Report of a

PRIVACY IMPACT ASSESSMENT

conducted by the UK Border Agency

in relation to the

HIGH VALUE DATA SHARING PROTOCOL

amongst the immigration authorities of the

FIVE COUNTRY CONFERENCE

Table of Contents

1. The FCC Protocol - Introduction and overview

This Protocol will enable secure data sharing based on fingerprint checks between the UK Border Agency and its partners in the Five Country Conference (FCC) - the immigration authorities of Australia, Canada, New Zealand and the United States of America:

- the Department of Immigration and Citizenship (DIAC) in Australia;
- Citizenship and Immigration Canada (CIC) and the Canada Border Services Agency (CBSA);
- the Department of Homeland Security (DHS) in the United States of America;
- and Immigration New Zealand (INZ).

The FCC countries are bound together by many historical ties and a common language. Data sharing trials have shown they also share many common patterns of both regular and irregular migration, and that proportionate and targeted data sharing activity between the FCC countries to improve the effectiveness of our border and immigration management systems would provide real benefits to our citizens. This Protocol is a next step in this activity, which is in addition to and complements the existing procedures for data sharing which the UK conducts with its European partners.

Under this Protocol, each FCC country will securely and confidentially check an agreed volume (initially 3,000 per year) of fingerprint sets of immigration cases against relevant fingerprint databases of the other FCC countries. Each country will decide which of its immigration cases it will check under the Protocol, to derive best value. The UK Border Agency intends to use the Protocol primarily to check asylum cases where there is good reason to do so – for example, if the person cannot be identified or there is reason to believe the person may be known to another FCC country – and those foreign national criminals who are difficult to remove from the UK due to identity and documentation issues.

Fingerprints exchanged under the Protocol will be destroyed securely once the matching has taken place, and used for no other purpose. On cases where fingerprints are found to match, the countries will exchange such other information as is relevant, proportionate and lawful to exchange for their immigration and nationality purposes.

This will support the process of immigration control and provide benefits both to genuine applicants and to the UK public. Information from fingerprint matching assists the genuine applicant by helping to confirm his or her account, whilst protecting the public by identifying and assisting with removal from the UK of false applicants and people who pose a risk.

The information will be shared securely via a Secure File Share Server (SFSS) hosted by the government of Australia.

The UK Border Agency has decided to publish this Privacy Impact Assessment (PIA) report after considering the recommendations of the Cabinet Office Data Handling Review and having received advice from the Information Commissioner's Office, the Ministry of Justice, and other interested parties.

2. What is this document for?

2.1 What is a Privacy Impact Assessment (PIA)?

Projects that involve exchanging personal information inevitably give rise to privacy concerns. Indeed, the cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of corporations and government agencies alike. Privacy Impact Assessment (PIA) is a process which helps organisations to anticipate and address the likely privacy impacts of projects, in order that we can foresee problems, develop solutions, and ensure that concerns are addressed appropriately. For this reason we have followed a PIA process whilst developing the arrangements for the FCC Data Sharing Protocol.

2.2 What does this PIA report cover?

This report sets out how the arrangements for the Protocol will operate, and how its operation can be expected to relate to the privacy of the individuals whose information is exchanged. This includes assessment of the arrangements for the central server through which the information will be exchanged, of the arrangements which each of the participating countries has put in place internally for processing the information, and of the overall adequacy of the data protection arrangements.

A previous version of this report was published on initial implementation of the Protocol between Australia, Canada and the United Kingdom. A second version was published on implementation of the Protocol with the US and this final version has been updated to reflect forthcoming implementation by New Zealand.

2.3 How have we conducted the PIA?

We have sought to examine the arrangements both objectively and from the point of view of the individual, to ensure that we meet the legitimate expectations of people whose information is exchanged.

In assessing the impacts and developing the arrangements, we have been informed by previous trial activities, and by the responses of people whose information has been shared in those trials. We have consulted a number of interested parties, in particular the Information Commissioner's Office, whose guidance has been extremely helpful, as has the assistance of the Ministry of

Justice. Our colleagues in the other FCC countries have also been assessing the privacy impacts of the arrangements, and we have worked closely together in developing them.

The arrangements reflected in this report are the fruits of these processes. We have found these processes useful to follow, and believe that the arrangements that we have put in place for the FCC Protocol demonstrate good practice in data sharing and protection, striking a fair balance between protecting the privacy rights of the individual and the interests of the wider public.

2.4 What type of PIA have we conducted?

The PIA process is relatively new in the UK. To date, it has largely been used in connection with new projects to collect and store personal information. We are not aware of its previous use in the UK in relation to international information exchange projects of this kind, where many of the privacy issues and risks manifest themselves in different ways than they do in projects related to new databases. We have therefore followed the general guidance of the Information Commissioner's Office in undertaking this process, and sought specific advice on how it can best be applied to this type of project. We hope this report reflects that this process has been effective.

In deciding whether to conduct a PIA, and what type of PIA to conduct, we considered carefully the nature and scope of the FCC Protocol proposition, and its potential to impact on the privacy rights of the individual, in particular that:

- the project does not involve the introduction of new legislation, or present a new policy area. Concepts and practices of data sharing based on fingerprint checks for immigration functions are already well advanced in other contexts, for example across Europe through the Eurodac system. However, whilst this project largely builds on such initiatives, it does contain new features, whose privacy impacts need to be understood and any adverse impacts minimised;
- the project does not involve collecting or storing new data from individuals, but it does involve new arrangements for exchanging personal data (including some sensitive personal data) with authorities of different countries. The ability of Her Majesty's Government to control the use of that data may therefore be diminished, or at least perceived to be diminished;
- the data will be used for limited purposes that are already well established, namely immigration and nationality purposes, which are generally the same as or similar to the purposes for which the data was originally collected. Nevertheless, these purposes involve inherent sensitivities;
- the project involves data sharing on a case by case basis, based on anonymised fingerprint matching, rather than bulk data exchange;
- the other countries with which data will be shared are outside the EEA and therefore not bound by European data protection legislation. It is therefore

important to find other ways to ensure that the rights and freedoms of data subjects are respected; and

- each of the countries participating in the project has committed to developing clear arrangements for how it will operate and how privacy risks will be minimised, with the guidance of privacy experts in each country. Having such arrangements in place should in itself be a major factor in mitigating the privacy risks, and the PIA process should help make sure they do so.

On the basis of our assessment and advice received, we decided to follow a small scale PIA process for the FCC Protocol arrangements. This is because the project had privacy issues associated with it, but not the large inherent risks that would warrant a full scale PIA, for example those typically associated with new policy areas, major new databases, or using data collected in connection with one purpose for very different purposes. Nevertheless, we found that a substantial range of issues emerged, and we expanded our approach to ensure that those issues were all addressed appropriately.

2.5 Is this report the end of the PIA process?

No. We decided to publish this report on the UK Border Agency website in order to increase transparency and public understanding of this activity. We would also appreciate any comments readers may have, either on the FCC Protocol itself or on the extent to which this document achieves its purpose. In particular, any suggestions on how we could improve our approach in future would be most welcome.

We and our FCC partners will closely monitor and review the Protocol's operation, including ongoing review of the privacy impacts, and monitoring compliance with the specific privacy and security arrangements. This will help us ensure that the Protocol continues to support the process of immigration control and provides benefits both to genuine applicants and to the public which outweigh any adverse impact on the privacy of individuals. Feedback would assist the review process. We will update this document, and publish updated versions, to reflect future developments.

3. What is the Five Country Conference Protocol for?

3.1 The immigration context

Immigration is one of the top concerns of the public in the United Kingdom. In some polls, it has been the number one issue, higher than the economy, and law and order. Two thirds of UK adults say that laws on immigration should be much tougher and nearly half say their biggest concern is pressure on public services and jobs. However, the public also want a system that meets the country's needs

for migration, and is compassionate to those who need our protection. The UK Border Agency is responsible for pursuing and balancing these objectives.

An important aspect of this task relates to identity management of foreign nationals coming to the UK. The public are heavily reliant on the UK Border Agency to ensure that the people who come into the UK are who they claim to be, and can readily be identified as such. This is important not just in immigration terms, but to protect the public and their services against all kinds of risk. We have deployed a wide range of capabilities to help us do this, such as the biometric visas we now issue globally.

