Privacy Commissioner
Te Mana Mātāpono Matatapu

Approved information sharing agreement: Reducing Gang-related harm to individuals and New Zealand society generally

Report by the Privacy Commissioner to the Minister of Police under section 96P of the Privacy Act 1993

August 2019

Executive Summary

This is my report on the approved information sharing agreement (AISA) between the New Zealand Gang Intelligence Centre (GIC) Agencies approved by Order in Council (OiC) on 3 December 2018 (and in force from 4 January 2019) under Part 9A of the Privacy Act 1993 and Section 81A of the Tax Administration Act 1994.

The purpose of this AISA is to:

- enable a more collaborative, cross-agency approach to preventing or reducing harm to individuals, families, communities, or society generally that is caused by, or contributed to by, the activities of gangs;
- enable the enforcement of the law; and
- produce data on crime trends.

The AISA enables the sharing of information by 12 government agencies (the GIC agencies) with the GIC (a unit established within Police that is staffed with employees of the GIC agencies) to develop and disseminate information and intelligence products to GIC agencies with the intention of addressing Gang Related Harm (as defined in the AISA).

The AISA is broad in scope and relatively complex in its operation. It has significant privacy implications for gang members and their associates, as well as victims and others, including family members, who may be harmed or potentially harmed by gang activities.

While there are risks to privacy, the safeguards in the AISA are intended to mitigate those risks. The AISA does not permit bilateral direct exchanges of information - these must be based on other forms of legal authority. There are also certain parameters that operate to manage the quantity of information that may be shared under the AISA. GIC agencies must comply with all relevant provisions of their own legislation. The AISA cannot override relevant provisions in legislation other than the Privacy Act and must be consistent with the New Zealand Bill of Rights Act 1990.

Considering both the AISA and the supporting processes and structures, I am satisfied that the AISA meets the statutory requirements in Part 9A of the Privacy Act, and in particular, the matters set out in section 96N. However, I was to be consulted on detailed safeguards that were to form part of more comprehensive operational protocols. While sharing has commenced under this agreement, the operational protocols are still under development – this is a situation that needs to be rectified.

I am satisfied that during the development of the AISA my views about the privacy risks and the necessary safeguards were acknowledged and led to improved safeguards in this AISA. The following comments about the AISA reflect those initially made in my April 2017 submission under section 96O to the Commissioner of Police.

Given the broad scope of the AISA and the wide range of sensitive personal information to be shared under it, I intend to review its operation and the effectiveness of the safeguards 12 months after the Order in Council took effect. My review will primarily consider whether the AISA is operating as intended and is not unreasonably impinging on individual privacy.

Context

Origins of the GIC

1. The GIC was established within the Police National Intelligence Centre on 1 March 2016 as a multi-agency response to improve the co-ordination of information about adult gangs and transnational crime groups. It also provides a cross-government, real-time, single view of an organised criminal group member or prospect.[1]

2. Since it was established, agencies could provide the GIC with personal information about individuals under relevant exceptions to the Information Privacy Principles (IPPs) in the Privacy Act 1993 (including exceptions for law enforcement purposes or to lessen a serious threat to personal or public health or safety).

3. However, the IPPs do not always enable broader sharing of personal information for wider medical, educational or social service objectives. In addition, Inland Revenue, due to statutory tax secrecy requirements, may only share information as specified in the Tax Administration Act 1994, including under an approved information sharing agreement.

In practical terms, an AISA enables the sharing of personal information under the Privacy Act, including how the information is collected, stored, checked, used, disclosed and exchanged.

Part 9A of the Privacy Act provides a mechanism for the approval by Order in Council (OiC) of approved information sharing agreements (AISAs) between or within agencies to facilitate the delivery of public services. The OiC is the legislative instrument that approves the terms of an AISA including:

- the nature of any exemptions or modifications to the information privacy principles (and the conditions of the exemption, if any);
- the public service(s) to be enabled;
- the personal information or type of information to be shared;
- how each party may use personal information;
- state the adverse actions that each party can reasonably be expected to take;
- the parties to the agreement and the lead agency; and
- the date that the agreement comes into effect.

