CONSIDERATIONS RELATING TO AN IDENTITY RIGHTS CHARTER

FOREWORD FROM PETER WHITTLE EXPERTS GROUP CONVENOR

It would be an easy matter to produce an Identity Rights Charter that might be similar to so many charters that institutions produce, that is, ones which are superficially reassuring but offer little of substance when tested. I know that this is not what the IPS nor the Experts Panel would want from the Identity Rights Charter. Consequently the Experts Panel has spent much time and effort considering the fundamentals that should underpin an effective and valuable Identity Rights Charter. We have tried to capture our thinking in the attached document.

I should emphasise that this is a working draft and while there is broad agreement amongst the Experts it has not been prepared as the definitive treatise on the subject, indeed there are aspects which I am sure we might want to expand and change given more time. What we have tried to do is lay out the fundamental principles and many of the practical considerations. The document is written for the well-informed IPS community, it is not written particularly for the lay reader. It does not attempt to draft a rights charter in tabloid terms but recommends some, at least, of the elements of a rights charter. If at times it seems that we are stating the obvious it is in part because my experience has been in the short time I have been involved in this area that clarity and precision are easily lost. An appendix is also attached that provides some valuable insights with regards to the issue of ensuring a unique biological identity and differences between this and other (possibly multiple) social identities. This has relevance here and to other issues which we have been asked to consider, for example, with regards to utility.

Structurally then we are offering a document to stimulate discussion on the fundamental principles of a rights charter, some recommendations on the specific content of a rights charter and some background on the core attributes of a biological identity versus other identities. Providing there is agreement on the fundamentals it would be a relatively easy matter to finish a draft of a rights charter (though putting it in the plainest language might require some iteration). The next stage would then be to link the elements in the rights charter with the operational practice to ensure that the delivery of the rights were hard-wired into the operational practice.

I believe that this document meets the brief at this first stage of developing an Identity Rights Charter. It also appears to me that the principles we address in this document should be ubiquitous to any government department that faces the challenge of implementing significant policies that have to be underpinned by substantial data systems. Any department that incorporates these principles into the fabric of its operations is likely to benefit in terms of transparency and clarity of purpose, and also in setting out the responsibilities of government and the rights of the citizen. Clearly this will have benefit for IPS but it also seems to offer an opportunity for IPS to provide leadership in this area for other areas of government.

BACKGROUND ON INFORMATION RIGHTS AND PRIVACY

Information rights are granted by statute (e.g. the Data Protection Act 1998) but, to the extent that they relate to the protection of privacy, are underpinned by human rights legislation (e.g. the Human Rights Act 1998 and the European Convention on Human Rights). Safeguarding these rights is important not only for the individual, but for society as a whole. Privacy is a value that is built into our concept of the civilised society in which we wish to live.

Privacy is also a condition that enables people to engage in transactions with organisations, and in social and political relationships with others in circumstances where personal information flows across the public and private sectors. Those engagements would be difficult or impossible without the ability of people to protect their privacy, or to have it protected by law or other collective means. This is because the trust that is necessary for these relationships depends in considerable part on the confidence that people have that their personal details are not collected or used in ways that they cannot know about, control, or have regulated on their behalf. Information security is vitally important, but it is only one of the required elements in a system of privacy protection. Privacy and information security are often wrongly regarded, at least colloquially, as the same. They are not the same. They are very distinct and different aspects of personal data protection. Technical solutions need to be supported by systematic organisational and procedural safeguards that are guided by principles of privacy protection and the minimisation of surveillance.

The Identity Rights Charter (with associated Guidance and Code of Conduct) is inspired by these considerations, and by specific rights. It aims to embody them in detailed terms that outline the rights, obligations and responsibilities of individuals and public or private bodies. Although it has no binding force, it is intended to make explicit both the nature of the social contract between government and citizens and the tacit agreements that exist about the use of personal data. In conjunction with existing legal requirements placed on those who collect or use personal data and effective information governance. It is intended to embody the key points in a compact between organisations that individuals have good reason to expect are upheld in this country. The Charter aims to make a significant contribution to the understanding of how personal information associated with and used to determine identity should be protected by organisations and individuals alike, and to the practical ways in which safeguards can be implemented.

