

Data Sharing Review Secretariat  
5.26 Steel House  
11 Tothill Street  
London SW1H 9LJ

14th February 2008

Dear Sirs,

Data Sharing Review Consultation Response

This letter is my response to the data sharing review, submitted as a member of the general public. Many of the questions on the review form have no relevance to me, so I have not used it, but instead set out my points below.

1. I am happy to be contacted about this review at the above address. No part of this response is confidential.

Data Protection Act. The Data Protection Act, and in particular the second principle cited in the review document, provides useful protections to the public from the misuse of personal data by commercial organisations.

However, government gave itself exemptions from the original Data Protection Act, and now seeks to dramatically broaden these exemptions under the banner of “Transformational Government”. The aim seems to be to allow wholesale sharing of personal data between government departments for purposes for which the data was not originally surrendered, and without the consent of the data subjects. This amounts to government giving itself a blanket exemption from every important aspect of the DPA. Despite Ministerial protestations of “efficiency” and “public safety”, the transformational government programme is indefensible, and must be suspended. The DPA must apply equally to government departments as it does to commerce.

In fact, there is an argument that DPA principles should apply more, not less, stringently to the public sector, precisely because the public usually cannot withdraw from using the “services” of most government departments. For instance, I have a statutory duty to provide my car registration details and address to DVLA for the purposes of taxation and law enforcement. However, since 2002 DVLA has taken it upon itself to sell these details to any car park owner which believes it has a private grievance against me. I cannot legally stop using DVLA’s “services”, and neither can I prevent it selling my personal data.

This small, recent example of a public body which uses data in contravention of DPA principle 2 has been corrosive of public trust in DVLA over the past five years. The “transformational government” programme to widen these exemptions in the name of the efficiency would destroy public confidence in government’s ability to defend individual privacy and security, and ultimately be completely counterproductive.

2. Use of personal identifiers. The United States has very high levels of identity fraud, with 3-5% of the population saying they've been victims each year. Much of the blame for this lies with the US Social Security Number, a nine digit identifiers for each legal US resident first introduced by the federal government in 1936, and now used as de facto national identification number by most of government and industry. The State of California calls SSNs, "the key to identity theft", and Americans are universally advised to try to keep them secret – which is largely futile, since someone's SSN is known to almost every organisation where he has a long-term financial relationship. There are many documented cases where simply knowing someone's name and social security number allows a fraudster to run up large debts in that name. Australia has similar problems; the introduction of an extensive Tax File Number has also increased identity fraud well beyond levels found in the UK.

The UK's relative lack of identity fraud is precisely because everyone is identified by different record numbers to different government agencies and private companies. While having separate identification numbers with the NHS, HMRC, DVLA, insurance company, gas board etc. may seem tediously inconvenient, it usefully "compartmentalises" identity information, ensuring that someone getting hold of one identification number would not automatically be able to impersonate that person to any of the other organisations (as would be the case in the US or Australia).

A central plank of central government's plans for "Transformational Government" is the National Identity Scheme (NIS), which would assign to each individual a single "National Identity Registration Number" (NIRN), with the long-term goal of using it to link personal records across all arms of government. Since legislation does not prohibit private companies from using NIRNs as customer identifiers, that would likely also become widespread over a period of years. The introduction of NIRNs would thus create perfect conditions for remorseless increase in identity fraud over the coming decades.

Hence the creation of a single cross-government cradle-to-grave citizen numbering scheme is a disastrous idea, and must not be allowed to proceed. Leaving aside all the other objections to the NIR which are outside the scope of this response (such as the vast cost, and potential for government supervision and monitoring of the individual's private affairs), this one aspect should be reason enough to cancel the NIS, because of the huge, long-term adverse effect it will have on identity fraud.

Yours sincerely,