Regulatory Impact Statement

Facilitating better information sharing: Using personal information for identity verification purposes in law enforcement

Agency Disclosure Statement

This Regulatory Impact Statement has been prepared by the Ministry of Justice. It provides an analysis of options to facilitate better information sharing for the purpose of identity verification in law enforcement.

The 'Government Inquiry Into Matters Concerning The Escape Of Phillip John Smith/Traynor' (the Inquiry) and the 'Multi-agency Review of the Phillip Traynor Incident' have detailed the weaknesses in our identity verification processes. These weaknesses largely stem from government agencies failing to share information necessary to verify whether individuals are who they say they are and whether they are permitted to leave the country.

The main constraint that we have faced in our regulatory impact analysis is time. The Government has committed to introducing legislation as quickly as possible to improve the ability of agencies to verify identities. This is compounded by the Government's decision to not implement recommendations by the Inquiry and to consider the full range of tools to enable better information sharing. This has resulted in the following constraints in our regulatory impact analysis:

- Limited opportunities for detailed agency consultation – We have not had sufficient time to collect definitive information from agencies regarding their information needs, but we have worked closely enough with key agencies to gain clarity for the purposes of designing a legislative mechanism.
- Privacy aspects: We have also been unable to consult the Privacy Commissioner, and we will look for opportunities to involve them as we proceed to the detailed design.
- Scope of change – The scope of change for the purposes of this analysis is restricted to identity verification. We intend to consider more transformative options over coming months.
- Evidence base – The Smith-Traynor review has made useful evidence available to guide the policy analysis, but its scope was limited to a fairly specialised facet of the identity verification landscape. We will undertake wider analysis of agency needs and drivers as part of our further work on information sharing.
- Costings – We have not been able to assess definitively the fiscal cost that may result from the options, but the legal mechanism to enable information sharing for identity verification purposes need not be tied to a particular technical solution.

Chris Hubscher,
Manager, Electoral and Constitutional Policy
Ministry of Justice

Status quo and problem definition

The Privacy Act provides tools to share information, while protecting individual privacy

1. The Privacy Act 1993 determines how agencies collect, use, disclose, store and give access to personal information. The Act provides a number of tools that enable sharing of personal information. Information sharing generally occurs in the public sector due to the unique need to deliver social services. These tools have detailed safeguards that ensure information sharing occurs only when there is a legitimate need for another agency to use that information. This in turn upholds the privacy of individuals.

A serious event led to the examination of identity management in government systems

2. In November 2014, a prisoner serving a life sentence for murder, illegally departed New Zealand while on temporary release from prison (the 2014 event). The prisoner left New Zealand on a passport under his birth name, having renewed his passport while in prison. He was subsequently arrested in Brazil and returned to prison in New Zealand.

3. The 2014 event was reviewed by an independent inquiry (the inquiry). This brought overlooked weaknesses in identity verification management to the attention of the government and wider public. The inquiry found that while systems and practices of relevant criminal justice agencies are not broken in a fundamental way, the management of identity verification provides an unacceptable risk to society. A multi-agency review was also completed with affected agencies examining how to improve their systems within existing means.

Legislative and technical barriers hinder information sharing among agencies to verify identity

4. There are legislative and technical barriers to information sharing among agencies which hinder identity verification and create gaps that can be exploited. These can be organised into three key problem statements:

    a) The New Zealand Police do not have access to sufficient and timely official identity information when establishing the identity of individuals if they have not previously entered the criminal justice system

    b) The identity established by prosecuting agencies is not required to be anchored to an official identity. Other government agencies are not reconciling the identities used by prosecuting agencies with identities in their systems

    c) Border agencies (Immigration New Zealand and New Zealand Customs Service) do not have sufficient access to personal information about individuals who should not be entering or leaving the country.

5. These problems are likely to produce system failures in a small number of cases. However, as the 2014 event highlighted, each failure has significant implications for the criminal justice system (such as to public safety, international reputation and fiscal costs).

6. Effective identity verification is also relevant for special and restricted mental health patients as well as special care recipients under the Intellectual Disability (Compulsory Care and Rehabilitation) Act 2003. The Ministry of Health considers that these individuals should not be able to leave New Zealand or be in the community without permission.

