
***Joint inquiry by the Independent Police Conduct Authority and the
Privacy Commissioner into Police conduct when photographing
members of the public***

September 2022

He Karakia

Whiti, whiti ora

Whiti ora ki te tipua

Whiti ora ki te tawhito

Whiti ora ki te kāhui ariki

Whiti ora tāwhiwhi atu

Ki a koe e Rongo

E Rongo whakairia ki runga

Tūturu o whiti

Whakamaua

Kia tina! Tina

HAUMI E

Table of contents

1 Introduction.....	6
Executive summary.....	6
General findings.....	7
Lawful purposes – IPP 1.....	8
Taking reasonable steps to inform the person of the purpose – IPP 3	14
Obtaining consent – IPP 4.....	15
Protections for youth.....	16
Use of photographs	17
Retention and destruction.....	17
List of Recommendations	18
Background to this Joint Inquiry.....	24
Terms of reference	25
Unconscious bias	27
The role of the Independent Police Conduct Authority Mana Whanonga Pirihi- mana Motuhake.	27
The role of the Privacy Commissioner Te Mana Mātāpono Matatapu	28
The role of Police Ngā Pirihi- mana o Aotearoa.....	29
Methodology	29
Limited available data.....	30
Overview of the rangatahi incidents	31
Rangatahi uplifted and photographed without consent or explanation	32
Reports of rangatahi being stopped and photographed without consent	33
Rangatahi photographed after he refused consent and explained his rights to Police	33
2 Relevant legislative framework	33
Policing Act 2008	35
Search and Surveillance Act 2012.....	37
Youth-specific protections.....	38
Special protections due to vulnerability.....	40
Limits on power to arrest	41
Privacy Act 2020	41
Privacy Act principles as constraint on Police action	44
Collection principles	46
Storage, access, retention and use principles	53
3 Consistency of Police practice with relevant law	55

Introduction	55
Understanding of NZBORA	55
Outline of this section.....	56
A issues relating to collection by photography and other identifying personal information	56
Introduction and initial observations	57
General policing scenarios involving taking photographs (collection).....	59
Findings – IPP 1.....	67
Findings – IPP 3.....	68
Findings – IPP 4.....	70
Findings – IPP 1.....	75
Findings – IPPs 3 and 4	76
B Police use of photographs	90
C Issues relating to storage, security, retention and disposal.....	91
Mobile device issues - storage and retention	92
D Application to the rangatahi complaints.....	95
Incident one.....	96
Incident two	97
Incident three	99
Incident four	100
Incident five.....	102
Whānau views	103
Consideration of tikanga	104
4 General Findings	106
Gaps in policies and lack of guidance	106
Lack of awareness of the Privacy Act 2020	107
Trust and confidence.....	108
5 Actions taken during Joint Inquiry and next steps	109
Compliance notice issued to Police.....	109
Police actions	109
Kanoahi ki te Kanoahi and Hui	110
Appendix 1 – Documents	112
A Police policies reviewed during the Joint Inquiry.....	112
B Terms of reference	114
C Compliance notice.....	117
Appendix 2 – About	133
The Independent Police Conduct Authority Mana Whanonga Pirihihi Mana Motuhake	133

Who is the Independent Police Conduct Authority?	133
What are the Authority's functions?	133
The Privacy Commissioner Te Mana Mātāpono Matatapu.....	134
Who is the Privacy Commissioner?	134
What are the Commissioner's functions?	134
About this report.....	135
Acknowledgement	135

1 INTRODUCTION

Waiho, mā te whakamā e patu!¹

The above pēpeha belongs to the oral traditions of Ngāti Awa, an iwi located in the Eastern Bay of Plenty. It describes an incident involving Te Tahi-o-te-rangi in which the actions of some of the people to abandon him on Whakaari/White Island were unsuccessful and brought whakamā or shame to the people.

In the context of this report, “waiho, mā te whakamā e patu” speaks to the whakamā that rangatahi and whānau members experienced as a result of Police photographing rangatahi without following correct procedure. In order to restore balance, the whakamā needs to shift from whānau to Police in acknowledging the impacts of their actions.

The Office of the Privacy Commissioner (OPC) and the Independent Police Conduct Authority (IPCA) acknowledge Ngāti Awa for giving permission for the pēpeha to be used for this report.

Heoi anō, e Ngāti Awa, ko tēnei te Mana Mātāpono Matatapu māua ko te Mana Whanonga Pirihihihi Motuhake e mihi ana ki a koutou.

