

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to **contact@datasharingreview.gsi.gov.uk**

Alternatively you can send a hard copy response to:

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

Thank you.

Section 1: Background

Question 1.

I am a member of the public who has had data about myself collected by and for various government agencies and by a number of data collection agencies over the course of my lifetime. I have voluntarily and freely given information of a personal nature to medical / legal and other professionals and to local and national government departments for various and several reasons. I have done so on the clear understanding that this data would always be protected and safeguarded from any and all others who may for any reason seek to access it.

While I have never had any objection to the addition of such information anonymously to state / governmental databases for statistical purposes, I have never given such information to any agency on any other premise than that it should always be protected and under no circumstances be 'shared' or in any way distributed or published, or be made accessible to any other state / government department or commercial / charitable [or any other type of] organisation for any reason whatsoever, up to and including national security or national / international criminal investigation or law enforcement purposes.

Since the adoption of monetarist policies by the labour party and the subsequent dilution of the concepts of accountability or responsibility to a voting public have been enshrined in legislation, it has been more than amply demonstrated that where a profit motive or even the slightest perceived personal or commercial advantage is at stake no duty of care or previously sworn oath has precedence or legal standing and the precepts of social responsibility, personal morality or moral authority have been effectively abolished.

Under these conditions and coupled with the ever increasing monetary value of personal data to commercial interests the idea of data 'sharing' is criminally irresponsible.

The fallibility of data security is patently obvious and the fragility and susceptibility of systems designed to protect data is well known. Even the most 'secure' data systems are penetrable [as any major financial institution can testify] and given the fallibility of human nature and even using a most conservative estimation of human error it is inevitable that any loosening or deregulation of control over personal data will lead to unacceptable levels of 'leakage' and the idea of personal privacy [and therefore of human dignity] will become a risible 'historical' concept.

Comments:

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2. There are no benefits to the individual from data sharing, quite the opposite will be the case. It would hasten the end of 'civil society', devalue completely the whole idea of individual freedom and hand over the hard won rights of the individual to any state or corporate body, and therefore to any person or persons in control of such a body, for any and all purposes that will seem convenient or pleasing to them at any time.

Comments:

Question 3. . Only the most unimaginative and ill informed body would need to have the risks ['key' or otherwise] to individuals and society at large explained and exemplified.

Think just for a few moments about why every country on the planet has a secret security service and what the aims and objectives of those services are.

Then think of the damaged to an individual, to a family, to an ethnic or religious group or indeed to a whole society, if data concerning their performance and behaviour at school were to be released and published. Think of the damage to an individual if data concerning their health, physical, mental and / or emotional, was to be accessible to persons unqualified to evaluate it and under no legal compunction to preserve its anonymity. Contemplate the nature and tenor of a society in which personal information is treated as a commodity. See the prices and values placed on 'anonymous' demographic statistics collected by the commercial 'social networking' sites and consider the increased prices and values that would be generated for 'personalised' information to individuals and commercial organisations. The recent spate of news articles about data losses are only the very smallest tip of the iceberg compared to the reality which already exists. To considerably widen the accessibility to data and to broaden its availability is simply an invitation to greater abuse and an excuse for even greater laxity in data protection.

Comments:

Question 4. While it may be of benefit to society and the individuals who make up that society to have better designed, more flexible and above all more accurate data available within one particular department of public service, i.e. the health service, it cannot be argued that sharing that data across disciplines and departments will be in any individual's interest.

As it stands there is a legal requirement that that the data held on any single individual should be made available to that individual. In practice it is almost impossible for any individual to actually get hold of that data without paying a considerable fee for the 'privilege' of seeing what data is actually held on them and a premium for getting it copied and or sent to them. In effect it is actually more difficult for an individual without training or specialist knowlege to access any data held on them without paying a third party 'agency' with this specialist knowlege to access, collect and collate such data and of course an individual has no way of checking if the data is complete or not.