The New Zealand Police rely on personal information they generate when holding people in custody

Summary: The New Zealand Police do not have access to sufficient and timely official identity information to establish the identity of individuals if they have not previously entered the criminal justice system. Restrictions on the ability to access and use personal information collected by other agencies limits their ability to identify new offenders effectively. This consequently limits Police's ability to provide services pertinent to an individual's needs.

7. In general, ascertaining the identity of a person who has previously been arrested and charged and to whom a Person Record Number[1] has been assigned is a relatively routine and error-free procedure for Police. The Police information management system holds biographical details, a photograph, criminal history details and fingerprint information of previous offenders.

8. Police file about 80 percent of all charges in New Zealand. Under the Policing Act 2008, Police have the power to take "identifying particulars" of those in custody or suspected of committing an offence. Identifying particulars are:

   - the person's biographical details (for example, the person's name, address and date of birth),
   - the person's photograph or visual image,
   - impressions of the person's fingerprints, palm prints or footprints.

9. Initial checks of biographical details can be carried out by using mobile devices carried by Police on patrol, over the radio or by any Police computer. Fingerprints stored in the Police Automated Fingerprint Identification System can verify the identity of a person who has previously entered the criminal justice system and whose details are stored in the Police information management system (National Intelligence Application).

10. Identity problems, however, may arise in situations where a person is stopped or arrested who has not previously entered the criminal justice system. In most cases such a person provides their true identity. But that is not always the case. In some cases, false identities may be given. Verification by way of information held by other agencies would mitigate the risks that arise when a person uses a false or alternative name to his or her official name.

11. However, the systemic difficulty is the lack of efficient access to information that would verify official identity. This flows from perceived legislative barriers and lack of interoperability between ICT systems in the justice, border and identity sectors.

Identity generated by prosecuting agencies are not anchored to an official identity

Summary: The identity established by prosecuting agencies is not anchored to an official identity, allowing individuals to be charged under an assumed name. Government agencies are not subsequently reconciling this identity with personal information held by each agency. This restricts how agencies identify offenders and fraudulent behaviour.

12. The Police and other prosecuting agencies (eg Customs) are not required to verify official identity at the point of charge. An alleged offender, whether arrested or summonsed, may be charged under an official or assumed name depending on the information available and the

[1] In use across the justice sector (used by New Zealand Police, the Ministry of Justice, and the Department of Corrections)

judgement of the charging officer. In many cases, an offender may be charged under an assumed name, for example:

- an alias or informal name
- a name supported by a New Zealand driver licence that might not necessarily reflect that person's official name
- a name used by a foreign-born person that does not match the name in their passport.

13. Verifying official identity for such people can be challenging for Police. Internal Affairs has an Identity Information Confirmation Service providing real-time lookup facilities for authorised agencies to receive confirmation of birth, death, marriage, civil union, citizenship and passport information under the Identity Information Confirmation Act 2012.

14. However, the Identity Information Confirmation Act requires the consent of the individual whose information is sought. If the individual does not consent, Police Officers requiring this information must make a manual request to Internal Affairs. This is normally responded to on the same business day, but there is no out-of-hours service. This has obvious limitations for 24-hour Police operations. Further, Police do not have immediate access to identity information for foreign persons entering the criminal justice system for the first time.

Border agencies (Immigration and Customs) do not have sufficient access to personal information about individuals who should not be entering or leaving the country

Summary: Border agencies (Immigration and Customs) do not have sufficient access to personal information about individuals who should not be entering or leaving the country. The current approach to verification of identity is inefficient and requires significant resources. This slows processes and limits the ability for Police Officers to detect fraudulent behaviour.

15. The border alert system is relatively resource intensive, produces a high number of false positives, and has capacity issues. To a large extent, these issues are driven by gaps in the base offender identity management system, e.g. many aliases, a lack of authoritative biometric information, and the possibility of fraudulently obtaining a passport.

16. Approximately 14,000 intercept alerts on departure are active in Customs' information management system at any given time. Alerts are put in place for a range of individuals, such as individuals with warrants for arrest, or individuals prohibited from leaving the country as part of their community-based sentence. Once an alert is triggered, a customs officer must take steps to see whether the traveller is the person to whom the alert properly relates. For Corrections border alerts, this checking procedure means an outbound passenger has to be stood to one side while, a Customs Officer in a control room telephones a Corrections number to seek information to verify the individual. The Corrections number is staffed 24 hours per day and responds to requests for biographical details and a photograph of the person to whom the alert relates. This checking procedure can take anything from 5 to 30 minutes.

