



Response to the Government's Consultation on Legislation on Identity Cards

Introduction and Summary

When I responded to the Government's previous consultation on 'Entitlement Cards', I made clear that my primary concern was to establish whether any proposed ID card scheme had the necessary data protection and privacy safeguards in place. To judge this I had to be certain what was intended and how a scheme would function in practice. I called for the publication of a draft bill to assist this process and I am pleased that the draft Bill has now been published to help focus in on the practicalities of the Government's plans and whether the necessary safeguards are in place.

Public debate now needs to extend well beyond the benefits and drawbacks of plastic ID cards. The current proposals involve a fundamental shift in the extent to which government collects, uses and shares personal information about individuals and – in some situations – about their activities.

The draft Bill outlines the infrastructure which will be necessary to support an ID card scheme. As the detail of this infrastructure – and the full magnitude of the proposals – start to emerge, my previous healthy scepticism has turned to increasing alarm. This infrastructure and the associated arrangements will include:

- The National Identity Register – a database of 80% of the economically active population by 2013;
- A unique personal National Identity Registration Number for each individual;
- The collection and indefinite retention – on a compulsory basis in many cases initially, and in all cases eventually – of significant amounts of personal information;
- A comprehensive record of each time registration details are checked and /or disclosed;

- Access to the personal information contained in the Register for many parts of government, and in some cases to the records of who has accessed the records.

It requires over three pages of the Bill (Clause 1(4) and Schedule1) simply to list the personal information which will be collected and retained in the National Identity Register. This includes:

- Full names and other known names;
- Date and place of birth;
- Physical characteristics;
- Photograph;
- Biometric information – fingerprints and/or iris scan;
- Residential address;
- Previous residential addresses;
- Addresses of “every other” residence – with dates;
- Nationality;
- Details of immigration status;
- National Identity Registration Number, ID card number, National Insurance Number, passport number and various other personal reference numbers;
- Validation information – including information provided to support initial registration or a modification;
- “Steps taken” to identify an individual or verify information provided;
- Security information;
- Access records - including “particulars of every occasion on which a person has accessed the individual’s record and of the person who accessed it.”

The organisations which – subject to purpose limitations and procedural requirements - will be able to access the personal information without the consent of the individual include:

- Security Services
- Chief Police Officers
- Inland Revenue and Customs & Excise
- Any prescribed government department
- Any other person (or organisation) specified or described in an Order made by the Secretary of State

In addition, the Security Services - and others in some circumstances - will also be able to access the record of who has accessed an individual’s entry in the Register providing a picture of an individual’s use of certain services and some of their movements.

It is especially ironic that – although some others will have this right – individuals themselves will not be able to access the record of who has accessed their details on the Register, whether to check for misuse or for any other reason. The draft Bill contains provisions designed to remove the individual's right of access under the Data Protection Act 1998.

I have set out below my concerns on the various elements of the proposals. My major concerns focus around:

- Continuing uncertainty about the lack of clear and limited statutory purposes for the proposals;
- The nature and extent of the personal information which will be collected and retained;
- Uncertainties and risks relating to administrative and technical arrangements;
- The provisions relating to access to, and disclosure of, personal information stored on the National Identity Register;
- The need for stronger independent oversight;
- The absence of a “voluntary” option for driving licence and passport holders;
- The loss of some initial safeguards as and when the scheme becomes compulsory;
- The extent to which secondary legislation can be used to extend the scheme, thus fuelling anxieties about “function creep”.

Annex D to the consultation document sets out the Government's view on how the data protection principles are complied with in their proposals. This does not provide a complete picture of the situation. I have highlighted where I believe the approach suggested is inconsistent with the requirements of particular principles. A full list of data protection principles is set out at Annex A.

Purposes

1. I have always called for maximum clarity about the purposes of any ID cards system. Once we understand these we can judge whether what is being proposed is proportionate to those objectives. I still find myself unsure of what all the purposes for which the Register, the National Identity Registration Number and the ID card itself may ultimately be used. The Government's assurances about function creep seem to centre very much on items to be held on the Register rather than the use the identity system is actually put to in practice. The Government has defined the statutory purposes of the National Identity Register in terms of providing a record of registrable facts about individuals, issuing cards based on these, providing for the verification of facts to service providers with consent and disclosure to authorised

persons. This is not at all illuminating in terms of the use made of the identity system in practice.