THE PURPOSES AND OBJECTIVES OF A UK IDENTITY[1] SCHEME

The Identity and Passport Service (IPS) is the UK Government's National Identity Provider. It provides identity assurance for all UK citizens (identity subjects) through the provision of passports and identity cards. The IPS also issues identity cards to EU and EEA nationals resident in the UK. The United Kingdom Borders Agency (UKBA) issues identity cards to foreign nationals from outside the EU and EEA who are legally in the UK. For this purpose the National Identity Service provides linkage between citizens and separate biometric and biographic data bases via these tokens. The relying parties are principally foreign governments and

[1] For an explanation of what is meant by identity see Annex A

all UK Government entities, but particularly UKBA, law enforcement agencies and organisations dispensing entitlements reserved for UK citizens and legal residents. The IPS may also seek to be an Identity Provider to other commercial and third sector relying parties.

While there is a need for clarity about the purposes and objectives of the identity scheme, there is clear lack of coherence about the purpose(s) or objective(s) of the scheme and of the principles that will govern data handling and privacy issues associated with it.

The initial declared purpose was for the UK to comply with European requirements relating to the warranting of cross-EU border contracts and transactions. Between then and the passing of the Identity Cards Act 2006 a variety of other purposes have been cited. IPS most recently stated the purpose of the National Identity Service as; "providing the most convenient, secure and affordable way of asserting identity in everyday life"

When making each of these statements of purpose the government made different tacit agreements with the population about the way in which it would handle, store and use the data provided by individuals. Breach of such tacit agreements related to the final stated purpose(s) will seriously undermine public confidence in government data systems.

The IPS has responded to the changing political and policy landscape with an evolutionary work programme. While this is a pragmatic response to circumstances, there are risks as different objectives may raise different privacy, security, governance and operational issues that may not necessarily be adequately addressed within an evolutionary mindset.

The utility that government has suggested to individuals for the identity scheme is that the token provided by the scheme (the card) will enable people to demonstrate that they are an individual with the right to access certain goods and services for which they have an entitlement, usually as a result of their citizenship or UK residency. Biometric identifiers are associated with the identity card (and will also be associated with passports after 2011) to reduce the risk of people applying for multiple identity documents for illegal (mainly fraudulent) purposes and to increase the confidence that the bearer of the token is the individual to whom it was issued (by verifying the biometric at point of use). This, in itself, is complex and the issues are more fully covered in Annex A.

While universal holding of passports would achieve the same aim as an identity card it is unlikely that universality could be achieved. The identity card is expected to cost the individual less than a passport, giving it a price advantage. There may also be an advantage to the individual in having a card as a token (in addition to or instead of a passport) as it can more easily be used in electronic transactions (since it could be used with an authentication device in the same way as a chip and pin or magnetic stripe card).

Currently the government holds information on its citizens in a variety of settings. In most cases the information is linked to simple biographical data that identifies

individuals. In many cases it may only be useful when there is a clear link to an individual. At the instant of use, however, the need is to be certain that the token relates to the person presenting it, and there may be no need, at that time, to link back to biographical data. In establishing such entitlement databases the government must consider the purposes to which the data will be put, and the means of identifying the individual to whom the data refers in a secure and accurate manner.

Most databases contain personal information. This may have been given in ignorance or in haste. In other cases it may have been given voluntarily or after specific consent to record and store data. When giving the data individuals (data subjects) should always be informed of the purposes for which it may be used, how it will be stored and their other rights under data protection law. Individuals may decide to give information because of the benefits such disclosure will give them. For example they may give their personal data to the IPS to get a passport so they can travel, or to the NHS so they can benefit from healthcare.

