Ministerial Policy Statement

Publicly available information

Summary

It is lawful for GCSB and NZSIS to obtain, collect and use publicly available information. This ministerial policy statement (MPS) provides guidance on the conduct of this activity. In making decisions related to obtaining, collecting 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.*

Open source intellligence *means intelligence products produced from publicly available information.*

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.

GCSB *means the Government Communications Security Bureau.*

NZSIS *means the New Zealand Security Intelligence Service.*

Context

Obtaining, collecting and using publicly available information occurs within a wider information collection context

1. GCSB and NZSIS obtain or collect information through a range of methods under the Act in order to perform their statutory functions. These authorities include:
    a) Intelligence warrant;
    b) Business records directions;
    c) Authorisations to access restricted information; and
    d) Direct access agreements.
2. GCSB and NZSIS also collect information through means that do not require a specific legal authorisation, including
    a) Through the disclosure of information - this may be provided in a number of ways, including:
        i. unsolicited, without any prior request from GCSB or NZSIS;
        ii. in response to a request from GCSB or NZSIS under section 121 of the Act (*Section 121 requests* MPS);
        iii. by collecting, requesting and receiving information from a person (known as human intelligence activities) (*Collecting human intelligence MPS*);
        iv. from overseas public authorities (*Cooperating with overseas public authorities MPS*);
    b) Obtaining, collecting and using publicly available information (this MPS);
    c) Through the conduct of other lawful activities, such as conducting surveillance in a public place (*Conducting surveillance in a public place MPS)*.

Publicly available information

3. To perform their functions, GCSB and NZSIS may access publicly available information. For example, the GCSB and NZSIS may need to access and obtain or collect information about an individual's social media posts, or their contacts or group memberships. GCSB and NZSIS may also collect publicly available information (including large data sets) in order to identify people, events, or activities of interest – for example, accessing or monitoring specific open online communities or social media platforms, or for reference purposes to support their functions more generally.
4. Publicly available information supports GCSB and NZSIS functions, including by developing different forms of open source intelligence. Publicly available information may be combined with other sources of information (including that obtained or collected under authorisations) to inform assessments and/or identify details that are not immediately obvious from a piece of information considered in isolation. Open source intelligence supports intelligence activity across all GCSB and NZSIS activity, including in operations, investigations, and maintaining situational awareness (for example, of the geo-political context). The range of uses include:
    a) discovering previously unidentified actors, events, or activities that may pose a risk to New Zealand's national security;

b) providing further information on identified individuals and threat actors (for example violent extremists);

c) supporting other sources to corroborate, support, or provide a counter-narrative;

d) using indicators of compromise in providing consented cyber-security activities; and

e) supporting vetting of security clearances.

Guidance for GCSB and NZSIS

Scope of this MPS

5. This MPS applies to the lawful collection and use by GCSB and NZSIS of information that is publicly available, including publicly available personal information.

6. People sharing information in a way that makes it able to be obtained by a member of the public would not necessarily have a reasonable expectation of privacy with regard to the use of that information (for example, in an open social media group, or Tweet). Publicly available information includes information shared within groups where there is an ability to 'opt in' with minimal restrictions or vetting of the membership of the group (for example simply providing an email or other login details). This level of scrutiny is usually about determining interest in the group, rather than verifying the real identities of those seeking access.

7. Online communities also exist where only people that are proactively approved members can view and/or participate. Such information could not be viewed by a member of the public without undergoing greater level of scrutiny than simply 'opting in' as outlined in [paragraph 6]. It would therefore be more likely for people sharing information this way to have a reasonable expectation of privacy. Information shared in this way is beyond the scope of this MPS, it may still be within the scope of an authorisation or activities outlined in the *Collecting human intelligence MPS*.

8. Information that is behind a paywall may still be publicly available information. For example, online forums or comment sections of publications that require a one-off payment or subscription are publicly available, or publicly available information that has been aggregated by a third party. GCSB and NZSIS must consider whether collecting publicly available information may be in breach of a service's terms and conditions and seek legal advice as appropriate on whether collecting information through this method requires additional authorisation. In providing information for creation of an account for a paywalled subscription, the *Assumed Identities MPS* or *Legal Entities MPS* must be considered, as appropriate.

Principles

9. The following principles constitute a framework for good decision-making and set out best practice conduct. They must be taken into account by GCSB and NZSIS when obtaining, collecting 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

10. There may be some privacy interests in publicly available information, particularly where that information is personal information. This does not preclude the agencies from collecting or using that information. As outlined in the *Information Management MPS* protections

applied to information may be able to mitigate privacy impacts. Such protections may include limiting the number of employees who may have access to analysis of personal information, or anonymising personal information.

