Office of the Inspector-General of Intelligence and Security

Review of NZSIS use of closed circuit television (CCTV)

Public Report

Brendan Horsley
Inspector-General of Intelligence and Security
June 2021

CONTENTS

Introduction 1
Key legal principles applicable to CCTV 1
The Service's current use of CCTV 3
Applicable policies 4
    CCTV SOP 4
    Surveillance SOP 4
    Analysis 5
Record-keeping 6
Basis for access to CCTV network 8
    Service's basis for access 8
A note on classification 8
Findings and recommendations 9
List of abbreviations 10

INTRODUCTION

1. As part of my functions under the Intelligence and Security Act 2017 (ISA),[1] I have conducted a review of the New Zealand Security Intelligence Service's (NZSIS or Service) access to, and use of, closed circuit television (CCTV). In undertaking this review, I have consulted with the Privacy Commissioner and had the benefit of his expertise in this area.[2]

2. This report is a "baseline review"; a relatively brief review geared toward developing a basic understanding of the Service's operations in this area with a view to ongoing consideration. Importantly, the review is focussed only on the Service's current access, rather than future potential uses. As part of this review, I have visited a location used by the Service for CCTV access, attended briefings with Service personnel and reviewed all available documentation relating to the use of CCTV in general, including the CCTV logs and the applicable Standard Operating Procedures.

3. During the review, the Service has engaged with my Office, and the Privacy Commissioner, in a meaningful and constructive way. As outlined below, the Service has taken some steps that will improve its operations in this area. These include strengthening record-keeping in relation to CCTV usage and formalising access to any CCTV network by way of a Memorandum of Understanding (MOU). I set out my findings and recommendations fully below.

KEY LEGAL PRINCIPLES APPLICABLE TO CCTV

4. The use of CCTV surveillance in public places is generally, albeit not always, lawful. As Blanchard J noted in *Hamed v R*, "[p]eople in the community do not expect to be free from the observation of others, including law enforcement officers, in open public spaces such as a roadway or other community-owned land like a park, nor would any such expectation be objectively reasonable."[3]

5. While the use of CCTV footage in public places is largely unregulated,[4] there are a number of key principles that apply to the state's use of, and access to, CCTV footage. With respect to the security agencies' activities, these are comprehensively set out in the Ministerial Policy Statement, "Conducting surveillance in a public place" (the MPS), which sets out the Minister's expectations on the conduct of surveillance in a public place.[5] The MPS must be reflected in each agency's internal policies and procedures[6] and, in making any decision or taking any action, all employees must have regard to the relevant MPS.[7] In conducting this

---

1 ISA, s 158(1)(f).
2 ISA, s 161 refers.
3 *Hamed v R* [2011] NZSC 101, [2012] 2 NZLR 305 at [167].
4 In 2017 the Law Commission proposed policy statements to regulate CCTV within the law enforcement context, but these recommendations have yet to be implemented. See Law Commission "Review of the Search and Surveillance Act 2012" (NZLC, R141, 2017) at [11.70] to [11.71].
5 While the Ministerial Policy Statement (MPS) only applies to lawful public surveillance, the key principles of respect for privacy, necessity and proportionality remain directly relevant to warranted activities.
6 MPS "Conducting surveillance in a public place" (2017) at [4].
7 ISA, s 209.

review, I have also had regard to the MPS and the extent to which the Service has had regard to it, as I am required to do.[8]

6. As stated in the MPS, unwarranted public surveillance must not breach a person's right to freedom from unreasonable search pursuant to s 21 of the New Zealand Bill of Rights Act 1990 (NZBORA). Public surveillance will constitute a "search" for the purposes of s 21 whenever it infringes a person's "reasonable expectation of privacy".[9] The concept of a "reasonable expectation of privacy" is "directed at protecting a 'biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination by the state' and includes information 'which tends to reveal intimate details of the lifestyle and personal choices of the individual'".[10]