The AISA must set out these terms and, in addition:

- the purpose of the agreement;
- an overview of the operational details;
- the safeguards that will be applied to protect the privacy of individuals and ensure that any interference is minimised; and
- other administrative matters.

[1] Cabinet Paper — Whole of Government Action Plan to Reduce the Harms Caused by New Zealand Adult Gangs and Transnational Crime Groups, para [42].
http://www.police.govt.nz/sites/default/files/publications/cabinet-paper-whole-of-govt-action-plan-to-reduce-harms-caused-by-adult-gangs-and-transnational-crime-groups.pdf

Development of the AISA under Part 9A of the Privacy Act 1993

4. The Privacy (Information Sharing Agreement between New Zealand Gang Intelligence Centre Agencies) Order 2018 was approved on 3 December 2018. This Order and the AISA came into force from 4 January 2019.

5. The AISA enables a broad range of personal information to be shared by the participating agencies to the GIC. This sharing enables the GIC to create intelligence products and assist decision-makers in participating agencies to consider taking further action with respect to Gang-Related Harm. For example, it will allow enforcement activity or provide social assistance to families connected to gangs or other affected individuals in the community.

6. The GIC is defined in the AISA as the unit established within New Zealand Police, staffed with employees of GIC Agencies, whose purpose is to collect, combine and share information relating to gangs and gang criminal activity; and to respond to requests for information from GIC agencies.

7. Over time, the GIC will allow relationships between gang members and other individuals to be mapped, including potential victims. This will provide decision makers with information to determine the appropriate social and/or law enforcement interventions, priority actions and delivery mechanisms.[2]

8. The participating agencies in the AISA are:

- New Zealand Police;
- Accident Compensation Corporation;
- Department of Corrections;
- Department of Internal Affairs;
- Housing New Zealand;
- Inland Revenue;
- Ministry of Business, Innovation and Employment;
- Ministry of Education;
- Ministry of Health;
- Ministry of Social Development;
- New Zealand Customs Service; and
- Oranga Tamariki - Ministry for Children.

Scope

9. The scope of the AISA is broad. Factors contributing to the breadth of the AISA are:

- its dual purpose to reduce 'Gang Related Harm' by means of criminal enforcement and through targeted social interventions, services and support;
- the wide range of sensitive personal information that is eligible for sharing;
- the wide range of individuals potentially affected by the AISA; and
- the number of participating agencies in the AISA, including large multi-functional agencies such as the Department of Internal Affairs and MBIE.

---

[2] Ibid

Purpose

10. The purpose of the AISA is to allow information about gangs to be shared by participating agencies to enable the GIC to provide information and intelligence that agencies require in order to take steps to reduce Gang Related Harm.

11. The intent is not to enable broad bilateral information sharing between the parties, rather to provide legal authority for highly managed information sharing and intelligence generation with the GIC at the centre of all information flows.

Comments on the Agreement

12. Under section 96N of the Privacy Act, the Minister of Police was required to be satisfied of the following matters (in bold italics) before recommending the making of an Order in Council to approve the information sharing agreement. The following comments reflect the matters that were initially raised in April 2017 in my submission to the Commissioner of Police under section 96O.

Does the information sharing agreement facilitate the provision of any public service or public services?

13. I am required, under section 14(a) of the Privacy Act, to have due regard for the protection of social interests that compete with privacy. Based on the Gangs Action Plan I am satisfied that the GIC is a considered and potentially effective cross-government initiative to identify and support actions to address the impacts of Gang Related Harm on individuals, families and communities.

14. The information sharing agreement is intended to facilitate information sharing between the GIC and the GIC Agencies to "share information and intelligence to reduce gang-related harm and achieve the objectives [of the Agreement]".

15. The purpose is framed broadly, encompassing both harms caused by gang-related criminal activity and social harm caused to gang family members and their communities.

16. The OiC (clause 7) sets out the public services these purposes and objectives are intended to achieve, namely maintaining public safety, preventing the commission of offences, enforcing the law, and identifying vulnerable persons, including children and young persons in need of care and protection, and providing them with the necessary social assistance and support.

17. The operational overview (page 13 of the AISA) explains that the GIC may collect information from GIC agencies to maintain a national repository of intelligence about gangs. Information may be disclosed, either on request or at its own behest, to GIC agencies to inform decision making on preventative, investigative and enforcement interventions related to gangs, and to identify gang-associated vulnerable children, youth, and family members in need of medical, educational or social service support.