EXECUTIVE SUMMARY

1. This joint inquiry was prompted after whānau reported Police photographing their rangatahi in circumstances they considered unfair or unjustified. Subsequent media coverage led more people to report similar experiences. As a result, IPCA and OPC undertook a joint investigation beginning in March 2021, to examine Police photography of persons who have not been detained for the suspected commission of an offence.
2. In the course of the joint investigation, we considered five individual complaints in which whānau claimed Police had either uplifted rangatahi for care and protection reasons but had then photographed them in relation to a criminal investigation or had stopped their rangatahi in public places and photographed them without their consent. Two of these complaints were historic in nature and, given the time that had passed and the lack of records or other available information, we were unable to establish the facts or make any findings.
3. In relation to the three remaining complaints, we found that Police were not justified in photographing the rangatahi, as the photographs were not necessary for a lawful policing purpose. We also found that, in these incidents, Police had not properly sought consent from the rangatahi or their parents or caregivers before taking the photographs, and had not adequately explained why the photographs were being taken and what they would be used for.

¹ No Ngāti Awa tēnei pēpeha. The full pēpeha is “Waiho mā te whakamā e patu. Waihi hai kōrero i a tātau kia atawhai ki te iwi – Leave them for shame to punish. Let us acquire fame by being merciful.” See Hirini Moko Mead and Neil Grove *Ngā Pēpeha a ngā Tipuna: The Sayings of the Ancestors* (Victoria University Press, Wellington, 2001) at 418 (pēpeha 2624).

In one incident, we found Police had wrongly threatened to arrest a rangatahi if they did not consent to being photographed.

4. Our interviews with officers in relation to these complaints suggested that there were broader questions about the appropriateness of current Police practice in this area. We therefore extended the inquiry to an examination of the way in which photographs or video recordings of members of the public (referred to in the remainder of this report as “photography”) are being taken, used and retained in a variety of policing contexts. We interviewed a range of front-line officers and managers in four Police districts about their own practice, whether this was representative of general practice and their understanding of the law and Police policy.
5. During this broader investigation, we also found that Police were regularly taking duplicate sets of “voluntary” fingerprints from youths who ended up in Police custody for suspected offending and retaining them for a longer period than permitted by the regime for compulsory prints under the Policing Act. We have included consideration of that practice within the scope of this report.

General findings

6. Police use of photography depends on the relevant powers that are available in each policing situation and the respective constraints that apply.² Where Police are taking a photograph of a person or persons under any statutory power (which relate primarily to a search scene or a person in custody), they need to comply with the relevant specific legislative threshold and applicable constraints. The Privacy Act should not be used as a basis for taking photographs which circumvent those constraints.
7. Where Police take photographs of people in contexts outside those specific statutory situations, officers must comply with the Privacy Act and the information privacy principles (IPPs) within it, taking into account the status of digital photographs as sensitive biometric information.
8. The way that the privacy principles operate as a constraint depends on the policing purpose and the particular circumstances that Police encounter. IPPs 1- 4 are the source of the privacy safeguards that apply when Police are taking photographs. These dictate the need for a lawful purpose and set out the expectation that the person will be informed at the time of the purpose for the photograph and their consent sought.
9. The privacy safeguards are flexible and Police can depart from these where necessary. For example, the Police can use covert photography where this is justified and proportionate to their policing purpose.
10. Overall, we have found aspects of both Police policy and practice are inconsistent with this framework and breach individual rights.
11. Officers are routinely taking photographs when it is not lawful for them to do so. Many are under the misapprehension that if they obtain the consent of the person photographed, this gives

² Refer to table in section 2.

them the necessary authority, even though they do not have a lawful purpose in terms of the Privacy Act.

12. When they do take photographs in circumstances that comply with the information privacy principles, many officers appear to have very little understanding of the law relating to the retention of these photographs under the Policing Act or the Privacy Act. As a result, thousands of photographs of members of the public are kept on the mobile devices (mobile phones, tablets etc) of individual officers or, if transferred to the Police computer system, not destroyed after there is no longer a legitimate need for them.
13. Fundamentally, these problems have arisen because Police as an organisation have not developed appropriate training, guidance or policies to enable officers to use their powers and collect personal information effectively and lawfully. In particular, their roll-out of technology and mobile devices has not been accompanied by sufficient training and support, which has resulted in inconsistent and improper practices.
14. We have therefore **concluded** that Police policy, procedures and training need to be significantly revised and enhanced to reflect that photographs are sensitive biometric information and to ensure that, when Police are photographing people, they are doing so only when either there is a specific statutory authorisation or there is full compliance with the information privacy principles.³