The UK has one of the strongest immigration controls in the world. Nevertheless, as with all other countries, the international nature of migration and absence of globally joined-up solutions mean that some of our functions within the UK are exercised without having the sorts of information that we would require from an overseas applicant. In particular, within the asylum and enforcement processes we regularly encounter people who are unable to substantiate their claimed identity or account, for which we may have no previous record to check.

This presents serious issues both for the individual and the public. Asylum seekers in genuine need of protection would benefit from an enhanced ability to verify their credentials. Equally, there are strong public protection reasons for wanting to enhance our ability to identify claims that are fraudulent, or applicants who are not who they say they are. And the unsuccessful claimants who are presently difficult to remove from the UK because we do not know who they are or, sometimes, even to which country we should be removing them, will be able to be processed far more effectively with the aid of international capabilities to verify their identities.

3.2 Five Country Conference activity

These issues can only be addressed internationally. As well as working with European partners, we have been working with our FCC partners to scope the issues and to develop proportionate solutions. FCC data sharing trials, based on exchanging biometrics in an effectively anonymous manner, and then sharing data on the cases where biometric matches are achieved, have shown that substantial opportunities exist to improve our abilities to address the patterns both of legal and illegal migration that affect our countries.

Checks on visa applicants have shown largely compliant patterns of behaviour within this population. However, trials with asylum and enforcement populations have consistently shown high levels of abuse as well as legitimate activity. For example, fingerprint checks of 30,000 UK asylum cases against US Department of Homeland Security data provided fingerprint matches on 429 cases (1.43%), and high value findings on the great majority of these. 63% of cases had given a

different identity to the UK than the identity known to the US. 29% of cases also presented a different nationality. The US was able to supply a verifiable identity for 63% of cases which could (if appropriate) be used to re-document and return the person to country of origin. 89% of matching cases that were claiming asylum as unaccompanied children had given details to the US indicating they were adults. There were also many other relevant findings, such as whether the whereabouts of a person when fingerprinted by the US authorities tallied with their claim.

The proportion of cases which achieve a fingerprint match varies between countries and increases over time. For example, whilst the above trial achieved a 1.43% match rate overall, the more recent cases within it achieved a match rate of around 3%, and another trial of searching Canadian asylum fingerprints against the UK system achieved a match rate of 3.5%. Checking fingerprints across the FCC countries via the Protocol will provide a higher combined match rate, which will also increase over time alongside the expansion of immigration fingerprint holdings.

It should be stressed that the figures from the example trial above relate to asylum and enforcement cases where fingerprint matches were achieved between the UK and US, that is to say, they were known to both countries. These are not representative of asylum and enforcement cases more generally, not least because the people concerned predominantly have travelled by air between continents - a very different pattern to those who migrate through Europe by land and sea. The capabilities we are developing across the FCC are complementary to and a logical extension of the checks we already conduct with our European partners.

These findings also reflect opportunities presented by recent capability advances: for example, collecting fingerprints of asylum seekers has been well established for some years, but the ability to use these to establish a true identity rests on cross-checking with more recent advances such as biometric visas, as people will have produced their passports in connection with their visa transactions.

3.3 The Protocol as next step

This Protocol is a next step in FCC activity. It will enable each country to check 3,000 sets of anonymised fingerprints per year against the other FCC countries, and share appropriate data on matching cases, for use for immigration and nationality purposes. The data will be shared via a fully accredited Secure File Share Server hosted by Australia. As fingerprints will be checked on a request basis, each country will (within parameters) decide which of its cases to check, thus obviating the need to check bulk samples and enabling each to derive best proportionate value.

In the UK we intend to derive best value by using the Protocol primarily for asylum cases where there is good reason to do so – for example, reason to believe the person may be known to another FCC country – and for foreign national criminals who are difficult to remove due to identity and documentation issues. We expect to derive the following direct benefits for data subjects and the UK public:

- better informed decision making, hence greater confidence that genuine applicants who need our protection will be successful whilst fraudulent applicants will be refused;
- increased ability to remove foreign criminals and failed asylum seekers from the UK, by linking them to their true identities and travel documents;
- harm reduction by identifying and enabling action on cases that present risks to the public, such as through identity fraud or where they are known to be dangerous criminals;
- savings to the UK taxpayer, by ending expenditure on people who consequently leave the UK and by withdrawing public services from people who are not entitled to them. This includes for example costs of foreign criminals in British prisons, asylum support costs, and NHS costs of those who falsely claim asylum to access free NHS treatment; and
- improved child protection, for example by validating the ages and identities of those seeking to access UK child care services.

The Protocol will deliver specific benefits both to the genuine applicant and to the public. Information from fingerprint matching that is consistent with a person's account is seen as supporting evidence for their claim, thereby assisting the genuine applicant, whilst information that contradicts their account needs explanation. The UK Border Agency believes that the Protocol represents a proportionate step, which is necessary in view of pressing social needs and strikes an appropriate balance between safeguarding the private lives of the individuals concerned, protecting the public and meeting public expectations.

Whilst operating the Protocol we will also continue to develop more systematic solutions for the longer term. Each of the FCC countries is implementing biometric immigration capabilities, but we are at different stages in rolling these out. The Protocol provides a flexible arrangement by which we can derive good value for each of our countries during that rollout. Once there is greater consistency in our biometric capabilities we intend to implement arrangements for systematic biometric checks of appropriate immigration cases across the FCC countries.

4. What does the FCC Protocol involve?

4.1 The data sharing conundrum

People are naturally concerned to ensure that there is an appropriate balance between the individual's right to privacy and the state's need to share data in order to carry out its functions effectively. People often have very different perspectives on where this balance should lie. Whilst the great majority of people agree that government agencies should share relevant data to an extent that is necessary and proportionate for their purposes – which is also the basic essence of UK data protection law – what this extent actually is in practical terms is often hotly debated. In many ways this is because of the effect of what we might call the 'data sharing conundrum':

"Government agencies should share data that is relevant to their purposes. However, it is impossible for them to tell what data will turn out to be relevant, until they have shared it. What then, should they do?"

Data sharing initiatives can therefore involve sharing a relatively substantial amount of data in order to find relevant nuggets within. Whether the data sharing is seen as justifiable is likely to depend on how many, and how valuable, those nuggets are, in comparison with the totality of the data sharing. The broader the data sharing, the more intrusive people will find it to be and the more value they will expect it to provide before they consider it to be justified. It is therefore important for Government agencies to ensure they target their activities to derive the maximum benefit for the public from the minimum data sharing, as a matter of public trust as well as legality.

4.2 What approach have we taken in the FCC Protocol?

In developing the FCC Protocol, we and our partners were anxious to ensure that our approach to the 'data sharing conundrum' provided greatest benefit for our immigration controls with minimum intrusion. We examined on all levels how this could be done, and arrived at the following proposition:

- the Protocol will be used only to check immigration cases of types which present the highest value in doing so, in particular asylum and enforcement cases, and will not be used to check nationals of the UK or other FCC countries (see section 4.3);
- checks will be based on nigh anonymised fingerprint matching, so that otherwise identifiable data is only shared on cases where fingerprint matches occur, between the two countries that have a legitimate interest in the individual (see section 4.4);
- on the cases where matches do occur, a Search Code Guide will be used to identify data for sharing only to the extent that is necessary for the specific type of case (see section 4.5); and

- checks will only be made against relevant databases of the other countries (see section 4.6).

We believe this multi-layered approach ensures as far as possible that data will only be shared where it is directly relevant to the case in question.

4.3 Whose information will be exchanged?

The Protocol will enable the immigration authorities of each FCC country to check the fingerprints of up to 3,000 immigration cases per year against the fingerprint systems of the other FCC countries. The countries may over time agree to increase the volume of fingerprint checks. Each country will decide which of its immigration cases to check using the Protocol, in order to derive best value from the arrangement. The arrangements provide that these cases are likely to include, but not limited to:

- immigration cases with an indication of derogatory activity or other associations of concern such that the person would be inadmissible to one or more of the FCC countries;
- immigration cases where the identity of the individual is unknown or uncertain;
- immigration cases where there is reason to believe that the person has been encountered by another of the FCC countries; and
- other sensitive immigration cases.

