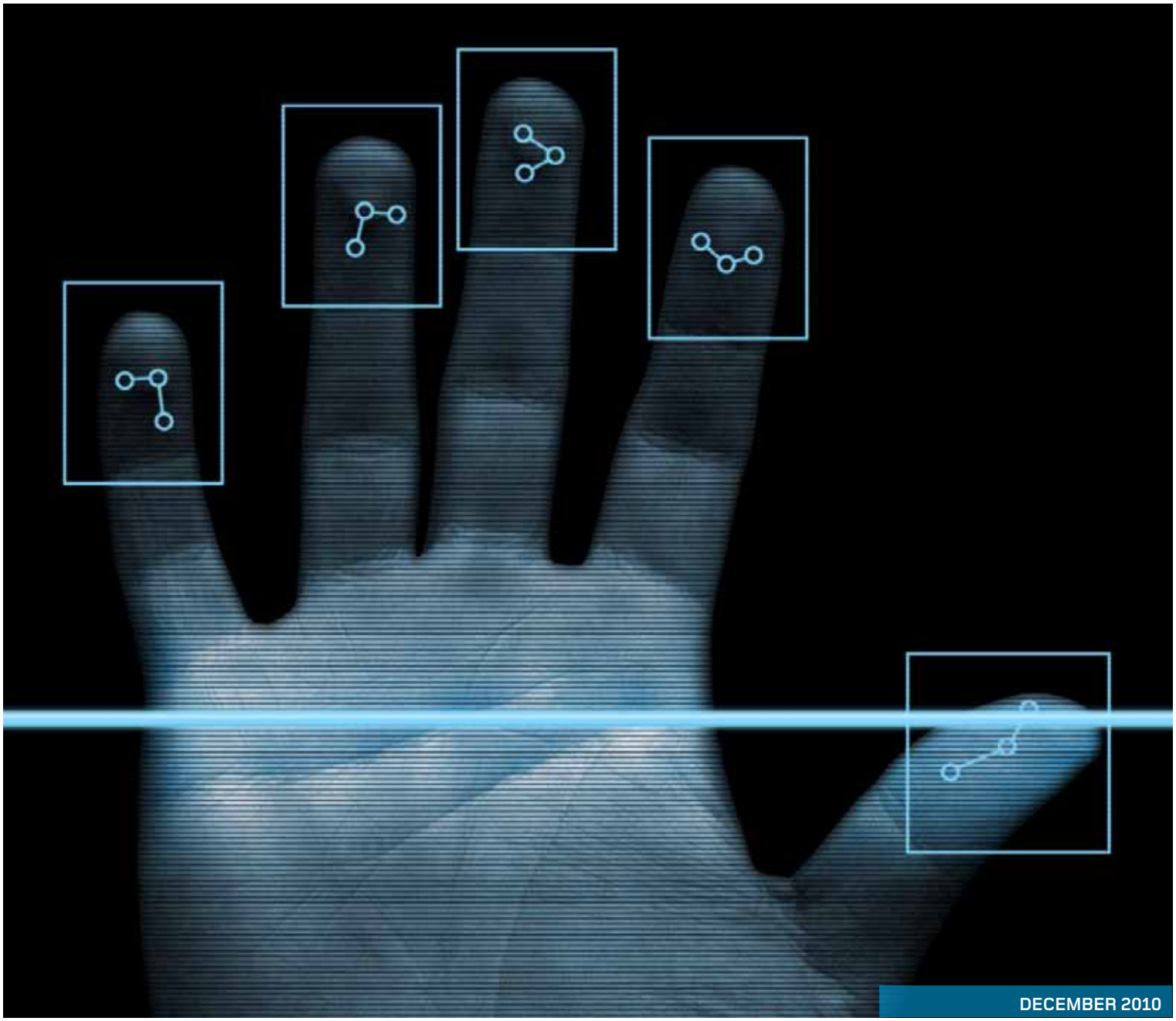
Privacy Impact Assessment

For Exchanges of Information between the New Zealand Department of Labour and Citizenship and Immigration Canada and the Canada Border Services Agency, as part of the Five Country Conference High Value Data Sharing Protocol



DECEMBER 2010

Agencies Involved

- **NZ Department of Labour – Immigration New Zealand**
  NZ Sponsor
- **New Zealand Police**
  NZ Data Custodian
- **Citizenship and Immigration Canada**
  CA Joint Sponsor
- **Canada Border Services Agency**
  CA Joint Sponsor
- **Royal Canadian Mounted Police**
  CA Data Custodian

Contents

Executive Summary & Summary of Risks

A. Background

New Zealand and other countries are increasingly concerned about identity fraud being used to circumvent immigration and border controls.

The fraud may be used, for instance, to hide a criminal record or to take advantage of immigration processes that are seen to be vulnerable. For example, individuals use a false identity to claim refugee protection when they already hold residence or citizenship in a safe jurisdiction.

Governments are now working together to exchange information about high risk situations to reduce the impact of these types of fraud. One group includes Australia, Canada, New Zealand, the United Kingdom, and the United States of America – the Five Country Conference (FCC).

The High Value Data Sharing Protocol (The Protocol) is designed to allow the FCC countries to share information about high risk individuals applying to the immigration authorities of those countries.

Given the legal and operational differences in the five countries, it was decided that all sharing of information would take place as bilateral exchanges under the umbrella Protocol. Each bilateral exchange would be operated under a Memorandum of Understanding (MOU) between each pair of countries.

B. Benefits

The proposed exchanges are expected to deliver the following benefits:

- Improved integrity of New Zealand's immigration system. This will happen through the improved early detection of fraudulent identity and immigration claims, and the ability to close previously open files regarding absconders who may have covertly left New Zealand to an FCC partner country.
- Improved public safety through earlier detection of persons using false identities to hide criminal histories or terrorist backgrounds.
- Cost savings from the:
  - earlier detection of fraudulent identities and applications,
  - prevention of fraudulent secondary migration, and
  - prevention of fraudulent use of public services (for example, benefit payments, health care, legal aid, public housing, police, courts and custody costs).
- Improved international reputation through maintaining parity and interoperability with modern immigration capabilities and ability to participate in security arrangements.
- Enhanced ability to:
  - detect and analyse immigration trends
  - respond to and manage trends in the future.

C. The exchanges

Under the bilateral arrangement there is a cap of 3,000 match requests that can be made by each country per year. Under future arrangements, this may be increased to 75,000 with Canada (refer to sections 5.5.2 and 5.5.3) and FCC participants have agreed to review their privacy impact assessments before such an extension.

The overall FCC programme scale varies depending on the participants. In this bilateral exchange with CIC, exchanges are expected to be small in terms of numbers of cases exchanged as outlined below.

The records of known nationals of any FCC country are excluded from these exchanges. No fingerprints of any known FCC national will be sent for pseudonymous matching.

The scale of the Programme is expected to change with time.

In stage 2, (to which this PIA refers) the exchanges will be limited to enquiries on 3,000 cases per year per participating country as processing will be largely manual.

In stage 3, (note: this PIA will be updated for stage 3) that maximum will increase to 75,000 cases per year with Canada and will be dependent on the development of a real-time automated identity checking system.

Initially, it is expected that New Zealand will send up to 3,000 fingerprints per year to Canada for matching. They will be sent in batches of up to 50 records with the maximum permitted being 100 records in a week.