7. Some examples of surveillance of public places that may infringe a reasonable expectation of privacy include the use of technology such as infra-red imaging, night vision or the use of zoom lenses.[11] Other factors will also be relevant. These include the nature of location of the surveillance within the spectrum of "publicness",[12] the nature of the activity being surveilled[13] and duration of the surveillance.[14] For example, surveillance of a target's movements in their vehicle for an hour may not interfere with reasonable expectations of privacy, whereas prolonged tracking of that target over the course of days will almost inevitably do so.[15]

8. Where the surveillance impinges on a person's reasonable expectation of privacy, it will constitute a "search". The question which then arises is whether the search is "unreasonable" for the purposes of s 21 of the NZBORA. For example, an unwarranted search may well be unreasonable where there was sufficient time to obtain a search warrant.

9. The other key legal principles relevant to surveillance in a public place are the principles of necessity and proportionality. In terms of necessity, surveillance in a public place should only be undertaken where necessary to enable the agencies to carry out their statutory functions.[16] The proportionality principle means that the intrusiveness of the surveillance must be proportionate to the purpose for which it is being carried out. As stated in the MPS, 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".[17] The factors that are relevant to this assessment include the duration of the surveillance, the number of people impacted by it and the nature and sensitivity of the activities under observation.[18] A further consideration may be the vulnerability of those inadvertently surveilled, for example whether children might be captured in any collection.

---

8 ISA, s 158(2).
9 *R v Alsford* [2017] NZSC 42, [2017] 1 NZLR 710 at [63].
10 *Alsford*, above n 9, at [63] citing *R v Plant* [1993] 3 SCR 281 at 293.
11 See *Hamed*, above n 3, at [167].
12 MPS at [23] to [25] and [29].
13 MPS at [30].
14 MPS at [31].
15 For an example of consideration of the duration of surveillance in the context of tracking movements via cell phone location, see *Carpenter v United States* 585 US (2018).
16 MPS at [32].
17 MPS at [33].
18 MPS at [33].

10. There are, of course, other principles and protected rights that are relevant to surveillance of public places by the state. These include the right to freedom of expression, including a right to peaceful protest, and rights to freedom of association and movement.[19] The state must also always consider whether the intelligence need can be met by a less intrusive means of collection and take reasonable steps to minimise the impact of the surveillance activities on third parties.

THE SERVICE'S CURRENT USE OF CCTV

11. As part of this review, I examined a particular example of the Service's access to a CCTV network (the CCTV network) which has been provided to the Service by the network's operator (the CCTV network provider). These cameras cover most of a New Zealand city centre.[20] The Service has round-the-clock access to the CCTV network, which is accessed from a secure room within the Service's premises.[21]

12. There are a number of practical limitations that, while not all geared towards necessity or proportionality, nonetheless impose significant checks on the Service's access. First, only a limited number of Service personnel can access the CCTV network.[22] Second, the Service only logs in from specific terminals. In addition, the secure room housing the Service's CCTV access has a number of controls aimed to prevent unauthorised entry.

13. More importantly, the Service only uses its CCTV access to support specific operations involving physical surveillance. It does not use the CCTV network as a general surveillance system. This practice imposes a significant restriction on the Service's current use of CCTV. Physical surveillance operations are resource intensive. As Alito J observed in *United States v Jones* (regarding a GPS tracking device) (emphasis added):[23]

> *In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.* Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case – constant monitoring of the location of a vehicle for four weeks – would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one we used in the present case, however, make long-term monitoring relatively easy and cheap.

14. The Service has confirmed to my Office the number of instances it accessed CCTV over the 12 months ending in April 2021. Most access related to targets that were the subject of a warrant authorising visual surveillance. It is noted that CCTV was accessed in fewer than 15 percent of all surveillance deployments within the region over that same period. The CCTV network is primarily used to track and observe a deployed surveillance team and its target. Access to the CCTV network is also used to mitigate health and safety risks. It can assist to forewarn the surveillance team of any threats. Sometimes, the CCTV network will also be used to obtain an understanding of the area prior to deploying the surveillance team.