Each country has considered which types of case it intends to check using the Protocol. The UK Border Agency considers that we will derive best value for the public by using the Protocol primarily to check:

- people who are due to be removed from the UK, in particular foreign nationals who are in UK prisons, but where this is not presently practicable because we cannot sufficiently confirm their identity and/or nationality. Where another FCC country is able to confirm this, it will help enable us to arrange the person's re-documentation and return to country of nationality; and
- asylum seekers, where there is a particular reason to do so, for example because the person's identity is in question, or because the person is believed to have been known to other FCC countries. This will help to confirm or deny the person's claim and, where their claim is unsuccessful, to re-document and return the person to the country of nationality.

The other FCC countries intend to use the Protocol to check similar types of case in the first instance. There will also be other scenarios where there is good reason to use the Protocol. Each FCC country seeks to derive maximum value from the Protocol, and will therefore use it to check the cases which present greatest proportionate value. This has been informed by the trials we have undertaken, and we will develop our approach according to our experience of using the Protocol. However, we have also built in safeguards to ensure that

operation of the Protocol remains proportionate and does not stray from the purposes for which it was intended:

- it is limited to check on immigration cases (see above);
- the purposes for which shared data may be used, and the extent to which it may further be disclosed, are defined (see section 5); and
- the data that may be shared is defined (see section 4.5) to ensure that it does not go beyond what is relevant and proportionate for those purposes.

4.3.1 Will we use the Protocol to check our own citizens?

We have also agreed that the fingerprints exchanged for searching under the Protocol will **not** contain fingerprint data of known FCC nationals. Thus a national of the UK or another FCC country, who does not purport to be otherwise, may be assured that his or her fingerprints will not be searched under this arrangement. The only scenario in which the fingerprints of a FCC national may be searched under the Protocol is where that person is purporting not to be a FCC national. For example, one person whose fingerprints we exchanged during trials because he was claiming asylum in the UK as a Somali, was found to be an Australian citizen, who was wanted in Australia for rape. Identifying this enabled the UK Border Agency to resolve his asylum claim and return him to Australia. This is appropriate activity for immigration purposes.

In the case of the UK, this also means that we will not search fingerprints of known EEA nationals or their family members, who have free movement in the EEA and we would not therefore have an immigration reason to check their fingerprints outside the EEA.

4.4 How will the information be exchanged?

All of the data exchange will be conducted securely through a Secure File Share Server (SFSS). The arrangements for this are set out further in section 7.1 of this paper.

The data exchange will happen in two stages. In the **First Stage** nigh anonymised fingerprints will be transferred for the purpose of searching against the other countries' fingerprint databases. Only in the instance of a fingerprint 'match' being identified will the **Second Stage** data sharing take place, transferring biographical and other relevant data between the country that supplied the fingerprints and the country that identified a fingerprint match. Thus the first stage represents the effectively anonymous checking of fingerprints between the two countries, and the second stage applies to those cases where this yields fingerprint matches, that is to say, those cases which are already known to and whose fingerprints are held by both countries.

The **First Stage** of the intended transfer data will involve transferring nigh anonymised fingerprints. By 'nigh anonymised', we mean that whilst the

fingerprints do in themselves constitute personal data, and it is right to protect them as such, they are shared with no biographical data attached, and therefore it could not readily be ascertained to whom they relate. The fingerprints will be transmitted accompanied only by:

- a unique reference number, which in the case of UK fingerprints will be allocated as part of the exercise and only be identifiable to the UK Border Agency officials administering the Protocol. This is in order to be able to identify the cases on which fingerprint matches are achieved; and
- a search code to indicate the type of case to which the fingerprints relate, for example, an asylum seeker or foreign national prisoner. As different types of data are relevant to be transferred in different types of case, the search code is to enable a country that obtains a fingerprint match to ascertain what data will be relevant to transfer (in the second stage) in respect of that person.

A person whose fingerprints are checked through the Protocol may be assured that this does not present any significant risk to his or her rights and freedoms. The arrangements provide that:

- the fingerprints will be transferred securely in a nigh anonymous manner;
- the fingerprints will only be used for the purposes of matching against the relevant databases, and for notifying the supplying country of the result;
- the matching will be done and results notified within three days wherever possible; and
- the fingerprints will securely be destroyed as soon as the matching has been carried out (whether or not a match is achieved).

Thus the country which has received the fingerprints will not retain or use them for any purpose of its own. Where a country achieving a fingerprint match has itself a legitimate purpose connected with the fingerprint match, this will be considered in the second stage of data sharing, rather than by retaining or otherwise using the fingerprints.

Even in the unlikely event that the fingerprints were obtained by an unauthorised person, it is highly unlikely that the data subject would suffer any adverse consequences, as an unauthorised person would only be able to identify the data subject in the event that they themselves had access to a fingerprint database which already contained the person's details.

4.5 What information will be exchanged?

Where a fingerprint 'match' is identified, the **Second Stage** of the process involves the two countries concerned sharing relevant biographical and other data on a bilateral basis. Certain information will be shared as a matter of course, as it will always be relevant, whilst further information sharing will depend on the nature of the case.

The data elements that will be shared as a matter of course on matching cases (to the extent that they are available within the relevant country's biometric system), are:

- Date, location and reason fingerprinted
- Last name, first name, any other names
- Date of birth, place of birth, nationality and gender
- Travel document number
- Photograph, facial image, and/or scan of the travel document biodata page

These data elements provide information about the **identity** presented by the person and the **transaction** in which it was presented. Both countries concerned need the identity data to establish whether the person has presented the same identity to both countries. If the identity held by both countries is the same, this serves to add assurance that the person is who he or she claims to be. If different, the countries will need to consider what action or conclusions should flow from the discrepancy (for example, how to establish whether either or both of the identities is genuine). The transaction information is important in determining the level of assurance that may be attached to an identity, as, for example, identities presented by people bearing their passports whilst applying for visas will carry more assurance than identities presented in transactions which only reflect who the subject claimed to be at the time.

The countries concerned will share additional data, where appropriate, in accordance with an agreed Search Code Guide (SCG), which will specify what additional data (if any) will be shared as a matter of course. As different types of data are relevant in different types of case, the SCG assists in ascertaining what data will be relevant to transfer in any given case, according to the search code that was originally sent with the fingerprint searching request, and the nature of the information held by the country that identified the fingerprint match. This enables more effective and efficient data sharing.

The SCG also helps ensure that the data shared will be relevant and proportionate to the legitimate use, as the data sharing will focus only on those data elements that are pertinent to the specific type of case. For example, on types of case where the purpose of the check is purely to obtain the person's identity and passport details, the SCG sets out that no further data needs to be exchanged beyond these items. There are other types of case where the

person's history or current location needs to be confirmed, and the SCG sets these out.

Either country may also request additional information from the other on a case by case basis, and will provide sufficient reasons for such requests to enable the other country to determine the legality of disclosing such further information. In the case of the UK, we will only share such further information where we are satisfied from the reason given for the request that the further data transfer is proportionate and lawful. Information may only be exchanged to the extent that is relevant and proportionate to the countries' immigration and nationality purposes. These purposes are set out further in section 5 of this paper.

4.6 What databases will people be checked against?

The fingerprints that are exchanged will be searched securely against the other countries' biometric databases that are relevant to immigration purposes. These are:

- the Immigration and Asylum Fingerprint System (IAFS) in the UK, which is administered by the UK Border Agency;
- the Biometric Acquisition and Matching System (BAMS), in Australia, which is administered by the Department of Immigration and Citizenship;
- the Automated Fingerprint Identification System (AFIS) in Canada, which is administered by the Royal Canadian Mounted Police for their own purposes and on behalf of Citizenship and Immigration Canada and the Canada Border Services Agency
- the IDENT System in the USA, which is administered by the Department of Homeland Security; and
- the Immigration Biometric System (IBS), which is administered by the Department of Labour New Zealand

Some of these systems include both immigration and policing entries. The data that will be shared, however, will only be data that is relevant and lawful to exchange for immigration and nationality purposes, as set out in section 4.5. Each country is responsible for ensuring that the records it searches, and the information it discloses, supports this construction.

4.7 How will we know the information is accurate?

Each of the countries' fingerprint matching systems operates to a high degree of assurance. Potential matches are identified by the fingerprint systems and verified by appropriately qualified fingerprint examiners. In some systems, all potential matches are manually examined, whilst others differentiate between 100% certain automated matches that do not need further verification and less certain ones that are then manually examined. The outputs are acceptable as evidence in each of the countries' domestic courts up to and including the level of

proof required in criminal cases, a higher benchmark than generally operates in immigration matters. The accuracy of fingerprint matching has been the subject of much study which is freely available, and which we have not sought to replicate in this document.

