralisation, and the loss of the current geographic compartmentation, and because the cultural problems that emerged following the child benefit data loss will take years to fix (even if ministers keep trying), we are concerned that centralisation will lead to growing risks of unauthorised access (e.g. by private eyes or journalists doing social-engineering attacks on careless staff). We therefore assess the new centralised systems as *Privacy impact:* **amber**.

2.7 Department for Work and Pensions

The Department for Work and Pensions is upgrading and rationalising its infrastructure in a large transformation programme begun in 2005.[123] A major priority is reducing fraud. The Department operates both directly and through agencies such as Jobcentre Plus and the Child Maintenance and Enforcement Commission (formerly Child Support Agency). As with the tax systems in the previous section, we will do the assessment for the main database system, the Customer Information System (CIS), rather than trying to allocate individual assessments to the component systems that work with it.

Customer Management System

The Customer Management System (CMS) was introduced to support Jobcentre Plus in summer 2003, with full roll-out complete in 2008.[124] It is a front-end system for primary benefit processing systems[125], gathering information and evidence to support claims for Income Support, Job Seekers Allowance, Incapacity Benefit and secondary benefits. Although it does not determine eligibility for Housing or Council Tax Benefit, CMS also gathers the information needed for these claims, which are then sent to the relevant Local Authority[126] (of which more below). It is a system for data collection, rather than storage (which is done on CIS and elsewhere).

Payment Modernisation Programme

The Payment Modernisation Programme (PMP)[127], started in 2002, was a project to move from indirect (cash, girocheque) payments of benefits (and pensions, below) to direct payments into bank, building society, or post office accounts, to reduce fraud and error, and to improve accounting, with an estimated total cost of £824m[128].

Pensions Transformation Programme

State pensions information currently appears to be fragmented across legacy IT[129] and paper-based systems[130]. The Pensions Transformation Programme, with an overall expected spend of £598m[131] and expected end date in 2010/11[132], is intended to allow front-line customer agents to handle both state pension and pension credit in the same contact, with no paper-based processing. It is being introduced in six 'waves'. Wave 0 concerns internal preparation; waves 1–2, from April 2006, involved new applications for state pension and pension credit in local pension centres; waves 3–5 are said to be *"just adding richness and functionality"*[133]. The project is now at the point where new applicants can apply for pension credit, state pension, housing benefit and council tax benefit in a single call.

Employment and Support Allowance

The new Employment and Support Allowance (ESA) replaced incapacity benefit and income support paid on incapacity grounds for new claimants from October 2008. Systems and processes to support ESA have an overall estimated cost of £295m.[134]

Customer Information System

The Customer Information System (CIS) is described in DWP's 2008 report as "one of the largest databases in Europe". It will hold 85m records[135] and will gather data from existing sources into a centralised database to provide "a single, accurate view of key information and identity for all citizens who have ever had a National Insurance number"[136], including deceased and their beneficiaries, and details of ethnic backgrounds.[137] The cost of the system is estimated at £89m, which makes it one of the smallest of the DWP's major IT systems in terms of expenditure.[138] It is available over secure channels to 80,000 members of DWP staff, 60,000 users from seven other government departments, and over 445 local authorities.[139] It is "central to the Government's ID management proposals". It was due to be completed in October 2008 and to replace the existing Personal Details Computer System and Departmental Central Index.[140] As the system has been deployed in early 2009, there have already been reports of abuse; in February 2009 it emerged that staff at over 30 local authorities had been abusing the system, despite warnings in January that it was not acceptable to look at records of friends or relatives, and it also emerged that CIS data was being made available to private-sector firms such as BT.[141] For all these reasons, and because of the centralisation that will (as with NIRS2 in the case of tax) invite ever-more-capable attacks from the illegal information broking industry, we rate the CIS as *Privacy impact:* **amber**.

Although the National Identity Register will use some of the capabilities of the CIS, it is claimed that it will not use any of the data held in the CIS system.[142] On the other hand, there might be a shared identity service based on CIS; as part of the National Identity Scheme, there has been some exploration of this possibility between the DWP and the Identity and Passport Service.[143] If the systems became linked in this way, then CIS would share our assessment of the National Identity Scheme as *Privacy impact:* **red**.

Tell us Once

DWP is keen on running shared services for other departments. In addition to its support for the ID card scheme[144], it runs HR for the Cabinet Office and others[145], as part of the shared services agenda. It also has a growing cross-government role in citizen-facing services; an example is *Tell us Once*[146], with HMRC, DVLA, IPS, and local authorities, which was set up partly in response to Sir David Varney's *Report into Service Transformation*[147]. He recommended letting citizens tell

government just once of changes in their circumstances, initially to cover bereavement, birth and change of address.

Tell Us Once has recently launched pilots at Southwark, Wolverhampton, and Rotherham for citizens reporting bereavements and births.[148] A change of address service could follow in 2010.[149] A business case should be presented to local authorities and DWP, HMRC, IPS, DFT, Cabinet Office, HMT, CLG and the Information Commissioner's Office in April 2009.[150] As it is in effect a pilot for a service that would be rolled out through the Government Gateway, we will leave the assessment to that system.

DirectGov and the Government Gateway

The most prominent citizen-facing project run by DWP is DirectGov,[151] a portal for citizens' access to e-government. As a rule, it does not hold personal data.

The main e-government interface for citizens, businesses and public servants is the 'Government Gateway', established in 2001 and now approaching 14m registered users.[152] This provides registration, authentication, and transaction management for online government services, providing a single point of entry.[153] Services currently available through the Government Gateway include online self-assessment, electronic VAT returns and some benefit claims. Citizens can get a state pension forecast, and employers can notify vacancies to Jobcentre Plus. A few local authorities have also enabled Government Gateway authentication for council tax and other services.[154]

The Government Gateway is run by the e-Delivery Team[155], which moved from the Cabinet Office to the DWP in April 2008.[156] Perhaps of greatest significance for this report is the fact that it is also the provider of the Employee Authentication Services (EAS) Project, which will enable employees in local government, schools and other organisations to access and share sensitive information.[157]

A privacy assessment of the Gateway has to take into account not just the potential consequences of a compromise but the fact that it is funnelling all the relationships between the state and each individual citizen down a single path – a single path for both the state's supportive and coercive functions. Increasingly, it will also leave the citizen at the mercy of the automation; the Transformational Government programme is unapologetic about minimising unnecessary personal contact. The incentives in public service tend towards ever more complex services; but if citizens end up having to 'feed the beast' by supplying ever-more information through automated channels, will the interface end up as call-centre hell but with ID cards? Automated delivery mechanisms need some serious thought, and where they are centralised we would venture that a principled rethink is needed. Hence our assessment is *Privacy impact:* **amber**.

Income Support Computer System

The Income Support Computer System is one of a number of legacy systems being replaced by CIS/CMS/PTP. It deals with means-tested benefits ranging from Income Support, Pension Credits (claimed by over 2.7m households[158]), One Parent Benefit, and Child Maintenance Bonus.

Personal Accounts

The Pensions Acts 2007 and 2008 set up new scheme of low-cost Personal Accounts to provide pensions for low-to-moderate earners.[159] In issuing the Prior Information Notice for the scheme, the Personal Accounts Delivery Authority estimated it should have up to 7m active savers.[160]

Child Maintenance and Enforcement Commission (formerly CSA)

The Child Support Agency had terrible problems, with a large backlog of manual processing and an old system, CS2, that doesn't work well. The agency has been abolished and replaced by the Child Maintenance and Enforcement Commission. The new agency is working on a new 'PR1' system, which was started by the CSA and is supposed to be introduced soon; and a new vendor will be appointed in January to build an entirely new system. Given the misery that the existing intrusive systems have caused, we have to assess this project, however well meant, as *Privacy impact:* **amber**.

Links from and to DWP

The department exports and imports large volumes of data. It makes use of the Data Matching Service[161], which has been in operation for over ten years and matches data sets including DWP Benefits, Royal Mail Redirect, TV Licences, and many more. There are two matching services to detect fraud and errors in benefits: the General Matching Service and the Housing Benefit Matching Service. DWP also makes CIS data available to 22 000 local authority users via 'IT Information Flows for Local Authorities' (ITFLA1), while a project called NTC will supplement this data with HMRC tax credit data, required for the administration of Housing Benefit and Council Tax Benefit.[162] The Corporate and Cross-Government Matching Unit uses GMS to deliver non-fraud activities such as identifying target clientele for policy initiatives.

In response to a written question in the House of Commons, Employment Minister Stephen Timms said: "The Department carries out many large and small scale data cross-checks and matches between its own various systems and between its systems and those of other Government Departments, as the law allows. This is in order to deliver effective services to many different types of customers. However, detail of the individual linkages and checks is not held centrally and could be obtained only at disproportionate cost."[163]

Data is also imported from and exported to the private sector. Jobcentre Plus has been investigating matching its benefit data on Income Support with data held by credit reference agencies, and, in the longer term, the DWP intends to extend the range of data to which it has access.[164] Also, the Home Office National Identity Scheme Strategic Action Plan involves "biographical data gleaned from the Department for Work and Pensions National Insurance database and biometric data held by the Home Office and the Identity and Passport Service" – and remarks that these data are not necessarily high quality.[165]

In other words, this Department shares sensitive data with many controversial users, and does not know with whom it is sharing data. A thorough review is essential and we have to assess its broader sharing as *Privacy impact:* **red**.

Analytical Data Integration for Government

Analytical Data Integration for Government (ADIG) is a cross-government project which has looked at the feasibility of establishing a longitudinal information base for cross government policy-making, research, and analysis. The ADIG Feasibility Report was delivered to the Cabinet Office,

DCSF, DWP, HMRC, HMT, MoJ and ONS in January 2008. It is envisaged that data for analysis will involve data remaining in individual departments and being drawn on to create anonymised datasets. These could be analysed independently or 'mashed together', or could involve matched and then anonymised datasets, segmented datasets, and new datasets combining administrative with survey data.[166] Because of the enthusiasm for sharing in the absence of clear goals, and the lack of awareness that anonymised data can very often be re-identified, we have to assess this as *Privacy impact:* **amber**.