However, those limits under the protocol may never be reached. Cases will be selected for sending to US according to two priority levels:

'A' – national security, asylum, fraud, compliance and detention cases where there are doubts over identity

'B' – individuals who have been granted leave to remain in NZ, but where doubts remain over identity

In order to be sent for matching, the cases will also have to meet one or more of these criteria:

- Immigration cases where identity of the individual is unknown or uncertain;
- Immigration cases where the individual's whereabouts are unknown; and/or
- Immigration cases where there is reason to suspect that the person has been encountered by more than one of the countries participating in the Protocol.

d. Purpose

The information that New Zealand receives from Canada will be used exclusively for immigration and nationality purposes in both countries. From the MOU clause 1.3, those are; *"…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."* The information is necessary in order for DoL to carry out its responsibilities under both the 1987 and 2009 Immigration Acts.

e. Notice

DoL is publishing a formal notification to advise of the implementation of the FCC Protocol with each partner country. This notification will be placed on the DoL website and other relevant communication channels.

Summary of Privacy Risks & Mitigations		
	Risk	**Mitigation(s)**
1	The right of people outside the country who are not New Zealand citizens or residents, to access and request correction of their personal information.	The New Zealand *Privacy Act 1993* (as amended 7 September 2010) provides that right. In addition, DoL *Privacy Act Policy 2005* says that in immigration matters those people will be treated as if they have the same rights as citizens and residents. Similarly, the CIC allows affected people not in Canada access to their personal information via a request through a Canadian resident under their *Access to Information Act*. The participating countries also specifically agree to extend these rights under section 6.14 & 6.15 of the *MOU*.
2	Automated decision making and absence of human judgement.	In New Zealand, all fingerprint matches will be assessed by a human expert before any information is released. In Canada,fingerprint matches may be confirmed automatically when the fingerprint set images meet or exceed high quality thresholds. Fingerprint sets which do not meet the auto quality match confirmation setting will be manually verified by a fingerprint expert prior to the release of any information to CIC.
3	Adverse action being taken against an individual without that person being given the opportunity to explain or challenge potentially prejudicial information.	All potentially prejudicial information will be presented to the individual for their comment or rebuttal.
4	Information collected for one country's immigration purposes will be used by another country.	The disclosure of immigration information to another country and the use of another country's immigration information are explicitly permitted by statute. The FCC protocol and the MOU provide additional safeguards for the personal information subject to the exchanges.
5	DoL will be using information collected from its partner agencies in the FCC rather than directly from the individuals.	DoL has explicit statutory authority to collect and use this information.
6	The biometric information is compromised by a lack of security in storage or transmission.	All transfers of information will be protected by encryption. All information will be kept securely according to DoL standard procedures.
7	Information will be kept beyond the business requirements of DoL.	The Protocol and MOU restrict retention of information under these arrangements and require destruction of fingerprint records used in the match process.
8	Widespread use of a common Unique Identifiers (UIs)	None of the participating agencies will assign UIs already assigned by another agency. For NZ records, special UIs will be created to identify the fingerprints during the initial pseudonymous matching process so that internal DoL UIs are not used for that process. CIC uses its internal UIs to identify fingerprints sent for initial matching but DoL will not keep those UIs.
9	Individuals will not know what is happening with their information.	Information about the Protocol including Frequently Asked Questions is available on the DoL website. Notice of the implementation of the Protocol was also published on the website.
10	"Fishing" in government records	The Protocol targets only "high value" situations where identity documents are absent or there is reason to be concerned about a claimed identity.
11	Inaccurate information transmitted through multiple agencies' systems	Both the Protocol and the MOU require that the information exchanged be accurate and as complete and up-to-date as possible and that when errors are discovered, the other parties are notified.

1. Background

New Zealand and other countries are increasingly concerned about identity fraud being used to circumvent immigration and border controls.

The fraud may be used, for example, to hide a criminal record or to take advantage of immigration processes that are seen to be vulnerable. For example, individuals use a false identity to claim refugee protection when they already hold residence or citizenship in a safe jurisdiction.

Immigration fraud is damaging for two reasons. Firstly, fraudulent immigration claims displace or delay applications and claims by genuine applicants. This is particularly damaging for asylum candidates, many of whom are in difficult or dangerous situations[1]. Secondly, once individuals obtain NZ residence – and potentially citizenship – through fraud, it is difficult, time-consuming and expensive to fix this.

Governments are now working together to exchange information about high risk situations to reduce the impact of these types of fraud. One group includes Australia, Canada, New Zealand, the United Kingdom, and the United States of America - the Five Country Conference (FCC).

The High Value Data Sharing Protocol is designed to allow the FCC countries to share information about high risk individuals applying to the immigration authorities of those countries.

Given the legal and operational differences in the five countries, it was decided that all sharing of information would take place as bilateral exchanges under an umbrella Protocol. Each bilateral exchange would be operated under a Memorandum of Understanding (MOU) between each pair of countries.

New Zealand has started information exchanges under the protocol with Australia. It is hoped that a Memorandum of Understanding with Canada will be signed in early 2011. This PIA will inform the MOU between the two responsible agencies.

There is a broader PIA in progress on the privacy impacts of biometrics collected and handled for immigration purposes[2]. The wider PIA may result in amendments or updates to this PIA.

1.2 The Issue

The weaknesses of traditional means of managing identity crime have led governments around the world to increase their use of biometrics to complement biographic identity checks used in immigration and border processes.

Biometrics are useful when people arrive undocumented or with false or suspicious documents. They are also useful when people try to prevent their correct identification by DoL.

Biometrics can help in the:

- early detection and prevention of immigration fraud,
- reduction of public safety risk by identifying individuals with criminal or adverse immigration histories, and
- reduction in the time and cost of dealing with immigration fraud downstream[3].

The immigration system is a significant contributor to the economic development of New Zealand. It is also a means for meeting New Zealand's obligations under international agreements, such as the 1951 Convention Relating to the Status of Refugees and 1967 Protocol Relating to the Status of Refugees.

DoL is expected to assess immigration and asylum cases for legitimacy and to prevent abuses of the system. The proposed information exchanges with Canada involve high risk cases with the objective of maintaining the integrity of the immigration system.

1. The Canadian government has introduced reforms to their immigration processes to address these problems and increase Canada's ability to accept and resettle refugees http://www.cic.gc.ca/english/refugees/reform.asp
2. *Immigration Act 2009*, s.32
3. Other agencies directly affected by immigration fraud include Police, Housing, Health, Education and MSD

1.3 Benefits of the Exchanges

The proposed exchanges are expected to deliver the following benefits to both countries:

- Improved integrity of New Zealand's immigration system. This will happen through the improved early detection of fraudulent identity and immigration claims.
- Improved public safety through earlier detection of persons using false identities to hide criminal histories or terrorist backgrounds.
- Cost savings from the:
  - earlier detection of fraudulent identities and applications,
  - prevention of fraudulent secondary migration[4], and
  - prevention of fraudulent use of public services (e.g., benefit payments, health care, legal aid, public housing, police, courts and custody costs)
- Improved international reputation through maintaining parity and interoperability with modern immigration capabilities and ability to participate in security arrangements
- Enhanced ability to:
  - detect and analyse immigration trends
  - respond to and manage trends in the future

A final objective is to develop a statistical base on which to assess the value of different forms of data sharing. Preliminary statistical results and two case examples from the trials conducted by other FCC participants are provided in Appendix C.

