Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy Commissioner's submission to the Justice Committee on the Policing Amendment Bill (268-1)

Contents

1. I am pleased to provide a submission to the Justice Committee (**the Committee**) on the Policing Amendment Bill (**the Bill**).
2. One of the Privacy Commissioner's functions under the Privacy Act is to examine proposed legislation that may affect the privacy of individuals.
3. The Bill would amend the Policing Act 2008 (**the Act**) to:
    - authorise the collection of information by the New Zealand Police (**Police**) for specified purposes, including intelligence purposes (Part 1)
    - expand Police's temporary road closure powers under the Act (Part 2).
4. This submission is concerned with Part 1, and I have no comments on Part 2.

Overview

5. I do not support Part 1 of the Bill and recommend that it not be passed. I consider it would create significant risks for the privacy and rights of New Zealanders. If it does proceed, I recommend that it be amended to provide for safeguards.
6. The authorisation for Police collection of information provided by Part 1 is too broad and has not been adequately justified. It will not provide the certainty sought by Police and therefore will not achieve Police's objectives. It also risks harming trust and confidence in Police.
7. My main concerns are that Part 1 of the Bill:
    - provides Police with a very broad authorisation to collect information, including for an undefined 'intelligence purpose', which could lead to excessive collection and retention of personal information
    - partially displaces the application of key principles in the Privacy Act and therefore affects my ability to provide oversight of Police information-gathering
    - includes no meaningful safeguards.
8. A 2022 report by the Office of the Privacy Commissioner (**OPC**) and the Independent Police Conduct Authority (**IPCA**) into Police photographing of members of the public (**the Joint Report**) demonstrated the importance of a robust legal framework to prevent indiscriminate information collection.[1]
9. Police's objective is to increase certainty and remove risks that information collection will be found to be unlawful. However, I consider that the arguments for the Bill overstate the current constraints on policing activity. I am not persuaded that current

[1] *Joint Inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police Conduct when Photographing Members of the Public*, September 2022 (hereafter *Joint Inquiry*).

legal settings prevent Police from effectively performing its functions. While the Bill may minimise the risk that the Privacy Commissioner finds Police information gathering unlawful in future, this is because it provides an overly broad information-gathering power which will displace key parts of the Privacy Act. I do not consider the Bill provides greater clarity than the status quo or reduces the risk of Police information collection being challenged in court.

10. I believe the potential adverse impacts of the Bill have not been adequately assessed. The Bill is likely to disproportionately affect Māori and to harm the privacy interests of children and young people. It is also likely to significantly infringe on the right to privacy of all New Zealanders, by giving Police a broad power to collect personal information without any meaningful constraints on retention, use and disclosure of that information

11. The Bill also includes no safeguards. If it proceeds, it should be amended to provide for safeguards in either primary or secondary legislation. Those safeguards should be subject to oversight by the Privacy Commissioner, IPCA or the new Inspector-General of Police (**IGP**).

12. I also think there is a case for a specific statutory framework for Police intelligence-gathering, particularly given the technologies for collecting and analysing information that are now available to Police. Such a framework would give Police certainty about its powers to collect information for intelligence, while also providing for safeguards. That framework is not in this Bill. Developing such a framework would take time and require consultation.

13. I provide a summary of all recommendations made on this Bill at Appendix 1.

What Part 1 of the Bill does

14. The objectives of Part 1 are said to be:[2]

- to 'reaffirm' Police's ability to record images and sounds in public places and private places where Police is lawfully allowed to be, and to collect personal information for lawful purposes, including intelligence
- to provide certainty and clarity for Police officers about their lawful authority to collect information, in the wake of uncertainty said to have been created by the Joint Report and the Supreme Court's decision in *Tamiefuna v R* (***Tamiefuna***).[3]

15. In this part of my submission, I discuss each new section introduced by Part 1 and raise some specific concerns about these sections. Wider issues about the impacts of these sections are discussed later in the submission.

[2] See the General Policy Statement for the Bill and the first reading speech by the Minister of Police.
[3] *Tamiefuna v R* [2025] NZSC 40 (hereafter *Tamiefuna*).

16. Part 1 of the Bill consists of clause 4, which amends the Act to insert new sections 45A to 45E.[4] These new sections would appear in Part 3 of the Act ('Powers, operations, and offences'), in a series of provisions headed 'Operational provisions'. That part of the Act deals with routine operational policing matters such as court processes and dog handlers. By contrast, the new sections authorise Police to undertake certain activities that will regularly affect members of the public. Their inclusion under 'Operational provisions' is arguably misleading. While the new powers have operational implications, they should not be viewed in narrow operational terms.

17. Sections 45A to 45D authorise actions by Police employees, not Police constables. A Police employee is anyone appointed under section 18 of the Act for the exercise and performance of Police's powers, functions and duties, and can include persons seconded to Police. A Police constable is a Police employee appointed to the position of constable after taking the constable's oath, and must be adequately trained to exercise a constable's powers and capable of exercising those powers. Some sections of the Act apply generally to Police employees, but a number of powers under the Act can be exercised only by constables.

18. It is unclear why the authorisations in sections 45A to 45D have not been limited to Police constables. I encourage the Committee to request advice on the rationale for these powers applying to all employees rather than constables.

Section 45A: purposes for which Police may collect information

19. Section 45A provides that Police may collect information for one or more broadly-expressed purposes. The purposes relate to the safety of Police employees, the integrity of policing, intelligence purposes 'connected with a function, or an activity, of the Police', and other lawful purposes connected with Police functions or activities. The section applies generally to 'information', not only to personal information.

20. As discussed further below, in Privacy Act terms section 45A provides for purposes for which Police may lawfully collect personal information and authorises Police to collect information for those purposes ('Police may collect…'). While some specific purposes are referred to, section 45A(d) is a catch-all 'any other lawful purposes' provision, providing that those purposes are connected with Police functions or activities. Police functions are set out in a non-exclusive list in section 9 of the Act, but Police activities are not statutorily defined.

21. Here and in section 45D 'intelligence' or 'intelligence purpose' are not defined, nor are they defined elsewhere in the Act. Given that Police has stated that the intelligence value of information may not be known at the time of collection, this

[4] Section 45E provides that nothing in sections 45A to 45D limits or affects Police's intelligence-gathering function at common law, or the ability of Police or any other agency to collect information under other legislation or the common law.

provides Police with a very broad authorisation to collect information. I **recommend** that 'intelligence' or 'intelligence purpose' should be defined in the Bill.

Section 45B: recording by Police employee: public places

22. Section 45B provides that a Police employee may, for one or more of the purposes in section 45A, record 'by any means':

    - 'visual images of any person or thing that is in, or that can be observed from, a public place' (s 45B(a))
    - 'any sound that is emitted from, or that can be heard in, a public place' (s 45B(b)).

23. This section is overly permissive. In particular:

    - The section would authorise targeted (i.e., more than incidental) recording of images or sounds on private property, so long as the Police employee is recording from a public place, such as the roadside.[5]
    - Recording 'by any means' does not exclude technologically-enhanced collection, such as the use of devices that allow things to be seen or heard that could not be seen or heard using ordinary human vision and hearing. For example, it appears that a powerful microphone could be used to record the conversation of two individuals sitting at a park bench who would not expect to be overheard. I **recommend** that section 45B is amended to provide that recording 'by any means' does not include technologically-enhanced collection, such as the use of devices that enhance ordinary human vision or hearing.
    - 'Public place' is not defined in the Bill. It is defined in the Summary Offences Act 1981, and the Search and Surveillance Act 2012 refers to 'non-private premises'. I expect those definitions to apply in the absence of a definition in this context, Parliament may wish to define it in this context to make very clear what the scope of the power is.

Section 45C: recording by Police employee: private property

24. Section 45C provides that a Police employee who is lawfully on private property may, for one or more of the purposes in section 45A, record 'by any means' anything they can see or hear there, and that they do not need a surveillance device to see or hear.

[5] I note that section 46(1) of the Search and Surveillance Act 2012 requires a surveillance warrant to be obtained for the use of a visual surveillance device to observe or record private activity in private premises, or to intercept private communications.

In contrast to section 45B, this section rules out the recording of information that can only be observed with the use of a surveillance device.

25. Private property is one of the zones of privacy that is protected against intrusion by officers of the State, unless for justifiable reasons. Because section 45C is concerned with private property, there is a heightened privacy expectation of property owners, their family and invited guests or persons lawfully present.

26. This section would authorise Police officers who are on private property executing a search warrant to record information that is not related to the purpose of the warrant. Similarly, it would allow Police officers who are exercising warrantless powers associated with drugs or firearms, or who are lawfully on property for another purpose (such as a family violence call-out) to record unrelated intelligence while on private premises. This information might relate to individuals whose presence has nothing to do with the purpose of the Police's entry to the property. Given the potentially broad scope of 'intelligence purpose', it could also be information that does not relate to any current or likely investigation.

27. Police officers are empowered to enter private places under the Search and Surveillance Act for defined and specific purposes. My first concern is that this section could allow Police to avoid the constraints imposed by access under warrant, such as particularity requirements (warrants must describe in detail the place to be searched or the things to be seized, to put bounds on the exercise of the power and prevent general searches).

28. Second, I am concerned that section 45C does not expressly connect the authorisation of recording with the reason for the Police presence on private property. More specific safeguards would be needed to protect the interests of individuals who may be lawfully present for purposes unconnected with the purpose of Police entry onto private property. There are no stated protections for children and young people who may be present at the time.

29. Third, I am concerned that the unintended consequences have not been fully considered. For example, some people may be deterred from contacting Police when they have been victims of crime (including family violence), because a Police call-out could result in Police recording images for an unrelated purpose.

30. For these reasons, I **recommend** section 45C should be deleted, and any potential changes to Police powers to record when lawfully on private property should be considered as part of policy work on the Search and Surveillance Act.

31. Similar to my comment above about 'public place' not being defined, 'private property' is not defined in the Bill. The Search and Surveillance Act uses and defines 'private premises' and I expect that definition will be relevant. I also suggest the Committee consider whether a definition would provide a clearer statement about the scope of this power.

Section 45D: restrictions on Police employee collecting information for intelligence purpose

32. Section 45D is expressed as placing restrictions on Police's ability to collect information for intelligence purposes. Unfortunately, these restrictions are inadequate.

33. Section 45D(a) provides that, despite anything in sections 45A to 45C, a Police employee 'must not collect information for an intelligence purpose unless they consider that the information will or may support the Police in performing a function, or carrying out an activity, of the Police'.

34. Given that 'intelligence purpose' is not defined, it is hard to see how section 45D(a) significantly constrains Police. It appears that, under this provision, information may be collected simply because it 'may', in some unspecified way, support the Police in carrying out its functions and activities. As an indication of the potential breadth of this authorisation, the Regulatory Impact Statement (**RIS**) for the Bill refers to collection for general intelligence purposes in terms of collection for 'an **unknown or unspecified** future policing purpose', and 'a known or **unknown** future lawful use' (emphasis added).[6] As discussed further below, the ability to collect for an unknown future use has significant privacy implications.

35. Section 45D(b) provides that a Police employee may make a continuous sound or video recording solely for an intelligence purpose only if section 45D(a) does not prevent the making of the recording, and if the making of the recording solely for the intelligence purpose is reasonable and the recording's duration is reasonable in the circumstances.

36. I understand that section 45D(b) is intended to allow Police to take short, targeted video clips for intelligence purposes, but not to use the authorisation provided by the Bill to engage in ongoing, continuous surveillance. However, the effect of this section is that Police *can* record continuously solely for intelligence purposes, subject only to a general reasonableness test. This is a particular concern, given the growing capacity of digital technologies to collect and analyse data. As the reasonableness limits are likely to be tested in the courts, in my view, Police will need to consider not only the reasonableness of continuous recordings for intelligence purposes, but also the necessity, justification and proportionality of such recordings, and the relative intensity of the privacy intrusion. These principles should be reflected in the Bill.

[6] 'Regulatory Impact Statement: Amendments to the Policing Act 2008' (hereafter 'RIS'), 11 September 2025, p 13.

Part 1 of the Bill will partially displace the Privacy Act

37. The Information Privacy Principles (**IPPs**) are the Privacy Act's key framework for the handling of personal information. Policy documents for the Bill state that it is not intended to displace any of the IPPs or confine the Privacy Commissioner's jurisdiction.[7] Despite this stated policy intent, the statutory authorisation in part 1 of the Bill will displace the privacy principles to the extent that it is more permissive than the IPPs.[8] This displacement will also significantly limit the Privacy Commissioner's ability to accept complaints or take compliance action in relation to Police's collection of personal information if there are instances of over-collection or indiscriminate intelligence gathering.

Information privacy principle 1

38. IPP 1 states that personal information must not be collected unless the information is collected for a lawful purpose connected with an organisation's function or activity, and the collection of the information is necessary for that purpose. 'Necessary' in IPP 1 does not mean strictly or absolutely necessary, but it does mean more than merely desirable, expedient, reasonable or convenient.[9] A key purpose of IPP 1 is to protect individuals against indiscriminate collection of their information and the collection of information that agencies have no good reason to hold or to use.

39. Section 24 of the Privacy Act governs the interaction between other legislative provisions and the Privacy Act and means that IPP 1 defers to another statutory provision authorising the collection of personal information. Section 45A is expressed as permitting the collection of information if **supporting or connected with** a Police function or activity. This is a lower threshold for collection than the necessity test under the Privacy Act in IPP 1. I believe the same point applies to recording authorised under sections 45B and 45C.

40. For intelligence-gathering, section 45D introduces a test that an officer collecting information for an intelligence purpose must consider that the information 'will or may support the Police' in performing a Police function or activity. This test does require Police officers to turn their minds to the way in which particular information collected for intelligence may support Police functions or activities. However, it is still a very broad and subjective test, particularly as 'intelligence purpose' is not defined. It does not require Police to consider whether the collection is objectively 'necessary' for the particular purpose, only that it would support a function.

---

[7] 'Policing Amendment Bill: Approval for Introduction', paper for the Cabinet Legislation Committee, 2026, pp 5, 10.
[8] Privacy Act 2020, s 24(2).
[9] *Tan v New Zealand Police* [2016] NZHRRT 32, at [77]. See also the discussion in Privacy Commissioner, *Inquiry into Foodstuffs North Island trial use of facial recognition technology*, 2025, pp 37-38.