2. At the time of the Government's original consultation in July 2002, a number of possible uses were suggested and these centred on combating illegal working, better administration of public services and as a safeguard against identity theft. The fight against crime and terrorism were scarcely mentioned. In the latest proposals, however, crime and the terrorist threat have been given increased prominence. I remain concerned that we need to be clear about what are the pressing needs for an identity scheme and that any such scheme is limited to dealing with these. I am mindful of the fact that at the time of the introduction of the last national identity scheme in 1939 three administrative uses were envisaged (national service, security and rationing). Some eleven years later thirty nine government agencies made use of the records for a variety of services.¹ At the time of the debate on the abolition of that scheme, preventing bigamous marriages had become one of the main arguments in favour of the retention of the scheme².
3. Clarity of purpose is particularly crucial when use for purposes such as terrorism and crime prevention are envisaged because a register, a card and a number may not be of much assistance in dealing with such matters in isolation. The circumstances where the citizen is asked to produce the card, and the details recorded, will be crucial. Will very large volumes of apparently benign transactions need to be recorded in order to spot likely terrorist activity? If defeating terrorism is a major aim we need to understand how such an identity scheme serves this objective in practice as this may give an all together more worrying picture of how we may have to conduct our lives in future by having to produce identity documentation and have our details recorded in many of our daily transactions. **(1st, 2nd and 3rd Principles)**

Administrative and Technical Arrangements

4. The system for establishing the Register and the issuing of ID cards is a crucial feature. The Government believes that the scheme will be the 'gold standard' for identity. If this is the case then it must inevitably become the main target for the serious identity fraudster who may well capitalise on the existing identity documents of others in order to gain their identity. Although it is impractical to go into great detail on the minutiae of the issuing process in a draft Bill, it is worrying that issues such as governance and the high level issuing procedures are not addressed, these still being open to debate. In my response to the Government's earlier consultation I made clear my desire for

¹ PRO HO45/25015 'Report of Committee on National Registration'

² Modern Horrors: British Identity and Identity Cards- John Agar: Documenting Individual Identity Princeton UP 2002

independent oversight of the Register/enrolment process and this is not achieved by the proposal that these functions should fall to an existing executive agency under the direct control of the Secretary of State. I am pleased that the accompanying consultation paper indicates that the Government is still open to argument on this issue and I urge it to consider establishing an independent body to oversee the administration of the National Identity Register and card scheme, with responsibilities to ensure that the statutory limitations are complied with in practice and rectify problems for individuals. The body should be required to make an annual report to Parliament on the operation of the scheme and to educate the public and service providers on the proper operation of the scheme

(3rd, 4th and 7th Principles)

5. It is similarly disappointing that the issues surrounding the vital functions of identity enrolment, maintenance, verification and card manufacturing are still left unresolved. It is argued that the precise arrangements cannot be set out in the draft Bill but will be left to Regulations due to ongoing testing of different options. I am mindful of the cautionary words of those with unbiased professional expertise in this area such as the British Computer Society who express substantial concerns about the lack of fixed objectives of the scheme jeopardising the successful delivery of the necessary IT systems. Similarly, unless we are certain of the rigour of the application procedure it is difficult to be confident that any system will work and that there will not be the potential for a significant impact on individuals who find difficulties with the operation of the system. These difficulties range from the theft of identity before individuals enrol through to delays in processing changes or producing replacement cards. The consequences for individuals arising from potential failures in the system should not be underestimated. Even with the best will on the part of those administering the Register there will inevitably be delays in resolving any such problems and individuals may well suffer delay in gaining access to services, or worse. This will particularly be the case if registration is made compulsory whereby an individual may be required to produce a card to gain a service without the opportunity to utilise alternative means of identification. We must be careful not to let the UK population become the test bed for the development of a comprehensive yet untried identity system which has the potential for a significant detrimental impact on the day to day lives of individuals if the technical and/or administrative systems are found wanting. **(1st, 3rd, 4th and 7th Principles)**
6. The importance of understanding the architecture and operation of the system cannot be overstated as it is possible for activities such as identity verification to operate in different ways with differing levels of impact on privacy. For example it is not clear the extent to which identity verification will involve checking the central data base or how this will be undertaken. If the biometric information and the enrolment procedures are reliable presumably fewer checks will need to be made against the Register. A card reading device

could compare information retained on a chip on the card with the biometric of the person presenting the card. This clearly has the advantage of reducing the amount of intrusive transaction details recorded about an individual on the Register and may reduce the higher error rate with 'one to many' biometric checks. **(1st, 3rd, and 4th Principles)**