1.3.1 New Zealand experience to date

New Zealand commenced biometric data matching with Australia under the Protocol in July 2010. Available information shows that:

- Approximately 130 false identities are detected at the border each year. This does not include false identities detected by DoL offshore or onshore.
- The number of people who successfully entered or departed New Zealand using false identities is (obviously) unknown
- Since August 2005, 257 false identities have been referred to the Police for inclusion in the identity Protection Register
- Identity fraud is the most common type of immigration prosecution
- Numerous cases where persons have concealed 'safe third country' citizenship to obtain refugee status in New Zealand
- 29 cases of cancelled refugee status (serious fraud proved) involved identity fraud

1.3.2 Anticipated cost avoidance

Improved detection and prevention of attempted fraudulent entry to New Zealand is expected to reduce the costs of managing cases at the border and removals. Those costs can be significant.

Each case of refugee fraud conservatively costs DoL NZ$28,550. Additional Crown costs accrue from services provided by government, for example legal aid, health, education, housing and welfare. These additional downstream costs are not available.

There are reputational costs and public trust costs to having known criminals remain in New Zealand or leave with and misuse a fraudulently obtained New Zealand passport.

1.4 Alternatives to the Exchanges

The only other agencies that hold comparable information to that held by DoL are the partner immigration authorities in the other FCC countries. Each country shares a desire to:

- maintain a secure border
- be better informed about those who remain illegally in their countries
- be better informed about those without a legal basis to remain in the country who have left other countries, voluntarily or by deportation/removal.

4. 'Fraudulent secondary migration' occurs when a principal applicant successfully acquires NZ residence through identity fraud and as a result helps other claimed family members to also migrate.

The Auditor General's report on identity management in DoL[5] highlighted the inadequacy of existing systems. Those systems cannot ensure that asylum and refugees status are granted only to genuine claimants, nor can DoL associate each individual with a consistent identity used across all immigration transactions. The Report noted the absence of consistent routine use of biometrics to ensure reliable, consistent, person-to- identity verification.

FCC countries will use pseudonymous fingerprints only for matching. That will allow identification of individuals in each agency's records without disclosing any other personal information about that individual. In particular, no biographic information and no photographs will be disclosed with the fingerprints. That will only occur after a match of sufficient quality is made through the pseudonymous fingerprints and which warrants further disclosure.

Alternatives considered by the FCC would have required more disclosure of personal information in order to establish a shared interest in an individual. The current solution was decided upon as the least privacy-intrusive.

1.4.1 Alternative 1 - Using biographic information only

If DoL were to use biographic information only, the amount of information required from individuals would be greatly increased. The type of information and the amount of detail about each type of information would have to increase.

Increased amounts of biographic information would be easily useable by many other agencies and for many other purposes. Biometric information requires specialised equipment and specialised training of the human operators in order to be useful. This provides a natural limit on its wider use.

The increased amounts of information collected would increase the potential for scope creep and requests from other agencies for the information for purposes unrelated to immigration.

In addition, all that extra biographic information would be less effective than biometric information and increase the chance of misidentification. It would be completely useless for people who arrive in New Zealand with no travel documents or invalid, altered, counterfeit, or other suspicious travel documents or identities.

Biographic information also has limitations when dealing with people with similar or identical names and dates of birth. This difficulty often occurs or is increased when information has to be translated into English or to the Western calendar[6].

1.4.2 Alternative 2 – Using photographs of people's faces

Another alternative considered was the use of pseudonymous photographs. Photographs are widely collected and available on travel documents and are a normal part of an immigration application to ensure that the person who enters a country is the same as the person who applied for entry.

However, photographs of people's faces (digital or otherwise) are easily viewed and recognised. In contrast, the specialised equipment and training required to identify a person from their fingerprints is not widely available. Face images (photographs) were therefore considered to be more risky to privacy than fingerprint images.

Face recognition biometrics are also less accurate than fingerprint biometrics when run against large databases, with a correspondingly greater chance of error or ambiguity in the identification of matches.

5. Controller and Auditor General, Performance Audit Report, Department of Labour: Management of Immigration Identity Fraud. June 2007. ISBN 0-478-18188-4

6. Many cultures do not use the Western calendar, and other cultures do not necessarily place the same emphasis on date of birth as do our records systems. Transliteration of foreign-language names into English can be inconsistent.

2. General Privacy Concerns

2.1 Adequacy of Privacy Protection

The New Zealand *Privacy Act 1993* (NZ Act) was amended on 7 September 2010 to extend the right to make information privacy requests to foreign nationals outside New Zealand. Even before that, the Department of Labour's published policy was "to respond to requests as if the person were eligible to make a request, even where they are not a New Zealand citizen or resident, and are outside New Zealand." [7]

The Canadian *Privacy Act 1985* which applies to federal government agencies has a restriction (section 12) where the right to request access to and correction of personal information is limited to citizens, permanent residents, and "all individuals present in Canada".[8] This is similar to the provisions of the NZ Act before September 2010.

However, like DoL, CIC enables access to information for individuals outside Canada by permitting them to make requests through a representative in Canada under the *Access to Information Act 1985*[9].

In addition, the MOU between New Zealand and Canada includes the requirements in clause 6.14 and 6.15 that:

- Either participant is expected to afford to a person who is not present in the territory in which the Participant exercises jurisdiction, to whom the information exchanged under this MOU relates, access to the information as well as the opportunity to seek correction if it is erroneous or add a notation to indicate a correction request was made.
- The opportunity provided by either Participant for access, correction and notation with respect to such information should be afforded in circumstances similar to those available to persons present in the territory in which that Participant exercises jurisdiction.

The MOU in clause 6.16 also requires participants to notify each other of disrupted transfers, security breaches, or unauthorised disclosures.

The specific requirement for access and correction rights is supported by clause 6.2.4 of the Protocol that states:

- Personal information, should, to the maximum extent feasible, be as accurate, timely, relevant, and complete as reasonably necessary to assure the propriety of identification of individuals whose personal information is contained in the system and of actions taken under this agreement with respect to that information.
- Either a Requesting Country or a Providing Country may take appropriate action made by the other for access, additions, or changes to, or deletions, or corrections of personal information. In addition, all countries should notify one another of any data errors discovered.

2.1.1 Analysis of the Canadian Privacy Regime

While the overall Canadian privacy regime is made up of legislation and privacy authorities at the federal and provincial levels, federal government agencies are covered by the CA Act[10], its regulations[11] and the policies and directives of the Treasury Board Secretariat (TBS)[12].

As in New Zealand, the CA Act established a Privacy Commissioner responsible to Parliament and required to report annually on the operations of her Office. The Commissioner

7. Department of Labour Privacy Act Policy October 2005 http://www.dol.govt.nz/PDFs/privacyactpolicy.pdf
8. The Privacy Act section 12 for citizens and permanent residents and as amended by the Privacy Act Extension Order, No.2 to all individuals present in Canada. http://laws.justice.gc.ca/en/P-21/index.html
9. http://www.cic.gc.ca/english/department/atip/faq.asp#Q2 The Canadian equivalent to DOL's manual is available on their website at http://www.cic.gc.ca/english/resources/manuals/index.asp. The specific instructions regarding non-resident access to their personal information is found on p.35 of Overseas Processing: Procedures available at http://www.cic.gc.ca/english/resources/manuals/op/op01-eng.pdf.
10. http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-p-21/latest/rsc-1985-c-p-21.html
11. Such as: http://www.canlii.org/en/ca/laws/regu/sor-83-508/latest/
12. http://www.tbs-sct.gc.ca/pol/index-eng.aspx?l=P

has powers to receive and investigate complaints from individuals, to initiate investigations, and to conduct special studies. Along with the New Zealand Office, the Office of the Privacy Commissioner of Canada is a member of the Asia Pacific Privacy Authorities[13] and is a founding member of the Global Privacy Enforcement Network[14].

