Ministerial Policy Statement

Obtaining and using publicly available information

Summary

It is lawful for the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) to obtain and use publicly available information. This ministerial policy statement (MPS) provides guidance on the conduct of this activity. In making decisions related to obtaining and using publicly available information, GCSB and NZSIS must have regard to the following principles: respect for privacy, necessity, proportionality, least intrusive means, respect for freedom of expression, including the right to advocate, protest or dissent, legality and oversight. This MPS also specifies certain matters to be included in internal policies and procedures.

Definitions

The Act *means the Intelligence and Security Act 2017.*

GCSB *means the Government Communications Security Bureau.*

NZSIS *means the New Zealand Security Intelligence Service.*

Personal information *means information about an identifiable individual.*

Publicly available information *means information that:*

a) is published in printed or electronic form or broadcast:

b) is generally available to members of the public free of charge or on payment of a fee:

c) is included in a public register (including public registers not covered by the Privacy Act 1993).

Purpose

1. This MPS is issued by the Minister Responsible for the GCSB and the Minister in Charge of the NZSIS pursuant to section 206(f) of the Act.
2. The purpose of this MPS is to provide guidance to GCSB and NZSIS on lawfully obtaining and using publicly available information. The MPS comprises the Minister's expectations for how GCSB and NZSIS should properly perform their functions and establishes a framework for good decision-making and best practice conduct.
3. MPSs are also relevant to oversight of the agencies by the Inspector-General of Intelligence and Security in the exercise of her propriety jurisdiction (the Act requires the Inspector-General of Intelligence and Security to take account of any relevant MPS and the extent to which an agency has had regard to it when conducting any inquiry or review).
4. Every employee making decisions or taking any action related to obtaining and using publicly available information must have regard to this MPS. Employees should be able to explain how they had regard to the MPS. This might amount to an explanation of their consideration of any relevant internal policy or procedures that reflect the MPS. The Directors-General are responsible for ensuring the MPS is reflected in their agency's internal policies and procedures. If any action or decision is taken that is inconsistent with the MPS, employees must be able to explain why the action was taken and how they had regard to the MPS.

Scope

5. This MPS only applies to the lawful collection and use of information that is publicly available information, including publicly available personal information, by GCSB and NZSIS. A social media group that is completely open to the public or a Tweet that is broadcast to the world at large clearly contains publicly available information. Such information could be retrieved and viewed by any member of the public from their computer at any time, and people sharing such information with an unrestricted audience would not likely have a reasonable expectation of privacy with regard to the use of that information.
6. At the opposite end of the spectrum, people may share information within closed groups or to people they have proactively accepted as being able to view that shared information. Such information could not be retrieved or viewed by any member of the public at any time, because an additional step (ie, being approved by the information sharer) is required before it can be viewed. It would be reasonable for the people sharing this information to have an expectation that it would remain private within the particular group or audience and that such information is not generally available to the public. This information is beyond the scope of this MPS.
7. Information that is not publicly available may still be able to be lawfully obtained by GCSB and NZSIS, including by a person voluntarily disclosing that information or pursuant to an intelligence warrant. This MPS does not apply to obtaining or using such information. The MPS on *Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78* will be relevant to such activities. Where an authorisation has been issued in relation to such activity, it must be conducted in accordance with the terms of that authorisation, including any restrictions or conditions set out in the authorisation.
8. Similarly, this MPS does not apply to the undeclared attendance of GCSB or NZSIS employees at a public meeting, or when the agencies are conducting other forms of human intelligence

or surveillance activities. The MPSs on *Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78* and *Surveillance in a public place* will be relevant to such activities.

Context

9. GCSB's and NZSIS's objectives are set out in the Act. Both agencies contribute to:
    a) The protection of New Zealand's national security;
    b) The international relations and well-being of New Zealand; and
    c) The economic well-being of New Zealand.
10. GCSB and NZSIS do this through the performance of their statutory functions, which include:
    a) Intelligence collection and analysis; and
    b) The provision of protective security services, advice and assistance.
11. MPSs are an important component of the measures put in place by the Act to ensure the functions of GCSB and NZSIS are performed with propriety and in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.
12. GCSB and NZSIS obtain information from a range of sources to perform their intelligence collection and analysis function. Those sources include those that the agencies are able to access due to their statutory powers (for example, through the use of covert surveillance, or the interception of private communications under the authority of an intelligence warrant), and information available to any member of the public (for example, information published in the media or openly on the internet).
13. Publicly available information may lead to the production of intelligence (often referred to as 'open source intelligence'). For example, NZSIS may produce intelligence reports about threats of terrorism or violent extremism based on information available on publicly accessible forums. That information may also be used by GCSB and NZSIS to support the collection and analysis of information from other sources (for example, GCSB may research and develop methods of obtaining information through publicly available technical information).
14. The agencies also use information from a range of sources – including publicly available information and open source intelligence produced using that information – to perform their other functions. For instance, GCSB may use publicly available indicators of compromise in providing consented cyber-security activities, or NZSIS may use information published online when vetting for security clearances. Covert and specialised collection of information is both expensive and may involve intrusive powers of the State. For this reason, it is beneficial for GCSB and NZSIS to be able to meet information needs as much as possible from publicly available sources.
15. Unlike most individuals (but similar to many commercial organisations), GCSB and NZSIS may be able to obtain relatively large amounts of publicly available information without the knowledge of persons concerned (including when using an assumed identity), may analyse that information alongside information obtained from other sources, and may have sophisticated ways of analysing that information. These capabilities mean GCSB and NZSIS may be able to use publicly available information to inform assessments and/or identify details that are not immediately obvious from a piece of information considered in isolation.