The National Identity Register

7. Turning to detailed comments about the National Identity Register, there are a number of concerns that warrant further clarification. The Register is primarily founded on the concept of 'applications' thus giving an illusion of choice. However individuals who have driving licences or passports that expire or who apply for such documents will have no choice. There is no provision for non ID card variants of these documents so inclusion in the Register will in effect be compulsory for a substantial part of the UK population. The first phase will not be genuinely "voluntary". Similarly entries can be made in the Register irrespective of an application for a card (clause 2 (4)). The ability to keep details of those already identified as not entitled to register is cited as the motivation but the provisions in the draft Bill contain no such limitation with the consequence that an individual may be entered on the Register without their knowledge. In this context it is particularly important to understand the relationship between the National Identity Register and other planned databases such as the Citizens Information Project and the planned database of all children envisaged under clause 8 of the Children Bill. These may provide the particulars for individuals to be given an entry in the National Identity Register. In the case of the latter, for rising sixteen year olds. If such individuals contained on these other databases have no intention of applying to go on the National Identity Register and there are no suspicions about them in case of a future application then such details would be excessive. **(1st and 3rd Principles)**
8. Other significant data protection concerns relating to the Register and the 'registrable facts' within it requiring further consideration include:
 - The relevance of all other places of residence, previous identities and previous residential status when an identity has satisfactorily been established using the principal place of residence and other current details (clause 1, clause 3 and sch. 1). The details of other places of residence seem to have more to do with service delivery than identity verification **(1st, 2nd and 3rd Principles)**
 - The requirement to keep all information, including transaction details (sch 1 (7) and (9)) with out precise time limits. **(5th Principle)**
 - The inclusion of all official reference numbers (sch 1 (4)). The relationship with the unique numbers to be issued as part of the Citizens Information Project and the database of all children under the Children Bill will require clarification. **(1st, 2nd and 3rd Principles)**

- Potentially wide amount of information recorded about an individual on request (clause 1 (4) (i)). **(3rd Principle)**
- Extension of the registrable particulars by order (clause 3 (4)). **(3rd Principle)**
- Open ended requirement on an applicant for registration to provide such information as the Secretary of State sees fit to require (clause 5 (5) (d)). **(3rd Principle)**

The ID Card

9. There are a number of issues surrounding the procedures for the issuing of the card and the information required to validate the registration applications that raise data protection concerns. The most significant of these is that there is no specific detail of the extent of information to be recorded on the card or the form in which it is recorded. This is particularly worrying as there is no provision for 'non ID card' variants of designated documents so there is no opportunity for an individual to limit the amount of information that may be available to those to whom the document is being presented for its primary purpose by being able to use a non ID card version. For example, a person who produces their driving licence on many occasions when hiring cars may wish to have a non ID card variant of that document to ensure that the additional identity card details on a dual purpose card are not revealed to car hire companies. **(1st and 3rd Principles)**
10. Similarly the form in which the information is retained is crucial as this will determine what is visible on the card and what is available on a chip. The technical arrangements for the reading of the chip have not been specified. There are dangers if a contactless chip is used without any form of encryption, such as is specified by ICAO for travel documents (known as open contactless chips). It is possible at the point of it being interrogated by a legitimate card reader for the details to be captured by others who may be electronically 'eavesdropping'. The requirement to have information recorded on a contact chip or encrypted if a contactless one is used should be clearly set out. **(7th Principle)**
11. Other areas of data protection concern on the card issuing arrangements include:
 - Lack of certainty of the administrative arrangements for designated document authorities (clause 10 (3)). **(7th Principle)**
 - Open ended requirement on unspecified 3rd parties to provide information for application validation purposes (clause 11 (1)). **(1st and 3rd Principles)**
 - Extensive duties on individuals to notify changes of information on the Register even though this may have little ongoing value (e.g. other places of residence) (clause 12). **(1st and 3rd Principles)**

