Liberty’s Response to the Cabinet Office Performance and Innovation Unit consultation paper “Privacy and data-sharing: the way forward for public services”.

July 2002
Liberty (The National Council for Civil Liberties) is one of the UK’s leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research. It is the largest organisation of its kind in Europe and is democratically run.
Introduction

1. The Report “Privacy and data-sharing: the way forward for public services” published by the government’s policy making think-tank, the Performance and Innovation Unit (PIU) proposes wide-spread sharing of data between central government and local government departments, government agencies and other public bodies.

2. Data-sharing is defined in the Report as the disclosure of personal information within the public sector, whether the information is contained in electronic or paper files. The Report treats information shared on a single item basis in the same way as information shared on a block basis. The doctrine of the indivisibility of the Crown is not applied in the data-sharing context because government departments, agencies and other public bodies are regarded as separate entities for the purposes of data-sharing. In fact, there can be data-sharing within one public body because if a public body obtains information for one purpose but uses that data for another purpose then it is sharing data and must comply with the legal framework in place (see annex A, paragraph A.03-05)

3. The Report argues that the existing statutory or other powers to share data are piece-meal and that more efficient and effective public services can be provided if information about the public were to be shared between public bodies. What becomes clear when reading the Report is the extent to which data-sharing powers have been increasing over the last few years. An enormous amount of data-sharing already takes place under express or implied statutory powers or administrative powers. For example, section 127 of the Finance Act 1972 already permits data-sharing between H M Customs and Excise and the Inland Revenue “for the purpose of assisting them in the performance of their duties.” Sections 20 and 21 of the Asylum and Immigration Act 1999 permit the supply of information to the Secretary of State “for immigration purposes” and by him to others for police, customs and other purposes. Part 3 of the Anti Terror Crime and Security Act 2001 allows personal and private information to be obtained by the police and others without any controls checks or safeguards. It allows the police to trawl through the files held by other government departments. Clauses 112-117 of the Nationality, Immigration and Asylum Bill create powers of disclosure covering local authorities, the Inland Revenue, the police and medical inspectors. At present, data-sharing takes place within the confines of particular statutory or other powers, for particular purposes and between particular government agencies.
4. The purpose of the government’s proposals is to allow data-sharing to take place more generally within government. The Report highlights three main aims of increased data-sharing which are: (1) better, more “joined-up” and personalised public services, (2) more effective and better targeted policy-making and (3) more efficient public services.

5. The first aim focuses on the availability of one-stop shops for service provision and the advantages to be gained by the public if public services are provided from one physical or online outlet. This requires a central database of information so that the provision of services can be administered by one body as opposed to a number of separate bodies. Different government departments can team together to provide their services as a single-team focused on the needs of the service user. For example, Care Zone is a scheme which has been produced to protect children in public care by providing a central database of information accessible by health, social and education services with the aim of caring for all the needs of the child. The database is said to be secure so as to prevent access by paedophiles or other unauthorised users. A distinction can be made between information which is put into a database which is shared overall by a hybrid group of people for a particular purpose, and the non-specific generalised sharing of information. The Care Zone example falls into the first category and the difficulty in that case is to identify who is the true owner of the database. In the more general case of simply “pumping” data from one Department to another, the risks that are of concern relate to (a) correct person matching and (b) ongoing updates. The “person matching” risk is that a record pertaining to “John Smith” coming from Department (A) will be linked in error to the wrong “John Smith” in Department (B). Without the ability to know where the original information has been syndicated by Department (A), or the right to be told that information has been merged by Department (B), both individuals are at risk.

6. The second aim is concerned with using available data to identify those in need of services and concentrating public services on those in need. In particular, the government aims to make more use of anonymous statistical information.

7. The third aim includes reducing management time incurred in collecting and using information because the information could be gathered by one body and held centrally as opposed to various government agencies all collecting the same information for their own purposes. A
further aim is to tackle and reduce crime by sharing data between agencies, in particular, fraud such as social security fraud or fraud in the NHS.

