



Ministerial Policy Statement

Conducting surveillance in a public place

Summary

It is lawful for the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) to conduct surveillance in a public place without a warrant, subject to some important limits.

This ministerial policy statement (MPS) provides guidance on the proper conduct of this activity. In making decisions related to the conduct of surveillance in a public place, GCSB and NZSIS must have regard to the following principles: legality, respect for freedom of expression, respect for privacy, necessity, proportionality, less intrusive means to be considered, minimisation of impact on third parties and oversight. This MPS also specifies certain matters to be included in internal policy 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*.

Public place means a physical place that is routinely open to the public or is used by the public, whether for free or on payment of a charge, and includes any form of public transport. For the avoidance of doubt, it also includes places that the owner or occupier is lawfully entitled to exclude or eject any person from.

Surveillance in a public place means activity that involves the use of NZSIS or GCSB employees collecting intelligence in a public place, primarily through monitoring, observing or listening to persons, their movements, conversations or other activities. This primarily occurs through observation and opportunistic or temporary deployments of technologies, and may involve recording.

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(e) of the Act.
2. The purpose of this MPS is to provide guidance to GCSB and NZSIS on the conduct of surveillance in a public place. 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 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 surveillance in a public place 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 surveillance activity that is conducted in a public place and lawful. This means that the surveillance can be carried out without GCSB and NZSIS employees needing to do any unlawful activities that would require the agency to obtain a warrant or other form of authorisation issued under the Act. Unlawful acts that would require the agencies to obtain a warrant would include trespass or offences in relation to private property, or that involve the use of particular technology or interception of private communications.
6. Surveillance activity that involves otherwise unlawful acts may only be carried out in accordance with an authorisation issued under Part 4 of the Act. Surveillance activities conducted pursuant to an authorisation must be conducted in accordance with the terms of that authorisation, including any restrictions or conditions set out in the authorisation. They must, like all activities of GCSB and NZSIS, be conducted with propriety. This MPS does not address activities carried out under an authorisation.

Context

7. 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.
8. 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.

9. 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.
10. To perform any of their statutory functions, it is necessary for GCSB and NZSIS to use a range of methods to collect information, including surveillance. Surveillance may need to be carried out using covert methods in order to obtain information that could not be obtained if the subject of the surveillance was aware it was occurring, or to avoid alerting persons to other covert activities of GCSB and NZSIS. Such surveillance methods are a legitimate element in the toolkits of many New Zealand government agencies with an intelligence collection or law enforcement function. NZSIS carries out surveillance more routinely than GCSB.
11. For example, NZSIS might conduct surveillance in relation to an individual who is the subject of a counter-espionage investigation in order to identify people they are in contact with, their movements, and their whereabouts on any given day. The information gathered from such surveillance can be useful in ascertaining the individual's intentions, identifying other persons of concern, and eliminating individuals from the scope of investigations.
12. Surveillance activities (especially when carried out covertly) may give rise to risks to the particular operation, to individual GCSB or NZSIS employees and others, and to the reputation of GCSB and NZSIS and the New Zealand Government, in the event an operation is uncovered.
13. Surveillance in a public place may give rise to concerns about individual privacy, with those concerns likely to vary depending on the nature of the activity and the location of the surveillance (expectations of privacy are likely to be much higher, for example, in relation to a funeral service at a cemetery, than in relation to the conduct of supermarket shopping). In a particularly public place (for example, in a public park) reasonable expectations of privacy may be minimal, however individuals are unlikely to expect to be singled out for attention.
14. The nature of the activity will also be relevant. While generally individuals may have a low expectation of privacy during supermarket shopping, individuals may have a higher expectations of privacy during a consultation at a supermarket pharmacy regarding a health issue. Similarly, most people would consider there are still privacy interests at stake in a personal conversation held in a public park despite the location clearly being public in nature, and would not expect their conversation to be listened to or their meeting to be watched.
15. There may even be reasonable expectations of privacy associated with a private conversation in a public place, depending on the circumstances. For this reason the Crimes Act 1961 defines "private communication" to mean:

Private communication—

- (a) *means a communication (whether in oral or written form or otherwise) made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but*
- (b) *does not include such a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so.*

16. More generally, the New Zealand public reasonably expect that activities conducted in public places are not subject to systematic surveillance by the state and that agencies with surveillance powers and capabilities will use them with restraint.
17. These concerns might arise on the part of those who are the subject of surveillance (should the surveillance become known to them), and others who interact with them or come into close proximity with subjects while they are subject to surveillance. Whether the concerns amount to a reasonable expectation of privacy will depend on the nature of the place and other circumstances and will need to be assessed on a case-by-case basis.