17. Longer time frames may occur where confirmation is required from Community Corrections that an offender has approval to travel, or where airport Police attempt to cross-reference Police information management system's identity and photograph information. Confirmation of the person is determined by the three agencies' agreement. Customs is concerned with the possibility of reputational damage should, as a result of a false positive, a passenger miss their outbound flight.

18. The efficiency of the system depends on the technical solution that provides the information. The option resulting from this paper will only partially deal with this issue. Efficiency will be dependent on enforcement agencies implementing an effective technical solution.

Objectives

19. To develop the options that ameliorate the problem whilst providing a robust regulatory solution, the following two primary objectives have been developed, both with complementary secondary objectives:

- ***Primary objective A [Effectiveness]*** **–** Enforcement agencies[2] can verify the identity of individuals by using relevant biographical or biometric information
  - ***Secondary objective A*** **–** The personal information is provided to law enforcement agencies in a timely and cost-effective manner with data quality caveats that enable officials to make well-informed assessments on the identity of individuals
- ***Primary objective B [Proportionality and transparency]*** **–** Information shared for identity verification purposes upholds the privacy of New Zealanders with sharing targeted to likely identities and being proportionate to the need for the information
  - ***Secondary objective B*** **–** The public has trust and confidence in the security and integrity of the processes that law enforcement agencies undertake when obtaining or using personal information to verify identity.

20. The preferred solution needs to be implemented in a timely manner to ameliorate the ongoing risk of shortcomings in identity verification in the criminal justice system.

Options and impact analysis

21. The Privacy Act 1993 provides that, generally speaking, personal information collected for one purpose cannot be used for any other purpose[3]. This means that any change to the status quo will require legislative amendments or the use of existing regulatory tools in the Privacy Act 1993.

22. There are also a range of statutory provisions outside the Privacy Act that limit the sharing of certain personal information (eg section 200 of the Land Transport Act 1998). Relevant agencies have taken responsibility for highlighting these provisions that need to be amended to enable information sharing.

23. Bespoke legislation has not been considered as part of the options analysis. Bespoke legislation should be considered when the proposals are inherently inconsistent with the Privacy Act. In this policy process, the strategic objective is to manage a range of information flows for a defined purpose. This requires an enabling mechanism, but is not a radical departure from the concepts in the Privacy Act. It is also desirable from an accessible law perspective to keep privacy related matters together in a single piece of legislation.

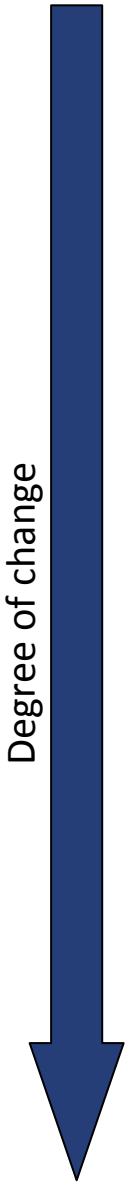
24. To meet the objectives stated, five options have been identified for comparison with the status quo. These options are mutually exclusive means to achieve the same outcome. The table below outlines the options and the degree of change from the status quo. The degree of

---

[2] New Zealand Police, Ministry of Justice, Immigration New Zealand (Ministry of Business, Innovation and Employment), New Zealand Customs Services, Department of Internal Affairs.

[3] Information Privacy Principle 10 – Limits on use of personal information.

change notes the scale of resources required to design and implement the legislative mechanism.



Option	Description and change from status quo
Status quo	Agencies continue to use available biographical information to verify identity under existing statutory constraints.
Information matching agreement	NZ Police will be included as a specified agency in the information matching provisions in the Privacy Act. This will provide NZ Police with the ability to enter into information matching agreements to facilitate transfers of information through database-to-database matching with other agencies.
Schedule 5 amendment	Schedule 5 of the Privacy Act will be amended to include law enforcement agencies and the personal information they can share with other named agencies. This will allow request-based access when necessary to verify identity. Legislative safeguards will be attached to define the scope of sharing.
Approved information sharing agreements	Agencies would create approved information sharing agreements in accordance with Part 9A of the Privacy Act. Depending on implementation, this would likely lead to two separate agreements – one for border processes and another for fraudulent behaviour on suspicion of offending. This could allow both request-based and large-scale data transfers.
Code of Practice	Agencies could ask the Privacy Commissioner, in accordance with Part 6 of the Privacy Act, to issue a Code of Practice that exempts them from the Information Privacy Principles that need to be overridden in order to share information. This could allow both request-based and large-scale data transfers.
General empowering provision	A provision could be put into the Privacy Act that generally empowers law enforcement agencies with real-time access to personal information if it is for the purposes of maintenance of the law.

