March 2003

Entitlement Cards: Do the Home Secretary's Proposals Comply with Data Protection Principles? Part I [1]

By Dr Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, Kings College London

Introduction

At the end of January 2003, the official period of consultation ended on the U.K. Home Secretary's proposals for an entitlement card for all legal residents in Great Britain and Northern Ireland. What is proposed is not unreasonably regarded an identity card in all but name. In essence, the scheme is for a smart card, which it would be compulsory for all U.K. residents to possess. Although they would not be strictly legally required to carry it at all times, in practice it would probably be difficult to leave home without it. Behind the scheme would be a central population register containing a wide range of personal information. The governments hope is that it would help to combat identity fraud, although they have carefully avoided suggesting that it would help in combating crime generally, or even social security fraud, let alone terrorism.

The government's consultation paper claimed that the scheme would be compliant with the letter and spirit of data protection legislation. This two-part article is concerned with the question of how far both limbs of that claim are true. The article reviews in turn each of the major areas of concern around the application of the data protection principles Article 8s necessity test, fair processing, purposes, function creep, excess, accuracy, disclosures and security.

The proposals were set out in *Entitlement cards and identity fraud: a consultation paper* (Secretary of State for the Home Department, 2002), referred to from now as ECIF; I shall also refer to the entitlement card as EnC for short (EC would have been more logical, but its common use to mean the European Community would have made it confusing).

One matter of principle must be established at the outset. 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. The only question is whether *this particular scheme*, as proposed by the Home Secretary, is compliant.

If as this article argues it is not, then in principle there is no reason why the government could not produce a revised scheme that would be compliant.

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 the argument of this article, and I would not expect them to be. However, it is important to work with the principles as they are presently expressed.

Article 8: the Necessity Test

While the processing of data in the central register would be deemed 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 added]

The fact that the United Kingdom 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 U.K. 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 United Kingdom, out of a 13.8bn estimated value of fraud in total, cannot really be used to demonstrate a failure on the scale required to meet a necessity test, precisely for the reason that the government cannot demonstrate that 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 United Kingdom 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. The European courts have ruled that states have some latitude in defining what is necessary. 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 (see section 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, could 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, nor do they address the fair processing implications. Firstly, as ECIF notes (see section 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.

More generally, 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. Such a code should specify the occasions on which production of a card may be demanded, ways of minimising unnecessary repetition in requests, information to be provided to a citizen when their card is processed, *etc*., and should also provide for means of administrative redress by individuals aggrieved by violations of the code.

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 (see section 6.3)

• to provide people who are lawfully resident in the United Kingdom with a means of confirming their identity to a high degree of assurance;

• to establish for official purposes a persons identity so that there is one definitive record of an identity which all departments can use if they wish;

• to help people gain entitlement to products and services provided by both the public and private sectors;

• to help public and private sector organisations to validate a persons identity, entitlement to products and services and eligibility to work in the United Kingdom.

(As it is written, the third purpose could not 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. The underlying argument is that citizens cannot be expected to trust in governments and in public services that 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, 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 United Kingdom 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. 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 a multi-functional 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 (see section 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 ECIFs 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 to try to put in a purpose for the scheme that allowed the data on the central register 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 December 11, 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. 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 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. The advantages in terms of the convenience to the cardholder of having one card to fulfil a number of purposes 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.

First, 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 the 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 cardholder'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 persons date 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 cardholders 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 taxpayer's 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 subjects 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, ones 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 parents 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 (see 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 may. 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 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.

The second part of this article, to be published in the April issue of World Data Protection Report*, goes on to consider the issues of accuracy, disclosures of information from the central register and security.*

References

6 P, 2003, *Entitlement cards: benefits, privacy and data protection risks, costs and wider social implications*, Office of the Information Commissioner, Wilmslow, published at www.dataprotection.gov.uk/dpr/dpdoc1.nsf/24afa328dcbf83d8802568980043e730/2924d87f53cb414180256cc5003fcd96/$FILE/perri6_annexb_ecards_paper_ic_rvsd_final_ver.doc.

Secretary of State for the Home Department, 2002, *Entitlement cards and identity fraud: a consultation paper*, Cm 5557, The Stationery Office, London.

NHS Information Authority, 2002, *Caring for information: model for the future*, NHS Executive, London and Leeds.

1 This article uses material from a much longer report prepared for the Information Commissioner: see 6 (2003). 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 work 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.