The CA Act is not structured around underlying principles as is the NZ Act but there are strong parallels. Where the two Acts do not line up directly, there are several areas where matters addressed directly in the New Zealand Act are deferred to regulations or "the designated Minister"[15] under the CA Act or are addressed by Treasury Board Secretariat policies, directives, and standards.

For example, the Privacy Regulations (SOR/83-508) prescribe for federal agencies, the minimum retention periods for requests for access to and correction of personal information and notification requirements if correction is refused.

The following table summarises those parallels with references to sections of the CA Act and relevant TBS documents[16].

New Zealand Privacy Act 1993	Canadian Privacy Act 1985
Principle 1 Purpose of Collection	Section 4 - No personal information shall be collected by a government agency unless it relates directly to an operating program or activity of the institution. Supplemented by the *Directive on Privacy Practices*[17] which requires that agencies have parliamentary authority for the agency's program or activity before collecting personal information
Principle 2 Source of personal information	Section 5(1) - A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution under subsection 8(2).
Principle 3 Collection of information from subject	Section 5(2) - A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.
Principle 4 Manner of collection of personal information	Covered by TBS's *Directive on Privacy Practices*. It requires that personal information is only collected, retained, used, disclosed and disposed of in a manner that respects both the privacy of individuals and the provisions of the *Privacy Act 1985*[18] and *Privacy Regulations*.[19]
Principle 5 Storage and security of personal information	Covered in TBS Policies & Directives: The *Directive on Privacy Practices* requires agencies to apply safeguards for the use and disclosure of personal information. The *Directive on Privacy Practices* prescribes responses to privacy data breaches. The *Policy on Privacy Protection*[20] requires (when applicable) privacy impact assessments be conducted, maintained, and published and has as an expected result: "5.2.1 Sound management practices with respect to the handling and protection of personal information, including identifying numbers;"

13. http://www.privacy.gov.au/aboutus/international/appa#appa
14. https://www.privacyenforcement.net/
15. The Minister of Justice for certain provisions in the Act.
16. CIC has had PIAs prepared relating to the Protocol and the April 2009 PIA contains references to the TBS Data Matching Policy. That policy is no longer (13/10/2010) in force.
17. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309
18. http://laws.justice.gc.ca/en/showtdm/cs/P-21
19. http://laws.justice.gc.ca/en/showtdm/cr/SOR-83-508/?showtoc=&instrumentnumber=SOR-83-508
20. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510

Principle 6 Access to personal information	[Note: Sections 6.14 & 6.15 of the MOU address rights to access and correction of their information to ensure those rights are accessible regardless of nationality or country of residence.] As described above, CIC advises individuals who are not entitled under the following section of the CA Act or under its subsequent extension, that they may make applications through the Access to Information Act. Section 12. (1) - Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of subsection 2(1) of the Immigration and Refugee Protection Act has a right to and shall, on request, be given access to (a) any personal information about the individual contained in a personal information bank; and (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution. *Privacy Act Extension Order No.2* says "The right to be given access to personal information under subsection 12(1) of the *Privacy Act* is hereby extended to include all individuals present in Canada to whom that right has not been extended previously." These are supplemented in the TBS *Directive on Privacy Requests and Correction of Personal Information*[21] which details what is expected of government agencies in their handling of requests for access to and correction of personal information.
Principle 7 Correction of personal information	[Note: Sections 6.14 & 6.15 of the MOU address rights to access and correction of their information to ensure those rights are accessible regardless of nationality or country of residence.] As described above, CIC advises individuals who are not entitled under the following section of the CA Act, that they may make applications through the Access to Information Act Section 12(2) - Every individual who is given access under paragraph (1)(a) to personal information that has been used, is being used or is available for use for an administrative purpose is entitled to (a) request correction of the personal information where the individual believes there is an error or omission therein; (b) require that a notation be attached to the information reflecting any correction requested but not made; and (c) require that any person or body to whom that information has been disclosed for use for an administrative purpose within two years prior to the time a correction is requested or a notation is required under this subsection in respect of that information (i) be notified of the correction or notation, and (ii) where the disclosure is to a government institution, the institution make the correction or notation on any copy of the information under its control. This is supplemented in the TBS *Directive on Privacy Requests and Correction of Personal Information* which details what is expected of government agencies in their handling of requests for access to and correction of personal information.

21. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18311

Principle 8 Accuracy etc of personal information to be checked before use	Section 6 (2) - A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible. Supported by accuracy provisions in the Directive on Privacy Practices requiring for example, "direct collection or validation with the individual or indirect collection or validation when authorized or consent was obtained …".
Principle 9 Agency not to keep personal information for longer than necessary	Sections 6 (1) & (3) - require agencies to keep information long enough for the data subjects to have a reasonable opportunity to obtain access to the information and that it should be disposed of in accordance with the regulations and in accordance with any directives of guidelines … Supported by retention and disposition provisions in the TBS Directive on Privacy Practices.
Principle10 Limits on use of personal information	Section 7 - Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2). Section 8(2) - lists acceptable disclosures including the purpose for which the information was collected or a use consistent with that purpose, in accordance with any Act of Parliament or any regulation …, to an investigative body … for the purpose of enforcing any law of Canada, under an agreement with … the government of a foreign state. Other exceptions are for research purposes, and where the disclosure clearly outweighs any invasion of privacy that could result.
Principle11 Limits on disclosure of personal information	Section 8. (1) - Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section. TBS Directive on Privacy Practices Appendix C details specific requirements around disclosure to investigative bodies under paragraph 8(2)(e). TBS *Guidance on Preparing Information Sharing Agreements Involving Personal Information*[22] provides advice in the consideration and development of information sharing agreements involving personal information shared with other governments within Canada and across international borders.
Principle 12 Unique identifiers	There is no comparable prohibition except that "any identifying number, symbol or other particular assigned to the individual" is explicitly included in the definition of personal information. Protections for unique identifiers are covered in TBS documents such as the *Directive on the Social Insurance Number*[23].

22. http://www.tbs-sct.gc.ca/atip-aiprp/isa-eer/isa-eer00-eng.asp
23. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13342

2.1.2 The Framework of Formal Agreements

The FCC information exchanges are governed by the Protocol, the Hunter Valley Declaration, and a series of bilateral memoranda of understanding between pairs of participants (none of which are legally binding treaties).[24]

The Hunter Valley Declaration states:
We intend to uphold high standards of privacy and the protection of personal information, in accordance with the privacy legislation of our respective countries.

The draft MOU between New Zealand and Canada includes the commitment to:
2.6 The Participants intend to ensure that the fingerprints exchanged for searching under this MOU are not to contain fingerprint data of known FCC nationals.

