Proposal to make an Approved Information Sharing Agreement (AISA) to share information on name changes, deaths, and non-disclosure directions

Summary of submissions

May 2019

1.0 Executive Summary

This report summarises the submissions made to the public discussion document: *Information Sharing Agreement for the supply of registered deaths, name changes, and non-disclosure directions to assist New Zealand Police for law enforcement purposes.* The discussion document was jointly produced by Police and the Registrar-General, Births, Deaths and Marriages (Registrar-General). It outlined a proposal for the two parties to enter into an Approved Information Sharing Agreement (AISA). Under the AISA the Registrar-General would share some specific information with Police regarding registered name changes, registered deaths, and non-disclosure directions.

This report summarises the feedback received from submitters in response to the consultation. This feedback will be used to inform further policy development and to provide advice to Ministers.

Five submissions were received. In summary, there was broad support for the AISA across submitters, although three submitters made suggestions to improve/revise the AISA. None opposed the proposed AISA.

Issues raised included the level of specificity that the AISA describes the information to be shared (see section 5.1); how the information would be shared (see section 6.0); and the policy justification for the AISA covering 'non-offenders' (e.g. victims and witnesses) (see section 8.1). The majority of submitter feedback, however, covered privacy issues – including:

- Comment on the AISA's proposal that Police dispense with the adverse action notice requirement under section 96Q of the Privacy Act (see section 7.1)
- Potential wording changes to clause 9 (Privacy safeguards) of the AISA (see section 7.2)
- The timeframe for destruction of non-matched information (see section 7.3)
- Communicating with the public that name change information will be shared with Police (see section 7.4)
- Potential risk of name change information being released before a non-disclosure direction has been obtained if a person applies for both at the same time (see section 7.5)
- The process for privacy breaches (see section 7.6).

2.0 Introduction

2.1 Summary of the proposals in the public discussion document

The proposed AISA would enable the Registrar-General to regularly and proactively supply to Police details relating to registered name changes and registered deaths. It is also proposed to enable the Registrar-General to provide Police with information on non-disclosure directions on their records. These directions restrict access to records to protect the safety of the persons they apply to.

On receiving the information, it is proposed that Police would run a match against existing records in Police's National Intelligence Application (NIA) – the information system Police uses to maintain the law. If a successful match in NIA is found the person's NIA record would be updated to show if they are now deceased, have changed their name, or have a non-disclosure agreement in force. Police would only update existing records in NIA, not create new records.

The core purpose of the proposed AISA is to improve the accuracy of Police information regarding names, vital status, and existing non-disclosure directions. This will help Police to better link multiple identities to one person; maintain accurate records by correcting identity information; detect and correct false information; and protect the identity of people who have a non-disclosure direction in

force. This is not a new purpose. Police can currently request such information on a case-by-case basis to use for law enforcement purposes. The effect of the proposed AISA will be to enable the Register-General to proactively provide such information to Police. This is needed because in most cases Police is not aware that a person has died, changed their name, or obtained a non-disclosure direction. Police cannot therefore readily update its identity information unless Police is notified of such changes. Under the proposed AISA such information would be compiled weekly and provided to Police in bulk so that it can maintain accurate records for all of the identities it holds.

The proposed AISA will benefit New Zealanders by enabling Police to carry out their law enforcement functions with more accurate information. This is expected to reduce the risk of offenders using multiple identities as well as the number of events relating to misidentified individuals. There are also benefits to the wider public from enabling Police to have more accurate information about members of the public they engage with, whether as victims, witnesses to a crime, or people that Police is providing or connecting to a service.

The AISA would be established under provisions in the Privacy Act 1993 and the Births, Deaths, Marriages, and Relationships Registration Act 1995 (BDMRRA).

- Part 9A of the Privacy Act 1993 sets out the process and requirements for making AISAs – including undergoing a public consultation process. AISAs can allow the sharing of information collected for one purpose to be used for another purpose to provide a public service (in this case law enforcement).
- Section 78AA of the BDMRRA allows the Registrar-General to disclose birth, death, marriage, civil union, and name change information under an AISA.

2.2 Methodology

On 9 October 2018, a set of documents was released for public consultation, which described the proposals and sought feedback from submitters. The documents included:

- the public discussion document
- the draft AISA
- a Privacy Impact Assessment.