There remain some issues about varying standards in different countries, and about the ability of an authority in one country to evidence a fingerprint match for the purposes of an authority in another country. For this reason, in the event that a fingerprint match is disputed, the fingerprints held on the database of the country which confirmed the match will be supplied to the other country, whose own fingerprint experts will re-examine both sets of fingerprints. Thus a person whose immigration case is being dealt with in the UK need not fear that he or she may be affected by a false fingerprint match provided by another country, which could not then be subject to scrutiny. Both sets of fingerprints would be available in the UK, the fingerprint match examined by a UK qualified examiner, and the fingerprint match and any conclusions following from it would be subject to the requirements of UK law.

There are some risks around the accuracy of the biographic information exchange on the cases where biometric matches are identified:

- data may be inaccurate because of errors in the source database;
- data may be inaccurate because it has been incorrectly transcribed; or
- data may be incorrectly interpreted by the country receiving it.

In trials, we have sought the best ways to mitigate these risks, and reflected these in the Protocol arrangements:

- each country will provide the other countries with an Interpretation Guide which explains how to interpret the information it will be sharing, including, for example, any quirks of its biometric system which need to understood by the other countries;
- all of the data exchange will in each country be handled by a central team, trained both on how to provide information to the other countries in a readily understandable form, and on how to interpret the information provided by other countries;
- the information which is exchanged on all matching cases will wherever possible be produced automatically from the relevant country's biometric database. This is information that has been captured during a fingerprinting encounter, whose accuracy and interpretation will be readily understandable from the information and the guidance from the country concerned. This further mitigates the risks to the accuracy of the information pertaining to the biometric encounter;
- other information to be exchanged in accordance with the Search Code Guide will be provided in an agreed and understood format. It will be restricted to clear, factual information and will not include any subjective

information that is liable to misinterpretation, such as the opinions of an immigration officer that had dealt with the case;

- each country will have an internal procedure for vetting and clearing any further information which is to be shared on a case by case basis. This will be the same procedure that will ensure that such sharing is proportionate and lawful; and
- the arrangements provide for co-operation between the different countries' central teams to liaise and correct any data that is found to be inaccurate.

4.7.1 Can I see and if necessary correct any information held about me?

It is important for the fair processing of people's information and for public trust that there is transparency in the arrangements. Whilst we have taken a range of steps to ensure that the data shared is accurate and is correctly understood, there always remains some level of accuracy risk. However, we have confirmed in our assessment of the other countries' data protection arrangements (see section 6.3) that each provides individuals with adequate rights to access information which is held on them, to correct any erroneous information, and for the opportunity to seek redress against breaches of the law. We have also specifically set out that no data may be exchanged under the Protocol which may not be disclosed to the individual to whom it relates.

Any issues concerning personal data provided by the UK to the other countries would also be actionable through the UK Border Agency under the Data Protection Act 1998.

The Protocol further supports our duty under the fourth data protection principle in the Data Protection Act 1998 to ensure that data is kept accurate and up to date. Checks made under the Protocol will help us to correct and update our systems. For example, where they show that an immigration offender believed to be in the UK is now elsewhere, we will be able to update our records accordingly.

5. How will we use the information that has been exchanged?

How information will be used is of as much legitimate concern to the public as how it will be collected, stored and exchanged. People naturally do not like to find that information about themselves which they have provided for one purpose then gets used for a very different purpose. In developing the FCC Protocol we were anxious to ensure that the information shared under it could only be used for our and our partners' proper purposes, as the immigration authorities of the FCC countries.

However, we also considered it necessary to ensure that we did not prevent ourselves from acting on the information in any of the ways that the public would rightfully expect. Wherever data that is shared indicates a need to take action in

line with our proper purposes and in the public interest, we need to be able to take that action. Precluding ourselves from taking proper and necessary action would be as great a disservice to the public as not having the information in the first place.

The remainder of this section explores how we have reconciled these objectives in the Protocol arrangements.

5.1 For what purposes will the information be used?

The fingerprints exchanged in the first stage of the process will only be used for the purposes of matching against the relevant databases, and for notifying the supplying country of the result, and for no other purpose. The information that is shared in the second stage of the process on the cases where fingerprint matches are achieved may then be used for any of the immigration and nationality purposes of the relevant FCC country.

'Immigration and nationality purposes' are defined in this context as 'the consideration, regulation and enforcement of whether, and on what basis, any person may enter or remain in the territory of one of the Participants.

These provisions are designed to allow only appropriate use of the information by each FCC country's immigration authorities, including assisting them to make accurate and informed casework decisions, and to remove unsuccessful applicants to their countries of origin.

The information that is shared in the second stage may also be used for determining the person's eligibility for public benefits or services which are connected with his or her immigration status. Thus if the information received indicated that a person who was being accommodated and supported by the UK Border Agency was not entitled to that support, we could act on that information to end such support. For example, trial exercises showed that several people who were claiming asylum and asylum support, had previously been granted asylum and citizenship by other European countries, but were fraudulently claiming in the UK as being their original nationality. The information was used successfully to end that support.

However, access to benefits and services would not in itself be a reason to check fingerprints through the Protocol. Fingerprints will only be checked through the Protocol for direct immigration and nationality purposes. Use of information received in relation to immigration-related benefits and services will occur where this is a necessary consequence in view of the information received.

5.1.1 Use in judicial proceedings

All of the relevant functions are potentially subject to judicial scrutiny in some form. For example, asylum decisions made by the UK Border Agency are appealable to the Asylum & Immigration Tribunal and further to the higher Courts. The Protocol arrangements explicitly provide for disclosure of the information shared in relevant judicial proceedings. Judicial scrutiny provides a fundamental safeguard for people's rights and freedoms in immigration matters. If any of the authorities using the Protocol made a wrong decision about a person based on information that had been shared – whether because the information itself was wrong, or a wrong conclusion had been drawn from it – the person affected would have the ability to challenge this in the Courts.

5.1.2 Use to verify identity and return to country of origin

Where identity and/or identity document information exchanged under the Protocol indicates that a person may be a national of, or have status in, a particular country, that information may also be disclosed to the relevant authorities of that country, for the purposes of verifying the person's true identity, establishing the provenance of the identity documents, and/or in connection with re-documenting and returning the person to that country.

For example, if a fingerprint match shows that a person claiming to be a national of country X was using a passport issued by country Y when he or she was encountered by another FCC country, it may be necessary to contact the authorities of country Y:

- to verify whether they genuinely issued the passport to that person, who is one of their citizens (as opposed to it being either a false document, or one that was issued to someone else), and
- if the person is confirmed as a citizen of country Y, to arrange new travel documentation for his or her return there.

Such disclosure is part of normal immigration processing. Using identity and travel document details which have been obtained from another FCC country for this purpose presents no more risk to the rights and freedoms of data subjects than disclosing similar details provided by the data subject, or obtained from another source. Therefore in this process the FCC countries will apply the same safeguards to the shared information as they do with other information used for these purposes. However, for additional clarity we have agreed two explicit restrictions on such use of the shared data:

- like other data shared under the Protocol, any such disclosure is subject to the appropriate human rights and other protection considerations (see section 5.4.1); and
- only identity and/or identity document information may be disclosed under this provision, and not other forms of information – such as about a person's

behaviour. Thus whilst a person who has concealed his true identity in order to avoid being returned to his home country can expect that identity, once uncovered, to be used for that purpose, this will not result in his home country finding out other information, which might potentially be more sensitive.

5.2 What organisations may use the information?

The full range of immigration and nationality functions are not carried out by a single agency in each of the FCC countries. For example, in Canada the main functions are divided between the Canada Border Services Agency (CBSA) and Citizenship and Immigration Canada (CIC). There are also circumstances where an immigration function may fall to a different authority – for example in the UK, the police may investigate and the Crown Prosecution Service may prosecute an immigration crime, and they would clearly need the relevant information to do so. The Protocol therefore provides that the authority receiving the information may disclose it to other appropriate domestic authorities that are responsible for pursuing immigration and nationality purposes. However, we have agreed some further safeguards to ensure that the need to share the data domestically will not provide a gateway for inappropriate disclosure or use:

- the data will only be shared for immigration and nationality purposes, and where necessary for the consequential immigration–related benefits and services adjudication (see section 5.1);
- the data will thus be shared only to the extent that the other authority has a need to know in order to carry out its official duties. For example, whilst information relating to a particular immigration crime being investigated by UK police may be communicated to them, data received under the Protocol more generally would not; and
- wherever one of the participants in the Protocol does share data with another authority, they will ensure that authority applies an equivalent level of protection to the information, and limitations on its use and disclosure.