This reflects similar conditions in other MOUs between the FCC participants. Consequently, neither Canadian nor New Zealand citizens would normally be subject to the activities under the Protocol. However, a match might uncover the fact that an individual using a fraudulent identity was also a citizen of an FCC country. That could result in an investigation for immigration fraud.

For example, in a match between US and UK records, a Somali asylum claimant in the UK was found to be a naturalised Australian citizen.

If a similar situation arose in New Zealand, it is possible that a person who received New Zealand citizenship by grant or descent (or the Canadian equivalents) might be retrospectively investigated for fraudulent acquisition of citizenship. Such a person would be entitled to protection under the NZ Act until after both their citizenship was revoked and they were removed from New Zealand, if either of those actions was eventually taken against them.

2.1.3 Procedural issues

The DoL immigration policy manual[25] provides standard guidelines for immigration officers. They cover the verification of credentials to meet criteria for entry visas (temporary or permanent). Verification ranges from relatively superficial checks to thorough background investigations. It may include the use of specialised expertise such as forensic analysis.

In each area of credential verification, the third tier of investigation is always an in-person interview.

Where potentially prejudicial information exists, "applicants will be given the opportunity to comment before a decision is made on the basis of any potentially prejudicial information that they are not necessarily aware of."[26]

The Canadian operational manuals mentioned above have similar instructions for officers processing applications and interviewing applicants, including providing the opportunity to respond to the officer's concerns regarding the application.[27]

In addition, clause 5.5 in the MOU permits disclosure of information received under the agreement to the subject as part of an immigration case and subject to that country's domestic laws and policies.

2.2 The Information Exchanges

As described below, the scale of the programme is limited by:

- number of agencies involved,
- number of individuals whose information will be exchanged or
- amount of information that will be disclosed

as described below.

Under the bilateral arrangement there is a cap of 3,000 match requests that can be made by each country per year under stage 2. Under a future stage 3 arrangement, this may be increased to 75,000 with Canada (refer sections 5.5.2 and 5.5.3) and FCC participants have agreed to review their privacy impact assessments before such an extension.

The costs to DoL are minimal as the initiative uses existing infrastructure and arrangements.

The information flows and key decision points are shown in the diagram in section 2.2.5.

24. Copies of the High Value Data Sharing Protocol and the Hunter Valley Declaration will be provided to the New Zealand Privacy Commissioner with this document.
25. Immigration New Zealand Operations Manual http://www.immigration.govt.nz/migrant/general/generalinformation/operationsmanual/
26. Operational Manual E7.15 http://workforce.dol.govt.nz/toolkit/html/inzmanual/index.htm
27. Found at page 39 onwards http://www.cic.gc.ca/english/resources/manuals/op/op01-eng.pdf

2.2.1 Number of Agencies

There are two New Zealand agencies involved in this bilateral exchange. The New Zealand Police currently act as custodian for DoL fingerprints and provide the expertise necessary to assess potential matches.

DoL fingerprints are stored in a segregated environment provided by the (NZ) Police and are isolated from Police records. When match files are received by DoL from Canada, the matching will be performed against these DoL fingerprints only.

Matching against the NZ Police criminal fingerprint database will not be conducted under the FCC Protocol.

Like DoL, CIC does not maintain a fingerprint database and expertise in-house. The Royal Canadian Mounted Police (RCMP) acts as custodian for the immigration fingerprints and provide the expertise for their analysis. Like the New Zealand Police, the RCMP will not retain any FCC information. If a fingerprint submitted to the RCMP matches a criminal record rather than a CIC/CBSA record, the submitting country is informed that no information can be provided. The arrangements between the CIC, CBSA and the RCMP are governed by a separate Service Level Agreement.

2.2.2 Number of Individuals

The overall FCC programme scale varies depending on the participants. In this bilateral exchange with CIC, exchanges are expected to be small in terms of numbers of cases exchanged as outlined below.

The records of known nationals of any FCC country are excluded from these exchanges. No fingerprints of any known FCC national will be sent for pseudonymous matching.

The scale of the Programme is expected to change with time.

- In stage 2, (which this PIA refers to) the exchanges will be limited to enquiries on 3,000 cases per year per participating country as processing will be largely manual.
- In stage 3, (Note: this PIA will be updated for stage 3) that maximum will increase to 75,000 cases per year from Canada and will be dependent on the development of a real-time automated identity checking system.

Initially, it is expected that New Zealand will send up to 3,000 fingerprints per year to Canada for matching. They will be sent in batches of up to 50 records with the maximum permitted being 100 records in a week.

However, those limits under the protocol may never be reached. Cases will be selected for sending to Canada according to two priority levels:

'A' - national security, asylum, fraud, compliance and detention cases where there are doubts over identity

'B' - individuals who have been granted leave to remain in NZ, but where doubts remain over identity

In order to be sent for matching, the cases will also have to meet one or more of these criteria:

- Immigration cases where identity of the individual is unknown or uncertain;
- Immigration cases where the individual's whereabouts are unknown; and/or
- Immigration cases where there is reason to suspect that the person has been encountered by more than one of the countries participating in the Protocol.

Even the potential maximum of 75,000 per year with Canada in Stage 3, is relatively small in comparison with the numbers of total cases handled by DoL as in 2008/09:

- 1.4 million people granted a temporary permit
- 88,300 permanent and long-term arrivals

New Zealand has a comparatively small number of asylum seekers. In 2008/09, only 246 people sought this status in New Zealand. If all asylum seekers were checked through the Protocol exchanges, it would amount to less than 10% of the cases allowed for matching in Stage 2.

2.2.3 The Amount of Detail Exchanged

Each match progresses through up to 3 processes of information disclosure. These are known in the Protocol as "tiers". An unsuccessful match request results in a tier 1 response which simply advises 'no match.'

INITIAL MATCH REQUEST

In the initial match request, fingerprints are encrypted and transmitted from the 'Requesting Country' to the 'Providing Country' with no accompanying identifying information other than a unique identifier (UI) and a search type code. Records sent from New Zealand use a UI

created specifically for the purposes of these exchanges not related to the core DoL UI for the individual. Canada uses their internal UI for this purpose but NZ has no continuing use for it and will delete it as soon as possible.

This has been referred to as pseudonymous or nigh-anonymous information disclosure. The UI is completely separate from any UIs used by the agencies in their own systems and any UIs that relate to the individual such as a passport number. Prints are usually sent in batches of 50 but may be sent in smaller batches if warranted.

TIER 1

All match requests are run by the Providing Country. If a match occurs, the Providing Country that received and matched the prints against their own records, will respond within three (3) days with Tier 1 information that there was a successful match. They will also include as much of the following information as they can obtain within the three days:

- date, location, and reason fingerprinted
- last name, first name, and any other names the person is known by
- date of birth, place of birth, nationality, and gender
- any travel document number(s)
- any photograph(s) held in their files or any other facial images, and/or a scan of the passport bio-data page
- any caveats around information source and usage
- other information as deemed appropriate by the Providing Country

All the fingerprint sets in a batch that did not match, will also be recorded in the Tier 1 information sheet list as a no-match (i.e. the record will give the fingerprint UI plus the NO MATCH indicator).

TIER 2

Information returned under Tier 2 is determined by the search code for each matched record. Those codes limit the information returned depending on the nature of the case. For example, the information provided for a refugee claimant will be different from that for a re-documentation case.