---

19 New Zealand Bill of Rights Act 1990, ss 14, 16, 17 and 18.
20 "Surveillance Unit – [CCTV network provider] – SOP" (27 April 2018) (CCTV SOP) at [2].
21 I have been informed that there are some cameras on the CCTV network that are not available to the NZSIS.
22 This number may fluctuate depending on staffing and Service resources.
23 *United States v Jones* (2012) 132 S Ct 945 at 963.

15. In some instances, the Service can manoeuvre the cameras.[24] Whether this capability is available depends on the technology of each individual camera being accessed. The policies regarding these particular uses of the CCTV cameras are discussed further below.

APPLICABLE POLICIES

16. The Service should have clear and coherent policies covering the application of key principles in the context of CCTV. The MPS requires these policies and procedures to be consistent with the principles contained in the MPS.

17. The key policies that relate to the Service's use of the CCTV network reviewed by my Office are "Surveillance Unit – [CCTV network provider] – SOP" (the CCTV SOP) and "Surveillance Unit – Surveillance in a Public Place" (the Surveillance SOP).[25] The Surveillance SOP covers warrantless surveillance in a public place generally, whereas the CCTV SOP relates specifically to use of the CCTV network. The Service's "Collection Concepts" policy, which provides high-level principles relevant to all collection, also applies.[26] However, I have focussed primarily on the SOPs, since they translate these high-level principles to the context of public surveillance and CCTV. I have, however, referred to the Collection Concepts policy where relevant.

CCTV SOP

18. The CCTV SOP has a brief legal section. It states that that the cameras are installed in public locations and, in their default state, "afford a view of the public domain whereby there is no expectation of privacy".[27] The CCTV SOP cautions that, where a deployment is undertaken without a warrant authorising visual surveillance, the operator must be "cautious to ensure they are not manipulating a camera view to the point where it may breach a subject's reasonable expectation of privacy".[28] It does not, however, provide any clear guidance as to what a "reasonable expectation of privacy" is — a key concept for any kind of visual surveillance.

19. The CCTV SOP does not engage with the principles of necessity and proportionality.

Surveillance SOP

20. The Surveillance SOP has a more detailed section on the applicable principles. It explains that there are different levels of privacy that a subject in a public place can reasonably expect.[29] It refers to the location and nature of the activity as factors that may be relevant to any expectation of privacy. It also notes that a surveillance officer must assess whether a subject

---

[24] Letter from NZSIS Director-General to Acting Inspector-General of Intelligence and Security (1 November 2019) at [9]; Training Manual.
[25] There is also a Training Manual but this is a handbook covering the mechanics of the system.
[26] "NZSIS Policy – Collections Concepts" (DMS3-2-79).
[27] CCTV SOP at [23].
[28] CCTV SOP at [23].
[29] Surveillance SOP at [4].

has a reasonable expectation of privacy and whether it would be reasonable to breach that expectation.[30]

21. The Surveillance SOP also briefly deals with proportionality, stating that "[s]urveillance in a public place needs to be proportionate, and less intrusive means considered".[31] In this respect, it notes that the surveillance officer should consider the number of people that will be impacted as well as the nature of the impact and intrusion, the length of time surveillance will be conducted, and the environment surveillance will be undertaken in.[32]

Analysis

22. Taken together, the SOPs are a useful starting point with respect to the key principles of proportionality and respect for privacy. However, they could be strengthened by further explanation of these principles. In addition, the SOPs do not, but should, refer to the principle of necessity in the context of public surveillance or CCTV.