16. Publicly available information may be used to corroborate, support, or provide a counter-narrative to information obtained secretly. Open source intelligence supports intelligence activity across all GCSB and NZSIS activity, including in operations, investigations, and maintaining geo-political awareness. As with information available from any source, publicly available information can be useful in ascertaining an individual's intentions, identifying persons of concern, and eliminating individuals from investigations. Publicly available information also may form the basis of secret intelligence once assessed and combined with other intelligence sources.

Principles

17. The following principles constitute a framework for good decision-making and must be taken into account by GCSB and NZSIS when obtaining and using publicly available information. This activity should be subject to ongoing review as to whether it continues to be consistent with these principles.

Respect for privacy

18. There may be some privacy interests in publicly available information, particularly where that information is personal information. This does not preclude the agencies from accessing or using that information, but special precautions may need be taken to protect particularly sensitive information once collected. This may include taking steps to mitigate the privacy impact of obtaining and using publicly available information, such as limiting the number of employees who may view analysis of personal information, or anonymising personal information. Importantly, GCSB and NZSIS are subject to the Privacy Act 1993 and information privacy principles 1, 4(a), and 5-12 apply where the agencies have access to personal information.
19. Obtaining publicly available personal information will activate the obligation under privacy principle 8 (accuracy, etc, of personal information to be checked before use). GCSB and NZSIS must take steps that are reasonable in the circumstances to ensure that the information is accurate, up to date, complete, relevant and not misleading (having regards to the purpose for which the information is proposed to be used) before using that information. This is relevant, for example, in performing the NZSIS's security vetting function.
20. The public register privacy principles within section 59 of the Privacy Act 1993 will be relevant to the manner in which GCSB and NZSIS seek to gain information from public registers.

Necessity

21. Publicly available information, including personal information, should only be obtained and used for a purpose that is consistent with GCSB and NZSIS performing their statutory functions. GCSB and NZSIS should be clear that any activities involving the collection of publicly available information have a clear purpose, and ensure the purpose continues to remain throughout the course of the collection activities.
22. Examples of purposes where it will be necessary to obtain and use publicly available information include acquiring background or contextual information relevant to the performance of a statutory function, acquiring information to identify behavioural patterns of interest, and obtaining information to assess the accuracy of information already held.

23. Collecting information for the personal interest of an employee (unrelated to their role) while acting in their official capacity, for example, would not satisfy the necessity principle.

Proportionality

24. The collection and use of publicly available information should be proportionate to the purpose for which it is carried out. The amount of information may be one factor to consider when assessing proportionality. For example, bulk collection of publicly available information should only be carried out where this is proportionate to the purpose. The age of information may also be a consideration, as there may be an increased risk that the information is out of date and less likely to be fit for purpose.
25. Publicly available information may be collected and used to identify associates or contacts of a person of security concern. Publicly available information and analysis carried out using that information may contain personal or sensitive information about individuals not relevant to the purpose for which information is sought. Where practicable, GCSB and NZSIS should minimise the collection of publicly available personal information about persons who are not relevant to the purpose for which information is sought.
26. When publicly available personal information is collected, assessed, collated and combined across multiple sources, GCSB and NZSIS should assess the additional privacy impact of collection from each additional source. When considered with the least intrusive means principle below, this places some bounds on the collection of publicly available personal information.
27. Privacy principles 10(a) and 11(b) place limits on using and disclosing personal information sourced from a publicly available publication where it would be unfair or unreasonable to do so, unless there is reasonable grounds to believe the use or disclosure is necessary to enable GCSB or NZSIS to perform any of its functions (privacy principles 10(2) and 11 (fa)). Fairness and reasonableness are therefore important tests when making a proportionality assessment.

Least intrusive means

28. In collecting publicly available information, GCSB and NZSIS must use the least intrusive means available to obtain the required information in a secure, timely and reliable manner (noting that open source collection is one of the least intrusive means of collection of intelligence, especially compared to warranted methods).