The scope of information available on 'classes' of people, defined by age, gender or any other arbitrary division is astonishing, and obviously a powerful tool for any marketing company seeking to place advertising or product most efficiently. The power of demograhic statistical information has been well understood for a long time but in the last two decades it has become the holy grail of both sales and propaganda. The fact that an individual's actual personal details can be distilled back out of a swathe of statistics has only recently been understood by those with responsibility for handling and protecting the greatest quantities of it but as yet a state of total denial is maintained in order to protect public 'confidence'.

Comments:

Question 5. In my view public authorities hold too much of some kinds of data and in other cases insufficient data.

For example the data held by the Home Office on me is thorough and comprehensive, [if highly subjective and inaccurate in many places] but that held by the NHS is patchy and incomplete. I am expected to inform any and every health professional who ever deals with me that I have a fatal allergy to penicillin, and once when I was delirious and suffering from severe septicemia I was actually injected with penicillin which induced a coma and necessitated extreme emergency treatment to save my life. The present state of the NHS 'IT for Health' programme is so parlous that it is a national scandal and yet we are informed that it ought to be fixed 'early this year'. When I made a complaint to the local NHS trust about the dreadful inefficiency and hopelessly inadequate nature of both the appointment booking software and the Doctor's case record software I was informed by the chief executive that 'the doctor can access a patient's records, images and data from the computer on their desktop', but in practice I have found that this is seldom the case. It is impossible to book an appointment to see my GP in advance and I have to enter a Darwinian system of fighting for a phone line at the surgery on the morning of the day I wish to attend a surgery for a consultation with my GP. This same surgery has no system in place for leaving messages for ones GP and the reception staff in the majority do not have English as their first language.

Comments:

Question 6. Personal data has recently become one of the most sought after commodities there is. The legislation to protect an individual's privacy is so hopelessly inadequate and so poorly policed that it may as well not exist at all. It is impossible to buy things from some internet vendors without providing them with more personal data than I would feel comfortable sharing with a legal or health professional and it is then collated and copied and sold on to any group or individual with the price and the perceived need. This sort of protection needs to be beefed up considerably and the ability of so called 'social networking' internet sites to collect, collate and sell-on data needs to be severely curtailed and enforced by heavy gaol sentences and swingeing financial penalties.

I have been refused services because I wish to keep my date of birth private. I now refuse to deal with any organisation that wants to collect my personal 'details' before they will do business. I am a free born Englishman and I have certain hard won rights for which I will gladly fight if I have to. I will not surrender such guarantees and privileges for the ease and convenience of any entrepreneur with something to sell.

Take a look, if you are really interested, at the latest pamphlet sent out to British Gas customers explaining their recent 'rule' changes, the section on privacy protection is as fine an example as I could hope to find of the overweening double standards of business interests in this corporate friendly political climate. It boils down to admitting that it will pass on [sell] all the data it has collected on you to almost any organisation that asks for it on almost any pretext. Yet they are entitled to do so and not to admit having done so by cast iron rulings and draconian legislation enshrining the inviolability of 'commercial sensitivity'. The laws on 'fraud prevention' actually encourage agencies and organisations to 'share' data in the supposed interest of protecting their money but not in the interest of any individual's right to privacy.

Comments:

Question 7. I have nothing to say in favour of 'sharing' information held on individuals and can see almost no situations where it might be beneficial to do so. Allowing the private sector equal access to local and national governmental and state agency's data banks is like giving copies of the Bank of England's keys away with 'Burglar's Weekly'.

Comments:

Question 8. I believe it to be true that for a relatively trivial sum of money, most national databases are open to any buyer. Certainly the Police are usually happy to 'help' their 'friends' in the fourth estate with classified information, for a small consideration, while Town and City hall employees are sometimes seen and heard auctioning off such data as they can 'safely' access to all comers. The civil service is probably the largest employer in the country and yet it is one of the slackest in applying good security practice to its employees. How many successful prosecutions have there been of persons failing in their duty to keep personal data secure?