25. The following table provides impact analysis of each option. The impacts are rated either: significant, moderate, or minimal. This enables the analysis to weight the outcomes and determine the overall impact of option.

Options – compared with status quo	Advantages	Disadvantages	Overall impact
Information matching agreement	**Moderate** ***Effectiveness –*** Agencies will have access to information matches, but this will continue to be provided through large transfers of information. ***Proportionality and transparency –*** Inbuilt transparency and safeguard measures contribute to greater levels of public trust compared with other mechanisms. This includes the Privacy Commissioner's ability to review agreements and report to Parliament on the operations of information matching programmes.	**Moderate** ***Effectiveness –*** Information matching agreements are organised around the bulk transfer of databases from one agency to another. This data can become out of date quickly post transfer, which detrimentally affects decision-making. ***Proportionality and transparency –*** The amount of data transferred is not proportionate to the need for that information.	**Neutral impact** Would have some benefit because it is a reasonably transparent process. However, this is negated by the transfer of bulk data providing a disproportionate amount of data flowing between agencies, which then becomes out of date quickly.
Schedule 5 amendment	**Significant** ***Effectiveness –*** Will provide agencies with access to the specific information needed to identify individuals. ***Proportionality and transparency –*** Provides the empowering of information sharing to verify identity in one accessible place in the Privacy Act. It provides for a performance-based technical solution that can be developed to meet the safeguard protections required.	**Minimal** ***Effectiveness –*** Will require amendments if agencies develop new functions or obtain new needs for verification in processes yet to be developed. ***Proportionality and transparency –*** Does not include built-in safeguards or transparency measures. However, this mechanism requires such features to be added on at the implementation stage, which will uphold public trust.	**Significant benefit** Accessible mechanism that will provide transparency and uphold public trust. Safeguards are not built-in, however. Legislative safeguards will be provided through the ability for Privacy Commissioner consideration and clearly defined boundaries of what can and cannot be shared.
Approved information sharing agreements	**Significant** ***Effectiveness –*** Experience with this mechanism aids in understanding how it can be used effectively. These agreements can be multi-lateral, reducing the need for a significant number of approved information sharing agreements. ***Proportionality and transparency –*** The transparency and safeguards are built-in, assisting with public trust and confidence. These include Privacy Commissioner oversight and public reporting.	**Moderate** ***Effectiveness –*** This mechanism requires significant resources initially to identify the technical solution before agencies are empowered to share. There is a general perception that this mechanism includes a process that is bureaucratic and unwieldy. This has the effect of this process being perceived as a disproportionate cost to the outcome. ***Proportionality and transparency –*** There are very limited disadvantages relating to this objective.	**Minimal benefit** The mechanism enables effective information sharing while providing high levels of transparency. However, there is a perception that the process is bureaucratic and unwieldy compared to the outcome, so will attract undesirable costs and resources for agencies. It will also require significant resources to determine a technical solution before the agreement can be completed.
Code of practice	**Significant** ***Effectiveness –*** Will relax provisions to empower the sharing of information needed to achieve the outcomes. ***Proportionality and transparency*** **-** The control of this mechanism sits with the Privacy Commissioner. Transparency and safeguards are also built-in to the mechanism due to Privacy Commissioner oversight.	**Moderate** ***Effectiveness –*** Control of this mechanism sits with the Privacy Commissioner. This means that the Privacy Commissioner will make the ultimate decisions around how it will operate and whether amendments can be made. ***Proportionality and transparency –*** There are very limited disadvantages relating to this objective.	**Minimal benefit** This is a strong transparency and oversight mechanism. However, it provides little flexibility due to the oversight and control the mechanism provides for the Privacy Commissioner.
General empowering provision	**Significant** ***Effectiveness –*** Will relax provisions to empower the sharing of information needed to achieve the outcomes, while being future-proofed for developments in technology and agency needs. ***Proportionality and transparency –*** Brings statutory provisions together and is easy to access and implement.	**Significant*** ***Effectiveness –*** There are very limited disadvantages relating to this objective. ***Proportionality and transparency –*** It could be challenging to develop specific safeguards for a generic provision in the absence of understanding the service design model. *However, once the scope is defined this option may have a moderate or minimal impact.	**Neutral impact*** The empowering provision will be effective in enabling information sharing, but may not provide sufficient safeguards to protect the privacy of individuals. *Once the scope is defined, this will likely improve proportionality and transparency. The impact may then provide a moderate or significant benefit.

