

Data Sharing Review

Richard Thomas and Dr Mark Walport

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.

NO2ID is a campaigning organisation. We oppose broad government data-sharing and population registers, as altering fundamentally the relationship between citizen and state, and damaging both privacy and liberty.

For that reason in what follows we frequently take issue with the questions. The Review in our opinion can achieve nothing if it strives only to “balance” the unequal fight between the existing legal constructions of data protection and the pursuit of corporate goals and administrative expediency. We submit that if it chooses to work in ill-fitting categories, the problems created for individuals and social institutions by the technological propagation of personal information cannot be made sense of, let alone solved. We do not hold ourselves out as having complete answers, but we do have some proposals towards a coherent framework for privacy in society.

All organisations of any size collect personal data for their management purposes. We collect and hold contact details in relation to some 40,000 individuals and organisations, and in some cases details of financial contributions and other personal contributions. We also have accounting records.

We do not share the information we have without specific individual approval to giving one party’s contact details to another identified person or (rarely) to publishing them.

We do provide email and web facilities, such as all-mail-all email lists and web forums, on which it is open to individuals to publish their own information. We accommodate anonymity and pseudonymity for our contacts as far as is practicable, and we do not seek to verify individual's 'identities' save in the exceptional circumstances when there is a good reason to do so.

The information is held in a variety of password-protected electronic forms, accessible to limited numbers of known people, and on paper held in our offices. In the case of our main contact address records, these are now in a proprietary database which is password protected at more than one level. Backups are physically as well as password protected.

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

Question 2.

Comments:

The question is ill-posed in making a bipartite distinction between the benefits to individuals and to society. There are no intrinsic benefits of data-sharing (which is a name for a wide class of processes or acts, not a coherent thing), and we do not accept the implied trade-off between individual privacy and any generalised social benefit. While all social relationships depend on some form of communication of personal information, data-sharing is purely ancillary to the relationships and individual or collective enterprises it facilitates. Individuals and groups within society can benefit from data-sharing that facilitates their aims, which aims may well conflict; conflict both with the interests of other groups and what NO2ID sees as the rights of privacy and personal control that belong to individuals. NO2ID regards privacy and personal control of personal information as primary goods, interfering with which requires specific justification in each case.

A more useful distinction in this discussion than that between individuals and society is that between the "users" and "objects" of data-sharing. Users can be large collective enterprises, and objects need not be individuals. Yet objects can also be users. That a system involves a powerful collective user or a large set of objects may lead one to mistake the user(s) for "society".

In any data-management system the effects for objects and users are not separate. But their interests can easily conflict. Objects always lose privacy and control, and such losses ought to be minimised and compensated as a matter of principle. It is possible for users to benefit without any benefit for the objects – and therefore at their expense. Such "parasitic" cases require strong justification in public policy. That sharing personal information would be useful for the user is not enough, even if the user is big and powerful enough to be confused with "society".

Question 3.

Comments:

The language of risk is also inappropriate. It implies ready quantification, which as we point out below is not straightforward even with a much clearer framework of rights in place.

A sensible analysis distinguishes between risk (quantitative) and hazard (qualitative). We can describe some of the hazards of typical data-sharing activities. We cannot quantify them (which is hard to do even in a specific case), though we can be clear that some forms of data-sharing have considerably more capacity to do harm (and thus represent in some sense a higher risk) because of the nature of the use to which information will be, or may be put.

We would distinguish between the “internal” and “external” hazards of massive information processing. External hazards are those arising from mis-use of the systems in their own terms – where an unauthorised outsider obtains information from the system or an authorised person uses it in an unauthorised way. Security measures usually purport to deal with external hazards. Internal hazards are more subtle, and arise from unintended consequences of authorised use; they are built-in.

External hazards include: misappropriation (including “identity theft” and various frauds), use for criminal purposes other than fraud (blackmail, intimidation, the tracing of specific persons for persecution of various kinds), and simple exposure which might be embarrassing or socially harmful to the objects of exposure, or give rise to fraud or other criminal purposes.

Internal hazards include: use of information that is oppressive in effect (even if not necessarily in intent), corruption of data, unlimited propagation of errors, interpretive mirages, unsuitable or unverified data used without sufficient knowledge of its provenance and the risk of resistance to legitimate use as the objects of data traffic withhold information they fear may be shared for other purposes.