Principles

18. The following principles constitute a framework for good decision-making and must be taken into account by GCSB and NZSIS when planning and conducting surveillance in a public place. All surveillance in a public place should be subject to ongoing review as to whether it continues to be consistent with these principles. This is particularly so given that, in most cases, it is not possible to know in advance the location or locations that the activity will take place in.

Legality

19. GCSB and NZSIS must ensure surveillance in a public place is undertaken in accordance with the law. Section 21 of the New Zealand Bill of Rights Act 1990 (freedom from unreasonable search and seizure) is not limited to searches for law enforcement purposes,¹ and therefore applies in respect of activities undertaken by the intelligence and security agencies. In addition, surveillance may impact on the enjoyment of the rights to freedom of expression, association and movement (affirmed by sections 14, 17 and 18 respectively of the New Zealand Bill of Rights Act 1990).
20. Some forms of surveillance in a public place are unambiguously lawful. For example, the Supreme Court has said video surveillance taken in a public place is generally lawful because it does not involve any state intrusion into privacy.² The question of lawfulness in this context is a fact-specific judgement. There are a number of factors that are relevant to determining legality. These factors, which go to lawfulness in any given situation, are discussed below.
21. GCSB and NZSIS should consider these factors carefully. If there is any doubt as to legality in any situation, GCSB and NZSIS should apply for a warrant before proceeding. Where surveillance activity is prolonged, the question of legality must be kept under review.

Use of equipment

22. The use of technology that captures images not able to be seen by the naked eye, such as the use of infra-red imaging, or the use of a zoom lens enabling surveillance in an otherwise unobservable area, may constitute an unreasonable search under the New Zealand Bill of Rights Act 1990.

¹ See, for example, *Hamed v R* [2011] NZSC 101 at [225] per Tipping J

² *Ibid*, at [167] per Blanchard J

The nature of the location of surveillance

23. What surveillance is lawful without a warrant also depends on the location of the surveillance. What is a 'public' place is not always clear-cut, with there being a spectrum of 'publicness'. Some places are clearly public in nature (such as the street). Others are clearly private (such as inside a private residence or inside a hired hotel room). However, some locations might be one or the other – or somewhere in between – depending on the circumstances (for example, a place of religious worship or a hospital waiting room).
24. Whether the subject of surveillance is within public view is also relevant. For example, the viewing of someone in their front yard from the street does not raise concerns about lawfulness. However, if a fence needs to be climbed in order to undertake the surveillance or to plant a camera, that action is likely to constitute a search and therefore require an assessment of reasonableness from a Bill of Rights Act perspective.
25. In addition to considerations of reasonableness, the agencies also need to exercise particular caution where the legal basis of their access to the location is an implied licence (for example, an implied licence to members of the public to undertake recreational activities on privately-held land).³ The scope of that licence is relevant; where the agencies go beyond that scope, or where the basis of the implied licence to enter is inconsistent with them being present and conducting surveillance activities (particularly where they start using technology), the surveillance may become unlawful.

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

26. 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 of itself justify an intelligence and security agency taking any action in respect of that person or class of persons. This important protection should be a key factor in the planning and undertaking of surveillance activities.
27. GCSB and NZSIS must ensure the conduct of surveillance in a public place does not infringe upon that right. In addition, the agencies must be alive to sensitivities around surveillance of protest activity and public gatherings or meetings. Where surveillance at events where the right to freedom of expression is being lawfully exercised, the agencies should ensure the act of advocacy, protest or dissent is not, of itself, the justification for the surveillance. As with any surveillance undertaken in a public place, GCSB and NZSIS must ensure such surveillance is undertaken only where necessary to enable the agency to carry out one of its statutory functions in furtherance of one of its objectives.