National Identity Registration Number

12. The form of the National Identity Registration Number is not specified in the draft Bill and will be left to Regulations. This will be a significant piece of information as it will allow the linking of records as well as being a reference number cited by an individual when others are verifying their identity. The number should not be based on an existing number with comparatively wide current circulation such as National Insurance Number to ensure the appropriate level of security. Nor should the number itself include any other information pertaining to the person to whom it relates, such as including date of birth among the digits. The widespread recording of the number by disparate service providers runs the risk not only of greater currency and less security but also that it may allow a picture to be built up of an individual based upon their dealings with many service providers, all linked together by a common reference number. The Government's assurance in the accompanying consultation paper that the number will be designated as an identifier of general application under the Data Protection Act 1998 is welcome but any Regulations must contain effective safeguards against the unwarranted capture and recording of such details by service providers. ***(1st, 2nd and 7th Principle)***

Disclosure of Information

13. A substantial concern centres on those who may have access to the Register details showing previous access by others. Although this information is differentiated from the rest of the information in an entry, whole classes of organisation are granted potential access without having to justify their need. For example the Director General of the National Criminal Intelligence Service may have access to such details for any of his functions whereas a chief officer of police could only have access in relation to serious crime. A number of the Director General's functions are similar in nature to the intelligence functions of an ordinary police force, for example in relation to football related crime. He also acts as the UK's National Central Bureau for Interpol providing responses to requests for information from overseas police forces via Interpol. It is possible that the Director General may be able to gain access to information on the Register on behalf of a foreign police force that a domestic chief officer would not be entitled to. Access should be on the basis of need in relation to the severity of the matter being investigated. ***(1st, 2nd and 8th Principles)***

14. The arrangements for disclosure of information from the Register and the circumstances where a card may be checked are also worrying. A significant concern centres on clause 14 (4). This appears to remove any right, including any provided by statute, to an individual having access to the record of accesses made to their Register details. It is understood from discussions

with Home Office officials that this provision is an attempt to remove the right of subject access provided under the Data Protection Act 1998. The Data Protection Act does have a specific provision aimed at overriding such restrictions (S. 27(5) DPA) but this may not safeguard the right of access, as this restriction would be created in subsequent legislation. If the concern underlying this provision is that records of accesses by security and police services may reveal to an individual their interest in them, then the existing exemptions from the right of access under the Data Protection Act in relation to national security and crime prevention purposes would be sufficient. This clause should be removed from the draft Bill as it represents a significant diminution of rights in an area of particular relevance to an individual who has accessed their Register details. The existence of such a provision may also call into question whether the UK has properly implemented the EU Data Protection Directive (95/46/EC). **(6th Principle)**

15. Clause 19 contains a provision prohibiting the production of an ID card as a condition for the delivery of a service, subject to certain exceptions such as allowing alternative means of identification. However, there is no similar restriction in relation to checks on the Register, the safeguard against this appears to be the individuals' consent being necessary for such checks (clause 14 (1)). There should be an equivalent provision as the potential for disclosure with consent to be manipulated by others should not be underestimated; a persistent problem under data protection legislation is enforced subject access where an individual is required to use their access rights to produce information as to their bona fides for the benefit of others. Great care needs to be taken in the procedures to be established by Regulations under this section. **(1st Principle)**

16. Further specific concerns include:

- The extent, in practice, to which an individuals' consent to a check will be freely given, specific and informed (Clause 14) **(1st Principle)**
- The lack of precision about the public services who could require an identity check leaving this to Regulations with potential for function creep over time (clause 15 (2) and (5)) **(2nd Principle)**
- The expansion of checks via other legislation and the ability to check the Register even though no card has been issued (clause 16) **(1st and 3rd Principles)**
- The disclosure without consent of general Register information to the Secretary of State for any of his purposes (clause 20 (5)) **(2nd and 3rd Principles)**
- The power to extend the provisions on disclosure without consent still further by Regulations permitting potential function creep (clause 23) **(2nd Principle)**