41. It is hard to reconcile the stated intent that the Bill is not intended to displace any of the IPPs or the Privacy Commissioner's oversight with the lower threshold used in the Bill. The LEG paper states that the Bill seeks to 'overcome the narrow approach to IPP1', which suggests that it is intended to shape how IPP 1 is interpreted, rather than displacing it.[10] However, this is not how section 24 of the Privacy Act works. To the extent that Police collection of personal information is authorised under the new sections of the Act, IPP 1 will simply not apply. I note this may also have flow-on implications for the application of the Biometric Processing Privacy Code to Police's activities. This Code was recently issued to govern the use of biometric technologies.[11] There may be a small residual jurisdiction for the Privacy Commissioner, for cases in which Police has collected information outside the statutory authorisation, but such cases are likely to be rare.

Other information privacy principles

42. It is true that some IPPs will not be affected by the Bill. For example, Police will still need to comply with the requirements in IPP 5 to hold personal information securely. IPPs 6 and 7 will require Police to uphold the individual's rights of access to and correction of personal information, on request. However, the displacement of IPP 1 by the broad authorisation provided by the Bill will also affect some other IPPs.

43. IPP 9 provides that an agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used. This is a crucial protection against agencies holding on to information 'just in case', or neglecting to delete information that may be irrelevant or out of date. Like the limits on collection in IPP 1, it is also an important security protection, since it limits the amount of information that can be lost, stolen or compromised in a privacy breach.

44. Because the Bill would authorise collection of personal information for broad intelligence purposes, it will be hard to make a meaningful assessment of when Police no longer has a lawful purpose for using the information. Throughout the policy papers for the Bill, Police has emphasised its wish to be able to collect information whose use may not be known at the time of collection. Police considers that the intelligence value of information can often only be determined in hindsight.[12] If that is so, it is hard to see how IPP 9 could act as a meaningful constraint on Police

[10] Policing Amendment Bill: Approval for Introduction', paper for the Cabinet Legislation Committee, 2026, p 10.
[11] Biometric Processing Privacy Code 2025. Under the Privacy Act, the Privacy Commissioner can issue codes of practice that affect how the IPPs apply to particular types of information, activities or sectors.
[12] 'Policing Amendment Bill: Approval for Introduction', paper for the Cabinet Legislation Committee, 2026, p 10.

retention of information, if information collected for intelligence *may* still be used for any lawful purpose in future.

45. IPPs 10 and 11 provide that personal information collected for one purpose cannot be used (IPP 10) or disclosed (IPP 11) for another purpose, unless an exception applies. Given the broad purposes of collection that would be authorised by the Bill, these IPPs are unlikely to act as a meaningful control on Police's use and disclosure of personal information collected for policing purposes.

Conclusion about impacts on the Privacy Act

46. My view, then, is that the Bill would effectively displace or undermine key protections in the Privacy Act. My jurisdiction under the Privacy Act is focused on investigating complaints or taking compliance action in relation to breaches of the IPPs. My jurisdiction and oversight will therefore be reduced to the extent that the IPPs are displaced or are less effective in regulating the collection of personal information as a result of the Bill.

47. I **recommend** that, if that Bill proceeds, it be amended to ensure that the effect of the IPPs is maintained by reflecting an objective threshold for the collection of personal information, with clear limits on secondary use and retention of that information. Any breach of these limits should clearly engage the complaint mechanism in the Privacy Act and the Privacy Act's compliance framework to address systemic issues.

Part 1 lacks safeguards

48. I am concerned that Part 1 of the Bill includes no meaningful safeguards to protect privacy and other rights. I have already noted that the Bill will affect my ability to provide oversight under the Privacy Act. It is therefore even more important that, if the Bill proceeds, it be amended to include safeguards.

Safeguards that should be included in the Bill

49. I **recommend** that, if the Bill proceeds, the following safeguards should be provided for:

    - appropriate thresholds and safeguards for the exercise of Police's powers to collect personal information, incorporating an assessment of the necessity and proportionality of collection and proposed use
    - requirements for the purpose for which personal information is collected to be recorded, to facilitate auditability and assurance reporting and downstream use of the information

- requirements for regular auditing of and public reporting on the exercise of information-gathering powers, including analysis of differential impacts on Māori and other communities
- requirements for Police policies on the exercise of the powers in the Bill to be published
- standards on storage, retention, destruction and secondary use of personal information obtained by Police, including requirements for regular reviews to assess whether information should be deleted
- protections for the collection of information on vulnerable populations, particularly children and young people
- oversight of Police compliance with the safeguards by an independent body, with the ability to receive complaints and undertake proactive investigations.

50. My preference is for safeguards to be provided for in the Act itself. This would require allowing further time for the passage of the Bill, so that officials can develop appropriate safeguards. I recommend that advice should be sought from the Legislation Design and Advisory Committee (**LDAC**). The amended Bill should then be returned to the Justice Committee so that members of the public can have their say on the adequacy of the safeguards. Providing for safeguards in primary legislation would provide the greatest transparency and certainty for the public.

51. Alternatively, if the Government does not support the inclusion of safeguards in the Act, the Bill should be amended to provide for the making of regulations setting out safeguards. In that case:

- The Bill should require such regulations to be made, rather than giving the Minister discretion to decide whether to make regulations or not.
- The regulation-making power should set out matters that must be addressed in the regulations.
- The Bill should require that the regulations be subject to public consultation, and to consultation with the Privacy Commissioner and other relevant oversight bodies.
- Part 1 of the Bill should not commence until the regulations have been made.

52. Providing for safeguards in primary or secondary legislation would support public trust and confidence in Police use of their powers and provide additional clarity for frontline Police officers in the exercise of their duties.

53. Regardless of whether safeguards are provided for in the Act or in regulations, the exercise of Police powers and Police compliance with safeguards should be subject to independent oversight. This oversight could come from any combination of OPC,

the IPCA or IGP, or another body. Without such oversight, the public cannot have the assurance it deserves that Police is complying with the law and human rights.

Operational policies alone are insufficient

54. In the absence of any safeguards in the Bill, Police has stated that it will maintain safeguards through internal Police policies, and 'strengthened internal governance and assurance processes'. The Cabinet policy paper states that:[13]

> Police guidelines and policies will ensure that when material is collected it is aligned to policing purposes, functions, and activities, and that material is retained only when it is of value to those purposes and functions.

55. The RIS considers and rejects the option of prescribing safeguards in primary or secondary legislation. The RIS argues that legislative requirements could be overly prescriptive, have an unintended constraining effect, be time consuming to amend, reduce Police's ability to respond flexibly to developments, be overly complex and impractical, and have disproportionate compliance costs.[14]

56. I believe some of Police's objections to prescribing safeguards in legislation can be addressed through careful and balanced design of the safeguards. It should also be possible to strike an appropriate balance between prescription and flexibility, with high-level safeguards in legislation and more detail in internal policies. Police has not made a convincing case that the Bill should include no safeguards at all.

57. I believe safeguards must be in legislation rather than internal policies for the following reasons:

- Legislation has a democratic mandate and is subject to debate and public input. It allows Parliament to express its expectations about how the exercise of the power is to be managed by Police.
- Legislative safeguards provide greater certainty, assurance and transparency. The public can know the key requirements Police needs to comply with, and that these will not be changed without a democratic process.
- The public has no assurance that Police will develop internal policies, or that Police will give priority to doing so. Neither can the public be certain that robust internal policies will be retained by successive Police executives.
- Compliance with legislative safeguards is a legal requirement, and is subject to independent oversight by regulators and the courts. Police policies can be enforced only through internal processes such as disciplinary proceedings for breaches of the Police code of conduct.

[13] 'Amendments to the Policing Act', paper for Cabinet, 2025, p 5. Also RIS, pp 20, 34-35.
[14] RIS, pp 27-28.

58. For these reasons, I believe that legislative safeguards will support public trust and confidence in Police, while internal controls will not. Internal policies and procedures do, however, have an important role to play in expanding on and supporting legislative safeguards.

Impacts of Part 1 on the public

Impacts on Māori

59. Under section 21(c) of the Privacy Act, I am required to take into account cultural perspectives on privacy. It is with that in mind that I make the following comments.

60. The Joint Report was prompted by concerns about Police photography of rangatahi Māori. Evidence discussed in the Joint Report indicated that over half of intelligence photographs retained by Police relate to Māori.[15] This apparent over-representation of Māori is consistent with the well-recognised over-representation of Māori in the criminal justice system generally.[16]

61. Police's analysis of the impacts of this Bill on Māori and of the Bill's consistency with te Tiriti o Waitangi is completely inadequate. The RIS comments that Police will consider and give effect to its obligations to Māori and the Treaty, including consideration of ways of mitigating any disproportionate impacts on Māori and of data sovereignty issues, as part of the implementation of the legislative amendments. The RIS acknowledges that there has been only limited consideration of the proposals through a Tiriti lens, and that there has not been engagement with Māori 'despite data showing that Māori could be an impacted population'.[17]

62. This failure to consult with Māori, undertake proper Tiriti analysis or consider impacts on Māori prior to the introduction of legislation that is likely to have significant impacts on Māori is unacceptable. The Crown must ensure that legislation does not disproportionately harm Māori, and that the Crown actively works to achieve equitable outcomes. It is not enough to consider mitigations of impacts on Māori at the implementation stage: the Crown has a responsibility to consider how those impacts can be avoided well before new legislation is implemented. Failing to engage with Māori and undertake this analysis may have negative implications for the trust that Māori, and in particular rangatahi Māori, have in Police.

63. In the absence of the views of Maori due to the lack of consultation, I urge the Committee to seek independent advice on the potential impacts of the Bill on Māori and to listen carefully to submissions from Māori individuals and groups, including tikanga experts. In my submission, I will focus on two points about impacts on Māori.

---

[15] *Joint Inquiry*, pp 30-31.
[16] For example, Ministry of Justice, *Reducing the disproportionality of Māori in the criminal justice system: wāhine Māori*, Sector Insights, 24 February 2026.
[17] RIS, pp 36-37.

64. First, photographs of individuals, and particularly of their faces, have particular significance in te ao Māori. In OPC's consultations with Māori about regulation of biometric processing, we heard that, from a Māori perspective, biometric information such as facial images is related to whakapapa and carries the mauri of the individual it was taken from.[18] As such, it is tapu to the individual, and their whānau, hapū and iwi. Collection, storage and use of images of moko (traditional tattooing) raise particular concerns.

65. Speaking extrajudicially, Justice Christian Whata (Ngāti Pikiao and Ngāti Tamateatūtahi - Kawiti of Te Arawa) has usefully described how a tikanga Māori framework could apply to the facts of *Tamiefuna*:[19]

> **Mr Tamiefuna was not obviously in a vulnerable tapu** state or domain (whether public or private) when the photograph was taken. Put in tikanga terms, he was in a state of **noa**, and able to interact with others safely. … But, captured in that photo is Mr Tamiefuna's whakapapa – a matter, within te Ao Māori, of deep intergenerational importance, and the control of the use of his whakapapa is an aspect of both personal mana and mauri, and that of his whānau. It is that core part of him, handed down from generation to generation, **that is inherently tapu**. In this context, the tapu of his whakapapa mirrors privacy's right to retain control over that which defines us from state intrusion.
>
> The **critical issue** then is whether the taking and then use of the photo amounts to an improper intrusion or perhaps more accurately is justified. This brings into frame … the purpose or kaupapa to which the information is to be put. Put another way, the proposed kaupapa may **elevate or moderate** the force and application of the tapu.

66. Interpretation of tikanga Māori is a matter for Māori themselves, and Māori could have outlined tikanga considerations to Police if a full public consultation had taken place. However, I suggest a few points flow from Justice Whata's perspective.

    - In terms of tikanga Māori, taking a photograph or video of a person, particularly one that features the person's face, requires careful consideration of what controls are appropriate for the taking of the image and its subsequent storage and use.

---

[18] Māori report higher levels of concern about facial recognition technology than non-Māori. In the most recent annual public opinion survey conducted by OPC, 52% of Māori expressed concern about law enforcement use of FRT in public places, compared to 41% of all respondents: Office of the Privacy Commissioner, *Research on Privacy Concerns and Use of Personal Information*, March 2025, p 7.

[19] Justice Christian Whata, 'The tapu of privacy: privacy through a tikanga lens', Sir Bruce Slane Memorial Lecture, 25 February 2026, paras 67-68. Emphasis in the original. Justice Whata describes tapu as speaking to 'the inherent worth, alongside mana and mauri, of all aspects of creation, with corresponding restrictions to protect that worth', while noa 'denotes freedom from restriction and the power to remove restriction, including tapu' (para 40).

- As the Supreme Court found in *Tamiefuna*, the use to which an image is to be put is also of critical importance. If the image is to be held by Police for potential use in a future criminal investigation, this is likely to elevate the force and application of the tapu of that image.
- Tikanga, like public law, has protective principles that mitigate risks to affected people and would inform how a more protective statutory framework for Police information collection could be designed.
- Where personal information is an expression of key Māori concepts such as whakapapa, Māori rights under Article 2 of te Tiriti o Waitangi to exercise tino rangatiratanga with respect to their taonga are likely to be engaged.[20]

67. Second, the Bill will make it easier for Police to build up a database of photographs in which Māori are likely to be over-represented. This is likely to have compounding effects on Māori over-representation in the criminal justice system.

68. The Law Commission examined an issue which closely parallels this one when it reviewed the law relating to the use of DNA in criminal investigations. In its issues paper for that review, the Law Commission reported that domestic and international literature recognises 'the potential of known person databanks to exacerbate any pre-existing societal issues of racial disparity.'[21] In its final report for the review, the Law Commission commented that:[22]

> Māori comprise around 16.5 per cent of the general population but since 2009 Māori have provided between 38 and 41 per cent of all DNA samples obtained on arrest or intention to charge. The Crown has an obligation under the Treaty to reduce inequalities between Māori and non-Māori. There are, however, no measures in the [Criminal Investigations (Bodily Samples)] Act to support this obligation, such as independent oversight or reporting requirements.

The Commission recommended that the Crown take active steps to reduce inequities and promote equity in the DNA regime, including through independent oversight with Māori representation.

