

Data Sharing Review: a consultation on the use and sharing of personal information in the public and private sectors

Response of the Open Rights Group

Detail of Respondents

Prepared by: Becky Hogge

Responding on behalf of: The Open Rights Group

Address: Open Rights Group
7th Floor
100 Grays Inn Road
London WC1X 8TY
United Kingdom

Telephone: +44 (0)20 7096 1079

Email: info@openrightsgroup.org

Website: <http://www.openrightsgroup.org>

Introduction

In a speech to the UK e-Summit in November 2002, Tony Blair, then Prime Minister, outlined his intention to harness the power of information technology to create “a new relationship between citizen and state”¹.

Such an endeavour should not be taken lightly.

The link between increased sharing of personal data and better delivery of public services is not evidence-based; it is merely asserted. In the rare cases that this link is not simply assumed, it is defended through misleading recourse to extraordinary cases of harm, such as the Victoria Climbié case.

In the meantime, the increased gathering and sharing of personal data is beginning to exhibit harmful side effects. Wholesale loss of personal data is one such side effect - not a

¹ Prime Minister's Keynote speech to e-Summit, 19 November 2002, available at: <http://www.annualreport.gov.uk/output/Page1734.asp>

symptom limited to HMRC, but presented also by the Ministry of Justice, the Ministry of Defence, the Department for Work and Pensions, the DVLA, and several police forces and NHS trusts in the last six months alone². Another side effect is the surveillance society, into which this country has both sleep-walked and now woken up³.

This review is therefore timely and we welcome the opportunity to respond to it.

The Open Rights Group

The Open Rights Group is a grassroots technology advocacy organisation, founded in 2005. Our core operations are funded by hundreds of tech-literate UK citizens who want their voices heard in national debate around technology issues. We speak out against the poor regulation and implementation of digital technology. We aim to protect and promote civil, human and consumer rights in the context of digital technology.

Technology

Networked, digital technology has a number of key characteristics which are pertinent to the issue of data-sharing:

- **Ease of storage:** thanks to development in component design and file compression techniques, the cost of storing digitally-encoded data is rapidly approaching zero.
- **Ease of replication:** digital technologies make it trivial to copy sets of digitally-encoded data.
- **Ease of transfer:** These first two principles combine to facilitate the easy transfer of digital data.
- **Automated data interrogation:** Sophisticated automated data interrogation techniques are constantly improving in their ability to produce new information from existing data sets.

As personal information about citizens is increasingly stored digitally, it is these characteristics which will fundamentally alter the relationship between the citizen and the state. Once the cost of destroying personal data exceeds the cost of keeping it, we will move

2 A comprehensive list of “UK Privacy Debacles” is maintained by the Open Rights Group community at: http://www.openrightsgroup.org/orgwiki/index.php/UK_Privacy_Debacles

3 We refer to the two most recent annual reports from the Information Commissioner's Office, available at: http://www.ico.gov.uk/about_us/what_we_do/corporate_information/annual_reports.aspx

into an “age of perfect memory”⁴. And as automated interrogation techniques are perfected, relying upon them to identify citizens who are, say, at risk of harm, will lead to a sort of mechanised compassion, a welfare state where automated discrimination trumps professional judgement and human dignity is eroded.

The impact of technological advance is better viewed as a challenge, and not an opportunity, for the delivery of public services. Until this fact is fully appreciated, and strategies have been put in place to meet this challenge, expanding either the scope or the spectrum of personal data-gathering and -sharing is irresponsible in the extreme.

Current technical architectures of schemes to facilitate greater data-sharing are unimaginative. Large databases which need to grant access to many hundreds of users will inevitably fail along one of three axes - scale, functionality or security. As recent high-profile cases of data loss demonstrate, it is most often the latter axis on which projects fail. Because of the value of personal details in the age of electronic commerce and identity theft, the risk models (in particular insider threats) associated with large datasets to which many people have access are simply too high for adequate security measures to be built in.