Lawful purposes – IPP 1

15. IPP 1 stipulates that, whether or not a person consents, personal information about them, in this case a photograph, should be collected only when there is a lawful purpose for doing so and the collection of the information is necessary for that purpose. Individual officers must ultimately make a judgement call about purpose and necessity, as they do for other elements of policing. For this reason, it is imperative that Police policy provides clear and practical guidance for frontline staff about the circumstances in which a lawful purpose for taking a photograph applies. It does not presently do so.
16. We have considered the variety of contexts in which officers may see photography of members of the public as providing benefits for policing. The report outlines whether photographs in each context are likely to have a lawful purpose and, if so, what thresholds for taking them should be incorporated into Police policy.
17. The thresholds we recommend in this report provide a link between the purpose for which a photograph is taken and the assessment of whether that photograph is a necessary collection for that lawful purpose. The thresholds provide a framework for that analysis.

Intelligence gathering

18. We understand that intelligence gathering is an integral part of policing that directly contributes to functions required of New Zealand Police under section 9 of the Policing Act 2008. This report

³ See Recommendations [22 – 23].

therefore does not preclude the gathering of photographs, including of members of the public, as part of intelligence activities to support Police's statutory functions. However, the report finds Police need to ensure that it is collecting this sensitive biometric personal information in a way that is limited to only what is **necessary** to support the purpose for which the personal information is collected.

19. Traditionally police gathered intelligence through taking detailed notes or "intel notings". Today Police intelligence gathering through photography is commonplace. Digital technology now allows Police officers to take thousands of photographs using mobile phones and other mobile devices. However, this has not been matched with policy guiding Police officers on how to use the technology appropriately to collect this sensitive personal information. As such there is a risk that ease and efficiency leads to indiscriminate collection.
20. Photographs of individuals are not, and cannot be treated as, the same as "intel notings". A digital photograph is not a description of an individual, it is an exact biometric image of that individual and no other. As such, it is sensitive personal information and must be treated accordingly. It is also capable of being analysed using facial recognition technology and other digital techniques which makes it even more important that the information is being collected, used, retained and stored lawfully.
21. Our joint inquiry observed that officers regularly photograph individuals involved in activity deemed "suspicious". They also told us that they take routine photographs to: collate information on gang members and their associates; keep "tabs" on other known offenders; record unknown people who are associating with known offenders; and record changes in the appearance of known offenders.
22. In our view, the benefits of photography for these sorts of intelligence purposes are over-stated. One reason for this is that, unless photographs are linked to a particular investigation or likely investigation, Police lack the systems to organise and categorise them. Further, unless officers take steps to save the photograph somewhere alongside notes on the relevance and significance of the photograph, it is difficult for them or other officers to look back at those photographs and gather any useful information. Thus, unless photography for intelligence purposes is linked to a particular circumstance that might require investigation, it is likely to result in the systematic over-collection of personal information in breach of IPP 1. Indiscriminate collection of the exact biometric image of a person because it "may prove useful" also means law-abiding members of the public may have their image stored on police systems without the ability to exercise their rights to challenge that collection.
23. We therefore **recommend** that Police policy should provide instruction to officers that when photographing or video-recording an individual for general intelligence purposes the officer 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.**⁴

⁴ See paragraph [346] and recommendation 1.