The documents were published on the Police's website.[1] The Registrar-General also posted information about the consultation process on DIA's website and provided a link to Police's website. Police contacted some key stakeholders to advise them of the consultation. The Minister of Police also issued a media release about the consultation.[2]

The consultation period ran from 8 October to 6 November 2018. Submitters could respond via email[3] or by letter. Five submissions were received in response to the consultation:

- 2 from individuals[4]
- 1 from a government organisation[5]

[1] Available at: http://www.police.govt.nz/about-us/programmes-and-initiatives/name-changes-deaths-and-non-disclosure-directions-information
[2] Available at: https://www.beehive.govt.nz/release/information-sharing-help-prevent-crime
[3] A specific email address was set up: dia.informationsharing@police.govt.nz
[4] Referred to as submitters 1 and 2.
[5] Human Right Commission (submitter 3).

- 1 from a professional organisation[6]
- 1 from a non-government organisation[7].

All submissions were reviewed by Police and the Registrar-General. The key themes and issues raised were identified and used to inform this report.

3.0 Generic views

Across the five submissions there was broad support for the AISA.

One submitter stated their generic support for the proposals and noted that they consider them "entirely reasonable", "...would be happy for this information to be shared as it will help Police perform their duties as well as reducing the time/cost of investigating the details/whereabouts of both criminals and victims". The submitter noted that they "...assumed that information would already be shared in this way...".[8]

Two submitters (including the submitter above) expressed support for aspects of the AISA in the context of providing responses to questions in the discussion document.[9] Three submissions also provided comments or suggestions to improve/revise the AISA, so can be interpreted as providing qualified or conditional support about such parts of the AISA. These views are discussed below under the relevant subheadings.

None of the submitters explicitly stated (or implied) that they were opposed to the proposed AISA.

One submitter did not specifically refer to the AISA in their submission.[10]

4.0 The information sharing purpose and process

Two of the five submitters noted their support for the purpose and process for sharing information from the Registrar-General to Police to help improve the accuracy of Police records in NIA.

Submitter 1 supported the purpose and process without providing further specific reasons.

Another submitter provided their support and noted that the AISA could help enhance the safety and wellbeing of both the public and victims of crime and trauma in a number of ways.[11]

- Victims' safety will be improved if the Police are informed of an offender's name change. This minimises the chance of an offender using multiple identities to evade arrest or a border alert, or to gain in a way that may harm the public. The AISA will also aid Police in enacting court orders and conducting criminal investigations.
- In the case of victims who wish to have a non-disclosure direction, having their information automatically passed to Police will enable the Police to better protect them by keeping their personal information confidential.

[6] New Zealand Law Society (submitter 4).
[7] Victim Support (submitter 5).
[8] Submitter 1.
[9] Submitters 1 and 5.
[10] Submitter 2.
[11] Submitter 5.

- In cases of sudden death when the deceased has changed his/her name, the AISA will enable Police to deliver the death notification with increased speed and accuracy to the bereaved victims. This will improve accessibility of support, minimise the risk of the bereaved hearing the news from elsewhere first, and improve the accuracy of early information they receive.

The submitter noted that it works closely with Police and that the majority of their referrals come from the Police. They felt that the proposed AISA will help their organisation to better support victims in the circumstances mentioned above.

Police and the Registrar-General response

Police and the Registrar-General have noted these comments, which are supportive of the proposals.

5.0 Information to be shared

Two submitters[12] noted their support for the range of information proposed to be shared without providing further comments. Submitter 3 specifically supported the AISA's exclusion of the sharing of pre-sexual assignment personal information.

Submitter 3 raised issues that trans/non-binary people may face when they change their names – particularly in the context of Police vetting services. For example, a Police vetting check could potentially reveal their former name to potential employers. The submitter noted that the AISA will address this issue in some degree as it will result in registered name change information being shared with Police, but this will not capture 'informal' name changes.

Police and the Registrar-General response

Police and the Registrar-General noted these comments and agree that the AISA will not be able to capture 'informal' name change information, which is not proactively provided to Police. The AISA was never intended to try and capture such information. If Police are provided such information in the usual course of their duties then they can add it to NIA on a case-by-case basis.

5.1 How the AISA describes the range of information to be shared

Clause 3 of the proposed AISA describes the types of personal information to be shared by listing three subsets of information contained in the:

- registered death record on the death register
- registered birth record for persons whose birth is registered in New Zealand and who are the subject of a registered name change or a non-disclosure direction
- registered name changes for overseas born applicants who are the subject of a registered name change or a non-disclosure direction.