2.8 Department for Transport

The Department for Transport has a number of executive agencies that are responsible for the delivery of government policy and as a result hold extensive information on citizens and their movements. The main ones are the Driver and Vehicle Licensing Agency (DVLA), which is responsible for driver and vehicle licensing and the Highways Agency (HA), which operates many automatic number-plate recognition (ANPR) systems. There's also the Vehicle and Operator Services Agency (VOSA), which oversees MOT tests, and the Driving Standards Agency (DSA) which administers driving tests. Finally there's ITSO, an interoperability scheme for transport smartcards. The Department deserves praise for transparency; its website has a detailed explanation of "Who we share information with and why".[167] This is in stark contrast to DWP's inability to say who they share data with.

DVLA

The Driver and Vehicle Licensing Agency[168] registers drivers and vehicles and collects road tax. Its stated goals are to improve road safety, reduce crime, contribute to sustainability, collect tax and improve its public image. The databases it operates are not of themselves controversial – no-one is suggesting that DVLA be replaced by a network of local offices – but there are a number of issues. The driver cards it issues currently function (alongside passports) as ID cards, and thus its driver register is in effect a population register, covering over 40m licence holders, and has had some involvement with the ID card project.

However the main complaints concern its vehicle register, which is used to identify vehicle keepers not just following traffic offences but also where private parties such as car park operators wish to bring civil claims. In 2007 it was reported, for example, that DVLA will knowingly sell vehicle keepers' names and addresses not just to wheel-clampers with criminal records, but to a company owned by two men who were actually in prison for extorting money from motorists.[169] A code of practice was supposed to be introduced in October 2008[170] but the press reported in November 2008 that criminals could still buy drivers' names and addresses without any checks.[171] This episode raises more general questions about private access to government data. Until the governance and access problems are honestly tackled, though, we have to rate DVLA as *Privacy impact:* **amber**.

Highways Agency

The Highways Agency is principally responsible for maintaining and improving Britain's motorways and other trunk roads.[172] Their National Traffic Control Centre receives data from the MIDAS system[173] (which has loops in the road to detect vehicle movement), from commercial data feeds such as Trafficmaster[174], and also from automatic number plate recognition (ANPR) cameras. This is a UK invention, and surprisingly old: the first arrest due to a detected stolen car was in 1981.[175]

However the development of smaller, cheaper cameras has led to rapid growth in deployment nationwide: the agency now has over 1,000 cameras in 480 locations, and further cameras are operated by local authorities. The plan is to increase total numbers over the next few years from the 'low thousands' to the 'high thousands'.[176] The data is fed to the National ANPR Data Centre in Hendon, which is described in the Home Office section above. There are also significant and growing public concerns about ANPR. We rate it *Privacy impact:* **amber**.

Vehicle and Operator Services Agency

Most of the Vehicle and Operator Services Agency's activities relate to commercial vehicles but it also oversees MOT testing and vehicle identity checks. As a result it holds data on most cars. However, in practice, a wrongdoer wanting to link individuals with vehicles would use DVLA instead. For now we assess VOSA's *Privacy impact:* **green**.

Driving Standards Agency

The Driving Standards Agency administers driving tests. It thus holds data on learner drivers and on drivers who have passed their tests recently. This is relevant to present purposes because of a publicised data loss and because of a proposed pilot to issue smartcard provisional licenses – which has drawn DSA into the identity-card ambit. As these concerns appear peripheral, we would assess it as *Privacy impact:* **green**.

ITSO smartcards

The Department has a vision of a single smartcard for road pricing, parking, transport tickets, concessionary travel and so on across local authority boundaries. A first step in this direction is the ITSO interoperability framework,[177] which is used by a number of operators (although not by Oyster, the biggest such scheme). The incentives for the operators are faster boarding, customer relationship management, revenue protection and timetable planning. There are significant technical problems; the Mifare cards that ITSO uses turn out to be insecure, and there are serious technical and political problems to be overcome if ITSO-compliant cards are to become a universal and interoperable system for ticketing, not just bus passes.[178] As for privacy, many concession and ticketing schemes appear innocuous but the framework needs watching. Some cards may contain personal information when initially issued, and even if a card does not, a bus company might write identifying data to it when a customer tops it up using their bank card. For this reason we assess ITSO systems as *Privacy impact:* **amber**.

2.9 Non-departmental Agencies

TV Licensing

TV Licensing is a trading name used by private companies under contract to the BBC Licensing Authority.[179] The largest contractor is Capita Business Services Ltd, with a 10-year contract worth £500m from July 2002, in partnership with advertising group AMV.[180] At the end of 2003, there were just under 24m licences in force.[181] The licensing companies maintain a database of over 29.5m home, business and student addresses, to which all licence enforcement officers have access.[182]

One of the relevant questions is to what extent TV licence information is shared across other government activities. There have been repeated suggestions that it should be shared with other government bodies. In 2000 the Performance and Innovation Unit suggested that a Single Government Account would enable citizens to "monitor what they have paid to government and what they still owe"[183]; the 2005 Citizen Information Project report noted that the licensing database had the most current details on pensioners and could be used to share contact data through the National Identity Register[184]; and the Home Secretary recently implied that data sharing for dealing with anti-social behaviour could include TV licensing, among other databases.[185] However, the TV licensing database can only be used for administering the television licensing system.[186]

The TV licensing companies do use external data feeds. For example, retailers are legally obliged to inform them of equipment sales and rentals[187]; social security information may be made available to verify eligibility for a free TV licence for people over 75[188] and for the Digital Switchover Help Scheme[189]; and name and address data are gathered from the Post Office Address File, the electoral register, and other public sources. So long as data sharing plans are not implemented, though, we would rate *Privacy impact:* **green**.

Office for National Statistics

The 2011 Census will be run by the Office for National Statistics. ONS is an executive office of the UK Statistics Authority, a non-ministerial department which reports directly to Parliament. In August 2008, ONS contracted Lockheed Martin for £150m to provide the IT, including software development services, for the 2011 census. This will, for the first time, allow census questionnaires to be completed via the Internet.

Detailed questions for 2011 are not yet defined, but ONS is aiming for compatibility with the last (2001) census which recorded name, sex, date of birth, and marital status, and asked sensitive questions about religion, ethnicity, health, caring, employment, qualifications and commuting. ONS has argued that *"if the census responses were to be matched to other data sources a far richer database could be created, giving a far greater understanding of the state of the population"*.[190]

Other work done by ONS includes longitudinal studies, data collection, data analysis, medical research and a virtual microdata laboratory (VML). It is also due to complete in 2008 its three-year 'Digitisation of Vital Events' (DoVE) project under which Siemens will scan, digitise and index more than 250m birth, marriage and death certificates, dating from 1837. It keeps a Geographic Referencing Infrastructure based on national address lists.

Resistance to the census is bound to persist with such an extent and breadth of personal data outsourced to a single supplier. This goes well beyond what is done in other European countries and in itself poses serious risks. It's also not clear that enough has been done to reconsider the role of the census in the light of other contemporary developments in the database state. In particular, researchers (for example, in medicine) appear to have relatively easy access to identifiable census data in order to analyse the demographics of their subjects, and this should certainly be reviewed as it runs counter to European law. On balance though it is not clear that the illegality is embedded in the systems – just in the attitudes of their managers. We would assess this as *Privacy impact:* **amber**.

Audit Commission

Since 1996, the Audit Commission has run the National Fraud Initiative (NFI) which matches data within audited bodies in central and local government to detect fraud and overpayment; they claim to have detected over $140m in 2006–7. The Serious Crime Act 2007 gave them statutory powers to conduct data matching exercises. Audited bodies must provide data to the Commission, and others may provide information: the Act absolves them from any breach of confidentiality. A Code of Data Matching Practice provides that matching must be done in line with the Data Protection Act.[191] However, as noted, this Act does not properly implement EU law, and the ICO does not see the enforcement of the Directive (or the ECHR) as his business. The net result is that there are insufficient safeguards against improper data matching, and we must rate NFI as *Privacy impact:* **red**.

2.10 Local Government

Local governments run a number of systems that we have already described and rated under the departments that regulate them; we discussed eCAF and ICS under DCSF, while Housing Benefit and Council Tax Benefit fall under DWP. There are other systems that are perhaps best examined at a local level.

CCTV

One privacy issue that has attracted repeated public attention, and protest, over the years is CCTV. Video surveillance systems were described in Orwell's '1984' and are now operated by a range of public and private sector players; the systems that cover UK city centres and that cause the most controversy are mostly operated by local authorities. Following initial local experiments in the 1960s and 1970s, mostly of stations and football matches, street-based CCTV was introduced in Bournemouth in 1985 and spread slowly during the early 1990s.[192] From the mid-1990s, the bulk of the Home Office crime-reduction support for local authorities was directed towards projects that involved CCTV, and the industry grew rapidly. The recent move towards digital transmission, storage and processing of image data bring CCTV increasingly within the ambit of the database state.

A 2005 report commissioned by the Home Office concluded that while CCTV is effective at cutting crime in car parks and other spaces with restricted egress, it is ineffective elsewhere.[193] But the over-investment in CCTV has continued with over a million cameras now watching public spaces in Britain (and millions more in shops, banks and other business premises). Some local authorities are now starting to question whether their crime-reduction budget should be spent on other measures instead. As the over-investment continues in the teeth of the evidence, we rate CCTV as *Privacy impact:* **amber**.

Electoral Registration

Electoral registration is conducted by local authorities. Copies of the electoral register were available for sale to anyone for any purpose from at least 1832 until 2001 when a legal case limited the commercial sale of the full register, based on the DPA and the Human Rights Act.[194] In response to that case and the Howarth Report of 1999, the register has been compiled in both 'full' and 'edited' versions since October 2002.[195] Electors can opt out of the 'edited' version and only this version is now sold commercially; around 40% of electors opt out.[196] The 'full' version is,

however, still available to non-government bodies for specific purposes – notably to political parties (free) and credit reference agencies (on payment of a fee). Moreover, some online search services make use of pre-2002 'full' electoral registers, which appears to be legal unless the organisation fails to remove such personal data on request from the individual concerned. In that case, the ICO can issue an enforcement notice under the DPA, which it has done after receiving almost 1,600 complaints about a website called B4USearch.[197] The Thomas-Walport review of data sharing recommended that electoral registration data should no longer be sold; the full version should still be available to political parties and CRAs, but the edited version should be abolished.[198]

It is not proposed to change the local collection of electoral data, but the Ministry of Justice is leading a project for a Co-ordinated Online Record of Electors (CORE) which will provide a single source of (full) electoral registration data for authorised users. Clearly there is the possibility of linking CORE with other databases, including the National Identity Register, and its use for non-electoral purposes. There does not appear to be a set date for live operation. However, the Ministry of Justice now requires all electronic electoral registration data to conform to their standards by December 2009 to enable the future operation of CORE.[199] Given the past abuses and potential for future harm, we rate it as *Privacy impact:* **amber**.