5.3 Data exchange across the FCC countries

The Protocol provides that the information may only be shared between the country that requested the search and the country that confirmed the fingerprint match. It may not be shared across the other FCC countries. There may be occasions where multiple countries confirm fingerprint matches in relation to the same person. In such cases, the fact that there is a multiple match will be notified across the countries concerned, which will then arrange any necessary exchange of personal data on a bilateral basis. The exchange of personal data will thus be limited to the countries that have a legitimate interest in the individual.

5.3.1 Limitations on the above use and disclosure – protection of the data subject

All of the FCC countries are committed to protecting the human rights of data subjects, and to various international instruments which seek to protect those rights, specifically, the 1951 Convention relating to the Status of Refugees, its 1967 Protocol, the Convention Against Torture or Other Cruel, Inhuman or Degrading Treatment or Punishment and, in the case of the UK, the European Convention on Human Rights. Each FCC country has existing arrangements in place to prevent information being processed in ways which could lead to a person being persecuted.

For the avoidance of doubt, the arrangements for the Protocol also expressly prohibit the countries from exchanging, using or disclosing any of the information in any way such that the information could become known to any government, authority or person from which the subject of the information is seeking or has been granted protection under one of those instruments, or under their domestic laws implementing those instruments, or in any circumstances where, by virtue of the government, authority or person becoming aware of such information, the subject of the information may become eligible for such protection.

A person whose data is checked through the Protocol may therefore be assured that this will not enable his or her information to be communicated to any party from which he or she has a legitimate reason to fear persecution. This also means that, in the rare event where an issue of persecution by one of the FCC countries may arise, the person may be assured that the Protocol would not be used to check that person with the FCC country in question.

5.3.2 Limitations on the above use and disclosure – stipulation by providing country

Cases may arise where the country providing the information may not be able to allow its full use as set out above. This may arise, for example, where some of the information has been collected by another government agency and its further use is subject to the permission of that agency, or it has been collected in circumstances or for purposes with which the above uses would not be fully consistent.

For this reason, under the Protocol a country may in any case attach additional restrictions on the use or disclosure of information that it exchanges, which will be complied with by the country receiving the information.

The explicit exception to this is the area of subject access rights. A country may not attach a restriction preventing the information being disclosed to the person to whom it relates. A person may therefore be assured that his or her information will not be exchanged in a way that prevents him or her being able to see that

information in accordance with the subject access provisions of the relevant countries' laws. Further information on the rights of people whose data is exchanged is set out in section 9 of this paper.

5.4 Further use and disclosure

We have set out above the ways in which the information exchanged may, as a matter of course, be used or disclosed. No further disclosure or use of the information for any other purpose or to any other person may take place without the prior written approval of the country that supplied the information. In the case of the UK, we would not agree to such further use or disclosure unless we were satisfied that the proposed disclosure or use was lawful, and was consistent with the rights and freedoms of the data subject.

6. What is the legal basis for the information exchange?

This section summarises the legal basis for the FCC Protocol, including how the arrangements have been set out and agreed across the FCC countries, how the data sharing complies with UK law, and our assessment of why the data protection arrangements in the other participating countries are adequate.

6.1 How are the Protocol arrangements set out between the FCC countries?

The arrangements for the Protocol are set out in Memoranda of Understanding (MoUs) agreed between each pair of participating countries, supported by a suite of agreed business documents which relate to the practical arrangements for how it will operate. Wherever we refer to 'the arrangements for the Protocol' this means the terms and provisions set out in those documents, which are reflected in this report. The suite of documents currently includes:

- bilateral MoUs between each pair of participants, presently being Australia, Canada, the US, New Zealand and the UK's immigration authorities, setting out the general Protocol provisions;
- a Service Arrangement between Australia and the other countries which sets out how the central SFSS will be managed (section 7 explains);
- a Search Code Guide which sets out what information is appropriate to be shared according to the type of case (section 4.5 explains); and
- an Interpretation Guide from each country which explains how to interpret the information shared by that country (section 4.7 explains).

Although each participating country has its own systems and processes, we have agreed a consistent approach to the Protocol by which we can be confident that each participating country will operate it as is reflected in this report and the separate privacy documents which the other countries have produced in accordance with their particular requirements.

Although these documents are not legally binding, we can reasonably expect the Australian, Canadian, New Zealand and US governments to honour these arrangements in view of all the circumstances, and in particular, their stability and integrity, their close relationship with the United Kingdom individually and collectively, and our mutual interest in successful operation of the Protocol, which will be of benefit to each of our countries.

6.2 How is the FCC Protocol compliant with UK law?

There is no single source of law that determines when and how the UK Border Agency can share and use personal data. The principal considerations are:

- the UK Border Agency needs to have the power to share the data, either under statute or common law, and not be precluded from doing so by any other legislation or international obligation;
- the data sharing also needs to fulfil each of the following requirements:
  - comply with, or be exempt from, each of the eight data protection principles set out in the Data Protection Act 1998 (DPA);
  - comply with the Human Rights Act 1998 (HRA) and other human rights obligations; and
  - be consistent with our duty of confidence under common law.

6.2.1 What power does the UK Border Agency have to share the information?

As an agency of a government department headed by a Minister of the Crown, the UK Border Agency has broad common law powers to share data in connection with its immigration and nationality purposes, provided that such sharing complies with the other relevant legal requirements and is not expressly or impliedly prohibited by statute. All of the data sharing to be conducted under the Protocol falls within the ambit either of our common law powers or of specific legislation.

Some of the data disclosed under the Protocol is categorised as “personal customs information” as a consequence of the Borders, Citizenship and Immigration Act 2009 (“BCI Act”). This will include information (for example, a record of a person entering the UK) which may be relevant both for immigration and customs purposes, but which is known to have been acquired initially in the exercise of a customs function. It will also include information which is capable of being acquired in the exercise of a customs function in circumstances where it cannot be said that it was *not* acquired in that way. Such information will therefore only be shared under the Protocol where lawful to do so under the provisions of the BCI Act.

The UK Border Agency needs and is empowered to share data both inwardly and outwardly in connection with its immigration and nationality purposes. Our trials demonstrated the practical necessity of two-way data sharing, as both of the countries involved in a fingerprint match need to share data in order to receive the benefit, for example, by seeing whether the information known to each is consistent. It is also clearly necessary to share appropriate data outwardly with our partners as part of a reciprocal arrangement in order to serve the legitimate purpose for the United Kingdom. Further, a false identity used to penetrate another country's border can equally be used to penetrate the UK border, and it is directly in the interests of the UK to work together with other countries to identify false and compromised identities in order that they can be taken out of circulation.

There are no legislative barriers or international obligations preventing this activity. To the extent that international obligations relate to the Protocol, the arrangements provide for the activity to be carried out in accordance with those obligations – for example, section 5.4.1 sets out how the activity will comply with specific human rights obligations. More generally, the arrangements for the Protocol expressly provide for each participating country to comply with its domestic laws and international obligations.

6.2.2 How do the arrangements comply with the Data Protection Act 1998, and other legal requirements?

The Data Protection Act 1998 (DPA) sets out eight legally enforceable Data Protection Principles (DPP):

- 1st principle – fair and lawful processing. Section 9 summarises the issues in relation to how the Protocol arrangements are fair to the person whose data is being shared. This principle also provides that personal data may only be processed where one of the conditions in Schedule 2 to the DPA is met, and that sensitive personal data may only be processed when one of the conditions in Schedule 3 is also met. Some of the data to be processed under the Protocol will be sensitive personal data. However, the UK Border Agency's processing of data under the Protocol will go no further than is necessary for the exercise of its immigration and nationality functions. Accordingly, at least one condition in Schedule 2 and at least one condition in Schedule 3 will be met. Sections 4 and 5 of this document set out how the arrangements ensure that data may only be processed to the extent that is necessary for the exercise of these functions.
- 2nd principle – obtained for limited purposes and not further processed for incompatible purposes. Section 5 sets out how the Protocol provides for processing only for legitimate immigration and nationality purposes.
- 3rd principle – adequate, relevant and not excessive for the purpose. Section 4 sets out the multi-layered approach which will ensure, so far as practicable, that data will only be processed to the extent necessary for the legitimate purposes.