Respect for privacy

28. The right to privacy is a human right, protected under the United Nations Declaration of Human Rights and under article 17 of the International Covenant on Civil and Political Rights (the ICCPR). Article 17 of the ICCPR applies to surveillance and interception, which must be authorised by relevant legislation. The right to privacy (in the form of freedom from

³ *Implied licence to enter land may exist in the absence of an express permission from the occupier; generally the scope of this licence will be limited by reference to the reason it is implied to exist. For example, in the most common scenario in which implied licence arises, an uninvited visitor may enter a property for the purpose of communicating with the occupier or to seek entry to the property more generally. In such situations, the implied licence is limited to what is necessary to achieve this purpose. It may also be revoked at any time by the occupier.*

unreasonable search and seizure) is protected by section 21 of the New Zealand Bill of Rights Act 1990. In addition, both GCSB and NZSIS are subject to relevant [information privacy principles](#), including principle 1 (purpose of collection) and principle 4(a) (lawful manner of collection).

29. As discussed above, the location of surveillance activities – ie, the ‘publicness’ or otherwise – affects expectations of privacy. When planning and conducting surveillance in a public place, GCSB and NZSIS will often not know in advance where the subject of the surveillance is going to go and therefore it will be difficult to make assessments as to reasonable expectations of privacy in advance. For this reason it is important that the possible impacts from the surveillance are kept under review as activity is occurring. This will involve ongoing consideration of the location of the proposed surveillance activity, whether it is in fact public, private, or possibly somewhere in between. The agencies should seek to minimise any intrusion into privacy as much as possible.
30. The nature of activities undertaken in that place is a relevant factor in assessing the possible privacy intrusion; for example, the intrusion into privacy in respect of surveillance in a public cemetery will be greater than if the surveillance was undertaken in a supermarket, since the nature of activities commonly undertaken in cemeteries may be of a sensitive and personal nature.
31. The extent of impacts on privacy may also be determined by reference to the duration of surveillance. For instance, a warrant is required by law enforcement officers under the Search and Surveillance Act 2012 for observation of private activity in the curtilage (which includes a porch or deck) of a private premise, and any recording of that observation, beyond a certain duration.⁴ This illustrates that while some surveillance of a limited duration may have been considered reasonable by Parliament, a more prolonged period of activity requires a warrant to be obtained in the law enforcement context.

Necessity

32. Surveillance in a public place should be undertaken only where necessary to enable the agencies to carry out their statutory functions. This may include surveillance for operational security purposes and training in surveillance techniques. When carrying out training activity GCSB and NZSIS should only use willing participants who are aware of the nature of the activities of which they are the target.

Proportionality

33. The intrusiveness of any surveillance in a public place should be proportionate to the purpose for which it is carried out. In each case, the scope of the proposed surveillance and level of intrusiveness should be balanced against the degree to which it will meet a defined intelligence need. Relevant factors in assessing proportionality may include the duration of the surveillance, the number of people impacted by it (including those who are not the target of the surveillance), and the nature and sensitivity of the activities under observation.
34. Where surveillance activity is prolonged, the question of proportionality must be kept under review.

⁴ Section 46(1)(e) Search and Surveillance Act 2012.

Less intrusive means to be considered

35. As it is a lawful activity and takes place in a public place, surveillance involves a lower level of intrusiveness than some other methods of intelligence collection. However, GCSB and NZSIS should always consider whether the intelligence need can be met by a less intrusive means of collection.
36. The location in which surveillance will be undertaken is a relevant factor in considering the degree of intrusiveness. The nature of a public place or the activities that routinely occur there may give rise to particular sensitivities. For example, people in a hospital waiting room may be particularly distressed, and any visual surveillance carried out in such a location should have particular regard to the principle of minimisation of impact on third parties (see below). GCSB and NZSIS should also have regard to the extent to which surveillance in a public place might need to be carried out in places of religious or cultural significance and should ensure that the potential impacts of any surveillance on the enjoyment of those places by members of that religious or cultural group are minimised.
37. The extent to which technology will be involved is also relevant. It may enhance GCSB's and NZSIS's ability to collect intelligence from surveillance in a public place and ensure that intelligence is reliable, but it may significantly increase the intrusiveness of the surveillance (for instance, use of a high-powered lens, as discussed above). Importantly, a warrant will be required to record any private conversations where a reasonable expectation of privacy arises.

