

# **REGULATORY IMPACT STATEMENT – IMMIGRATION ACT: BIOMETRIC IDENTITY INFORMATION**

## **Statement of the Public Policy Objective**

To ensure the legislation provides for the use of technology to protect New Zealand's borders and the integrity of the immigration system.

## **Statement of Feasible Options**

### ***Power to require the provision of biometric identity information***

**Policy Problem and Magnitude:** Identifying people is a crucial element in facilitating the entry of non-citizens to New Zealand and managing the potential risk of identity fraud. Improvements in document forgery and increasing identity theft has led to more opportunities for individuals or organised groups to circumvent New Zealand's border controls. The Department of Labour (the Department) has identified many cases of individuals lodging multiple refugee claims under different identities and people who have been removed from New Zealand returning under new false identities.

Reliance on traditional paper-based identity documents is becoming increasingly inadequate to manage identity fraud risks to New Zealand. This is particularly true for very high-risk individuals on terrorist, Interpol and other criminal watch lists. Such individuals seldom travel using their own, genuine travel documents.

The Department cannot currently ensure that every person entering New Zealand on a visa is the same person that applied for that visa. The Department cannot ensure that a person previously removed or deported from New Zealand or who appears on alert lists, and who enters under a new fraudulent identity, is detected. Investigations may reveal identity fraud, but these investigations are time and resource intensive, and are only undertaken where there is suspicion around an application or individual.

**Status Quo:** Comparison of an individual with their identity documentation is done through a face-to-passport check on enrolment and on arrival and at various other interactions with the Department within New Zealand and/or during travel to New Zealand. Comparison of individuals with alert list information is based on known names and aliases, or a visual comparison with photographs.

**Preferred Option:** To enable immigration officers to require the provision of biometric identity information (such as photographic/facial recognition, iris and fingerprint information) from non-citizens engaging with the immigration system, seeking to travel to, enter, or remain in New Zealand. This information would be stored and used to confirm the individual's identity in future interactions with the Department.

The proposal also would also allow immigration officers to require the provision of photographic/facial recognition based biometric identity information from those presenting at the border as New Zealand citizens to confirm their citizenship (and

therefore their right to enter New Zealand). This information would not be stored unless a discrepancy was noted and the information was required as evidence.

**Net Benefit of the Proposal:** The systematic use of biometric information within the context of an immigration identity management framework would benefit government by:

- improving the integrity of the immigration system in terms of:
  - identity confirmation in immigration decision-making and confirming the identity of a non-citizen if they seek New Zealand citizenship
  - providing greater assurance that identity fraud and persons posing risks to New Zealand will be detected
- enabling the detection of multiple, false uses of an identity or attempts by an individual to enter or remain in New Zealand under another identity
- allowing for processing immigration applications more quickly and effectively
- facilitating processing of arrivals at the border, particularly of those deemed “low risk” travellers and New Zealand citizens, which would improve processing times in airports and assist in reducing peak processing time congestion, and
- taking advantage of technology to automate the current face-to-passport check that is a standard aspect of current border processing, reducing the subjectivity of this comparison.

Biometric identity information is not perfect and may generate false connections. This can be managed by the Department continuing to rely on documentary evidence to support the immigration process, and noting that a discrepancy may be an error, or the result of previous fraud.

False matches will require some additional processing by immigration staff. However the use of this system is likely to allow the Department to focus such additional verification work on potential risks rather than spread verification resource across all applicants/arrivals. Processing for people not previously enrolled in the system may cause some delays on arrival to New Zealand. However, the proposed systematic collection of information on all arrivals at international airports, as well as reduced processing times for “low risk” travellers, are likely to mitigate delays.

### **Statement of Consultation Undertaken**

**Stakeholder Consultation:** Many submitters commented on the safeguards for the use of biometric information that need to be addressed in the legislation. Submitters commented that the legislation should be consistent with privacy and human rights legislation. A number of submitters also commented on the reliability of the technology used to collect biometric information. One submitter commented that facial recognition technology had been found to be inaccurate in some countries. Another noted that DNA testing requires a sufficient database of the background ethnic population, which may not always be possible in the immigration context. Others commented that reliability issues need to be addressed in the legislation.

**Government Departments/Agencies Consultation:** The Ministry of Justice did not support the proposed power being activated in the new legislation without the chance for the Privacy Commissioner to be consulted on an actual implementation proposal. This has been addressed by proposing that these powers be activated through an Order in Council process following consultation with the Privacy Commissioner, the Ministry of Justice and the Department of Internal Affairs on an implementation proposal.