Government departments are required to collect and process information according to the Data Protection Principles, and to use that data in a manner which complies with the spirit as well as the letter of Data Protection law. IPS describes its guiding principles as;

- You (that is the citizen) will provide the information at the start of the process and be able to ensure its accuracy;
- You will be able to check the record we hold and correct any inaccuracies;
- We (that is IPS) will store the information needed to identify an individual and to meet the statutory purposes under the Identity Cards Act 2006;
- We will make it easy for you to keep us up to date with any change in your information;
- Your subject access rights to your information under the Data Protection Act 1998 remain;
- Transactions involving the NIR must be done with your consent except in very limited circumstances principally involving national security or crime; and
- There will be a full record kept of information held which is changed or provided, which will be available to you in accordance with your subject access rights under the Data Protection Act 1998.

What does data sharing mean in terms of the IPS scheme? The DPA defines data disclosure (which is now commonly described simply as data sharing) as "disclosure of the information or data by transmission, dissemination or otherwise making available"[2]. In practice this means that identifiable personal data will be disclosed for uses other than those for which it was given where that is legal, necessary and proportionate to the gain. Government does not have carte blanche to disclose data to whomever they wish. They are bound by the DPA and by the social compact that exists with the public who provide data for specific and defined purposes – such as obtaining the token of identity.

[2] Section 1 (1) of the Data Protection Act 1998, under the definition of processing (c); also at 1 (1) (2) (b) of the Act where it says "using" or "disclosing", in relation to personal data, includes using or disclosing the information contained in the data.

It is also clear that government departments share data, with other departments, relating to the identity of individuals, for a variety of purposes. This is not always explicitly explained to individuals at the time of the collection of personal data. It is often for the efficient execution of Government data processing rather than the benefit of the individual – frequently using approved gateways between Government data bases. It is unclear whether the data subjects are aware, when they give data, about all the purposes to which it may be put and the extent to which it may be shared with other government departments. For example, there is currently no information in passport application forms that the information may be shared with other government departments. This raises questions about compliance with the DPA. It is essential that this lack of clarity does not extend to the identity card scheme or any other form of identity authentication by Government.

As a point of principle it is unsatisfactory to have any system where a department (or even government as a whole) can act as judge and jury on whether it is compliant with standards of legality, necessity and proportionality (and particularly the last two where the assessment may be a matter of opinion).

For the above reasons the principal purpose(s) of the identity scheme must be clarified and remain unchanged after that clarification.

If the purpose of the identity card is **only** to provide citizens with a means of demonstrating their **citizenship or legal status** in the UK, that leaves the card or token holder free to use the card for other purposes as s/he chooses, accepting that in doing so s/he might be revealing stored information to those accepting the card as proof of citizenship/ legal status.

If the purpose is to enable **all** Government Departments, Agencies and third party suppliers to assure the identity of individuals and to link applications for entitlements or services to personal information about the individual, those applying for cards must be informed, as this changes the purpose and use under data protection law. Seeking information from individuals requires clarity about the nature of the information that is necessary, which links directly to the purpose for which it is sought, and then on to the uses to which it will be put.

Many individuals are content to share potentially sensitive personal information with a limited number of people, but expect that sharing will not go beyond a core group. The government has a responsibility to ensure that there is clarity about the limits to data sharing, including the principles under which data sharing is managed.

There are arguments about whether all data sharing between government departments is legal or not, since the right to share data for the purpose of the efficient working of government has not been legislated in some areas. It is certainly possible that government could, by statute, make the legality beyond question in all circumstances. What is clear is first that this raises serious ethical questions; it breaches the social contract made with individuals about the use of their data. Such breaches will undermine public trust in the system and lead to

increasing reluctance to share data with any government department; government has to be seen to respect the rights of individuals to act autonomously in relation to sharing their personal data. In addition, it is not clear that there is public understanding of such sharing, and this potentially leads to breaches of trust.

The result of the lack of coherence about purposes, and of confusion about the principles under which gathered data will be used, may lead to the misuse of personal data and loss of public trust.