23. With respect to privacy, both SOPs give some guidance on privacy, but do not explain what a reasonable expectation of privacy actually is. The Collections Concepts policy does, however, provide such an explanation. It would be useful if the SOPs referred to that policy or otherwise provided guidance on the principle of privacy. More importantly, however, the SOPs' application of privacy to public surveillance is somewhat incomplete. The Surveillance SOP identifies some factors as relevant to assessing expectations of privacy, being the nature and place of the activity. It also provides some helpful examples of how these are relevant. However, these are not the only factors relevant in assessing privacy expectations. For example, the duration of surveillance as well as the use of technology are both factors that are important to this assessment. Either of these are factors that could well be decisive in determination of whether there is a reasonable expectation of privacy.

24. In addition, I note that the CCTV SOP should also be corrected as it suggests that there can be no expectation of privacy when a camera is viewing the public domain. That is incorrect; as discussed above, the concept of a reasonable expectation of privacy requires a more nuanced consideration than whether the location is "public" or "private".

25. The Surveillance SOP has a helpful list of factors to consider in assessing proportionality. However, neither SOP engages with the ultimate assessment, namely whether the scope of the surveillance and the level of intrusiveness is justified in light of the extent to which the surveillance will meet a defined intelligence need.[33] The overarching Collections Concept policy does and it would be useful if the SOPs referred to this or explained the principle of proportionality within the context of surveillance. I also note that the duration of surveillance is not, but should be, mentioned as a factor relevant to proportionality.

26. The use of technology within the context of CCTV, particularly the capabilities available to the Service, should be addressed comprehensively. The courts have been clear that the use of

---

30 Surveillance SOP at [6].
31 Surveillance SOP at [13].
32 Surveillance SOP at [13].
33 MPS at [33].

technology to enhance images may well infringe reasonable expectations of privacy. However, the SOP only addresses this briefly by requiring operators to be careful not to manipulate a camera so that it breaches reasonable expectation of privacy. This brief statement requires further explanation with examples regarding the circumstances in which manipulation would breach reasonable expectations of privacy. The matters the SOP should address include manoeuvring or manipulation of cameras. It would also be useful if the SOPs provided clear guidance as to when a warrant is required. The CCTV SOP does mention warrants that authorise surveillance, but does not provide clear guidance on when a warrant would be required. In this respect, I note that in recommending policy statements for public surveillance, the Law Commission recommended they include guidance on "[w]hen a specific warrant or order should be sought".[34]

27. The policies should also provide guidance on when footage may be copied or retained. While the Service has not yet collected any of the actual footage, it has the potential to do so. Any retention and subsequent use will likely be relevant to proportionality and privacy concerns. In this respect, I note that the Law Commission recommended policy statements on public surveillance should include guidance on the use, storage and destruction of information obtained.[35]

28. **Recommendation 1:** I recommend that the Service strengthens its policies relating to CCTV by including reference to the principle of necessity (see [22]), amending the CCTV SOP's explanation regarding privacy (see [24]) and strengthening its guidance on the principles of respect for privacy and proportionality, eg, what can comprise a reasonable expectation of privacy (see [23], [25]). In addition, the SOPs should cover the use of technology, the circumstances in which a warrant is required and guidance on when footage can be retained.

RECORD-KEEPING

29. The MPS requires the NZSIS to 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".[36] The Public Service "Information and Records Management Standard" also acknowledges the importance of sound record-keeping to accountability and to good management more generally.[37] More specifically, the Privacy Commissioner's guidance on CCTV states that agencies should regularly check that CCTV operators are following the relevant policies including by checking "the audit trails that record which staff have accessed footage and the way cameras are used by staff".[38]

---

34 Law Commission, above n 4, at [11.71].

35 Law Commission, above n 4, at [11.71].

36 MPS at [40].

37 Archives New Zealand "Information and Records Management Standard" (July 2016) at 1: "Information and records are key strategic assets at the core of public sector business and government accountability. They help organisations plan for and achieve valuable and relevant short-term and long-term outcomes that benefit business, government and the wider community."