11. The right to privacy (in the form of freedom from unreasonable search and seizure) is protected by section 21 of the New Zealand Bill of Rights Act 1990. In addition, GCSB and NZSIS are subject to the Privacy Act 2020 and privacy principles 1, 4(a), and 5-13 apply where the agencies have access to personal information.
12. Collecting publicly available personal information will activate the obligation under privacy principle 8 (an organisation must check that the information is accurate, up to date, complete and relevant before using). GCSB and NZSIS must take reasonable steps to check the accuracy of the information, including potentially collecting further publicly available information. This is relevant, for example, in performing the NZSIS's security vetting function.

Necessity

13. Publicly available information, including personal information, should only be obtained, collected 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 a purpose continues throughout the course of the collection and use of publicly available information.
14. Examples of purposes where it will be necessary to obtain, collect 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, collecting information for reference purposes and collecting information to assess the accuracy of information already held.
15. For reasons of operational security, GCSB and NZSIS may need to obfuscate their interest in certain information. This may be achieved by transferring a copy of a broader set of publicly available information to a secure environment before analysing the relevant information.

Proportionality

16. 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. The age of the 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.
17. 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 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.
18. Privacy principles 10 and 11 of the Privacy Act place limits on government agencies using and disclosing personal information. Certain exceptions (privacy principles 10(2) and 11(1(g))) allow for the GCSB or NZSIS to use or disclose such information when there are reasonable grounds to believe the use or disclosure is necessary to enable GCSB or NZSIS to perform any of their functions.

Least intrusive means

19. In collecting publicly available information, GCSB and NZSIS must use the least intrusive means available to obtain or collect the required information in a secure, timely and reliable manner (noting that the collection of publicly available information is one of the least intrusive means of collection of intelligence).

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

20. 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.
21. GCSB and NZSIS must ensure collection of publicly available information related to advocacy, protest, or dissent is undertaken only where the purpose of doing so is necessary to enable the agency to perform one of its statutory functions. For example:
    a) Protesting, or planning a protest, will not be sufficient justification by itself for collecting information. If, however, a security concern arises, the agencies may be justified in collecting publicly available information about the threats. One indication of a security concern could be if the views expressed in the protest include a serious threat to lives or security.
    b) Public expression of certain views will generally not be sufficient justification on its own for collecting publicly available information. However, if there are security concerns about the views that are expressed (such as advocating online a serious threat to lives or security), this might provide justification for collecting information.

Legal obligations

22. GCSB and NZSIS must ensure that the collection and use of publicly available information will be carried out in accordance with the law. Care must be taken to ensure that only publicly available information is collected – unless the agencies have a warrant or other authorisation under the Act. Where appropriate, or if there is any doubt, legal advice should be sought.
23. 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). 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.
24. 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

25. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight. This includes keeping appropriate records of the collection of publicly available information for the purposes of fulfilling the agencies' function.

Matters to be reflected in internal policies and procedures

26. As public service agencies, GCSB and NZSIS must comply with legislation, policies and procedures common to all public service agencies.[1]

27. In addition, 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

28. GCSB and NZSIS are subject to information privacy principles 1, 4(a), and 5 to 13 of the privacy principles in section 22 the Privacy Act 2020. All policies relating to collecting 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.

Consideration of impact on rights affirmed under New Zealand Bill of Rights Act 1990

29. In developing policies and procedures relating to obtaining, collecting and using publicly available information, GCSB and NZSIS must consider the impact of obtaining, collecting and using publicly available information on the rights affirmed under the New Zealand Bill of Rights Acts 1990, including, as relevant, sections 14, 15, 16, 17 and 19 (manifestation of religion and belief, freedom of peaceful assembly, freedom of association, and freedom from discrimination).

Sensitive category individuals

30. 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, holders of the privileges outlined in the Intelligence and Security Act 2017, New Zealand journalists, refugees, asylum seekers and protected persons, and people vulnerable by reason of illness or other incapacity).

31. 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.

Collection of large personal datasets

32. GCSB and NZSIS may collect large datasets which might include personal information relating to a number of individuals. GCSB and NZSIS must have a policy that provides guidance on the collection, use, retention and disposal of this type of information.

---

[1] *This includes the Public Service Act 2020 and the Health and Safety at Work Act 2015.*

Copyright

33. 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. In many instances, GCSB and NZSIS's collection of publicly available information will not result in a copyright infringement, however, where GCSB or NZSIS employees have concerns or uncertainty about a potential copyright infringement, they should seek legal advice.

Training

34. All employees of an intelligence and security agency who use publicly available information collected by the GCSB OR NZSIS 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

35. 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; the issue is escalated appropriately and where necessary expert advice, including legal advice, is sought.

Duration of ministerial policy statement

36. This MPS will take effect from 01 March 2022 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 Andrew Little

Minister Responsible for the Government Communications Security Bureau
Minister Responsible for the New Zealand Security Intelligence Service
01 March 2022