Recommendation 1
Government must produce clear information about the purposes of the Identity Card Scheme including whether it is meant to underpin the accuracy of other government databases. It must also set out what data will be available to those reading identity cards, or passports or relying upon them, or how it will ensure the privacy of personal data at this point.

Overview of Identity Management Principles, Rights and Responsibilities

Identity rights and responsibilities are context sensitive. Different trust models and governance structures, including the rights and responsibilities of all parties, are appropriate in different circumstances.

In the digital age, it is easy to create and store data, including personal data. This makes practical obscurity a thing of the past and creates new challenges for the state and the individual in maintaining a level of privacy that all citizens find acceptable. It also means that the state and others holding personal data see benefits (of efficient service delivery and citizen choice) in accessing and sharing personal data for many purposes. When personal data is held and shared for reasons of national security and crime prevention the acceptable balance between security and privacy differs from the test of proportionality needed for commercial or social activities.

In considering rights and responsibilities of provider, subject and relying parties in identity management it is vital to consider:

- the totality of what is being held secure,
- the purposes for which the identity needs to be assured,
- the consent to access and use the personal information associated with identity given by each of the parties to any transaction or contract,
- the governance and accountability of all the parties.

Principles for Government associated with Identity Management

The government has a responsibility to protect its citizens from having their rights removed by others (be they other individuals or the State). The trust of the governed may depend on how well Government protects their rights.

Citizens retain rights to identifiable personal data that constitutes personal identity.

Information about citizens should remain under their individual control.

Citizens have to accept that some personal data may be needed for some State functions to be performed.

Citizens should not be asked to prove their identity unless it is necessary, and when it is necessary this proof should be achieved by accessing the minimum personal data possible.

Government should not give to others or use the personal data associated with personal identity without the consent of their citizens except for defined legal purposes (principally defence and criminal justice). This means that citizens must normally be given the choice of opting in to plans to extend access to and share their personal data beyond what they agreed to at the point of original data capture, unless there are overriding lawful reasons for this extension.

Government must be transparent in their dealings with citizens concerning their use of information collected for the purpose of identity assurance and authentication, respecting their rights to privacy.

Government must ensure that citizens are not discriminated against or socially excluded as a result of their approach to identity management or authentication.

Recommendation 2
The IPS should adopt the principles identified above, as a minimum, in any Identity Rights Charter

RIGHTS [3] AND RESPONSIBILITIES OF THE IPS AS AN IDENTITY PROVIDER

The IPS has the responsibility to register Identity Subjects, including confirming claimed identity and linking an individual to their biography with biometrics and electronic credentials.

The IPS must ensure that there is nothing in the design or operation of the identity scheme that excludes or prejudices any individuals or groups. Effective alternative measures must be in place if everyone's needs cannot be accommodated in the scheme (e.g. through disability, age, failure to update their biometric template frequently enough, all types of system malfunction, etc.).

The IPS has responsibilities to ensure the integrity, confidentiality, availability and non-repudiation of the identity data it holds.

The IPS must demonstrate clear accountability for its policies processes, staff and actions in relation to identity management. (This should be expanded in a published Code of Conduct, Guidance and associated training).

The IPS has the responsibility to repair an individual's identity, where the registration or credentials have been compromised or mistakes identified, with fast corrective action.

The IPS is responsible for redress to the Identity Subject if compromise of the individual's identity is the fault of the provider, with fast corrective action.

[3] Some of the Rights listed are rights in law, others are not

The IPS has the responsibility to ensure that the consent of the Identity Subject has been secured for all purposes for which the data is subsequently shared or used (other than where they are legally obliged to pass personal data on to government bodies).

The IPS should not reveal personal data in situations where the Relying Party does not need to know the identity of the subject to provide the service (e.g. the service provider simply needs to know if the subject falls into a specific age bracket or resides in a geographic area).

The IPS has responsibilities to all Relying Parties that should be clearly specified in the contracts with those Relying Parties (these will differ widely according to the use and purpose of the identity authentication and transaction(s) involved).