It is worth noting that objects are directly injured by such hazards (or fear of hazards); the consequences for users and others are emergent or consequential on the changes in behaviour of objects. It is easy for users to think everything is fine from their point of view, but the system may not behave in predictable ways.

Question 4.

Comments:

Hazards are enhanced by structural distance between the source of the data and its use which implies more scope for loss or corruption. Sharing by proxy, wide sharing and multiple sharers imply creating many more opportunities for interception for misuse, or use for unsuitable purposes, to outweigh the objects' gains where there are any.

The nature of the information is of course critical to the consequences of misuse, but even quite limited semi-public information can be a severe danger if accessible to the wrong people, as the animal rights extremists' use of company registers shows.

Question 5.

Comments: "Too much" can be quantified in several ways. It is not just the collection of unnecessary information, though that is rife. Information can be held to too many purposes. (There is a temptation to add catch-all provisions to pre-empt problems.) Or it can be held for too long – typically, in public sector cases, for ever. There are very few cases where public authorities do not hold more personal information than is legitimately required for the purpose it is purportedly collected.

Examples where the information held is grossly disproportionate to the purpose include:
Scottish Citizens Accounts
ITSO travel cards
The use of children's biometrics in schools and colleges

We are not aware of any cases where public authorities do not hold enough information, though there are plainly many cases where the information held is not of good quality, or well applied to the purpose.

Question 6.

Comments:

Examples where the information held is grossly disproportionate to the purpose include:
Many proof of age schemes
Fingerprint and document-scanning systems for entry to pubs and bars (e.g. Club Scan). (These latter often involve a situation where the collection and sharing of data is notionally voluntary, but effectively coerced, for both the objects *and* the primary user, as licensing authorities in some areas make them a license condition, citing their statutory duties under the Licensing Act 2003 as justification.)

A particularly subtle, complex but egregious example is found in the Facebook social networking software, where the degree of sharing is very largely up to the member - but there is no way back. The company claims to own the right to keep and display any of the data uploaded to the member's account - for ever. There the disproportion is both qualitative – an inadvertent or casual decision is

completely binding – and quantitative – the sharing of a momentary idea is eternal.

Question 7.

Comments:

There are none of which we are aware. The question begs another: beneficial to whom? As we indicate above, we don't assume that a notional benefit to a user can be traded off against the cost to the object.

There are frequent examples of organisations that do not have adequate procedures for authenticating customers, or which use "data-protection" as a pretext for making non-standard interactions difficult, which get put forward as evidence that privacy law interferes with people getting on with things. But these really have little bearing on the issue.

Question 8.

Comments:

In almost every case where information traffic takes place the data collected is greater than necessary, held for longer than necessary, and is collected for formally much broader purposes than the original context of collection would indicate.

A specific example of personal information being shared where it should not be is the NHS 'Secondary Uses Service'. The wholesale sharing, or selling, of medical data (even in pseudonymised form) without the explicit consent of the patient risks undermining medical confidentiality and the public health. If people no longer feel that information shared with their clinician will remain private, some may withhold details that could affect their diagnosis or treatment – which, beyond being a personal health hazard, may allow diseases to spread.

Such erosion of trust illustrates a general problem with creating universal data-traffic mechanisms, even where specific additional measures may be applied to data considered more sensitive, e.g. HIV/Aids or STD-related.

Section 3: The legal framework

Question 9.

Comments:

We are rather sceptical of the value of the DPA.

The data protection regime copes particularly poorly with the activities of public authorities, which can, in effect, have the law rewritten so they can do what they like. But in our view the institutional model of regulatory oversight is very badly matched with an infinite number of infinitely various items to police. The resources available to the Commissioner are tiny (compare the hundreds of millions deployed by Health and Safety officials) and controlled by the state which is potentially his principal opponent

Data Protection is just like society overtaken by technological change. We note that it really wasn't invented to control the database state, as it now is. Its origins are in consumerism (junk mail control) and employment relations (which latter is responsible for the decision in the 1998 Act to extend the scope to paper records). The conception of an invertible file in the discussion surrounding the 1984 Act is actually more prescient and relevant than much more recent material. The Principles are a brave attempt to future-proof, but broad principles are scope for cajoling of users rather than actual enforcement of the rights of objects.