[12] Submitters 1 and 2.

Submitter 4 felt that all information on the types of records that the proposed AISA deals with could potentially fit within one or other of these subsets and this created the potential for uncertainty. The submitter considered that clause 3 of the AISA, as drafted, gave insufficient detail about what information will be shared under the AISA and the broad and inclusive language used created a risk that the range of information that will be shared could be increased without notifying the public or amending the AISA.

The submitter noted that the PIA indicated there was a high degree of certainty about what information is useful and necessary from the testing process. They therefore suggested that the AISA's wording be more specific about the information that will be shared and felt that this could be achieved by redrafting clause 3 to reflect the table of information at page 6 of the PIA. The submitter noted that this would provide greater certainty and would prevent scope creep.

Police and the Registrar-General response

Clause 3 of the AISA describes the type of information to be shared under the AISA. The text was developed to provide clarity and certainty to the public about the type of information to be shared – without providing overly prescriptive or excessive detail about each relevant information field in the relevant registers. The information contained within each of the registers is prescribed through Regulations.

The wording was developed with input from Parliamentary Counsel Office and the Office of the Privacy Commissioner. The wording of clause 3 of the AISA does cover most of the information fields listed in the PIA and consultation document, and Police and the Registrar-General do not consider that there are any material categories of information that will be shared that are outside of the existing description in the AISA. The Registrar-General advises that the level of information specified in the AISA is also consistent with other AISAs that have been implemented.

With the changes in the BDMRRA on the horizon there is potential that some of the Registrar-General's information fields may also need to change because of the proposed reforms. Clause 3 was deliberately drafted in the AISA to be a little more 'general' than the table in the supporting PIA. This still ensures clarity and certainty for the public, but also provides some degree of flexibility for efficiency reasons. For example, in the case of providing name change information, the proposed AISA refers to a person's "former names" and "new names", rather than describing all of the name-related fields noted in the supporting PIA and discussion document (such as: "surname at birth", "first names at birth", "former surname", and "former first names", new surnames", "new first names" etc).

During initial implementation of the AISA, agencies may identify that minor changes to the information provided are needed to enable more efficient and accurate matching. This is allowed for within the wording of the AISA. Being overly prescriptive may make it difficult to include such information without having to amend the AISA and consult all over again. In contrast, if there was ever a proposal to share any type of information that is materially different to that described in the AISA then Police and the Registrar-General would need to undertake further consultation in order to amend the AISA. A reasonable balance is required and Police and the Registrar-General consider that the current wording of clause 3 in the AISA provides this.

It should be noted that the documented Operational Procedures that will be developed to sit under the AISA, and guide its implementation, will contain details of all the specific information fields to be supplied by the Registrar-General. The Office of the Privacy Commissioner will be required to

review them once developed and if they are to be amended. This provides another safeguard in the system to ensure that information outside the scope of the AISA is not shared.

Although Police Operational Procedures are generally not publicly released, they are still subject to the Official Information Act 1982. Accordingly, Police and the Registrar-General propose to release a version with any justified redactions made to it.

6.0 When/how information will be shared

Submitter 1 agreed with the proposed approach for sharing of information without providing further specific reasons. Submitter 5 also noted it supported the automatic and regular sharing of information and considered that this would help prevent information from "falling through the gaps", which might otherwise help protect the public and victims of crime or trauma.

Submitter 3 noted that the proposed AISA will provide for automatic information sharing of the personal information set out in the AISA. They noted that the Registrar-General will not filter any of the specified information before doing so. The matching of information and discarding of non-matched information will be done by Police. The submitter suggested that this raises inherent issues as regards necessity and proportionality at the point of collection. Consistent with a risk flagged in the PIA, the submitter noted a potential risk that some of the information collected by Police exceeds that required, thereby exceeding the necessity to collect that information.

Police and the Registrar-General response

Police and the Registrar-General consider that the risk of Police collecting information beyond that required under the AISA is very low. Testing of the necessary fields required for a successful match was carried out by Police and the Registrar-General during the development of the AISA, and the parties are confident that the fields are limited, but also include enough information to ensure accuracy.

The Registrar-General is also not aware of who is in Police's NIA information system so cannot readily provide updates for just for those people in NIA. NIA is also very regularly updated, so it is more efficient for Police to do the matching after receiving information from the Registrar-General. The regular transfers of information to Police will just capture those registered name changes, death registrations, and non-disclosure directions obtained after the previous transfer of information.