69. Similar points can be made with respect to Police collection of images of individuals and their storage in a database in which Māori are likely to be over-represented. If anything, the point is stronger with regard to photography, as the DNA regime relates to people who have been arrested. By contrast, this Bill would authorise photography that will allow Police to build up a database of individuals who may never be charged with a criminal offence. To paraphrase the words of the Law Commission, and apply

---

[20] Data as a taonga is discussed in T Kukutai, K Campbell-Kamariera, A Mead, K Mikaere, C Moses, J Whitehead and D Cormack, *Māori data governance model*, Te Kāhui Raraunga, 2023, pp 13-14.
[21] Law Commission, *The Use of DNA in Criminal Investigations | Te Whakamahi i te Ira Tangata i ngā Mātai Taihara*, Issues Paper 43, 2018, pp 248-249.
[22] Law Commission, *The Use of DNA in Criminal Investigations | Te Whakamahi i te Ira Tangata i ngā Mātai Taihara*, Report 144, 2020, p 10.

them to Police photography: if, all else being equal, a Māori individual is more likely to be photographed by Police than a non-Māori individual, the databank will amplify this bias. That is because the person whose photograph is on the databank is automatically more likely to come to the attention of Police again in the future. Further, that person is treated as a 'pre-suspect' with the associated stigma that entails.[23]

70. Based on the evidence presented in the Joint Report, which indicated that Māori are already over-represented in photographs taken and retained by Police, I consider that the guarantee of equal treatment of Māori in Article 3 of te Tiriti is engaged by this collection of personal information. Further Tiriti analysis is therefore needed. As the Law Commission observed in its report on the DNA regime, the Crown has an obligation to take steps to reduce inequities between Māori and non-Māori. There is no evidence that that obligation has been properly considered in this Bill.

Impacts on children and young people

71. The RIS discusses the impacts of offending for children and young people and suggests that better access by Police to information, as a result of the proposed amendments, will help Police to respond and reduce risks of reoffending. However, the RIS does not adequately address the impacts of Police activities on the rights and interests of children and young people, particularly where there is little evidence or reason to justify Police interventions. It does acknowledge risks including 'possible overcollection, unintended profiling and long-term retention of data' about young people.[24]

72. The RIS comments that the proposed amendments do not seek to legislate additional protections for the collection, use and retention of images of children and young people for a number of reasons. These reasons include that existing legislative requirements relating to children and young people will continue to apply, that children and young people are not the focus of the legislative change, that restrictions on information-collection could hinder Police's ability to address victimisation of and criminal offending by young people, and that other parts of the Policing Act do not provide specific protections for children and young people.[25]

73. The RIS notes that Police 'will continue to consider and give effect to its obligations through internal operational practices, policies and guidance.'[26] However, this is not reassuring when the Joint Report findings indicated a lack of understanding of

---

[23] Law Commission, *The Use of DNA in Criminal Investigations | Te Whakamahi i te Ira Tangata i ngā Mātai Taihara*, Issues Paper 43, 2018, p 249. The wording in this paragraph is a not a direct quote from the Law Commission, but a close paraphrase, substituting references to photography for those to DNA profiling.
[24] RIS, p 33.
[25] RIS, p 34-35.
[26] RIS, p 35.

Police's obligations in relation to information gathering, particularly about children and young people.

74. The Joint Report identified the feelings of shame, embarrassment, frustration and anger towards the police for young people and their families when they had their personal information collected without their consent and where this collection was not clearly connected to a lawful purpose.

75. Broader Police powers will permit wider collection of personal information about children and young people than is necessary for a lawful purpose. As noted above, the Bill's authorisation for this collection will displace some of the privacy safeguards that were the subject of key recommendations of the Joint Report. It will therefore increase the likelihood of children and young people being subject to unnecessary intrusions of privacy, particularly in the absence of any specific protections for young people in the Bill.

Impacts on human rights

Right to privacy

76. New Zealand is a signatory to international human rights instruments that include the right to privacy, and those human rights obligations are given effect to, in part, through the Privacy Act.[27] Privacy is not an absolute right, and can be subject to limits imposed by law in order to protect other rights and interests. However, legal limits on the right to privacy must be justified, proportionate to the objective, and not arbitrary.

77. This Bill has the potential to significantly infringe on the right to privacy by giving Police a broad power to collect personal information without a clear purpose for doing so, and without any meaningful constraints on Police retention, use and disclosure of that information, so long as there is some connection to a policing purpose. That includes the ability to use digital technology to compare and analyse the information. While Police does not currently use live facial recognition technology (**FRT**), it does use FRT for retrospective analysis of facial images for investigative or intelligence leads, comparing images of persons of interest to images already lawfully held by Police.[28]

78. Privacy risks created by this Bill include:

    - subjecting individuals to close scrutiny and analysis of their location, movements, appearance and activities, without good reason to do so

[27] International Covenant on Civil and Political Rights, art 17; Convention on the Rights of the Child, art 16; Privacy Act 2020, s 3(b).
[28] New Zealand Police, *Police Use of Facial Recognition Technology (FRT)*, 29 September 2025.

- gathering sensitive personal information, such as about a person's political beliefs or physical or mental health,[29] as well as sensitive biometric information (facial images)
- treating people as potential suspects or criminal associates based on their presence on the Police database
- false matches which incorrectly identify a person on the Police database as a suspect in a criminal investigation.[30]

79. I emphasise that these are examples of privacy risks, but there are also other risks, particularly bias and racial profiling.

80. I acknowledge that these risks can be mitigated through Police policies, guidance and procedures, and I have no doubt that Police will take steps to mitigate them. Nonetheless, providing a broad authorisation for the collection of personal information, without effective legislative safeguards, undoubtedly increases the level of risk to individuals' privacy. In its current form, the Bill's impacts on privacy have not been shown to be justified and are not proportionate, while the exercise of Police power risks being arbitrary in its application.

Other human rights and democratic freedoms

81. While my jurisdiction is concerned with privacy, the Bill's impacts on privacy are likely to have implications for other human rights, including those protected under the New Zealand Bill of Rights Act 1990 (**NZBORA**). If individuals are aware that Police can record them going about their everyday lives, based only on an officer's belief that the information could be useful for broad policing purposes, this could have a chilling effect on the exercise of other rights. In particular, concern that Police may, without good cause, be recording what people do, where they go or who they associate with could inhibit people from exercising their rights to freedom of thought, expression, religion, peaceful assembly, association, and movement, and inhibit members of minority groups from exercising their right to express their culture and religion and use their language.[31]

82. More generally, privacy supports our ability to live free of undue scrutiny from the state and other powerful institutions, allowing us the space to express our individuality and participate in the life of a democratic society. When people have

---

[29] This information might be apparent not only through recorded speech, but also through records of a person being at, for example, a political rally or a sexual health clinic.
[30] In a recent UK case, a man whose image was on a Police database was arrested for a burglary he could not possibly have committed, based on a facial recognition match. The man's image was only in the database because he had been wrongly arrested some years before, and his photograph had never been deleted. The police force concerned conceded to the man that his arrest 'may have been the result of bias within facial recognition technology'. Mark Wilding, 'The Rise of Facial Recognition Policing', Liberty Investigates, 1 April 2026.
[31] New Zealand Bill of Rights Act 1990, ss 13-18, 20, and corresponding rights in the International Covenant on Civil and Political Rights.

confidence that their information will be collected by the state only when necessary, and will be handled with care, they are more likely to have trust in government and to feel able to engage with democratic processes. Conversely, when protections for personal information are weakened, as I believe they would be by this Bill, New Zealanders may lose confidence in public institutions and democratic processes.

Section 21 of the New Zealand Bill of Rights Act

83. Section 21 of NZBORA guarantees the right to be secure against unreasonable search or seizure. This right is based, in part, on the protection of privacy. The Ministry of Justice's advice on the Bill's consistency with NZBORA concludes that the Bill is consistent with section 21.

84. The Ministry's analysis describes new sections 45A to 45E of the Act as providing 'a very wide power for Police to collect information' which, in some circumstances, would amount to a search. However, the advice concludes that these sections do not create a regime that requires Police to exercise search powers in a way that would be unreasonable. Because section 6 of NZBORA requires public agencies to interpret enactments in a way that is consistent with guaranteed rights and freedoms where it is possible to do so, Police can and should interpret the new sections in a way that is consistent with section 21. Police must therefore only carry out searches under these sections in a way that is reasonable, and as a result the Bill is not inconsistent with section 21.[32]

85. I agree with the NZBORA advice that the exercise of Police powers under the Bill will sometimes constitute a search, but often it will not – although the advice probably underplays how often Police will need to consider whether a search is being untaken, and the reasonableness of any search. However, I believe the NZBORA advice's analysis of section 21 issues is inadequate. Appendix 2 sets out some additional matters that should be considered in relation to the Bill's compliance with section 21.

86. One issue is that any search under the powers in the Bill will be warrantless. The LDAC *Legislation Guidelines* state that a compelling reason must exist to create warrantless search powers.[33] This is because such powers are not subject to judicial oversight, and do not provide the documentation that allows for accountability and oversight.

Background to Part 1 of the Bill

87. Police has stated that the amendments in Part 1 of the Bill are necessary due to the recommendations of the Joint Report and the 2025 decision of the Supreme Court in *Tamiefuna*. Both the Joint Report and *Tamiefuna* commented on how the law applies

[32] Ministry of Justice, 'Consistency with the New Zealand Bill of Rights Act 1990: Policing Amendment Bill', 5 March 2026.
[33] Legislation Design and Advisory Committee, *Legislation Guidelines*, 2021, p 112 (section 21.2).

to Police officers taking photographs or collecting information about people in public settings.

Report into Police photographing the public

88. The Joint Report was a response to news reports of Police stopping and photographing rangatahi Māori in the street. The Joint Report considered several such incidents, all involving rangatahi Māori. In each case, it appears that Police officers did not explain, or did not adequately explain, the reasons for taking the photographs or how they would be used. Whānau have spoken about their feelings of whakamā (shame), embarrassment, frustration and anger at the actions of Police, and their belief that the rangatahi were targeted due to racial bias. The Joint Report noted that, based on the limited data available, more than half of intelligence photographs retained by Police were of Māori.

89. The Joint Report also discussed wider issues about Police practices when photographing the public. The issuing of smartphones to Police officers has allowed Police to take photographs much more easily and in greater volumes. The Joint Report commented that photographs are sensitive biometric information, because they capture the unique likeness of the individual. Photographing is also more privacy-intrusive than observing or taking notes because digital images can be retained, shared and matched, and used to adversely affect the individual's interests.

90. It found that many Police officers had limited understanding of the Privacy Act and often took photographs without a clear purpose for doing so. Officers described taking photographs simply because individuals or their behaviour appeared 'out of place' or 'suspicious'. There were also significant issues with the storage and retention of photographs taken by Police officers, with officers often storing thousands of photographs on their phones.

91. A particular area of concern was Police taking photographs for general intelligence purposes. The Joint Report found that, to comply with IPP 1, Police officers needed to be able to identify and record the specific reason for taking a photograph or video recording. It proposed that, when photographing or video recording an individual for general intelligence purposes, Police must be able to articulate a reasonable possibility that collection of the image will be relevant to a particular or likely investigation.

92. Police accepted the Joint Report's recommendations about the photographing of rangatahi but had concerns about some of the broader recommendations.

93. OPC also issued a compliance notice to Police in 2021, requiring Police to stop unlawfully collecting photographs and biometric prints from members of the public, particularly young people, and to delete unlawfully-collected material stored on their systems. Police has complied with most requirements of the compliance notice, but

has been unable to find and delete all unlawfully-collected information, due to the limitations of Police's information-management systems.

94. More details of the Joint Report are provided in Appendix 3.

Tamiefuna v R

95. *Tamiefuna* concerned the use of photographic evidence in relation to the right to be secure against unreasonable search and seizure. It involved a challenge to photographic evidence used to convict Mr Tamiefuna of aggravated robbery. The Supreme Court found that the photographic evidence had been improperly obtained and should have been excluded.

96. Mr Tamiefuna had been photographed by Police when required to exit the car in which he was travelling following a routine traffic stop. The majority in the Supreme Court found that, in the specific circumstances, the taking of the photograph was a search. Factors in this finding included that Mr Tamiefuna was only in a public place because of Police action and that the photograph was to be retained in a Police database. The majority further found that the search was unlawful and unreasonable. The majority concluded that Police's common law powers did not extend to authorising a warrantless search for the purpose of gathering general intelligence.

97. More details of *Tamiefuna* are provided in Appendix 4.

My Office's role in the policy process leading to Part 1

98. Police consulted OPC about the policy proposals for Part 1 of the Bill throughout the policy development process. OPC provided successive rounds of feedback, under tight timeframes. Over that time, some adjustments were made to the policy proposals and draft Bill in response to feedback from OPC and others. However, the consistent policy intention throughout the policy process has been to introduce a simple authorising provision for information-gathering, rather than a comprehensive framework for intelligence gathering with built-in safeguards.

99. Throughout the policy process, OPC opposed the proposed amendments as unnecessary and unreasonably intrusive on privacy and other rights. OPC repeatedly offered to work with Police on operational protocols and procedures to provide clarity for Police intelligence-gathering; and to assist Police, the Ministry of Justice and other officials to develop a bespoke legislative authorising framework for intelligence-gathering, with appropriate safeguards. However, Police did not take up these offers.

Why Part 1 is not needed

100. I am not persuaded by the arguments advanced in support of Part 1 of the Bill. I consider these arguments in more detail in Appendix 5.

101. Police argues that the Bill is needed because the Joint Report and *Tamiefuna* have:

- 'narrowed' the law on Police information collection, and Part 1 simply 'reaffirms' the previous legal position
- created significant obstacles to Police being able to collect information for general intelligence purposes and to make visual and audio recordings, so Police will be less effective in keeping the public safe
- led to frontline Police officers being uncertain about their ability to collect personal information, and required complex case-by-case assessments of the lawfulness of information collection
- imposed restrictions that leave Police with fewer rights to record images than the general public, who are said to be free to take images in public places.

102. Police has also argued that the amendments in Part 1 are necessary to allow the adoption of body-worn cameras (**BWCs**) and other technologies. Police has stated that the amendments will allow Police to use BWCs to record continuously in public and private places for a range of purposes.