- 4th principle – accurate and up to date. Section 4.7 sets out how the arrangements will ensure the accuracy of the data exchanged, and its interpretation, and how this will support the wider accuracy of our data.
- 5th principle - not kept for longer than is necessary. Section 8 sets out the arrangements we have agreed for retention of the information.
- 6th principle – processed in line with rights under the DPA. The Protocol does not interfere with the right under section 7 of the DPA to make a subject access request to the UK Border Agency, nor does it otherwise contravene this principle.
- 7th principle – secure. Section 7 sets out the technical and practical arrangements to ensure the security of the data.
- 8th Principle – not transferred to countries without adequate protection. Section 6.3 sets out how we have assessed the adequacy of the data protection arrangements in our partner countries

As well as operating in accordance with the DPA, the UK Border Agency respects its duties of confidentiality and ensures that the human rights of people whose data is shared are respected. This includes both ensuring that the data sharing itself is consistent with people's rights – in particular the right to a private and family life under Article 8 of the Human Rights Act 1998 – and ensuring protection of the rights of people whose information is shared with our partner countries.

The maintenance of a fair and effective immigration control is a legitimate social aim which is necessary in a modern and democratic society. Sections 3-5 of this document set out why the UK Border Agency believes the FCC Protocol is in general a proportionate step to take, which strikes an appropriate balance between safeguarding the private lives of the individuals concerned and protecting the public. Information is shared only to the extent necessary for the specific purpose, and with appropriate protection in relation to onward disclosure or use.

An individual will only have his fingerprints disclosed under the Protocol if it is thought that value could be derived from that disclosure. Further information will be exchanged only where there is a match. Even if there is a match, only basic levels of information are shared automatically. Disclosure of more detailed information will only take place where it is relevant, proportionate and lawful in the individual case.

To any extent that this arrangement may interfere with an individual's right to a private life, we consider such interference to be proportionate to achieve our legitimate aim of upholding immigration control.

Equally, the duty of confidentiality is not absolute, and we consider it is outweighed by the public interest in checking fingerprints of relevant immigration

cases, and sharing relevant data between countries that have a legitimate immigration interest in the individual.

6.3 Are the other FCC countries' data protection arrangements adequate?

6.3.1 Why did we conduct an 'adequacy assessment'?

As all European countries' domestic legislation enshrines the rights and freedoms set out in European data protection law, we can have reliance on the adequacy of data protection arrangements within Europe. However, when considering sharing people's data outside the EEA, it is important for us to ensure as far as possible that adequate protection for rights and freedoms also exist in the countries to which we may be sending people's data. Specifically, the eighth data protection principle in the DPA prevents the transfer of personal data outside of the EEA unless either:

- the receiving country ensures an "adequate level of protection" for the rights and freedoms of data subjects in relation to the data processing; or
- the eighth data protection principle does not apply, by virtue of one of the conditions in Schedule 4 of the DPA being met.

One of the conditions in Schedule 4 is where the transfer of data is necessary for reasons of substantial public interest. We consider that data processing under the Protocol is necessary for reasons of substantial public interest, and that the 8th data protection principle therefore does not apply. However, as a matter of policy, the UK Border Agency seeks to ensure as far as possible the adequacy of the protection arrangements for data shared outside the EEA, rather than simply relying on exemptions. We have therefore assessed the data protection arrangements in Australia, Canada the US, and New Zealand and developed the specific arrangements for the Protocol with a view to ensuring their adequacy in all the countries.

6.3.2 How did we conduct the adequacy assessment?

We considered both the General Adequacy and Legal Adequacy Criteria in relation to these countries, in accordance with the UK Information Commissioner's guidance and in consultation with his office and the Ministry of Justice. We also checked our findings with our colleagues in those countries to ensure that our understanding of their arrangements is correct. In line with the DPA's requirements, in assessing adequacy we took particular account of:

1. the nature of the personal data;
2. the country or territory of origin of the information contained in the data;
3. the country or territory of final destination of that information;
4. the purposes for which and period during which the data are intended to be processed;
5. the law in force in the country or territory in question;

6. the international obligations of the country or territory in question;
7. any relevant codes of conduct or rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
8. any security measures taken in respect of the data in that country or territory.

6.3.3 What were our findings on the General Adequacy criteria?

We assessed the arrangements for fingerprint sharing in the first stage of the Protocol process separately from the arrangements for sharing biographical data in the second stage (see section 4.4), as the levels of inherent risk involved and the necessary steps to mitigate those risks were very different:

- in relation to the first stage, having taken into account all the circumstances, we concluded that Australia, Canada, the US and New Zealand would each provide an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data transferred to them. No significant risk to the rights and freedoms of the individuals involved would be presented by the transfer of nigh anonymous fingerprints under the agreed arrangements for the Protocol; and
- in relation to the second stage, we considered that the personal data to be transferred carried significant risk, being readily identifiable and in some cases sensitive personal data which may need to be retained for a considerable time for the recipient authority to complete its processing. However, we also considered that the risks to the rights and freedoms of data subjects would be sufficiently mitigated by the security of these countries' existing arrangements, and by the specific arrangements implemented for the Protocol, as to allow for adequacy under the eighth data protection principle, provided that the legal adequacy criteria can also be met.

6.3.4 What were our findings on the Legal Adequacy criteria?

We were able to recognise Australia, Canada the US and New Zealand as stable states, with no real danger of prejudice, and have confidence that they recognise the rule of law and have effective legal frameworks for the protection of rights and freedoms of individuals generally. Each has specific legislative arrangements for protecting the rights and freedoms of data subjects, including a Privacy Act incorporating similar data protection principles as are set out in EU law and relevant international instruments, such as the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These principles are more widely recognised as the core of personal data protection.

Compliance with data protection law in Australia, Canada and New Zealand is overseen by independent national Privacy Commissioners and is enforceable in their national courts. The US compliance framework is in contrast a networked and layered approach, directly involving a range of actors and processes across

the executive, legislature, judiciary and public community. There are a number of similarities and differences between these countries' arrangements and the European framework. None of these countries is currently subject to a general finding of adequacy by the European Union, although the EU has put in place arrangements with each, for which it has made findings of adequacy.

In making our assessments, and in developing our arrangements, we took account of the principles and arrangements already agreed by the EU, and the European Data Protection Supervisor's published Opinions thereon, intending to ensure that the Protocol arrangements met our test of adequacy and also met or exceeded the standards agreed and recommended at European level.

The key question we sought to answer in our adequacy assessments was whether the specific terms of the MoU, and the wider legal framework within which each country operates, would between them ensure adequate protection for the rights and freedoms of people whose data we would share. In doing so, the key differences we encountered were:

- none of the other countries' privacy legislation differentiates 'sensitive' personal data from other forms of personal data. However, the Protocol arrangements are such that all personal data disclosed by the UK Border Agency (whether sensitive personal data or not) will only be processed by the legitimate state authorities of those countries for their immigration and nationality purposes. Therefore, protection comparable to that provided in the UK by Schedule 3 of the DPA is in place (see section 6.2.2);
- the approach to retention in the Privacy Act in Australia is formulated differently. However, the Protocol arrangements provide an agreed approach to retention (see section 8);
- Canada's and the US' legislation does not explicitly require restrictions on data processing that are imposed by the originating party to be respected. However, the Protocol arrangements provide for this (see section 5.4.2);
- whilst Canada's legislation requires its institutions to ensure the accuracy of their information, rights of access and corresponding rights to request corrections and notations can only be exercised by people who are citizens or residents of, or are physically present in Canada. Foreign nationals would thus be able to exercise these rights only if they were present in Canada. However, our arrangements for the Protocol specifically provide that similar opportunity for access, correction and notation will extend administratively to all people whose data is shared. This is a similar approach to that taken in the EU-Canada API/PNR treaty, which is publicly available;
- equally New Zealand's legislation requires foreign nationals to be physically present in New Zealand to exercise their rights of access and corresponding rights to request corrections and notations. However, New Zealand's Department of Labour does already go beyond the requirements of its Privacy Act by providing in its internal policies the right of access and correction to all people about whom it has made a decision on an immigration matter

regardless of location. The Protocol will also extend these arrangements to all people whose data is shared under it.