To reduce the risk further, Police will undertake an analytical review of the matching process after 6 months of operation under the AISA to identify the number of successful matches using the data type of information to be shared and to check that over-collection (or under-collection) of data is not happening.

Additionally, the majority of the information disclosed by the Registrar-General to Police will not be included in the Police NIA system. Instead, once a successful match is found, an individual's record in NIA will be updated with either a "deceased" indicator, the individual's new registered name with a flag noting that the name was sourced from the Registrar-General, and/or an indicator that the individual has a non-disclosure direction in force.

The remaining information supplied by the Registrar-General under the Agreement will be destroyed by Police, including any information provided by the Registrar-General that does not

match a NIA record. Police will only update existing records in NIA and will not create new records. The exception will be the creation of a new record in NIA for a person with a non-disclosure direction who has not come into contact with Police before, so that Police will know to protect the name of that individual if they come into contact with them in the future.

7.0 Privacy issues

Privacy issues formed the bulk of the feedback provided by submitters.

Submitter 1 supported the proposed privacy protections without providing further specific reasons. Submitter 3 also commented on potential privacy impacts of the AISA. They considered that the AISA appears to broadly confirm with the 'principle of legality' as it is underpinned by the Privacy Act 1993 as regards its development, implementation and public accessibility.

Two submitters noted that there was the potential for people to have their information shared with Police against their wishes.[13] Submitter 5 suggested that this may apply especially to victims of violence, stalking, and witnesses of crime. While many victims in these groups may perceive their name change being shared with Police as positive, or already presume such sharing to take place, for others it could exacerbate existing distrust in authorities or add to a sense of their past being inescapable. Despite this, the submitter agreed that the benefits of automatic name sharing outweighed the risks to the victim.

7.1 Adverse action

Section 96Q of the Privacy Act requires a party to an AISA to give written notice to an individual before it takes any adverse action against the individual on the basis (whether wholly or in part) of personal information about the individual that was shared under the agreement. Under section 97R parties can agree to dispense with such requirement to give notice.

Clause 7 of the AISA proposes that Police can dispense with the notice requirement under section 96Q where the sharing of personal information under the AISA gives Police reasonable grounds to suspect that an offence has been committed or will be committed and the personal information is relevant to the detection, investigation, or prosecution of that offence.

Two submitters provided feedback on the proposal to dispense with the notice requirement.[14] Submitter 3 noted that clause 7 of the AISA argued that advance notification of an adverse action could prejudice the integrity of the investigative process. They felt that this justification was in line with the "maintenance of the law" exception set out in the Privacy Act under Information Privacy Principles 3(4)(c)(i), 11(e)(i) and elsewhere.

Submitter 4 also acknowledged that providing an individual with advance notification of adverse actions could be prejudicial to Police investigations. The submitter noted that clause 7 of the AISA proposed to enable Police to dispense with a notice requirement under section 96Q where the sharing of the information gives Police reasonable grounds to suspect that an offence has been or will be committed and the information is relevant to the detection, investigation, or prosecution of that offence. The submitter recommended retaining these two prerequisites in the AISA, but also felt that a further prerequisite should also be included – namely, that there also needs to be "a real risk of

[13] Submitters 3 and 5 refer.
[14] Submitters 3 and 4 refer.

prejudice to Police's ability to investigate" in order for Police to dispense with providing advance notice of an adverse action.

Police and the Registrar-General response

The most common use of the information provided under the AISA will be to enable more accurate information on a person's identity or status so that Police can manage its records. Police and the Registrar-General consider that it is very unlikely that there will be any potential adverse action for the individuals concerned because their registered name change, or death, or non-disclosure direction status is updated into the police NIA system. Rather the adverse action will be a secondary consequence of Police holding accurate information.

The main outcome will simply be that Police records in NIA are updated and made more accurate, which will help with law enforcement purposes and support Police's interaction with, and service provision to, the wider public (e.g., being notified of the death of a fire arm licence holder can help ensure the firearms do not pass to unlicensed people). Police is in a different position to other agencies who receive information which could lead to an adverse action – for example, information being shared about a person that could lead to an adverse action such as a benefit payment being stopped.

One potential scenario for an adverse action against an individual is if the information about them provided under the AISA then influences Police's decision-making about whether to investigate them for possible commission of an offence. For example, where there has been a name change for the purposes of committing fraud or an attempt to evade a border alert. In such cases giving notice to the person will likely always prejudice the investigation of that offending.