There are massive exceptions for public authorities already (even on the face of the 1998 Act) and every new item of legislation creates more – particularly where the aim is specifically to permit data-traffic. A classic example is the Serious Crime Act 2007, where one section amends the DPA to get it out of the way and then another section affirms it (as amended) as a figleaf for parliament.

We would like to see a more accessible legal regime based on a much more clearly defined approach to data-use, the upholding of confidentiality, and directly enforceable remedies for individuals.

Question 10.

Comments:

The principle is adhered to scarcely at all, in spirit. In practice there are frequently catch-all provisions, so that a user can be assured they have always an excuse.

An arrant example (though a statutory one) is the definition of “necessary in the public interest” in the Identity Cards Act 2006, which captures any conceivable function or activity of government as a purpose for which the information in the Register may be processed.

A more typical one is found in surveillance camera notices with references to the

prevention of “crime and disorder” and to “public safety”. Neither disorder nor public safety is well defined, and “prevention” effectively justifies the use of information on all those occasions when no crime is occurring.

We think the principle is a very good one and ought to be strengthened. A version of the second principle is at the core of our proposals for “information privity”, but we do not think it is actually effective in current practice save where information users make no effort to avoid it.

One cannot erect a proper system of rights over information traffic without the rights actually granted being appropriately limited. The very least that can be done here is to create a default limit of time during which the information may be held and processed. But we would like to see much stronger control on purposes – which is to say information should not be collected or distributed save for the purpose(s) that would be reasonably attributed to the object in providing the data. It should not be possible to add further purposes in small print that are effectively conditions of service.

That is: *the object’s purpose, not the user’s purpose should control*. Much current legislation allows “whose purpose?” to be moot.

It will be objected that information ought to be obtainable by police and intelligence services, and so adding riders about “detection of crime” (and so forth) serves society. Let them obtain a warrant. Obtaining personal information of specified individuals is effectively a personal search. That requires good reason. Obtaining personal information of unspecified individuals by “data-matching” or “data mining” or sampling files is in effect a general search warrant and ought, we submit, to be subject to much stricter control.

Question 11.

Comments:

There are few technical barriers. But technical progress has outpaced the social grasp of its powers. Data trafficking has become easy to do even without thinking about it. The HMRC case is one of the clearest examples. In order for data protection to be effective, there have to be barriers to breaching it inadvertently, and appropriate sanctions to deter the casual security menace. (Though sanctions on individuals are certainly not sufficient, punishment being no cure for the damage done.)

There are strong institutional barriers. Leaving aside that the legal structures of the DPA are not robust. It is in the interest of users to subvert it. This is a classic public choice problem. Many millions of individuals with no clear idea that there is a problem suffer the costs of the use of their information. The “benefits” (perhaps characterised as “social benefits”) are in the pursuit of the goals of corporate and public sector administrators with a different set of interests.

Societal barriers, contributing to the imbalance of the institutions include the absence of any

significant body of common understanding concerning the issues of identity, authentication, privacy, and the technologies of privacy and data management, and a cultural tendency to the denigration of privacy and those who seek it as asocial.

Question 12.

Comments:

Increasing the powers of the Information Commissioner or his sanctions, we think a red herring. He is already overstretched, and giving him more things to do without a radically larger budget would have no effect.

If the framework of data protection is to be bolstered, then it must be by making scope for individual actions and enforcement without the ICO having direct oversight. Even approval of prosecutions would strangle the process he is supposed to promote.

A key improvement to the DPA would be to radically reduce or abolish the exemptions for and on behalf of public authorities. Though this is of no help if legislation continually creates new ones willy nilly.

It is also worth considering whether the original limit of the Act to data not paper (and by extension restricted to automated processing of files, to digital archives and computer generated batches not individual emails) should be restored. Alternative legislation could address the mischief that the extension was intended to deal with (if it is still relevant, and not covered by the law of confidence) in an overt fashion, while relieving both the ICO and businesses of what are data protection issues only by virtue of the peculiar circumstances of the 1998 Act.

Question 13.

Comments:

Yes. There are very many. There have been two or three Acts every year since 1997 with implications for data protection, and of course more statutory instruments.

Every department of UK government is implicated in the "Transformational Government" agenda, and is contributing to the enlargement of what NO2ID calls "the database state". The broadest possible 'information sharing' is the whole purpose and actuating spirit of that programme, and the government has expressly set out that it wishes to weaken data protection, human rights law, common law confidentiality, and even *ultra vires* (DCA, Information sharing vision statement, September 2006).