8. Information provided by individuals to government agencies or held by particular government agencies about individuals is usually of a personal and private nature. For example, information about income, which is provided to the Inland Revenue or health records held by a GP or hospitals. Furthermore, the information is provided for a particular purpose and, in some circumstances, there is no choice but to provide the information. For example it can be a criminal offence not to provide information to the Inland Revenue. Furthermore it is necessary to provide information in order to obtain government services, such as social security benefits or to obtain documentation such as a passport or driving licence so as to be able to enjoy freedom of travel.

9. The paper recommends a number of particular data-sharing proposals which include:

   a) sharing data between agencies, include local authorities, social services and the police to identify children at risk of social exclusion so that support services can be provided;
   b) data sharing between the Department of Work and Pensions and the Legal Services Commission on a case by case basis to combat fraud and speed up information gathering,
   c) enabling NHS, social services and social care agencies to share data with Sure Start partnerships which work to ensure the families with children receive all the right services;
   d) disclosing anonymous health information to evaluate drug treatment programmes;
   e) allowing the UK Passport Service and Criminal Records Bureau access to other private and public databases to allow corroboration of identity and prevent identity fraud;
   f) allowing regulated debt enforcement agents access to information about names and addresses of debtors so that debts can be enforced.

10. The paper proposed two legislative methods for introducing the changes. The first is to allow data-sharing where an individual consents to the sharing of data. The second is to allow data-sharing without consent where operational necessities militate against the obtaining of consent e.g. in relation to criminal investigations. The changes are to be introduced by secondary legislation backed up by Codes of Practice and other “safeguards”.
11. Legislation as well as the common law provides protection to those providing or required to provide personal data for use by public authorities. The Data Protection Act 1998 provides safeguards for the processing of personal data. Article 8 of the Human Rights Act 1998 protects the right to privacy, which will usually be in play in data-sharing situations. The common law right of confidentiality also provides protection to the individual providing personal data in circumstances of confidence, for example, information provided by a patient to a doctor is confidential (W v Edgell [1990] 1 Ch 359).

12. The proposals contained in the PIU paper raise a number of legal, social philosophy and practical problems, which are discussed below.

Matters that we agree with

13. This is a thoughtful Report, much of which we welcome for a number of reasons:

a) It highlights the extent to which data-sharing is already taking place between government, local government and related bodies.

b) It contains research highlighting the concern which many people feel about disclosure of personal information about themselves (this point is developed in paras. 27-30 below).

c) It highlights the inaccuracy of much data and the impossibility of providing 100% security for data held on computers.

d) It highlights the legal uncertainty created by the main law protecting personal data, the Data Protection Act 1998, many of the provisions of which are notoriously obscure and difficult to interpret. In particular the Report makes the valid point that different organisations have different views on the interpretation of the Act.

e) It calls for a consistent approach by all public authorities to proposals which might involve data-sharing and makes a number of practical suggestions for ensuring such consistency.

f) It calls for the appointment of Chief Knowledge Officers, board-level officials with clear responsibility for ensuring that data protection and human rights issues are taken into account in the planning and implementation of schemes which involve processing personal information. We differ from the Report in holding the view that such appointments should be mandatory, rather than merely recommended where resources permit. After all, if the organisation is small, the job does not have to be a full-time one, but it is essential that there is in each organisation a high-level official with clear responsibility for these matters. Indeed anything which communicates the idea that such posts are optional implies that the security for personal information is in some way “optional” too.
g) It calls for the provision of more information about the rights of citizens to have their data protected.

h) It calls for greater openness and consultation in the policy-making process where the privacy of personal data is at risk.

14. At the same time, however, the Report signals an intention that details of our private lives should be shared to an even greater extent than at present and in so doing raises a number of matters of serious concern. There are recent developments that demonstrate how this may develop. The white paper on civil registration proposes to open up the Births Marriages and Deaths register to Internet access for widespread use. Meanwhile the Criminal Records Bureau services look as though they are to be turned into a money-making venture, where there will be an active policy to “sell” criminal records checks to an ever-wider range of organisations.