However, even in such cases, the shared information will only be a very small part of the information actually considered by Police when making such decisions about whether to investigate or potentially charge a person with an offence. Such information is very unlikely to be the most significant piece of information to influence Police decision-making. In reality it will be the person's responses to any questions Police ask, their actions, and the gathering and considering of other evidence that will be the most material to a Police decision to investigate someone further – not the fact that the Police finds out that they have legally changed their name.

In practice, the shared information will be used to update NIA to support Police interactions with the public. Police will not be searching through all name changes and registered deaths received in order to initiate enforcement activity in the first place.

Additionally, the relevant Registrar-General privacy notices on its website and applications forms will be amended to describe the nature of the information sharing with Police under the AISA – so there is already some advance notice to people contemplating changing their name or applying for a non-disclosure direction.

The AISA also notes that Police will comply with all Police policies and guidelines as well as the Solicitor-General's Prosecution Guidelines (Guidelines), before taking any adverse action. These Guidelines assist in determining:

- whether criminal proceedings should be commenced
- what charges should be filed
- whether, if commenced, criminal proceedings should be continued or discontinued.

The Guidelines also provide advice for the conduct of criminal prosecutions and establish standards of conduct and practice expected from those whose duties include conducting prosecutions.
If information shared under this Agreement forms part of the prosecution's evidence in a criminal case, the information may be disclosed to an individual in accordance with the Criminal Disclosure Act 2008. Any dispute about the provision of such information will be managed by the courts as part of the subject matter of the prosecution.

Police and the Registrar-General therefore do not consider that there is a need to require Police to take on an additional process and have to make a specific assessment about whether there is a real risk of prejudice to Police's ability to investigate by giving such notice. There is unlikely ever to be a case of the information leading to an adverse action. However, were this to occur, Police consider that giving notice would prejudice any investigation. Police and the Registrar-General therefore propose to keep the existing wording in the AISA in clause 7.

7.2 Wording of clause 9 of the AISA (Privacy safeguards)

7.2.1 Use of "will"/"may"

Submitter 3 suggested a wording change to clause 9 of the AISA. Clause 9 states that applicants for name changes or non-disclosure directions should be given upfront notice that the Registrar-General *may* release their information to Police and that police *may* subsequently disclose it to other parties in accordance with legislation. The submitter suggested that the word "may" should be replaced with "will" in the relevant places in clause 9 of to ensure consistency with wording in clause 7 of the AISA.

Police and the Registrar-General response

Police and the Registrar-General agree that the word "may" should be changed to "will" in clause 9 when referring to the Registrar-General providing the information to Police. This reflects what will happen in practice under the AISA. The relevant information *will* be provided (likely on a weekly basis) to Police – it is not a case of the Registrar-General deciding whether it may or may not pass the relevant information to Police. This wording change has been made in three places in clause 9 of the draft AISA (see bullet points 2, 3, and 4 of clause 9).

Clause 9 also states that Police "may" subsequently disclose the relevant information to other parties in accordance with legislation. This word "may" is appropriately used here as the information will not automatically be passed on by Police to other parties in all cases – only when there is a justification. The word "may" in this context has been retained in clause 12 of the draft AISA (see bullet points 2, 3, and 4 of clause 9).

7.2.2 Communication with funeral directors

Submitter 4 noted that the majority of death notices currently come via an online form from funeral directors. On rare occasions notification may come via a party known to the deceased. In the latter case, the party known to the deceased is advised that information may be released to other parties who may subsequently disclose it to additional parties in accordance with legislation. The submitter noted that, where information is provided by funeral directors, affected people will only know that information about the deceased will be supplied to Police if the funeral directors let them know

directly. They noted that while the Registrar-General cannot *require* funeral directors to provide information to affected parties, the proposed AISA should record that the Registrar-General will *ask* funeral directors to let the relevant people know that certain types of information about deaths is being provided to Police.

Police and the Registrar-General response

The Registrar-General advises that requesting funeral directors to provide such information is not currently standard practice. The Registrar-General also has concerns about the practicalities, timing, and cultural sensitivity about asking funeral directors to provide such a notice to families when they are dealing with a bereavement. Information about the process is currently available to families on DIA's website if they wish to know what the Registrar-General does with registered death information (https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Legal-Privacy-Births-Deaths-Marriages-Civil-Unions-Name-Changes-Passports-and-Citizenship-Privacy-Notice).