There are also numerous EU and international initiatives with consequences for privacy. The most prominent is the worldwide surveillance of travel and travellers through e-Borders schemes, and Passenger Name Record data passed to governments. But there is considerable cause for concern in the Schengen protocols and

Prüm Treaty, which are internal to the EU.

Question 14.

Comments:

Statutory powers are not in short supply when government bodies wish to traffic personal information between them. What is noticeably lacking and is not adequately supported (and in some cases actually undermined) by government is the more widespread use of existing techniques of authentication using strong cryptography to permit appropriate credentials to operate without the exchange of personal information.

A proper approach would involve the repeal of some statutory powers and the lightening of some regulatory regimes – notably those imposed on banks which have a strong interest in doing things properly, but which are tied to notions of “identification” that endanger their customer’s and their own security.

Question 15.

Comments:

Yes.

The clumsy way the 1998 Act extends data protection to all documents rather than mass processing means that numerous administrative and personnel and legal problems are created for businesses who find any communication about staff members or prospective staff members potentially risky as a result.

Meanwhile there are numerous legislative and regulatory requirements on business that mandate or encourage the unnecessary, intrusive and burdensome collection of personal information on staff and customers. (e.g. Know Your Customer and fact-find protocols in financial services.)

It would be reasonable, we consider, to place a greater burden on business to enforce the rights in data of the objects whose information it is. Given modern technology, tagging information in databases with sources, expiry dates or limits on purpose or transfer is not particularly onerous and many organisations that handle data in any quantity are already doing some or all of those things for their own purposes. This is not incompatible with reducing the burden by removing unnecessary regulatory requirements to collect data, or subjecting single documents to a different regime.

Section 4: Consent and transparency

Question 16.

Comments:

As far as NO2ID's own policy is concerned we always require express consent. The only cases where we would not are in informal person-to-person correspondence where an introduction is being made.

As recent use of "implied consent" in the NHS Summary Care Record trials and the mass collection of children's biometrics in schools without explicit consent or even proper consultation has shown, the state sector's attitude towards consent is at best haphazard. At worst it is cavalier, deceptive and coercive.

Except in a very limited set of circumstances (e.g. serious criminal or national security investigations), the individual's explicit consent should always be sought prior to collection.

Consent should be properly informed so that the individual knows, before submitting any personal information, who will have access to it (including all agencies and organisations with which it will be shared), to precisely what uses it will be put and for how long it will be retained. This list is neither sufficient nor exhaustive, but the degree to which it would prove difficult for many organisations to comply is a measure of how far actual consent is currently overridden.

Question 17.

Comments:

It ought to be a great barrier, and one that is thoroughly desirable, contrary to the implicit suggestion in the question. We advocate fully informed and valid consent as fundamental to mass information sharing. Proper consent criteria are likely to reduce unnecessary and undesirable information traffic.

In practice "consent" is frequently coerced, or obtained by deception, particularly where greater scope is requested than necessary to pursue the objects' purpose.

It ought also be possible to withdraw consent. People's view of what information they are willing or wise to share can change depending on the circumstances. One-time only opt-out (or perhaps opt-out many times, opt-in only once) from a whole system of reporting and traffic as proposed by the NHS NPfIT (for example) is utterly repugnant to privacy.

Question 18.

Comments:

No.

What we suggest is that the rights of individuals (and perhaps other objects such as families and firms – or pseudonymous identities) be based on their choice and consent (or that of those authorised to act on their behalf) so that they would have a clear right to check the chain of use and transfer accorded with the extent that permission had been given. That does imply access rights both to data and to an audit trail of its use. However, transparency to third parties creates a further trail of personal information, and is undesirable.

Question 19.

Comments:

It should not be developed that way. What is needful is fewer codes of practice and more directly enforceable rights for the objects of data transfers.

Privacy impact assessments might be a flag for civil libertarians and lobbyists, but there must be some doubt about their likely effect. It is a danger that they will become an exercise in departmental form filling, comparable to the Regulatory Impact Assessment, Race Equality Impact Assessment, Environmental Impact Assessment and Declaration of Compatibility with the Human Rights Act – used to mollify the doubts of government backbenchers about passing legislation unamended, but of no utility to privacy itself.

Section 5: Technology

Question 20.