38 Privacy Commissioner "Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations" (2009) at 24.

30. As noted, the Service is only accessing the CCTV network to support physical surveillance operations. The Service keeps a number of records in relation to physical surveillance operations. Before an operation, it prepares a plan that may, but will not necessarily, refer to the use of the CCTV network. This document is primarily concerned with operational details and so does not explicitly deal with necessity, proportionality, privacy and the other principles underpinning surveillance. Following the deployment, staff record the physical surveillance in a separate document. Sometimes this includes details of CCTV usage.

31. The primary record of the Service's access to the CCTV network is contained in two documents; the "Post Deployment Log" and the "CCTV Access Log". The "CCTV Access Log" records the date of the access to the CCTV network, the person who conducted the access and the time the Service logged on and off the CCTV Network.[39] The "Post Deployment Log" references the particular operation involved, the target, the general location of the surveillance and also whether CCTV was accessed. During the course of my review, I raised questions about the extent of the information contained in this log. As a result, the Service now records further details regarding the ways in which it has operated a camera.

32. We acknowledge that there are some practical limitations regarding the extent of the records that the Service may keep. The person accessing the CCTV network is often dealing with a dynamic situation involving numerous tasks and significant time pressure. Nonetheless, I consider it may be possible to add further details regarding CCTV usage and manipulation (where that manipulation increases the privacy intrusion involved), without record-keeping becoming overly burdensome. These details, which would better enable oversight of respect for privacy, necessity and proportionality, include: whether the cameras were manoeuvred, whether the footage was retained in any way and the justification for other specific actions taken in relation to the operation of the cameras. I understand that these additional records will not be overly onerous.

33. I also recommend that the Service explicitly record its consideration of the necessity and proportionality of physical surveillance operations, including the use of CCTV. The Service advises that these principles are considered by a Collection Hub meeting prior to any operation, and also by the Planner when he or she puts together a document regarding the operation. For oversight and accountability purposes, it would be useful if consideration of these principles were clearly documented.

34. Adding these additional details to the Service's CCTV records will facilitate and support my oversight function. It will strengthen decision-making by requiring consideration of the core principles that govern surveillance in a public place and a record of that process. It will also promote accountability and enable the Service to regularly check that its policies are being adhered to, as contemplated by the MPS and the Privacy Commissioner's guidance on CCTV.

35. **Recommendation 2:** I recommend that the Service implement appropriate policies and practices to strengthen its record keeping in relation to the use of CCTV footage. The additional details that should be recorded include: whether cameras were manipulated[40],

---

[39] CCTV Access Log (2019).

[40] Where that manipulation increases the privacy intrusion involved.

whether the footage was retained and the justification for other specific actions taken in relation to the operation of the cameras. I also recommend the Service explicitly record its consideration of the necessity and proportionality of the physical surveillance operation involving CCTV.

BASIS FOR ACCESS TO CCTV NETWORK

Service's basis for access

36. I have explored the legal basis for the Service's access to CCTV, from when it first began accessing the network in March 2017, to present. My full analysis of the legal position of the Service's use of CCTV, provided to the Service, raised some difficult and unresolved questions as to the legal basis for the Service's initial and ongoing access to the CCTV network provider's feeds. Given the questions I have raised I consider it is important that the Service ensures the lawful basis for its access to CCTV. This is best achieved by obtaining advice from the Solicitor-General on the issue.

37. Following engagement with my Office and the Privacy Commissioner the Service also accepts that the MOU placed too much emphasis on public safety as the purpose of NZSIS's access. The Service is now reviewing and revising the MOU.

38. **Recommendation 3:** I recommend that the Service review and revise the legal basis for accessing CCTV footage with the benefit of advice from the Crown Law Office.

39. **Recommendation 4:** The Privacy Commissioner and I both consider that the Privacy Impact Assessment (PIA) that was required by the MOU should have been completed before operationalisation of the arrangements. Following correspondence with the Privacy Commissioner and my office, I am pleased to note that the Service has now finalised the PIA.