The Joint Report and *Tamiefuna* have not changed the law

103. While the Joint Report and *Tamiefuna* identified legal constraints on Police information-gathering, neither has changed the law. They have simply stated what the law is, in relation to particular scenarios. The fact that Police has had a different understanding of the law, or that certain Police practices may have been 'longstanding', does not mean that the law has been changed.

Police information-gathering is not excessively constrained

104. I do not accept that the constraints on Police information-gathering in the Joint Report and *Tamiefuna* are as great as Police has argued. The Joint Report threshold for recording images for intelligence purposes required only the '**possibility**' that the images might be relevant, though this should be based on more than mere conjecture. The images could also be relevant to either a current or a **likely** investigation. Similarly, the Supreme Court in *Tamiefuna* did not make a general finding that Police cannot record individuals in public for intelligence purposes. The Court's decision related to a particular set of facts.

105. Police has acknowledged that there is no specific evidence of an operational risk to Police's ability to carry out its functions.

106. If there is a case for providing Police with additional authorisation to collect information, this should be done in a targeted way, with clear limits.

The Bill will not provide certainty for frontline Police

107. I do not believe the Bill will provide the certainty Police is seeking. Police officers will still need to make decisions about their legal authority to collect information, and those decisions are still likely to be challenged in the courts.

108. Officers will need to assess whether their collection of personal information is for one of the purposes set out in new section 45A. The courts will also still be able to assess whether Police actions constitute a search and whether the search is unreasonable. Officers will still need to consider whether their actions may breach the right to protection against unreasonable search and seizure.

109. The Bill also seeks to provide certainty for Police authorisations, while providing no certainty with regard to safeguards. Police has argued that prescribing safeguards in legislation would be overly prescriptive and remove Police's ability to make decisions case by case.

It is appropriate to restrict Police recording in public places

110. I do not accept the assumptions underlying the claim that the Bill is needed to give Police the same rights to record in public places as the general public, because:

- *Tamiefuna* is specific in its application to the particular facts and does not impose a general restriction on Police recording in public places.
- The Privacy Act applies equally in public and private places. The Privacy Act allows individuals to collect personal information, including taking photographs, for 'personal or domestic affairs'. That is why members of the public will not generally breach the Privacy Act if they take personal photographs, regardless of the location. The same exception does not apply to organisations, like Police, which must have a good reason for taking photographs that record personal information.
- Individuals can expect some privacy in public places. While individuals may reasonably expect to be casually observed while in public, they do not expect to be subject to close, targeted or prolonged scrutiny, or targeted recording of their appearance, actions or movements.
- The Police does not occupy the same position in society as members of the general public because Police exercises coercive powers on behalf of the state. It is a well-accepted principle in liberal democracies that law enforcement agencies should be subject to constraints and oversight to ensure that their powers are exercised in a way that is consistent with democratic rights and norms.

The law already allows Police to use body-worn cameras

111. I believe the developing ability of technologies to collect and analyse huge amounts of personal information is a reason to introduce greater, not lesser, protections for individual privacy.

112. In addition, BWCs can be used within the regulatory framework of the Privacy Act. So long as Police sets its lawful purposes for collection (such as officer safety and integrity) and can establish that the use of BWCs for those purposes is reasonably necessary, it is free to collect, hold and use personal information for those purposes. If Police wishes to use or disclose the footage collected with a BWC for a purpose other than officer safety and integrity (for example, for an investigation), there are exceptions in IPPs 10 and 11 that potentially allow it to do so.

113. While I do not believe that legislation is needed to allow Police to use BWCs, my Office could support Police to develop a specific legislative framework for use of BWCs, if Police feels this would provide greater operational certainty and safeguards.

The broader policing context

The importance of maintaining trust and social licence

114. It is one of the principles of the New Zealand Police that 'Effective policing relies on a wide measure of public support and confidence', and 'strengthening trust and confidence' is one of the three goals in Police's Vision.[34] Police's *National Intelligence Operating Model* also states that:[35]

> We serve the New Zealand people, and we treasure public trust. We comply with the laws of New Zealand and our obligations to protect the privacy, civil liberties, and human rights of our community. We are committed to proportionate and reasonable use of collection methods.

115. Surveys indicate that most of the public continues to have trust in Police.[36] At the same time, a significant proportion of New Zealanders has low trust in Police, and trust is unevenly spread across New Zealand communities. In particular, Māori

[34] New Zealand Police, 'New Zealand Police overview', Police website.
[35] New Zealand Police, *National Intelligence Operating Model*, 2025, p 12.
[36] New Zealand Police, 'Survey results show continued high levels of trust and confidence in Police', media release, 19 March 2026 (reporting on New Zealand Crime and Victims Survey results for October 2024 to October 2025); Lilian Hanly, 'New polling shows a quarter of New Zealanders have little or no trust in police', Radio New Zealand, 29 January 2026 (reporting on an opinion survey conducted in January 2026).

consistently report lower-than-average levels of trust in Police.[37] Trust can also be lost if Police is seen to be acting unlawfully, unethically or arbitrarily. With new targets for Police to increase public trust,[38] it is important to consider the potential implications of the Bill for trust in Police, and the social licence under which Police operates.

Proposed establishment of an Inspector-General of Police

116. In the wake of the IPCA report that found serious failings in the Police response to complaints made against former Deputy Police Commissioner Jevon McSkimming,[39] it is all the more important to maintain trust in Police. In response to the IPCA report, the Government has announced that it will establish a new position of Inspector-General of Police, which it has described as providing 'the most robust level of oversight available to the Government'.[40] It is currently unclear when the IGP will be established.[41]

117. It is unfortunate that this Bill is proceeding before the establishment of the IGP, as it is unclear what jurisdiction or powers the IGP will have to provide oversight of Police implementation of the Bill. Ideally, the Bill should not proceed or come into force before the IGP is established.

Potential impact of Part 1 of the Bill on public trust

118. One of my greatest concerns about the Bill is that it has been subject to no public consultation prior to introduction. This is in contrast to the process to create the Policing Act 2008, which involved extensive public consultation. Proposals for changes which create new authorisations for Police collection of information, and therefore affect privacy and other human rights, should have been subject to broad public consultation, as well as specific consultation with Māori and other communities that may be particularly affected. This consultation should have been open-ended in the first instance, and if there was a case for legislation, the Government should have consulted on an exposure draft of proposed amendments. Consultation on a Bill at select committee is not an adequate substitute for wider consultation. As I have discussed above, Police has provided no evidence that the amendments needed to be progressed with urgency.

---

[37] The 2024 National Crime and Victims Survey found that 60% of Māori had high trust in Police, compared to the New Zealand average of 73%, while 49% of Māori had a high level of agreement with the fairness of Police, compared to the average of 65%: Ministry of Justice, *Public Perceptions Module (PPM) key results: Public perceptions of the justice system*, 2025, pp 29, 34.
[38] Adam Pearse, 'New police targets revealed to improve trust, reduce public violence', *New Zealand Herald*, 2 December 2025.
[39] Independent Police Conduct Authority, *Review of Police Handling of Complaints against Jevon McSkimming*, 11 November 2025.
[40] Hon Judith Collins and Hon Mark Mitchell, 'Damning IPCA report prompts oversight move', 11 November 2025.
[41] Sam Sachdeva, 'No timeline for new police watchdog after McSkimming scandal, Govt says', Newsroom, 16 April 2026.

119. It is not clear what impact the Bill will have on trust and confidence because there has been no public consultation on the proposed amendments.

120. Police has argued that the public can be assumed to expect that Police is empowered to perform its duties, and that any limitations on Police's ability to carry out its functions, as a result of limits on the collection of information, could reduce public trust and confidence in Police.[42] Police has therefore implied that the Bill will support public trust and confidence. Police has acknowledged that there is likely to be public concern about perceived intrusions on privacy, but states that this concern can be mitigated through appropriate safeguards.[43] As discussed above, however, the Bill provides no safeguards.

121. While it is not clear what the public thinks of the proposals in this Bill, I believe public trust and confidence in Police is best supported when Police is seen to be acting in accordance with the law and human rights standards, is subject to independent oversight from regulators and the courts, and exercises powers that are proportionate, reasonable and subject to clear limits. I am particularly concerned that expanded Police information-collection powers are likely to have a disproportionate impact on Māori, risking a further loss of trust among Māori. Ensuring public trust and confidence is a critical reason for including clear limits and safeguards in the Bill.

122. I recognise that, following the findings of the Joint Report and the IPCA's McSkimming report, and the appointment of a new Police Commissioner in 2024, Police has been working to improve its practices and systems, and has had a focus on integrity. These are welcome developments. However, public trust in Police requires the creation of legislative safeguards to provide assurance that Police will respect privacy and human rights, regardless of changes of leadership or other changes in the internal or external context for Police operations.

The inadequacy of Police information management and oversight

123. The Joint Report highlighted serious inadequacies in Police systems for managing information, and this has continued to be a problem for Police's response to the compliance notice issued by OPC. A key reason why Police has found it difficult to comply with the requirement to delete unlawfully-obtained information is that many images were stored on Police systems without labels that would allow them to be searched automatically. I commented in October 2024 that:[44]

> I am concerned that the current state of Police's information management systems and the extremely large number of stored images make it very hard to find and delete images in a practical way.

---

[42] RIS, p 14.
[43] RIS, p 21.
[44] Office of the Privacy Commissioner, 'Police well on the way to compliance; one critical step remains', media release, 17 October 2024.

These same issues may make it difficult for Police to find and use the information they have collected and retained to fight crime and keep communities safe.

The recent Performance Improvement Review of Police also commented that 'Information and corporate systems have grown over time around specific functions, leading to fragmented data, multiple tools, and manual workarounds.'[45]

124. Unfortunately, it appears that these issues have not yet been resolved, and there is no plan to address them before this Bill is implemented. The Cabinet policy paper simply states that Police will 'look to improve its information management systems and internal controls, and to enhance system capability'.[46] The RIS further states that Police will 'consider' capability improvements in information management 'to maintain probity and enhance control mechanisms for the collection and use of personal information'. It continues that 'further information management investment will assist with strengthening these safeguard[s]', but that an assessment was needed to determine whether any investment could be met through existing baseline funding or through a Budget bid.[47] It appears, however, that work on information management upgrades to support the changes in the Bill has not started and that no additional funding has been sought.[48]

125. OPC has repeatedly advised Police that, without significant upgrades to Police information management systems, which may well require additional investment, Police will be unable to safely manage the increased volume of information that could be collected under this Bill. This means that Police is likely to continue to struggle to meet its obligations under the Privacy Act to store personal information safely, delete it when no longer needed, and make it available to individuals who request access to their own information. In addition, it is hard to see how the amendments will achieve their intended aims if Police systems do not allow Police to readily and reliably access the very large volumes of personal information it holds for intelligence and investigation purposes.

126. I therefore believe this Bill should not proceed without the necessary major improvements to Police information management systems.

---

[45] Public Service Commission, *Performance Improvement Review of the New Zealand Police*, April 2026, p 15.
[46] 'Amendments to the Policing Act 2008', paper to Cabinet, 2025, p 10.
[47] RIS, p 31.
[48] Phil Pennington, 'New police powers: No new money for vital technology', Radio New Zealand, 2 April 2026.

Establishing an appropriate legislative framework

The case for an alternative legislative framework for Police intelligence-gathering

127. New Zealand Police, like its counterparts in other jurisdictions, has an increasing focus on intelligence as part of an intelligence-led policing approach.[49] This trend has been facilitated by the ever-increasing power of digital technologies which allow data to be collected and analysed much more readily (although growing volumes of data can also create problems of separating the signal from the noise).

128. Police practices when collecting personal information for general intelligence purposes were a key area of concern in the Joint Report. In that report, OPC and the IPCA explained how the Privacy Act applies to Police taking of photographs and videos for intelligence purposes. Currently, the Privacy Act and the Independent Police Conduct Authority Act together provide important oversight of and controls on Police intelligence-gathering.

129. However, there is a case for developing a separate regulatory framework for Police intelligence-gathering, as was recognised in the decision of Justice Kós in *Tamiefuna*.[50] New Zealand may be better placed than the other jurisdictions discussed below to create such a framework, because we have a single police service covering the whole country.

130. Police defines intelligence as 'the collection, collation, analysis, and dissemination of information to inform decisions to prevent and combat crime.'[51] Intelligence is a crucial part of policing, but it also raises significant risks to the democratic freedoms and the rights of individuals and groups.[52] These risks include:

- invasion of privacy through intrusive, and potentially wrongly-targeted, surveillance
- profiling of communities, particularly along ethnic or political lines
- taking action against individuals on the basis of information that may be partial or incorrect, and which the individual cannot challenge until after the action has been taken.

---

[49] Angus Lindsay, Trevor Bradley and Simon Mackenzie, 'Organisational barriers to institutional change: The case of intelligence in New Zealand policing', *Howard Journal of Crime and Justice*, vol 61, 2022, pp 407-426; New Zealand Police, *National Intelligence Operating Model*, 2025.
[50] *Tamiefuna*, at [326] (Kós J). See also [272], [291] (Glazebrook J) for commentary on Police policy.
[51] New Zealand Police, *National Intelligence Operating Model*, 2025, p 4.
[52] See Lyria Bennett Moses, 'Oversight of Police Intelligence: A Complex Web, but Is It Enough?', *Osgoode Hall Law Journal*, vol 60, no 2, 2023, pp 293-296.

131. A particular concern, with the rise of artificial intelligence and algorithmic prediction, is that intelligence may be used to target individuals or groups based on predictive analysis that is hard to access, understand or challenge.[53]

132. Another issue highlighted by this Bill is that intelligence can involve the collection of information whose specific value and potential use is not known at the time of collection. This feature of intelligence means that a purpose-based data protection law like the Privacy Act may not be the best framework for regulating intelligence-gathering. At the same time, the non-specific nature of the purpose of collection of information makes it all the more important that limits on collection, independent oversight and accountability remain in place.