Consultation

26. The regulated parties[4] have been involved in the analysis and resulting proposal. All of these agencies were involved in the Multi Agency Review following the 2014 event. They support the use of Schedule 5 to facilitate sharing between law enforcement agencies for identity verification purposes as one potential option. NZ Police, however, prefer the option of a general empowering provision as they consider that it provides the best opportunity for a wider information sharing cultural change amongst government agencies.

27. Wider consultation on this analysis and resulting proposal has been limited due to timing constraints. Consultation with agencies[5] was conducted in a short timeframe. Further discussions with agencies are necessary to gain better insight into how options might be operationalised.

28. The Ministry of Justice internal Regulatory Impact Analysis panel have reviewed this Regulatory Impact Statement. They consider that it partially meets the quality assurance criteria.

Conclusions and recommendations

29. This analysis of options has highlighted that an amendment to Schedule 5 of the Privacy Act 1993 will best meet the objectives stated. However, further development of a general empowering provision could provide similar benefit if the safeguards are effective in providing transparency and proportionality.

30. The schedule 5 option would be a timely solution that enables sharing between key agencies. The option will also provide necessary transparency to the public regarding which information is shared and when. The safeguards attached to this option will help uphold public trust and confidence.

31. The regulated parties, excluding the NZ Police, support this option as the best means of achieving the stated objectives.

Implementation plan

32. Successful implementation will be reliant on the engagement of the regulated parties and their subsequent discussions with the Office of the Privacy Commissioner.

33. The Ministry of Justice alongside the Government Chief Privacy officer will work together to create an operational framework that:

- enables proportionate sharing (likely through a request-based system)
- produces protocols that uphold the privacy of individuals
- encourages engagement with the Privacy Commissioner, who may then provide formal comment to the Minister of Justice.

---

[4] New Zealand Police, Ministry of Justice, Immigration New Zealand (Ministry of Business, Innovation and Employment), New Zealand Customs Services, Department of Internal Affairs and Ministry of Health.

[5] The Treasury, Ministry of Health, Customs, Department of Prime Minister and Cabinet, State Services Commission, Ministry of Business, Innovation and Employment, Department of Internal Affairs, Department of Corrections, New Zealand Police, Ministry of Transport, New Zealand Transport Agency.

34. The discussion regarding technical solutions is ongoing and agencies are accountable to their Ministers for implementing a cost-effective solution.

Monitoring, evaluation and review

35. The Ministry of Justice will continue to monitor and evaluate the effectiveness of the Privacy Act and relating regulatory tools in accordance with its stewardship obligations. The Ministry of Justice is accountable to the Minister of Justice and the State Services Commissioner regarding its stewardship obligations. To give effect to this obligation, the Ministry of Justice will continue to engage regularly with the Government Chief Privacy Officer and the Office of the Privacy Commissioner about the state of information sharing in the public sector. We will also continue to examine cases and data regarding information sharing provided by these monitoring stakeholders.

36. The responsibility for effective information sharing practices lies with the regulated parties. These parties are required to work collaboratively to achieve goals (such as by sharing information) as part of their own stewardship obligations. The Ministry of Justice and the Government Chief Privacy Officer will continue to be available to discuss how information sharing arrangements can be improved through legislative and non-legislative means (respectively).

37. The Office of the Privacy Commissioner will be able to enquire and investigate any information sharing practices. This provides the public with trust and confidence that the parties may be investigated by the Privacy Commissioner through either a proactive investigation or a complaint from a member of the public.