The general approach of the Report

15. One of the key recommendations of the Report is that there should be a model Analytical Framework “to assist public bodies in considering the important questions surrounding better use of information in order to improve delivery of their objectives.”¹ The introduction of such a Framework is intended to secure consistency of decision-making. As indicated above, we support the principle of consistency of decision-making in general and the introduction of such a Framework in particular.

16. However we have considerable concerns about the adequacy of the Framework as a means of protecting personal data. The Analytical Framework provides a set of criteria against which to judge any proposed scheme involving data-sharing within the public service, or between the public service and the private sector. The criteria are all thrown into the balance of a cost-benefit analysis, with the judges of where the balance lies being the officials in charge of the proposed scheme. This gives rise to two difficulties:

   a) The first is that, as indicated below, cost-benefit analysis is too simplistic an approach to decisions on data-sharing.

   b) The second is that the judges of disclosure should not be the very officials who have an interest in promoting or operating the scheme that requires disclosure: it would only be

¹Para. A.04.
human nature for such officials to give a consistently low importance to the protection of privacy where it conflicts with the success of their project. This is exemplified by para. C30 of the Report, which shows that the public at large generally attaches far more importance – “emotional charge” is the phrase used – to the risks of data-sharing than to the benefits. Civil servants are unlikely to share that view.

17. Throughout the Report a number of justifications for data-sharing are put forward. The various justifications tend to be lumped together in the Report in order to illustrate the benefits of data-sharing. This approach leads to a dangerous under-analysis of the justification for sharing data, creating an impression that data-sharing is generally a good thing provided only that it is properly controlled. There are huge potential risks if this impression governs policy: it must never become the norm to share and combine information. We firmly believe that the requirements for justified data-sharing will vary enormously from one class of case to another.

18. For example, one of the perceived benefits of data-sharing is the delivery of better, “joined-up” services and another is more efficient action against crime. Data-sharing in the former case can only be justified if the beneficiary of the service consents to it, whereas in the latter situation consent will often be impractical. A Framework which merely weighs the pros and cons of a particular scheme in the balance, rather than imposing absolute, mandatory requirements for data-sharing in certain situations, fails to draw an adequate distinction between the different purposes of data-sharing.

19. Apart possibly from a passing reference in the flow-chart illustrating the Framework to “DPA compliance” and “Statutory changes”, the effect of which is not entirely clear, the Framework contains no absolute barriers to data-sharing. The decision whether or not to share data is made in each case by the relevant officials, simply weighing the advantages against the disadvantages. There is no reference whatever in the Framework to the consent of the data subject.

20. In our view this approach is misconceived in principle. In particular:
   a) Lack of consent from the data subject ought to be an absolute barrier to data-sharing in a number of situations.
   b) In some situations the decision whether data should be shared should be a matter for a person independent of the relevant department or authority, usually a judge.
c) In other situations where lack of consent is not an absolute barrier, it ought to be given very great weight.

21. The principal classes of justification considered in the Report are:
   a) To enable the provision of “joined-up” services - i.e. giving a better service to those to whom public bodies provide a service.
   b) To improve the targeting of services.
   c) To improve policy-making.
   d) To improve the enforcement of civil judgment debts.
   e) To improve revenue-collection and to reduce fraud.
   f) To combat crime.

22. In our view the particular benefit to be obtained from data-sharing in any particular case will often provide the key to whether it should be shared at all. Accordingly, if the justification for a particular project involving data-sharing is the provision of “joined-up” services, then data-sharing should only be possible if those who are intended to benefit from the project give their express consent. A good example is the proposal to enable people to report a change of address just once, with the change of address then being notified automatically to all other relevant public authorities. Those who wish to have the benefit of this scheme will no doubt be prepared to consent to the data-sharing necessary to ensure its implementation. Those whose concern about the security of their data or the use to which it may be put is such that they do not wish the data to be shared should be entitled to absolute respect for their views. In her Guidance on the Use and Disclosure of Health Data, published in May 2002, the Information Commissioner noted “statements by Department of Health Ministers that in the foreseeable future all processing of patient records should be on the basis of informed consent”\(^2\). This is an approach which we wholeheartedly endorse, and one which needs to be built in to any framework for the disclosure of such information.