To a trained computer scientist, building secure databases that centrally hold large-scale datasets and grant access to many hundreds of users is intuitively infeasible. It is the equivalent to the layman's perception of the feasibility of building towerblocks 5,000 storeys high, or drilling through the centre of the Earth to create a high-speed rail link to New Zealand. Unfortunately, in the UK, trained computer scientists are poorly represented in key positions such as Parliament, the senior civil service and the media. Indeed, those trained computer scientists who do raise questions about the Government's plans to centralise ever-larger data sets in databases to which hundreds of civil servants have access have historically been sidelined or ridiculed⁵ by this Government, which eagerly listens to the sales pitches of commercial technology providers.

How might this and future Governments meet the challenge that technological advance poses to the delivery of public services? The methods suggested in the call for evidence -

4 Foundation for Information Policy Research (FIPR) response to the House of Lords Constitution Committee Inquiry into Surveillance and Data Collection, available at:
<http://www.parliament.uk/documents/upload/Foundation%20for%20Information%20Policy%20Research%20%28FIPR%29.doc>

5 In their Sixth Report, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, the House of Commons Science and Technology Committee found an “an inconsistent approach to scientific evidence” and “lack of transparency surrounding the incorporation of scientific advice”, particularly with regard to ICT.

encrypted hard drives, pseudonymisation, anonymisation - are ineffectual sticking plasters. Rather, the technical architecture of large-scale data-sharing and data-gathering projects needs to be turned inside out, putting service users in charge of the data that pertains to their condition (to control their identity and manage their health and finances, for example). A version of the "subsidiarity" principle should apply, with minimal sets of identifying information stored locally or nationally. The emphasis should be where it is in the legislation that protects personal details - on explicit informed consent to data-sharing on a case-by-case basis. Research on privacy-enhancing technologies is ongoing, but designing in a user-held token to unencrypt personal details each time a public service agency wishes to access them is one model.

Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Benefits

There is an apparent perception among public servants that "data-sharing" is in itself a benefit. This is odd: we might describe better service to the public, increased trust or financial savings as "benefits" but data-sharing per se is no more a benefit than are larger filing cabinets.

Just as banks introduced customer relationship management (CRM), Government is committed to offering "personalised" services. The banks' CRM systems promised to offer better and more appropriate services but have been disappointing for customers. First they were used to cut costs and depersonalise services into call centres. More recently they are used to identify and drive out unprofitable customers (such as the Egg credit card holders who repay their bills in full on time⁶). Similarly, a "Transformative" Government⁷ of personalised services based on data sharing is set to become a euphemism for cost-cutting, de-skilling and discrimination in which the computer says "no" and there is no recourse to human common sense.

At the extreme end of the scale, it is perceived that sharing information about individual children and young people's school or college performance, access to mental health services, and wider family situation could identify at risk individuals early on – even before birth - and promote intervention. Behind this lies the illiberal hope - on which the public is

6 See O'Connor, Rebecca, "Egg blocks card spending for 'sensible' customers", *The Times*, 4 February 2008, available at: <http://business.timesonline.co.uk/tol/business/money/borrowing/article3303975.ece>

7 We refer to the *Transformational Government* strategy published in November 2005. See <http://www.cio.gov.uk/documents/pdf/transgov/transgov-strategy.pdf>

not consulted - that massively shared data create a rich source of intelligence to keep society safe from terrorist threats and tackle criminality and deviance.

Early intervention in at-risk cases might be perceived to lighten the burden that anti-social individuals place on society. More broadly, a more efficient public service sector enabled by information-sharing could be perceived to deliver the aims of the welfare state more exactly, and at reduced cost to the tax payer. It was no doubt this perception that led the Government's e-Envoy, Andrew Pinder, to say in 2002 that the Government's target of putting all services online by 2005 "could cost 800,000 public sector employees their jobs"⁸.

But these perceived benefits are rarely backed up by actual evidence. Instead they rely on a simple cognitive metaphor which equates the digitisation and cross-agency analysis of personal details in the delivery of public services with the implementation of IT business systems on the factory floor.