Criminal investigations

24. Police commonly take photographs for the purpose of a criminal investigation in three situations. First, they take crime scene photographs for evidential purposes. This is covered by existing Police policy, which in our view is fit for purpose, although it is important that Police take into account the privacy rights of the individuals captured inadvertently in crime scene photographs.
25. Secondly, they take photographs (or more commonly video recordings) of victims and witnesses at crime scenes. Again, we think use of photography in this area is largely unproblematic and is particularly important for evidential purposes in family harm incidents.
26. We therefore **recommend** that Police policy should confirm that Police may take photographs of a crime scene, including victims and witnesses at it, provided that the privacy of those unrelated to the incident is taken into account. This could be addressed by the redaction of images that include individuals who are not relevant to the investigation.⁵
27. Thirdly, and perhaps most commonly, officers take photographs when they are investigating a specific reported incident and come across individuals who they suspect may have been involved. The inquiry has found there is a risk that Police practice is potentially overly broad and that there is a need to develop an appropriate threshold to ensure that photographs and recordings are justifiable.⁶
28. The officers we interviewed explained they took photographs of suspects either to confirm their participation in the offending, or to rule them out. Officers explained that the intention is to capture the suspect and their clothing as they appear at the time, and to show the photographs to an eyewitness or compare them to any CCTV footage of the incident.
29. Photographing members of the public to either confirm or exclude their involvement in alleged offending is, in theory, a practical and useful Police investigative technique. However, it is casting the net too widely for officers responding to a report of an offence in a particular location to indiscriminately photograph any person who may be in the general vicinity. For example, where Police have descriptions of alleged offenders, we do not consider that it would be appropriate for them to photograph an individual who clearly does not match the descriptions, unless they observe something other than mere proximity to the crime scene that potentially links the person to it.
30. We therefore **recommend** that Police policy should provide that photographs of potential suspects for investigative purposes may be taken only if there is **a reasonable possibility, based on more than mere conjecture, that the suspect could be relevant to a specific investigation that is currently underway.**⁷

⁵ See paragraphs [375]-[379] and recommendation 8.

⁶ See paragraphs [386]-[390].

⁷ See paragraph [386] and recommendation 5.

Traffic checkpoints and other traffic stops

31. Photographs are commonly taken at traffic checkpoints and other traffic stops when an infringement notice is being issued, so that there is proof of the identity of the driver if the notice is contested. However, it is not appropriate that this be done as a matter of routine. It will be a lawful purpose only when the driver's identity is not able to be ascertained in other way (e.g. by examination of the driving licence and accompanying photograph). We **recommend** that Police policy should make that explicit.⁸
32. However, we are aware that traffic stops are also employed as an opportunity to gather intelligence, especially about gang members. This is generally unlawful. The power to stop under the Land Transport Act may be used only for Land Transport purposes. Depending on the circumstances, photographs for intelligence or investigative purposes may occasionally be lawful if the necessity for them arises after the stop, but a stop that is simply a pretext to follow up an unrelated and pre-determined line of inquiry by way of a photograph is unlawful.
33. We therefore **recommend** that Police policy should state that checkpoints and other traffic stops may not be established primarily for the collateral purpose of collecting photographs or other personal information.⁹

Protests and other large gatherings

34. The extent to which officers may take photographs at protests and other large gatherings is currently addressed by Police in the *Unlawful Assembly and Riot* policy and the *Demonstrations* policy.
35. The former allows photographs on the approval of the Operation Commander for investigative purposes where the gathering reaches the threshold of a riot or unlawful assembly, both of which are by definition unlawful. We see no need for any change to that policy.
36. The latter states that Police photographers should be deployed only on the authority of the Operation Commander where the prevailing circumstances indicate "*a probability of disorder*". In contrast, officers we interviewed spoke of photographing protesters for more general intelligence purposes – that is, to enable them to be identified for future events.
37. We think that the *Demonstrations* policy sets the bar for capturing demonstrators' images too high. We **recommend** that it should be revised to allow officers to photograph demonstrators where they believe, based on some articulable facts, that there is a *reasonable possibility* of disorder occurring and that the photographs may assist in providing evidence, identifying suspects, protecting against unjustified complaints, or exerting a controlling influence on Police behaviour.¹⁰ We also **recommend** that the policy make clear that photographing demonstrators for no reason other than their presence in an otherwise lawful and peaceful demonstration, with the aim of identifying them in potential future demonstrations, is not a lawful Police purpose.¹¹

⁸ See recommendation 9(d).

⁹ See recommendation 9(b).

¹⁰ See recommendation 10(a).

¹¹ See recommendation 10(b).

Issuing notices and proof of service

38. Officers we interviewed said that they routinely photographed members of the public when serving documents on them, such as a summons, an infringement notice, or a trespass notice. This is done so that if individual later denies being served, Police have photographic evidence establishing service.
39. We agree that this is a necessary policing purpose. We **recommend** that as part of their general review, Police ensure that their policy reflects this.¹²