23. At the other end of the spectrum is data which it is desired to share for the purpose of preventing or investigating crime. The obtaining of consent to data-sharing cannot be the litmus test in this context, as it will often be unrealistic to obtain it. Generally our view is:

\(^2\) Foreword.
a) If the information in question was given in confidence then, save where the disclosure of data is specifically authorised by legislation, or where consent has been obtained, sharing ought not to take place without a court order. This is because, even if the “public interest” defence to a claim for breach of confidence may be available, the decision whether the public interest justifies disclosure is a matter for the courts to decide.

b) We recognise however that there is already a large body of statutory provision regulating data-sharing for these purposes - e.g. ss. 122 and 123 Social Security Administration Act 1992 or ss. 17 and 19 of the Anti-Terrorism etc. Act 2001. Even here, however, the legislation in question usually creates a power rather than an obligation to disclose, and in the case of the 2001 Act this power is subject to a test of proportionality - see s.17 (5) and 19 (3). In such cases we believe that a modified form of the Report’s Analytical Framework would be of use in ensuring consistency of decision-making and a proper consideration of the weight to be given to the protection of private data.

24. In between these two extremes are the other situations listed in paragraph 6 above. We consider them in turn:

a) **Improved targeting of services:** The illustrations given in Chapter 11 of the Report give helpful indications of what is meant by this concept. They include sharing of information between NHS, education, social care agencies and Sure Start partnerships to tailor services to family needs, and sharing information to identify children who are missing school.

   We start by noting a general concern. Whilst the Government’s programmes to combat social exclusion are clearly laudable, there is a concern that in trying to achieve the aims of these programmes the rights of families who are, or who are at risk of being, excluded should not be compromised. The notion that the poor are a group who can be snooped upon “for their own good” is not acceptable.

   In relation to programmes such as Sure Start, which is primarily concerned with offering services to families which they are free to accept or reject of their own volition, consent to data-sharing should be a requirement unless the sharing is of an established routine nature such as a hospital notifying social services of a birth.

---

3See Annex A to the Report at para. A.61 (though note that the reference there to Church of Scientology v Kaufman is a
In relation to programmes to identify those who are missing school, clearly the obtaining of consent is not practicable, and non-consensual data-sharing is justified in principle, provided that adequate safeguards are in place and the sharing is the minimum necessary to achieve the objective.

In connection with targeting, there is an important distinction to be drawn between anonymous data and that which relates to identifiable individuals. We generally support the use of genuinely anonymised data to enable services to be better targeted – e.g. on a micro-geographical basis – provided that the anonymity is secure. However, that is entirely different to a system of targeting which enables a social worker to arrive on your doorstep with a printout of personal information saying “you are in need”.

b) Improved policy-making: We accept that good quality data are essential to good policy-making and identifying appropriate target groups for the application of policy. As Chapter 11 recognises, this aim can be achieved by anonymising data. We have no difficulty with the use of anonymised data in principle. The concerns are over the adequacy of the arrangements for the security of the personal data upon which the anonymised data are extracted. We endorse the recommendations in the Report, both technical and organisational, which are intended to achieve this aim.

c) Improved enforcement of civil judgments: Chapter 11 of the Report gives two examples of proposals in England and Wales for the improvement of debt collection through the courts. One allows a court officer to have access to data from designated third parties, including Government departments, in order to identify the whereabouts of the debtor. The second allows the court to make a Data Disclosure Order where there has been wilful non-compliance with earlier orders.