7.2.3 No intent for Police to verify matched information back to the Registrar-General

During the consultation Police and the Registrar-General noted an ambiguity in the drafting of one of the bullets in clause 9 of the proposed AISA. In the draft AISA released for consultation the text stated that after the information had been transferred from the Registrar-General to Police, Police would verify any matched data *with* the Registrar-General before the NIA record is amended. This clause should have read Police would verify any matched data *from* the Registrar-General before the NIA record is amended. Police does not intend to provide verification back to the Registrar-General of the information it adds to NIA. The Registrar-General does not expect Police to provide any such verification. Any verification refers to Police internal activities between matching any information and making updates to NIA.

Police and the Registrar-General response

The wording on clause 9, bullet point 10, of the draft AISA has been amended to read: "Police will verify any matched data from the Registrar-General before the NIA record is amended".

7.3 Timeframe for destruction of non-matched information

Two submitters discussed the destruction of information[15]. Submitter 3 noted that the proposed AISA did not specify a timeframe for destruction of non-matched information after updates to the NIA have been completed. Clause 8 of the draft AISA states that all information received from the Registrar-General will be securely destroyed by Police in accordance with Operational Procedures, following completion of the matching process. Clause 11 goes on to state that all personal information will be destroyed within the timeframe specified within Operational Procedures. It also notes that after the relevant information from the Registrar-General has been updated in NIA no personal information will be uploaded into any other Police system.

Submitter 3 felt that there was a need for *immediate* destruction of non-matched or excessive information. They suggested that clauses 8 and 11 of the AISA be revised to explicitly provide that:

[15] Submitters 3 and 5.

- All non-matched and excess information provided to Police is to be destroyed immediately after the matching process and all other information will be destroyed immediately after the NIA is updated (as per the requirement under IPP 9).
- The process for immediate destruction of information is set out in the DIA/Police Operational Procedures and includes verification that the information has been destroyed back to the Registrar-General.
- This process is set out in the Registrar-General's Privacy notices made available to name-change and non-disclosure applicants.
- The DIA/Police Operational Procedures are made publicly available.

Likewise, submitter 5 felt that that any information that does not match an existing record should be destroyed *immediately*. The submitter argued that staff must be educated about the responsibility of handling non-disclosure direction data, and the serious risks and fears that often underlie an individual's decision to apply for a non-disclosure direction.

Police and the Registrar-General response

The parties do not believe a set period for destruction of the information needs to be specified in the AISA – but this will be included in the Operational Procedures developed to support the AISA. The parties have suggested some wording changes to stress that destruction will occur as immediately as is practicable after the matching process has been completed and in accordance with Operational Procedures.

Clause 8(h) of the draft AISA has been amended to read (new text in *italics*):

> "All information received from the Registrar-General will be securely destroyed by Police, *as soon as reasonably practicable,* in accordance with the Operational Procedures, following completion of the matching process".

Clause 11 of the draft AISA has been amended to read (new text in *italics*):

> "All personal information received from the Registrar-General will be destroyed *as soon as reasonably practicable, once the matching process has been completed,* within the time period specified in the Operational Procedures".

Police's system will also log when destruction occurs. Compliance with destruction Operational Procedures will be considered as part of Police's internal audits of the system to confirm that the safeguards are operating as intended.

The Operational Procedures for the AISA will be consulted upon with the Office of the Privacy Commissioner when developed. Police and the Registrar-General generally do not publicly release such Operational Procedures in full. However, given that they are still subject to the Official Information Act 1982, Police and the Registrar-General propose to agree a version for public release, with any justified redactions made to it.

7.4 Communication to the public that name change information will be shared will Police

Two submitters[16] noted that the consultation documentation (including the PIA) stated that privacy risks will be mitigated by a range of methods. These include:

- the Registrar-General amending its privacy notices and application forms to inform people that the information they provide the Registrar-General will be shared with Police
- a communication strategy accompanying the implementation and operation of the AISA will help raise public awareness of the information sharing and its purpose
- development of joint Operational Procedures between Police and the Registrar-General around the same time the AISA comes into force
- a review of the AISA's operation after 6 months.

Submitter 5 felt that a communication strategy needs to be victim-focussed in order to minimise the risk that victims will lose confidence in the both the Police and the option of changing their name to make a fresh start. The submitter offered its expertise to support the development of a communication strategy that supports victims in this situation.