Responding to monitoring of Police by members of the public

40. Some officers we interviewed said that they often turned their own cameras on members of the public who started recording them. These officers' attitude can be summarised as: *"If they can do it to us, we can do it to them"*. Some officers described how these people did not like having cameras on them and would often then stop their own recording. It was clear that the officers' intention in turning their camera on these members of the public was to get them to stop recording them while they try to do their jobs.
41. While only a relatively small number of officers described engaging in this conduct, the practice appeared to occur frequently enough to concern us. The lack of understanding of any boundaries on their rights as Police to photograph members of the public is particularly concerning.
42. However, persons acting in their capacity as Police officers are more restricted than the general public in what they can do. They are not justified in turning their cameras on someone simply because they find the experience of being photographed or video recorded by a member of the public to be annoying, bothersome, or a distraction. Their feeling of annoyance does not provide a lawful policing purpose.
43. We **recommend** that Police policy should make clear that officers are justified in photographing a member of the public who is recording them only if they have reasonable grounds to believe the person's behaviour poses a threat or is obstructing them in the performance of their duty.¹³

Where a youth is detained in a Police station on suspicion of offending

44. Where a youth (or adult) has been detained for committing an offence and is in Police custody, Police have express powers to take identifying particulars, including photographs and biometric prints, under section 32 of the Policing Act 2008. However, because charges against youth are frequently resolved through the Youth Courts without resulting in a conviction, photographs and prints collected by Police using powers under the Policing Act are generally unable to be retained. That is because section 34 of the Act requires such photographs and prints to be destroyed as soon as practicable after a decision is made not to commence a prosecution, or the prosecution does not result in a conviction or other outcome that authorises continued storage.

¹² See recommendation 11.

¹³ See recommendation 12.

45. In order to circumvent this statutory restriction, officers we interviewed reported that, following arrest or detention, they not only took a formal custodial photograph under section 32 on the custody unit digital camera, but sometimes supplemented this with a duplicate set of “voluntary” photographs on their mobile devices. These would then be retained on the officers’ mobile devices, or uploaded to the cloud or the Police database, used for Intel notings, or emailed to the officer’s computer. What was done with the second set of photographs was left to be determined by the officer taking the photograph.
46. We also found that there was a widespread practice of Police obtaining what they referred to as a duplicate “voluntary” set of biometric prints from youth. Police considered that they were allowed to obtain the duplicate “voluntary” set until the youth or their parent or caregiver expressly asked for them to be destroyed, without being subject to the statutory destruction requirement that applies to the compulsory set.
47. We were told that the underlying rationale for taking duplicate photographs and biometric prints is that it has been an important tool in reducing youth offending, in that youth are less likely to offend if they know that their photographs and fingerprints are on file and that they will be able to be identified if they commit a crime. We were provided with no evaluative material to support this claim. Even if such an evidential basis for this rationale exists, that is not a reason for a practice which is clearly not permitted by law; Police should rather seek an amendment to the Policing Act.
48. The Acting Privacy Commissioner issued Police with a **compliance notice** under IPP 9 (retention of personal information) in December 2021, requiring Police to cease the practice of collecting voluntary photographs and prints from youth.¹⁴ The Privacy Commissioner has been pleased with the constructive way in which Police have been engaging with OPC on the compliance notice and its requirements. Police are reporting regularly to OPC on progress towards compliance under IPP 9.
49. We **recommend** that Police policy makes it explicit that the practice of both “voluntary” photographs and “voluntary” prints is unlawful when a young person has been detained in a Police station.¹⁵

Where a youth has been uplifted for care and protection purposes

50. Officers told us that they sometimes took photographs for care and protection purposes when they were transporting youth home, either via a casual car ride offered by Police, or when officers were engaging with youth under section 48 of the Oranga Tamariki Act. Specifically, officers described the practice of photographing runaways, so that they have a picture for future use if that youth should run away again.

¹⁴See the terms of the compliance notice issued by the Privacy Commissioner to Police on 22 December 2021 at Appendix 1C.

¹⁵ See recommendations 13,14 and 15.

51. We accept that there will be situations where there are safety or wellness concerns, either in the home of a youth or related to the youth themselves, which may justify photographs being taken to allow Police to quickly identify and track down the runaway.
52. We **recommend** that Police policy reinforces the need for a case-by-case consideration of whether there is a justification for a photograph in this context. Officers should be reminded of the importance of taking and using a photograph *only* for care and protection purposes and not for law enforcement, and of recording the purpose for which the photograph is being taken.¹⁶