In the same speech quoted at the beginning of this response, Tony Blair observed⁹ that:

"Many companies are already taking advantage. One example is sheet metal suppliers Allsops in Huddersfield who invested in technology to enhance their production process and improve customer service. Enquiries from customers can now be instantly answered from any of the company's networked computers. Customers in a hurry for a quotation can send detailed and complex computer-aided design drawings by email, enabling Allsops to respond quickly and effectively. It's given them competitive edge - and saved them time and money. "

It should be clear on deeper reflection that a system designed to supply customers with the amounts of sheet metal that they require will not necessarily scale to a system designed to deliver social justice. Crime prevention, social care, community cohesion, welfare, education and health rely on trust, on personal relationships and on professional judgement. Above all they rely on students who learn, people who maintain their own health and fitness, socially active citizens who keep neighbourhoods safe and self-respecting and who look after themselves as well as co-operating with authorities. Active, willing participation is far more important to public services than the wide availability of personal details.

8 See Lettuce, John. "E-government could cost 800,000 jobs, says e-envoy", *The Register*, 14 May 2002, available at: http://www.theregister.co.uk/2002/05/14/egovernment_could_cost/

9 Prime Minister's Keynote speech to e-Summit, 19 November 2002, available at: <http://www.annualreport.gov.uk/output/Page1734.asp>

Risks

Over-emphasis on the ability of information sharing to deliver social justice through improved public services is the obvious risk associated with this strategy. Beyond this, reliance on automated interrogation of large data sets to target services or predict social outcomes is likely to lead both to false positives, where individuals are unduly intruded upon because their data complies to some identified pattern, and to false negatives, where individuals at risk of real harm are ignored because of a lack of professional or localised oversight. Over time, automated, centralised control of public service delivery replaces local professional judgement and discretion and erodes the skills-base of professional public servants in the field. This also damages morale and effectiveness, further exacerbating the situation.

In the meantime, the catastrophic data losses that are inevitable if large datasets are stored centrally and accessed by hundreds of different people, will continue. This will significantly affect the lives of those individuals who, as a result, are the victims of identity fraud and harassment. It is also likely to further complicate - or even threaten - the lives of those who are fleeing abusive relationships or on witness protection schemes. The general public's trust in Government to safeguard their personal details has been seriously eroded, and nothing in the Government's data sharing plans will reverse this.

A long-term risk of increased data-sharing is a gradual, wholesale invasion of privacy. This should be of concern since privacy is essential to human dignity, and human dignity is the foundation for all human rights. The pervasive surveillance represented by some data-sharing proposals will ultimately undermine human dignity, and thus support for human rights. As security expert Bruce Schneier has observed, "it is poor civic hygiene to install technologies that could someday facilitate a police state"¹⁰: increasingly centralised, detailed profiles of UK citizens are just one of the good intentions which might pave the way at best to a more disciplinarian and discriminatory society, and at worse to one which undermines the basic principles of democracy.

Too much information

In both the public and private sectors, there has been a tendency to over-collect personal data.

For example, the Oyster Card, Transport for London (TfL)'s electronic ticketing system, retains centralised logs of individuals' journey details on an eight-week rolling basis before

¹⁰ See Schneier, Bruce, *Secrets and Lies: Digital Security in a Networked World* Wiley, John & Sons, Incorporated, August 2000

anonymising the data and retaining it for research purposes. Such data have never been collected before, and have the potential to present a detailed picture of an individual's life. The merits of storing such data centrally are not immediately clear from the perspective of functionality. It is therefore unclear why this feature was built into the system. Why, if the data are primarily being used for research purposes (as is stated by TfL) are they not anonymised immediately?

A Freedom of Information request to TfL revealed that between August 2004 and March 2006 TfL received 436 requests from the police for Oyster card information. Of these, 409 requests were granted and the data was released to the police¹¹.

In this example, a whole new data set, capable of revealing detailed pictures about individual's private lives, has been created without public consultation or even justifiable public function. Through it the police have gained greater investigative powers, again without public or Parliamentary consent. Transaction records, such as the data collected by TfL's Oyster Card scheme, are a powerful surveillance tool, and their collection, storage and sharing should ideally not take place at all. Where they are collected, routine access to such records must be strictly limited to a few, fully-accountable individuals within the organisation. Sharing with law enforcement agencies must continue to take place only on a case-by-case basis, under the provisions of the second principle of the Data Protection Act. We are concerned that future projects, such as the National Identity Register, will tend to over-collect transaction records without thinking through the ethical implications of owning such detailed pictures of individuals' lives.

In this regard we also note the agreement between TfL and the Metropolitan Police to share data sets generated by the network of automated numberplate recognition cameras that enforce the London Congestion Charge for the purpose of serious crime investigation¹².