- similarly, access, correction and notation rights under the US Privacy Act only apply statutorily to US citizens and residents. However, US DHS has administratively extended these to foreign nationals whose data is provided to DHS under the Protocol arrangements, and this is explicitly provided for in the arrangements, a similar approach as with the publicly available EU-US PNR agreement; and
- the networked and layered US compliance framework is very different from the European model, involving a range of checks and balances between the executive, legislature, judiciary and public community. We assessed that a person whose data is shared with DHS through the Protocol would have adequate opportunity to exercise and enforce his rights through the various US administrative and judicial mechanisms.

Having taken into account all the circumstances, we considered that Australia, Canada, the US and New Zealand would each provide an adequate level of protection for the rights and freedoms of data subjects under the Protocol, and that the Protocol can therefore take place in compliance with the Eighth Data Protection Principle.

7. What are the technical and practical arrangements?

7.1 How do we know the data exchange will be secure?

Other than in the contingencies set out in section 7.3 below, all of the data exchange will be conducted securely and using encryption between designated points of contact in each country, through a Secure File Share Server (SFSS) hosted by the Government of Australia. The security measures include appropriate technical measures in line with ISO17799/BS7799 standards for transferring the fingerprints via the SFSS, which will be fully accredited by the system security accreditors of each of the FCC countries before they implement the Protocol. This will minimise the risk of any outside interference in the data transfer.

The SFSS is constructed in such a way that data can only be accessed by the country for which it is intended. The country retrieving the data from the SFSS will delete that information from the SFSS upon retrieval. Thus all data exchange is bilateral between two of the countries, no data will be seen by any authority for which it is not intended, and the data will not remain on the SFSS for longer than the short time that is necessary for the rightful recipient to retrieve it.

The security and management arrangements for the SFSS are set out in an agreed Service Arrangement between the government of Australia and the other participating countries.

7.2 How do we know that each country will protect the data appropriately?

Each country has made arrangements for the data exchange to be carried out securely by named individuals in a central unit, interfacing directly with the other countries via the SFSS, with the operators of their fingerprint system, and with other parts of their organisation.

The fingerprints that are shared in the first stage of the process will be removed from the SFSS by the receiving country, transferred securely to the fingerprint system operators for matching, and after matching, will be destroyed. Thus the fingerprint processing will occur within a closely controlled process undertaken between the Protocol operators and the fingerprint system operators, each of which will operate within a closely controlled environment, presenting minimal risk of error of interference.

The personal data that is shared in the second stage of the process, on cases where fingerprint matches are identified, will also be processed securely by the central unit in each country. However, it will necessarily have to be transferred elsewhere within (or sometimes beyond - see section 5.2) the organisation in order to be acted on by the relevant operational unit. In order that the rights and freedoms of people whose data is shared are not weakened by this further transfer, the arrangements require additional safeguards in each country to ensure the continued security of the data received from the other countries.

In particular, each country will maintain the data in a manner at least as secure and with similar privacy and data protection rights being afforded to the data subject as is the case with its own citizens. Specific minimum standards include:

- personal data received will be handled in accordance with an appropriate level of classification. The countries' classification systems are different, but each will apply a broadly equivalent classification. In the UK this will be the "restricted" classification, in Australia and New Zealand "in confidence", in Canada "protected B", and in the USA "sensitive but unclassified".
- personal and official information will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information. Each country will store the data in secure electronic and/or paper storage systems at all times.
- access to the data received will be restricted to those authorised personnel who have a need to know the information to carry out their official duties, for uses which are consistent with the purposes of the Protocol;
- all persons who have access to the data will have been appropriately educated and trained regarding the handling and restrictions on use of this information to ensure the overall safeguarding of the information and compliance with the Protocol arrangements; and
- each country will ensure that information received is protected from unauthorised dissemination, and will take appropriate action under its

administrative, civil, and/or criminal laws in the event of misuse, unauthorised alteration or deletion, or unauthorised access or dissemination of the information by its own employees, agents or any third party.

7.3 What will happen if there is a problem with any of the arrangements?

If the Secure File Share Server is unavailable for any reason, there are two agreed contingencies for data transfer:

- information may be transmitted via direct country-to-country e-mail transfer, which will be encrypted using an Advanced Encryption Standard (AES) 256 bit key; or
- in the unlikely event that the SFSS and encrypted e-mail are both unavailable, but there is an urgent need to share information, it may be hand delivered, with appropriate protection, by one of the designated contacts to the relevant Embassy or High Commission of the other country, for onward transmission to the latter's home government within its secure e-mail network.

As these two contingencies provide secure alternate methods of communication, the possibility of the SFSS being unavailable for any reason does not present any significant risk to the security of the arrangements.

We have also agreed further safeguards in the event of unforeseen difficulties occurring in any of the countries, in particular:

- for each country to notify the others immediately in the event of a disaster or other situation that disrupts the intended transfer of information between them; and
- as soon as reasonably practicable, but no later than twenty-four hours after becoming aware of any breach of the security of the information systems containing, or unauthorised use or disclosure of, any personal information that has been shared.

Whilst each country reasonably expects the other countries participating in the Protocol to implement the agreed arrangements in good faith, as a further safeguard we have specifically provided for reporting and audit facilities:

- the countries will produce comprehensive, joint performance and management information about the operation of the Protocol, which will explicitly identify the number and severity of any security or privacy breaches and of remedial actions taken;
- any country may request assurance from another country that sufficient safeguards are being maintained in respect of the information shared, which may include an audit of the safeguards, to be carried out by an appropriate internal or external auditor with terms of reference agreed between the countries; and
- in the unlikely event that a country considered it necessary to decline to provide further information to another because of perceived deficiencies in

safeguards, it could do so. This would be notified to all of the countries participating in the Protocol, which would consult each other immediately to decide upon the appropriate course of action.

8. What are the arrangements for retaining the information?

There has been much debate about the circumstances in which personal information should be retained by government agencies, and for how long. The general principle is that it should be retained for as long as it remains relevant for the necessary purpose, and for no longer. However, the continued relevance of a set of information is likely to vary in different circumstances. Thus a fixed 'retention period' is likely to be a very blunt instrument, both from the point of view of the person who does not want his information kept longer than is actually necessary, and from the perspective of the organisation that wishes to keep it for as long as it may be needed. For how long it may be needed is also a difficult question, as the organisation cannot necessarily predict whether it will come into contact with a particular person in the future, or whether the information would again be relevant if it did.

In developing the FCC Protocol and assessing its impacts, it was clear that a 'one size fits all' retention policy would not serve anyone's interests very well. Therefore we considered which information would need to be kept in which context, and how we could best regulate that. This section sets out the approach we formulated, and why we believe it is the most appropriate. Personal information that is exchanged under the Protocol may only be retained as set out below, unless the agency that supplied the information has given its prior written approval. The UK Border Agency would not give such approval unless we were satisfied that the information was still relevant and further retention was appropriate.

8.1 Retention on the Secure File Share Server (SFSS)

There is no need to retain information on the SFSS after it has been retrieved by the receiving country. All personal information will therefore be deleted from the SFSS upon being retrieved successfully. This will be done by the person retrieving the information, backed up by an automated deletion mechanism. The SFSS will not hold a back up copy of the information. This provides confidence that the data is no longer held in the central system, without presenting risk of data loss, as the relevant countries' tracking arrangements would identify any data that was missing, which could then simply be re-sent via the SFSS.

8.2 Retention of the fingerprints that are shared for searching

As the fingerprints may only be used for searching against the biometric database, and for no other purpose, there is no need to retain them after the

searching has been done. Each country will therefore destroy them securely once they have been searched.

8.3 Retention on the case file for the person whose information is shared

Where information that is shared is included in the case file (either electronic or paper) for the individual to whom the data relates, because it has ongoing relevance to the file, it may be retained as part of that case file in accordance with the domestic laws and data retention policies of the country that has received it. Thus if we receive information about one of our customers, which is pertinent to our decision, we will reflect that information in our decision, and keep the information as part of the file for the same period we would keep other relevant information. This is both appropriate and inevitable.
People would expect their personal file records to be kept complete and accurate, for as long as they are kept. This does not present the same privacy risks as retaining data in other systems. Removing part of the information which led to a decision would corrupt the file record, and it would not in any case be possible where the information in question had been reflected in other case papers, for example, in the decision letter issued to the person. There would be no logic in seeking to apply an arbitrary retention limit to information held on case files. Each FCC country has laws and policies applying to retention of case files and we have agreed that those will apply in this context.