Where an adult or youth has attended a Police station on a voluntary basis

53. Officers reported that when a person (most often a youth) attended a Police station on a voluntary basis, they would sometimes take a photograph.
54. The only lawful purpose potentially arising in a Police station setting will be the furtherance of a specific investigation or intelligence gathering. Since the person's identity is already known, the threshold for taking a voluntary photograph in a Police station setting is likely to be met only on an exceptional basis.
55. We **recommend** that Police policy should reflect this.¹⁷

Taking reasonable steps to inform the person of the purpose – IPP 3

56. IPP 3 requires an agency to take reasonable steps to ensure an individual is sufficiently aware that their personal information is being collected, and the purpose for its collection. Accordingly, whenever Police take a photograph of a person when in a public setting, under IPP 3 they must inform the individual about the purpose for the photograph, unless one of the relevant exceptions applies.
57. The exceptions to the notification requirement provide that Police may be justified in not informing the individual of the purpose for the photographing where Police have a reasonable belief that:
- informing the individual would prejudice the maintenance of the law; or
 - compliance would prejudice the purpose of collection; or
 - an explanation is not reasonably practicable in the circumstances; or
 - the photograph will not be used in a form in which the individual concerned will be identified.
58. The maintenance of the law exception is particularly relevant in the context of Police photographing. This exception will not automatically apply in every case where informing the individual may hinder collection of photographs. Rather, to rely upon this exception in any particular case, Police must identify the particular detriment to the maintenance of the law that notification to the individual would create, with due consideration being given to the rights being displaced by reliance on the exception. Whatever exception an officer relies upon as a

¹⁶ See recommendation 14.

¹⁷ See recommendation 16.

basis for not informing the individual, that officer should record the basis for their reliance upon the exception so that the decision is capable of later audit or review.

59. We **recommend** that Police policy reinforces the requirement to inform individuals of the purpose for taking the photograph and other information required under IPP3, unless an exception applies. Police policy should set out the applicable thresholds for exceptions to the requirement to inform the individual, as set out in paragraph 57, above. In relation to the maintenance of the law exception, that requires a reasonably held belief that not complying with IPP 3 is both necessary to avoid prejudice to the maintenance of the law and proportionate given the intrusion on the rights of the individual.¹⁸

Obtaining consent – IPP 4

60. IPP 4 requires a collecting agency to consider how it is collecting personal information, whether its process is lawful and fair in the circumstances, and, if the collection is unreasonably intrusive on the individual, whether there are less intrusive means to collect the personal information.
61. The key theme relating to IPP 4 in this report is one of consent.¹⁹ We consider that, given the intrusive nature of photographing, IPP 4 always requires officers to consider if obtaining the consent of the individual is necessary when taking photographs in a public setting to ensure fairness and to limit unreasonable intrusion on the individual's privacy rights.
62. However, it will not always be necessary for a Police officer to obtain consent from a subject before taking a photograph, for example, where Police officers have a specified power under the Policing Act allowing a photograph to be taken. There will also be circumstances where it is not unfair or unnecessarily intrusive to take a photograph without consent, because the situation is urgent or otherwise poses evident risk to an individual or the public, or where it is otherwise impracticable to obtain consent without creating a disproportionate risk of prejudice to the particular policing purpose.
63. If the individual does not give their consent on request, the photograph should not be taken unless proceeding without consent is proportionate to the importance of the photograph for an investigation, and outweighs the fairness to the individual, who should be informed that the photograph is mandatory.
64. We are concerned that current Police practices are not sufficient to ensure that, where consent is sought, any consent obtained is truly voluntary and informed.
65. We **recommend** that Police policy stipulates:²⁰
- (a) the presumption that an individual's consent to photographing must be obtained unless one of the exceptions in paragraph 61 apply;

¹⁸ Refer to recommendations 1(b) – (c) and 5(b) – (c).

¹⁹ We refer to "consent" throughout this report to be consistent with the language Police uses in its policies and guidance. However, the Privacy Act 2020 uses the term "authorisation" rather than consent.

²⁰ Refer to recommendation 1(d) and 5(d).

- (b) that, if the individual's consent is sought but is refused, the photograph must not be taken unless proceeding without consent is proportionate to the importance of the photograph for the particular lawful policing purpose, and outweighs the fairness to the individual;
- (c) that, if a photograph is taken after the refusal of consent, the individual must be informed that the photograph is mandatory.