Rights and Responsibilities of the Identity Subject

Identity Subjects have the right to multiple identities, assured by multiple Identity Providers of their choice.

Identity Subjects have the right to anonymity. However, they must accept that if they choose not to assure their identity with a designated Identity Provider, in some situations, they will be unable to gain specified benefits (e.g. the right to cross border travel).

Identity Subjects have the right to obtain a copy of the personal information that the Identity Provider holds on them and to have incorrect or out of date personal information corrected by fast corrective action.

Identity Subjects have the right to fast redress that is proportionate to the harm they suffer if the Identity Provider is at fault in compromising their identity.

Identity Subjects have responsibilities to provide accurate data to the Identity Provider and to assist in the maintenance and repair of that data as it changes over time.

Rights and Responsibilities of the Relying Party

Relying Parties have rights and responsibilities which will vary according to context and contract. They are not covered in this document.

Recommendation 3
The IPS should set out the rights and responsibilities of the IPS as an Identity Provider, of Identity Subjects and Relying Parties relevant to each and all of the purposes for which the Identity card will be used.

Recommendation 4
IPS should produce a Code of Conduct, Guidance and training for staff in the IPS to ensure understanding of Identity Rights, privacy and the management, associated processes, governance and accountability in the Identity Card Scheme.

ANNEX A - WHAT IS MEANT BY IDENTITY

- A *person* is a human uniquely identified by their *biological identity*
- *Biometrics* can identify a person with reasonable confidence but never with certainty. Both false positives and false negatives will occur, and reducing the probability of one type of error will often increase the probability of the other type of error.
- *Biographical details* such as a person's name do not usefully identify them. If identity is established biometrically, it should be permissable for people to have multiple identity documents in different names.
- When we *identify* someone, we establish that they are the same person as the person who did something at a different time.
- What we use to identify someone therefore depends on what evidence we have from that other time, and what error rate is tolerable.

In their paper *Identity and its Verification*[4]*,* Bohm and Mason describe identities in this way:

> *Human individuals have continuity of personal existence: you are today the same person you were yesterday, and indeed you remain all your life the same person you were on the day of your birth, despite the many changes that have occurred in you since that day.*

We might call this your **biological identity.** In this Annex, when we use the word *person*, we mean a human individual uniquely identified by their biological identity.

Your biological identity is subjectively obvious - you yourself know who you are, most of the time - but it is far harder to establish biological identity objectively. In fact, it seems a meaningless question to ask "what is your biological identity". In all cases, the required question turns out to have the form "are you the same person as the person who ...". In other words, as Bohm and Mason say, the key question about establishing identity is *identity with what?*

For example:

- a bank needs to know whether the person withdrawing money from an account is the same person who set up the account or who was subsequently authorised to operate it;
- a border control officer needs to know whether the person in front of them is the same person to whom the passport they are carrying was issued;
- a court needs to know whether the person they are sentencing is the person who committed the crime;
- an employer needs to know whether an applicant is the same person as the one to whom the documents giving right to work in the UK were issued (and similarly for example for driving license, tax code, and security clearance);

4 *Computer Law and Security Review,* Vol 26, No 1, January 2010, pp 43-51.

- a mother needs to know whether that baby is the one that she gave birth to yesterday;
- and so on, endlessly.

Even in the extreme case of gender reassignment, where the person might say "I am not the person that I used to be. That was someone else", they will still accept responsibility for the past actions of their former self, and society requires them to do so. Continuity of biological identity is fundamental to society.

Therefore when we use the phrase "*identify* someone" it means "show that a person who did one thing (such as withdrawing money from a bank account) is the same person who did something previously (such as opening the account)".

PERSONAL ATTRIBUTES

A person has many *attributes*: name, address, date of birth, gender, mother's maiden name, place of birth, DNA profile, fingerprints, iris pattern, facial geometry, gait etc. Are these unique and unchanging, as we have said that biological identity is? If so, can they be used to identify someone?