133. While I consider that this Bill is not the right way in which to authorise Police intelligence-gathering, there is a plausible case for starting afresh to develop a specific authorising framework, with appropriate safeguards, in legislation. A legislative framework for Police intelligence-gathering could include not only the kinds of activities anticipated in the Bill, but also other intelligence activities, such as Open Source Intelligence (OSINT), which involves the collection and analysis of information from publicly-available sources. The development of such a framework must involve careful design and extensive public engagement. My Office would be able to contribute to policy work to help ensure that any new framework involved the proportionate use of Police powers, and was subject to independent oversight and privacy protections.

Regulatory frameworks in other countries

134. I am not aware of any other jurisdictions that have introduced a regulatory framework specifically focused on police intelligence-gathering, but I briefly note here some countries that either have specific requirements for law enforcement as part of privacy regulation, or include some police intelligence activities within broader oversight arrangements for intelligence agencies.

Data protection frameworks for law enforcement in the UK and EU

135. The UK and EU both have bespoke data protection (privacy) frameworks for police and other agencies that process (collect, use, share and store) personal information for law enforcement purposes. These frameworks are not limited to intelligence activities, but they include safeguards that are relevant to intelligence.

136. The UK and EU frameworks, which are very similar, outline six principles police must comply with across the full lifecycle of their information collection, use and

[53] Mareile Kaufmann, 'AI in Policing and Law Enforcement', in Regine Paul, Emma Carmel and Jennifer Cobbe (eds), *Handbook on Public Policy and Artificial Intelligence*, Edward Elgar, 2024, pp 295-306.

handling practices.[54] Of particular note are principles 1 and 2, requiring lawful and fair processing for a specified, explicit law enforcement purpose, and principle 5 outlining rules around storage and retention of personal information.

- Principle 1 (lawful and fair processing) requires a lawful basis for the processing *and* that processing is necessary for the performance of a task carried out for a law enforcement purpose. The fairness limb requires a level of transparency and that information is not processed in a way that is unexpected, misleading or unduly detrimental to the people concerned.
- Principle 2 (purpose specification and limitation) requires the identification of a *specified*, *explicit* and *legitimate* law enforcement purpose for the collection of personal information. It also requires that the information not be processed in a way that is incompatible with this purpose (processing for a different purpose is permitted where it is necessary and proportionate).
- Principle 5 (limits on retention) outlines a general limit that requires information is not kept for longer than necessary and that the agency establishes appropriate time limits to periodically review the need to continue to store the personal information for any of the law enforcement purposes.

137. The UK and EU frameworks include an accountability principle, requiring the law enforcement agency to implement appropriate technical and organisational measures that ensure and demonstrate that they comply with the framework (such as staff training and internal audits of processing activities).

138. In addition, there is a higher threshold for law enforcement agencies to collect and process sensitive information, like genetic or biometric information. For this information, police must show that it is strictly necessary, requiring a rigorous justification for the collection and use of this information.

Independent oversight of police intelligence activities in Canada and Australia

139. In Australia and Canada, bodies that have oversight of national intelligence agencies have had their jurisdiction extended in recent years to cover intelligence activities more broadly, including police intelligence activities.

140. In 2019, Canada established the National Security and Intelligence Review Agency (NSIRA), which can review any activity carried out by a department that relates to national security or intelligence. Its jurisdiction includes the national security and intelligence-related activities of the national police service, the Royal Canadian Mounted Police.[55] The NSIRA can cooperate and share information with

[54] Part 3, Data Protection Act 2018 (UK); Law Enforcement Directive 2016/680 (EU). The EU and UK frameworks are very similar, although the UK framework has less stringent notification and transparency requirements where there is an ongoing investigation.
[55] National Security and Intelligence Review Agency Act 2019.

other oversight bodies, including the Canadian Privacy Commissioner.[56] The NSIRA has full access to all information held by the government, including classified and sensitive information (apart from documents relating to Cabinet deliberations and documents).

141. In a very similar reform, in 2025 Australia strengthened and expanded the oversight responsibilities of its Inspector-General of Intelligence and Security, as well as the Parliamentary Joint Committee on Intelligence and Security, to cover the intelligence activities carried out by multiple agencies, including by the Australian Federal Police.[57]

142. These developments highlight the growing recognition of the importance of formal oversight of Police intelligence activities.

Commencement of Part 1 of the Bill

143. Clause 2(1) of the Bill provides for Part 1 to come into force a month after Royal assent. This is far too soon, considering that:

- Police will need to develop internal policies, procedures, guidance and systems for the implementation of the powers authorised by Part 1.
- Police has not yet undertaken necessary upgrades of its information-management systems, or secured any additional funding that may be needed for these upgrades.
- The IGP, which will likely provide essential oversight of the exercise of Police powers, has not been established, nor has legislation to establish it been introduced.

144. If the Bill proceeds, I **recommend** that it be amended to provide for a later starting date for Part 1. This could be done in a number of ways:

- a fixed date, such as 12 months after Royal assent
- a date to be set by Order in Council, based on advice that certain key conditions have been met
- a conditional date, such as the day after regulations providing for safeguards come into force (if the option of establishing safeguards in secondary legislation is chosen) or after legislation establishing the IGP comes into force.

[56] Sections 13-15.1, NSIRAA.
[57] Strengthening Oversight of the National Intelligence Community Act 2025.

Conclusion

145. I welcome the opportunity to submit on this Bill to the Committee, because Parliament has an important role in scrutinising the powers of the Police and ensuring appropriate checks and balances are in place. By providing a broad statutory authorisation for Police information-gathering, while leaving safeguards to be covered in internal Police policies, Part 1 of this Bill effectively removes the ability for Parliament to determine the scope and limits of Police powers. This is particularly problematic given the growing potency of new technologies.

146. Police does important work in enforcing the law, keeping the peace, maintaining public safety and carrying out other functions and activities. To undertake its functions, Police needs to be able to collect information and gather intelligence, and to use developing technologies. It is vital, however, that Police carries out its activities in ways that protect rights and maintain public trust and confidence. I do not believe that Part 1 of the Bill gets that balance right. However, I am confident that, through a more careful and consultative policy process, a legislative framework can be developed to give Police the authorisations it needs while providing assurance to members of the public that their rights will be respected.

Recommendations

147. I do not support the Bill and **recommend** that it not be passed. If the Bill does not proceed, I **recommend** that serious consideration be given instead to creating a new regulatory framework for Police intelligence.

148. If the Bill proceeds, I **recommend** that it be amended to introduce safeguards and make other changes as set out in Appendix 1.

149. I trust my comments are of use to the Committee. I would like to present my submission to the Committee in person.

Michael Webster

Privacy Commissioner

30 April 2026

Appendix 1: Summary of recommendations

1. This appendix records all recommendations made throughout the body of my submission, for completeness.

Substantive recommendation

2. I do not support the Bill and **recommend** that it not be passed. If the Bill does not proceed, I **recommend** that serious consideration be given instead to creating a new regulatory framework for Police intelligence.

Recommendations should the Bill proceed: new safeguards

3. If the Bill proceeds, I **recommend** that it be amended to ensure that adequate safeguards are in place. My recommendations about safeguards are:

    - Amend the Bill to ensure that the effect of the IPPs is maintained by reflecting an objective threshold for the collection of personal information, with clear limits on secondary use and retention of that information. Any breach of these limits should clearly engage the complaint mechanism in the Privacy Act and the Privacy Act's compliance framework to address systemic issues.
    - Amend the Bill to provide for safeguards in relation to Part 1. My preference is that safeguards should be provided for in the Policing Act itself. Alternatively, the Bill should be amended to create a regulation-making power requiring regulations to be made establishing safeguards.
    - Whether in primary or in secondary legislation, key safeguards should include necessity and proportionality assessments; record-keeping requirements; auditing and public reporting; transparency of Police policies; standards on storage, retention and destruction, and secondary uses of information; and protections for children and young people, and other vulnerable populations.
    - Police compliance with these safeguards should be subject to independent oversight by the Privacy Commissioner, IPCA or IGP.
    - If safeguards are provided for through a regulation-making power:
        - the Bill should require such regulations to be made, rather than giving the Minister discretion to decide whether to make regulations or not
        - the regulation-making power should set out matters that must be addressed in the regulations
        - the Bill should require that the regulations be subject to public consultation, and to consultation with the Privacy Commissioner and other relevant oversight bodies

- Part 1 should not commence until the regulations have been made.

Recommendations for drafting should the Bill proceed: other matters

4. I **recommend** that the Bill should be amended to:

   - provide for a later commencement date for Part 1 than that in clause 2(1) of the Bill
   - define ‘intelligence’ or ‘intelligence purpose’
   - provide that recording ‘by any means’ in s 45B does not include technologically-enhanced collection, such as the use of devices that enhance ordinary human vision or hearing
   - delete s 45C, and address any potential changes to Police powers to record when lawfully on private property through policy work on the Search and Surveillance Act 2012.

Minor recommendations and suggestions

5. I encourage the Committee to request advice on the rationale for these powers applying to all Police employees rather than only to constables.

6. I recommend that the Committee take advice about defining ‘public place’ and ‘private property’.

Appendix 2: section 21 of the Bill of Rights Act

1. Section 21 of NZBORA guarantees the right to be secure against unreasonable search or seizure. The Ministry of Justice's advice on the Bill's consistency with NZBORA concludes that the Bill is consistent with section 21.

2. The Ministry's analysis describes new sections 45A to 45E of the Act as providing 'a very wide power for Police to collect information' which, in some circumstances, would amount to a search. However, the advice concludes that these sections do not create a regime that requires Police to exercise search powers in a way that would be unreasonable. Because section 6 of NZBORA requires public agencies to interpret enactments in a way that is consistent with guaranteed rights and freedoms where it is possible to do so, Police can and should interpret the new sections in a way that is consistent with section 21. Police must therefore only carry out searches under these sections in a way that is reasonable, and as a result the Bill is not inconsistent with section 21.[58]

3. I agree with the NZBORA advice that the exercise of Police powers under the Bill will sometimes constitute a search, but often it will not – although the advice probably underplays how often Police will need to consider whether a search is being untaken, and the reasonableness of any search. However, I believe the advice misses some important points.

4. First, the Bill confers a warrantless search power: that is, it is not subject to any prior judicial authorisation or subsequent systematic oversight.

5. It is a basic principle of New Zealand constitutional law, drawn from United Kingdom common law dating back to the seventeenth century, that searches require warrants, except in exceptional circumstances. As the Law Commission wrote in 2007, in its report which led to the current overall scheme of the Search and Surveillance Act 2012, that principle serves several purposes:[59]

   > The requirement to obtain a warrant is designed to ensure that the decision to undertake a search or seizure is not left in the hands of the party who conducts it. There are a number of compelling reasons for this.
   >
   > - It is an essential component of the checks and balances that should exist in a system operating according to the rule of law. While the state through its agents may be expected to act in good faith when exercising coercive powers against individual citizens, that cannot be guaranteed and should not be assumed; it is fundamental to the protection of individual liberty that the need for the exercise of the power should be demonstrated to the

[58] Ministry of Justice, 'Consistency with the New Zealand Bill of Rights Act 1990: Policing Amendment Bill', 5 March 2026.
[59] Law Commission, *Search and Surveillance Powers,* NZLC R97, 2007, pp 49-50.

satisfaction of an independent officer and authorised by that officer before the exercise of the power rather than justified afterwards with the benefit of hindsight.

- It introduces its own disciplines and constraints into the routine procedures and activities of law enforcement agencies. …
- It acts as some protection for the agencies themselves against claims of civil or criminal liability. It gives their actions the imprimatur of a judicial order and may to some degree pre-empt the filing of court proceedings by those under investigation who would otherwise seek either to prevent the exercise of the power or to obtain damages for that exercise. In other words, the requirement for a court order acts as a protection not only to the suspect, but also to the agency.

6. Because of those risks and pitfalls, the Law Commission went on to observe, warrantless powers require justification:[60]

> [T]he importance of the warrant requirement is such that departures from it can be justified in only exceptional circumstances. Nevertheless, whilst the warrant process is the primary means of authorising and justifying an entry, search and seizure, many Commonwealth jurisdictions accept that in urgent circumstances, such a process may be too time-consuming and detrimental to the end result; in such situations the public interest may better be served if the police act without a warrant.

7. Parliament has previously proceeded on that basis, in particular in the broad and very carefully-developed regime of the Search and Surveillance Act. Warrantless search powers directed at the general public are properly justifiable, for example:[61]
    - Where necessity or urgency calls for intervention to prevent:
        - danger to life or property
        - the loss of evidential material
        - a person suspected of an offence from absconding.
    - Where the existence of a firearm or dangerous thing that could be used to harm others is suspected.
    - Where the search of people and vehicles would occur in a public place, for which common law has never required a warrant.
8. Unlike the Search and Surveillance Act, the power conferred by the Bill is not directed to urgent or other circumstances that mean that it is not reasonable for

---

[60] Law Commission, *Search and Surveillance Powers,* NZLC R97, 2007, p 130.
[61] *Garrow and Turkington's Criminal Law in New Zealand* (2025ed) [SS7A].

Police officers to obtain independent authorisation. Likewise, and unlike existing and well-understood powers, the Bill does not impose any substantive preconditions (for example, urgency or particular suspicion) on the exercise of the power.

9. The LDAC *Legislation Guidelines* state that a compelling reason must exist to create warrantless search powers:[62]

> Generally, a real risk must exist that some serious harm or damage will occur or evidence will be lost if officers are required to obtain a search warrant.
>
> However, consideration must still be given to whether or not any risk can be satisfactorily addressed by obtaining a warrant but delaying notice to the person or the occupants of a property that is the subject of the search. In the law enforcement context, compelling reasons must exist for granting warrantless search powers in respect of non-imprisonable offences.
>
> In the regulatory context, it may be appropriate to allow warrantless inspections to take place without notice if it is the only effective way to ensure that certain regulatory standards are being adhered to (for example, the inspections of restaurants). Regardless of the context, all search powers must be proportionate to their objectives and all searches must be carried out by properly authorised and trained officers.
>
> Warrantless search powers should rarely extend to dwelling houses or marae and only in circumstances where there is a compelling justification for such a high level of intrusion.

10. Warrantless search powers require a compelling reason because they are not subject to judicial oversight, and as a result they do not provide the audit trail of documentation that allows for accountability.

