

USE AND SHARING OF PERSONAL INFORMATION
IN THE PUBLIC AND PRIVATE SECTORS
REPOSE

This submission has been prepared specifically for the consultation. I am submitting this as an individual. I am an IT professional with 15 years experience working in software and website development. I work extensively with databases and am aware of the dangers inherent in them.

USE AND SHARING OF PERSONAL INFORMATION **IN THE PUBLIC AND PRIVATE SECTORS**

The following submission is a response to questions 27 and 28 of the consultation document.

1. The use of data sharing in the public and private sectors is eroding UK citizens' privacy. Anonymity is not a crime - English common law is built upon a right to anonymity implicit in the right to go unchallenged provided you are not doing something specifically legislated against. Yet it is becoming increasingly difficult for law abiding citizens to enjoy any meaningful sense of anonymity.
2. Data sharing should be for the benefit of the citizen and should only be allowed where explicit consent is granted by a citizen. The government's desire to remove current safeguards and allow wholesale data sharing would further erode and even abolish UK citizens' privacy.
3. Public sector data sharing is the cornerstone of the government's controversial Identity Card scheme – or more specifically the database behind the scheme, the National Identity Register. To understand how data sharing and the ID scheme are intrinsically linked, it is necessary to look at the way in which databases can be used to automate the sharing of data.

The tools of data sharing

4. The use of computer databases is at the heart of the government's data sharing agenda and yet the inner workings of database software is not known either to law makers or to most members of the public. As a result the true implications of widespread data sharing are not appreciated by the people who want to introduce such measures, or by those they will affect.

Concept of a database key

5. Data within a database is organised into database tables. Within the tables each record requires a unique identifier known as a key to distinguish it from other records. The current situation affords the citizen at least some privacy. If two organisations hold information about a person in two different databases, one organisation might give that person's data a key of '01' and the other might use a key of '23'. The two organisations would not easily be able to exchange data about the person because the databases would not be able to link the two records and so human intervention would be required.
6. A system of universal unique record keys, such as the proposed National Identity Register Number, would allow the two organisations to link the two database entries readily. In fact if such a system were introduced it would be possible to link all existing database records in all organisations using that person's unique key.
7. If privacy is: “The desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behaviour to others”¹, then such a system would abolish privacy. The government's desire to number every

1 A.F. Westin, *The Right to Privacy*, Atheneum, 1967.

citizen with a National Identity Register Number, or in the case of children a Unique Learner Number, suggests that just such a system could be created in the UK and this is unacceptable.

8. Even if a state created citizen numbering system were not used to identify individuals, the level of data sharing without explicit consent or knowledge of the citizen proposed by the government is unacceptable.

Privacy

9. The United Kingdom lacks an explicit privacy law. Where supposed safeguards are in place they are riddled with opt outs such as “national security concerns”, “fighting serious crime” and “the smooth running of public services”. Such opt-outs make existing safeguards toothless. Concepts such as “implicit consent” are being used to hide the fact that citizens increasingly have no choice in the way in which they interact with the state. There is clearly an urgent need for a privacy law that can protect the citizens of the UK.
10. In Germany, where much tougher privacy laws exist and they are more acutely aware of the dangers inherent in giving too much information to the state, the government is not permitted to create a central database of biometrics for their ID cards. In addition ID numbers are linked to the actual card rather than a citizen and when a card is replaced a new number is issued, thus preventing many of the problems associated with a unique database key.

Nothing to hide?

11. Recent high profile losses of personal data by government departments such as HM Revenue & Customs have shown how hollow phrases such as “Nothing to hide, nothing to fear” really are. 25 million UK citizen's receiving Child Benefit had done nothing wrong but clearly they did have something to fear from the state claiming to be guardian of their information.

The private sector within government

12. Increasingly private companies are doing work inside government and therefore widespread data sharing raises serious concerns about accountability of private companies and the degree to which the public may find out who holds what information about them.

13. Ownership of data

14. Citizens should own their own data and the state should always seek judicial approval to access such data. Removing essential checks and balances from the system will put citizens at risk.

Joining the dots

15. In the United States the Pentagon set up its Total Information Awareness (TIA) project in 2002 to capture the “information signature” of people to “assist tracking terrorists”. In 2003 the US congress stopped funding the project but its work has been continued by a myriad of other data mining and data sharing projects.

16. In the UK when data sharing is viewed in conjunction with projects such as 'Transformational Government', the recent 'Service Transformation Agreement', measures introduced in the Serious Crime Act 2007, Regulation of Investigatory Powers Part III, and the National CCTV strategy you begin to see the UK government's compulsion to surveille and their very own de facto Total Information Awareness project.
17. We need to ask serious questions about how free and functioning our democracy is. There are not enough safeguards in place to protect citizens from an over-bearing state and the proposed levels of data sharing would exacerbate the situation further.
18. "We shall find, in ten or twenty years time, that serious crime has risen yet further, terrorism will be more strongly embedded and law enforcement agencies will still be failing in their intelligence and ability to prevent such activities. Yet we, as decent citizens, will have sacrificed completely our rights to privacy and anonymity. This is a very serious matter." ('Biometrics and privacy: A sacrifice worth making?', Julian Ashbourn, 'Biometrics' Times supplement, 31st July 2006)