Land and Property Gazetteers

Every large local authority in England and Wales is required to complete a Local Land and Property Gazetteer conforming to BS7666. These feed into the National Land and Property Gazetteer[200] which contains not only residential and commercial property but also multiple occupation, buildings within complexes, and other structures. The LLPG/NLPG systems are cross-checked against national datasets such as Council Tax, National Non-Domestic Rates, and the Post Office Address File (which contains over 28m addresses).[201]

LLPG is non-personal data, and so cannot fall foul of the DPA.[202] However, LLPG and NLPG are related to CORE because, as part of standardisation, MoJ suggests that Electoral Returning Officers match electoral registers against the Gazetteers to identify mismatches and to assign a Unique Property Reference Number (UPRN), part of BS7666, to electoral registration data.[203] This matching can bring the gazetteers into the scope of the DPA, which would raise questions similar to those mentioned in relation to the Electoral Register. However, on their own, we rate the gazetteers as *Privacy impact:* **green**.

Council Tax

Council Tax is levied on domestic properties according to a banded valuation. However, data relating to council tax is nevertheless personal data. Since data about a property is used to determine an individual liability for Council Tax, it is used to "inform or influence actions or decisions affecting an identifiable individual" and thus is personal.[204] Nonetheless *Privacy impact:* **green**.

Customer Relationship Management

The push for 'joined-up government' and citizen-centred services has led local authorities, as other government bodies, to attempt to integrate their existing data.

In terms of front-office service and better customer service, the Office of the Deputy Prime Minister

(ODPM) launched a National Customer Relationship Management Project in January 2003.[205] Case studies by the ODPM in March 2004, divided Customer Relationship Management (CRM) integration into 'deep' and 'shallow' and also found that as well as front-office/back-office integration, CRM was accompanied by other changes and integration in the back office.[206] For example, Calderdale Metropolitan Borough, with 194,000 inhabitants, claims a Citizen Database giving a '360° view' of its customers. It's not clear whether this is at all desirable; we'll discuss government and CRM in the next chapter.

There is a question about the extent to which LAs can legally populate a CRM system with personal data from existing sources[207]: council tax, non-domestic rates, housing and council tax benefits and the electoral register. Information collected for one purpose should not be used for another incompatible purpose. Regarding Council Tax data, the recent guidance from the Information Commissioner is that his office will not use its enforcement powers unless there is evidence of unfairness or unwarranted detriment to individuals[208] – revising earlier, more restrictive advice.[209]

Currently at least 321 councils are using some form of CRM.[210] The leading provider is Lagan.[211] Its ECM system provides full Enterprise Case Management, including 'advanced business intelligence' and 'sophisticated role-based security'. The development of new, integrated databases and the joining up of existing data raises the possibility of information being available in new ways, without the citizen being properly informed about them, and to council and other staff to whom it was previously not available. Therefore it is prudent to rate CRM systems as *Privacy impact:* **amber**.

2.11 European Databases

Finally, a number of European databases relating to police and criminal ('Third Pillar') matters exchange information with the systems of Member States, or require the exchange of information between Member States. The process of establishing and expanding them suffers from a serious 'democratic deficit', their governance is not satisfactory, and they have been criticised for not meeting the normal ('First Pillar') data protection standards. Yet their number will undoubtedly grow over time. There is the Prüm Treaty of 2005, under which a law enforcement officer in one state is entitled to information held by law enforcement officers in another state. Thankfully, the UK is not a signatory (yet), but this whole area merits attention. A useful summary of the issues and options was recently presented by Thomas Hammerberg, the Council of Europe's Commissioner for Human Rights.[212] We highlight three of the relevant systems here.

Schengen Information System

The Schengen Information System (SIS) is a 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 (there is an existing 'Eurodac' system used to exchange fingerprints). The House of Lords noted that SIS-II will contain "an enormous amount of personal data", and the European Commission acknowledged it will be transformed "from a reporting system to a reporting and investigation system"[213]. Because of the concerns raised by their Lordships, the democratic deficit and the likely function creep, we rate this as *Privacy impact:* **amber**.

Customs Information System

The Customs Information System similarly supports EU customs authorities and holds information related to allegations and inferences of customs fraud, terrorism, drug-smuggling and money-laundering, as well as charging and conviction data. Again, governance concerns drive us to rate this as *Privacy impact:* **amber**.

The Prüm Framework

Under the 2005 Prüm Treaty, some (not all) EU Member States agreed that law enforcement officers in each of them would be entitled to information held by law enforcement officers in any other one: this established the so-called principle of 'availability'. The UK is not a signatory to the Prüm Treaty. However, a recent Council Decision (the Framework Decision on the protection of personal data in the field of police and judicial cooperation in criminal matters) has adopted the 'availability' principle for exchanges relating to police and judicial matters across all EU Member States.

The Decision has been criticised because it does not require relevant domestic law and data to conform to the European data protection standards, and because it does not apply to police and intelligence activities in the field of national security. This means there are serious gaps and loopholes in the European 'Third Pillar' data protection system, to which, unfortunately, the UK is now linked. We rate the system as *Privacy impact:* **red**.

Chapter 3.
IT and Better Government

The previous chapter described how government departments have built systems that will radically change the nature of the relationship between the citizen and the state. There is no reason to suggest that any of these systems was conceived with evil intent, and many of the initiatives were debated and approved by Parliament. They have come about because of the incentives on ministers and civil servants to deliver better public services, or to deliver basic services at less cost.

But just as individually well-meant regulations can amount collectively to a stifling thicket of red tape, so the systems described here, collectively, amount to something quite new. All aspects of our lives will be surrounded by masses of data collected without our consent, and shared well beyond the purposes for which they were originally collected. Citizens are starting to realise this, and are progressively losing trust in government.

There is a false hope to be had in the idea that many of the gigantic systems will never work– the NHS National Programme for IT in particular appears set to become the world's largest civilian IT project failure ever. However, even though over half of all public-sector IT projects fail, some worthwhile projects fail and some intrusive projects succeed. If we want better government, we need better governance. In an ideal world, departments would only set out to build worthwhile systems, and they would succeed in these projects.

There are thus two aspects to the problem. First, what view should we take of privacy? Second, how can systems be managed better? In both cases we can learn from how things are done better abroad; and it turns out that the two problems are linked.

3.1 Privacy and Human Rights

Throughout this report, we have used the word 'privacy' to refer to people's right not to have sensitive information about them shared without their consent or an overriding legal reason. Privacy is actually shorthand for a complex bundle of issues, ranging from dignity to discrimination, and rooted in our need to control what we tell others about ourselves. Some privacy tensions are eternal: merchants want to charge rich customers more, and governments want to tax rich citizens more. Other tensions are driven by technology, and changing globally: the falling cost of data storage and communication makes it easier for merchants and governments to collect more data on people and thus become more efficient at discrimination. Other tensions are due to local factors. Britain, for example, has gone a lot farther down the road towards the database state than comparable developed countries. IT professionals in both the USA and Europe have watched projects such as NPfIT with considerable interest and apprehension.

Some of this was due to one-off factors, such as the Blair government's second-term decision to invest heavily in IT following the dotcom crash, not merely to placate IT industry lobbyists but also as a substitute for structural public-service reform. But it was also partly due to the fact that data protection law is implemented poorly in the UK and thus appeared to be less of an impediment than elsewhere in Europe.

UK data protection law comes from the EU Data Protection Directive, which is transposed into domestic law via the Data Protection Act of 1998. However, this Act is a defective implementation in a number of respects, and the UK has been in dispute with the European Commission over this for many years.[214] The Information Commissioner can only enforce the UK Act. The consequences are discussed in detail in a FIPR report to the Information Commissioner's Office.[215] The effect for present purposes is that many of the systems described in this report probably contravene the ECHR (as the National DNA Database was found to while we were writing it).

Many departments have tried to fix the problem using consent, particularly in the context of the NHS and children's databases. However, EU law applies strict tests as to when consent to data sharing can be deemed valid, and these tests must be strictly applied when consent is obtained from children. In other Member States it is held that no-one, and certainly no child, can give valid consent to wide-ranging, poorly-specified, long-term uses of their data (and especially not sensitive data) and that professionals should not rely on consent from minors without involving the parents whenever possible (unless there are special reasons not to do so). In one area where this has been tested in the UK courts – consent by minors – it was held in Gillick[216] (and confirmed in Axon[217]) that parents should generally be involved in consent decisions, unless the child refuses this. Again, the UK government has taken a perverse view: that children from age 12 can generally consent to information sharing, and that their parents need not usually be involved.

The UK public sector is starting to rely on systems that will have to be changed drastically once a litigant takes a case to Europe. This has been made quite clear first by *I v Finland*, which upholds a patient's right to keep her medical records private from clinical staff not involved in her care, and *S & Marper v UK* in which the National DNA Database was found in breach of ECHR.

The sooner the government changes its approach, the less the inevitable changes will cost. So our first recommendation is simple: that government system builders should set out to comply with the ECHR rather than avoid it.

Recommendation 1

Government should compel the provision or sharing of sensitive personal data only for clearly defined purposes that are proportionate and necessary in a democratic society. Where consent is sought for further sharing, the consent must be fully informed and freely given.

This has many implications. The Transformational Government vision of collecting all data about everyone, and keeping it forever, must be abandoned. For all but the most serious offences (sexual and violent offences), data must be forgotten after an appropriate period. In fact, it would also be of great benefit to industry if government adopted a simple default rule that all government data on citizens should be deleted after six years.

Our second recommendation relates to enforcement. Even if the Information Commissioner were given the power to enforce the ECHR, it is doubtful that he would use it vigorously against the state; he is appointed by the government and reports to Parliament, in which the Government of the day has a majority. The present incumbent, like his predecessors, sees his role more as encouraging 'good practice' (as he sees or accepts it) and even facilitating the Government's data-sharing agenda than as a vigorous guardian of the law or of fundamental principles (despite being a lawyer he is dismissive of a principled approach as 'legalistic'). In some countries the privacy authorities are more independent and demanding; in Germany the right to privacy is enshrined in the constitution, and state and federal privacy authorities even compete to some extent.