In addition, if the information available from the Providing Country at Tier 1 is incomplete or unavailable within those three days, the providing Country may send a second (Tier 2) information response within the next seven (7) days. That second response can include any of the standard data elements listed above that are not available in the biometric system, but are available elsewhere.

In all cases where the match includes a travel document issued by a country of which the person is not a national (e.g. a refugee travel document), confirmation of the type of document, the country of issue of the document and the nationality of the person will be shared under Tier 2. This may be accomplished through the use of, for example:

- a scan of any travel document pages showing port stamps or visas
- a scan of any additional identity documents that are available
- dates that the person was in the Providing Country, and how this is known
- current and previous immigration status in the providing country.

In all cases where a match is achieved against a watchlist, the reason for the watchlist entry should be shared.

TIER 3

If further information is required, then information sharing moves up to Tier 3. This requires the Requesting Country to send an approved FCC 'Request for Information' form to the Providing Country.

The Request for Information includes who the request is about (UI, biographic information, etc), what additional information is requested from the Providing Country, and why this information is requested.

The Providing Country may then provide further information if this is appropriate and permitted under their laws. Note: the Protocol does not require participating countries to guarantee to provide Tier 3 information.

SEARCH CODE LIMITATION

The search code attached to each initial request:

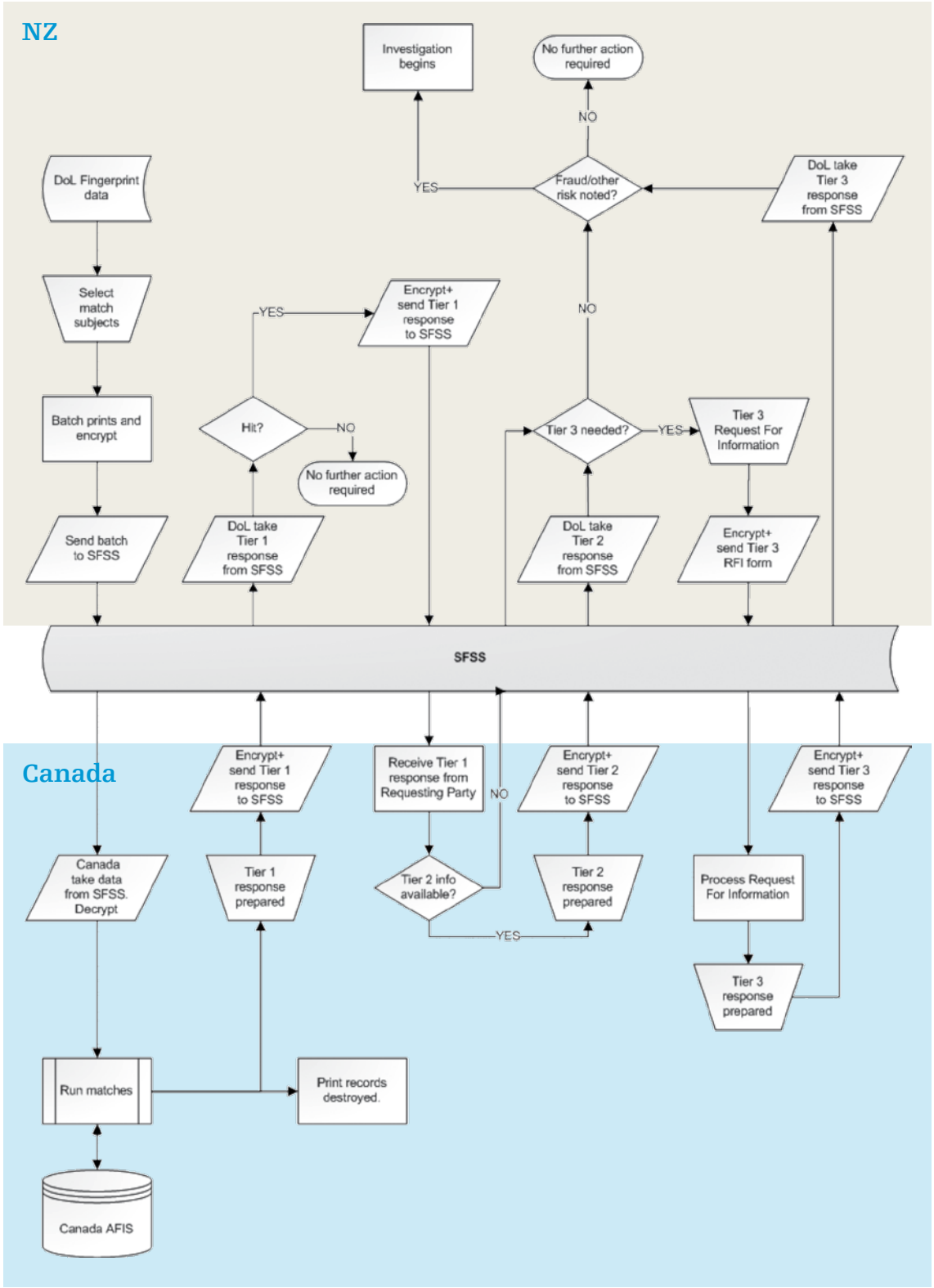
- identifies the reason for the fingerprint being sent for matching, and
- determines the type and amount of information that is sent back.

This helps to ensure that only relevant information is returned with each response.

2.2.4 The Cost of implementation

The project leverages off existing Government systems and arrangements between DoL and Police. The cost of implementation is approximately NZ$50,000.

2.2.5 The information flows and FCC Protocol data matching & sharing process



3. Compliance with the NZ Information Privacy Principles

3.1 Principle 1 – Purpose of collection of personal information

The information New Zealand receives from Canada will be used exclusively for immigration and nationality purposes. From the *MOU* clause 1.3, those are 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. The information is necessary in order for DoL to carry out its responsibilities under the *Immigration Act 1987* and *Immigration Act 2009*.

3.2 Principle 2 – Source of personal information

Neither country will be receiving the information directly from the individuals concerned. In some cases, the information they receive will not have been collected directly from the individual by the supplying agency. For example, this will be the case where the information relates to criminal activity.

DoL is authorised under the *Immigration Act 1987* to exchange information with equivalent authorities in other countries for immigration purposes by sections 141AA and 141AB of the *Immigration Act 1987* and sections 305 and 306 in the *Immigration Act 2009*.

3.3 Principle 3 – Collection of information from subject

All visa applicants complete a formal application to enter or remain in New Zealand. Application forms have a formal statement about the purpose for collection and how the information will be used and possible disclosures of the information.

All entrants to New Zealand (including those who do not require a visa to travel to New Zealand) complete an arrival card on entry that states that the information is being collected for immigration purposes. The arrival card states that the information collection is mandatory, required under the Immigration Act, contact information is provided for immigration information and enquiries, and the New Zealand Customs Service (Customs) is clearly identified as the chief collection agency with appropriate contact information provided.

There is a formal Privacy Statement explaining how the information may be shared among border agencies and a statement about authorised information matching programmes. That statement also includes information about rights of access and correction and contact information for exercising those rights.

In the case of asylum claimants, fingerprint data may be collected by a Refugee Status Officer under subsection 129 (H) (1) (e) of the *Immigration Act 1987*[28] for the purpose of ascertaining or confirming the claimant's identity or nationality.