As to the first proposal, clearly the consent of the data-subject cannot be the litmus test here, and we accept that it is appropriate for disclosure to take place in the absence of consent. Any application to trace a debtor should have to go to at least a District Judge. On that basis, provided that the only data which can be required by the court enforcement agent is

mistake: the case is called *Hubbard v Vosper*).
that concerning the whereabouts of the debtor, and subject to the usual safeguards, we agree with this proposal.

As to the Data Disclosure Order, this is the subject of a separate Green Paper upon which it would be inappropriate to comment here. In principle, however, the scheme as outlined in the Report would appear to be an admirable example of respect for the privacy of data, requiring a court order which is only obtainable in circumstances where it is proportionate to do so, i.e. where there has been wilful default.

d) **Improved revenue collection**: This is really in the same category as crime, which we have dealt with above.

**Public attitudes to data-sharing**

25. The key focus of the Report is the benefits to public services and the public which will flow from data-sharing, in particular, joined up and more personalised public services and greater efficiency. What is interesting is that the Report’s perceived benefits of data-sharing do not seem to be recognised by the public. It is clear from the Report that these changes are not being driven by public demand as much as by the official love of collecting and collating information.

26. Annex C of the Report contains a brief survey of studies of public attitudes to data-sharing and privacy that have been undertaken by the government, as well as other organisations. The results that emerge from these various surveys show that the public has become increasingly concerned about privacy in recent times. The Report compares the growing interest in privacy with that in food safety over the last decade or so (page 9). The result is that there is considerable public concern about data-sharing and the extent to which it will impact on privacy.
27. The government’s focus group study⁴ revealed that few people felt very positively about the benefits of data-sharing, except some who regarded fraud control and crime detection of real importance. As stated in the Report:

“Even exercises and prompts to elicit benefit perception sometimes tended to elicit risk perception instead. People nearly always found themselves unable to concentrate on benefits without also calling for safeguards against risks.” (C.27)

28. The benefit of eliminating or reducing multiple requests for information failed to attract much excitement or interest. As regards benefits for public services, few people felt that they would benefit personally. Interestingly, those who attached greatest weight to the benefits to public services were those who used public services least frequently.

29. By contrast, the public did identify a large number of risks of data-sharing including errors in data-handling, infection with inaccurate data, malicious provision of data from anonymous sources, unjust inference, unauthorised access to or disclosure of personal information and disclosure of “soft data” in the form of professional opinions etc. Furthermore, significantly more categories of risk were elicited without prompting in almost every group questioned, than was the case when asked about benefits of data-sharing. The “emotional charge” associated with the risk was also much greater than the benefits.

30. In our view, the public attitudes revealed by the government’s focus group study as well as other surveys raise important challenges to the foundations upon which the Report is based. In particular, the proposals aimed at convenience, such as the ability to notify a change of address only once, do not appear to be of particular interest to the public.

31. We consider that the current public feeling about data-sharing is an important backdrop to the government’s proposals, particularly given the proposals about sharing without consent. Present public attitudes suggest that, in many cases, consent may not be forthcoming. In that climate, proposals to share without consent will need strong public interest justification with full and proper consideration of whether a legitimate aim under article 8(2) of the European

---

⁴ Strategies for Reassurance: Public concerns about privacy and data-sharing in government. Findings from focus
Convention on Human Rights is being pursued and whether the aim could be achieved by a method which is less intrusive of privacy.

32. Also of interest is the public’s apparent lack of knowledge about how data is currently shared in government and the public sector as well as the detail of their rights under the Data Protection Act (see C.06-C.08). As referred to above, data-sharing is already going on in government. It is lamentable that the public has not been properly informed to date about the use that is made of personal data. We fully support the proposals in the Report for informing the public fully about data-sharing. This will, in any event, be necessary so as to obtain their consent in circumstances where consent is required. It should also be noted that the Information Commissioners Office requires sufficient resources to enforce DPA protection. We are concerned that the office is underfunded and is unable to carry out its regulatory role properly.

The inherent risks of data-sharing

33. The Report highlights a number of initiatives proposed to ensure security of data such as Public Key Infrastructures and Digital Signatures. The target is to provide 100% of government services on line by 2005 and the commitment to match at least best practice in the private sector for information security is welcomed, but raises the question whether that is sufficient. Those who give their personal data to the private sector have a choice in the matter. Much, possibly most, of the information given to the public sector is given under compulsion. There are numerous threats to the security of data, ranging from hacking (against which experience has shown government systems not be immune) to unauthorised use by staff. However, there is also considerable potential for unwitting misuse such as caused by the transfer from paper to electronic recording systems. It is essential that the public is informed and recognises the security risks that emerge from data-sharing and take these into account when considering whether to disclose personal information to officials or to give consent to data-sharing, even where anonymity is promised.

34. One important area of concern is that of data accuracy. The Report accepts that it is essential that public services achieve improvements in the accuracy and reliability of personal
information (7.01). Data quality has been measured rarely and inconsistently. The evidence suggests that data quality is highly variable and that the criteria and standards to measure data vary too. The causes very from data becoming out of date (e.g. passport information) through to keying errors by staff, often operating under pressure as a result of a productivity drive within their department. The electoral register has an estimated accuracy only of just over 80% and the Police National Computer has an error rate varying between 15% and 66%! The accuracy of data is a major concern in data-sharing because any inaccuracies in data may be disseminated to a number of public bodies who draw wrong conclusions on the basis of inaccurate or incorrect data. For example, inaccurate Benefit Agency information could be provided to the Legal Services Commission, which wrongly declines public funding for a case.

35. Furthermore, as the Report fairly recognises, the wider the access to data the greater the risk of deterioration in the quality of such data by inexperienced users or those unfamiliar with the particular system. However, the problems go further than that. Even a properly operated system can be thrown into confusion by data sharing. If information about “John Smith” is made available by Department A to Department B, there is an obvious risk of an incorrect match by Department B with another John Smith on its database. Unless the data subject has a clear and easily unable right to be told which other departments have access to the information he gave to Department A, and to be told of the merger by Department B, both he and his namesakes are at risk. The problem is exacerbated if one department then updates its information on him, without the other doing the same. This creates a potential for uncertainty in terms of ownership of the information and the responsibility for correcting errors. If Department B discovers that the data from Department A are inaccurate, whose responsibility is it to correct the error, and how is this accountability audited in the event of a later dispute?

36. We welcome the commitments in the Report to the improvement of data accuracy and the introduction of agreed standards for recording data (including labelling techniques i.e. metadata), measurement of data accuracy and stronger incentives to improve data quality. However, our concerns relate more to the need to have regular checks of data to ensure accuracy. Although the Report encourages the use of external and internal audits to improve data accuracy and asks the Lord Chancellor to develop a data quality audit methodology based on the Information Commissioner’s Office data protection audit manual, it does not propose the imposition of an obligation to audit on public bodies, whether regularly or at all. In fact, the
Report states that there are “substantial numbers of databases in the public sector, so regular or annual audits would impose excessive costs.” (7.19) The Report only encourages public services “to consider” using the audit methodology as a diagnostic tool to assess the quality of data (Recommendation 12).

37. In our view, public bodies should not consider data-sharing plans unless the proposed data satisfies agreed quality standards of accuracy and reliability. The nature of personal data is that it changes frequently, for example, when someone’s financial circumstances change or someone moves house. Unless there is a requirement of regular data audit, the accuracy and reliability of data cannot be guaranteed. The dangers of sharing inaccurate data and the drawing of inaccurate assumptions are clear. Further, there is a potential breach of the fourth principle of the Data Protection Act, if data is inaccurate. Also, the surveys of public opinion reveal that the inaccuracy of data was a specific concern (see Annex C.29). It is not acceptable for the government to take the view that it is too expensive to have regular audits of public databases. This cost is simply a downside that has to be weighed in the balance against the potential benefits of data sharing.

38. More profoundly, there is a real danger of both Government which prides itself on modernity and the general public being lulled into a false sense of security by technology. The fact that more and more sophisticated security systems are becoming available should not blind us to the fact that none of them is 100% effective, and that every advance in computer security is matched, indeed often prompted, by an advance in the sophistication of hackers. Indeed, the more comprehensive the data, the more attractive it becomes as a target, because of the increased value of the aggregated information. The more limited and mundane the database, the less attractive it is, and the less the danger that arises from unauthorised usage. The very insecurity of personal data, both generally and in particular systems, should act as an important brake on the drive to make it available to more and more officials and contractors. As a recent editorial in Computer Law and Security Report put it, “There are strong fears that safeguarding mechanisms are not yet in place to a satisfactory degree to permit us to sleep peacefully in the knowledge that these powers are not being used.”

“Building Public Trust and Engagement”

39. Chapter 6 of the Report, which bears the above title, proposes a “Public Services Trust Charter” and service-specific Privacy Statements. These contain statements of principle for the public services in general and for specific public services. Whilst we welcome the provision of such charters or statements in general, it is important to see that they do not use language which actually misleads the public.

40. In our view the draft Charter at Box 6.2 does precisely that. It includes, for example, the following statements:

“Your personal information is only seen by staff who need it to do their jobs.”

“Decisions affecting you are only made on the basis of reliable and up to date information.”

Each of these statements is thoroughly misleading. No system is 100% perfect, and the Report itself contains clear evidence that government, local government and similar bodies are no exception. As indicated above, the information shared is often out of date or unreliable and there are numerous documented examples of unauthorised use of data. Given that both the Charter and the Privacy Statements will be taken into account by those who disclose information to officials and by those who consent to data-sharing, it is essential that such statements are not misleading and contain clear warnings of the risks involved. The public will neither “trust” nor “engage” if it is induced to do so by misrepresentation.

41. For similar reasons any disclosure of data and any consent to data-sharing should be on the basis of a clear explanation not only of the purpose for which the data will be used, but also on the basis of a clear warning of the risks involved. Failing this, any consent to the use of such data will not be “informed consent”, and will contravene the fair processing requirement of the First Data Protection Principle.

The Legal Framework

42. The Report analyses the legal framework within which data-sharing takes place and makes a number of recommendations.

43. The first of these highlights the difficulty created by the requirement of the First Data Protection Principle that all data should be processed “lawfully”. The effect of this requirement is that information obtained by a statutory body for one statutory purpose cannot, in the absence of a clear statutory power, be used by that body for another purpose even where

44. The Report suggests that a single statutory “gateway” be created to enable the sharing of data by public authorities where the data-subject consents, provided that the individual is able to change their mind at any time. In theory, provided that the consent to such sharing is informed and provided that all the other requirements of the Data Protection Act are complied with, we would agree with this proposal. However, we would re-iterate concerns expressed earlier relating to sufficient funding of the Information Commissioners Office to ensure Data Protection Act protections be properly enforced.

45. The other proposal for legislative change is that further “gateways” be provided by secondary legislation. We strongly disagree with this suggestion. Although one of the justifications for this proposal is the difficulty of finding Parliamentary time, we do not believe that this creates an insuperable barrier or that it is sufficient justification for avoiding a full debate every time that further powers are conferred on officials to pry into or disclose to others information of a personal nature. The statute book is full of legislation in recent years conferring or extending such powers, often on a block basis – see, e.g., the list of statutes in Box 10.2 on page 112 of the Report (which does not give the full picture even for the period it covers) and s.17 of the Anti-terrorism Crime and Security Act 2001.

46. It is suggested that Codes of Practice and other tangible safeguards could be included in any secondary legislation creating further gateways. We agree with the inclusion of such safeguards but there is no reason why they should not be included in primary legislation.

47. Overall we agree with the explanation of the law related to data-sharing contained in Annex A to the Report. However, we are of the view that insufficient explanation and emphasis has been given to one aspect of the European Convention on Human Rights. This omission is critical because if policy is to be developed on the basis of this Report, it is essential that those making policy fully understand the rights which citizens have in maintaining the privacy of personal information about themselves.

48. No interference with the Article 8(1) right to privacy can be justified except by reference to one of the legitimate aims set out in Article 8(2). However, the Report contains no explanation
of these legitimate aims, and by that omission creates the impression that the decision whether
to breach privacy is one taken by merely balancing the individual’s interest in privacy against
the perceived greater good of society. It is essential that policy-makers understand that there
will be an automatic breach of Convention rights if private data are disclosed for any purpose
other than the six “legitimate aims”.

49. We also note two important concerns about the shortcomings of the Data Protection Act as a
means of regulating the enormous increase in data-sharing contemplated by the Report. The
first is the price of subject access. Paragraph 6.27 of the Report makes the point that the £10
fee for the exercise of the right of access under s.7 has been considerably eroded by inflation, a
paragraph which the Treasury is likely to latch on to. To be fair to the authors of the Report
they do not recommend an automatic inflation-related increase, but point to the need to
maintain a fair balance between the need to have access to information and the burden placed
on organisations by dealing with subject access requests. One of the essential checks and
balances if the thrust of this Report is to be implemented is that individuals should be able to
verify the accuracy of information held by the Government about them. In order to be really
effective, the s.7 rights should be very much easier to exercise than they are now. Indeed,
given that the information under consideration is generally in electronic form, there is an
obvious subject access case for electronic access to information about oneself, which could be
made available without charge. The paradox of that proposal is that unless security is
drastically improved, there is a real risk of any member of the public being able to look up
information about another. Until that problem is overcome, if it ever can be, the case for on-
line access to information about oneself is not made out, but this only serves to highlight the
weakness of the case for others to have on-line access to information about us.

50. Our second concern under the DPA relates to compensation in the event of unauthorised
disclosure or use of sensitive personal data. S.13 gives individuals a right to compensation for
damage caused by a data controller acting in breach of the Act, and a right to compensation for
distress if the individual has also suffered damage or if the contravention relates to the
processing of data for literary, journalistic or artistic purposes. Accordingly, if you suffer
distress, but no actual damage, because a Council official leaks sensitive information about you
on your estate, you have no right to compensation. Even where compensation is payable, it is
likely to be in fairly limited sums – see, e.g., Naomi Campbell v MGN [2002] EWHC 499
(QB), where £2,500 was awarded under the Act. Furthermore, in the example quoted there
may be no remedy at all, as it is a defence for the data controller to prove that he took all such care as was reasonably required in the circumstances. We have set out above good reasons for doubting the security of the proposed data sharing. If the proposals are to go ahead in the interest of the “greater good”, the very least that is required is that there should be substantial compensation for the innocent victims of this extension, and that the right to such compensation should not be blocked by a claim to have “done the best we could”.

**Conclusion**

51. This is not the place to criticise in detail the enormous extension in the last few years of the powers of officials at all levels to require disclosure of, and to disclose to others, highly personal information about individuals. Only the latest batch of extensions has anything to do with September 11th, and Liberty’s concern over all these extensions is on record elsewhere. The Cabinet Office Report proposes to move this whole process into a different gear, largely in the name of efficiency. Our concern is that the proposed extension of this process is driven by a rose-tinted view of the security of the systems by which this sharing will take place and by a significant undervaluation of the importance to individuals of their privacy. Information about us is our property – ours to keep private or to share as we wish. Any proposal to give away that property which does not make the issue of consent absolutely central to decision-making devalues our right to privacy and is seriously flawed.

52. Article 8 of the Human Rights Act 1998 protects the right to respect for privacy and family life. However, we still have no specific privacy law. Recent rulings (notably the Zeta Jones privacy case, December 2000) demonstrate that the right to privacy exists - but there is a danger that it is only enforceable if you have the wealth to pursue it through the civil courts. If there is to be wide spread sharing of data between public authorities there it is important that a privacy act is introduced to act as a counterbalance against increased powers of intrusion.

Jeremy Morgan

Nicola Greaney

39 Essex Street, WC2