Protections for youth

- 66. The origin of the inquiry was the Police photography of young Māori (rangatahi). The inquiry therefore undertook an in-depth examination of whether the relevant youth-specific legal protections are reflected in Police policy and practice.
- 67. Children and young people have special protections in the criminal justice system, set out in both the United Nations Convention on the Rights of the Child (UNCROC) and the Oranga Tamariki Act. These protections recognise that the vulnerability of youth entitles them to special protection during any investigation into possible offending and prioritise the interests of youth to reduce the potential for offending and the impacts of a criminal record on their life outcomes.
- 68. We found Police practice and procedure to be, in many cases, inconsistent with those protections. We found a widespread belief amongst officers that there was no difference between photographing adults or youths for intelligence-gathering or investigative purposes, with some officers telling us they did not believe that youth are afforded any extra rights or protection in these circumstances.
- 69. This is clearly incorrect. While the thresholds for taking a photograph under the Privacy Act may be the same, there are particular considerations of fairness when Police are seeking the consent of a youth to be photographed in a public setting, including the need to properly explain the purpose for the photograph and what it will be used for in an understandable way. In cases where consent is being sought for the photograph, the request for consent should properly allow the youth (and in the case of those under 14 years, their whānau or family) the choice not to consent.
- 70. We consider that Police policy should highlight that compliance with IPP 4 will need to reflect the youth justice principles to be applied in Police interactions with youth for intelligence gathering or investigative purposes. The wellbeing and best interests of the youth must be considered, and the role of their whānau properly recognised. This means that officers wherever practicable should engage with family and whānau when interacting with youth and in particular obtaining consent for photographing youths in the absence of statutory powers.
- 71. More specifically, we **recommend** that in relation to a child (under 14) being photographed in a public place, consent should be sought from the family, whānau or caregiver (or if they are unavailable another appropriate and independent adult) as well as the child, and the purpose of and necessity for the photograph and how it will subsequently be used by Police fully explained to them. Where it is not possible to immediately obtain the consent of their family,

whānau, caregiver or appropriate adult, it will be necessary to defer the taking of the photograph until that opportunity is available.²¹

72. We also **recommend** that Police policy provide that in the case of a youth who is at least 14 being photographed in a public place, where it is not possible to provide an opportunity for the engagement of family, whānau or another independent adult, Police will need to take care to ensure that the purpose and necessity for the photograph and how it will be used are explained to the youth in suitable and understandable terms and that they are given an opportunity to ask questions. This includes an opportunity to not consent to the photograph being taken, where this choice is being extended to them in the particular circumstances.²²

Use of photographs

73. The way in which Police use photographs is as important as the manner in which they have been collected.
74. Under IPP 10, once a photograph has been obtained for a lawful policing purpose under IPP 1, it may only be used for that purpose, unless one of the specific exceptions set out in IPP 10 applies. The exception most relevant to the Police photographing context is that personal information may be used for a purpose other than that for which it was collected if that other purpose is necessary to avoid prejudice to the maintenance of the law, including prejudice to the prevention, detection and investigation of offences. In the absence of any such exception, Police must securely dispose of that photograph as soon as practicable after the valid purpose for which the photograph was collected has been satisfied or no longer exists.
75. We **recommend** that these rules governing use are set out in Police policy. The policy should reflect the use exceptions in IPP 10 as described above, with guidance on how they should be applied in practice.²³

Retention and destruction

76. Storage, retention and destruction of personal information (including photographs) are also covered by the IPPs. IPP 5 requires Police to ensure there are reasonable safeguards in place to prevent loss, misuse or disclosure of personal information. IPP 9 provides that Police may not keep photographs for longer than is required for the purpose for which they may lawfully be used. Indefinite retention is incompatible with IPP 9.
77. We identified significant issues relating to Police's storage, retention and disposal of photographs.
78. We found that Police do not have a policy covering the use of Police-issued mobile devices when collecting photographs, nor a comprehensive process for audit and deletion of those

²¹ See recommendations 2(c) and 6(c).

²² See recommendations 2(b) – (c) and 6(b) – (c).

²³ See recommendation 18.

photographs. As a result, photographs were routinely indefinitely retained on officers' mobile devices, with the numbers of photos stored on an officer's device often being in the thousands.