BIOGRAPHICAL ATTRIBUTES

Attribute	Unique?	Unchanging?	Could identify?
Name	No	No	No
Address	No (possibly in combination with name)	No	No
Date of birth	No	Yes	No (even if it was unique, there is no way to tell that the person in front of you has a particular date of birth).
Gender	No	No	No
Mother's maiden name	No	No (she may have had several names before getting married and – if never married – may have changed her name subsequently)	No (It is usually public information)
Place of birth	No	Yes	No

While it is clear that the properties of most biographical attributes are well defined, (as the Table above shows) this is less the case with biometric attributes. Biometric attributes, however, have the advantage of being directly bound to an individual and, with some caveats, may generally provide the uniqueness and stability for more reliable identification. This line of reasoning leads to the conclusion that *only biometric data can be used to identify someone* with a low

probability of error; that even biometric identification can only be used if the same biometric data was presented and recorded on the separate occasions for which identity is sought; and that even then there will be some probability of error. The error rate will increase with the passage of time, unless the biometrics are re-registered (this is known as *template ageing*). The whole area is difficult and complex and requires deep thought about false negatives, false positives and exception handling.

Combinations of attributes are commonly used to identify people. This can reduce the error probability, but only if the attributes can be established with confidence as belonging to a particular person.

It is common for a person to use several different names for different roles in their life, and this is lawful without any formality so long as it is not done for the purposes of criminal deception. Examples of people using multiple identities include:

- an actor or writer with a professional *nom de guerre*
- a married woman who uses both her married and maiden names
- a worker in the probation service who is required to use a new name to reduce the risk of being identified by offenders
- a person escaping an abusive relationship who wishes to reduce the risk of being found by the abusive partner

and there are many others.

It is therefore inconsistent to restrict a person to having identity documents only in one name, as this would require them to use the same name for every transaction where identity might be needed, irrespective of the part of their life, or role, in which that transaction occurred. As can be seen from the examples above, this could even lead to serious injury to an individual or their children. For consistency with common law and established behaviour, either identity documents should not reveal names, or it should be possible to obtain as many identity documents as you wish, in whatever names you choose.

ANNEX B GLOSSARY

AUTHENTICATION

The verification of an individual's identity.

BIOMETRICS

The unique physical characteristics that can be used to identify you. These include facial images and fingerprints.

BIOGRAPHICS

The facts and events associated to an individual.

CITIZENS

A legally recognised subject or national of a state or commonwealth.

CONSENT

The specific, informed and freely given agreement to the use of information.

DATA SHARING

There are two main sorts of information sharing. The first involves two or more organisations sharing information between them. The second involves the sharing of information between the various parts of a single organisation, for example between a local authority's various departments.

DATA SUBJECTS

An individual who is the subject of personal data

DPA PRINCIPLES

Schedule 1 to the Data Protection Act 1998 lists the eight data protection principles.

DISCLOSURE

The information or data by transmission, dissemination or otherwise making available.

FAST

The quickest period of time for a course of action that is deemed acceptable and reasonable between a citizen and identity provider

IDENTITY PROVIDER

A service provider that creates, maintains, and manages identity information and provides user authentication to other service providers e.g. UK - Identity and Passport Service.

IDENTITY SUBJECT

The citizen to whom an identity and associated identifying data relates.

Information Assurance

The term used to describe confidence in the processes of information risk management.

Information Security

Ensuring that information that is given by customers is stored, transported, disclosed and disposed of securely in line with organisational policy and procedures

National Identity Service

The National Identity Service (the NIS or the Service) – which was previously referred to as the National Identity Scheme – comprises identity cards, passports and the National Identity Register, and the supporting infrastructure.

Necessity

The state or fact of being required or indispensable

Privacy

The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.

Proportionality

Information used or disclosed is relevant and necessary (proportionate) for the purpose for which it is requested.

Relying Party

An organisation that uses citizens identity data as part of its provision of a service.