18. I am satisfied that public agencies acting together in a coordinated way under the GIC model to share personal information as necessary to address Gang Related Harm is a public service that will be supported by the AISA.

Is the type and quantity of personal information to be shared under the Agreement no more than is necessary to facilitate the provision of that public service or those public services?

19. The scope and types of information that may be shared under the AISA are significant and outlined in an extensive list in Schedule 1 to the OiC. There are 21 broad categories of information, with each agency contributing information in one or more of those categories on request, as specified.

20. Given the important purpose and aims of the GIC AISA and the constraints and safeguards wrapped around the sharing, in my view it appears justified and not disproportionate.

21. I note that information was previously being shared for certain purposes under the Information Privacy Principles allowing disclosure where necessary to avoid prejudice to the maintenance of the law or for health and safety reasons. The AISA is covering these existing disclosures as well as enabling disclosures for additional purposes.

22. There are certain parameters that operate to manage the quantity of information that may be shared under the AISA. GIC agencies must comply with all relevant provisions of their own legislation. The AISA cannot override relevant provisions in legislation other than the Privacy Act. This includes sections 17, 19 and 21 of the New Zealand Bill of Rights Act 1990 that may guide information sharing in particular cases.

23. The AISA notes that GIC Agencies are not compelled to provide information and disclosures are therefore discretionary. Agencies are to use existing compulsion mechanisms such as warrants or production orders if information is required for evidential purposes.

24. It is also relevant that information shared under the AISA can only be used for the stated purposes, and that the GIC acts as a 'gatekeeper' for information going in and out. The GIC is subject to a requirement to report publicly on its success in meeting the objectives of the AISA. Bilateral sharing of information from one GIC agency to any other agency (including any GIC agency) is not covered by the AISA.

25. On the basis of these factors I am satisfied that the type and quantity of personal information to be disclosed under this AISA is reasonably necessary to facilitate the provision of the public services identified given the breadth and complexity of these services.

Will the Agreement unreasonably impinge on the privacy of individuals and contain adequate safeguards to protect their privacy?

26. This AISA enables the collection and disclosure of a much wider range of personal information about people affected by Gang Related Harm and will also allow disclosure of information that is subject to tax secrecy provisions pursuant to section 81A of the Tax Administration Act. The AISA enables the creation of an authoritative and up to date list of current members of gangs, and to provide collated intelligence products to GIC agencies.

27. The AISA is intended to allow for collection and disclosure along clear channels via embedded GIC agency staff members, and through a formal Request for Information process. This structure is an important constraint on potential privacy infringements. If the AISA had been structured to explicitly permit free disclosure between GIC agencies I would have concerns about whether the regime was a proportionate response to an acknowledged problem.

Safeguards

28. As required by section 96I(2)(d), the AISA specifies the safeguards that will apply to protect the privacy of individuals and to ensure that any interference with their privacy is minimised. Section 96N requires that the Minister be satisfied that the AISA contains adequate safeguards to protect the privacy of individuals.

29. The Privacy Impact Assessment report (PIA), notes that it could appear that the AISA might permit untrammelled disclosures and use of information about gang members, their families and associates within the group of GIC agencies.[3]

30. I have considered whether the AISA is a proportional response to Gang Related Harm based on the range of safeguards identified across the AISA, the PIA and the operational protocols. I have looked at whether there is a comprehensive range of safeguards that limit unjustified intrusions on the privacy of the individual and the potential for unwarranted fishing expeditions.

31. The PIA identifies that disclosures are limited by the:

- AISA purpose statement;
- controls imposed by the GIC assessment and processing regimes; and
- permitted communications between the GIC and the GIC agencies.

The PIA also identifies that the ASIA does not permit bilateral direct exchanges of information - these must be based on other forms of legal authority.

32. The GIC operating model also has controls to ensure that information flows and intelligence generation stay within operating limits to reduce the risk of fishing expeditions for information that is not directly related to addressing Gang Related Harm, or not directly connected to gang activity.