Comments:

The entire question has developed because it has become practical to manage, exchange, match and mine vast quantities of information about people and their personal lives, rapidly and without their involvement. The technological capacity and the bureaucratic imperative to record and report that it facilitates have far outpaced social change. It is like the Black Death: the population has no natural resistance and no real understanding of what is happening and why.

Question 21.

Comments:

Probably not. It is generally undesirable to have the state fixing a technical requirement. To provide for a minimum standard – rather than a particular one – and to enforce it might be something worthwhile. But our analysis of both external and internal hazards is not much affected by encryption.

In the recent HMRC Child Benefit records case the fact the lost discs were not encrypted was a contributor to the disaster, but has also been a red herring. What was far

more disturbing from our point of view was the availability of the information to one employee to burn onto discs, and the fact that it was considered acceptable and appears to have been lawful to transfer the information (which was wholly disproportionate to the purpose) from one agency to another on a simple request between officials.

Question 22.

Comments:

Such techniques are well established and essential – not just desirable. We are alarmed by the implicit instrumental attitude the question exhibits to personal information. Medical research involving direct experiment on patients requires fully informed consent. However, it is implied that a third party goal trumps privacy and individual interests when personal information rather than the body is involved.

We would point out that pseudonymisation or anonymisation may not be effective in the presence of broad data-sharing for other purposes, since cross-referencing can readily reverse the process in many cases. It is therefore just as important to protect and control anonymised or pseudonymised data as it is plain, unencoded information.

The “barriers” to either using the techniques or protecting the resulting data are merely cultural and technical, though there is a disturbing tendency to institutionalise unprotected data traffic on such a scale as to make them redundant – as in the National Programme for IT in the NHS.

Section 6: International comparisons

Question 23.

Comments:

There is nowhere in the world that we are aware of that has a wholly adequate framework. European and Old Commonwealth jurisdictions frequently take data protection more seriously than Britain does, but our doubts about data protection as pure regulation apply equally if with less force to those jurisdictions.

Question 24.

Comments:

No. The German constitutional protections appear superficially attractive, but they are neither capable of reception nor a relevant guide to practice.

Question 25.

Comments:

It is exceptionally hard to identify consequences and causes even with well-understood social phenomena.

One should distinguish between legal permissiveness and state-provided infrastructure facilitating information traffic. The United States provides a bad example of both in that 1) information traffic is typically only limited by contract, and it is common for form contracts both to demand information on pain of perjury and contractual penalty, and to include waivers of all rights of confidentiality; and 2) the social security number is widely used as an identifier for private and public-sector transactions. The latter in particular is widely suspected of providing scope for the United States' high level of identity theft. The former illustrates that having a law about it may not be sufficient: a legalistic culture can be a disadvantage in protecting personal information.

Question 26.

Comments:

We are not aware of any rigorous research comparing attitudes. That is not surprising. The concepts of information technology of databases and data management, and identity/authentication/authority/credentials are obscure to most people in most places. It is difficult to conduct research into attitudes to matters for which there is no popular language anywhere, let alone comparable terms. There may not even be ascertainable public attitudes where there is little public awareness.

What is apparent anecdotally (our direct contact with people from other countries) is that ascertainable attitudes do vary, but that people everywhere tend to be complacent about what happens whatever they happen to be. It is seen as a "natural" feature of government, which only strange foreigners, subversives or liberal intellectuals make a fuss about. We would point out that the same is true of corruption, arbitrary imprisonment of political dissidents and torture in many places. Public acquiescence is not a guide to what is morally acceptable.

Section 7: Additional questions

Question 27.

Comments:

The review should consider the maintenance of trust and its value. We consider information traffic is having a radical impact on trust in society – both trust between individuals and trust of individuals in institutions – but this appears to be largely invisible either to public or policy makers.

The foundation of social interactions throughout most of human history has been the exchange of and distribution of trust. Specifically, there are chains of trust in

which people refer one another to each other as commercial partners or social contacts. This is built on an understanding of the exchange of confidences in circumstances where the capacity to pass on personal information is limited, both in speed and quantity. Most people and social institutions still unconsciously expect the limitations of that “natural” state of data traffic when they give out personal information today. The limitations were not just technological; trustworthiness was historically enforced by mutual informal obligations – instantiated in the law of confidence. The informal sanctions are not available against organisations trafficking in massive amounts of information about many individuals.