Police and the Registrar-General response

The Registrar-General will make appropriate changes to the relevant website notices and relevant application forms to clearly describe when and how information will be shared under the AISA.

The two agencies will also develop joint Operational Procedures to support implementation of the AISA.

Police and the Registrar-General will work together to communicate the AISA's implementation and existence. Appropriate consideration will be given to the different audiences and messaging.

7.5 Risk of name change information being released before non-disclosure directions

There is a potential timing issue for those who seek both a name change and a non-disclosure direction at the same time. There is the chance of a delay in time between an individual registering a name change and also having a non-disclosure direction approved by the Registrar-General, as the approval of a non-disclosure direction relies on a decision by the Registrar-General. In such a scenario Police could be notified of the name change first, and the non-disclosure direction potentially at a later date. In the period between the two notifications a Police officer could inadvertently disclose the new name that is later subject to a non-disclosure direction.

Submitter 5 noted this issue and felt that the Registrar-General has a responsibility to inform all individuals who apply for a simultaneous name change and nondisclosure direction that doing so could result in the Police releasing information about them, and thus sharing their new identity before the non-disclosure is in place. The submitter felt that individuals in this situation should be advised that they may like to delay their name change application until the non-disclosure direction has been approved to avoid this occurring.

[16] Submitters 3 and 5.

Police and the Registrar-General response

The Registrar-General provides information in the application form instructions and on the website. This information will be amended to provide further advice for people who apply for a name change and a non-disclosure direction simultaneously. They will be informed that once the name change is registered it will be shared with Police and that this may be prior to the non-disclosure direction being approved. This therefore offers the individual the opportunity to delay applying for their name change until the non-disclosure direction is in place. It will be up to the individual concerned, however, if they wish to take this approach – for some the name change will be their main focus and they may choose to focus on that first. The Registrar-General will communicate this issue to front line staff who receive/process such applications so they can guide customers.

Police and the Registrar-General will develop Operational Procedures at the same time as finalising the AISA. Any delay between the AISA coming into force and the Operational Procedures being agreed is expected to be short. This will minimise the number of disclosures by the Registrar-General to Police of name changes that have non-disclosure directions in force, prior to Police being informed about the non-disclosure direction.

7.6 Process for privacy breaches

Submitter 4 noted that clause 15 of the proposed AISA outlines the process to be followed if there is a privacy breach. This included Police and DIA's internal investigation processes being applied. The proposed AISA also refers to notifying the Privacy Commissioner about "significant" privacy breaches.

The submitter noted that the Privacy Bill (the Bill), currently before Parliament, proposes to introduce mandatory notification of privacy breaches. The Bill does not specify that the threshold for notification must relate to the 'significance' of the breach. The Bill also contains a range of other obligations on parties, such as notifying individuals, and providing certain specified information in that notification. While the proposed agreement will not override those provisions, the submitter suggested adding a generic reference to clause 15 of the AISA to minimise any potential confusion or uncertainty. This could state that: "The parties will observe any new legal requirements to notify the Privacy Commissioner or individuals of breaches (such as those in the proposed new Privacy Act) once that law is in force."

Police and the Registrar-General response

Police and the Registrar-General do not consider that the AISA should refer to proposed legislation (which may or may not become law), but note the importance of trying to future proof the wording in the AISA as much as practicable. The parties therefore to propose adding the following text to clause 15:

"The parties will observe any legal requirements to notify the Privacy Commissioner or individuals of privacy breaches."

8.0 Other issues raised

8.1 Policy justification for non-offenders

Submitter 4 noted that there was a clear policy justification for matching offender information in the NIA with the information supplied by the Registrar-General. However, they questioned whether there was sufficient justification provided for updating information about third parties (such as victims of crime, witnesses and family members). The submitter acknowledged that the benefit of sharing non-disclosure directions covering victims of crime is plain. However, they felt it was less clear that there might be benefits from updating a victim's name if they change it. Similarly, it is unclear why the fact a family member (of an offender or potential offender) is now deceased might need to be updated in NIA. The submitter felt that benefits of doing so should be made clear in the proposed AISA.

Police and the Registrar-General response

Under the AISA Police will receive information about name changes, deaths, and non-disclosure directions for all persons, not just about offenders, potential offenders, and persons of interest. There are clear benefits to Police and the wider public of enabling Police to have more accurate information about members of the public they engage with, whether as victims, witnesses to a crime, or people that Police is providing with, or connecting to, a service.