33. The PIA also notes:

- the existing robust processes to manage agency requests (the RFI process) and the assessment of requests by the GIC;
- there are no direct connections between the GIC agencies' computer systems and the GIC system;
- that agencies provide information they already hold, and are not authorised by the AISA to collect any additional information to fulfil a request; and
- when receiving a GIC Intelligence Product, an agency must have a valid business purpose for collecting, using or retaining that information related to the purposes of the AISA.

---

[3] Privacy Impact Assessment, p 16.

34. Detailing the safeguards of the RFI process usefully demonstrate the necessity and relevance constraints that control the quantity of information sharing about an individual who is, in some circumstances, only remotely connected to a gang. For example, the RFI request template must identify purpose, justification, rationale and necessity of a request for information from the GIC.

35. Other relevant safeguards are:

- the GIC List verification process for including or excluding people as gang members or prospects;
- GIC mechanism that means the GIC is acting as "gatekeeper" of the information flows;
- GIC controls and constraints on the delivery of timely intelligence, including expiry;
- the role and responsibilities of the GIC Manager, including discretion and intelligence best practice procedures; and
- GIC governance and review procedures.

36. On the basis of these operational safeguards, I am satisfied that this AISA does not unreasonably impinge on the privacy of individuals and contains adequate safeguards to protect individuals' privacy. However, I was to be consulted on detailed safeguards that were to form part of more comprehensive operational protocols. While sharing commenced under this agreement in January 2019, the operational protocols are still under development – this is a situation that needs to be rectified.

Will the benefits of sharing personal information under the Agreement be likely to outweigh the financial and other costs of sharing it?

37. The GIC has been operating since March 2016 and sharing information and intelligence subject to the Privacy Act provisions. I understand that the AISA is unlikely to create significant additional financial costs.

38. The intrusions into privacy are also a cost to be balanced with the benefits the AISA is intended to achieve and, on balance, I consider those costs can be expected to be outweighed by the projected benefit of reducing Gang Related Harm. This is a dynamic balance and ensuring that the benefits are being achieved will be a focus of the monitoring regime for the AISA and my review of the AISA under section 96W of the Privacy Act.

Are there any potential conflicts or inconsistencies between the sharing of personal information under the Agreement and any other enactment, and have they been appropriately addressed?

39. It is important to note that the AISA does not provide any additional legal basis for disclosure of information between GIC agencies, only between the GIC and GIC agencies - a 'hub and spokes' arrangement. This AISA does not allow the free disclosure of information between parties except as permitted or required by other legislation.

40. The AISA creates a discretionary ability to collect, hold and disclose information that does not override any other legislative provision. No agency can be required to disclose information because of its participation in the AISA.

41. There are many existing and anticipated enactments that will operate concurrently with the GIC AISA, generally allowing the disclosure of information or, more rarely, requiring or prohibiting it. For instance, Parliament has recently passed legislation that allow for improved identity management at the border, information sharing about at-risk children, family violence, and money laundering, and updating the social security legislation.

42. One significant effect of the AISA is that Inland Revenue will be permitted to share tax information that would otherwise be subject to statutory confidentiality. Section 18E of the Tax Administration Act enables Inland Revenue to provide information under an approved information sharing agreement made under Part 9A of the Privacy Act.

43. As noted in the AISA, it does not purport to override any provisions in any enactment other that the Privacy Act. GIC Agencies are required to use existing compulsion mechanisms such as warrants or production orders if information is required for evidential purposes. As noted above, relevant provisions of the New Zealand Bill of Rights Act may guide information sharing in particular cases.

Monitoring and Review

44. The novelty, size and complexity of the AISA means that monitoring compliance will be crucial. This is particularly the case for information about individuals associated with gangs, family members and victims being collected and disclosed by the GIC and GIC agencies. My Office is working with the GIC to establish a monitoring regime that is robust, effective and ensures the AISA operates appropriately.

45. The breadth of the AISA's purpose, the number of agencies involved and the potential risks to privacy means that I will be conducting a review of the operation of the AISA under section 96W. I will undertake this review 12 months after the Order in Council took effect.

46. Following my review under section 96W, section 96X of the Privacy Act provides for me to report to the Minister of Police about an AISA and recommend if necessary its amendment or revocation.

John Edwards
Privacy Commissioner