However, the best model for the UK may be the USA, where constitutional law is often enforced as a result of private action. The critical enabling factor is that while in the UK, someone who sues a government department may be faced with a ruinous bill of costs if he loses, in the USA the default rule is that each party bears its own costs. The implications of this for data protection were discussed at greater length by FIPR in our submission on the Thomas-Walport review.[218] In a nutshell, Britain gets the worst of both worlds; we have neither Europe's solution of strong privacy regulation, nor America's solution of private constitutional lawsuits. FIPR's recommendation was already set out in that submission, and the response to it has been positive, so we repeat it here.

Recommendation 2

Litigants who bring a case founded on the ECHR should be shielded from costs orders.

There is then the task of cleaning up the Augean stables that the next Government will inherit. We hope that this report will provide a useful guide, and that its green / amber / red traffic light system will help focus attention where it is most needed. The amber systems may well be contrary to the ECHR, and the red systems almost certainly are. The government has no business building illegal systems.

Recommendation 3

The systems rated amber in this report should be subjected to an independent review, for both their privacy impact and their overall benefits to society, while the systems rated red should either be scrapped (ID cards, communications database) or rewritten to support effective opt-outs (NHS Secondary Uses Service).

Next, we need a direction of travel for departments repairing or replacing systems that are unlawful or dysfunctional. So what is our guiding vision of what public-sector IT will look like in twenty years' time? Experience teaches that a system can have security, or functionality, or scale, and with good design it may even have any two of these; but it is not feasible to achieve all three. It follows that systems that deal with personal information must be either simple or local. Indeed, the systems that had grown up over time, before the Transformational Government initiative, largely followed this pattern.

The police, for example, relied on relatively simple national systems such as DVLA and PNC, while keeping sensitive intelligence information in force-level systems. The NHS had a small number of national frameworks, such as the Administrative Register (the forerunner of PDS) to link patients to NHS numbers, while the actual medical records were kept in the surgery or the hospital. This is also how other countries largely operate. The attempt by Whitehall to know everything so that it could micromanage everything was profoundly mistaken, and has been counterproductive at just about every level.

Recommendation 4

By default, sensitive personal information must be kept on local systems and shared only with the subject's consent or for a specific lawful purpose. Central systems must be simple and minimal, and should hold sensitive data only when both proportionate and necessary.

The complex systems that do hold large amounts of personal data should also be specified and purchased by front-line provider organisations, whether GPs, hospitals, social work departments or police forces; the role of the centre should be to ensure interoperability, and to provide a small number of simple, national frameworks that tie systems together. Central specification and purchasing of operational systems leads to the problems of NPfIT and ICS; as systems are optimised to 'feed the beast' in Whitehall they become less usable by front-line staff, leading to resentment, alienation and inefficiency. Overcontrol damages public services rather than improving them.

Our fifth recommendation serves three functions. First, it helps deter departments from building empires around unnecessary personal information. Second, it provides a principled mechanism whereby citizens can deal with the unlawful and intrusive systems built under the Transformational Government programme while they are being replaced. Third, it sets out to minimise discrimination in service provision. The key is anonymity. Until very recently, most of a citizen's dealings with the public sector were anonymous, at least to central government. Some public services are still anonymous (bus passes); others need names (criminal records); the big question is what happens in the middle. We believe that most public-sector systems should offer anonymous service to those who need or want it.

Recommendation 5

Citizens should have the right to access most public services anonymously.

At present, for example, someone needing medical treatment involving radiography, but who is unwilling to have their images stored on the PACS servers in Swindon, has to go private, go abroad, or join the armed forces (where they can get treated under a pseudonym). In practice, everyone should have the right to be treated under any name they wish to use. It may be argued that this will lead to foreigners or even illegal immigrants getting free NHS treatment. There are two possible answers to this. The first is, so be it; that will be orders of magnitude cheaper than NPfIT has been, and is perfectly defensible on both practical and ethical grounds. The second option is for people wanting anonymous healthcare to prove their entitlement, for example, by getting a certificate from their GP that they are entitled to care at the expense of the local Primary Care Trust. The choice between these options is for the Government of the day.

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. The incentives here must change. It is also in line with tradition. A name in Britain was always just that by which you were known, and you could use as many as you liked so long as you did not commit fraud. Recently the ID card program has led to a Napoleonic philosophy that people have names only because the state deigns to issue them. An explicit right to anonymity will not only restore an ancient right but poison future governments' attempts to hedge in citizens' freedoms.

3.2 Developing Effective Systems

The second enormous problem is government incompetence at developing IT systems. It has been known for many years that maybe a third of large system projects in the private sector fail; this is perhaps to be expected, as profit is the reward for risk. One might hope that in the relatively risk-averse public sector, things would go more smoothly: but this is not what we observe, and it was finally admitted in 2007 that only 30% of government IT projects succeed.[219] Why should this be?

The classic study of large-project failure revealed that big software disasters were usually due to specifications that were unclear, contradictory, the subject of conflict between stakeholders, or that kept changing in the course of the project.[220] This appears to explain part of the gap between the public and private sectors: politics is fundamentally about resolving conflicts between different interest groups in society, and ministers are under constant pressure to announce minor changes to policy.[221] Even so, the UK seems to fare worse than other comparable countries.

Britain is greatly afflicted by government naivety in purchasing. Many departments outsourced too much of their IT in the 1980s, and now do not have people with the skills to manage complex procurements. One noticeable effect is that the UK public sector always appears to get sold whatever technology or methodology is just going out of fashion in the private sector: business process re-engineering, which was popular in business in the 1980s, arrived in government in the 1990s (contributing among other things to the London Ambulance Service disaster); PKI was the

big fashion in the late 1990s but vanished with the collapse of Baltimore in 2000, only to resurrect itself phoenix-like as the identity management programme; and customer relationship management, which private firms are now starting to see through, is selling well in Whitehall and local government. Again and again, the state gets palmed off with private-sector retreads.

Another problem in Britain is the procurement process. Under EU rules, public-sector supply and service purchases over about £130,000 have to be advertised in the Official Journal of the European Union (OJEU), and Britain is particularly punctilious about compliance. The effect is that all but the smallest systems go through the OJEU process. As a result, a department wanting to build a new system must reckon with two years for contracting, a further two to build the system, and then maybe three years for roll-out. This has dire effects. First, it is highly unlikely that either the minister or the permanent secretary who commissions a system will still be in post when it comes into service; and second, if a department can only get one new system a decade, there is a strong temptation to make it all things to all people. Scale increases complexity, multiplies conflicts, and ensures multiple specification changes during development.

How can this be fixed? John Suffolk, the Government Chief Information Officer (CIO) has suggested that the UK should use its influence in Europe to raise the OJEU limit for IT projects. We endorse this suggestion here.

Recommendation 6

The UK should use its influence in Europe to raise the OJEU limit for IT projects to at least £10m

Another possibility, suggested by industry people we consulted, would be to just adopt the more relaxed interpretation and codes of practice that are found in France, Germany and elsewhere. Either way, by tilting the playing field against monster projects, we could prepare the ground for a new approach to public-sector IT with greater decentralisation of complex functions while the core systems are kept simple. This is how many European countries approach administration, even though the driver tends to be more devolved government; for example, health IT is more decentralised in countries such as Sweden and the Netherlands because health service management is also more decentralised. Privacy law is sometimes also a driver: in Germany, for example, population registers are kept locally, rather than in a federal system, because the constitution gives strong protection to privacy.

Britain will need other mechanisms. In addition to changing the incentives facing civil servants, we need to change the choice architecture. At present, public-sector systems are a complex mess of legacy applications running on a bewildering variety of platforms. Departments seek to cut through this by building their own centralised database systems, as described in this report. If we are to improve things, the Government needs to ensure that departments follow a strategy of interoperable systems. There should be a chief systems architect responsible for the structure and evolution of public-service IT. The office of the CIO is a start, but it is too far down the food chain: at present, the CIO reports to someone who reports to the Cabinet Secretary. This needs to be fixed. A heavyweight CIO could also help fix the retread problem.

Recommendation 7

The Government Chief Information Officer should be at permanent secretary level and report to either the Chancellor of the Exchequer or the Deputy Prime Minister.

Cultural change is also needed. At present, billions are wasted on systems that do not work well or at all, and the failures are covered up using a range of tricks from shifting the goalposts to claiming commercial confidentiality. Better government will be hard to achieve until government starts to learn better from its mistakes. That means that ministers and officials should be sure that their sins will find them out.

Recommendation 8

The procurement of government systems must be much more open than at present, with specifications, contracts and progress reports being made public by default, and with departments publishing full information about what information they collect on citizens and how it is processed. In the case of classified systems, this material must be made available on demand to anyone with a SECRET clearance.

Ease of public access to data matters as well as its raw availability. It has taken us quite some effort, while writing this report, to find out what data is shared with whom. There have been occasional beacons of good practice, such as the Caldicott Committee's report into health data sharing in the 1990s[222] and the Department for Transport's publication of information about what data it holds and for what purpose. European law requires that citizens be able to find out what data is held about them; without this they cannot challenge inappropriate sharing or even find and change inaccurate data. The present mechanism – registration under the Data Protection Act – is not fit for purpose. It needs a rethink. As many public services are monopolies (and some are actively coercive), the public sector should take the lead.

After fixing the framework, the leadership and the incentives, the next thing needing fixed is the management. Britain, like most countries, nurtures a cadre of administrative-stream civil servants, recruited via public examinations and groomed to take top jobs in the public sector. Their selection and training is no longer fit for purpose. Administration nowadays is about managing complex socio-technical systems that not only have complex data flows and application logic, but tricky outsourcing arrangements and often unforeseen interdependencies with other public and private-sector systems. Managing the evolution of these systems requires technical as well as political and leadership skills. It is unsustainable for a company, or a nation, to hire technophobes to run complex systems. Already 20 years ago, FTSE 100 companies were tackling this problem – by

hiring numerate graduate trainees, and/or insisting that managers acquire IT experience as well as sales, manufacturing and international experience before promotion to top jobs. The public sector must catch up.