11. The warrant principle, and the prerequisites for justifiable warrantless powers, are also basic components of the human right against unreasonable search and seizure as understood not only in New Zealand but also, for example, in Canada, the United States and among the 46 member states of the Council of Europe.[63] However, this principle is not addressed in the Ministry of Justice advice.

12. Second, Police has not given adequate consideration to more rights-protective alternatives to the amendments in the Bill. The LDAC guidelines state that, if a protected right is implicated by a legislative proposal, officials must consider whether it is possible to achieve the objective without limiting that right, or in a way that limits it no more than is reasonable.[64] I do not believe that the RIS for this Bill constitutes

---

[62] Legislation Design and Advisory Committee, *Legislation Guidelines*, 2021, p 112 (section 21.2).
[63] See, for example, *R v Nolet*, [2010] 1 SCR 851, [21] (Supreme Court of Canada); *Gutsanovi v Bulgaria* (2017) 64 EHRR 22, [2013] ECHR 982 (European Court of Human Rights); *Terry v Ohio*, 392 US 1 (1968) (United States Supreme Court).
[64] Legislation Design and Advisory Committee, *Legislation Guidelines*, 2021, pp 34-35 (section 6.1).

the kind of thorough analysis to identify the least rights-restrictive option to achieve the policy objective that I would expect to see when a protected right is implicated.

13. Third, and alongside the omission of justification for the warrantless character of the power, the Bill does not address how the information (including video and audio recordings) is to be held, regulated or disposed of when not, or no longer, needed.

14. The requirement for specific, careful controls also forms part of the right against unreasonable search and seizure, for three reasons:

    - The retention of people's information – for example, video footage of members of the public who are not subject to any specific investigation – is justified only where there is adequate, concrete reason for it and where that reason is regularly reviewed.

    - As a basic principle of both constitutional and human rights law, powers to collect information must be prescribed by law. As with the Search and Surveillance Act, the terms of such information-gathering must be fixed by Parliament, not left to internal policies. That ensures both accountability and transparency and guards against the creation of unregulated databases.

    - Increasingly powerful and automated data analysis and matching mean that careful legislative regulation is needed if rights against unreasonable search – including unreasonable retention and compilation of data – are not to be abandoned.

15. These well-known principles governing search and information-related powers have not been addressed in the Ministry advice or in the background to the Bill.

16. This is not to say that data should not be collected or that Police should not be able to use analytical tools where that is justifiable. The critical point, as reflected by the warrant principle and by the need for safeguards, is that the relevant rules must be 'prescribed by law': that is, made publicly and in an accountable way.

17. Fourth, the absence of controls on the search powers conferred by the Bill creates further practical problems under NZBORA. As set out by the Law Commission in the excerpt above, warrant and other requirements both regulate and protect Police evidence-gathering.

18. The Ministry advice envisages that the Police not only must, but can in practice, limit officers' use of the search powers to ensure reasonableness. I understand that is not a principle that applies to, or has ever been accepted about, any other search power. The Bill does not provide any guidance or assurance that officers can in fact know, and demonstrate, that these powers are exercised in such a rights-consistent way. I

note, too, that the Joint Report found that a significant number of Police lacked a sound understanding of constraints under NZBORA.[65]

19. Without controls in the Bill, the main check on Police searches is the ability to challenge the admission of evidence under section 30 of the Evidence Act 2006. However, Evidence Act challenges relate only to information collected by Police that forms part of a criminal prosecution. They do not provide a remedy in relation to the much greater volume of information collected and held by Police. That is inconsistent with the need for a remedy under the section 21 right.

20. Where prosecutions do occur, the section 30 process then creates the prospect that a prosecution case put together by Police work may be thrown out, after the investigation is concluded, if the searches involved are found to be unreasonable. Prior safeguards avoid otherwise sound prosecutions being overturned.

21. In addition, the reliance on individual officers, or on internal policies or technological safeguards, means that the scope of proper use of these powers will, for the most part, occur out of public view and without Parliamentary or other accountability.

[65] *Joint Report*, pp 55-56.

Appendix 3: Joint Report findings

1. In 2020, news media reported that Police in Wairarapa had been stopping and photographing rangatahi Māori on the street.[66] Following these reports, OPC and the IPCA announced a joint inquiry into Police conduct involving photographing members of the public (**the Inquiry**). Terms of reference for the inquiry were released in March 2021. The Inquiry looked into several specific incidents, all involving rangatahi Māori. It also looked more broadly at Police photographing of members of the public, particularly in public places. The Inquiry issued its report in September 2022.

Incidents involving rangatahi

2. The specific incidents the Inquiry reviewed included:[67]

    - Two rangatahi waiting at a bus stop were questioned and photographed by Police officers who were responding to a burglary nearby, despite neither of the rangatahi fitting the description of the reported offenders.
    - Two rangatahi waiting outside a shop were questioned and photographed in relation to an alleged burglary nearby. The Inquiry was told that other rangatahi were also spoken to and photographed, but that Pākehā teenagers nearby were not photographed.
    - A group of rangatahi having an animated conversation in the street was approached by a Police officer who believed a fight or assault had occurred. The rangatahi involved were friends or relations of each other and were not fighting. The Police officer photographed members of the group and continued to do so even after some of them took action to shield their faces. One of the rangatahi involved had reportedly been stopped and photographed by Police on a previous occasion.
    - A rangatahi walking home in the middle of the night after playing basketball was stopped and spoken to by a Police officer, who said concerns had been raised by people in the neighbourhood. The rangatahi was photographed during the conversation, and was then returned home by the officer, who took a further photograph at his residence.

3. In each of these incidents, it appears that Police officers did not explain, or did not adequately explain, the reasons for taking the photographs or how they would be used.

---

[66] See, for example, Te Aniwa Hurihanganui and Hamish Cardwell, '<u>Questions raised after police officers stop youths to take their photos</u>', Radio New Zealand, 21 December 2020.
[67] *Joint Inquiry*, pp 33, 97-103.

4. Some of these incidents were historical, and it was not possible to identify the officers involved or to corroborate the events as reported by the whānau of the rangatahi in all cases. As a result, the Inquiry was unable to make conclusive findings for some complaints. Where it was possible to make findings, the Joint Report found that the Police photographing of the rangatahi had breached a number of IPPs. Where it was not possible to make a finding, the Joint Report commented that Police must take account of the relevant IPPs in relation to these types of encounters between young people and Police. In some cases, Police has acknowledged the incidents and sent letters of apology to the whānau.

5. Whānau of the rangatahi involved have spoken to the Inquiry and to media about their feelings of whakamā (shame), embarrassment, frustration and anger at the actions of Police, and their belief that the rangatahi were targeted due to racial bias. A number of whānau have requested meetings with Police to receive an apology, as well as action to address racial bias on the part of Police.[68]

6. As all of the incidents involved Māori, the Inquiry considered tikanga Māori.[69] The Joint Report commented that the whakamā experienced by rangatahi and whānau as a result of Police actions resulted in takahi mana, the trampling on the self-esteem or standing of an individual or group. Remaining in a state of whakamā can have a significant impact on whānau and a process to restore the balance is needed. The Joint Report proposed that Police apply Sir Hirini Moko Mead's 'Take, Utu, Ea' framework for restoring the balance.[70]

Wider consideration of Police photographing of the public

7. While the Inquiry was prompted by the incidents involving rangatahi, it became clear that there were more general issues about Police practices when photographing the public. The Inquiry therefore examined these wider issues.

8. A key part of the context for the Inquiry was the issuing to all Police officers of smartphones. The availability of mobile devices that can take photographs has greatly increased the ease of photography and the volume of photographs taken by Police officers. It has also created significant problems with managing this photographic data.

9. Another general point made in the Joint Report is that taking photographs is different in important respects from observing with the naked eye or making a note of what is seen or heard. The Joint Report commented that:[71]

---

[68] *Joint Inquiry*, pp 103-104.
[69] *Joint Inquiry*, pp 104-105.
[70] This framework involves identifying the issue, providing the form of redress that most appropriately addresses the imbalance felt by the whānau, and achieving a state in which balance is restored and all parties are satisfied with the outcome.
[71] *Joint Inquiry*, pp 42, 52.

such photographs will usually be sensitive personal information due to the unique nature of a person's image and the strong connection of the image with their identity, mana and personhood. Sensitive personal information may be tapu and is subject to higher standards of care under the scheme of the Privacy Act. Photographs of an individual are not simply a visual record or evidence of a point in time. A digital photograph is an exact biometric image of that particular individual and is capable of being analysed using facial recognition technology and other digital techniques. This makes it even more important that photographs of individuals are collected, used, retained and stored lawfully. …

… Police taking a photograph of an individual carries an inherent level of intrusiveness because of the sensitivity of the information captured (the unique likeness of the individual and their identifying particulars), the potential for the image to be retained for future reference by law enforcement and the potential for the image to be used to adversely affect the individual's interests.

Photography therefore represents a more intrusive observation of individuals in public than other forms of Police engagement with individuals such as a conversation and taking notes. This is because of the permanence of the digital image, the potential for sharing and matching of the image with other records, the extent of the information about the person that is part of the image, and the strength of the connection to the individual's identity, mana, tapu and autonomy.

10. Key findings of the Inquiry about Police practices included:

- Police had limited data on the number of photographs collected and stored and the characteristics of those photographed. From the limited available data on intelligence photographs retained by Police, over half had a recorded ethnicity of Māori.[72]
- Most officers interviewed by the Inquiry had a very limited understanding of the Privacy Act. Police had not developed adequate training, guidance or policies to enable officers use their powers and collect information effectively and lawfully, including collecting personal information in compliance with the Privacy Act.[73]
- As a result of the inadequacy of Police training and policies, Police had been collecting, using and retaining personal information in a way that was at best inconsistent with the Privacy Act, and in some cases unlawful. This would likely have resulted in systemic Privacy Act breaches affecting the rights of individuals.[74]

[72] *Joint Inquiry*, pp 30-31.
[73] *Joint Inquiry*, pp 55, 107-108.
[74] *Joint Inquiry*, p 108.

- It was common for officers to take photographs in public situations, without clearly linking the taking of the photograph to a particular purpose or considering whether taking the photograph was necessary.[75] Under IPP 1, personal information (including photographs of individuals) can only be collected when it is necessary to do so for a lawful purpose.
- Officers described taking photographs of people simply because they 'looked out of place', or because of their age, appearance, location or time of day or night, or other behaviour which officers deemed 'suspicious'. Such practices raised a risk of individuals being photographed by Police based on informal profiling, and potentially unconscious bias, rather than on an objective analysis of the purpose and necessity for taking a photograph.[76]
- While most officers said they would only take a photograph if they had a reason to do so, they were often unable to articulate what would be a good reason beyond referring to 'time, place, circumstance'. It appeared that officers were commonly taking photographs 'based on an inarticulable suspicion in case they potentially become useful at some undefined point in the future'. This approach was likely to have resulted in systematic overcollection of personal information, in breach of IPP 1.[77]
- There were significant issues with the storage and retention of photographs taken by Police officers. The Inquiry found that Police did not have a policy about the use of mobile devices for collecting photographs, or a comprehensive process for audit and deletion of photographs. Photographs were commonly kept indefinitely on officers' devices, which often held thousands of images. In addition to officers' mobile devices, there were multiple other systems and locations where officers could store photographs, but little guidance and no systematic process for transferring, storing and retaining photographs.[78]
- As a result of the inadequacy of the approach to storage and retention, Police was unable to easily audit its holdings of photographs. IPP 9 of the Privacy Act requires that personal information be held for no longer than necessary for the information to be used for a lawful purpose. Photographs were being held for longer than is allowed under IPP 9.[79]

[75] *Joint Inquiry*, p 57.
[76] *Joint Inquiry*, pp 58, 64-65.
[77] *Joint Inquiry*, p 65.
[78] *Joint Inquiry*, pp 91-95.
[79] *Joint Inquiry*, pp 92-93.

Photography and intelligence gathering

11. A particular issue addressed in the Joint Report, and that is relevant to the Bill, was the use of photography as part of intelligence gathering by Police.

12. The Joint Report recognised that gathering intelligence is an integral part of policing, contributing to the functions of Police under the Policing Act, and that Police can take photographs as part of intelligence activities in support of those functions. However, the Joint Report expressed concern about how Police undertook photography for intelligence purposes in practice.

13. Police officers interviewed by the Inquiry identified intelligence gathering as one of the most common reasons for photographing members of the public. The Joint Report observed that:[80]

> broad surveillance through the use of Police cameras on mobile devices is carried out under the intelligence gathering function, but without necessarily serving a useful purpose for Police. For example, many of the officers we interviewed will take photographs of people they identify as 'suspicious' while out patrolling, but those photographs are held on the individual officer's phone until eventually deleted without ever being used to support an investigation.

14. The Joint Report's discussion of concerns about Police's approach to photography for intelligence gathering covered photographs of youth in public, as well as Police monitoring of gang activity and membership, suspicious activity and unknown individuals, and known offenders.[81]

15. The Joint Report concluded that Police officers need guidelines to help them properly comply with IPPs 1, 3 and 4 in particular.[82] It recommended that Police should develop a comprehensive policy on the use of photography of individuals for general intelligence-gathering purposes, with practical guidelines for complying with the Privacy Act, and specific guidelines in relation to young people.[83]

16. In relation to the threshold for taking photographs for intelligence purposes, the Joint Report noted that IPP 1 requires Police officers to assess whether taking a photograph is necessary for a lawful purpose connected with a Police function. Police must be able to articulate the *specific* purpose for which they are taking a photograph or video recording, and should be required to record the circumstances and considerations they relied upon to justify the taking of a photograph for intelligence purposes. The Joint Report proposed that an appropriate threshold, when photographing or video recording an individual for general intelligence purposes, is that 'Police must be able to articulate **a reasonable possibility, based on more than mere conjecture, that collection of the image will be relevant to a**

---

[80] *Joint Inquiry*, p 60.
[81] *Joint Inquiry*, pp 61-67.
[82] Issues concerning IPPs 3 and 4 are discussed in *Joint Inquiry*, pp 68-71.
[83] *Joint Inquiry*, pp 71-72, recommendations 1 to 3.

particular or likely investigation'. The Joint Report suggested factors Police officers could consider in making this assessment.[84]

Photography on private premises

17. Another issue addressed in the Joint Report, and that is relevant to the Bill, was Police photography on private premises where Police is lawfully present (for example, while executing a search warrant). The Joint Report concluded that the Search and Surveillance Act 2012 does not authorise Police to take photographs during the execution of a search warrant for purposes of intelligence-gathering that are unrelated to the purpose of the search authorised by the warrant.[85] The Joint Report commented that:[86]

> Lawful powers of entry should not be used as an opportunity to gather unrelated intelligence by taking photographs, as the Police's authority for entry onto private premises does not extend to this activity. Permitting general photography on private premises for any law enforcement purpose would undermine the constraints on Police search powers such as the particularity requirements of a warrant.