Respect for freedom of expression, including the right to advocate, protest, or dissent

29. Section 19 of the Act provides that the exercise by any person in New Zealand or any class of persons in New Zealand of their right to freedom of expression under the law (including the right to advocate, protest, or dissent) does not itself justify an intelligence and security agency taking any action in respect of that person or class of persons.
30. GCSB and NZSIS must ensure that its use of particular information sources or platforms to obtain publicly available information is consistent with the protection in section 19. Acts of advocacy, protest or dissent are not, of themselves, justification for collecting publicly available information. GCSB and NZSIS must ensure collection of publicly available information related to such acts is undertaken only where the purpose of doing so is necessary to enable the agency to perform one of its statutory functions in furtherance of

one (or more) of its objectives. For example, the fact of a protest itself is not sufficient justification for collecting information but following up on a legitimate security concern that arises in relation to a planned protest may be sufficient justification.

Legality

31. GCSB and NZSIS must ensure that the collection and use of publicly available information will be carried out in accordance with the law. Where appropriate, legal advice should be sought. As noted above, particular care must be taken to ensure that, without a warrant or using other methods recognised under the Act, only information that is publicly available is collected by GCSB and NZSIS.
32. GCSB and NZSIS may collect publicly available information using collection methods that are not available to the public (for example, by using specialist techniques for collecting information or through relationships with other people who have access to the information). The agencies must take particular care to ensure that any collection of publicly available information using methods not available to the public does not involve any unlawful activity, unless done so with an authorisation under Part 4 of the Act.
33. In addition to complying with the law, GCSB and NZSIS must consider the impact of obtaining and using publicly available information on the rights affirmed under sections 15 (manifestation of religion and belief), 16 (freedom of peaceful assembly), 17 (freedom of association) and 19 (freedom from discrimination) of the New Zealand Bill of Rights Act 1990.
34. GCSB and NZSIS must have regard to the statutes that establish and govern individual public registers, including any relevant restrictions and privacy protection mechanisms they contain. The legality of collection and use of public register information by GCSB and NZSIS should be assessed on a case by case basis.

Oversight

35. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight, including through the keeping of appropriate records of collection of publicly available information made in respect of particular individuals.

Matters to be reflected in internal policies and procedures

36. GCSB and NZSIS must have internal policies and procedures that are consistent with the requirements and principles above, and must have systems in place to support and monitor compliance. Those policies and procedures must also address the following additional matters:

Compliance with the information privacy principles
GCSB and NZSIS are subject to information privacy principles 1, 4(a), and 5 to 12 of the information privacy principles in the Privacy Act 1993. All policies relating to obtaining publicly available personal information and the handling of any information collected or held as a result of such activities must incorporate guidance about compliance with the information privacy principles.

Compliance with State Services Code of Conduct
The Directors-General of the GCSB and NZSIS must issue policies and procedures that reflect their agencies' obligations under the State Sector Act 1988.

Health and safety

The collection and use of publicly available information must be undertaken consistently with GCSB's and NZSIS's obligations under the Health and Safety at Work Act 2015.

Sensitive category individuals

GCSB and NZSIS must have a policy setting out the restrictions and protections necessary in the conduct of activities in respect of sensitive categories of individuals (for example, children and young people aged under 18 years of age, Members of New Zealand's Parliament, members of the New Zealand judiciary, journalists, lawyers, registered medical practitioners or other providers of health services attracting medical privilege, and people vulnerable by reason of illness or other capacity).

Authorisation at a high level within the relevant agency is required for activities conducted in respect of these individuals. This will provide reassurance that appropriate measures are in place in the event that publicly available information may be obtained or used in respect of sensitive category individuals.

Copyright

Collection of publicly available information by GCSB and NZSIS may raise issues about access to and use of copyrighted information. Section 63 of the Copyright Act 1994 provides that copyright is not infringed by any use of material by or on behalf of the Crown for the purpose of national security, although for any such use the Crown is liable to pay equitable remuneration to the copyright owner.

GCSB and NZSIS should have a policy that provides guidance to employees about the issues raised by copyright in publicly available information to ensure that the Crown's legal obligations are met.

Training

All employees of an intelligence and security agency who use publicly available information in their work must be provided training on all relevant law, policies and procedures in relation to the collection and use of publicly available information.

Authorisation procedures

37. GCSB and NZSIS must ensure that where any difficult or sensitive issues regarding the legality or propriety of the collection and use of publicly available information arise, these are dealt with at a sufficiently senior level within the agency. For example, publicly available information may include information that has been previously leaked from or mislaid by its owner. In situations where this is known or suspected to have occurred, employees must ensure that the issue is escalated appropriately and where necessary expert advice, including legal advice, is sought.

Duration of ministerial policy statement

38. This MPS will take effect from 28 September 2017 for a period of three years. The Minister who issued an MPS may, at any time, amend, revoke or replace the MPS.

Ministerial Policy Statement issued by:

Hon Christopher Finlayson
Minister responsible for the Government Communications Security Service
Minister in charge of the New Zealand Security Intelligence Service

September 2017