Recommendation 9

There must be dramatic change in civil service recruitment and training to improve the service's ability to procure and manage complex systems.

For a start we recommend three things. First, from 2012 no civil servant should be promoted or hired to grade 3 or above without experience of IT, whether as a user on a procurement or even just managing a helpdesk. Second, from 2012 the civil service exam should contain a test of IT know-how. Candidates who cannot perform even a simple task – such as opening a file, reading some data, doing some basic manipulations and writing a web page – should not be hired. Third, if a department has to spend seven years building a new strategic system, its accounting officer should stay in post for the duration. Reform is, in fact, so large a task that much more will be needed. It will take a determined Prime Minister, but is now absolutely necessary.

We also need to wean Government off the idea that IT projects can substitute for effective policy action. For too long, ministers have used IT as a displacement activity. IT must rather be seen as just one of the tools of modern management; and often not be the most important tool (so neither ministers nor voters should expect too much). To paraphrase the late Roger Needham, "if you think IT is the solution to your problem, then you don't understand IT, and you don't understand your problem either." This brings us to our last formal recommendation:

Recommendation 10

There should never again be a Government IT project – merely projects for public-sector business process change, some of which will have an IT component.

Finally, we must stop confusing means and ends. The goal is surely to build a civilised state that is our servant rather than our master, and in which the supportive aspects are uppermost rather than the coercive aspects. We hope our report can contribute in some small way to getting this project back on track.

Glossary

The world of the database state is full of acronyms. Here's a brief guide for the perplexed.

ADIG Analytical Data Integration for Government (**amber**); a proposed longitudinal information base for cross government policy-making, research, and analysis; section 2.7

ANPR Automatic Number Plate Recognition (**amber**); sections 2.4 and 2.8

ASSET A Home Office system containing personal information about young offenders for use in sentencing, probation and so on (**amber**); section 2.2

CCTV Closed-Circuit TV (**amber**); public-sector systems are largely operated by local authorities; section 2.10

CfH Connecting for Health: an agency of the Department of Health responsible for healthcare IT, including the National Programme for IT; section 2.1

CIS DWP's Customer Information System (**amber**); holds data on everyone's national insurance, state pension, and other benefits; feeds the NIR; section 2.7

CMS DWP's Customer Management System; provides a front end to CIS and other systems; section 2.7

C-NOMIS The National Offender Management Service's system; part of Omni; used to run prisons; section 2.5

ContactPoint A DCSF system to register all children (**red**); records their relationships with public services; section 2.2

COP Computerisation of PAYE; a legacy system for processing PAYE tax data that had 12 separate regional databases, being replaced by NIRS2; section 2.6

CORE The Co-ordinated Online Record of Electors (**amber**); will provide a single electronic electoral register; all local electronic electoral registration data must now conform to CORE standards; section 2.10

CRM Customer Relationship Management systems (**amber**); used by many local authorities to hold extensive information on local residents; section 2.10

CRS The Border Agency's Central Reference System (**amber**); holds information on people entering and leaving the country, visas, and so on; section 2.4

CS2 The legacy system left by the Child Support Agency to the new Child Maintenance and Enforcement Commission; being replaced by PR1; section 2.7

DCR The NHS Detailed Care Record (**red**); holds your GP and hospital records in remote servers controlled by the government; section 2.1

DirectGov A DWP portal for citizens' access to e-government; section 2.7

DPI Deep Packet Inspection; communications surveillance technique used by IMP; section 2.4

DSA Driving Standards Agency (**green**); holds driving test data; section 2.8

DVLA	Driver and vehicle Licensing Agency (**amber**); holds data on vehicles, drivers, licensing and motoring convictions; section 2.8
eCAF	The DCSF electronic Common Assessment Framework (**red**); holds an assessment of your child's welfare needs; section 2.2
EPS	The NHS Electronic Prescription Service (**amber**); will handle all NHS prescriptions; section 2.1
ESA	The new Employment and Support Allowance; replaced incapacity benefit; section 2.7
GMS	The government's General Matching Service (**red**); used to match a wide range of data to detect fraud and errors, and to identify target clientele for policy initiatives; section 2.7
ICS	The Integrated Children's System (**amber**); operated by local government but specified by DCSF, this is being imposed for record-keeping in child social work; section 2.2
IDENT1	The National Fingerprint Database (NFD); section 2.4
IMP	The Interception Modernisation Programme (**red**); will hold everyone's communications traffic data such as itemised phone bills, email headers and mobile phone location history; section 2.4
IMPACT	A project by the NPIA to give police forces access to other forces' soft intelligence; this has led to the INI; section 2.4
INI	The NPIA IMPACT Nominal Index (**amber**); allows police forces to find out if another force has soft intelligence on a suspect, and data such as child protection, custody and firearms license refusals; will be subsumed into the PND; section 2.4
ITSO	Interoperability scheme for transport smartcards (**amber**); transport companies may write personal data to cards; section 2.8
Libra	The Court Service's case management system; feeds the PNC and DVLA; section 2.5
LLPG	Local Land and Property Gazetteer (**green**); every local authority keeps one; section 2.10
MIAP	The DIUS Managing Information Across Partnerships system (**amber**); section 2.3
MoPI	An NPIA project on the Management of Police Information; standardises guidelines for dealing with law enforcement data; section 2.4
MPPC	Modernising PAYE Processes for Customers; an HMRC project to move tax processing from COP and other legacy systems to NIRS2; section 2.6
NCOD	The National Childhood Obesity Database (**amber**); section 2.1
NDNAD	The National DNA Database (**red**); holds genetic information on criminals, suspects and former suspects; found unlawful by European Court of Human Rights; section 2.4
NFD	The National Fingerprint Database (**green**); also known as IDENT1; contains fingerprints of arrested persons and others; section 2.4

NFI	The Audit Commission's National Fraud Initiative (**red**); holds information from many sources; section 2.9
NIR	The National Identity Register (**red**); registers the population and supports ID cards; section 2.4
NIRS2	HMRC's National Insurance Recording System 2 (**amber**); the core of tax processing, it contains, or gives consolidated access to, everyone's tax records; section 2.6
NLPG	National Land and Property Gazetteer (**green**); gathers data from LLPGs for comparison against Council Tax, Post Office address file, and rates; feeds CORE; section 2.10
NOMS	The Department of Justice's National Offender Management Service; sections 2.2 and 2.5
NPD	The National Pupil Database (**amber**); holds demographic, testing and discipline data; section 2.2
NPfIT	The NHS National Programme for IT; this is building systems such as the SCR, DCR, SUS, EPS, and PDS; section 2.1
NPIA	The National Policing Improvement Agency, a non-departmental public body sponsored and funded by the Home Office; runs the PNC, INI and PND; section 2.4
NSPIS	The National Strategy for Police Information Systems case preparation system; used by the court service; section 2.5
OASys	The Offender Risk Assessment System; part of Omni; used to manage probation; section 2.5
OGC	Office of Government Commerce; reviews central government IT projects
Omni	The Offender Management National Infrastructure (**amber**); consolidating information used to manage prisons and probation; section 2.5
ONS	Office of National Statistics (**amber**); collects and uses data from national censuses; supplies to diverse users; section 2.9
ONSET	A Home Office system for predicting which children will offend (**red**); hoovers up data from many sources; section 2.2
Out of Hours	Systems run by NHS Direct and Adastra (**amber**); support care at evenings and weekends; section 2.1
PACS	The NHS Picture Archiving and Communication System (**amber**); contains all radiography images taken in the NHS; section
PDS	The NHS Population Demographics Service (**amber**); contains contact details and full history of healthcare contacts for all NHS patients; section 2.1
PMP	The Payment Modernisation Programme; moved benefit payments from indirect (cash, girocheque) to direct (bank) payments; section 2.7
PNC	The Police National Computer, currently being redeveloped as the PND
PND	The Police National Database (**amber**); contains a wide range of information to support police operations, including intelligence data and links to many other systems; section

PR1	Temporary system being introduced by the new Child Maintenance and Enforcement Commission to replace CS2; section 2.7
Prüm	European systems built under the 'Framework Decision on the protection of personal data in the field of police and judicial cooperation in criminal matters' following the Prüm Treaty; share law enforcement information; section 2.11
PSIS	Personal Spine Information System (**amber**); another name for the SCR; section 2.1
PTP	The Pensions Transformation Programme will let call-centre staff handle both state pension and pension credit in the same contact; section 2.7
RAISE	A system by Careworks used to support Youth Offending Teams; front-ends stigmatising information on children drawn from ONSET and ASSET; section 2.2
RIAT	Risk Intelligence and Analysis Team; RIATs are based in local HMRC offices and use NIRS and other systems to investigate tax cases; section 2.6
RIS	The NHS Radiology Information System (**amber**); contains diagnostic opinions on PACS images; section 2.1
SCR	The NHS Summary Care Record or Shared Care Record: a database of patients' prescriptions and allergies, with more data to be added later, to support unscheduled care (**amber**); section 2.1
Sirene	A Home Office project to links the PNC to SIS; section 2.4
SIS	The Schengen Information System (**amber**); shares law enforcement and customs data such as wanted people, vehicles and banknotes; sections 2.4 and 2.11
SUS	The NHS Secondary Uses Service (**red**); holds summaries of your hospital and other treatment in a central system to support NHS administration and research; section 2.1
Tell us Once	A pilot for a system enabling citizens to report address changes and bereavements only once to government; section 2.7
UMIS	The Universal Monitoring & Evaluation Information System; used by Youth Offending Teams and others; front-ends stigmatising information on children drawn from ONSET and ASSET; section 2.2
VML	The Office for National Statistics' virtual microdata laboratory; section 2.9
VOSA	Vehicle and Operator Services Agency (**green**); has MOT test data, as well as information on trucks, commercial drivers and transport firms; section 2.8
UNIFY	A Department of Health performance management system used to hold data from NCOD; section 2.1
YJB	Youth Justice Board; section 2.2
YOIS	Youth Offender Information System; used to support YOTs; section 2.2
YOT	Youth Offending Team; section 2.2

References

Most URLs were verified in January 2009.