8.4 Retention for watch list purposes

Each of the FCC countries maintains one or more 'watch lists' which enable it to identify persons of interest who come into contact with it. Each country has its own system for managing the information placed on those watch lists, as an integral part of its immigration processing. Whilst it is important for each country to be able to put appropriate information that is uncovered through the Protocol onto those watch lists, and trials have shown high value in doing so, this would if unregulated present a number of risks to people whose information is shared. The Protocol arrangements therefore regulate how this will operate, and identify that personal information in relation to three categories may be placed onto watch lists:

- false identities and travel documents. It is strongly in the public interest for false identities and documents that are uncovered to be placed onto watch list systems, in order that they cannot be used again and, if they are, that they can then be taken out of circulation;
- multiple identities used by the same person. Trials have shown that where people are using multiple identities, it may be necessary to place all of these onto a watch list system. In some circumstances there is more value in putting such a person's true identity onto the system than the false one: for example, where someone is using a false identity within the country, whilst travelling in and out of the country in their true identity, it is putting the true identity onto the system that will result in the person being caught; and

- persons engaged in derogatory activity that would render them inadmissible to the other Participant's territory. For example, a serious foreign criminal who would be debarred from entering our country because of that criminality may be entered on our watch list, in order that he cannot enter the country whilst concealing his criminality.

The Protocol provides that such information may be retained for as long as it is relevant to that Participant's border controls, up to an initial maximum of ten years. Ten years is a sensible period for retention, coinciding with the length of validity of many travel documents (that is, they could otherwise still be used for up to ten years). However, false identities may be renewed and there may be a case for retaining some information for longer than ten years. The Protocol therefore provides that, as part of our ongoing review of watch list entries, the FCC countries will discuss the continued relevance of the information within the ten years and seek agreement on any further retention. However it is likely that wider international agreements on watch list arrangements will be in place within that timescale, with which we may simply agree to fall in line.

8.5 Retention in central record or elsewhere

Each of the countries may, to a greater or lesser extent, also need to keep information that it receives under the Protocol elsewhere, in particular, in a record held by the central team that administers the Protocol. This is particularly the case in the UK, where the central team will pass information to the relevant operational colleagues for action, but will also have an ongoing monitoring and liaison role to ensure effective action is taken, and will need separate access to the data for that purpose. However, none of our countries wish to allow the development of a database of personal information shared under the Protocol, or the possibility of the data being held unnecessarily elsewhere. The Protocol arrangements therefore provide that any such retention is limited to two years. This will allow time for the necessary operational action, but avoids the risks of data accumulation.

9. Is the data sharing consistent with the legitimate expectations of the people whose data is being shared?

We have set out in the other sections of this paper why the FCC authorities are implementing the High Value Data Sharing Protocol, and how it will operate legally, technically and practically. We considered it would be useful to complete our report by reflecting on whether its operation will be consistent with the legitimate expectations of people whose data is shared under it, and in particular, whether it will be fair to them.

9.1 Expectations notice and consent

People whose information may be shared through the Protocol are already routinely notified (usually when their fingerprints are initially captured) that their data may be subject to international checks. For some years, asylum seekers and certain categories of enforcement case have had their fingerprints checked against other European countries' data through the Eurodac database as a matter of course. The Protocol presents a further avenue for making such checks.

A person who has fled persecution may arrive in the UK from halfway across the world, by whatever route, with little or no means of demonstrating his credentials. If he has previously been encountered by a country with which we can conduct checks, this can only help to verify those credentials. We believe the general public would agree that we should have the facility to conduct such checks, with rigorous security, as a positive means of validating our customer's account. Thus the implementation of the Protocol supports our ability to identify and protect genuine refugees.

Conversely, however, we consider it our duty to make checks to detect those who make fraudulent claims on the UK public and to identify foreign criminals and others who seek to obstruct our ability to remove them to their country of origin by destroying their documents and concealing their true identities. For this reason, although we notify our customers that we make such checks, we do not make the checks dependant on the consent of the individual. The public would not be well served by a system which allowed fraudsters to escape detection simply by withholding consent.

9.2 Expectations on security and confidentiality

A person whose fingerprints are checked through the Protocol can legitimately expect his information to be handled securely and confidentially. A reasonable person would not expect us to be sharing personal information about our customers with other countries in an uncontrolled way. However, we believe a reasonable person would expect us to co-operate operationally with partner countries on cases presenting mutual immigration interest.

We believe that the Protocol arrangements as described in this report provide high levels of data security, and appropriate confidentiality. The fingerprints are checked in an effectively anonymous way, and are not retained or used for any other purpose. Personal biographic information is only then exchanged on cases where a fingerprint match is found, with another country which has already encountered and has a legitimate immigration interest in the individual. We believe this accords with what a reasonable person would expect.

9.3 Fair processing

It is most important that the processing of people's information is transparent and fair, both from the point of view of the individual whose information is being processed and for wider public trust.

We have reflected in this report how the UK Border Agency and its FCC partners have developed the Protocol to enable sharing of appropriate information within an arrangement that we believe provides high standards of data protection, with a range of safeguards to ensure the information will only be used for appropriate purposes, that it will be accurate, and that people whose information is shared will be able to see and if necessary correct that information.

We have seen how information obtained through the Protocol is in the interests of the genuine applicant as it helps corroborate his application. It is also important to consider how the information will be processed fairly within our operational processes. Where we receive information that introduces ambiguity because it contradicts what one of our applicants tells us, we intend to put the information directly to the person, give him an opportunity to respond to it, and take his response equally into account. This is part of fair processing. There may be a rational, innocent explanation for something that at first appeared to contradict a person's account.

However, the information obtained from the fingerprint matching is factual, and is susceptible of proof. It is also predominantly well known to the applicant - for example, a person will be well aware of whether he had previously visited the USA using a different identity – and it is incumbent upon him to respond truthfully to it. Our trials showed that in practice an applicant can respond in three ways when such information is put to him:

- he can tell us that he is the person who was fingerprinted by the other country, in his true identity. In this scenario the information has revealed the person's true identity, and associated information, and he will need to explain himself in the light of this;
- he can tell us that he is the person who was fingerprinted by the other country, but that he was using a false identity at the time. We will interview the applicant further to determine whether this is credible in the light of the associated information; or
- he can tell us that the fingerprint match is false, and therefore none of the information relates to him. We can confirm the accuracy of the fingerprint match to the standard of proof applicable in criminal matters (see section 4.7). In the unlikely event that the match was found to be false – which never occurred in our trials – the information relating to it would be disregarded.

In each scenario, the information assists in resolving the case, whether or not the person responds truthfully. Most people know that fingerprint matching is susceptible of proof, and in trials most applicants admitted that the fingerprint

match was genuine. A number provided potentially innocent explanations, which were then examined further in the interview. We were able effectively to determine whether those explanations were true. This is because a true account would tally with additional information known about the alternate identity, whereas the falsity of contrived explanations was demonstrable as they did not accord with other known facts.

The key question that always has to be considered is whether the person meets the criteria to be recognised as a refugee. This is clearly not the same as the question of whether the person is telling the truth, although these questions are linked. A person fleeing persecution may well have needed to use deception at some stage in his flight, and if he tells us the truth about this then it does not detract from his claim. Equally, a person who has previously been dishonest with us may, once the truth is established, turn out to qualify for refugee status after all. In all cases, the first aim is to establish the truth as it relates to the application.

However, it remains incumbent on an applicant to provide a true account of himself, which he has ample opportunity to do, and one who continues seeking to deceive will have little credibility, and his application is likely to be expedited for refusal and removal on the basis that it is clearly unfounded. Where people continue deceptively seeking to frustrate our endeavours to achieve the correct outcome for their case, we will consider criminal proceedings as appropriate. As with all other immigration cases, where necessary and appropriate, immigration detention may be used in managing a case to its conclusion.

9.4 Judicial scrutiny

All of our relevant functions are also directly or potentially subject to judicial scrutiny in some form. For example, asylum decisions made by the UK Border Agency are appealable to the Asylum & Immigration Tribunal and onward to the higher Courts. Judicial scrutiny provides a fundamental safeguard for people's rights and freedoms in immigration matters. If we made a wrong decision about a person based on information that had been shared – whether because the information itself was wrong, or a wrong conclusion had been drawn from it – the person affected would have the ability to challenge this in the Courts.

This is a fair process that is in the interests of the genuine applicant as well as the UK public.