Independent Oversight

17. The lack of a total system of independent oversight is of concern and I have already expressed my wish for the setting up of an independent body to undertake this function. One area where a positive attempt to introduce this within the draft Bill is in relation to disclosure from the Register without consent. Whilst the appointment of a National Identity Scheme Commissioner is a step in the right direction, it falls well short of the level of independent supervision required due to the limited remit. Indeed it is a concern that even if the Commissioner discovers misuse there is no provision to require him to bring this to the attention of the individual affected or to provide any remedy for such an individual. His ability to report to Parliament is subject to a Prime Ministerial override down to the level of 'prejudicial to the continued discharge of the functions of a public authority' (Clause 26 (4)). This undermines the independence of the supervisory arrangements.
18. The Draft Bill does contain welcome offence provisions relating to unauthorised disclosure, provision of false information and the tampering with the Register (clauses 29-31). However, the offence related to unauthorised disclosure (clause 29) is limited to those involved in the registration process. Others who may consult the Register as part of their official duties may also misuse the details available to them but are not covered by such a provision and would have to be dealt with by different means, presumably the offences at S.55 of the Data Protection Act. A more comprehensive offence provision should be considered. (*7th Principle*)
19. There is currently a further significant gap that should be remedied. There is no mechanism proposed under the legislation for an individual to be able to appeal against decisions of the Secretary of State when administering the National Identity Register. An individual could face a situation where their identity has been assumed by and allocated to another or they could be having real difficulties with the particulars entered in the Register. Given the consequences described above where an individual may potentially suffer great detriment as a result of such problems it is important that there is a mechanism to allow individuals to appeal against the actions of the Secretary of State. Even though I strongly support the creation of an independent body which could protect the position of individuals, there must also be a judicial remedy available in order provide the most effective safeguard for individuals. (*1st and 4th Principles*)
20. A further element of supervision would be to provide me with the same level of audit and inspection powers as enjoyed by my European counterparts. At present my powers are limited to inspecting processing activities with the consent of the data controller concerned. To provide me with a proactive audit power in relation to the scheme would enable me to provide an extra level of reassurance that those involved in the operation and use of the

scheme are doing so in full compliance with the safeguards provided by the Data Protection Act.

Future Compulsion

21. It is a significant concern that if and when clause 6 is used to introduce a compulsory scheme then important safeguards in the Bill will simply disappear. For example the very welcome provision making unlawful the requirement to establish identity by use of an ID card is undermined once clause 6 is applied (Clause 19 (2)(c)). This appears to mean that any private sector organisation could demand production of an ID card for any service it offered to an individual. In practice this could mean that an organisation may check the Register for the most mundane of transactions and the details of this recorded, building up an extensive picture of individuals' day to day activities. This clause also effectively removes the opportunity to produce alternative forms of identification. Similarly, if clause 6 takes effect then the provision of all public services can be made conditional on production of an ID card (clause 15 (2)). The description of a 'public service' at clause 15 (5) is extremely wide so even the most mundane of public services could become dependant on production of an ID card. The mechanism for extending the scheme to a compulsory one does require a significant level of parliamentary scrutiny; however trying to modify the existing non compulsory scheme using the suggested mechanism might cause difficulties in itself, as I have highlighted above. Consideration should be given to the use of primary legislation to make the scheme compulsory. (*1st Principle*)

Conclusion

22. The draft Bill, whilst helping to clarify many matters, still leaves many matters unresolved. There are over 20 order making powers within the draft Bill and I remain concerned about the extent of these and the real danger of function creep over time. What the draft Bill has made clear is that what is envisaged is an extensive national identity registration system, not just an identity card. This engages the substantial data protection concerns outlined above. In order to further clarify the impact of the proposed scheme on individuals' privacy and to identify further safeguards that may be incorporated, I intend to explore the possibility of commissioning an independent privacy impact assessment. I would make this available to Government. In any event I remain committed to assisting Government to understand the data protection issues surrounding this important issue and assisting it to develop measures to address these should it wish to proceed with its proposals.

Annex A

Data Protection Act 1998.

Schedule 1, Part 1.

The Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.