1 D Leask, Health records of Brown and Salmond 'hacked', Scotland on Sunday, Mar 1 2009, at http://scotlandonsunday.scotsman.com/politics/Health-records-of-Brown-and.5026950.jp

2 R Anderson, Security Engineering – A Guide to Building Dependable Distributed Systems, Wiley 2001, second edition Wiley 2008

3 http://news.bbc.co.uk/1/hi/uk_politics/3568468.stm

4 http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf

5 http://www.telegraph.co.uk/news/3374341/One-Whitehall-official-sacked-or-disciplined-every-34-hours-last-year-for-losing-our-personal-data.html

6 http://www.cio.gov.uk/documents/pdf/transgov/transgov-strategy.pdf

7 Technology and Policing: implications for fairness and legitimacy Peter Neyroud and Emma Disley, OUP

8 J Kirkup, R Prince, Gordon Brown says your data will never be completely safe with the Government, Daily Telegraph, Nov 2 2008, at http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/3367661/Gordon-Brown-says-your-data-will-never-be-completely-safe-with-the-Government.html

9 To Home Affairs Select Committee, 13 Nov 2008

10 http://news.bbc.co.uk/1/hi/uk_politics/7674775.stm

11 Oral answers to questions, Nov 12 2008, at http://www.theyworkforyou.com/debates/?id=2008-11-12a.754.6

12 Sir Ian Magee, Review of Criminality Information, July 16 2008, at http://police.homeoffice.gov.uk/publications/operational-policing/review-criminality-information/roci-full-report

13 J Prime, S White, S Liriano, K Patel, Criminal Careers of those born between 1953 and 1978, Home Office Statistical Bulletin 4/01, Mar 12 2001, at www.homeoffice.gov.uk/rds/pdfs/hosb401.pdf

14 N Heath. More data breaches to come, warns gov't. Silicon.com, Nov 27 2008, at http://www.silicon.com/publicsector/0,3800010403,39354289,00.htm

15 The Electronic Patient Record. House of Commons Health Committee, Sixth Report of Session 2006–7; at http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/42202.htm

16 NHS 23, at www.nhs-it.info

17 National Applications, at http://www.btplc.com/Health/NHSIT/TheSpine/NationalApplications/index.htm

[18] Information held on the PDS, at http://www.connectingforhealth.nhs.uk/systemsandservices/demographics/pds/contents?searchterm=pds

[19] GPs and their families urged to boycott NHS 'spine', eHealth Insider 20 Jun 2006, at http://www.e-health-insider.com/News/1956/gps_and_their_families_urged_to_boycott_nhs_'spine'

[20] TV presenters in NHS data fears, BBC, Dec 3 2008, at http://news.bbc.co.uk/1/hi/scotland/edinburgh_and_east/7763349.stm

[21] Medical Records of Gordon Brown and Alex Salmond Hacked, M Aiken, Sunday Mail, Mar 1 2009, at http://www.sundaymail.co.uk/news/scottish-news/2009/03/01/medical-records-of-gordon-brown-and-alex-salmond-hacked-78057-21162440/

[22] Operating framework 08/09, at http://www.connectingforhealth.nhs.uk/systemsandservices/sus/supports/framework

[23] Health Committee, op. cit., pp 84ff

[24] Security Engineering – A Guide to Building Dependable Distributed Systems, R Anderson, Wiley 2008, ch 9

[25] One in five could object to SUS data use, e-Health Insider, 30 Sep 2008, at http://www.e-health-insider.com/news/4191/one_in_five_could_object_to_sus_data_use

[26] Children's Databases – Safety and Privacy, R Anderson, I Brown, R Clayton, T Dowty, D Korff and E Munro, Information Commissioner's Office, November 2006, at http://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf (see chapter 7)

[27] Article 8(4) and (6) of the EC Directive on data protection. The UK has not notified the European Commission of any such special arrangements.

[28] Working Document on the processing of personal data relating to health in electronic health records (EHR), Article 29 Data Protection Working Party, 00323/07/EN WP 131, at http:// ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf

[29] I v Finland ECHR (Application no. 20511/03) 17/07/2008, at http://www.onebrickcourt.com/cases.asp?id=120

[30] Electronic Prescription Service, at http://www.connectingforhealth.nhs.uk/systemsandservices/eps

[31] Electronic Prescription Service Moves Forward, Health Informatics Now v 2 no 2 (Dec 2007), at http://www.bcs.org/server.php?show=ConWebDoc.16241

[32] Police have had access to opiate prescriptions since 1996, but this did not seem to help them catch Dr Shipman; see 2 above

[33] Adastra Applications, at http://www.adastra.co.uk/content/Products/applications/Adastraapplication.html

[34] EMIS launches care integration projects, e-Health Insider, May 9 2008, at http://www.e-health-insider.com/News/3733/emis_launches_care_integration_projects

[35] See http://www.chooseandbook.nhs.uk/

[36] Choose and Book functional overview Spring 2005, at http://www.chooseandbook.nhs.uk/staff/reference/appfunctionality

[37] ASSIST says idea NHS like a bank 'fundamentally flawed', e-Health Insider, Oct 8 2008, at http://www.e-health-insider.com/news/4219/assist_says_idea_nhs _like_a_bank _'fundamentally_flawed'

[38] Adverse effects of child protection on public health, J Robinson, Association for Improvements in the Maternity Services, AIMS Journal, 2008 v 20 no 1, at http://www.aims.org.uk

[39] Analysis of the National Childhood Obesity Database 2005-2006 http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsStatistics/DH_063565

[40] Department of Health Spending Review 2004 Public Service Agreement

[41] Children's Databases – Safety and Privacy. R Anderson, I Brown, T Dowty, D Korff, E Munro, Information Commissioner's Office, 2006; at http://www.fipr.org

[42] Full schemas can be downloaded from: http://www.teachernet.gov.uk/management/ims/datacollections/sc2008/

[43] http://www.teachernet.gov.uk/management/ims/datacollections/EY-PRUs-AP/

[44] http://www.everychildmatters.gov.uk/

[45] *"Information sharing is key to the Government's goal of delivering better, more efficient public services that are coordinated around the needs of children, young people and families. It is essential to enable early intervention and preventative work, for safeguarding and promoting welfare and for wider public protection"*, from http://www.everychildmatters.gov.uk/

[46] The Children Act 2004 Information Database (England) Regulations 2007 No. 2182

[47] Contactpoint Data Security Review: http://www.parliament.uk/deposits/depositedpapers/2008/DEP2008-0502.pdf

[48] http://www.everychildmatters.gov.uk/deliveringservices/caf/ecaf/

[49] http://www.everychildmatters.gov.uk/ics/

[50] Lifting the Burdens Task Force: Review of the department for children, schools and families, 2008 http://www.communities.gov.uk/documents/507390/pdf/682640.pdf

[51] Child Protection stifled by £30m computer system, at http://www.guardian.co.uk/society/2008/nov/19/baby-p-child-protection-system

[52] R Curtis, We failed over Haringey – Ofsted head. The Guardian, Dec 6 2008, at http://www.guardian.co.uk/education/2008/dec/06/ofsted-child-protection

[53] http://www.wiringupyouthjustice.info/site/

[54] http://www.socialsoftware.co.uk/Development/172.asp

[55] http://www.careworks.ie/products/youth_justice.htm

[56] ASSET: http://www.yjb.gov.uk/en-gb/practitioners/Assessment/Asset.htm

57 Youth Justice: The Scaled Approach. At http://www.yjb.gov.uk/publications/Scripts/prodView.asp?idproduct=410&eP=

58 http://www.wiringupyouthjustice.info/site/projects/easset.htm

59 ONSET: http://www.yjb.gov.uk/en-gb/practitioners/Assessment/Onset.htm

60 FIPR, Children's Databases, ibid

61 http://www.miap.gov.uk/

62 Learner Registration Service, Learner Record and Data Protection Summary, at http://www.southdevon.ac.uk/attachment/file/2192/MIAP_Information.doc

63 http://www.miap.gov.uk/faqs/

64 Review of Criminality Information, Sir Ian Magee, July 16 2008, at http://police.homeoffice.gov.uk/publications/operational-policing/review-criminality-information/roci-full-report

65 NPIA Business Plan 2008-2011, at http://www.npia.police.uk/en/docs/business_plan08_web_distilled.pdf

66 NPIA Police National Computer, at http://www.npia.police.uk/en/10508.htm

67 NPIA Firearms Licensing website, at http://www.npia.police.uk/en/10503.htm

68 Police IT body admits to failings over gun database, Computing, Oct 22 2008, at http://www.computing.co.uk/computing/news/2228816/police-body-admits-failure

69 NPIA Dangerous Persons Database (http://www.npia.police.uk/en/10510.htm)

70 The Sirene project, at http://www.sirene.gov.uk/

71 NPIA SIS II website, at http://www.npia.police.uk/en/9619.htm

72 JSA Schengen website, at http://www.schengen-jsa.dataprotection.org/

73 NPIA Impact Programme, at http://www.npia.police.uk/en/8489.htm

74 NPIA, IMPACT Programme: Report on the Outcome of the Equality, Diversity and Privacy Consultation, July 2008 ch. 4, at http://www.npia.police.uk/en/docs/Consultation_Response_paper_v1_0.pdf

75 Ibid. ch. 5

76 Code of practice on the management of police information, Made by the Secretary of State for the Home Department under sections 39 and 39A of the Police Act 1996 and sections 28, 28A, 73 and 73A of the Police Act 1997, at http://police.homeoffice.gov.uk/publications/operational-policing/CodeofPracticeFinal12073.pdf?view=Binary

77 NPIA, IMPACT Programme ch. 3

78 NPIA DNA database, at http://www.npia.police.uk/en/8934.htm

79 National Policing Improvement Agency, National DNA Database Annual Report 2006-2007, at http://www.npia.police.uk/en/11405.htm

80 Attorney General's Reference No. 3 of 1999 [2000] UKHL 63; [2001] 2 WLR 56 (14th December, 2000)

81 Meg Hiller, answer to PQ from Grant Shapps, Hansard Sep 1 2008 column 1565W)

82 James Randerson, DNA of 37% of black men held by police, The Guardian, 5 January 2006.

83 N Van Camp and K Dierickx, The retention of forensic DNA samples: a socio-ethical evaluation of current practice in the EU, J. Med. Ethics 2008: 34, 606–610

84 Christopher Hope, Crimes solved by DNA evidence fall despite millions being added to database, The Telegraph, 11 November 2008, at http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/3418649/Crimes-solved-by-DNA-evidence-fall-despite-millions-being-added-to-database.html

85 DNA database 'breach of rights', BBC, Dec 4 2008, at http://news.bbc.co.uk/1/hi/uk/7764069.stm

86 NPIA IDENT1 website (http://www.npia.police.uk/en/10504.htm)

87 Owen Bowcott, Police will use new device to take fingerprints in street, The Guardian, 27 October 2008. The NPIA Mobile Fingerprint Device website is currently at http://www.npia.police.uk/en/10046.htm

88 Tom Young, Criminals snared by new biometric cross-checks, Computing, 10 July 2008, at http://www.computing.co.uk/computing/news/2221180/criminals-snared-biometric-4112481

89 NPIA Biometrics, at http://www.npia.police.uk/en/7834.htm

90 NPIA Automatic Number Plate Recognition, at http://www.npia.police.uk/en/10505.htm

91 Paul Lewis, Fears over privacy as police expand surveillance project, The Guardian, 15 September 2008

92 See http://www.steve-kane.co.uk/words/misc/ANPR-Strategy-2005-08.pdf

93 A link is proposed to a Fraudulent Vehicles Database run by CIFAS, a fraud prevention service run by over 250 mostly financial-sector firms

94 Home Office, Border Control FAQ, at http://press.homeoffice.gov.uk/faqs/controlling-our-borders/

95 Statewatch, EU-PNR scheme being re-written by the Council, 4 October 2008, at http://www.statewatch.org/news/2008/oct/04eu-pnr-rewrite.htm

96 Identity and Passport Service, National Identity Scheme Strategic Supplier Framework Prospectus, August 2007, at http://www.securitydocumentworld.com/client_files/070809_nis_strategic_supplier_framework_prospectus_v2_2.pdf p. 20

97 Memorandum submitted by Liam Byrne MP, Minister of State for Immigration, Citizenship and Nationality, to the Home Affairs Select Committee, 23 June 2006 (http://www.publications.parliament.uk/pa/cm200506/cmselect/cmhaff/775/775awe62.htm)

98 Report of the Interception of Communications Commissioner for 2007, HC 947 printed 22 July 2008 p.8

[99] Home Office, A consultation paper: Transposition of Directive 2006/24/EC, August 2008 (http://www.homeoffice.gov.uk/documents/cons-2008-transposition?view=Binary)

[100] Information Commissioner's Office, A communications database would be 'a step too far', Press Release, 15 July 2008 (http://www.ico.gov.uk/upload/documents/pressreleases/2008/annual_report_web_version.pdf)

[101] Justice for All White Paper, July 17 2002, at http://www.crimereduction.homeoffice.gov.uk/criminaljusticesystem6.htm

[102] Computing 24/07/2008: HMRC announces delay to tax system rollout Available at: http://www.computing.co.uk/computing/news/2222393/hmrc-announces-delay-tax-system-4137701

[103] Computer Weekly 16/07/2007: 'Discrepancies plague 13m tax records' Available at: http://www.computerweekly.com/Articles/2007/07/16/225582/discrepancies-plague-13-million-tax-records.htm

[104] HMRC Departmental Report, July 2008 Available at: http://www.hmrc.gov.uk/about/dept-report-2008.pdf

[105] Information from HMRC 14/11/2008

[106] National Audit Office 6 July 2007: HMRC 2006-07 Accounts: The Comptroller and Auditor General's Standard Report Para 23 Available at: http://www.nao.org.uk/publications/nao_reports/06-07/0607626.pdf

[107] HMRC: Self Assessment Online - Frequently Asked Questions Available at: http://www.hmrc.gov.uk/efiling/sa_efiling/sa_faqs.htm

[108] HMRC June 2007: Users of Self Assessment Online in 2005 Available at: http://www.hmrc.gov.uk/research/sa-reg-online-user-report.pdf

[109] HMRC Collection of Student Loans Manual CSLM14015 – Matching records: the matching exercise: how the matching exercise works and monthly borrower rematch Available at: http://www.hmrc.gov.uk/manuals/cslmanual/CSLM14015.htm

[110] Student Loans Company: Student Loans for Higher Education in England, Financial Year 2007-08 (Provisional) Available at: http://www.slc.co.uk/pdf/slcsfr022008.pdf

[111] NAO 06/11/2003: Comptroller and Auditor General's Standard Report on the Accounts of the Inland Revenue 2002-03, Para 2.6 Available at: http://www.nao.org.uk/publications/nao_reports/02-03/02031072.pdf

[112] House of Commons Committee of the Public Accounts 2004: First Report of Session 2003-2004: Tackling fraud against the Inland Revenue: Oral Evidence Q40

[113] HMRC NTC Ensuring Compliance at www.hmrc.gov.uk/compliance/tax_credits.pdf

[114] NAO 07/10/2005: Comptroller and Auditor General's Standard Report on the Accounts of the Inland Revenue 2004-05 Paras 2.22-2.25 Available at: http://www.nao.org.uk/publications/nao_reports/05-06/0506446.pdf

[115] House of Commons Committee of Public Accounts January 2008: Eighth Report of Session 2007–08: Tax Credits and PAYE Available at: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmpubacc/300/300.pdf

[116] HMRC April 2008: Child and Working Tax Credit statistics Available at: http://www.hmrc.gov.uk/stats/personal-tax-credits/cwtc-apr08.pdf

[117] HMRC NTC Ensuring Compliance Ibid

[118] HMRC PAYE Manual: PAYE3001 - background: frameworks: introduction Available at: http://www.hmrc.gov.uk/manuals/pommanual/PAYE3001.htm

[119] BBC News: UK's families put on fraud alert Available at: http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

[120] PublicTechnology.net 22/01/2004: Inland Revenue's NIRS2 disasters highlighted by Audit Office Available at: http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=488

[121] HMRC: National Insurance Recording System 2 - information page Available at: http://www.hmrc.gov.uk/nic/nirs2.htm

[122] National Statistics: StatBase: Lifetime Labour Market Database: General Information available at: http://www.statistics.gov.uk/STATBASE/Source.asp?vlnk=1304&More=Y

[123] CIO 100 Directory 2008: Company Profile 5: Department for Work and Pensions Available at: http://www.cio.co.uk/cio100/companyprofile/index.cfm?companyId=4130

[124] DWP June 2008: Customer Management System A Guide for Local Authorities Available at: http://www.dwp.gov.uk/housingbenefit/claims-processing/working-with-dwp/docs/la_guide.pdf

[125] Stephen Timms, answer to PQ from John Redwood, 25 April 2008 (Column 2356W)

[126] DWP June 2008 Ibid

[127] Chief Information Officer Council/EDS: Department for Work and Pensions Payment Modernisation Programme: enabling £100bn in social security payments per annum. Available at: http://www.cio.gov.uk/documents/case_studies/payment_modernisation.pdf

[128] National Audit Office 17/11/2006: Delivering successful IT-enabled business change: Case studies of success Available at: http://www.nao.org.uk/publications/nao_reports/06-07/060733-ii.pdf

[129] House of Commons Work and Pensions Committee 23/02/2005: Third Report of Session 2004-05: Pension Credit: Para 70 Available at: http://www.publications.parliament.uk/pa/cm200405/cmselect/cmworpen/43/43.pdf

[130] Department for Work and Pensions 2004: Departmental Investment Strategy 2005/6 – 2007/8 SR2004. Available at: http://www.dwp.gov.uk/publications/dwp/2005/invest_strategy.pdf

[131] Anne McGuire, answer to PQ from Mark Harper, 29 September 2008 (Column 2373W)

[132] Hansard 05/03/2008: Written Answers (Commons): Work and Pensions: Departmental ICT: Column 2596W Available at: http://www.parliament.the-stationery-office.co.uk/pa/cm200708/cmhansrd/cm080305/text/80305w0026.htm

[133] House of Commons Work and Pensions Committee 23/02/2005 Para 72

[134] Hansard 29/09/2008 Ibid

135 Computer Weekly 06/09/2005: 'Department for Work and Pensions plans citizen database to hold 85m records' Available at: http://www.computerweekly.com/Articles/2005/09/06/211601/department-for-work-and-pensions-plans-citizen-database-to-hold-85-million.htm

136 Department for Work and Pensions Departmental Report 2008 Para 155

137 CW 06/09/2005 Ibid

138 Hansard 29/09/2008 Ibid

139 Chief Information Officer Council 2007: Transformational Government – our progress in 2007

140 DWP 2008 Ibid Figure 28

141 Computer Weekly 24/02/2009: 'ID Cards Database breached by nosey council staff', M Ballard; available at http://www.computerweekly.com/Articles/2009/02/24/235004/id-cards-database-breached-by-nosey-council-staff.htm

142 Computer Weekly 20/02/2007: 'DWP struggles to uncover cause of public data breach' Available at: http://www.computerweekly.com/Articles/2007/02/20/221838/dwp-struggles-to-uncover-cause-of-public-data-breach.htm

143 Chief Information Officer Council 2007: Transformational Government – our progress in 2007

144 Computer Weekly 20/02/2007 Ibid

145 Computing 22/03/2007 'Whitehall acts on shared IT' Available at: http://www.computing.co.uk/computing/news/2186144/whitehall-acts-shared

146 Department for Work and Pensions Departmental Report 2008 Para 23

147 Treasury 2006: Sir David Varney: Service transformation: A better service for citizens and businesses, a better deal for the taxpayer Available at: http://www.official-documents.gov.uk/document/other/011840489X/011840489X.pdf

148 DWP 14/11/2008: Press Release: Tell us once, because your time matters Available at: http://www.dwp.gov.uk/mediacentre/pressreleases/2008/nov/hse113-141108.asp

149 Rotherham Borough Council - Report to Members 05/11/2007: Briefing on the 'Tell us Once' Programme Available at: http://www.rotherham.gov.uk/nr/moderngov/Published/C00000693/M00005446/AI00029802/$TellUsOnce.docA.ps.pdf

150 Chief Information Officers' Council 2007: Transformational Government – our progress in 2007. Delivering better, more efficient services for everyone Available at: http://www.cio.gov.uk/documents/annual_report2007/tg_annual_report07.pdf

151 http://www.direct.gov.uk/en/index.htm

152 Chief Information Officer Council 2007 Transformational Government Annual Report 2007: section: Putting the citizen and the centre of transformed services Available at: http://www.cio.gov.uk/transformational_government/annual_report2007/0103citizen_centred.asp

153 What is the Government Gateway? Available at: http://www.gateway.gov.uk/

154 Which government services are available online? Available at: http://www.gateway.gov.uk/

155 CIO 2008: e-Delivery Team Available at: http://www.cio.gov.uk/edt/

156 DWP Press Release 24th April 2008: Government gateway moves to DWP Available at: http://www.dwp.gov.uk/mediacentre/pressreleases/2008/apr/emp075-240408.asp

157 SoCITM 2008: Shared Authentication Services Roundup Available at: http://www.socitm.gov.uk/NR/rdonlyres/569F0435-4383-4BBB-87EC-7CF6CD63E60B/0/SOCITMsharedauthenticationservicesarticle.pdf

158 EDS: Department for Work and Pensions' Pension Credit: keeping more than three million pensioners out of poverty Available at: http://www.cio.gov.uk/documents/case_studies/pension_credit_eds.pdf

159 Office of the Leader of the House of Commons: Draft Legislative Programme 2007/08: Pensions Bill: Available at: http://www.commonsleader.gov.uk/output/page2035.asp

160 Personal Accounts Delivery Authority June 2008: Discussion note supporting the Prior Information Notice (PIN) for contracts to run the personal accounts scheme from 2012: Available at: http://www.padeliveryauthority.org.uk/files/PASchemePINDiscussionNote.pdf

161 National Audit Office 23/01/2008: Department for Work and Pensions: Progress in tackling benefit fraud Available at: http://www.official-documents.gov.uk/document/hc0708/hc01/0102/0102.pdf

162 Government Connect web site: Partners: Department for Work and Pensions Available at: http://www.govconnect.gov.uk/business/dwp.php

163 Hansard 25/04/2008 Ibid

164 DWP 2007: Getting welfare right: Tackling error in the benefits system Available at: http://www.dwp.gov.uk/publications/dwp/2007/error_strategyPDFs/error_strategy_report.pdf

165 Information Commissioner's Office 2006/07 Available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007.pdf

166 Ministry of Justice: response to Consultation paper on the use and sharing of personal information in the public and private sector, extracts from ADIG Feasibility Report available at: http://www.justice.gov.uk/docs/Analytical-Data-Integration-for-Government-Data-Sharing-Response.pdf

167 Who we share information with and why, at http://www.dft.gov.uk/about/informationcharter/whoweshareinfo

168 The DVLA website is http://www.dvla.gov.uk; its IT strategy is at http://www.dvla.gov.uk/publications.aspx

169 DVLA sells your details to criminals. The Mail on Sunday Feb 12 2007, at http://www.mailonsunday.co.uk/news/article-369838/DVLA-sells-details-criminals.html

170 Time runs out for rogue parking wardens. B Webster, The Times, Apr 18 2007, at http://www.timesonline.co.uk/tol/news/uk/article1668526.ece

171 Martin Delgado, DVLA still sell your data without checks as 30,000 requests a month bypass vetting system, Daily Mail, November 8 2008, at http://www.dailymail.co.uk/news/article-1084169/DVLA-sell-data-checks-30-000-requests-month-bypass-vetting-system.html

172 See http://www.highways.gov.uk/

173 The acronym MIDAS is also, confusingly, used for the motor vehicle insurance database. Here, it stands for Motorway Incident Detection and Automatic Signalling; see http://www.highways.gov.uk/knowledge/15228.aspx

174 See http://www.trafficmaster.co.uk/

175 See http://en.wikipedia.org/wiki/Automatic_number_plate_recognition

176 See http://en.wikipedia.org/wiki/Police-enforced_ANPR_in_the_UK

177 See http://www.itso.org.uk

178 Smartcards – anarchy in the UK, Modern Railways Dec 2008 pp 21-23

179 TV Licensing: Who we are Available at: http://www.tvlicensing.co.uk/aboutus/index.jsp

180 Capita to run TV licensing, Computer Weekly 20/12/2001, at http://www.computerweekly.com/Articles/2001/12/20/184438/capita-to-run-tv-licensing.htm

181 BBC Licensing Authority http://www.bbc.co.uk/foi/docs/finance/licence_fee/TVLicencing.pdf

182 TV Licensing: Detection and Penalties Available at: http://www.tvlicensing.co.uk/information/detectionandpenalties.jsp

183 Cabinet Office Performance and Innovation Unit 2000: e.gov: Electronic Government Services for the 21st Century Available at: http://www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/strategy/e%20gov%20pdf.ashx

184 Citizen Information Project: Final Report: Better sharing of citizen data across the public sector Available at: http://www.gro.gov.uk/cip/Definition/FinalReportAnnexes/index.asp

185 Home Office Press Release 13/10/2008: Stepping up the crackdown on persistent offenders: speech by the Home Secretary on a visit to Henbury, Bristol Available at: http://press.homeoffice.gov.uk/press-releases/stepping-up-the-crackdown

186 BBC 05/10/2007 Freedom of information request response RFI2007000709 Available at: http://www.bbc.co.uk/foi/docs/freedom_of_information/selected_requests_and_responses/2007/SR2007000790_TV_licence_database.pdf

187 TV Licensing Press Release 18/11/2004: Retailers urged to keep TV Licensing in the picture Available at: http://www.tvlicensing.co.uk/mediaandcommunity/mediapressreleases.jsp?archive=49

188 Television Licences (Disclosure of Information) Act 2000 Available at: http://www.opsi.gov.uk/ACTS/acts2000/pdf/ukpga_20000015_en.pdf

189 Digital Switchover (Disclosure of Information) Act 2007 Available at: http://www.opsi.gov.uk/acts/acts2007/pdf/ukpga_20070008_en.pdf

190 The 2011 Census: a design for England and Wales, ONS, March 2004

191 Audit Commission, Code of Data Matching Practice, at http://www.audit-commission.gov.uk/nfi/codeofdmp.asp

192 A history of video surveillance in England, at http://www.notbored.org/england-history.html

193 Gill M & Spriggs A, Assessing the impact of CCTV, Home Office Research Study 292, at: www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf

194 Thomas, R & Walport, M 2008: Data Sharing Review Report Available at: http://www.justice.gov.uk/reviews/datasharing-intro.htm

195 Home Office 1999: Final Report of the Working Party on Electoral Procedures Available at: http://www.dca.gov.uk/elections/reports/procs/index.htm

196 Thomas & Walport 2008 Ibid

197 House of Commons Standard Note SN/PC/01020 2008: Supply and sale of the electoral register Available at: http://www.parliament.uk/commons/lib/research/notes/snpc-01020.pdf

198 Thomas & Walport 2008 Ibid. Recommendation 19

199 Ministry of Justice August 2008: CORE Project: Additional information to assist implementation of Electoral Registration Data Standards: England and Wales Available at: http://www.justice.gov.uk/docs/electoral-registration-data-standards-additional-info-eng-wales.pdf

200 The National Land and Property Gazetteer 2008a: Licensing the NLPG Available at: http://www.nlpg.org.uk/nlpg/link.htm?id=2071

201 NLPG 2008b: About the NLPG Available at: http://www.nlpg.org.uk/nlpg/link.htm?id=2007

202 Russell, P 2006: Local Government and CRM - The Legal Issues: Computers & Law 16:5: Available at: http://www.scl.org/editorial.asp?i=1091

203 MoJ 2008 Ibid

204 ICO 2007: Data Protection Technical Guidance: Determining what is personal data. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf

205 The Guardian 17/06/2004: Custom-build councils Available at: http://www.guardian.co.uk/technology/2004/jun/17/internet.it

206 ODPM 2004: Local e-Government National CRM Programme: S1.0 Baseline Environmental Scan and Analysis of Good Practice in CRM by Local Authorities: Available at: http://www.productshare.org.uk/pp/publication/detail.asp?ID=18059 (requires free login)

207 Russell, P 2006: Ibid

208 ICO 29/01/2007: Technical Guidance Note: The use of personal information held for collecting and administering Council Tax Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/use_of_personal_information_held_for_collecting_and_admini%E2%80%A6.pdf

209 ICO August 2001: Data Protection Act 1998 Compliance Advice: Reproduced in "CRM Legal Compliance Standards", Paul Russell/ODPM 06/05/2004 Annexe 9. Available at: http://www.idea.gov.uk/idk/aio/1011868

210 eGovernment Register - database of local authority e-government activities maintained by Brent Council Available at: http://www.brent.gov.uk/egr.nsf

211 http://www.lagan.com/landing.aspx

212 Protecting the Right to Privacy in the Fight Against Terrorism. Commissioner for Human Rights, Council of Europe, Dec 4 2008, CommDH/IssuePaper(2008)3

213 House of Lords European Union Committee, European Union – Ninth Report, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/49/4902.htm

214 Europe claims UK botched one-third of Data Protection Directive, Out-law News, Sep 17 2007, at http://www.out-law.com/page-8472

215 R Anderson, I Brown, R Clayton, T Dowty, D Korff, E Munro. Children's Databases – Safety and Privacy. Information Commissioner's Office, November 2006

216 Gillick v West Norfolk and Wisbech Health Authority [1985] 3 WLR 830 [HL]

217 R (Axon) v Secretary of State for Health. Child and Family Law Quarterly, 19(1): 81-97

218 Ross Anderson, Nicholas Bohm, Terri Dowty, Fleur Fisher, Douwe Korff, Eileen Munro, Martyn Thomas. Consultation Response on the Data Sharing Review. Feb 15 2008. At http://www.fipr.org/080215datasharing.pdf

219 T Collins, Only a third of government IT projects succeed, says CIO. Computer Weekly May 21 2007, at http://www.computerweekly.com/Articles/2007/05/21/223915/only-a-third-of-government-it-projects-succeed-says.htm

220 H Curtis, B Krasner, N Iscoe. A Field Study of the Software Design Process for Large Systems. Communications of the ACM 31(11): 1268-1287 (1988)

221 R Anderson, Security Engineering – A Guide to Building Dependable Distributed Systems, 2nd ed., Wiley 2008

222 Report of the Review of Patient-identifiable Information, Department of Health, December 1 1997, at http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4068403

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.

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

fipr

foundation for information policy research

THE Joseph Rowntree
REFORM TRUST LTD

www.jrrt.org.uk

ISBN 978-0-9548902-4-7

£15.00