Minimisation of impact on third parties

38. A key objective of surveillance in a public place is often to obtain an understanding of the people with whom a person of security concern has contact, or the people associated with a place of security concern. Surveillance activity must always be related to a particular person or place with relevance to the agencies' statutory functions. The agencies should consider the possible impact of surveillance activity on persons who are not relevant, and in particular, the risk of collecting information about such persons.
39. Where practicable, measures should be taken to avoid or minimise surveillance activity carried out in a public place that may affect people who are not relevant to the purpose of the surveillance. This might include persons who have only incidental contact with the subject of the surveillance or persons regarded as sensitive persons because of their age, occupation, or other vulnerabilities. In many cases, the question of who the subject is meeting or interacting with will actually be the purpose of the surveillance.

Oversight

40. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight, including through the keeping of appropriate records about the planning, approval, conduct and reporting of surveillance activities carried out in a public place.

Matters to be reflected in internal policies and procedures

41. GCSB and NZSIS must have, and act in compliance with, 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 matters:

Compliance with State Services Code of Conduct

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

Health and safety

All surveillance in a public place must be undertaken consistently with GCSB's and NZSIS's obligations under the Health and Safety at Work Act 2015. The health and safety of all employees and all other persons who are impacted by surveillance activities will be a key consideration in the planning and undertaking of such activities.

Training

GCSB and NZSIS employees may only participate in surveillance in a public place if they have been appropriately trained for the role they are expected to play, and on the relevant law, policies and procedures.

Cooperation with and assistance from other agencies

Where surveillance in a public place is carried out with assistance from other agencies, GCSB and NZSIS remain responsible for the conduct of these activities and the actions of employees of other agencies. All such activities will be open to inquiry by the Inspector-General of Intelligence and Security. Any employees of other agencies who assist GCSB and NZSIS in the conduct of surveillance activities should be appropriately trained for the role they are expected to play.

Where surveillance in a public place is carried out alongside or in cooperation with an operation led by another agency (for example, NZSIS and the Police each carrying out surveillance relevant to counter-terrorism), each agency shall remain subject to their own internal controls and subject to their usual oversight mechanisms.

Compliance with 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 surveillance in a public place and the handling of any information collected through such activity must incorporate guidance about compliance with the information privacy principles.

Information management

Information collected as a result of surveillance in a public place may be among some of the more sensitive information held by GCSB and NZSIS, given it may include sensitive information about identifiable individuals. This information must be handled and stored in accordance with clear access controls that correspond to the sensitivity of the information. The MPS on *Management of information obtained by the GCSB and NZSIS* applies in relation to management of this information.

Incidentally obtained information about third parties not relevant to the subject of surveillance may only be retained for the purposes of disclosing that information to other public authorities in order to assist them to perform their own statutory functions as provided for in section 104 of the Act. If there is no reason to disclose that information to another public authority, the information must be disposed of in accordance with the requirements detailed in the MPS on *Management of information obtained by the GCSB and NZSIS*.

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 Parliament, members of the judiciary, journalists, lawyers, registered medical practitioners or other providers of health services attracting medical privilege, and people vulnerable by reason of illness or other incapacity). 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 public surveillance activities need to be carried out in respect of sensitive category individuals.

Authorisation procedures

42. Surveillance activities should be authorised at a level of seniority within the agencies that is commensurate with the level of operational, reputational, health and safety and legal risk involved. The level of authorisation required should be dictated by the tactics to be deployed during the surveillance operation and the assessed overall residual risk exposure. For instance, the use of technology that may increase the level of intrusiveness of the surveillance should form part of any consideration of authorisation levels. The identification and management of operational, reputational, legal, and health and safety risks should be carried out in accordance with a risk management policy.
43. The Director-General of each agency should have delegations in place for such authorisations.

Duration of ministerial policy statement

44. 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