The National Health Service holds data on every single service user and on all of its employees and it will share data with drug companies or investigators for a fee or as a 'duty'. It cannot be held accountable for failures to remove personal data from statistic collection exercises and any number of 'consultants' and 'professionals' can gain access to this data with a reasonable sounding excuse.

When it comes to being 'ex-directory' individuals are never consulted. I have evidence that primary school age children are frequently asked to supply information on other family members and are sometimes coerced into giving information about themselves or their families which is then used by 'experts' to decide what is best for them. Nobody could object to social services being given information which might help an otherwise endangered child but when education professionals and social workers make blunders and mistakes with devastating consequences they are seldom held accountable and the local authorities which employ them are never held to account for any of their errors.

Comments:

Section 3: The legal framework

The DPA simply doesn't work. It is a toothless chimera which is ignored as a matter of course.

Comments:

Question 10. The 'second' principle [can there actually be such a thing? isn't it oxymoronic?] doesn't seem to enter anyone's head when they want to use data for purposes other than the one for which it was initially gathered. Who or what is there to actually police data protection? While the principle is invaluable there is nothing to make it enforceable.

Comments:

Question 11. The DPA is totally ineffective, ask any reporter or investigator.

Comments:

Question 12. Heavy prison sentences and massive financial penalties should be imposed on any who seek to profit or gain from accessing such data. Software exists which could alert appropriate bodies of attempts to access data and far more rigorous protocols need to be put in place to protect such data from unauthorised access or copying and more random checks on personell with access to such data need to be carried out.

Comments:

Question 13.I am not qualified in any way to have an opinion on such laws as may exist.

Comments:

Question 14. see above.

Comments:

Question 15. Why should anyone care about the 'burden' placed on business, whether reasonable or otherwise? In comparison to the issue of personal privacy and the freedom of the individual no burden can be considered too great or unreasonable if it protects our privacy and freedom.

Comments:

Section 4: Consent and transparency

Question 16. Nothing about this is clear. How is an individuals consent to be sought? I am no clearer on about the form such consent should take than I am that my consent has ever been sought when information about me is shared between public and/or private bodies.

Comments:

Question 17. All such barriers are purely notional and the reality is that personal information is up for grabs to all and sundry. Requirements to gain consent will remain meaningless unless they can be checked and enforced.

Comments:

Question 18. Individuals should have absolute rights of acces to all data held on them by all bodies in all forms. Organisations must do much, much more to justify and explain their use and sharing of data .

Comments:

Question 19. By not hiding the whole issue away from the public and making it the duty of all data collecting bodies to be absolutely open and truthful about what data they will hold and how they will use it and how they will safeguard it.

Comments:

Section 5: Technology

Question 20. Technological advances have occurred so fast and with such huge impact on this issue that no assessment of their impact would be meaningful for long enough to be worth commissioning.

Comments:

Question 21. Yes, 64 bit encryption should be the minimum acceptable standard, and the 'portability' of a device is simply a red herring. Wake up!

Comments:

Question 22. Privacy enhancing techniques would be of minor use but are better than nothing. The trouble is that with a minimum of two separate data sources using different anonymisation techniques all such techniques would be rendered hopelessly inadequate and with more than two sources all such techniques would be useless.

Comments:

Section 6: International comparisons

Question 23. Unfortunately I am not aware of any such jurisdictions or frameworks.

Comments:

Question 24. No.

Comments:

Question 25. No

Comments:

Question 26. Yes, try and sell data sharing to the population of New Zealand and see how long it takes to get tarred and feathered.

Comments:

Section 7: Additional questions

Question 27. Too many to put into this questionnaire.

Comments:

Question 28. I suggest you ask every periodical publication to carry copies of this questionnaire and to provide freepost envelopes with them. I think you would be surprised at what you would learn, even if they were all anonymised or pseudonymised.

Comments: