Conference paper

Entitlement cards:
benefits, privacy and data protection risks, costs and wider social implications

paper for the Information Commissioner

by

Perri 6

Dr Perri 6

Dr Perri 6 is Director of the Policy Programme at the Institute for Applied Health and Social Policy at King's College London: this paper was written in a personal capacity.

Address for correspondence:
Institute for Applied Health and Social Policy
5th Floor,
Waterloo Bridge Wing
Franklin-Wilkins Building
150 Stamford Street
London
SE1 8NN
Tel (dir): 020 8279 9704
E-mail: perri@stepney-green.demon.co.uk

Contents

Part I: Introduction

This paper has been commissioned by the Office of the Information Commissioner. The purpose of the paper is to provide advice to the Commissioner which he and his staff may take into account when preparing their response to the Home Secretary's proposals for an entitlement card scheme. Specifically, I have been asked to

- present an analysis of the benefits, costs and risks to individuals, including any privacy and/or data protection risks, and of wider social issues; and to
- consider how far the presentation of the scheme as a universal entitlement scheme might affect trends in public perception over time.

In particular, under the first heading, I have been asked to give consideration to risks of what has come to be known as "function creep" and notification.

Structure of the paper

The paper begins with a summary outline of the most important provisions in the scheme for an entitlement card that the government has presented in its proposals, *Entitlement cards and identity fraud: a consultation paper* (Secretary of State for the Home Department, 2002). The main benefits that the government believes will be available as a result of implementing the scheme are briefly discussed.

It is no part of the general provisions of British or European data protection law that it would rule out in principle any kind of identity card or entitlement card scheme. The fact that so many European Union countries have operated identity card schemes successfully, and without challenge for many years, suggests that it is rather unlikely that all such schemes would in principle or in any straightforward or automatic way fall foul of the European data protection law. Indeed, many of those countries have national data protection laws that are in some respects stricter than does the United Kingdom. However, it does not follow that *any* identity or entitlement card scheme would be compatible with British and European data protection law.

Therefore, the second part of the paper considers the issues and question of compatibility with data protection raised by the particular proposals in the government's proposed scheme. This section considers whether, how and how far the proposed scheme might meet each of the main conditions and principles in the Data Protection Act 1998. It argues that there remain important areas in which, despite the assurances in the consultation paper, the Home Office proposals do not meet some central standards of data protection and privacy. This section concludes by setting out what would need to be done to produce a scheme that would meet these standards.

The third section of the paper is concerned with the costs, for the economic assessment of whether the benefits are of sufficient magnitude to merit the costs is an important part of the overall assessment. Issues of implementation cost, of project management and of the card reader infrastructure are given particular emphasis. However, the argument links to that of the previous section, for it is important to examine the costs for a scheme that would comply with the principles of privacy and data protection law, both in letter and spirit.

Next, there follows a short discussion of some issues in relation to public perception of the card and the underlying data system.

The fifth section considers a range of wider social implications of the proposed scheme. The section begins with an analysis of the argument for compulsion, grounding it in the normative literature on citizens' obligations. The most promising argument for compulsion is reconstructed, and then critically appraised. It is argued that in principle, some form of compulsion could be justified, but that the present proposed scheme does not yet meet the standards that would be required for an argument for compulsion to go through. After considering some issues of public administration, the role of professionals and public trust in them, questions of stigma and social exclusion, distributional issues

of inequality, and the risks of the culture of suspicion, the paper concludes with an argument about the importance of retaining a role for anonymity in many settings, and against allowing a scheme of this kind to be used in ways that effectively require identity to be disclosed in almost any transaction between individuals and organisations.

The concluding discussion deals with a number of general questions about the relative merits of manual and digital systems, and the ends with a short discussion of the appropriate stance that liberal democratic societies should take toward population registers.

It is in the nature of a public policy analytic paper of this kind that it must move very quickly between very different styles of argument. In the third section, much of the discussion is legal or jurisprudential in tenor, but with frequent references to matters of technological design. The analysis of public perceptions takes the paper into a more sociological manner of argument. In the discussion of compulsion, the paper uses approaches from normative political theory and philosophy.

The proposed Entitlement Card scheme

The Home Secretary's has presented proposals for a scheme in which all UK residents would be required to register for and possess a token – in all probability a smart card – for identification purposes (Secretary of State for the Home Department, 2002 – hereafter referred to as *ECIF*). In addition to a card validation system, that token would probably include a biometric of some kind to enable the person to show that the card is indeed theirs. The proposed scheme would build upon the two photocard schemes, the photocard driving licence and the already proposed passport card. A third type of card, which would be a simple entitlement card, would be available for those who are either ineligible for a passport or driving licence or who do not wish to have one. However, the whole system of entitlement card tokens would be linked to a population register, with a unique number for each person, which would be separate from the existing passport and driving licence databases. It would be compulsory to register for and possess the card, but there would be no additional powers for police officers or other public officials to demand its production or access to data held in it, other than those they presently. This, the paper describes as a "universal" rather than a "compulsory" scheme.

The general claim for the entitlement card (from now on, *EnC*)[1] is that it would provide *simpler, more secure and more accurate identification* than the means currently available for demonstrating that the holder is entitled to particular services, particular treatment by officials, etc., than the means currently available. In the government's view, the two main categories of benefits of the scheme would be the following:

- The EnC would be more *convenient*, because it would eliminate the need for a plethora of other documentation and checks, which would thereby eliminate delays, and because the data flows supported would replace much manual data entry, and eliminate duplication in requests for the same information. ECIF also states (2.36) that the underlying population register would support greater data matching and sharing between public services to eliminate errors and increase efficiency.
- The EnC would help to *combat identity fraud*, by providing a greater assurance than with presently available means that the holder is indeed the person they say they are.

[1] "EC" would have been more logical, but its common use to mean the European Community would have made it confusing.

The specific fields in which the government expects to see the most significant benefits are

- Greater convenience:
  - faster processing as a *travel* document than the present passport book;
  - easier *proof of age* for young people than with presently available instruments;
  - eliminating duplication in requests for information to the *electoral register*;
  - faster and more appropriate *emergency medical treatment* where the cardholder consents to permit a limited amount of their health status and treatment information to be accessible via the card;
- Combating identity fraud:
  - reducing *illegal immigration and illegal working* (and related convenience benefits such as reduced costs to employers of compliance with laws on illegal working); and
  - reducing crimes in which identity fraud is an important component, such as *money laundering* and *organised crime*.

It is proposed that the central population register would hold the following information:

1. name;
2. date and place of birth;
3. residential address;
4. unique personal number;
5. other personal numbers (NI number, driver number, passport number and, if either the card scheme or the particular card were extended, with the cardholder's, consent to link with other services, other numbers used by those services);
6. nationality;
7. sex;
8. digitised image of signature;
9. photograph (presumably digitised);
10. validity dates for the card and issuing agency;
11. issue number of all cards held (for many people will have both a driving licence and a passport card);
12. employment status;
13. biometric information; and
14. PIN, password or passphrase.

The central database would not hold information on other service entitlements, although these would be linked as appropriate.

In addition to the photograph and the name of the card holder, displayed on the face of the card would be

- unique personal number;
- national insurance number;
- nationality; and
- employment status.

The information held in the card would include

- for driving licence cards, all the present driving licence information such as the types of vehicle the holder may drive, any endorsements; and
- for passports, all the present passport information;

The card might also contain an electronic signature.

ECIF recognises a number of risks and presents some safeguards. The following risks (usually noted as "potential drawbacks") are identified within ECIF itself:

- *Unfair denial of service*: Some citizens could be denied services to which they are in fact entitled, simply because they are waiting for an EnC to be issued, or because they have lost it or it has been stolen from them and they are still waiting for a replacement (3.7).
- *Fraud*: The EnC will itself be counterfeited, and therefore the subject of some identity fraud (3.11; 4.6). As the Cabinet Office report on identity fraud notes "An identity card is only as secure as the processes used to issue it and the safeguards employed against counterfeiting and theft. In the US, where the social security number and associated card have, through use and custom, become the *de facto* unique identifier and identity card, identity theft is rife." (Summary, paragraph 6)
- *Project risks*: Large government IT projects have a history of delays and cost overruns and other implementation difficulties.
- *Costs*: The scheme would have significant costs in many categories include investment, training and operation, and many of these are uncertain. It is difficult to quantify the monetary value of the benefits in advance, and so a rigorous cost-benefit analysis cannot be presented.

The consultation paper acknowledges that the proposal may raise privacy concerns, but does not acknowledge any specific risks. The government's view is that none of the data protection principles would be violated by the scheme. However, ECIF does acknowledge that there are some issues of risk that should be taken into account:

- *Legislation*: where additional public sector services are to use the central register as the main or sole means for identification, this would require legislation (6.4).
- *Consent*: Where private sector organisations use it for identification, whether as the main means or not, procedures for informed consent must be in place (6.4)
- *Purposes*: The primary legislation must define the purposes for the scheme, or there could be problems of "function creep" (see below).
- *More information disclosed than strictly necessary for some services*: The information displayed on the face of the card and accessible through the central register would "almost unavoidabl[y]" in any multi-use card scheme be more than strictly necessary for some services, but in the government's view, this problem in relation to the data protection that information must be limited to that which is relevant and must not be excessive for purpose is "probably outweigh[ed]" by the advantages.
- *Real time online subject access*: This would be permitted, using the EnC, only where the biometric security was sufficient to ensure that the risk was minimised that a stolen card could be used in this way, and that there would be no possibility of a subject changing information on the central register.
- *Data sharing*: The system will rely on a variety of flows of data sharing in order to work. For example, there will be data sharing in the course of the checks made on application for a card, and this may involve accessing private sector data from credit reference agencies. There will be data sharing using "gateways" at the

point of use of the EnC to establish its validity and genuineness. Where the EnC is used to establish entitlement to particular services, there will be access to the central register by those services to verify identity (6.20).

- *Additional data holdings and disclosures*: The results of the proposed additional checks for applications for both passport and driving licence cards may be recorded in "an identity database shared jointly between the passport and driving licence systems", which could be made available to government agencies and private bodies; in the case of the former, disclosures could in some circumstances "where there was a clear justification", and "provided the necessary legislative powers were in place", be made without consent (4.12).

Benefits

It is important to acknowledge that the benefits selected for particular attention in ECIF are quite limited. In particular, and unlike the previous administration in arguments presented by its ministers for its 1995 identity card proposal and unlike some of the supporters of the present proposal, the government has *not* claimed that the EnC would make a significant contribution to

- combating terrorism;
- reducing benefit fraud;
- reducing tax fraud;
- reducing smuggling;
- reducing types of crime other than those of illegal immigration, illegal working, and those areas of money laundering and organised crime that make intensive use of identity fraud.

By contrast, many advocates of such schemes have argued, rather implausibly, that they can make a significant contribution to tackling these kinds of problems (cf. Etzioni, 1999, ch.4)

The government has also been careful to avoid any suggestion that identity fraud could be eliminated, but merely that it might be reduced. Similarly, the government does not claim that all bureaucratic inconveniences experienced as a result of checks being made, or all duplication in requests for information, could be eliminated as a result of the introduction of the card, but instead ECIF talks of reduction.

This both strengthens and also weakens the case for the EnC. The modesty of the claims makes them much more plausible. For indeed, it would have been quite implausible to suppose that a card scheme of this nature could have done very much in itself to tackle these other evils.

Many terrorists have in fact not found it necessary to disguise their identities in order to hide their activities. Indeed, the facts that many IRA operatives have used their own names, that al-Qaida used people with no previous convictions of any kind in the attacks in New York and Washington on 11th September 2001 and that several of the group who committed those outrages in fact possessed identity cards from some European states, all show that it would be wrong to hope that such a scheme could achieve much there.

It is widely documented that most benefit fraud consists in the misrepresentation of circumstances rather than identity. The scale of the excess of national insurance numbers issued over the numbers of persons alive who have been of an age to be in the labour market and the infants with numbers since the government started to issue numbers at birth, suggests that there may be some identity fraud in that system, but it is not clear that the EnC would really help with this problem. The EnC might help at the margin with some very simple misrepresentations of circumstances, for if the entry in the database for employment status is always up-to-date and accurate, even for

people who frequently move into and out of work in any case, then it might help identify some people who are working and claiming at the same time. It has also been said that it might help to limit the ease with which people make multiple applications for benefit even using the same name, although it is hard to see what the EnC can add to existing capabilities for tracking multiple applications using the same name. The Department for Work and Pensions has recently acquired new powers for data matching and sharing to assist in the detection of benefit fraud, in any case, so it is not clear that the EnC will in itself add greatly to these capabilities.[2]

Likewise, police and customs officers report that for most categories of crime, their problems are in detecting, arresting and finding evidence sufficient to convict suspects, not in establishing the identity of persons already selected as suspects and arrested, so that the question of using an EnC to check their identity hardly arises. The Cabinet Office (2002) estimated that if identity fraud costs at least £1.3bn per year to the British economy, fraud as a whole costs at least £13.8bn annually.

However, the care with which the government has delimited the benefits does weaken the case in two respects.

Firstly, this modesty about benefits makes it more difficult to argue that the benefits outweigh the costs of the scheme, taken together with any risks.

Secondly, the fact that what can be expected is only a reduction in a variety of evils makes it difficult to quantify the benefits. Indeed, ECIF does not even estimate a range of monetary values for the benefits, nor does it offer any ranges of probabilities for the achievements of the benefits described.

Improvements in convenience are difficult to measure in advance, because numbers of persons using services cannot wholly be predicted, because the value to those individuals of those improvements varies according to their priorities and values (and is not, for example, any simple function of the value of their time as calculated by the compensation from their present or last employment), and because there are a variety of other administrative pressures that create imperatives for checking processes, to which the presence of the EnC can only be one contributory factor.

The Cabinet Office study on identity fraud (Cabinet Office, 2002) estimated that the cost to UK economy of identity fraud is about £1.3bn per year. However, it is very difficult to say by just how much the EnC scheme might reduce this. For, as we shall see

[2] When he was Minister of State in the Department of Social Security (now the Department for Work and Pensions, Jeff (now Lord) Rooker MP told the House of Commons that the additional powers for data matching and sharing that were in the Social Security (Fraud) Bill 2001 were only necessary because the UK did not have an identity card scheme. He argued that the powers that would be granted to government generally in an identity card scheme would provide for data sharing and matching of the kind that ideally government would have, were it able to join the credit industry's fraud avoidance scheme directly, allowing reciprocal exchange of data between public sector generally and private financial services agencies. The Social Security (Fraud) bill provided the department with equivalent powers for that department. Mr Rooker (as he then was) said that '… the Bill is part of the price that the country must pay for not having an identity card system. We are virtually unique in western Europe in not having such a system. Other countries do not need this sort of legislation' (27 March 2001, HC Debates, Vol 365, Col 917). (I am grateful to Christine Bellamy for this information.) However, the fact that these powers *have* now been given to that department, in that legislation, rather undermines any argument that the EnC would be an important weapon in the battle against benefit fraud, for now it is hard to see what the EnC could add by way of powers either for acquisition of data from or for disclosure of data to the private sector. The fact that ECIF does *not* claim that the EnC would help combat benefit fraud suggests that the government is indeed satisfied that the Social Security (Fraud) Act powers do indeed already provide the agencies with as much as they might have hoped for, from an identity or entitlement card.

below, this depends on three things. First, how great and how sustainable any reduction might be will depend the speed and quality with which fraudsters counterfeit EnCs. Where counterfeiting is not used, any reduction in identity fraud will depend on the quality of the checking process at the point of application to detect persons presenting supporting documentation which is itself fraudulent. Finally, it will depend on the quality of the checks, as actually implemented at the point of use, to detect cases where stolen cards are being used. Dealing with fraud is a classic "arms race", in which each technological advance by the law enforcement agencies is matched sooner or later by technological advance by the criminals. However, it is a race in which a great deal of the efficacy of even the most significant technological advances made by law enforcement agencies is affected by the variations in actual implementation. For example, Schulman (2002) shows how the US / Mexico border crossing card scheme has been far less effective than was hoped, because it proved impossible to afford the card reader infrastructure, because of the scale of counterfeiting, because of the lack of training and support for officials, and because of the weaknesses in the checking processes at the point of application. He concludes that administering a scheme on a national basis in such a way that it makes a significant difference to illegal immigration is a much more demanding exercise in respect of its costs, in the project management requirements and in the general frontline administration, than most governments have appreciated. The fact that many European countries, including France, which have national identity card systems still nevertheless have significant problems of illegal immigration – some estimates for those who are *sans papiers* in France suggest that their numbers may exceed a million – indicates that introducing a card scheme neither guarantees general implementation nor success on this goal.

Moreover, as ECIF notes, the EnC is but one of a series of measures that the government proposes to take to tackle identity fraud, which were proposed by the Cabinet Office (2002). In his Foreword to the Cabinet Office report, the Rt. Hon. Andrew Smith noted that those other measures are not dependent on the EnC, which implies that they should have some significant impact upon identity fraud, even were the EnC not to be introduced. However, it is not really possible to quantify the likely value of the measures, either separately or together.

Like the Government, then, I am unable to find a method by which the monetary value of the benefits can readily be ascertained in advance; indeed some part of the value of the convenience benefits may be in principle impossible to quantify in monetary terms.

Part II: Privacy and data protection issues

ECIF deals with privacy and data protection issues relatively briefly, in a chapter of just 8 pages out of a total of 146. Inevitably, this means that a number of issues, or at least *potential* issues, are either not dealt with or else dealt with too swiftly (see e.g. Masons, 2002).

Exemptions

It is not completely clear from ECIF that the government does not intend to use any of the exemptions under the 1998 Data Protection Act to protect the EnC scheme from any of the conditions for processing or from the principles – for example, on the grounds of national security, or the prevention and detection of crime or the taxation purposes. The general and unqualified statement at the beginning of Chapter 6 that "the government will ensure that any entitlement card scheme will operate in accordance with the eight principles set out in the Data Protection Act 1998" seems to suggest that it will not. The fact that the benefits claimed and sought from the scheme do not include detection of terrorism, that tax fraud is not specifically mentioned, and the fact that only limited numbers of types of crime are discussed – namely, those involving identity fraud – together suggest that the government does not intend to invoke the exemptions. Indeed, having set out its goals in the way that it has, it would be difficult for the government to make out a strong case for an exemption.

In my view, a decision to submit any scheme to the full discipline of the Act would be welcome and it would be helpful for the government to make clear in the final statement of its position following the consultation period that indeed it will not seek to invoke any of the exemptions. The consequence of this for the argument of this paper is that I shall consider a number of the main conditions and principles, on the assumption that they will apply in full in any EnC scheme.

Indeed, the government would be wise not to seek exemptions for the scheme as a whole. To do so would make it difficult for them to demonstrate, in the statement of compatibility between the EnC legislation and the rights granted in Article 8 of the European Convention on Human Rights (which the Secretary of State is required to make to Parliament on presenting the bill, under S.19 of the Human Rights Act 1998), that the "interferences" with privacy which the creation of the central register represents are indeed made "in accordance with the law".[3]

Of course, once an EnC scheme were in operation, this would not preclude particular public officials such as police officers or fraud investigators, from applying for exemptions on a case-by-case basis where those exemptions could be shown to be reasonably necessary for their investigation, given evidence amounting to reasonable suspicion of wrong-doing in that particular case.

[3] Difficult, but not impossible, if the government were prepared to take political risks. The only way to make the statement of compatibility if the scheme were exempt from the Data Protection Act would be for the EnC legislation to set out detailed provisions on what would be done with the powers granted under the exemptions, how the use of the exemptions would be limited, and how oversight would be exercised to minimise infringement of Convention rights. Not only would this be difficult to draft: it would be politically difficult to explain to voters. Technically, the government could admit incompatibility and proceed with the scheme anyway (under S19.2, HRA 1998, ch 42), but to do so would risk enormous political embarrassment unless it could show that the EnC scheme was an urgent and effective response to a major national emergency that required the abrogation of Article 8 rights. In practice, this would be likely to require making a reservation to the Council of Europe, which would require detailed justification to Parliament, media and voters. Making a derogation is another possibility, but this has only been used for counter-terrorism measures (HRA 1998, Sch 3), and in any case ECIF specifically concedes that the EnC is not presented as effective in combating terrorism.

Conditions for processing

Schedule 2 of the Data Protection Act 1998 requires that, unless an exemption applies and where the data do not fall (as the government's proposal is that they will not) within the definition of "sensitive" data, certain preconditions must be met before processing of personal information can be lawful.

At the heart of the various limbs of the test is the concept that, where processing is not undertaken with consent, the processing should be *necessary* for at least one of various things. These include completing a contract, complying with a legal obligation, or protecting the data subject's vital interests (meaning, in the Commissioner's view, an emergency matter of individual life and death: see Information Commissioner, 2001), and the administration of justice. None of these is of central relevance to the present scheme, although undoubtedly cards would be produced and data processed from them, among many other settings, in the course of the administration of justice. Of more concern are the following three clauses, which permit processing provided it is *necessary*

- for the exercise of any functions conferred by statute;
- for the exercise of any of the functions of the Crown, or a minister or government department; or
- for the exercise of other functions of a public nature exercised in the public interest.

In principle, the government could simply use its powers to design the primary legislation in order to enable it to invoke one of these clauses in order to deem the EnC scheme to have met the conditions for processing. It could simply write into the statute that running the EnC scheme is one of the functions of the Home Secretary. This would comply with the letter of the conditions for processing in bureaucratically minimally required manner. However, that would be a rather shabby way to proceed, since it would not be a substantive argument for necessity.

While the processing might be technically necessary in the Data Protection Act sense for the fulfilment of a statutory duty put in the legislation to administer an EnC scheme, this does raise the wider consideration of whether the processing involved is really necessary *to administer the public and commercial public services that will be the major users of the card and the central register*. It is this substantive test of necessity that Article 8 of the Human Rights Act raises for any legislation or scheme that would "interfere" with privacy, as the proposed creation of the population register and the proposed powers of data sharing would. Article 8 reads as follows:

> Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is *necessary* in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
>
> [emphasis not in original]

The fact that the UK has conducted its affairs under roughly its present constitutional order and system of public services for many decades without a national population register suggests that the EnC scheme cannot be *necessary*, in general, even for the purposes of identifying UK residents or for administering the control of

entitlement to public services (which would presumably be part of the prevention of crime and perhaps of economic well-being). Necessity in this sense implies some fairly serious failing in the absence of the measure. For example, it is not the case that, for lack of a scheme of this kind to limit services only to those legally resident in the country or with a certain employment status, there is a crisis of public expenditure requiring major cuts in entitlements to NHS care or to means-tested benefits. In practice, these services have found ways over many years of defining the information they require for the demonstration of identity and entitlement and for the detection of fraud that have worked reasonably well, and that have been steadily augmented in recent years with new powers. Moreover, to the extent that there are problems of benefit fraud, they are not generally ones of identity fraud or indeed problems which the EnC might make a very large contribution to solving.

The figure of £1.3bn as annual value for identity fraud in the UK, out of a £13.8bn estimated value of fraud in total, cannot really be used to demonstrating a failure on the scale required to meet a necessity test, precisely for the reason that the government cannot demonstrate the EnC scheme will reduce identity fraud to any specifiable level in a sustainable way over time, given the probability that the EnC will itself be counterfeited and sometimes successfully applied for illicitly. It would be hard to say that as a reasonably successful developed economy, the UK exhibits the kind of extensive failure in economic life or public services that only an EnC scheme could correct.

Certainly, human rights legislation would not be interpreted in such a way that it ruled out any innovations that involved data processing save in the event of major crisis. That would be absurd. However, the fact that the Article uses the term, "necessary" – rather that say "convenient" or "beneficial" or "worthwhile" – as the test for acceptability is important. If the government is to make the substantive case for the scheme, then at the very least it must be shown that the problem to which it is presented as the solution is sufficiently great that the costs and risks, including the privacy risks, of the scheme, are ones that are worth paying.

Fair processing

ECIF only discusses the "fair processing" rule in relation to the possibility of private sector organisations using or abusing the unique identifier without good reason in ways that are not permitted by the primary legislation (6.5). However, there are other fair processing issues to be considered.

The main questions about fair processing do not arise in connection with the compatibility of the EnC scheme in principle as it might be set out in primary legislation, but rather in relation to risks of particular abuses that might be carried out by particular officials who demand the production of cards and who access data on the central register.

If a particular group in the population were to find that its members were subject systematically to more frequent demands for production of the card and identity checking which involves accessing and processing the data on the central register, this might not only be harassment in civil law, but could also be found to be unfair processing of the information accessible through the card. For unnecessary requests for identification data, and accessing those data from the central register, would well in these circumstances be "unfair" to the individual data subject. The Commissioner has said that the fair processing principle is to be considered in the light of the consequences of processing for the interests of the data subject. Discriminatory repetitious access to identification data could in particular threaten the interests of ethnic minority data subjects.

It is an understandable concern that a card which is explained to the public and to officials administering public services as one that is to be used, among other things, to

combat illegal immigration and illegal working will raise concerns among some ethnic minority groups that they may be asked to produce their card more frequently than, for example, people from the white, primarily Anglophone majority. Discriminatory practice in demanding production of identity or of other documentation, such as evidence of legal title to a car one is driving, has been criticised over many years in a number of reports on police practice, going back at least far as the Scarman report into the 1981 riots in Brixton. Traditionally, such requests have been for paper documents, and have not involved the processing of data online. When officials repeatedly and unnecessarily demand the production of a smart card, insert it into a reader device and access identification data from the central register, this will amount to "processing", and so will fall within the data protection principle.

The government may have two replies to this concern. The first is that no new additional police powers are being proposed to demand production of the card for identification over and above those which police officers already have. The second is that the card should provide a swifter and more efficient means by which to process and so dismiss any unfounded suspicions.

However, these points do not deal with the matter entirely, or with the fair processing implications. Firstly, as ECIF notes (2.16), police officers are not without powers, in effect, to demand identification: even minor offences become arrestable if identity cannot be ascertained or if there is suspicion that a name and address given are not genuine. More importantly and secondly, the EnC will be demanded by a great many more public servants, and indeed staff in private organisations working under contract to public authorities to provide services, than just police officers. One cannot rule out the possibility of systematic discrimination in the frequency with which cards are demanded and the information on the central register is read, checked with other documents the person may carry, and cross-checked with service-specific databases, and it will be important to ensure that there are safeguards in place.

At the very least, for example, data subjects could be given a receipt on each occasion that their card is taken and their data are read. This might either be in a printed form from a ticket printer attached to a card reader device, or it might be sent to them automatically by whatever means they agree to, when they make their application for the card. This would enable the creation of an audit trail with which data subjects whose data were being processed excessively could use to seek redress. (It is surprising, for example, that ECIF is silent on the issue of the need for an audit trail of occasions on which data were accessed, particularly in the light of the fact that the consultation paper discusses the possible health care uses. For the current Department of Health consultation paper on privacy in electronic health records does – and rightly – propose to provide for just such an audit trail in all new NHS systems: see NHS Information Authority, 2002, p.6) Otherwise, there could be cases brought before the Information Commissioner under the fair processing principle.

These are all matters that ought to be the subject of quite detailed guidance in a Code of Practice for public servants who may have occasion to ask for identification and to demand production of cards.

Purposes

The second data protection principle restricts processing to that which is compatible with the specified and lawful purposes.

ECIF states that the purposes for the EnC scheme will be (6.3)

1. to provide people who are lawfully resident in the UK with a means of confirming their identity to a high degree of assurance;
2. to establish for official purposes a person's identity so that there is one definitive record of an identity which all departments can use if they wish;

3. to help people gain entitlement to products and services provided by both the public and private sectors;
4. to help public and private sector organisations to validate a person's identity, entitlement to products and services and eligibility to work in the UK.

(As will be discussed below, as it is written, the third purpose could be achieved, for the card scheme does not itself add any new entitlements: any "gain" could only be in the ease with which a person might use the administrative processes required to secure their existing entitlements.)

This list of proposed purposes is extremely broad, and this breadth is in itself a matter of concern in data protection law. The expansion of the definition of purposes can be a way in which to evade the spirit and indeed sometimes the letter of the Act.

These proposed purposes are remarkable at the very least in that they are *independent of any particular service*, or of any *field of service*, or type of *substantive benefit* in the interests of the data subjects. Indeed, on the contrary, the purposes that the Home Secretary proposes are *generic* and *procedural*.

There are good reasons for thinking that these purposes are too broad. It would not normally be considered an acceptable purpose in data protection law that processing should be for the prevention and detection of crime or fraud quite generally. A set of purposes of this kind which in effect specify a purpose of providing a means for checking for the possibility of identity fraud is not much narrower than that, and should be questioned for the same reasons.

The point of the requirement in data protection law for specified purposes is to give citizens as data subjects and data protection regulators a clear understanding of the intended boundaries around uses, disclosures and around what information would count as relevant, and therefore to prevent "function creep" or the steady inflation in the range of uses (see below). The underlying argument is that citizens cannot be expected to trust in governments and in public services which do not adequately define and delimit the purposes for which citizens' personal information will be used. The four clauses listed in paragraph 6.3 of ECIF do not do this, for they do not exclude any categories of information as clearly irrelevant and excessive for purpose, nor do they clearly exclude any categories of inferences from data or any types or destinations of disclosures as improper. For a scheme of the political salience and sensitivity of this one, the government would be wise to provide a much more detailed, tightly delimited set of purposes defined around categories of public and commercial services and to specify just what will count as adequate evidence of entitlement for each of them, and for just which of those services, named identification is really necessary and why, and to spell out clearly just what benefits citizens can expect in each service from being able to or required to use the card.

The fact that the scheme is built upon the passport and driving licence systems (together with the new central register for third category of EnCs) is not of much help here, because in effect what ECIF is proposing is a very large extension indeed in the specified purposes for which passport and driving licence data may be processed.

Function creep

"Function creep" is the term usually used to describe the tendency over time of instruments or initiatives involving data processing initially for one specified purpose to come to be used for other purposes. This is of course a violation of the second or finality principle of data protection, but function creep does occur. In general, the more broadly framed the specified purposes of any instrument or activity of data processing, the greater risk of function creep, because broad purposes make it difficult for anyone to determine clearly what, if anything, might lie beyond their scope. The EnC proposal is quite specifically designed to be open-ended in the list of services that might use it as

the main or principal or even sole means of identification for applicants. Indeed, as was noted above, the way in which the purposes are set out in paragraph 6.3 provides very little guidance on what would be excluded.

ECIF envisages the extension of the central register into the control of entries into the electoral register. Since the question of whether a person is lawfully resident in the UK is a relevant consideration in applications for cash benefits, for tax exemptions and now for certain kinds of health care, it is clear that one of the implicit purposes of the scheme is to enable those who are expected by government to act as gatekeepers for services to patrol more effectively for compliance with the rules by which services are rationed. Although this is nowhere stated in ECIF, and certainly the consultation paper provides nothing so tasteless as estimates of the sums that might be saved to the taxpayer through excluding persons who are not lawful residents from public services (the savings identified are all to do with substitutions for current procedures, not to do with substantive savings on service expenditure), it is clear that this must be a consequence of the scheme. Does this represent a logical corollary of the purpose of identification for entitlement to public services, or does it represent function creep? The way in which the purposes are specified makes it very difficult to know.

Indeed, where the EnC becomes not just one or even a main but the sole means of identification, is it then fulfilling its purpose, or has it gone beyond it? Again, it is hard to be sure, but the question might well be litigated.

The question of function creep becomes even more difficult when questions of data matching and data sharing are considered. As has been noted above, some data sharing and matching activities are inherent in the nature of the proposed scheme. These occur at the point of application, at the point of voluntary presentation of the card in the use of services, and in the course of activities of public officials who may demand the card under powers to sanction citizens found to have abused services or committed crimes, or may access the central register in the course of their investigations without the presentation of a card. The four limbs of the purpose statement at 6.3 are not, even taken together, sufficiently precisely framed to enable anyone to determine just which practices of data matching and data sharing might represent fair processing in the light of these purposes, and which might represent disclosures in violation of the principles of the 1998 Act.

For example, ECIF envisages that the a multifunctional smartcard might be issued as an EnC which would include space for a directory that would support a season ticket for a transport service: the data on transport usage and payment would not be held on the central population register for the EnC, but there would be an ability to link between the two, not least because of the need to reconstruct the whole card in the case of loss of theft (6.11). The travel company would only be able to access the central EnC register subject to conditions set by the government on the use of the general identifier. However, exactly what conditions the government would impose are not spelled out in ECIF, and so it is not yet fully demonstrated that they will fully control risks of function creep. Transport companies have a variety of marketing reasons for wanting to acquire more information about their customers and passengers. Marketing would surely be a distinct purpose for the scheme, and it would be a purpose which would have to be declared for the central register and not only for the travel companies: however ECIF's stated list of purposes do not cover this, even though the consultation paper does acknowledge this use.

Consider the question of the use of the data from the central register in the course of criminal investigations. In principle, a police officer might access the central register, even without demanding the card from an individual and inserting it into a reader device, if they have other identifying data and online access to the central register from a computer. In the course of the investigation, for example, the police officer might come

to consider that it would be useful to see whether a person's entry on that central register shows them to have a particular employment status, or they might find it useful to discover other identifiers such as national insurance number or driver number or nationality or indeed to obtain the digitised photograph. Is this something that is within the second of the four purposes, as being a definitive identity that departments can use if they wish? Or within the first half of the fourth – that is, helping organisations to validate an individual's identity? Perhaps it is. Yet the statement of purposes says nothing about assisting the criminal investigations as a purpose: it would be clearer if it did. However, it would not clarify anything were the government try to put in a purpose for the scheme that allowed the data on the central register or accessible using it (e.g., through the other identifiers recorded there) to be used in any manner a public servant considered conducive to the prevention or detection of crime, fraud or abuse. In order to be adequately "specified", and to prevent function creep, purposes must be much more tightly delimited.

More generally, in answers to questions at public meeting on 11 December 2002 at the London School of Economics on the proposal, Lord Falconer of Thoroton, Home Office minister, said that function creep will be controlled by the requirement to obtain additional primary legislation for any additional functions. In a technical sense, as a statement of the principle, of course, this is true.[4] However, this is not a satisfactory answer to the concern, for unfortunately, the fact that the purposes are so widely defined means that it will not always be clear just when additional primary legislation would be needed and when it would not.

Excess

The third data protection principle requires that personal data shall be adequate, relevant and *not excessive* in relation to the purposes for which they are processed. This is one of the most important substantive principles, and the issue of what information might be is excessive for purpose is especially critical in the case of databases such as the proposed central population register for the EnC system, which are designed to interface with many other databases and thus are expected to provide a wide variety of disclosures.

The first problem in establishing just whether and how far the EnC system might meet the standard set in this principle is that – as has been noted above – ECIF provides a statement of the purposes of the scheme that is very broad indeed. The purpose statement is crafted in procedural terms. Because no particular services with their particular entitlement rules are identified, ECIF cannot proceed to use these to define the information requirements for each, which would result in a well-designed system of information requirements for each principal type of event accessing the central register. It is therefore very difficult to determine just what is excessive for the purposes.

ECIF admits that the EnC scheme will violate the third data protection principle, but claims that the benefits of the scheme will outweigh the costs and the risks. Paragraph 6.10 reads as follows:

> If they were used as entitlement cards, both the photocard driving licence and – to a lesser extent – the passport card would therefore show more information than was strictly required for their individual purposes. This is almost unavoidable in any scheme involving dual or multi-use cards.

[4] The meeting was hosted by Privacy International, Liberty and the Foundation for Information Policy Research. I am not aware of any official transcript of the proceedings of the meeting, but I have a full set of handwritten notes taken during the meeting. A news report of the meeting can be found at BBC Online (2002).

> The advantages in terms of the convenience to the card holder of having one card to fulfil a number of purpose probably outweigh the disadvantages of displaying on a single card slightly more information than in strictly necessary for each individual entitlement.

However, the question of information excess in the EnC scheme cannot be dismissed nearly so quickly.

Firstly, the issue does not arise solely in respect of the information displayed in plain text on the face of the card, but also in the case of the information stored in the chip or on the central register which is accessed by the card reader device. Dealing with this will require several things. First, the face of the card should contain as little information as possible. Secondly, the software with which card reader devices are managed must be so designed that it will limit then information that can be accessed both by the nature of the organisation holding the reader device and by the particular purpose of the enquiry for which the card was produced and read. Thirdly, there would have to be strict organisational protocols to ensure that each organisation only used reader devices configured for their particular legitimate interests and did not "borrow" devices from others, or trade them, or attempt to reconfigure their devices.

For example, information about the card holder's employment status may be relevant for applications for certain cash benefits, but will not be relevant in many driving-related contexts or in proof-of-age contexts. Again, consider the issue of a person's date of birth. The government proposes that the EnC might be used as an instrument for proof-of-age (3.23-3.24). However, in order to show that a person has the right to enter a public house, or purchase tobacco or a pet, the publican or retailer do not need to know the person's data of birth: the information is excessive for the particular purpose of this transaction, which is a case of the general class of purposes (identification for entitlement) that the government would set out for the scheme as a whole. It is necessary only that the card should reveal to the card reader device the information that the holder is of age to enter or to purchase, not that it should reveal the particular or exact age of the holder. Again, for these purposes, nationality and employment status are generally irrelevant and excessive. Indeed, even the name is excessive. Therefore, the card holder's name should not automatically even appear displayed on the face of the card if one of the aims is to support simple proof-of-age.

ECIF says very little about just how it will be ensured that information taken either from the card or from the central register will not be captured and stored in other databases after the particular transaction for identification using the card has been completed. Since much of the information in principle available through the card would be excessive for the purposes of many of the service transactions in the course of which it might be used, this is a major data protection concern. Capture and retention of information will be a very significant issue where the card is used in the private sector, not only for privacy reasons but also because it would represent a huge information subsidy at the taxpayers' expense to commercial database builders. However, capture and retention will be an important issue, not least because of the technical imperatives to allow audit trails (a matter on which ECIF is rather oddly silent), and the technical impossibility of enforcing any legal rule prohibiting retention.

The central problem about excessive information is the way in which the concept of identity is used in ECIF and indeed in much of the debate about identity and entitlement cards. From a data protection standpoint, identity is that irreducible minimum of information about an individual data subject that is strictly necessary for the purpose of the particular transaction or event to enable that transaction or event to be completed effectively and meaningfully with proper safeguards for data subject and organisations using their data, but no more. That is, from a data protection standpoint,

identity is *contextual*: for the necessary minimum of identifying information required for identification in the setting of passing through passport control, of satisfying a police officer of one's authorisation to drive a car, of purchasing fireworks, and so on, will be significantly different. For example, in a setting where the crucial issue is proof-of-age, one's name and address is excessive.

However, this is not at all how ECIF understands the concept of identity. Annex 4, paragraph 20 sets out the Home Office conception. It defines identity as a vector of characteristics – biometric characteristics, lifetime characteristics that are institutionally fixed such as date of birth, name and parent's names, and variable or "biographical" characteristics associated with particular events in one's life. Although the link is not spelled out in full, the information that has been selected to be proposed to be held on the central register seems to reflect an idea of a "core set" of these characteristics that can be assumed to be relevant, irrespective of context (Annex 4, paragraphs 85-95).

Beginning with this context-invariant conception of identity, an inability to comply with the third data protection principle follows fairly logically.

The general claim that the gains in convenience will outweigh the risks is not one that can be made without a great deal more analysis of the risks that might arise from the disclosure and probably retention of at least some of the excessive information about individuals. Unfortunately, the open-ended nature of the scheme, the fact that an indefinite number of services might use it, makes it almost impossible to conduct such a risk assessment.

May the benefits lawfully be "balanced" against the privacy risks in this way? It is far from clear that they can. The third principle is not drafted in such a way that it permits any balancing between convenience and excess or irrelevance. While gains in convenience might be "legitimate interests" of data controllers, the Data Protection Act only allows those interests to override privacy concerns where the processing is *necessary* to secure those legitimate interests. It would be very difficult to show that this is the case, for the benefits of the scheme cannot be established clearly (indeed, ECIF cannot credibly and does not attempt promise any particular level of reduction even in identity fraud) and because there are many other ways in which greater convenience in securing entitlements to services might be achieved.

Accuracy

Accuracy of data is the fourth and a very important principle of data protection law in the UK.

In the consultation paper, the government makes very large claims for the improvements in the accuracy and quality of personal data that can be achieved through the implementation of the EnC system and the population register. ECIF claims that the standard of accuracy of entries in the central register will be sufficiently greater than that of other government databases (2.26) that it will become the key tool in combating fraud (4.12), that overall efficiency in public services will rise (2.36), and that it could in time actually replace other registers such as the electoral register (2.36).

If these claims could be substantiated, then they would represent an important benefit from an EnC scheme, and one that would weigh with the Information Commissioner. However, it is not wholly clear from ECIF just what these claims are based on.

Accuracy of the central register for the EnC system would be, if this is possible, even more important than accuracy for other databases used to administer public services, if the intention is that it should be used to correct those other databases. For otherwise, it will present significant risks of "error infection" or the transmission of errors to other databases, making them harder to eradicate.

Most databases contain significant numbers of errors. The levels of errors in the Criminal Records Bureau databases were a major scandal during 2002. At various times in its history, the Child Support Agency has been in the news for the high rate of errors in its databases leading to inappropriate decisions. The Audit Commission has recently reported in a study of health records that it has found "obvious errors", some minor and some less so, without detailed checking, on the face of some 40% of health records (Dr Marion Chester, Association of Community Health Councils in England and Wales: presentation to the Privacy International, Liberty and the Foundation for Information Policy Research meeting at the London School of Economics, 11 December 2002: the Audit Commission (2002, 5) has recently declared that NHS bodies still "have a long way to go" to improve the quality and accuracy of patient-based information). The Driver and Vehicle Licensing Authority's own study of the accuracy of its databases suggests that between 24% and 30% of all records contain at least one error – mostly in postcode and address fields and also in names – even on the narrowest definition of an error, and 91% of all forms submitted contained some error (National Audit Office, 2002, 13-14).

Data will accrue to the central register for the scheme in several ways:

- some data will be *internally generated*: for example, the unique personal identifier will be generated by some algorithm internal to the system;
- individuals will *voluntarily supply* data at the point of application in the form of their own written information and in the form of any supporting documentation they must submit with their application, and at various times thereafter if they provide updating information;
- information will be *obtained through checks* made in the course of making decisions on applications, and this may involve some data matching and data sharing across the public sector, and may also involve buying data from commercial credit reference agencies; and
- some data will be *captured automatically*, for example, at the point of card validation, and in the construction of any audit trails of the use of the card.

Data accrued to the register may then reach the record for an individual in a variety of ways:

- it may be *entered manually* by a data entry clerk into fields in the record;
- it may be *read from some analogue source* by machine and transformed into digitised material and those data routed into fields in the record; or
- it may be *collected* from another digital source, its classification taken or else checked and corrected, and then routed into fields in the record.

Finally, there may be combinations of these methods for certain kinds of information that must be assembled from several sources. Having been entered, the data may then be checked either manually by a human being reading them and checking them against other sources, or they may be checked by using data matching. A data matching algorithm, having identified any items of discrepancy that could be errors, may simply flag up those discrepancies for a human being to make a decision upon, or may use some recommendation-generating system to identify a proposed correction, or could be programmed in some circumstances to make changes automatically.

Each of these methods of data accrual carry certain types of risk of generating errors at the stage of data gathering, data entry and data checking. In general, any system for reducing the numbers of errors in databases will only achieve those reductions if additional expenditure can be supported to enable additional manual and automatic

checks, and at the cost of additional time taken between the date of data acquisition and the date of signing off of a record as correct.

The cost estimates presented in Annex 5 of ECIF do not include a detailed breakdown of the costs for improving accuracy, nor indeed does the document as a whole include any specific targets for levels of errors. It notes that the process will require the hiring of staff and the investment in and installation of hardware and software including systems to support biometric recording and recognition. But little is said that is specific about how the aspirations for greater accuracy will be met. In general, in order to improve accuracy in the handling of biometric data, and to reduce false positive and false negative results, it is necessary to use more expensive systems.

Moreover, some of the ways in which the document as a whole discusses processes which would impact upon possibilities for error reduction do give rise to cause for concern.

For example, Paragraph A5:21 suggests that additional investment in capacities for biometric checking and other automated checking systems will reduce the need for staff. The history of large information technology projects is that net reductions in the demand for labour take a very long time to show up, and that in the short and medium run, additional staff are often required, albeit in very different roles from those which such organisations may have required before the new investment.

ECIF also stresses that the government will seek to simplify and speed up the application process. The Home Office "Frequently asked questions" document (Home Office, 2002), for example, states that few additional calls for information will be made over and above those required for passport and driving licences today, save for at most a single face-to-face meeting with the applicant (Q.23). Such a meeting would certainly increase the complexity of the application process, but would do little in and of itself to reduce the error rate in entries in the register, not least because meetings at the point of application would take place before much of the data to be entered had been acquired by the central registration body. If delays in handling applications are to be reduced in order to achieve the ambitious roll-out targets, and the goals for reductions in identity fraud also achieved, and the rate of errors in the register database at the same time reduced to levels significantly below those of other government databases, then substantial additional resources must be spent on checking. Only significantly increased resources can mitigate the trade-off between simplicity and speed on the one hand, and error minimisation on the other.

Many of the accuracy problems will arise after the initial application stage. ECIF states (6.13) that card-holders would be legally required to inform the central register authority of changes to information held about them, including a change of address. This is already a duty for holders of driving licences, but in practice significant numbers of people do not comply with the duty, and this has resulted in serious levels of inaccuracies on the database. It is often found to disproportionately costly, given the benefits of the scheme, to police non-compliance very actively. It is hardly possible to apply drastic sanctions for failure to provide up-to-date information in all but the most egregious cases, since most failures are the result of absence of mind rather than any deliberate attempt to defraud or deceive. Updating changes of address might become a less severe problem for those people who have reasons to access a number of public services, if data sharing between those services and the central register is permitted. However, that would require a number of specific "gateways" to be authorised in the statute, and ECIF does not set out adequate proposals for this. However, many people who work in the private sector and claim no means-tested benefits and are in good health may use no public services other than the Inland Revenue. Updating of information from the Inland Revenue to the central population register would raise a number of problems in the minds of the public, because personal financial details are

regarded by many people as a category of personal information that they want to feel is kept rather strictly separate from other kinds of information held about them. Even if this were to be overcome, it also has to be recognised that the Inland Revenue databases are always accurate or fully up to date: indeed, recent press reports have suggested that the numbers of errors in Inland Revenue databases may be increasing. In general, this method of updating by taking data from other public services itself raises accuracy risks by way of "infection" with data which are wrongly believed to be correct and up to date. These risks can be reduced only at greater expense per case, by providing for investigation and checking. Perhaps more fundamentally, it undermines a goal that ECIF sets out for the scheme, that the central population register should be so accurate that it will be used to update other public services' databases, and not the other way around.

It *may* be possible to produce a database of this kind that will be systematically more accurate than most databases currently in use in the public sector. However, it must be realised just what an undertaking this would be. To achieve greater accuracy than is achieved by other databases, and to sustain it over time, is extremely ambitious in a scheme which has the following characteristics:

- it is expected to be a register of almost the entire adult population, but one in which where many people will hold more than one card;
- it is to be assembled and in use in a period of just a few years;
- it is to be assembled using a variety of distinct sources of information each of which sources may contain errors;
- it is to be constructed using a variety of entry systems each of which runs risks of errors; and
- it is to interface with a wide variety of other databases for public and possibly commercial services.

The consultation paper does not really substantiate its claim that this is achievable, for it sets out no very clear and structured set of methods and costs for this. Moreover, the consultation paper does not explain how the three-cornered trade-off between controlling cost, reducing delays and complexity at the point of application and improving accuracy is to be managed.

This conclusion has, I believe, some important consequences for the whole EnC programme. If significantly greater accuracy than other public service databases cannot be achieved, then many of the programme's expectations, that it will enable officials to identify people who are not entitled to services and to deny services to those people more accurately and cost-effectively and with fewer "false positives" than current systems can, will in turn not be met. In that case, a significant part of the economic justification for the programme must be called in question, for in part that argument rests on the claim that the costs of administering the programme will be offset and even outweighed by the savings made from improved targeting of services and detection of illegal immigrants and people working illegally. If it is true that accuracy can be improved only with substantially greater expenditure on the programme, then the question must be asked afresh about the cost-benefit assumptions that lie behind the argument in ECIF.

Disclosures

Data Protection law regulates and limits permitted types of disclosures in a variety of ways. The most general is part of the fair and lawful processing condition, and this is interpreted (Information Commissioner, 2001, paragraph 3.1.4) to mean that disclosures must be limited by duties of confidentiality, the *ultra vires* rule and the scope of specific powers, legitimate expectations of the data subject, and Article 8 of the European Convention on Human Rights which provides for the right to private life. Secondly, the

general conditions for processing impose a series of necessity tests on disclosures, and the limb which permits disclosures in the legitimate interests of the data controller or the third party to whom the data are to be disclosed is also limited by a test of necessity; necessity here must be read in the light of the specified and limited purposes.

Regrettably, ECIF does not contain a clear and fully integrated discussion of the disclosures envisaged from the central register to other databases used to provide public and private services. What follows therefore is based on what can be gleaned from several paragraphs scattered across the document. The following are types of disclosures that would be made without specific consent.

1. Disclosures are made *visually*, when the information displayed on the face of the card is read manually, whenever it is presented.
2. Disclosures are made at the point of card *validation*. At the very least, at this stage, the card reader device receives the information that a valid card has been presented; the reader device may retain some kind of audit trail of card numbers, which could be retained by the particular service and, at least in principle, later be correlated with individuals.
3. Disclosures are made at the point of *biometric identification*. At the very least, the card reader device receives the information that the person presenting the card is indeed, on the biometric evidence, the person entitled to hold it; again, this may be retained by the particular service.
4. Disclosures are made at the point of *face-to-face contact* with service providers. In one scenario set out in ECIF, the card holder is asked for, say, the second word of a passphrase in order to enable a check with the central register: the whole passphrase is not revealed. However, if a different word were demanded on each occasion of face-to-face contact by a service used frequently, it would quickly become possible to assemble the phrase. The other principal example in ECIF of disclosure at the point of face-to-face contact is that of emergency medical care, where a person has consented in advance to the holding of some health information either in their card accessible through it, and a paramedical officer uses their card to access that information.

There would in addition be a number of disclosures that could be made with consent. Where the information sought is not statutorily required or deemed implicitly necessary for fulfilling a statutory requirement, the service provider might ask the cardholder for permission to download those pieces of information from the central register (and perhaps retain them on the service provider's database). The system might use the digital signature on the card, perhaps with a word from the passphrase, to record with the central database that consent had been given.

This will raise some complex issues which are not really addressed in ECIF, but which would have to be clarified, about the later withdrawal of consent. How would the cardholder communicate their withdrawal of consent? Could it be retrospective? How would this be processed?

However, where giving that consent became effectively a condition of accessing services at all, and where the services in question were basic and essential (e.g., NHS health care, income maintenance benefits, perhaps certain types of commercial credit) the meaning of consent would be eroded.

Thirdly, ECIF envisages data sharing from the central register, not so much on a case-by-case basis at the point of presentation of a card by an individual, but

- on an *automated* basis: For example, a person might provide updating information on a change of address to the central register, and the central

register would then provide that updated address to other public service databases, in order to reduce duplication in demands for this information.

- on an *individual* basis: In the course of investigating persons under suspicion of being illegal immigrants, or working illegally, or not being entitled to services that they have claimed, fraud investigators or law enforcement officers would secure access to the records on the central register of the individuals under suspicion. This would typically involve data matching.
- on a *routine* basis: ECIF speaks of the routine links between the two constituent databases of the central register – namely, the DVLA and the Passport Agency – as being "gateways". However, these are not the only gateways. Databases for other services would have gateways which are described as being subject to "rigorous access protocols" (5.32), but these protocols are not defined in the paper. Annex 4, paragraph 22 speaks of gateways to databases run by private sector services, mainly in the context of the central register obtaining data from credit reference agencies, and says that these would be operated in compliance with data protection law. However, it neither specifically rules out nor clearly defines and limits any disclosures from the central database on a routine basis through these gateways. Presumably what is meant by a gateway here is the same as is meant by the term in the Performance and Innovation Unit (PIU) report (2002, paragraph 3.50) – namely, both legal powers to construct links and those links themselves between databases, enabling data sharing between agencies, where the legal powers typically specify the uses and purposes for that sharing and in some cases specify the types of information that may be shared. Chapter 11 of the PIU report set out recommendations for a number of new gateways. Several of those involve the DVLA and the Passport Agency sharing information on a routine basis with other agencies include the Criminal Records Bureau, several criminal justice agencies, the Motor Insurance database, and perhaps the civil registration system.
- on a *bulk* basis: in the course of specific exercises to identify potential fraudsters or criminals, a number of records, or fields from a number of records might be transferred from the central register to databases run by particular service-providing or investigation agencies; and
- by *substitution*: ECIF envisages that the central register itself might substitute for other registers, such as the electoral registers.

Finally, Annex 5, paragraph 12 gives a brief list of links with other databases across which the flows of data expected are principally from the third parties into the EnC central register for checks at the point of application, rather than disclosures from it. However, the paragraph does not rule out disclosures to these databases. They include

- the Passport Service;
- the FCO passport database;
- DVLA and DVLNI registers;
- the online civil registration system if implemented by the time the EnC is introduced;
- the National Insurance central index;
- the Immigration and Nationality Directorate database; and
- databases held by one or more credit reference agencies.

In addition, there are already powers in law that would provide for disclosures, for example, in the course of investigations for fraud in relation to benefits, taxes and fees and charges, and general criminal investigations.

The information that can be gleaned from ECIF, even when read together with the proposals in Chapter 11 of the PIU report, does not suffice to enable one to be clear that the disclosures from the central register would in fact comply with the restrictions on lawful disclosures in data protection law.

The statement of the purposes is not sufficiently specified to enable any determination of what the legitimate expectations of confidentiality are. Secondly, it is not clear just which pieces of information that might be stored in the card but not on the central register – apart from emergency health-related information – would be subject to specific duties of confidentiality.

Most important, however, is that in order to meet the necessity tests in the conditions for processing, it would be critical to spell out just which pieces of information that will be held on the central register would be the subject of which types of disclosures to which agencies under which gateways and for which purposes. This would require a detailed tabulation of services, gateways, and fields that could be shared with and without consent and under which circumstances. ECIF provides no such set of tables.

Investigating fraud and crime is clearly a legitimate interest of governmental data controllers and third parties providing public services. It may be that almost any of the fields listed in ECIF as intended to be included in records on the central register might be relevant in a fraud or a criminal investigation.

However, matters are much more complicated where the benefit at issue is either the reduction of duplication in demands for information such as change of address information, or any of the efficiency improvements or improvements in the effectiveness of coordinated service provision that lie behind the PIU report's proposed additional gateways. For in these cases, the imperative for data matching and sharing is of a rather different order of "legitimate interest". Therefore, not every field may be necessary for every type or occasion of matching or sharing, and in some of these cases, as the PIU report itself notes, the Information Commissioner has already held that the consent of the data subject would be required before sharing could proceed lawfully. The Information Commissioner's legal guidance on the "legitimate interests" clause in the processing conditions states that those interests must be weighed together with the legitimate interests of the data subject (Information Commissioner, 2001, 3.1.1). In the case of convenience, efficiency and effectiveness justifications for sharing being claimed as legitimate interests of the data controller and third parties, the relevant interests of the data subject would include those in privacy, which might well militate against unrestricted sharing or at least would call for individual consent, and that could not be overridden so readily as in the case of the imperative for law enforcement.

Perhaps, although the Commissioner's guidance does not put it in these terms, there might be implicit in this argument, a conception that the benefits to be obtained from the legitimate interest in data processing must not be *disproportionately* small when weighed against the relevant interests of the data subjects and the risks that the processing might run of violating the data protection principles from the intended disclosures. The crucial question to be addressed is by what standard proportionality is measured. If the benefits are measured as a proportion of the total expenditure on the service by the data controller, a very different answer would be obtained than if they are measured for the individual data subject. The logic of the Commissioner's guidance and of the law would lead us to think that the latter is the more relevant standard.

Security

The seventh principle provides that data must be secure against accidental loss, destruction damage, disclosure, and unauthorised processing. I am not competent to comment upon technical aspects of security in smart card systems, card reader devices, or in online databases of the kinds proposed in ECIF. However, in a paper of this nature,

it is appropriate to pass some comment on the range of security issues that are raised by the argument as a whole.

The justification for the EnC at all rests heavily on the ability of the system to achieve very high levels of security, and to sustain them over time. For if the purpose of the scheme is one of securing for citizens a means of identification for the demonstration of entitlement, then the cards must be secure against counterfeiting both of the kind that creates an identity for an otherwise fictitious person and of the kind that steals the identity of an actually existing or a recently deceased person. ECIF admits that the EnC will be the target of counterfeiters. There have been cases in recent history in which criminals have successfully counterfeited smart cards. Satellite digital and cable television companies have particularly suffered from this. Because those cards had a single use, the incentive for criminals to counterfeit them might well have been *less* than the incentive to counterfeit an EnC, because an EnC could in principle provide access to a great many services at once.

The most important element of the security of the data held in the card is probably the strength of the encryption used. There is, however, a trade off between increasing security by increasing the key-bit length and improving convenience of use, for longer key bit strings take longer to conduct processing at the point of use.

The central register must also be secure against attack. There seems little doubt that there will be incentives for many organisations, both legitimate and criminal in the nature of their main business activity, to want to gain access to a register of details on all adults in the UK, and so to be tempted to use hacking methods to gain access to it. The central register will hold records employment status and a digitised photograph; it may hold a PIN and a digitised image of hand signature and even an individual's electronic signature. Even more valuably, the card or the register may be linked with other databases which in turn may hold medical information, financial information and a wealth of other service use and transaction data. While hacking may not be the most important risk, there are plenty of ways in which errors in the management of the database can result in inadvertent disclosures. In recent scandals, a utility company, a joint commercial loyalty point scheme based on a smart card, and the Inland Revenue have all experienced problems that resulted in people being able to access personal information about other people over a web site, as a result of incompetent management rather than external attack.

Security, within the meaning attached to it in the Data Protection Act, is not only a technical matter to do with firewalls, encryption, passwords, PIN numbers, levels of authorisation and so on. The Commissioner's legal guidance makes it clear that organisational and management issues are key to ensure that human failures, incompetence and corruption are minimised. In particular, the guidance notes that "sufficient resources and facilities" must be in place to ensure that the duty is fulfilled. Apart from the office management routines identified in the guidance, this will involve ongoing programmes of staff training. Given the scale of the proposed EnC scheme, encompassing as it would a huge range of public services, this would be a costly endeavour. Unfortunately, the ECIF cost estimates do not seem to include budgets for this: the staff costs identified relate only to those for the central registers at DVLA and the Passport Agency, and not to the costs of training for public servants who will access the data systems.

Security is also a crucial issue in the technical basis by which rules are policed against disclosure at the point of use of the card. For when citizens present their cards at the point at which they apply for a public service, they will want to be assured that the public service – or, perhaps of greater concern, the commercial body contracted to provide that service – is accessing only those fields upon their record on the central database or in the card (i.e. neither in fields nor even in directories other than the ones

they are authorised to access), or only those data held in other public services accessible through secondary gateways from the central register, that (a) they are authorised to do and (b) that the citizen has been informed that they are accessing, and that any audit trail or retained data meet the same criteria. They will also expect no data will captured from the central register and retained by the service provider, other than those about which they have consented or at least been informed, and which the service provider is permitted to store, within the purposes of the scheme.

Security is, as has been noted above, a technological arms race. The speed with which improvements in the capability to decrypt or to work around blockages and firewalls become available is such that no smart card can remain in circulation for very long without being insecure. In the case of systems that use encryption of today's typical key bit lengths, it is quite possible that they would become insecure before such time as they would begin to wear out through use in any case. In the same way, it would be necessary to upgrade the security systems of the central register on a constant basis.

To ensure all this requires significant and sustained investment. ECIF does not detail just what the full estimates would be, focusing instead mainly on the costs of biometric infrastructure, which are at most part of the card level security.

Conclusion: a data protection compliant scheme?

It was noted at the beginning of this paper that it is no part of the general provisions of British or European data protection law that it would rule out in principle any kind of identity card or entitlement card scheme. However, this part of the paper has argued the following:

- Unless the government is to use the rather shabby means of simply using statute to declare that running such a scheme is a function of the Home Secretary, the *necessity* test in Article 8 of the European Convention on Human Rights have not been shown by the proposals to have been met.
- The risk that certain groups would face more demands than the majority to produce the card for identification could raise issues of *fair processing* should be reduced by making detailed provisions in a Code of Guidance with statutory authority.
- The proposed *purposes* are very widely drawn and may be too widely drawn to meet the standards of specification that citizens will reasonably expect.
- This lack of specificity in the statement of purposes leads to significant risks of *function creep*.
- There is acknowledged an *excess* of information retained and sometimes disclosed for the individual purposes of the transactions with particular services; the government cannot simply say that this problem is outweighed by the benefits.
- The proposals do not demonstrate that the *accuracy* levels of the central register will be significantly higher than those of other databases in use.
- The range of *disclosures* involved in the scheme is not clearly bounded and so it is difficult to know how the scheme would meet the standards set in law for such disclosures; and
- The *security* requirements will be high and expensive, and the proposals do not demonstrate how they will be adequate to meet the standards expected in this principle.

However, it would be possible to imagine what a set of proposals for such a card scheme would look like, that might meet the requirements of data protection law.

1. To meet the *Article 8 necessity test*, the scheme would probably have to be tied to specific implicit or explicit duties in existing law to run a certain defined list of

services in ways that include specific protection against wasted expenditure due to unacceptable levels of identity fraud or other falsification of personal details or due to provision in ignorance of whether certain facts about applicants or citizens are established.

2. To meet the *fair processing* requirements, there would have to be some enforceable rules about the situations in which and the frequency with which the card might be demanded by public officials for each of the services within the scheme, and some system by which complaints that these rules had been violated could be handled fairly.
3. To meet acceptable standards of *specification of purposes*, a set of purposes should be written that would tie the card scheme quite clearly to a defined list of specific services or areas of law enforcement for which identity fraud is known and can be shown to be a significant threat, or where the absence of reliable authorising information can be shown to be a significant problem. Specifically, these purposes should be based on justifications, for each of the services or fields within the scheme, about the type of information required for that service to be provided. In some cases (e.g., the proof of age contexts), where the name of the individual is not required, what may properly be revealed should not be described as identifying information at all, but simply as authorising information.
4. To prevent *function creep*, the scheme would have to be confined to those services listed in the statement of purposes, and ideally, other services would be expected not to use it and, for example, would not be issued with card reader devices that would be adapted to use the card.
5. To ensure that only information that is *relevant* is held, and to ensure that excessive information is neither held nor disclosed, each of the services within the ambit of the scheme would be audited for the information requirements of their entitlement conditions, and the minimum set for identification would be determined. Then, the rights of access through gateways for data sharing, through reader devices for case-by-case access and otherwise would be limited to those fields within the minimum set for that particular transaction within that service. Thus, in a service such as the commercial purchase of fireworks or cigarettes, the only information accessed and disclosed would be the fact that the person is at least of the age required for that purchase, but nothing more. The scheme would require specific blockages to prevent access to other information. Each field should be given specific justification by reference to the purposes.[5]
6. If sustainably greater *accuracy* than for other databases cannot be guaranteed, then the aspiration for using the central register as the authoritative point of reference for the correction of other databases should be removed from the proposals.
7. A defined list of permitted *disclosures* of each type should be drawn up in tabular form, showing which fields could be disclosed to which services under which circumstances and showing how those circumstances would be defined and recognised within the system. Each entry in the table would require a specific justification by reference to the purposes.
8. A plan should be set out for ensuring the *security* of both the cards and the central register.

In order to ensure compliance with the requirements of points 5, 6 and 7 above, it would probably be essential to institute a rolling system of audit, perhaps on a

[5] This might be a case in which the "analytical framework" could be used, which was proposed by the Performance and Innovation Unit as a system for privacy impact assessment in (2002) their report on privacy and data sharing.

probability sample basis, both of the central register and of the use of the scheme by the public services that access the data most frequently.

If among the reasons for the introduction of the scheme are the fact that the United States may impose requirements upon British citizens to obtain visas, and that the Schengen countries are concerned about ease of movement for criminals between the UK and the mainland members, then there is no reason why the US and Schengen concerns cannot be met within a data protection compliant scheme.

I recognise that of course, a data protection compliant scheme of the kind outlined here would still be rejected by many of those who have criticised or rejected the Home Office proposals. Those who regard any such scheme as violations of liberty, or of a wider or deeper conception of privacy than that which is expressed in European data protection law, and those who distrust all public administration and believe that all data collections as unacceptably intrusive will not be satisfied with it, and I would not expect them to be. I recognise that a wide range of objections on quite other grounds could be brought against such a scheme: some of these issues will be considered in the final section of the paper. However, I believe that a scheme which met these standards could be justified on data protection grounds, and might be justifiable more generally, if and only if it can meet some additional concerns, to do with cost and benefit, and wider social implications. It is to these issues that the present paper now turns.

Part III: Costs

ECIF offers only very rough cost estimates. The problem is not that the main body of the paper contains so many options: had that been the only problem, a menu could have been presented. Rather, the issue is the fact that so many of the costs are uncertain. The government acknowledges the history of cost overruns in public service information technology projects and recognises that this makes it difficult to be precise in the estimates. Moreover, since the benefits are even more uncertain and hard to quantify, even rough cost-benefit comparisons, let alone rigorous cost-benefit analysis, is almost impossible.

Paper, magnetic strip, simple smart card or multifunctional card scheme?

ECIF leaves it open just which kind of physical token might be used. However, the Home Office cannot really be very open-minded, for many of the features of the scheme about which ECIF provides most detail cannot be implemented with, for example, a paper card: with paper cards, the manual online data entry and checking would be slow, prone to entry error, and crude. Moreover, since paper cards would display all the information they hold on the face of the card, they are much more prone to violate the data protection principle that no excessive or irrelevant information should be processed. While magnetic stripe cards allow easier online processing, and citizens are familiar with them from many years of using bank cards, they will not support any of the biometric features that the Home Office clearly regards with some enthusiasm as important for checking identity. The information that can be held in a magnetic stripe card is very limited indeed, and generally such systems are designed to reveal everything recorded in the magnetic stripe on each occasion the card is read. This makes them much less privacy-friendly than smart card options. More complex multifunctional smart cards are probably necessary for many of the things that ECIF envisages. If the system is to support card validation, unique identifier, selective access online to the data on the central register limited according to the requirements of the service using the card reader device, biometric identification of the card holder, a simple memory-only card with a single directory would not be a good solution. The data protection imperative for access to data conditional on the specific and differing purposes of different services in practice requires a multifunctional, processing and not only memory smart card. This pushes the costs of scheme toward the upper end of the ECIF estimates.

Costs of a data protection compliant scheme

A scheme that did comply with data protection principles and that was constructed on the basis suggested in the previous section would almost certainly be more expensive to design, implement and administer than the one envisaged in ECIF.

For a compliant scheme would be much more complex. The levels of expenditure on security might well be higher than for the presently proposed scheme. It would require much more specification of data standards, and many more restrictions on in-flows and out-flows of data into and out of the central register. The much more extensive set of specifications and controls on which data might be disclosed to whom in what circumstances would require higher expenditure on both the design and the perhaps also operation of the underlying information systems, and it might require more processing power and memory in the chip in the card than might be possible for a simpler but non-compliant scheme.

To ensure that a scheme remains data protection compliant, it will also be necessary to provide adequate and ongoing staff training and a rolling programme of audit. These costs should be included in the overall estimates.

Costs of card reader infrastructure: interoperability imperatives and disclosures

ECIF gives only very rough costs for the infrastructure. For example, and very surprisingly, there is no discussion whatsoever of card reader devices and their costs. However, reader devices are presumably going to be required within the public sector at every reception desk for every service providing agency. In many services, many individual professionals or case workers will need one of their own. For example, if part of the aim is to restrict certain types of NHS non-emergency primary and secondary care more tightly than perhaps it may be in practice today to those legally resident in the UK, then in addition to the card reader devices at GP and hospital reception desks, many individual paramedics and mobile doctors will need to carry reader devices with them. If significant numbers of people did choose to have emergency health information accessible in or through the card, then every ambulance would have to carry one. Beyond the NHS, many field social workers, all police officers, many probation officers, and many outreach workers might need one. This represents a very significant expenditure. ECIF seems to assume that this expenditure can be wrapped up in the coarse estimate of 25% of set-up costs for IT infrastructure. However, this seems very low (Schulman's 2002 argument suggests that many of the implementation costs are under-estimated).

Moreover, the more demanding the biometric system, the more expensive the card reader device required. The discussion in Annex 5 of ECIF (paragraphs 18 and 19) is confined to a brief presentation of the costs of the basic equipment. This does not seem to me to be adequate, given the importance from a data protection perspective of the accuracy of the data system. For all biometric systems, like all diagnosis and checking systems, generate some levels of false positive and false negative results. It must be a major priority to reduce these, and this will be costly. There is often a trade-off in designing any system between the minimisation of false positives and the minimisation of false negatives: a system designed to achieve one of these objectives is typically likely to run higher risks of the other. The government ought to set out exactly what thresholds of false positive and false negative results it would regard as acceptable for the different principal uses envisaged for the EnC. Only then is it possible to make judgments about whether the estimates of costs set out here are reasonable. For example, if biometric checks are used in checking entitlement for services for basic necessities – such as Income Support – then it could be argued that the costs to the data subject (who, if claiming Income Support, is likely to be very poor indeed), of a false negative result are much more severe than the costs of a false negative result for a person seeking to board an scheduled flight at an airport. Wrongful denial of welfare benefits to the very poor is a greater hardship than wrongful denial of boarding for a flight for almost anyone, whatever the emergency for which they are travelling.

A number of services are already introducing smart card schemes of their own. It is quite possible, for example, that the NHS will move toward a national smart card system for the electronic health record. A variety of cards are now in use in the education field that could be the basis of national schemes. The Connexions system already uses a card. There will be administrative pressures to avoid having the reception desks for public services littered with a plethora of different card reader devices for all these different public service cards; there will be some technical pressures for interoperability between the systems; finally, there will no doubt be political and administrative pressure for interoperability in order to extend data sharing between these schemes. Card reader devices that can read a variety of smart cards are of course typically significantly more expensive per unit than those which can read only one type.

The reader device problem is of critical importance from a data protection perspective too, for it matters that reader devices are so designed that they can access only the minimal set of information required for authorisation for each particular

service. In a data protection compliant scheme, therefore, the reader devices in use for, say, local authority social services departments will be very differently configured and programmed by the computers they service than will those on sale to commercial retailers whose legitimate need is only to have proof of age.

Costs of notification and other administration costs

ECIF is almost completely silent about the notification to citizens that is required by data protection law, for example under subject access and fair processing requirements. The administration of notifications, and the administration of informed consent where that is required, will represent a significant cost to many public services.

Project management, timetable and frontline costs

Weaknesses in project management, and especially on the client-side, have been identified for many years as explaining a significant part of the problems that British government agencies and departments have had in the implementation of major information technology projects. ECIF itself acknowledges that there is a well documented history of cost overruns, delays, technical problems and even failures.

The EnC would be a truly vast project. The scale of the population register alone is enormous. In Annex 5, paragraph 8, ECIF sets the goal of 67.5 million records on the register and 314 million cards issued or reissued by the end of the first ten years of operation. The complexity of the challenge from design through to implementation, and even of the interfaces between the register and of the enormous network of card reader devices and biometric recording devices, and with all the other public sector and private sector data systems, is much greater than has ever been attempted in the UK on a national level previously. Many of the technologies required – such as the biometric systems – have only been trialed on systems that process tens of thousands of people (e.g. asylum seekers and frequent flyers at major airports), not on systems for tens of millions of people. Quality management for these systems will be complex and crucial, for biometric systems raise problems of data quality and also of the speed of recording, as well as the quality of the experience. The aspiration stated in ECIF (paragraph 5.37 and Annex 5, paragraph 2) that the systems design for a project of this scale and also the hardware and software installation could be undertaken and completed in a period of just three years from letting the contract to the "go live" date seems to me to unrealistically ambitious. A number of pilots and trials on a smaller scale, using alternative options for the various elements of the system will certainly be necessary before it would be at all sensible to commit resources to the full national project implementation.

Annex 5 and the shorter summary of its argument in Chapter 5 are both written very much from the point of view of the centre. Most of the cost and timetable estimates have been conceived on the basis of costing the hardware and software required at the centre, and in hiring staff for the administration of the central processing. It is this weakness that probably lies behind the failure to recognise the implications of the requirement for the card reader infrastructure to be installed in thousands of public services. It is also vital to recognise that in every local authority department, every Primary Care Trust, every NHS Trust, in every local or regional network of the Employment Service, the Benefits Agency and many other central government service-provision bodies, there will have to be investment in project management for the installation of the data systems and the card reader devices, for managing the interfaces with existing systems and with other concurrent information technology investment, for staff training in the use and operation of the new system, in troubleshooting and in providing helpdesk support (a project as big as this one will need many tens and perhaps hundreds of different helpdesk functions for every level and stage). Adequate security for the flow of information between sites and online helpdesk functions will be

of great importance from a data protection perspective, because of the quantity of personal information that could flow from sites to the companies providing helpdesk functions. Helpdesk systems and user groups will have to be maintained over many years, and certainly long after "go live", to deal with bugs, upgrades, recovery from system problems and so on.

There would be large project costs of implementation in categories that ECIF does not seem to recognise, in the involvement of staff who will use the systems in local authorities, NHS bodies, the Employment Service, the Benefits Agency, police forces, etc., in the design of all the interfaces, data displays and reports. Many thousands of staff across the public services will have to be freed up on a part time basis to work on this, probably over periods of two to three years.

The project management system will have to be large, complex and tightly coupled, for the project to be delivered. Client-side project management must work seamlessly to link hardware and software, biometric systems, helpdesk functions, data load and data entry and all the local and frontline implementations of card reader systems. This will all require sophisticated communication systems between the elements of the project management system.

It would be a mistake to suggest that deep cuts in the client-side project management requirement can be safely made, not only for reasons of general project management principles, but more specifically because the goals of the EnC scheme in particular could be compromised without adequate project management. For example, ECIF sets goals for greater accuracy than other government databases and for early contributions to the reduction in identity fraud and illegal working that would not be achieved if the local implementation is not tightly overseen and well linked into other information systems.

Finally, ECIF does not discuss the risk management issues in any detail. Developing risk management plans for the wide range of contingencies that can be foreseen on a project of this scale is itself the work of several months. Secondly, it is a serious and important question of public policy whether an asset of the scale, administrative importance, commercial sensitivity and political controversiality of the central population register would be insurable in the commercial insurance market at premia that the government would be able and prepared to afford. Apart from insurance for the costs of reconstruction against accidental damage to the systems, in the present climate, it will be important to consider the question of whether the system can be insured against damage from terrorist attack, for the central population register could readily become a target for terrorist groups looking for ways to cause serious damage to the UK. A successful attack on the central system would be at once highly newsworthy, affect many people's daily lives, disrupt government business, affect other security systems that would come to depend on the system, and require large scale expenditure to rebuild. Premia for insurance against terrorist attack have, of course, risen sharply since 11th September 2001, and may rise again.

ECIF does not present any analysis of the lessons from other countries about project management and implementation. There is a short review of the nature of the identity card schemes in selected other countries, but no comparative review of costs, data systems integration, project management challenges and lessons. While there is much to learn on technical matters and on project management design from the experience of the roll-out of identity card systems in Singapore and in some continental European cities and small countries, there are few examples of the construction, from a base like that of the British DVLA and Passport Agency only, of a population register for more than 60 million people in ten years, with the issue of several hundreds of millions of smart cards in a short period, all using modern biometric systems.

In the decision to add a crude 50% to the set-up costs for unspecified contingencies (Annex 5, paragraph 15), ECIF seems to acknowledge implicitly that the basic cost estimates, and presumably therefore timetable estimates too, may well be very significantly under-estimated. The fact that the authors of the consultation paper did not feel able to do better than simply to add a round 50% to the cost estimates suggests both that they have limited confidence in their own figures and that they have few ideas at this stage about how to make them at once more robust against the range of contingencies but also more precise.

In my view, the figure 50% of the already identified set-up costs is too low by an order of magnitude to represent the true costs of project management, risk management and implementation costs of a system as vast as the one proposed in ECIF.

This will all have to be paid for. Presumably this will require the augmentation of the budgets of local authorities, NHS bodies, central government agencies etc. Because of the great range of different local authority services that will either be expected to use, need to use or may want to use the card for dealing with service users, and because of the complexity of the inter-departmental data systems management challenges (taking proper account of data protection restrictions on the flow of personal information between functions with different purposes), some of the most complex and costly project management challenges will be experienced there. In local government, either the EnC programme will have to be funded from the centre through a change in the formulae for the annual settlement – a change that would probably have to last for the whole of the decade or more as the system was put in place and bedded down – or else by allowing Council Tax levels to rise without local authorities' facing financial penalties. The second strategy runs significant political risks for central government, for local authorities could choose to blame central government for local tax increases in ways that might prove electorally damaging. The prospect of campaigns against "an identity card tax rise" must be a matter of concern, especially in the light of the fact that citizens will pay an individual fee at the point of application for registration in any case. Politicians would do well in this context to remember the protests against the Community Charge at the end of the 1980s. On the other hand, however, it may be both financially and politically difficult for the centre to shoulder the whole burden of the costs of local and frontline agencies' implementation and consequential systems adaptation.

There have been a series of embarrassing public sector information technology delays, cost overruns, failures in – for example – the Horizon / Pathway system, the Swanwick air traffic control system, the Passport Agency, the Child Support Agency, the Criminal Records Bureau and the Immigration and Nationality department as well as elsewhere. Most of these projects have been much simpler than the EnC system because they have not required very extensive inter-agency coordination. None, even when the overruns are taken into account, have cost as much as the EnC system as whole would cost. Politically, the prospect of a failure on a project of this public profile and privacy sensitivity would be deeply damaging. A failure or a major cost overrun and delay on this project would make it extremely difficult for any government to undertake any large scale project for information systems modernisation in the public sector, perhaps for a generation.

These considerations are not arguments for doing nothing or for rejecting any EnC scheme at all, still less for being resigned to high levels of fraud. However, they do provide very strong reasons for urging that government develop much more detailed, rigorous, robust and credible and genuinely comprehensive assessments of the costs and of the various different stages of the project, and show that detailed lessons have been learned from the implementation challenges faced in previous UK government information systems projects as well as from the experience of other countries of similar size population.

How worthwhile is the proposed scheme?

The ECIF estimate is that for a sophisticated smart card scheme, the cost would be £3.2bn. This has been criticised as too low in several quarters, for reasons that are partly acknowledged in the document – the history of cost overruns, the sheer scale of the project, the variety of costs at the local and frontline levels that have not been adequately estimated and the administrative challenge of managing the scheme.

In my view too, for the reasons given above, the cost calculations presented in Annex 5 of ECIF are very significantly under-estimated, even for the scheme that the Home Office is proposing. In respect of the complexity of at least the design and implementation and possibly the running costs for the underlying information system, they are under-estimated for a scheme that would be data protection compliant. The consultation paper also estimates that around £1.3bn could be raised from charges. Therefore, a large part of the justification of the scheme as worthwhile has to rest on the savings from reduced identity fraud, reduced levels of identity checking using instruments other than the EnC (which estimates may well also prove too optimistic, if either the accuracy or the security of the EnC system are less than convincing to companies and public authorities) and so on. Of this, only a fraction would be recouped to the Exchequer in taxation, and the absolute level of that amount would depend in part of the levels of economic activity in the country as a whole over the period of the first ten to thirteen years of the EnC scheme.

In my view, once all the cost pressures are taken into account, it must be considered doubtful that the scheme will prove to be worthwhile, even in its present form which is not, in my view, data protection compliant, and even more so when that is corrected (in any case, it would be absurd to argue that a legally doubtful scheme should be considered more seriously because it is cheaper).

Part IV: Public perceptions

I have been asked to consider whether my own previous research (6, 2002) on public attitudes to privacy and data sharing, commissioned by the Performance and Innovation Unit to accompany the 2002 report on that subject, might cast any light on how sections of the British public might view the disclosures inherent in the EnC scheme. That research consisted in a series of focus groups with people from client groups that are or may be affected by areas of data sharing. It was not specifically about identity or entitlement cards, and so no inferences can be drawn from it about people's attitudes to the particular token that the card constitutes. The general finding from that research is that most people perceive many privacy risks in data sharing and attach significant negative emotion to them, but perceive few benefits and when prompted to do so, attach little positive emotion to them. This suggests that we have every reason to be very cautious about the extent of data sharing that any EnC scheme would support.

More specifically, I have been asked to consider how far the fact that the scheme is described as an "entitlement" rather than an "identity" card would tend to support ways of framing the privacy risks other than those of "indignity" and "lack of control" which were identified in the analysis of the focus group data from that research.

Again, because the subject of the research was not the physical token of a card, one must be cautious about extending the interpretation of the findings to the present context. The most that can be done is to consider the logic of the theoretical argument explaining the framing, and to consider how the facts of the EnC, if they were correctly understood by people with those framing, might be received.

The "indignity" frame (of which the "out of control" frame is a more moderate form) for privacy risk in respect of data sharing were defined in 6 (2002) as characterised by the view that arbitrary surveillance and accessing and sharing of personal data is almost ubiquitous, demeaning but largely inevitable. Those who view privacy issues in this way tend to waver between powerless resentment and resignation.

One argument might be that describing the card as an entitlement card, and stressing the ways in which its use represents greater convenience in accessing goods and services to which one is entitled, might go some way to combat the "indignity" and "out of control" frames.

However, the logic of the argument presented in 6 (2002) suggests great caution about this, because frames for the perception of risks and benefits are not simply produced, changed or switched in response to the presentation of labels or even arguments. For labels and arguments are features of what was there called the secondary situation – that is to say, the short term conversational situation. The major determinant of human social framing of risk is argued to be the primary situation in social organisation – that is, the degree of actually experienced autonomy, regulation, bonds to others, and so on (6, 2003 forthcoming).

The EnC does not in and of itself bring any new entitlements, nor does it transform the experience of those who hold it of their encounters with large organisations or of particular services. Those who are asked to produce the card most often will be those using services which are suspected to be at greatest risk of exploitation by fraudsters. This will generally mean services for the least advantaged, who as a group may have fewer incentives than others not to defraud since their chances of improving their financial situation by legal means may be more limited. The fact of greater surveillance, of which the experience of presenting the card will be part, will have some effect of reinforcing the type of heavily regulated, weakly bonded primary situation that tends to lead to "out of control" and "indignity" frames for risks.

In the same way, the description of the scheme as "universal" rather than "compulsory" seems, if the logic of the theoretical argument presented in 6 (2002) is accepted, to be unlikely in itself to change perceptions very much. Although universality

stresses communality and solidarity, the actual experience of using the card will be one of being scrutinised individually. In any case, registration for and possession of the card will be compulsory: in practice, it will be difficult in practice for many people *not* to carry their EnC with them at all times.

It is known that significant majorities of the public do express in principle support for identity cards, when asked in large scale quantitative surveys. However, questions administered in such surveys cannot, by their very nature, provide respondents with extensive information on the nature of the scheme, or the particular privacy and information risks that it might present and how people might weigh benefits and risks. As more information becomes available to people about the full range of concerns and about the modesty of even the government's claims about the benefits, it may well be that public attitudes may shift. While the dramatic shifts reported in the 1987 campaign against the proposed Australia card (Davies, 1996) may or may not be replicated in the UK, it would at any rate be unwise to assume that the majority support in principle will be robust in the face of additional information, even if there were no pressure group campaigns against the card.

However, it is also possible that a scheme that would be genuinely data protection compliant in these ways might attract greater support, because its compliance with privacy principles should make it easier to explain and justify to the public, and make it easier to allay fears about particular privacy risks.

Part V: Wider social issues

The proposal for an EnC is one that raises many issues that range far beyond data protection or even privacy. Although these have generally been debated as if they were all arguments for or against the principle of any form of compulsory general identity token, some of them are really better considered as challenges that will be raised in any society in which the demand for individual identification has become generalised and integrated into the way in which people deal with large organisations (Lyon, 2001).

Compulsion

The ECIF proposal is for a scheme in which registration for and possession of the card will be both compulsory and charged for. Compulsion in almost any respect is something that societies that regard themselves as liberal democracies have traditionally engaged in only with special justification, for there has often been felt to be a general presumption in favour of liberty that must be overcome on a case-by-base basis using arguments of certain prescribed kinds. In all societies, there are *generalised* obligations such as the duties to obey the laws that are legitimately in force, not to seek to overthrow the legitimately constituted government by unconstitutional means, to pay taxes, to respect the constitutional rights of other citizens, and so on. These generalised obligations form a minimum set, which are thought to require no special justification, for these obligations are the ones that actually constitute liberty, for without their performance, no citizen's freedoms of speech, thought, assembly, property and religion can be secure against other citizens. Going beyond this minimum set to include more specific duties is what requires specific justification. Legally enforceable, sanctioned compulsion for activities or institutions that might be argued to be obligations or duties of citizens is justified variously (c.f. Janoski, 1998, ch.3). The following are some of the main justifications used:

a. *emergency*: The particular proposed obligations are an unavoidable response to an emergency, as in the case of conscription into the armed forces during wars in which the homeland is directly threatened with invasion and annexation and when the regular professional military forces will be inadequate to defend the integrity of the state.[6]
b. *citizenship*: The particular proposed obligations are intrinsic to citizenship, because performance of the obligation is regarded as internally related to the rights of citizenship (a) because the performance of the duty is the condition upon which rights are granted as a direct *quid pro quo* (as in those countries that make some form of national military service compulsory for all young adults for a period of time following the completion of education) or (b) because the obligation is to carry out something which is part of the participatory character of what citizenship is (as in the case of those countries that make voting in national elections compulsory).
c. *basic goods for others*: The particular proposed obligations are necessary for the promotion of very fundamental and basic goods for others. Most societies make it

[6] I would reject the argument advanced by Etzioni in his (1999) book on privacy, according to which privacy can legitimately be restricted, and – implicitly – citizens have obligations that would override any claims they might have to privacy, wherever there is a "well-documented and macroscopic threat to the public good", where no alternative is found available to the limiting of privacy, and where due effort has been taken to minimise the intrusion (ch.1). Despite the sensible safeguards, this seems to go far too far in justifying citizens' special obligations, because in effect it expands the category of emergency duties to the point that almost any public good that is not secure could justify obligations. This seems not only unnecessary but too big a departure from the liberal tradition to be acceptable to many people.

compulsory for parents to ensure that their children are educated either in formal schools or through some home education of approved equivalent standard, on the grounds both that the education of each benefits all through prosperity and competence and that the rights of children to be educated require these correlative duties upon parents. In the same way, some societies (e.g., France, although not, so far, the UK) make it compulsory for parents to ensure that their children receive certain vaccinations before they can be permitted to enter school, where education is also compulsory and support for education at home very limited.

d. *protection of basic social institutions*: The particular proposed obligations are essential where certain basic social institutions are deemed socially very important to the public good but which also rest upon the performance of private obligations. Thus, many societies enforce the payment of maintenance for the upbringing of children upon parents who no longer live with those children after the breakdown of the relationship between the parents. Singapore goes further and imposes legally enforceable obligations upon adult children for the maintenance of dependent elderly parents.
e. *limiting moral hazard in basic collective services*: The particular proposed obligations are essential for the limitation of moral hazard in the case of certain very basic collectively financed safety net services. Thus, most societies require those in receipt of support while unemployed to look for work and accept reasonable work when it becomes available, on the ground that to continue to secure resources from taxpayers beyond necessity is imposing an unfair burden on those taxpayers.
f. *paternalism*: Compulsion and enforcement for certain duties can be justified on the basis of the good to the individual who must perform the obligation, provided certain rather strict conditions are met (VanDeVeer, 1986; 6, 2000). For example, prohibitions on the use of heroin and cocaine are sometimes justified on this basis. Some of those who argue for compulsion of individuals to take out a second pension or for other types of savings would use this kind of argument.

Some putative obligations are justified by appeal to combinations of these things. For example, the compulsion upon owners of vehicles to ensure that they are insured at least for any damage that they may cause to others usually rests on a combination of a basic goods for others argument with some appeal to the limitation of moral hazard where for uninsured drivers who cause accidents the taxpayer would have to pick up the bill, for example, for health care costs, and may also appeal to the idea that the avoidance of torts such as uncompensated damage to others is a kind of basic social institution in respect of its importance not unlike that of the duties that parents owe to children. Some people combine paternalistic with moral hazard limitation justifications for obligations upon people receiving public unemployment benefit to seek and accept work (famously, Mead 1986). There may be other types of justifications for citizens obligations, but I believe that they will play a minor and specialised role. In any case, these are the ones that are mainly appealed to.

Which of these might be used to justify the compulsion proposed for the EnC?

ECIF itself rules out the use of emergency justifications, for it makes clear that the government does not seek to use national security considerations to justify the introduction of the scheme, and indeed this is strongly implied by the government's welcome decision not to seek an exemption for the from the Data Protection Act's provisions.

It is hard to see that an EnC protects social institutions that are as elementary in their forms as the duties that bind parents to meet basic needs of their children. If the

institution that an EnC would protect is that by which people identify themselves at the point of application for services, then, whatever its importance, it cannot seriously be claimed that this is a fundamental institution in the same sense at all.

The justification about basic goods for others seems to have limited grip in the case of the EnC, because the card system does not really provide any goods or services itself, let alone very basic ones like basic education or vaccination of children. That it might conduce indirectly to the provision of such goods is an argument that seems to stretch the idea too far: for without a measure of direct causal linkage, the argument is rendered worthless.

Similarly, the moral hazard issue does not really seem to be very compelling, for although there may be costs arising from the failure of citizens to perform the obligation of registering for and obtaining an EnC, these costs are not of the order or the specificity of those which flow through collectively financed income maintenance and health care, but instead they are rather diffuse, impossible to calculate but probably in most cases modest. Since the government admits that identity fraud in the context of collectively financed services is a problem which is much smaller in dimensions than the problem of fraud by misrepresentation of ones' circumstances, it seems implausible to place great weight on an argument that the EnC would enable the reduction of moral hazard in a variety of different services.

Again, because the EnC itself provides no benefits in and of itself, it is hard to see that paternalistic arguments can be used. The card is intended to produce the benefits of access to services and control of certain kinds of illegality. However, the thing that directly brings the benefit of the services to the individual performing the duty is the fact of entitlement, not the card. Therefore, paternalistic arguments seem inappropriate here. In any case, it would be very difficult to argue that the EnC would meet the other very special conditions in which paternalistic arguments can yield a basis for legally enforceable obligations on all citizens.

This leaves only one type of justification for compulsion remaining, which is the idea that the EnC might be something that is intrinsic to citizenship, either by conditionality or by intrinsicality.

ECIF does not really set out a detailed statement from first principles of the justification upon which the government seeks to rely. However, as I read the consultation paper, it seems plausible that something of this kind might be implicit in it, or at least consistent with the government's argument. It cannot be *exactly* this justification since the EnC is compulsory for UK residents and not only for citizens. However, some kind of *quid pro quo* argument seems to be suggested in the fact that the Home Office proposes in ECIF that the main sanction for non-performance of the duty would be denial of services, where for particular services it was decided that the EnC would be the sole means of acceptable identification. Certainly, a duty to register for and possess and EnC could not be a duty of the same degree of importance as that which countries using national service attach to that institution, and consequently, the penalties for non-performance would be correspondingly milder. The occasional suggestions from ministers, and more overtly from backbench MPs such as Dr Nick Palmer (presentation to public meeting 11 December 2002) that the fact of the universal obligation to register would or at least should in itself be understood as a badge of common or shared identity or even, a wider sense than the legal one, of citizenship (registration for and possession of the card will be compulsory for residents who are not British citizens), also reinforces the thought that perhaps some kind of intrinsic citizenship justification is intended, which might be analogous to the duty in some countries to vote.

How strong is this justification in the present case? Reconstructing the argument in full, it might go something like the following, which I shall call "Justification 'R'":

Justification "R"

1. *Premise 1*: For at least some non-trivial services, it is reasonable to draw a distinction in the extent of entitlement or in the appropriate manner of treatment between persons lawfully resident in a country (from now on, "residents", *tout court*) and persons who are not.
2. *Practical consequence of (1)*: In order to secure entitlements or appropriate treatment in those services, residents have a duty to put themselves in a position such that should they ever be reasonably required (e.g., not in repetition constituting harassment, not for trivial cause) by public officials to demonstrate that they are not illegal immigrants or working illegally, or to demonstrate that they are a person entitled to the services that they have in each case applied for, they are able to do so in ways and to a standard that will be convincing to a reasonable public official.
3. *Premise 3*: The duty in (2) above (a) is one that, in respect of demonstrating that one is legally resident in the country, is intrinsic to the concept of legal residence and (b) is one, the performance of which is reasonably held as a condition for receiving (or continuing to receive) public services claimed.
4. *Rule against arbitrariness*: It would be wrong in principle for there to be unacceptable variation, at least *within* any particular service, in what the reasonable official will accept, by way of identification. (There may be of course be variations *between* services, where they require quite different information to establish entitlement.) Therefore, there should be a centrally set standard of identification, at least for each service separately, and, if possible, for clusters of services which have common requirements.
5. *Consequence of (4)*: Having set those standards for residents, government must then provide them with the means of fulfilling them.
6. *Implementation of (5)*: The most effective means will be some kind of portable token held by residents, linked to a central register.
7. *Premise 4*: Centrally set standards of identification will only work effectively, at least in respect of demonstrating that one's residence or working in the country is legal, if possession of the means of fulfilling the duty is compulsory for all residents and if the register of legal residents in the country is a complete one, without exceptions.
8. *Conclusion*: Therefore, *all other things being equal*, registration and possession of the token should be compulsory for all residents.

Although Justification R does not appear in ECIF, I believe that it is the best argument – at any rate the best that I can reconstruct – available to the government to justify compulsion for a scheme of this kind.

Subject to a discussion below of the very important caveat that all other things that would have to be equal, as far as I can tell, Justification R is a valid argument, in the sense that if the premises are granted, then the conclusion follows. To defeat Justification R, it is necessary therefore to show either that all other things are not equal, or else that

(~1). There are no significant services in which it is reasonable to treat those legally resident in a country differently from those who are not.
(~2) Residents have no obligation to identify themselves to demonstrate their legal residence or valid entitlement, when reasonably asked.
(~3a). Identification of legal residents as such, even when reasonably demanded, is not intrinsic to what it is to be a resident in a country.

(~3b). Identification is not reasonably a condition for receipt of services.
(~7). Standards of identification can work, even in the context of demonstrating legal residence, without universal compulsion.

Proposition (~1) seems to me impossible to accept. It would mean either an indefinite extension of entitlements at the taxpayer's expense, or else, in order to protect the public purse, the abolition of many entitlements and services now thought fundamental to a civilised state.

It might also be argued that we ought to be clear, but perhaps are not clear in practice or perhaps even in law, for just which services, the kind of discrimination identified in (1) is appropriate. To some degree, and for services, this may be true: it is said that there is, in practice, uncertainty and variation in the provision of NHS services. However, for some services and some ways of treating people, there is reasonable clarity. For example, for the issue of treatment (it could hardly be called a service!) of arrest for violation of the immigration laws, there seems to be no lack of clarity. Again, for many welfare benefits programmes, there is no lack of clarity in the regulations about the legal status required for entitlement. For justification R to go through, it is not necessary that there be complete clarity for all services, only that there should be clarity for *some* services. If this is the case, then lack of clarity elsewhere is an argument for undertaking some collective deliberation about just who is and should be entitled to what services and treatment, and for settling the question, not an argument for rejecting compulsion in identification for those services where there is clarity.

It might argued that the real point of this argument is to make the case for delaying giving government these powers until such time as there is clarity about just which services and treatments discrimination on the basis of legal residence is relevant and about which it is not. It might said that "we ought not to give government the boots that will allow it to march off miles in the wrong direction, until we have sorted out which directions are right and wrong" (Stuart White, personal communication, 2003). The problem with this variant of the argument is that it is not obvious just how we might create such clarity, over what timescale, or what level of consensus among whom would be required for this argument's criterion to be met. It is hardly reasonable as a general argument to ask governments to delay policy making until political philosophers achieve consensus; consensus among political parties is equally unlikely.

If premise (1) is accepted, then (2) seems to follow as a matter of practicality. For if it is legitimate for some non-trivial services to draw distinctions between legal residents and others, then some means must be found of doing that. In practice, that must mean asking people to be prepared when asked reasonable to produce some information sufficient to enable the service provider to determine their status.

In the same way, (~3a) seems to me to difficult to sustain as a matter of practicality. While revealing the individual's name at the point of checking may be excessive for purpose, the fact of checking for entitlement at all is not. If premise (1) is accepted that the status of legal resident legitimately matters for determining entitlement to services and determining for how one is treated, then being able to demonstrate one's status in respect of that distinction must be part of what it means in practice to have that status.

(~3b) raises the challenge, therefore, of whether, outside the context of demonstrating that one is not an illegal immigrant, identification is reasonably a condition for services. I have already argued that if by identification, we mean the revealing of one's name, this will not stand as a general claim, for there are contexts in which it is not necessary. However, even accepting that what is necessary for demonstrating that one is a person who is entitled to a certain treatment will vary between services, one could devise a data protection compliant scheme in which the token could only reveal that which was contingently required in each context. If the

concept of identification in premise (3) is read as meaning authorisation in the way suggested in the previous part of this paper, then (3) may be acceptable and (~3b) would fail.

Proposition (~7) also seems unacceptable, because when the register is not comprehensive, it is hard to see how government can say that someone's absence from it is conclusive evidence that they are not legally resident in the UK.

Therefore, it seems to me that the remaining way in which someone could attack Justification R is to attack the argument that all other things are equal. What other things have to be equal before the otherwise valid argument R would go through?

Presumably, Justification R cannot support just *any* kind of scheme for a compulsory token.

Premise (1) itself suggests one fundamental issue. It reminds us that discrimination in entitlement to services between those who are legally resident and those who are must be limited in practice only to those services and those aspects of general treatment in which it is justified, fair and constitutionally acceptable, and there must be adequate redress for complaints that these rules have been violated in particular cases. It is far beyond the scope of the present paper to discuss whether the UK meets this condition. In any case, if it does not, then, from first principles, this would be an argument for rectifying the unjust discrimination in services and treatment, not for rejecting compulsion in identification.

Therefore, important as this is, I do not treat as a side-constraint, the violation of which would defeat Justification R.

I have already argued that at least the following three types of side-constraint would have to be met.

First, for example, it cannot be read as overriding considerations of data protection that will strike down some schemes, and which, I have argued above, suggest that the government's present proposals are inadequate.

Secondly, the sanctions must be proportionate to the real damage that non-performance represents or threatens. Since the government is not, at least in ECIF, proposing additional sanctions over and above denial of services where and only where a resident cannot find adequate alternative means of demonstrating authorisation (for services) or identification (for demonstrating their right to reside), in my view, this condition probably is met.

Thirdly, the scheme must surely be proportionate in its costs, its intrusiveness, its risks, its management, to the problems that it is intended to solve. This seems, I have argued above, to be a significant problem with the EnC scheme as proposed, because the costs are likely to be much higher than the government estimates, and may indeed be disproportionate.

On balance, therefore, I consider that the central problem with justifying compulsion for registration and possession of the card is not that no argument is available, nor that the argument is invalid, nor that its core premises are weak. Rather, the problem is that the scheme actually proposed in ECIF does not meet the side-conditions of compliance with data protection and of proportionality of cost to benefit that any such scheme must meet.

If this assessment of Justification R is accepted, then some of the liberty concerns about identity card schemes might be allayed. However, that is certainly not to say that all the liberty concerns would disappear if a scheme could be produced which met the side-constraints. For there remain serious liberty concerns about the manner of *implementation* of schemes of this kind, and about the possibility of their *extension by stealth*. Specifically, we have every reason on liberty grounds to want to be vigilant about the manner in which the card is demanded and the dangers of unreasonable demands, about the possibility that the range of types of information demanded for the

central register might grow over time, the possibility of the erosion of the principle that in many contexts a variety of types of information ought not to be considered necessary to demonstrate entitlement, the possibility that people might be unreasonably denied the opportunity to use other but equivalently informative tokens to demonstrate authorisation, and about the possibility that at some stage there might be attempts to impose disproportionate sanctions.

Slippery slope arguments

A number of slippery slope arguments against the EnC scheme are often put by opponents of schemes of this kind. Most argue that no scheme should be introduced that would grant powers to ministers or to officials that could be abused by illiberal and authoritarian governments.

The problem with arguments of this form is that there are many quite ordinary and rather uncontroversial powers routinely granted to ministers and public officials that could be abused, and at some point in history have somewhere been abused by authoritarian régimes. Powers of arrest for very ordinary crimes have been abused; regulatory powers for really very trivial things such as dog licences have been abused to harass people. A genuinely authoritarian régime will use almost any powers and indeed act quite beyond its powers. The slippery slope argument would disable civil government, to strip it of literally everything that could be abused by a government looking for ways to exercise arbitrary or intrusive power.

Moreover, all slippery slope arguments face the problem of showing that there are no "notches" on the slope, no proper and sensible ways of drawing lines between the acceptable and unacceptable within an area of governmental power (Govier, 1982; Walton, 1992). But in the present case, there seem to be a number of places in which notches can be set into potential slippery slopes. For example, three side-constraints were identified in the last sub-section: the scheme must meet the requirements of the data protection principles, sanctions for non-compliance must be proportionate to the real weight of the misdemeanour of not registering, and the costs, risks, intrusiveness and management must be proportionate to the problem it is intended to solve; I have argued that the first and third of those standards are not met by the Home Office's present proposals. There seems no reason why in principle these constraints could not be entrenched in some way. Perhaps they could be included in the enabling primary legislation for the scheme in order to provide the basis for challenge and redress through the courts if the scheme brought forward could be shown to violate any one of them.

Two other general slippery slope arguments should be considered briefly here. The first claims that the introduction and institutionalisation of a compulsory system of identification will in and of itself gradually lead to deeper discrimination between legal residents and others. In particular, the argument runs, the symbolic effect of the availability of the token will work in a way not wholly unlike the duty on Jews in Nazi Germany to display the star of David: it will function as a visible mark around which stigma against, in this case, those who are not legally resident will be organised, and over time, its actual use will lead to a situation in which discrimination will be extended unjustly to areas in which it is inappropriate.

There is no denying that this is a real practical danger. However, this fact does not suffice to defeat Justification R. Nor does it show that there are no "notches" on the slope. For the danger seems neither irremediable nor intrinsic to the nature of compulsion nor indeed to the nature of identification. The dynamics which produce stigma and unjust extensions of discrimination by a category into fields where it is not justifiable are social ones, that – to the extent that they are real – would no doubt find expression in other ways, if there were no EnC scheme. Moreover, those forces can be addressed, but can surely only be addressed effectively by challenging the unjust aspirations and practices, not by rejecting the identification scheme, if there is

independent justification for that scheme. An EnC – or indeed the inability to get one – is *not* relevantly like the badge of the star of David, for there is and there was no independent justification for requiring that anyone wear a label declaring their ethnic or racial background or status, because there are no services for which discrimination by that category would be justifiable (save with the possible exception of cases of positive discrimination, which is a quite separate argument). The real force of the point behind this argument is to call for closer vigilance against the abuse of powers to demand identification, not least by the Commission for Racial Equality.

A second general slippery slope argument is of a somewhat different character: we might call it a "final straw" argument. The reply to the general slippery slope argument was that any power given to government might be abused, and therefore one cannot use that point to justify denying particular powers to government. This argument would shift from the particular power to making a claim about the total number and extent of the powers of the state. The argument would be that while governments have to be given the means to pursue legitimate public purposes, it may be unwise to give the executive *all* the means that would be required to fulfil those purposes, since one cannot be confident that those governments will not be more likely to abuse their powers, the more powers they have. The claim would be that the loss suffered by citizens from government inefficiency and ineffectiveness due to having too few powers would, on balance and over the long run, be less than the loss that would be the consequence of the abuse. In the present context, the argument would be that adding to EnC to the powers that the executive already has in Britain represents a final straw.

The argument is certainly worth taking seriously, because the total extent of executive powers is a centrally important issue. However, there are several problems with the argument. One is that it still remains arbitrary to reject the EnC as the most recently proposed straw to be added to the pile, if there are reasonable *particular* arguments specifically in its favour. There may well be other powers that could be jettisoned to meet the aspirations behind the argument. A deeper problem with the argument is that it is not clear just what *would* satisfy a proponent of the argument. When *would* a state get the right to a full set of powers required to fulfil legitimate public purposes? Either the proponent of this argument takes the absolute line that no state ever could, just by virtue of being the state, or else they must allow that some set of constitutional provisions on rights and safeguards would suffice. If they take the latter view, then the argument ceases to be one against the EnC at all, but an argument for those safeguards. If, however, they would not permit any state the means to fulfil all the purposes they admit to be legitimate, then a new set of problems emerge. One is that the argument would give states no incentive to improve their practice in respecting citizens rights because they would not thereby gain any legitimacy with which to justify securing powers they need to fulfil legitimate public purposes. But a more fundamental one is that if this absolutist line is taken, then again the argument ceases to be about the EnC and simply becomes one for generalised suspicion or at least vigilance, and it is hard to see how this can always and everywhere trump good particular arguments in favour of particular powers. For a central problem with this line of argument is that it makes no distinction between the relative importance of different powers that a state may need to pursue different legitimate public purposes. If this argument is to weigh against something like the EnC, then surely it would be necessary to add some considerations to the effect that in those cases where identification is reasonably necessary, for example, to control entitlement in order to limit the burden on the taxpayer, this should be considered less important than other powers, and therefore a more appropriate power to deny the state. It is not clear how this is to be done, for there is no obvious metric along which we might weigh all the powers required for legitimate public purposes.

Therefore, it seems to me misguided to try to argue against the principle of schemes of this kind using general slippery slope arguments. A more useful way in which to read these arguments, as they apply to the question of compulsion, is to use them to identify the concerns that can be expressed as side-constraints upon the design, the implementation, the standards, the system of oversight, the system of redress, the principles of evaluation and the consideration for decisions about the continuation of such schemes.

If a slippery slope argument is to be made defensible, then it must be *specific*, not general, and it must show evidence that there are in the particular case no "notches". The concerns about function creep that have been considered above constitute just such a specific argument, in relation to the design of the scheme rather than to the question of compulsion. The argument of that subsection was that there could and should be "notches" in place that would limit function creep, but the Home Office's present proposals do not do so.

Public administration issues

The introduction of the EnC scheme would have significant consequences for public administration quite generally. For even when significant additional resources are not required to handle the checking, it will divert time away from other activities and it will skew the priorities in the first encounter between citizens and services from the ones that presently dominate.

It will have consequences for the nature of the entire e-government programme. For if the scheme is pressed ahead, then there will be pressure for all subsequent information technology initiatives to be designed in ways that are compatible and inter-operable with it. While this may be no bad thing in itself, it will irrevocably commit government to a very particular design of information and communication technologies for public services, and we can expect that almost all future investment will have to designed to work with it. Such a momentous choice must be made on the basis, not only of confidence that the particular EnC scheme is based on the right technology and represents good value for money, but also on the basis of well-grounded confidence that all the consequential investments in e-government should also be based on this technology and that this will represent value for money.

Moreover, there is a real risk that once a contract has been let for the administration of the central register, that contractor will build up sufficient "asset specificities" (Williamson, 1985) or knowledge that cannot be transferred to a competitor, so that in practice it will be very difficult subsequently to award the contract elsewhere subsequently. It has often been claimed by commentators that this is now the position of the global data processing contracting company, EDS, and the British Inland Revenue (e.g., Margetts and Dunleavy, 1995).

Again, neither of these issues is a reason for rejecting any kind of entitlement card scheme. However, they are reasons for wanting to insist on minimising the intrusiveness of the experience of using the card at the point of applying for services, for being careful to keep open as many options as possible about the technological infrastructure, and for designing the contracts from the beginning for the greatest available contestability.

Changing roles of service professionals and public trust

The EnC proposal has implications for the roles of service professionals, and therefore for the processes of public trust in professionals.

Many kinds of professionals who provide public services – social workers, health care clinicians and nurses and paramedics, staff who sell tickets for public transport, specialist workers dealing with drug and alcohol problems – have not hitherto had a role in determining whether individuals are eligible for certain services. Only recently has

the idea had any reinforcement that the NHS should be restricted to those legally resident in the UK (or, for some things, those who are EU citizens) and should exclude foreign visitors from the scope of its care. Many health and personal social services in particular have been focused on need, not least because of the greater importance of meeting needs irrespective of legal residence because of the risks that clients' unmet needs can present to other people. This orientation to need has been important in building public trust in the frontline professionals. Indeed, the relative openness signalled by the lack of detailed checks at the point of contact with services has been part of the implicit bargain between the professions and the public, and part of the account of what universalism has meant for these services. Many professionals in these areas are reluctant to take on a role that they see as "policing" especially in respect of immigration and nationality law. General practitioners, for example, express frustration that when they perform their professional and in many cases legal duty to refer people to hospitals for secondary care, those patients are then checked for their immigration status and denied service, making the position of primary care physician as gatekeeper very difficult indeed to legitimate.

If as a society we have decided that we want to ration services in these ways, then of course, the role of professionals whose job includes the administration of rationing will have to adjust. However, there remain important issues about motivating professionals to work in areas – especially certain areas around ports of entry and inner cities – where they can expect that this kind of thing will take up a lot of their time. In the longer term, there may also be issues about the effect upon public trust of a system that expects the initial encounter between client and professional to be one in which the client has to establish their legal right to be in the country and their eligibility for health care or for basic personal social services, especially in the fields of drug and alcohol work where professional confidentiality about a client's illegal behaviour is essential, or in the field of work around sexually transmitted disease where society has an interest in seeing anyone who is in the UK, legally or otherwise, treated and where confidentiality about the possibility of such condition is vital. As intercontinental travel has become more common, the issue may become increasingly difficult in respect of other communicable diseases which are not stigmatised but which are reasonably feared.

Shared collective identity

Dr Nick Palmer MP has claimed that the fact of universal possession of the physical token of identification will have a positive effect on the sense of shared collective identity among UK residents.

This seems to me rather unlikely. In the first place, shared collective identity rarely in the modern world attaches to the fact of residence. It may attach – often regrettably so – to nationality understood as legal citizenship, to ethnicity, to language, to religion, to political affiliation, to class, or to lifestyle or taste in popular music, but I can think of no case in the recent past in which either the fact of common legal territorial residence or the universal individual possession of a token of evidence of this status was the focus for shared collective identity.

Secondly, the token will be carried in the wallet if it is carried at all. Unlike many badges of a chosen lifestyle, it will not be worn visibly; unlike a language, it is not audible whenever someone speaks or writes something other than a proper name. Therefore, it is unlikely to be something that prompts much recognition.

Stigma and social exclusion

There is an issue of how far the introduction of an EnC might reinforce stigma against people who are not legally resident in the UK and who cannot obtain an EnC, or indeed against people who apply for services but are very visibly denied them on presentation of

their EnC. (Note that there can still be stigma and exclusion of those who are not legally resident even if there is no significant shred of collective identity among those who are legally resident in the country.)

This is a complex issue. Etzioni (1999, 132) is surely right to offer the argument in favour of such schemes that they can help those discriminated against today to establish (in this case) their right of residence and therefore gain access to, for example, employment which they might today be denied purely on the basis of looks or accent, and when today those people may have some difficulty in establishing their right to reside.

However, this does not deal with the problem of how often and in what manner they are expected to produce their card in order to establish their status.

Just where the balance might lie between the reinforcement of xenophobia at the level of attitudes and the provision at least at the margin of a slightly easier practical means by which to demonstrate right of residence, is hard to say. It will depend upon the manner in which popular sentiment – no doubt as informed by the popular press and other media – responds over time to the various pressures of immigration, asylum seeking, and also of skill and of labour shortages that the country might experience, and also – but to a lesser extent – upon the response of certain sections of the public to any efforts undertaken by the authorities and by others to combat xenophobia.

Again, this is best not used as an argument for or against an EnC or any similar scheme. Xenophobia has existed for much longer than identity cards of any kind, and will unfortunately no doubt outlast them. Rather, it is best understood as an important reminder of the kinds of efforts that should be made either in tandem with the introduction of such a scheme or ideally in advance, to combat any tendencies there might be to use it for exclusionary ends. However, it is fair to say that the history of universal identity registration schemes in the twentieth century is one that is associated in many cases with the less than humane treatment of those found not to be legally resident in countries where such schemes have been introduced, not least because such schemes tend to be introduced at times of great social fears about threats presented by foreigners (Stalder and Lyon, 2002). At the very least, alongside such a scheme, there is a case for a review of the humanity of the procedures in use by which persons found to be illegal immigrants or working illegally are treated. In particular, it would be important to provide for regular review of the extent to which the ways in which the scheme is used in practice by a range of public services are compliant with both the letter and the spirit of equal opportunities laws, and in particular with the race relations and disability discrimination legislation.

Distributional issues

There are important ancillary issues about just who will in fact have to make the greatest use of the EnC and for what, and what signals this will send to others about these groups.

It is highly likely that those who will be most often asked to produce the card will be those who are in most frequent contact with government. Certainly, where the card is used to access services that would be regarded as basic necessities, it will be in dealing with public services, and it is likely these will be services in which identification is asked for frequently and repeatedly from the same individual, who often has to make frequent visits to the same agency office to secure their entitlement. Today, in practice this means the poor and those working but on very low incomes. For it is these groups that are most often in contact with authorities responsible for programmes of income maintenance, vocational training and employment counselling, social rented housing, subsidised collective transport, subsidised leisure facilities, free school meals, education welfare services, health visiting services, child support and maintenance, child protection, public support for social care in old age, and so on. They are also more likely

to be found in areas in which the police devote more effort and attention. Again, poor people are much more likely to be in touch with multiple services that might demand production of the card than are the better off.

But for most people who are not on low incomes, contact with these functions is infrequent and after the first occasion of contact, there are few if any subsequent occasions on which proof of age or other characteristics of identity need be given. Most of the better off are likely to need the card little more often than they presently use their driving licence and passport on which the scheme will be based. The private sector – often serving the better-off – may well make use of the card for proof of age, and for identification at the point of application for mortgages, credit, insurance and employment, and (as passports are often now required) for admission to internal flights and (sometimes) for collection of undelivered mail. However, most of these are matters that will require one to produce the card but once.

Indeed, those who will need to present the card most often may well be those who find that they take the third type of card which is the pure EnC, offering neither passport nor driving licence facilities, and it may be this type of card which comes to attract stigma.

This could mean that unless efforts are made to combat the problem, this third type of card could in practice become the focus of stigma, and could reinforce social exclusion.

It could also mean that, again unless efforts are taken to minimise the risk, over time, respect for the confidentiality of the personal information of those who hold only the pure EnC and neither a passport nor driving licence could be eroded. For many – although of course by no means all, as Chapter 11 of the PIU (2002) report makes clear – of the initiatives in data sharing in the public sector are likely to be targeted on the less well off, because of the importance of fraud control in respect of benefits and taxes.

Distributional issues and charging

At present, there are charges for both driving licences and passports. Currently, the charge for a full driving licence is £29.00; changing a provisional to a full licence is charged at £12.00; duplicates are issued for £17.00; renewals for those over 70 cost £6.00 but replacements in the event of a change of name or address are free (see http://www.dvla.gov.uk/drivers/applydl.htm#cost).

The fees for passports were increased some months after the publication of ECIF (see http://www.ukpa.gov.uk/downloads/FE_11v42.pdf). In November 2002, the upratings were announced which increased fees to £33.00 for a full adult passport or a renewal, £63.00 for the fast track service; £19.00 for a child's passport or £49.00 for the same passport on a fast track basis. A 48 page full adult passport costs £40.00 or £70.00 on a fast track basis. Unlike the driving licence, changes of name and other information are charged for at £22.50 or £52.50 on the fast track basis.

ECIF (Table A5-2) proposes a range of supplements to the fees for full driving licences and for full adult passports, which might range from £10 up to £19, with the possibility that if the fees were increased by more than £15, then the fee for the simple non-driving and non-passport card might be removed for those – estimated ten million people – on the lowest incomes. However, if the lowest rate of fee increase of £10 were imposed, the government proposes to charge £5 for a plain plastic non-driving EnC or fully £15 for a simple smart card.

These figures are in 2001-2002 prices. ECIF notes that in real terms, prices might fall if by the time of implementation, prices for card production fell in real terms. However, it is not clear that such falls would materialise. Indeed, the introduction of the scheme, and the increase in demand for cards from the major suppliers that it would bring, might in and of itself have an simple market force effect of pushing up their prices, at least by enough to offset any gains resulting from cheaper production costs. Moreover, whether citizens would benefit from any such gains would depend on the

relative trends in inflation between the retail price index and the rate of inflation in the smart card production industry.

Are these fee increases justifiable?

The fees for driving licences and passports have presumably been set at levels that reflect the proportion of the administrative costs of processing applications that government deems it appropriate should be paid for at the point of use rather than from general taxation. ECIF seems to base the argument for these fees on the same kind of argument.

Since the government may have reasons to want to push up the costs of driving for environmental reasons, there may be some independent justification for an increase in the fee level for a driving licence card. Perhaps some of the same arguments might apply to passports if there are reasons for concern about aviation fuel emissions. However, in both cases, there are countervailing economic and trade reasons for not wanting to tax travel excessively heavily. Moreover, fee payments for driving licences and passports are not related to actual levels of travel.

Nevertheless, the main concern about the justifiability of the proposed fees does not relate to the driving licence and passport forms of the EnC, but to the bare non-driving card. In practice, those who will want this card will be likely to be the poorest citizens. If they have no intention of driving or of travelling outside the UK (ECIF does not suggest in paragraph 3.21 that it is the government's intention that the non-driving version of the card would be sufficient for travel within the EU, but only that the passport version would be), then they are certainly likely to be among those on the lowest incomes. Moreover, we know that those on the lowest incomes are likely disproportionately to be using only those public services which they have little or no choice but to use. For example, they are more likely to be claiming means-tested benefits at some point during their lives. Unlike drivers and those travelling outside the UK, the benefits they obtain from their non-driving card are much more limited, and will often be confined to things that our society has deemed to be necessities. There is therefore a strong argument that there should be no fee for the issue of a non-driving licence, non-passport entitlement card, registration for and possession of which is in any case going to be compulsory.

Suspicion and the presumption of innocence

The manner in which identification is asked for matters greatly, not only for the extent to which it can be experienced as demeaning and even as harassment, but for the general tenor of encounters between individuals and organisations in a society. It is a reasonable concern that identification should be asked for, if and where it must be asked for at all, in ways that do not carry with them the idea that organisations begin with a generalised suspicion of those who use their services, or – worse – a presumption that is not of innocence until there is reason to think otherwise. There have been societies in which this has been the general tenor of citizens' dealings with organisations of almost every kind, and they have been condemned by their own citizens when the chance presented itself, and by outsiders in more liberal societies. It would be ironic if, after many years in which the whole direction of the reform of public services has been to impress upon them the need for greater responsiveness to customers and more "customer-friendly" systems of access and choice, the direction should now shift to one of greater suspicion of customers.

Because schemes of this kind often tend to be introduced at times of great concern about threats, there is a real danger that they can institutionalise the routinisation of suspicion.

Two kinds of risk need to be avoided at the same time. On the one hand, one wants to avoid a situation in which the rule that one only enquires when there is special reason to doubt leads to a situation in which certain groups' obvious characteristics are routinely treated as reason for doubt – especially in the context of checking for illegal

immigration. On the other hand, it is of course important to be able to assure ourselves that services are not being abused and to track down the small minority who actually do so.

Ideally, one wants identifying or authorising information to be demanded, where it is taken routinely from everyone, only in the most courteous and even rather casual manner that does not suggest that the transaction with the card is any way a suggestion of suspicion of the particular individual whose card is being processed – much as is the case with most credit card transactions. Unfortunately, the fact that identity card schemes tend to be introduced when this presumption of innocence is already being eroded, and the fact that those who have to make the most frequent use of them are the poor, together mean that there is a risk that this cannot be assumed typically to be their experience of using their card. Where identifying information is required on the basis of suspicion of wrongdoing, again, ideally one wants it to be done on the basis of information about the individual in question that is directly and behaviourally related to the wrongful act suspected, and not on the basis of categorical information about some group characteristic that an individual exhibits. Again, however, without additional safeguards, we cannot have much confidence on the basis of the history of such schemes that this will be the case.

"Identification creep" and the future of anonymity

There is one slippery slope argument that seems to me worth taking more seriously than many, because it is much harder to see just what kinds of notches can be found on the slope, and because once the first movement has been made, the slope is very short indeed.

The danger is simply this. Once a context-independent conception of identity has been institutionalised in the form of a scheme of this kind, and once it become accepted that identification by a rich set of information is required for all sorts of services, then an important line is crossed when the true name of an individual can be demanded even when it is not necessary (i.e. is excessive for purpose). In effect, anonymity begins to cease to be available.

Anonymity or at least pseudonymity can be implemented in technology without great technical difficulty (Information and Privacy Commissioner, Ontario, Canada and Registratiekamer, The Netherlands, 1995; Registratiekamer for Netherlands, 1999; Working Party on Information Security and Privacy, 2001; Clarke, 1994, 1996, 2002; Burkert, 1997). It is unfortunate that ECIF contains no discussion of the role that pseudonymity and other privacy-enhancing technologies could and should play in an EnC.

Despite the generalised suspicions of some law enforcement officials that anonymity is something that only criminals would have an interest in, anonymity is in fact something that people typically have a quite basic and legitimate interest in, in many situations, and one that is distinct from many of the other values that lie behind other kinds of demands for privacy (cf. Westin, 1967). Specifically, anonymity represents at least the following two legitimate claims:

- *minimal necessary informational exposure*: that one should not be required to disclose even one's name in contexts where it is not necessary for anyone's legitimate business that it be revealed (cf. Westin's definition of privacy interests as interests in "determining for [oneself] when, how and what extent information about [oneself] is communicated to others' (Westin, 1967, 7).
- *protection against scrutiny in public, save when scrutiny is made necessary and unavoidable by some overriding and legitimate public interest grounded in specific protection against public risk*: when in public (i.e. geographically not within one's own home or other secluded place), one has a reasonable expectation

that one will not be subjected to scrutiny and called to explain who one is and to justify oneself unless absolutely necessary (cf. Schoeman's (1992) argument that the different kinds of privacy claim each serve to shield people from inappropriate social pressure).

Clarke (1996) gives the following examples of cases where the demand for anonymity is entirely legitimate:

- to avoid being found by people who wish to inflict physical harm (including ex-criminal associates, religious zealots, excessively enthusiastic fans, obsessive stalkers and overly protective fathers of ones' partner);
- to obscure the source information made available in the public interest (journalists' sources and whistleblowing);
- to avoid unjustified exposure of information about people's private lives; and
- to keep personal data out of the hands of marketing organisations.

Any or all of these may on occasion be legitimately important for particular individuals in the context of dealing with public services.

That anonymity sometimes has to be overridden is of course accepted by all reasonable people. A problem arises firstly when it comes to assumed that for almost any encounter with any service, it is expected to be overridden or waived effectively as a condition of receiving that service. Secondly, when anonymity has to be overridden, the information revealed should not be excessive for purpose, which, among other things, that the extent to which identification is required should be proportionate to the risks that identification is meant to combat. It hardly seems reasonable that the full range of personal information proposed to be held on the central register should be revealed, for example, whenever an EnC is presented in order to purchase a rail travel ticket or to apply for a retail company's loyalty card. The most extensive forms of identification should be required only for securing entitlement to those services where the costs of identity fraud or other errors with identity are highest, to the taxpayers generally or to other citizens.

For much of human history, anonymity was simply not available to many people, because most people lived in social formations in which everyone knew who they were. Since the rise of large scale urbanism and extensive social and geographical mobility, anonymity has been one of the things that many people have come to value about urban life (cf. Sennett, 1974) There have been rather fewer recent societies that have systematically sought to dispense with anonymity. Typically, these have been authoritarian societies and they have been found to be repugnant in this feature by their own citizens. It is not easy to distinguish just what is lost when chances for anonymity are lost from all the other things that are typically also being lost in societies in which anonymity is eroded. But its loss does bring about in people a generalised anxiety arising from a sense of vulnerability and exposure. How people's behaviour changes in response to this is also difficult to disentangle from their behavioural responses to the other things that they are also experiencing in societies that are eroding anonymity, and in any case, this will vary between people in different situations and different kinds of local social organisation and sub-culture. However, among the responses are likely to be decreased trust in large organisations generally and in government bodies in particular, increased investment in more furtive behaviour, attempts to engage in petty misrepresentation of identity when one believes that one can do so without consequences, deepening distrust of organisations, withdrawal from public engagement (Raab, 1997) and perhaps investment in the informal economy – all phenomena that can

be deeply corrosive of the very sense of communality that many people who advocate the limiting of privacy want to foster (cf. Etzioni, 1999).

What is of concern about an EnC scheme is straightforward. Unless it is designed in such a way that only the minimally necessary information is revealed, and that where the name of the card holder is not absolutely necessary, that too is shielded, and unless the norms by which the card is demanded constrain officials only to demand it when absolutely necessary, the card will become an instrument for the erosion of anonymity.

Western societies have already made very great strides toward the ending of anonymity. The combination of road charging and aspirations for the "smart road" are beginning to raise the possibility that, unless safeguards are built into such systems to enable anonymous payment, even road journeys will no longer be anonymous. (Bennett *et al*, 2002a,b). Closed circuit television systems are increasingly being developed that will support the identification of those filmed without their knowledge (Norris, 2002). Taken together with the gradual decline in cash and the failure of financial services to support true anonymous e-cash systems, these developments are leading to the steady erosion of anonymity in the context of our experience of retail shopping, one of the few areas of anonymity that still remained from that of the eighteenth and nineteenth century city.

The combination of pressures for protection against various risks and the imperatives of "convenience" have gradually led to this outcome. The advent in the UK of the identity or entitlement card, which – unlike many continental European states – has not traditionally used one, must be seen against this background. It is driven by the same pressures for protection against risk and for convenience. It is an additional feature of the social environment organised for these purposes.

At the very least, it could be designed in such a way that it does not add to or worsen these trends, by being designed to reveal only the minimum set of information necessary for each kind of transaction in the contexts for which it is being used.

More generally, though, the fact that what is being proposed is a general, all-purpose identifier gives the EnC a special status in the public imagination that single-context identifiers do not have. No doubt many law enforcement officials and policy analysts would dismiss that as evidence of the irrationality of the public. After all, they will argue, what is the difference between the identifier for purchasing that lies within a credit card and a general identifier?

We should not be quite so quick to dismiss public anxieties as irrational, or the distinction between general and less general identifiers as a distinction without difference. The fact that something is not tied to a particular context of use such as a defined service or a defined list of services gives it a vagueness, an open-endedness that not unreasonably leaves people with the feeling that they can do little to achieve control over the information captured in the course of its use, especially if they have no choice but to register for the database and posses the token, and where they know that it will sustain a variety of data sharing. Moreover, the day-to-day experience of the use of the scheme is likely to be one in which people will feel conspicuous in public places if they are asked for identification and it becomes the norm to use the card for particular purposes, but they alone either choose to or else are left to use other means to do this. There will also be anxieties about the difficulties one might face, should one lose one's card, both in securing a replacement and in securing access to a wide range of services in the meantime. In a liberal society, these are hardly inherently unreasonable concerns.

Once again, these considerations are not reasons to reject literally any scheme for a population register and a portable token carried by individual citizens. But they are very powerful reasons for suggesting that the scheme should be limited to a defined set of service-specific purposes, that the data revealed on use should be minimised and varied according to the requirements of each type of use rather than all the data on the register

being available on each occasion of use, and for giving card holders a very clear understanding of what disclosures of their data will be made. Unfortunately, the Home Office consultation paper does not offer these things.

Part VI: Conclusion

It is no part of the argument of the present paper that information technologies are somehow intrinsically undermining of privacy, or that somehow the interest of privacy was better served by keeping paper records, as if they were more secure and easier to keep control of. This is indeed argued by some privacy advocates (e.g., Marion Chester, presentation at the Privacy International public meeting on the entitlement card, 11 December 2002, concerning medical records; this view has long been argued in general by that implacable opponent of information technology, Simon Davies, e.g., 1996).

However, my argument here is precisely the reverse. Manual records were extremely insecure, and very easy to use to add irrelevant and excessive information without scrutiny. There have been many documented cases in which inaccurate and irrelevant information has been entered onto manual records, for example, in health care and social work systems. The advent of electronic record systems has brought to case record keeping a sense of appropriate formality which has happily reduced the numbers of cases of such bad practice. Moreover, it is much easier to remove a piece of paper from a manual file before making that file available to others, or indeed before making its contents available for subject access, than it is to remove an entry from a well-structured electronic record with defined fields and where there is an audit trail of both entries and deletions.

It is only by the deliberate use of the full possibilities of information technologies and in particular of the facilities for pseudonymisation and contingently modulated information release, afforded by smart cards, that privacy values can be effectively protected. My own view, which I have argued in the section on data protection, is that full compliance with data protection law requires no less, if schemes of this kind are to go ahead at all. If the costs of doing the things necessary to meet these concerns – listed in the eight points at the end of that section – render the whole scheme no longer worthwhile, when evaluated in a cost-benefit analysis, then so be it. But to conduct a cost-benefit analysis that finds a scheme economically worthwhile but undermining of privacy is to ask the wrong question: we should surely define the kind of system we care about, and then cost it: a cheap but doubtfully legal scheme is hardly compelling and certainly not conducive to public trust.

I have argued that consideration from first principles in a liberal democratic society should not lead us to conclude that *no* identity or entitlement card scheme can be accepted. A justification can be defined that would, in principle, permit a government to introduce compulsion for a scheme, with very light penalties of denial of service where someone cannot offer a satisfactory alternative way to establish authorisation, rather than civil or criminal sanctions, for those who do not register and take the card. But there are other conditions. The scheme must be one that supports privacy and also worthwhile and proportionate to the risk.

If – and it is a big if – these conditions can be met, fundamental opposition is as misguided as is enthusiasm. However, that consideration from first principles leaves us with a series of very important constraints upon how schemes of this kind should be implemented, if they are to be acceptable. Some require special technological design; some require innovation in forms of redress and oversight; some require changes to the everyday practice of officials providing public services.

In a liberal society, if it is necessary to introduce a scheme of this kind, it should be introduced in sorrow rather than in anger, and it should probably never be loved, but rather it should be a proper focus of ongoing vigilance. If a scheme can be designed that would meet the conditions specified in this paper, then it should be tolerated but regularly scrutinised. And if its consequences for privacy, for anonymity, for stigma and social exclusion, for equal opportunities, for the corrosion of the presumption of innocence begin to turn sour, then governments should be prepared to abandon it.

Acknowledgements

I am grateful to David Clancy (Strategic Policy Officer), Francis Aldhouse (Deputy Commissioner, Data Protection) and Jonathan Bamford (Assistant Commissioner, Strategic Policy) of the Office of the Information Commissioner for their decision to commission me to write the paper. Charles Raab, Stuart White, Christine Bellamy, Jonathan Bamford , Shelagh Gaskill and Claire Brown all gave me invaluable comments on an earlier draft. None of them should be presumed to agree with my arguments, nor do they bear any responsibility for my errors. This paper was commissioned and written in my personal capacity and should be taken as reflecting only my own views, and not necessarily those of the Information Commissioner or of King's College.

References

6 P, 2000, 'The morality of managing risk: paternalism, prevention, precaution and the limits of proceduralism', *Journal of risk research*, 3,2, 135-165.

6 P, 2002c, *Strategies for reassurance: public concerns about privacy and data sharing in government*, Performance and Innovation Unit, Cabinet Office, London, 166 pages, published at http://www.strategy.gov.uk/2002/privacy/report/papers/perri6.pdf.

6 P, 2003 forthcoming b, 'What's in a frame? Social organisation, risk perception and the sociology of knowledge' *Journal of risk research*.

Audit Commission, 2002, *Data remember: improving the quality of patient-based information in the NHS*, Audit Commission, London.

BBC Online, 2002, 'UK plans for ID cards under fire', BBC News web site, published at http://news.bbc.co.uk/I/hi/technology/2583651.stm.

Bennett CJ, Raab CD and Regan P, 2002a, 'People and place: patterns of individual identification within intelligent transportation systems', in Lyon D, ed, 2002, *Surveillance as social sorting: privacy, risk and digital discrimination*, Routledge, London, 153-175.

Bennett CJ, Regan P and Raab CD, 2002b, 'Onboard telematics and the surveillance of movement: the case of car rental systems', paper presented at the 6th internal Ethicomp conference, *The transformation of organisations in the information age: social and ethical implications*, 13-15.11.02, Lisbon.

Burkert H, 1997, 'Privacy enhancing technologies: typology, critique, vision', in Agre PE and Rotenberg M, eds, 1997, *technology and privacy: the new landscape*, Massachusetts Institute of Technology Press, Cambridge, Massachusetts, 125-142.

Cabinet Office, 2002, *Identity fraud: a study*, Cabinet Office, London.

Clarke R, 1994, 'Human identification in information systems: management challenges and public policy issues', *Information technology and people*, 7, 4, 6-37, available at http:www.anu.edu.au/people/Roger.Clarke/DV/HumanId.html.

Clarke R, 1996, 'Identification, anonymity and pseudonymity in consumer transactions: a vital systems design and public policy issue', paper presented at the conference, *Smart cards: the issues*, Sydney, 18.Oct 1996, available at http:www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html.

Clarke R, 2002, 'The mythology of consumer identity authentication', paper presented at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11. Sept 2002.

Davies S, 1996, *Big brother: Britain's web of surveillance and the new technological order*, Pan, London.

Etzioni A, 1999, *The limits of privacy*, Basic Books, New York.

Govier T, 1982, 'What's wrong with slippery slope arguments?', *Canadian journal of philosophy*, 12, 303-316.

Home Office, 2002, *Entitlement cards and identity fraud: frequently asked questions*, Home Office, London, available at http://www.homeoffice.gov.uk/ccpd/faqid.htm.
Information Commissioner, 2001, *Data Protection Act 1998: legal guidance*, Information Commissioner, Wilmslow, available at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf.
Information and Privacy Commissioner, Ontario, Canada and Registratiekamer for the Netherlands, 1995, *Privacy enhancing technologies: the path to anonymity, vols I and II*, Information and Privacy Commissioner, Ontario, Canada and Registratiekamer, The Netherlands, Toronto and Rijkswijk.
Information and Privacy Commissioner, Ontario, Canada and Registratiekamer for Netherlands, 1999, *Intelligent software agents: turning a privacy threat into a privacy protector*, Information and Privacy Commissioner for Ontario, Canada and Registratiekamer for Netherlands, Toronto and Rijkswijk
Janoski T, 1998, *Citizenship and civil society: a framework of rights and obligations in liberal, traditional and social democratic regimes*, Cambridge University Press, Cambridge.
Lyon D, 2001, *Surveillance society: monitoring everyday life*, Sage, London.
Margetts H and Dunleavy P, 1995, 'Public services on the world markets', in *Missionary government, Demos collection*, 7, 30-32.
Masons (solicitors), 2002, 'Entitlement cards- consultation', *Data protection and privacy practice newsletter*, December, Masons (solicitors), London, 2-4.
Mead LM, 1986, *Beyond entitlement: the social obligations of citizenship*, Free Press, New York.
National Audit Office, 2002*, Report by the Comptroller and Auditor General - Class III Vote 8 - Driver and Vehicle Licensing Agency*, HC 335-III Session 2001-02, National Audit Office, London
NHS Information Authority, 2002, *Caring for information: model for the future*, NHS Executive, London and Leeds.
Norris C, 2002, 'From personal to digital: CCTV, the panopticon and the technological mediation of suspicion and social control', in Lyon D, ed, 2002, *Surveillance as social sorting: privacy, risk and digital discrimination*, Routledge, London, 249-281.
Performance and Innovation Unit, 2002, *Privacy and data sharing*, Performance and Innovation (now the Strategy Unit), Cabinet Office, London, available at http://www.strategy.gov.uk/2002/privacy/report/index.htm.
Raab CD, 1997, 'Privacy, democracy and information', in Loader BD, ed, 1997, *The governance of cyberspace*, Routledge, London,155-174.
Schoeman D, 1992, *Privacy and social freedom*, Cambridge University Press, Cambridge.
Schulman A, 2002, 'The US/Mexico Border Crossing Card (BCC): a case study in biometric, machine-readable ID', paper presented at the *12th conference on computers, freedom and privacy*, San Francisco, California, available at http://www.undoc.com/bccnew.doc
Secretary of State for the Home Department, 2002, *Entitlement cards and identity fraud: a consultation paper*, Cm 5557, The Stationery Office, London.
Sennett R, 1974, *The fall of public man*, Faber and Faber, London.
Stalder F and Lyon D, 2002, 'Electronic identity cards and social classification' in Lyon D, ed, 2002, *Surveillance as social sorting: privacy, risk and digital discrimination*, Routledge, London, 77-93.
VanDeVeer, D, 1986, *Paternalistic intervention: the moral bounds of benevolence*, Princeton University Press, Princeton, New Jersey.
Walton DN, 1992, *Slippery slope arguments*, Oxford University Press, Oxford.
Westin A, 1967, *Privacy and freedom*, Athenaeum Press, New York.

Williamson OE, 1985, *The economic institutions of capitalism: firms, markets, relational contracting*, Free Press, New York.
Working Party on Information Security and Privacy, 2001, *Directorate for science, technology and industry: Committee for information, computer and communications policy; Report on the OECD forum session on privacy-enhancing technologies (PETs) Annex 2: A study of privacy-enhancing technologies*, (prepared by Laurent Bernat) Directorate for Science, Technology and Industry, Organisation for Economic Cooperation and Development, Paris, published at http://www.olis.oecd.org/olis/2001doc.nsf/c5ce8ffa41835d64c125685d005300b0/52810d7d5d053174c1256b170037d8cc/$FILE/JT00117775.PDF.