New Zealand Police (Police) may collect fingerprint data on behalf of DoL under subsection 140 (2) of the *Immigration Act 1987* for immigration clients who are taken into custody under a Removal Order, foreign criminals who are being deported, or immigration clients, including asylum claimants, who have no appropriate documentation for immigration purposes, or who appear to hold false documents. The equivalent provision for asylum claimants in the *Immigration Act 2009* is subsection 149(1) (e) which is currently the subject of a separate Privacy Impact Assessment.

The provision relating to individuals subject to custody under the *Immigration Act 2009* is subsection 333(3) which refers to section 41 of the Corrections Act 2004 permitting the taking of fingerprints.

28. A similar provision exists in the Immigration Act 2009 s.31 for collection by a refugee and protection officer.

3.4 Principle 4 – Manner of collection of personal information

DoL's collection of information from Canada is authorised by sections 141AA and 141AB of the *Immigration Act 1987*: and by sections 305 and 306: *Immigration Act 2009.*

The initial use of pseudonymous fingerprints to determine if the agencies involved share an interest in an individual is considered privacy protective. Alternative processes would be more vulnerable to subjective assessments of interest rather than an objective measurement of the similarity of two examples of a physical characteristic.

3.5 Principle 5 – Storage and security of personal information

DoL and CIC/CBSA are required under the Protocol and the MOU to take care to protect the information against loss, misuse, and unauthorised disclosure. Information will be encrypted by an internationally accepted protocol and handled in New Zealand as required by a "restricted" classification. In Canada, the equivalent security category is "Protected B". All fingerprint information will be securely deleted from the secure file server once the match cycle has ended.

Only specified employees of DoL will be permitted access to the information and all access will be logged and audited. Similar constraints will apply at the NZ Police. Both the Canadian and New Zealand agencies are entitled to request an audit of the other's handling procedures to provide assurance that appropriate security is in place[29].

3.6 Principle 6 – Access to personal information

The Protocol requires participating countries to abide by all legal requirements within their own countries including those relating to privacy. It also requires Canada and New Zealand to notify their partner if they discover that there are any changes to the information about an individual disclosed in this programme.

The MOU clause 6.14 specifically requires the Participants to provide access and correction rights to all affected individuals:

Either participant is expected to afford to a person who is not present in the territory in which the Participant exercises jurisdiction, to whom the information exchanged under this MOU relates, access to the information as well as the opportunity to seek correction if it is erroneous or add a notation to indicate a correction request was made.

And clause 6.15 stipulates that:

The opportunity provided by either Participant for access, correction and notation with respect to such information should be afforded in circumstances similar to those available to persons present in the territory in which that Participant exercises jurisdiction.

DoL already meets the new (September 2010) requirements of the Privacy Act by providing in its internal policies the right of access and correction to people about whom it has made a decision on an immigration matter. That right would apply to anyone subject to this exchange. Specifically:

In immigration matters, where the Department has made a decision on a person's application for a permit or a visa, the Department's policy is to respond to requests as if the person were eligible to make a request, even where they are not a New Zealand citizen or resident, and are outside New Zealand.[30]

However, even if an apparently ineligible individual is refused access to personal information, the letter they receive includes reference to their ability to contact the Office of the Privacy Commissioner. This is so that they can make their views known to the Commissioner or receive confirmation directly from the Commissioner that she has no jurisdiction to investigate the matter.

As discussed earlier, CIC have similar operational provisions to provide access to personal information for those not entitled to such access under the CA Act.

29. Under the MOU clause 6.19

30. Privacy Act Policy 2005 section A.3 http://www.dol.govt.nz/PDFs/privacyactpolicy.pdf

3.7 Principle 7 – Correction of personal information

As mentioned above, the MOU requires Participants to extend access and correction rights to all affected individuals which is in line with the recent amendments to the NZ Act.

In addition, the protocol requires that *"all countries should notify one another of any data errors discovered"* and clauses 6.11 – 6.13 of the MOU address processes to ensure that information is accurate and that Participants notify each other of corrections, deletions, additions, etc.

As discussed earlier, CIC have operational provisions to provide access to personal information and rebuttal of that information for those not entitled to such access under the CA Act or its extensions.

3.8 Principle 8 – Accuracy, etc, of personal information to be checked before use

The Protocol and MOU both require that the agencies abide by this principle. Specifically, the Protocol requires that:

6.2.4 Personal information, should, to the maximum extent feasible, be as accurate, timely, relevant, and complete as reasonably necessary to assure the propriety of identification of individuals whose personal information is contained in the system and of actions taken under this agreement with respect to that information.

3.9 Principle 9 – Agency not to keep personal information for longer than necessary

The Protocol and MOU both restrict retention of information exchanged under these agreements. Specifically the MOU states:

6.15 Subject to paragraph 2.12, each Participant is expected to assess the continued relevance of the information received under this MOU to its immigration and nationality purposes, and to destroy the information securely when it is no longer relevant. In particular:

i. Data subject case file. Personal information which is retained on an electronic or paper case file relating to the data subject, because it has ongoing relevance to that file, may be retained as part of that file in accordance with the domestic laws and data retention policies of the Participant that has received it.

ii. Watchlists. Personal information relating to:

a) false identities and travel documents;

b) multiple identities used by the same person; and

c) persons engaged in derogatory activity that would render them inadmissible to the territory of the Participant that has received it may also be retained for as long as it is relevant to that Participant's border controls, up to an initial maximum of ten years from the date of receipt. As part of their ongoing review of watchlist entries, the Participants will discuss the continued relevance of the information and seek approval before ten years on information appropriate for retention for a further period.

iii. Data held by central Protocol team. Personal information which is otherwise retained, in a central record of information received or otherwise, may be retained for no longer than two years from the date of receipt.

Any further retention is subject to the prior written approval of the Participant that supplied the information.

3.10 Principle 10 – Limits on use of personal information

There are specific legislative provisions for these exchanges: disclosure overseas is covered by sections 141AA and 141AB of the Immigration Act 1987. In the Immigration Act 2009 it is covered by sections 305 and 306.

3.11 Principle 11 – Limits on disclosure of personal information

There are specific legislative provisions for these exchanges: disclosure overseas is

covered by sections 141AA and 141AB of the Immigration Act 1987. In the Immigration Act 2009 it is covered by sections 305 and 306.

3.12 Principle 12 – Unique identifiers

New Zealand will only use its own assigned UIs within its own systems – for example client identifiers from the New Zealand Application Management System (AMS) will not be disclosed to Canada. When sending records to partner countries, New Zealand will create special UIs to identify each set of fingerprints. They will only be used for the exchanges and will not be entered into permanent DoL client records.

Canada uses its internal client UI to identify fingerprints sent to New Zealand but DoL has no internal use for that information and will delete it as soon as possible.

Once follow-up information is required, the participants will identify the persons of interest by standard biographic data and with photographs. However, the information transferred after the match may include information about travel documents including passports which contain UIs. Those UIs will be stored and used by the participants but will not be assigned by them to the individuals for the purpose of uniquely identifying the individuals.

Both participants already have successfully functioning systems for assigning unique identifiers to clients within their systems. Assigning these additional and questionable UIs would be inappropriate and counter-productive. As some of those "secondary" UIs may be from fraudulently acquired documents they are unsuitable for use as anything other than a piece of information about the individual.