We note the review uses the word “privacy” hardly at all. But the reasonable expectation of privacy is what is required for trust, is implicit in non-database social networks, and wholly lost in broad data-sharing.

Mutual trust is displaced when one can or (in the case of, for example, government mandated ID checks) must rely on third party information of incalculable provenance.

Question 28.

Comments:

We believe that a clearer conceptual and legal structure is sorely needed in order to help people (including policy-makers) cope with the possibilities of the information society and roll back those features that make the information society the surveillance society. This means, contrary to the naïve and reckless government policy of ‘removing barriers to information sharing’, extending and strengthening and clarifying confidentiality by new individually enforceable rights, limiting the exchange of unnecessary data, building a substantive law of privacy, and curbing the cult of identification.

1. New Rights

In particular we propose that the objects of personal information should have rights that are of a proprietary nature over what is casually (and currently meaninglessly) described as “their” information. This means an end to unlimited traffic – whether by coerced consent or otherwise.

What is required to restore and reconceptualise the chain of trust that our social institutions expect is something like “informational privity” – where the source and extent of each user’s entitlement to use information is known. Just as a lessor of property may only sublet where permitted, and in any case cannot grant any greater rights than he has himself, information users should not be permitted to extend their own grant – the uses, and period of use allowed would be limited by the grant from the original provider of the information. Given the same technological management that permits “sharing”, maintaining expiry dates and functional limits need not be especially onerous, and examples already exist of time- and function-limited information use: list rental, for example.

Given the possibility of clear limits on rights to use information, and an obligation to be aware of the source then limits can be imposed in an intelligible fashion. A default period of use can be imposed by law to stop indefinite rights being signed away under coercion. It also becomes possible for the object – now the owner – of the information to revoke a licence for misuse. A happy consequence is that some of the hazards of data traffic for both users and objects will also be constrained. Revocation gets corrupt information out of the system.

Problems arise in enforcement. Intellectual property is the closest analogy, but the injury done to an owner of intellectual property rights by an infringement is with very few exceptions a solely commercial loss, often quantifiable in damages or available as an account of profits. The damage done by improper information traffic is likely to be personal. And if it arises from an External Hazard (as defined above) it may not be traceable, though tighter control of traffic is likely to diminish the opportunities for criminal misuse. There is an analogy with defamation, which currently has a system of disguised punitive damages, but one that is so arbitrary that it is in disrepute itself. Civil enforcement clearly ought to be available, but that may not be sufficient, given that it strongly favours the rich repeat litigant over the poor one-off participant (though perhaps insurance has some place), and we are looking for ways of protecting individuals (largely) against the depredations of large institutions.

Perhaps a criminal jurisdiction for the infringement of information rights would be an inevitable consequence of such a structure, if it were to be effective. Note this is not the same as increasing penalties within the existing framework. Prosecutions driven by individual cases are systemically different to regulatory oversight. Nor is it equivalent to prosecution under statutory protection of specific information from disclosure (as in the Identity Cards Act 2006 or the new Counter-Terrorism Bill) an infringement of informational privacy would not just be committed by disclosure but by holding longer than permitted or use in violation of the conditions on which it was held.

2. The cult of “identity”

Much data collection, sharing, and matching is motivated by the perception that “we need to know who people are”. In general “we” don’t. Social transactions of all kinds, just like financial transactions, need trustworthy authentication of the subject matter of the transaction – Will I get the money? Is this person 18? Is he British? – not irrelevant personal details about the parties involved. Ideally NO2ID would love people to stop asking for “ID” when credentials are what they actually require. But we are aware that that deep cultural understanding of the difference is a long way off.

However it would help if government and large organisations that ought to know better would themselves make the distinction and stop undermining both the conceptual structure and the technologies – modern cryptographic techniques in particular – that make it perfectly possible to have and use very strong credentials without any transfer of, or reference to, significant personal information. Smart cards and biometrics have great potential roles in protecting individual and

collective security, but large data users – especially government – have, either through ignorance or a callous pursuit of their own agenda at everyone else’s cost, constantly undermined the possibilities by resisting encryption and insisting on being the man-in-the middle of (much less robust) authentication processes through large databases.

We would urge the Review to consider the possibility that much data-sharing is entirely unnecessary, and that closed authentication processes are in many cases preferable to identification through reference to personal information.