Where new data sets are being created, as in these examples, data subjects need to understand both the protections afforded them by the DPA, and the precise circumstances where those protections might be over-ruled. Further, there should be no financial or welfare sanctions imposed on the subject should they not agree to the purposes to which their data

11 See <http://www.coofercat.com/wiki/OysterCardRFI>

12 For a thorough analysis of function creep in the use of automated numberplate recognition cameras, see "Surveillance State Function Creep - London Congestion Charge 'real-time bulk data' to be automatically handed over to the Met etc", available at Spyblog: http://p10.hostingprod.com/@spyblog.org.uk/blog/2007/07/surveillance_state_function_creep_london_congestion_charge_realtime_bulk_data.html

may be put. Only then can we say that an individual data subject has truly consented.

The law

It is clear that processing of personal data beyond the specified purposes under which that data was obtained is precluded by the Data Protection Act in the absence of further consent, except in extraordinary circumstances. Such extraordinary circumstances include the prevention and detection of serious crime and the protection of children at risk of harm. They do not include more general aspirational purposes like improving public services or doing medical research. Personal autonomy should only be overridden on the basis of necessity, and not on the basis of convenience.

Data protection remains an externality to most data controllers: financial, social and personal costs associated with poor data handling and data loss are generally born by someone other than the data controller, and sanctions imposed by the Information Commissioner continue to be too small when compared to the relatively large costs of correctly handling and securing personal data.

As we have previously noted¹³, the present powers granted to the Information Commissioner's Office are not commensurate with the data protection risk presented by advances in data-collecting and data-mining technologies and practice. In particular, we believe that the Information Commissioner should push for the right to audit and inspect, without having obtained prior consent, any commercial, public sector or third sector organisation where poor data protection practice is suspected.

We are concerned by the weak enforcement of the Data Protection Act to date. For example, when “[a] string of high street banks and the Post Office [break] data protection rules by dumping customers' personal details in outdoor bins”, we would expect a greater penalty than the signing of “a formal undertaking to comply with [the] Data Protection Act”¹⁴. We believe that the Information Commissioner's Office should be able to impose stronger and swifter penalties, including criminal sanctions, on those who breach the Data Protection Act. We believe it is appropriate for the Information Commissioner's Office to demand powers similar to those of the Health and Safety Executive. The Data Protection Act will not be taken

13 We refer to the Open Rights Group's response to the Information Commissioner's Office Data Protection Strategy Consultation of 27 September 2007.

14 See Press Association “Banks 'dumped personal information in bins” *The Guardian* 13 March 2007 <http://money.guardian.co.uk/saving/banks/story/0,,2032962,00.html>.

seriously in businesses at Board Level until this happens. We support the idea of a data breach notification law.

We note in the tone of the consultation document a reluctance to burden business, which indicates that the rhetoric¹⁵ of those opposed to the Data Protection Act has to a certain extent sunk in. We therefore feel it is prudent to point out the benefits that data-gathering and data-mining have offered modern business. For example, it is partly the success of the Tesco Clubcard that commentators have suggested allowed the retailer to overtake Sainsbury's as the UK's top supermarket in the 1990s¹⁶. It is our belief that business would be highly likely to comply with stronger regulatory pressure from the ICO rather than stop collecting personal data.

Conclusion

Data sharing is a risk and a responsibility. It is not in itself a benefit.

If customers were to participate fully in the design and decision-making of the public services intended to benefit them it seems to us very unlikely they would come up with the centralised databases and data sharing approach of Transformational Government.

Proposed technological solutions are infeasible. Viable alternatives are still in their development phases. The regulatory environment is weak, under-resourced and immature. The public debate over a civic infrastructure centred around shared personal data and pervasive surveillance never happened. The advance towards greater data-sharing at this stage is therefore reckless and irresponsible.

15 The Data Protection Act was labelled “expensive bureaucracy” by the Conservative policy group in their recent publication *Freeing Britain to Compete*

<http://standupspeakup.conservatives.com/Reports/FreeingBritaintoCompete.pdf>

16 See “Stores at War: winning secrets” *bbc.co.uk* 4 June 1999

http://news.bbc.co.uk/1/hi/business/the_company_file/360997.stm