A NOTE ON CLASSIFICATION

40. The Service's use of CCTV was, until relatively recently, a classified capability. For this reason there was limited access to, and knowledge of, the MOU. Under the terms of the MOU, the CCTV provider was not permitted to keep a copy of the MOU because of its classification.[41] Knowledge of the MOU was also very limited within the CCTV provider's organisation: only three people knew of its existence. One was the Chief Executive (CE), who signed the MOU on behalf of the organisation. According to the MOU, the CE was aware of the arrangements but not the details of the Service's CCTV access.[42] The classification of the MOU may have been a barrier to the CE obtaining legal advice and advising their board of the arrangement.

41. I am pleased that the Service now acknowledges that the use of CCTV as an operational tool should not be classified. The use of CCTV is commonplace among law enforcement agencies and it is an obvious and important tool for intelligence agencies. By declassifying the use of CCTV, problems such as those identified in paragraph 40 above can be avoided. It also enables me to publish a meaningful public report. The consequent transparency can only

---

41 MOU at [31].

42 Schedule 4 to the MOU.

benefit public debate on the use of such surveillance. In this case the public can also be assured that the Service is using what could be a highly invasive technology in a limited and proper manner.

FINDINGS AND RECOMMENDATIONS

42. My review has established that the Service uses CCTV in a targeted and specific way rather than as a mechanism for general surveillance. It only uses CCTV in support of physical surveillance operations. The Service does not currently retain or record any of the footage. There are also practical constraints on the use of CCTV, including the number of people who have access to the network and the number of terminals available. Overall I am satisfied that the Service's current use of CCTV is lawful and is conducted in a responsible and proper manner.

43. I have also considered the policies and practices that underpin the Service's use of the CCTV network. While the SOPs and record-keeping arrangements provide a reasonable starting point, I recommend that they be revised and strengthened.

44. **Recommendation 1:** I recommend that the Service strengthens its policies relating to CCTV by including reference to the principle of necessity (see [22]), amending the CCTV SOP's explanation regarding privacy (see [24]) and strengthening its guidance on the principles of respect for privacy and proportionality, eg, what can comprise a reasonable expectation of privacy (see [23], [25]). In addition, the SOPs should cover the use of technology, the circumstances in which a warrant is required and guidance on when footage can be retained.

45. **Recommendation 2:** I recommend that the Service implement appropriate policies and practices to strengthen its record keeping in relation to the use of CCTV footage. The additional details that should be recorded include: whether cameras were manipulated[43], whether the footage was retained and the justification for other specific actions taken in relation to the operation of the cameras. I also recommend the Service explicitly record its consideration of the necessity and proportionality of the physical surveillance operation involving CCTV.

46. **Recommendation 3:** I recommend that the Service review and revise the legal basis for accessing CCTV footage with the benefit of advice from the Crown Law Office.

47. **Recommendation 4:** The Privacy Commissioner and I both consider that the Privacy Impact Assessment (PIA) that was required by the MOU should have been completed before operationalisation of the arrangements. Following correspondence with the Privacy Commissioner and my office, I am pleased to note that the Service has now finalised the PIA.

48. Finally, this report is a baseline review that covers only the current use of CCTV. Should the Service consider new technology or enhancements, both the Privacy Commissioner and I would expect a fresh PIA to be undertaken. And, as is the case with all Privacy Impact Assessments, the Privacy Commissioner remains available for consultation.

---

[43] Where that manipulation increases the privacy intrusion involved.

LIST OF ABBREVIATIONS

CCTV – Closed Circuit Television

ISA – Intelligence and Security Act 2017

MOU – Memorandum of Understanding

MPS – Ministerial Policy Statement

NZSIS – New Zealand Security Intelligence Service

PIA – Privacy Impact Assessment

Service – New Zealand Security Intelligence Service

SOP – Standard Operating Procedure