Fingerprints received by each participant will be processed through that participant's fingerprint analysis systems and the biometrics templates created used to search for matching fingerprints within the receiving participant's records. Fingerprint information sent under the Protocol will be destroyed after use.

4. Additional Protections for the Privacy of Affected Individuals

4.1 Informing people likely to be affected

DoL published a formal notification prior to implementation of the FCC Protocol. This notification was placed on the DoL website and other relevant media channels.

During the initial period (July 2010 until full implementation under the Immigration Act 2009) fingerprint collection will be as authorised or required under the Immigration Act 1987.

4.2 Security of on-line transfers of personal information

The information transfers for the matches will be through a secure file transfer system hosted by the Australian Government. All transmissions will be encrypted. In the event of failure of that system, the Protocol calls for alternate secure encrypted electronic transfers. As a last resort, encrypted electronic files may be transferred physically through diplomatic channels.

The information on the SFSS is contained within a dedicated directory structure. Each bilateral MOU is assigned a separate sub-folder and only registered authorised users from the two relevant FCC participants can access each sub-folder. So, for example, only registered NZ and Canadian users can access the NZ-Canada folder.

4.3 Technical standards of operation

A copy of a draft Technical Standards Report (TSR) is provided with this document to provide additional background information on how the exchanges will operate.

In the interests of continued transparency of operation, any variations to that TSR before the commencement of operation of the matching programme will be reported to the Privacy Commissioner. Similarly, any changes to the TSR that are agreed to by the agencies after the commencement of the match will also be provided to the Privacy Commissioner.

4.4 Safeguards for individuals affected by the results of the exchanges

The structured and controlled release of information according to the Protocol helps to protect individuals from poorly considered actions being taken as a result of the match.

When a confident match on the fingerprints is made the requesting agency will receive Tier 2 information. In New Zealand, all automated fingerprint matches on FCC fingerprints are manually confirmed by a NZ Police fingerprint expert.

In Canada, all fingerprints received will be assessed for "image quality" before being processed against the RCMP files. If the fingerprints are of a sufficient quality to conduct a confident and reliable search of the AFIS the search will be conducted. Fingerprint sets that do not meet the image quality threshold (for example, fingerprint images which are not completely recorded or friction ridge detail which is indistinct) will be subject to human examination and possible rejection.

Tier 2 information includes a photo of the individual, if available. That allows the receiving country to compare the more detailed information against its own records. It should help to confirm or disprove whether the individual concerned is likely to be the same person.

DoL has a structured process for assessing information about applicants for entry to this country. It will be applied to all matches under the Protocol. The process has five stages for each type of information assessed and level three is an interview.

Included in this process is a letter outlining all Potentially Prejudicial Information (PPI) available[31] related to the individual's case.

31. Subject to the withholding provisions in the Privacy Act Parts 4 & 5.

That letter invites client comment or explanation which may be done through an interview if appropriate. The case is re-assessed once client comment is obtained, and a final immigration decision is made. If the client is unsatisfied with the outcome, there is a well established administrative review process followed by a formal appeals process.

4.5 Destruction of biometric information

The Protocol requires participating agencies to destroy the matching information as soon as the match has been performed. This is enforced by the SFSS system, which automatically purges all bilateral folder data seven days after the information has been downloaded by the Providing Country.

The Protocol also requires that the more detailed information received after a successful match should be kept for no longer than 10 years, as follows:

6.2.6 Unless otherwise agreed, the Providing Country should destroy the biometric data received from the Requesting Country straight after matching has been completed.

6.2.7 Unless otherwise agreed and in accordance with all requisite national laws of the Five Countries, returned results (see 8.3.3) should be retained by the Requesting Country for no longer than ten years, as codified in the bilateral memoranda referenced in section 7.

The MOU clause 6.15 requires each participant to assess the continued relevance of the information received under the MOU to its immigration and nationality purposes, and to destroy the information securely when it is no longer relevant. It also requires participants to delete information if requested by the providing agency.

4.6 No new databanks or new shared databanks

No new fingerprint databank or register of individuals will be created as a result of this match. DoL will retain information received from Canada for as long as it takes to either confirm or deny its validity with respect to the individual whose fingerprints appear to match those in Canada's records. The SFSS does not act as a databank and all biometric holdings are self-purged.

If the information is found to be true of an individual in DoL's records, it will be kept according to the requirements under the Immigration Act (1987 and/or 2009 respectively) for the determination of the individual's eligibility for entry or continued stay in New Zealand. If adverse action is required, the information will be kept for as long as the Act requires and at least until all appeals are exhausted.

4.7 Operation only under the provisions of the FCC High Value Data Sharing Protocol and the MOU between Canada and New Zealand

No matches will be undertaken until after the MOU between DoL, CIC and CBSA has been signed. New Zealand and Canada have already signed the Protocol. These two documents, in their practical effects, form the arrangement to match information.

The agencies in this bilateral agreement will not charge each other fees for stage 2 exchanges. The matter of cost sharing for stage 3 has not yet been determined.

4.8 No unreasonable delays in acting on the information received

DoL undertakes to decide if at all possible within 60 days on whether it will take adverse action against an individual and actually carry out that decision within 12 months of operating the match.

The time constraints agreed to in the Protocol are specific enough that DoL will have sufficient information to request the client explain the new information within specified time frames or flag that client record if DoL has lost touch with the client.

4.9 Advising individuals about possible adverse action as a result of the matches

DoL's standard processes for handling immigration applications of all types will apply. Those processes include informing applicants about PPI held or acquired by the DoL and inviting them to respond with an explanation, comment, or refutation. Typically, that is done through a letter and may include an interview[32].

4.10 Public reporting on the matches

DoL is willing to provide the Privacy Commissioner with an annual report on the results of the FCC Protocol. It may also make this information publically available, for example on its own website. Publication will demonstrate the actions undertaken to ensure the integrity of our border and refugee processes, and to deter potential fraud.

32. Subject to the withholding provisions in the Privacy Act 1993.

Abbreviations Used

Responsible agencies	NZ Department of Labour Citizenship and Immigration Canada
DoL	NZ Department of Labour
CA Act	The Canadian *Privacy Act 1985*
CIC	Department of Citizenship and Immigration Canada
CBSA	Canada Border Services Agency
RCMP	Royal Canadian Mounted Police
DIAC	Australian Department of Immigration & Citizenship
MOU	Memorandum of Understanding between The New Zealand Department of Labour and The Citizenship and Immigration Canada.
NZ Act	The New Zealand *Privacy Act 1993*
The Protocol	High Value Data Sharing Protocol of the Five Country Conference
FCC	Five Country Conference
PIA	Privacy Impact Assessment
PPI	Potentially Prejudicial Information
SFSS	Secure File Sharing Server (operated by DIAC)
Requesting Country	The Country sending to the other Country (the 'Providing Country') either an initial biometric information match request, or request for further information following a successful biometric match
Providing Country	The Country which receives the initial biometric match request from the Requesting Country and either matches the biometric provided against the specified database, or who provides information to the Requesting Country from the specified databases.
UI	Unique identifier
Watchlist	Personal information relating to: i. false identities and travel documents; ii. multiple identities used by the same person; and iii. persons engaged in derogatory activity that would render them inadmissible to the territory of the Participant that has received it

newzealand.govt.nz

DOL 11600 DEC 10