18. The Joint Report recommended that Police policy should include guidance on the limits of an officer's power to take photographs or video recordings when that officer is lawfully on private premises.[87]

Compliance notice

19. As noted above, the Inquiry found that Police practices regarding retention and deletion of photographs did not comply with the requirements of IPP 9 of the Privacy Act. As a result, in December 2021 (before the completion of the Joint Report), my Office issued a compliance notice to Police.[88] The compliance notice required Police to stop unlawfully collecting photographs and biometric prints from members of the public, particularly young people, and to delete unlawfully-collected material stored on their systems, including mobile phones. It also required Police to establish practices and procedures, including providing training to staff, to ensure unlawful practices do not continue.

Police response to the Joint Report

20. Police accepted the Joint Report's findings relating specifically to the photographing of rangatahi. Police also acknowledged the broader findings about Police practices

---

[84] *Joint Inquiry*, pp 67-68.
[85] *Joint Inquiry*, pp 62-63.
[86] *Joint Inquiry*, p 63.
[87] *Joint Inquiry*, p 72, recommendation 4.
[88] *Joint Inquiry*, p 109. The Compliance Notice is reproduced in Appendix 1C of the Joint Report.

and policies regarding photographing members of the public, but former Police Commissioner Andrew Coster said Police would:

> take some time to consider the broader findings, which have implications for Police's ability to effectively investigate and prevent crime. … [S]ome of the findings and recommendations present significant challenges to our staff being able to carry out their duties successfully.

Commissioner Coster stated that Police accepted that aspects of its intelligence-gathering policy required 'refinement, particularly in relation to retention and disposal of information that is no longer needed for the purposes of investigation.' He said Police had started a training programme 'to increase awareness of the need to appropriately manage images once they have served their investigative or prevention purpose.'[89]

21. Police also took action to meet the requirements of the compliance notice issued by OPC, which required Police to remedy breaches of the Privacy Act. Police has taken steps to improve training, policies and procedures about photographing the public, particularly young people, and to ensure that Police officers have a clear lawful purpose and rationale for taking photographs.[90] However, Police formally advised me in 2025 that it considers it is unable to complete the requirement to find and delete all unlawfully-collected information, due to the limitations of Police's information-management systems and the extremely large number of stored images. OPC is continuing to engage with Police to identify ways in which unlawfully collected information can be kept safe from inappropriate access and use until information management systems are put in place which will allow these images to be found and deleted.

[89] New Zealand Police, 'Police response to joint IPCA/OPC investigation', 8 September 2022.
[90] Office of the Privacy Commissioner, 'Police well on the way to compliance; one critical step remains', media release, 17 October 2024.

Appendix 4: *Tamiefuna v R*

1. *Tamiefuna* concerned the use of photographic evidence in relation to the right to be secure against unreasonable search and seizure.[91]
2. The appellant, Mr Tamiefuna, was convicted of one charge of aggravated robbery. He challenged the inclusion of photographic evidence used by Police to obtain this conviction. Mr Tamiefuna appealed a Court of Appeal decision which determined the photographic evidence was improperly obtained but declined to find the evidence should have been excluded from his trial.
3. The Privacy Commissioner was granted leave from the Supreme Court to intervene as an independent expert, as the appeal would have broad consequences for the interaction between information privacy, NZBORA and Police information-gathering powers.
4. The Supreme Court found both that the photographic evidence was improperly obtained and that it should have been excluded from Mr Tamiefuna's trial under section 30(4) of the Evidence Act 2006. A retrial was ordered.

Background

5. Mr Tamiefuna was a passenger in a car which was the subject of a routine traffic stop. The driver of the car was found to be unlicensed and the car was impounded. This required the occupants to exit the vehicle. A Police officer ran a National Intelligence Application (NIA) check for the occupants of the vehicle and discovered Mr Tamiefuna and the others had previous convictions relating to property offending.
6. Mr Tamiefuna and the others stood on the footpath while waiting to be picked up. The Police officer noticed there was a lot of property in the car, and became suspicious the property may have been stolen. The officer took photographs of the property and the car's occupants using his Police-issued smartphone. The information was collected and retained as the officer thought it might be useful in future. The officer added a note of his observations, with a photograph of Mr Tamiefuna, to the NIA.
7. The photographs were critical identification evidence at Mr Tamiefuna's trial, linking him to an aggravated robbery, as the clothing worn by Mr Tamiefuna in the photographs matched that of a man captured in CCTV footage at the scene of the offending.
8. There is no statutory authority authorising the taking of these photographs or the retention of one of those photographs on the NIA.

[91] For a summary of the Supreme Court decision, see Office of the Privacy Commissioner, '[Court decision summary - Tamiefuna v R [2025] NZSC 40]', 20 March 2026.

The majority decision in the Supreme Court

9. The majority in the Supreme Court (Winkelmann CJ and Ellen France and Williams JJ) considered that the Court of Appeal was correct to find that the photographic evidence was improperly obtained for the purpose of section 30 of the Evidence Act, as it was obtained by means of an unlawful and unreasonable search contrary to section 21 of NZBORA.

10. In determining whether Police taking photographs of a person in a public place, after the person was required to leave a car following a lawful traffic stop, was a search, the majority considered four key factors: the nature of the place, the use to which the information was put, the manner of collection and the nature of the information. In the particular circumstances of Mr Tamiefuna's case, the majority concluded that the taking of the photographs had been a search.

11. Significant weight was given to the fact that Mr Tamiefuna was only in a public place because he had been required to leave a vehicle. The majority stated that:[92]

> the fact Mr Tamiefuna's photograph was taken whilst he was on a public road is not a conclusive factor against the asserted reasonableness of his expectations of privacy. It remains important to preserve a sufficient zone of privacy for individuals. That in turn is a part of preserving the fundamentals of a liberal democracy.

12. While the manner of collection was not at the higher end of intrusiveness, the majority considered the use to which the information was put (in particular, its retention on the NIA) increased the level of intrusiveness. They also noted there were very few controls over the retention and use of Mr Tamiefuna's personal information. The majority considered the police power exercised was intrusive and for a very generalised purpose.

13. In assessing the nature of the information, the majority relied on the Joint Report's conclusion that photographs of individuals are sensitive biometric information. The majority added that the sensitivity of biometric information is recognised in the fact that statutory regimes are required to govern its use and collection.

14. As a result of these factors, the majority concluded that the Police officer's actions amounted to a search.

15. The majority further concluded that the taking and retention of the photographs was not lawful. Police are subject to statutory controls when conducting searches and it was not appropriate to extend their common law power to authorise a warrantless search for generalised intelligence gathering. In reaching this conclusion, the majority also considered the IPPs, which it viewed as relevant, though not decisive, in an analysis of section 21 of NZBORA and section 30 of the Evidence Act. The majority

---

[92] *Tamiefuna*, at [33].

found that Police failed to comply with IPPs 1, 3 and 9, and that this failure suggests the search was not reasonable, as a reasonable person would expect Police to comply with the IPPs.

16. Having concluded that the search was unlawful, the majority also concluded that it was unreasonable, having considered not only the unlawfulness but also the intrusiveness into privacy, the reason for the search and the nature of what was being searched. The majority commented that:[93]

> on the best view of the facts from the police perspective, the purpose of the intrusion on Mr Tamiefuna was to seize his image because of suspicious articles in the car. In addition, there was some reliance on the fact the group was travelling in the early hours of the morning and the occupants of the car all had criminal convictions. But the initial purpose evaporated relatively quickly and the goal became one of general intelligence gathering just in case something came up, a purpose which also meant the search here was an unlawful one.

17. The majority therefore found that that the photographic evidence was improperly obtained for the purposes of section 30 of the Evidence Act. Finally, the majority decided that excluding the evidence would not be disproportionate to the breach. There was a breach of an important right and an overextension of police powers (though the Court noted the police officers involved acted in good faith).

Police response to the decision

18. A May 2025 Police briefing to the Minister of Police stated that, while the Supreme Court judgment 'generally affirms Police's current operational practice, and no immediate response is required to ensure Police compliance, it confirms the status quo' (that is, the position following the earlier Court of Appeal decision and the Joint Report). Despite saying that no immediate response was required to ensure compliance, Police considered that the position following *Tamiefuna* was not sustainable and undermined Police's ability to carry out its functions. Accordingly, Police recommended urgent amendments to the Act 'to mitigate the uncertainties and risks that Police now faces in light of the SC Judgment'.[94]

---

[93] *Tamiefuna*, at [99].
[94] New Zealand Police, 'Urgent amendments to the Policing Act 2008 to address recent Tamiefuna Supreme Court Judgment outcomes and uncertainties', briefing to the Minister of Police, 13 May 2025.

Appendix 5: Addressing arguments for Part 1 of the Bill

1. In this appendix I set out what I understand to be the key arguments for Part 1 of the Bill and provide my responses to these arguments.

Restoring the previous legal position

Police's view

2. Police has argued that the combined effect of the Joint Report's recommendations and *Tamiefuna* has been to change or 'narrow' the law governing Police information collection. For example, the RIS states that Police has operated on the understanding that common law and statutory authorities:[95]

> allow Police to record images and collect information for any, or all, lawful purposes, including the purpose of general intelligence …, noting that at the point in time that it is collected, that the value of the information to a particular function may be unknown.

3. Further, the RIS states that, with regard to recording images in public, expectations of privacy were previously considered to be low.

4. The combined effect of the Joint Report and *Tamiefuna* is said to be a significant narrowing of Police's understanding of its ability to collect information for general intelligence purposes, and to record images in public places. The RIS notes that the Joint Report's view of what Police could record in private places was also narrower than Police had previously understood to be the legal position.

5. Part 1 of the Bill is therefore said to merely 'reaffirm' what Police describe as its 'longstanding' ability to record images and sound in public and to collect personal information for policing purposes, including intelligence.

My response

6. The Joint Report and *Tamiefuna* identified legal constraints on Police information-gathering, particularly for general intelligence purposes, although I explain below that these constraints are not as far-reaching as Police has suggested. However, neither the Joint Report nor *Tamiefuna* has changed the law. They have simply stated what the law is as it applies to specific scenarios, as is the role of the courts and independent regulators. The fact that Police has operated on the basis of a particular understanding of the law, or that certain Police practices may have been 'longstanding', does not mean that the law has been changed. These independent findings and decisions reflect relevant legal requirements in light of Police's increasing use of technologies to collect, store and retain information.

[95] RIS, p 10.

Removing unreasonable obstacles to Police intelligence-gathering

Police's view

7. Part 1 has been presented as a necessary correction of restrictions imposed by the Joint Report and *Tamiefuna*, which are said to have introduced significant obstacles to Police being able to effectively carry out its functions. In particular, Police states that its ability to collect information for general intelligence purposes will be significantly limited, with the result that Police will be less effective in keeping the public safe.

8. The Cabinet policy paper comments that:[96]

> The IPCA/PC Joint Report imposed constraints on Police's ability to record images in public for intelligence purposes, limiting collection only to circumstances where there is a reasonable possibility of a particular or likely criminal investigation. This means Police may not be able to take photographs of known offenders who have changed their appearance, or unknown individuals associating with gang members, or individuals involved in suspicious activity. These photographs may be taken for intelligence purposes supporting a Police function, as opposed to a known investigation.

9. The Cabinet paper also argues that '*Tamiefuna* solidified this constrained position and signalled a high bar for when images can be recorded in public places.'[97] The RIS for the Bill further states:[98]

    - Prior to *Tamiefuna*, a photograph or video of a person in public was not generally treated as a search under section 21 of NZBORA, because people in public places lacked a reasonable expectation of privacy.
    - The Supreme Court in *Tamiefuna* found that a 'zone of privacy' can exist in public places.
    - The Supreme Court found that whether Police photography constitutes a search is not limited to the subject's reasonable expectations of privacy at the time of the search but also depends on the whole interaction with Police, including the subsequent use of the information.
    - The *Tamiefuna* judgment also found that Police does not have a common law power to conduct warrantless searches for generalised intelligence purposes.
    - Consequently, *Tamiefuna* cast considerable doubt on Police's ability to take photographs in public for general intelligence purposes, and more broadly to collect personal information for such purposes.

---

[96] 'Amendments to the Police Act 2008', paper to Cabinet, 2025, p 3.
[97] Amendments to the Police Act 2008', paper to Cabinet, 2025, p 3.
[98] RIS, p 12.

10. Police argues that the Joint Report and *Tamiefuna* have had operational impacts on Police in two main ways:[99]

    - Police now has guidelines that taking photographs of the public can be lawful for intelligence purposes, but only where there is a reasonable link to a particular or likely criminal investigation, which Police describes as a narrower interpretation of intelligence purposes than that previously applied.
    - Frontline Police staff are said to be uncertain about collecting information for intelligence purposes or whether recording an image will amount to a search (reasonable or otherwise), so they are unsure whether their actions will be lawful. As a result, they may be reluctant to collect information or record images.

11. These operational impacts, according to Police, have resulted in fewer images being recorded and less personal information being collected. Police considers that such data constraints will hamper Police's ability to detect and prevent crime.

12. Throughout OPC's engagement with Police about the policy for Part 1 of the Bill, it has been difficult to get a clear indication from Police of the scenarios in which they believe Police officers are constrained by the Joint Report and *Tamiefuna*. It appears that a key concern of Police is with its ability to monitor and take action against gangs. However, the broad scope of the powers conferred by this Bill mean that they can be used for purposes well beyond anti-gang activity.

My response

13. I do not accept that the constraints on Police information-gathering are as great as Police has argued. If there are areas in which Police is unduly constrained, these should be addressed in a targeted way, not through a broad authorising provision.