Police has contact on a daily basis with members of the public, including providing support and reassurance, dealing with complaints, referring to services, activities relating to crime prevention, as well as engaging with victims and witnesses. Having accurate information on a person's name or whether a person has died enables Police to continue to provide these public services, whether it is helping Police to contact that person in future or to ensure the safety of that person. Being aware of a new name will help police to engage with people, whether to assist in knowing their preferred name when contacting them for reasons such as following up on a complaint lodged, discussing a crime against the person, or to provide a service to them.

Death information will assist Police to maintain an accurate record of current firearms licence holders, to manage Police biometric databases (DNA, fingerprints, face), to track down next of kin following death, and to obtain evidence of death for use in court proceedings. For example, Police will be notified of a person who has died and who is registered on the firearms licence register. Police can then revoke the licence and ensure that any firearms of the deceased person are either held by a licenced person or are destroyed. Unless Police is involved following the death, they are not currently aware when a firearms licence holder dies.

Police may be dealing with the person in relation to an offence, such as a witness to historic offending, or there may be outstanding actions by Police, such as an outstanding arrest warrant that would need to be revoked if a person was deceased. If Police did not know the person was dead they would execute the warrant, using Police resources and potentially upsetting the family of the person.

Having accurate information on whether a non-disclosure direction is in force enables Police to better manage the use of that person's information and protect the personal information that is subject to the non-disclosure direction. For example, a Police staff member may deal with a report by an individual that they are a victim of a crime. When checking in Police's system, the person record flags that the individual has a non-disclosure direction in force. Police can then ask the individual what name they would prefer used on the documents relating to the offence, which may be disclosed to the defendant if charges are laid.

Police and the Registrar-General propose to add text in the Objective and Purpose section of the AISA to clarify that the AISA applies to all persons in NIA, and is not limited to offenders, potential offenders, and persons of interest.

8.2 Police vetting and disclosure

Submitter 3 raised issues that trans/non-binary people may face regarding the use of their personal information held by the Police in the context Police vetting (e.g. in pre-employment conviction checks). The submitter noted that some trans-gender people will change their name, either legally or informally, to one more in line with their gender identity. Police vetting checks could lead to sensitive information being made available to potential employers, or police/court documents being addressed to an old name, which can raise privacy, safety and security concerns. While acknowledging Police vetting was out of the scope of this AISA, the submitter supported improving the current Police vetting processes to so that vetting does not risk disclosing the person's trans-gender status to a potential employer.

The submitter referred to the United Kingdom's Disclosure and Barring Service (DBS), which offers a confidential checking service for transgender applicants, known as the sensitive applications route. This is managed by a specialist team and gives applicants the choice not to have any gender or name information disclosed on their DBS certificate that could reveal their previous identity. The submitter recommended that consideration is given to adopting a similar process in New Zealand.

Police and the Registrar-General response

Police and the Registrar-General consider the comments raised about vetting are outside the scope of this AISA. Such issues are best considered as part of Police's work on potential reforms to the Police vetting system.

8.3 Parallel reform to the BDMRR

Information about pre-sexual assignment or reassignment birth registrations are excluded from the proposed AISA. Submitter 3 noted the BDRMM Amendment Bill proposes to enable trans-gender and non-binary people to change the gender markers on their birth information without having to apply to the Family Court and provide medical evidence. If the Bill is passed the submitter recommended that provision is made to ensure that any updated gender marker information that is recorded under such provisions is updated on Police's NIA system in the event an information match is made. The submitter recommended that further consultation with the trans-gender/non-binary community be undertaken about the most appropriate mode for this (i.e. amendment to the AISA or through a voluntary notification system).

Police and the Registrar-General response

Police and the Registrar-General consider the comments raised about the BDMRR Amendment Bill are outside the scope of this AISA. Such issues are best considered as part of the Registrar-General's ongoing work on the Bill.

8.4 Birth/death certificates

One submitter provided an anecdotal example of a person who had created a false identity using a deceased infant's birth certificate to obtain a driver licence and Inland Revenue Department number. The person had remained in New Zealand illegally until he was uncovered after being reported by a former girlfriend. The submitter suggested doing retrospectives checks on death certificates to check in case others have done something similar.[17]

Police and the Registrar-General response
Police notes this comment, which is outside the scope of the AISA.

[17] Submitter 2.