The Joint Report

14. Police appears to be particularly concerned about the implications of the threshold for Police photography for intelligence-gathering set in the Joint Report. It is important to note, first, that the Joint Report did not question the important role of intelligence in Police investigations, or that information (including photographs) can lawfully be collected for intelligence. The Joint Report stated that 'Police intelligence gathering through the collection of photographs, video recordings and biometric prints is a key component of many investigations, as this intelligence informs investigative decisions and helps to solve criminal investigations'.[100]

15. However, the Joint Report was concerned at the extent of Police photographing of individuals that was taking place under the banner of intelligence-gathering, and the inability of many officers to articulate the reasons why individuals were being

[99] RIS, pp 13-14.
[100] *Joint Report*, p 60.

recorded in particular instances. The Joint Report concluded that officers needed guidelines about the circumstances in which the collection of photographs was necessary, and needed to be able to articulate the purpose for which information was being collected.

16. With regard to the threshold for recording for general intelligence purposes proposed in the Joint Report, this did not require a definite link to a current investigation. It required that Police must be able 'to articulate a reasonable possibility, based on more than mere conjecture, that collection of the image will be relevant to a particular or likely investigation.' In other words:

    - There need only be a 'possibility' of relevance (though the extent of the possibility, and Police's basis for believing the possibility exists, must be reasonable in the circumstances).
    - The photograph does not need to be relevant to a specific investigation that is already under way – it could be relevant to an investigation that, in the circumstances, seems likely to take place.

17. Police has incorporated this threshold into its guidance on photographing and videoing members of the public,[101] but I recognise that Police considers the threshold to be impractical or unrealistic. If Police can make a clear case that it needs additional authorisation to collect information, this should be done in a targeted way, with clear limits.

Tamiefuna

18. It is important to be clear that the Supreme Court in *Tamiefuna* did not make a general finding that Police cannot record individuals in public places for intelligence purposes. *Tamiefuna* must be viewed in relation to the specific facts of the case, and the conclusions reached by the Court on the basis of those facts.

19. First, Mr Tamiefuna was only in a public place because he had been required to leave the car in which he was travelling as a result of the exercise of Police powers. This is quite different from the situation of a person who is in a public place voluntarily.

20. Second, in the specific circumstances, taking account of a number of factors, the Court concluded that the taking of a photograph was a search, and therefore NZBORA applied to it. In other circumstances, Police photographing an individual in public will not be a search, but will be subject to the protections in the Privacy Act.

21. Third, in this case the Police officer was not investigating a crime, but was taking a photograph for an unspecified future purpose. The Court found that there is 'no free-

[101] New Zealand Police, *Photographing and Videoing Members of the Public*, version at 4 July 2025, p 12.

standing warrantless search power for intelligence gathering',[102] either at common law or in statute. It is only because the photograph was found to be a search in the first place, however, that consideration of warrantless search powers became relevant. The Court **did not find**, as summarised in the RIS, 'that there is no common law police power to photograph people for "intelligence gathering" purposes'.[103]

22. Given this accumulation of very specific factors in *Tamiefuna*, I do not believe the decision is as constraining as Police has maintained.

No evidence of a problem

23. The RIS for the Bill acknowledges that there is no specific evidence of an operational risk to Police's ability to carry out its functions, partly due to the recency of the *Tamiefuna* decision. Despite this lack of evidence, the RIS argues that an approach where Police's authority is tested case by case 'is not operationally feasible or sustainable'.[104] The RIS also acknowledges that 'There is limited information about the size and scale of the information gathering problem and the proportionality of the proposed solutions.'[105]

24. I simply note in response that, in the absence of clear evidence of a specific and urgent problem, it is important to take the time to ensure that an appropriate response is developed and is subject to wide public consultation.

Providing certainty for frontline Police

Police's view

25. As already noted, Police has argued that the Joint Report and *Tamiefuna* have created uncertainty for frontline Police officers about their ability to collect personal information for intelligence purposes and to record images in public places. Police maintains that this uncertainty is leading to the collection of less information and fewer images than before. The RIS states that, in the absence of clear authority, Police's ability to record information in public will require a case-by-case assessment of whether the circumstances may amount to a search, which is 'overly complex for a dynamic environment' and may need to be undertaken by thousands of staff multiple times on each shift.[106]

My response

26. I do not believe the Bill will provide the certainty Police is seeking. Police officers will still need to make decisions about their legal authority to collect information, and

---

[102] *Tamiefuna*, at [72].
[103] RIS, p 12.
[104] RIS, p 6.
[105] RIS, p 7.
[106] RIS, p 24; see also p 13.

those decisions are still likely to be challenged in the courts, given the potential impacts on privacy and other human rights.

27. In particular, officers will need to assess whether their collection of personal information is for one of the purposes set out in new section 45A. If they are considering collecting information for an intelligence purpose, they will need to consider:

    - whether the collection *is* in fact for an intelligence purpose and, if so, whether that purpose is connected with a Police function or activity, and which function or activity that is
    - whether the collection will or may support the Police in performing the function or activity in question
    - whether the collection will involve making a 'continuous' sound or video recording solely for an intelligence purpose and, if it does, whether making the recording solely for that purpose is reasonable and what duration of recording is reasonable in the circumstances.

28. This set of decisions arguably involves at least as much case-by-case judgement and potential uncertainty as the status quo.

29. The RIS acknowledges that 'Clear guidance will be needed for appropriate settings for taking images in private places. This **may still require complex assessments for frontline officers**, however guidance is feasible to implement through operational policy and increased access to updated training' (emphasis added).[107] I believe the same point is true of the Bill's authorisations for collection in public places. I also note that guidance is already an option for assisting frontline officers with making complex assessments and managing uncertainty.

30. Further, the RIS notes that the courts will still be able to assess whether Police actions constitute a search in the circumstances, and whether the search is unreasonable. The RIS maintains that the starting point for a court's assessment will be different. However, the fact remains that officers will still need to consider whether their actions may breach the right to protection against unreasonable search and seizure, and courts may still reach decisions on the unlawfulness or unreasonableness of Police information-gathering in any particular case.

31. I also note that the Bill seeks to provide certainty for Police authorisations, but provides no certainty with regard to safeguards. Police has argued that case-by-case assessments by Police officers are undesirable when it comes to the exercise of Police powers. At the same time, Police appears to view case-by-case assessments as desirable for the application of safeguards associated with those powers. For example, the RIS states that legislative protections for the collection, use and

[107] RIS, pp 23-24.

retention of images of children and young people is not a preferred option in part because 'legislating special protections will remove the ability for Police to consider the necessity of collecting and retaining this information on a case-by-case basis.'[108] Elsewhere, the RIS comments that legislative prescription of safeguards would likely compromise the benefits of the proposed amendments, reduce Police's ability to respond flexibly to developments, create complexity and have disproportionate compliance costs.[109] In my view, this approach to non-prescribed safeguards risks continuing review by the courts.

Giving Police the same right to record images as the general public

Police's view

32. Police has argued that the restrictions imposed by the Joint Report and *Tamiefuna* should be removed because they leave 'the Police with fewer rights than the general public to record images'.[110] This argument is based on the belief that Police previously 'had the same authority as members of the public who may take images in public places'.[111]

My response

33. I do not accept this argument, for a number of reasons.

34. First, as discussed above, *Tamiefuna* does not recognise a general right not to be recorded by Police in public places. It recognises only that, in particular circumstances which amount to a search, Police must ensure any recording is collected lawfully, as required by NZBORA (which applies to public bodies, not to ordinary people).

35. Second, public and private entities, including the Police, are required to comply with the IPPs when collecting personal information, regardless of where the collection takes place. That means that any organisation[112] taking photographs must only take photographs of identifiable individuals when it is necessary to do so for a lawful purpose, regardless of whether the photography occurs in a public or a private place.

36. It is true that members of the public will generally not be in breach of the Privacy Act if, for example, they take photographs of street scenes that include other people. However, this is not because the photographs are taken in a public place. It is because the Privacy Act includes an exception for an individual collecting and holding personal information solely for that individual's personal or domestic

---

[108] RIS, p 35.
[109] RIS, pp 27-28.
[110] Policing Amendment Bill, General Policy Statement.
[111] RIS, p 11.
[112] Other than the limited number of entities that are excluded from the Privacy Act's coverage. For example, the news media is generally able to take photographs (and otherwise collect information) without breaching the Privacy Act due to an exception in Privacy Act 2020, s 8(b)(x).

affairs.[113] This exception does not relate to whether the collection takes place in a public or a private place – an individual is equally free to take personal photographs at a private party, for example.

37. Third, individuals can reasonably expect some privacy in public places.[114] In particular, while individuals may reasonably expect to be casually observed while in public, they do not expect to be subject to close, targeted or prolonged scrutiny, or targeted recording of their appearance, actions or movements. Individuals going about their business in public can reasonably expect that they will not have their images recorded, stored and potentially used by law enforcement agencies without those individuals' knowledge or consent, unless there is a good reason to do so.

38. Fourth, members of the Police do not occupy the same position in society as members of the general public. Police exercises coercive powers on behalf of the state, and these powers are not available to individuals or to most other organisations. The social contract under which Police operates involves these powers being not only authorised by law but also exercised in accordance with limits set by the law. It is a well-accepted principle in liberal democracies like ours that law enforcement agencies should be subject to constraints and oversight to ensure that their powers are exercised in a way that is consistent with democratic rights and norms.

39. While there is generally a lower privacy interest when people are in public places, a broad power to record people in public will raise concerns about public and individual surveillance if it is not subject to clear limits. Exercising the power may also amount to a search in particular cases. A Ministerial Policy Statement in relation to the intelligence and security agencies states:[115]

> The New Zealand public reasonably expect that activities conducted in public places are not generally subject to surveillance by the state and that agencies with surveillance powers and capabilities will use them with restraint. Privacy concerns might arise from those who are the subject of surveillance (should the surveillance become known to them), and others who interact with, or come into close proximity with, people while that are subject to surveillance. Whether there is 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.

---

[113] Privacy Act 2020, s 27.
[114] Arguments for recognising privacy in public places are discussed, in relation to tort law, in Nicole Moreham, 'Privacy in Public Places', *Cambridge Law Journal*, vol 65, 2006, pp 606-635.
[115] Ministerial Policy Statement, 'Conducting surveillance in a public place', issued by the Minister Responsible for the Government Communications Security Bureau and the New Zealand Security Intelligence Service, March 2025, para 7.

Allowing Police to use body-worn cameras and other devices

Police's view

40. Police has argued that the proposed amendments are necessary to future-proof Police information-gathering powers as Police continues to adopt new technologies. In particular, I understand that the potential adoption of body-worn cameras (BWCs) by Police is a significant factor behind the proposed authorisation in the Bill of recording of images and sound in public places.

41. The RIS notes that:[116]

> The methods and channels by which Police collects personal information have changed as a result of technological developments. … Some of this personal information may have an unknown specific intelligence use at the time of collection. …
>
> Technologies include use of body worn cameras, mobile phones, high-resolution cameras, drones, Police Eagle helicopter footage, Closed Circuit Television (CCTV) camera networks in urban and rural locations, Automatic Number Plate Recognition (ANPR), retail camera convergence platforms (for example, Auror and SaferCities), online open-source search tools, waste-water testing, and geospatial and geolocation tools. Separately, and in combination, these tools enhance Police's ability to gather information to support Police to deliver its policing functions and duties.

42. The RIS also states that the proposed amendments will allow Police to use BWCs to record continuously in public and private places for a range of purposes, rather than officers needing to make a decision to turn the cameras off or on depending on what is happening at the time. The RIS notes that 'images primarily collected [using a BWC or other continuous recording device] for officer safety and integrity purposes, may also be required for other policing purposes such as crime prevention or investigative purposes.'[117]

My response

43. As a general comment, I believe that the developing ability of technologies to collect and analyse huge amounts of personal information is a reason to introduce greater, not lesser, protections for individual privacy. Concern about technological capacity for surveillance was one factor behind my recent decision to issue a code of practice under the Privacy Act governing biometric processing, such as the use of FRT.[118]

---

[116] RIS, pp 29-30.
[117] RIS, pp 14, 30.
[118] Biometric Processing Privacy Code 2025.

44. In relation to BWCs specifically, I have stated publicly that it is possible to use them within the regulatory framework of the Privacy Act.[119] BWCs certainly have significant implications for privacy, but compliance with the Privacy Act allows them to be used in a way that mitigates and manages privacy risks.

45. A key requirement is to clearly establish the lawful purpose(s), connected with Police's functions, for which BWCs are to be used. These purposes are likely to be officer safety and integrity. So long as Police can establish that the use of BWCs for those purposes is reasonably necessary, it is free to collect, hold and use personal information for those purposes. If Police wishes to use or disclose the footage collected with a BWC for a purpose other than officer safety and integrity (for example, for an investigation), there are a number of exceptions in IPPs 10 and 11 that allow them to do so. In particular, Police could use the BWC footage for a purpose other than the original purpose of collection if they have reasonable grounds to believe the use of the information is necessary for the maintenance of the law (including preventing, detecting, investigating, prosecuting and punishing offences) or to prevent a serious threat to individual or public health or safety.[120]

46. I have shared this view with Police, and the Government has acknowledged, in responding to a recent petition about Police use of BWCs, that use of BWCs is enabled by the Privacy Act. The Government has also stated that this Bill will further clarify Police's ability to record using BWCs in public, including continuous recording for officer safety and integrity purposes.[121]

47. While I do not believe that legislation is needed to allow Police to use BWCs, I would be happy to support Police in developing a specific legislative framework for Police use of BWCs, if Police feels this would provide greater operational certainty and safeguards.

---

[119] 'Privacy Commissioner speech to the Police Association Annual Conference', 16 October 2025.
[120] Privacy Act 2020, s 22, IPP 10(1)(e)(i) and (f).
[121] 'Government Response to the Petition of Hakepa of the *Te Wahine Ora o Hakepa Foundation* on Uniformed Sworn Police Officers to Wear a Body Camera', paper for the Cabinet Legislation Committee, 2026; *Government response to the Petition of Hakepa of the Te Wahine Ora o Hakepa Foundation on Police wearing body cameras*, paper presented to the House of Representatives, 2026.