79. In addition to officers' mobile devices, there are multiple systems and locations where officers can store photographs. Officers we interviewed described routinely moving or copying photographs from their mobile devices to one or more of the available systems and locations, with little guidance about where and how photographs can be stored, or how long Police may retain that information.
80. We found that the lack of a fit-for-purpose technology policy and the existence of multiple storage systems mean that Police cannot easily audit their holdings to determine how many photographs are held, where, and of whom. This means that photographs are routinely held by Police for longer than is justified by IPP 9.
81. We **recommend** that Police provide regular training for its staff to ensure their use of mobile devices for taking and storing photographs complies with the Privacy Act and other relevant law.²⁴
82. We also **recommend** that Police review and amend relevant policies to ensure its technology policy is fit for purpose and supports compliance with Police's obligations under the Privacy Act. Police policy should ensure consistent storage of photographs, minimising the retention of images on individual devices and the duplication of images across multiple storage systems. The policy should also provide guidelines covering limits on the use and retention of images, routine review and deletion of images from mobile and desktop devices, and protocols for purging and replacing devices.²⁵
83. Further, we **recommend** that, once the technology policy is updated, Police implement the ability to audit compliance with that policy, and with any requirements for the deletion of photographs in accordance with statutory time limits.²⁶

LIST OF RECOMMENDATIONS

Taking photographs for intelligence purposes

	Recommendations
1	<p>Police should develop a consolidated and comprehensive policy covering the use of photography to collect personal information under the Privacy Act for general intelligence gathering purposes. This policy should develop clear, practical guidelines for complying with the Privacy Act when stopping individuals in public and taking photographs for intelligence gathering purposes including:</p> <p>(a) setting an appropriate threshold under the Privacy Act (IPP1) for the collection of personal information: when turning their minds to their reasons for collection</p>

²⁴ See recommendation 20.

²⁵ See recommendation 19.

²⁶ See recommendation 21.

	Recommendations
	<p>officers must be able to articulate <u>a reasonable possibility</u>, based on more than mere conjecture, that the individual being photographed could be relevant to a particular or likely investigation (the lawful purpose).</p> <ul style="list-style-type: none"> (b) unless an exception applies, informing the individual of the purpose for taking the photograph, the consequences for the individual if the photograph is not provided and other information required under the Privacy Act (IPP 3); (c) setting out the applicable thresholds for exceptions to the requirement to inform the individual. In relation to the maintenance of the law exception, that requires a reasonably held belief that not complying with IPP 3 is necessary to avoid prejudice to the maintenance of the law; (d) the circumstances that require the consent of the individual to ensure that photographing the individual is fair and does not intrude to an unreasonable extent on their personal affairs. For example: <ul style="list-style-type: none"> (i) if an officer is engaging with an individual and informing them of the reason and purpose for the photograph, it will generally be fair to also obtain their consent, particularly if the individual is a youth; or (ii) if seeking the individual's consent would be disproportionately prejudicial to the reason for taking the photograph or to the maintenance of the law, that risk of prejudice can justify proceeding without consent; and (iii) that, if a photograph is taken after the refusal of consent, the individual must be informed that the photograph is mandatory.
2	<p>Police policy should provide clear guidelines for complying with the Privacy Act when stopping a youth in public and taking photographs for general intelligence-gathering purposes including:</p> <ul style="list-style-type: none"> (a) reflecting the youth specific protections in the Oranga Tamariki Act and UNCROC; (b) tailoring the explanation under IPP 3 to youth in an age-appropriate way; and (c) reflecting the requirements of IPP 4 when officers are deciding to proceed with a photograph of a youth and require officers to engage with the youth's family, whanau or caregiver and, in the case of a child or tamariki under the age of 14, to obtain their consent (or if they are unavailable another appropriate and independent adult), before taking a photograph of the youth.
3	<p>Police policy should require officers to record the circumstances and considerations that they rely on to justify the collection of personal information for purposes of intelligence gathering.</p>
4	<p>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.</p>

Taking photographs for investigation purposes

	Recommendations
5	<p>Police should develop a consolidated and comprehensive policy covering the use of photography to collect personal information under the Privacy Act for non-crime scene identification. This policy should develop clear, practical guidelines for complying with the Privacy Act when stopping individuals in public and taking photographs for purposes of investigations including:</p> <ul style="list-style-type: none"> (a) setting an appropriate threshold under the Privacy Act (IPP1) for the collection of personal information: when turning their minds to their reasons for collection officers must be able to articulate <u>a reasonable possibility</u>, based on more than mere conjecture, that the individual being photographed could be relevant to a specific investigation that is currently underway (the lawful purpose); (b) unless an exception applies, informing the individual of the purpose for taking the photograph, the consequences for the individual if the photograph is not provided and other information required under the Privacy Act (IPP 3); (c) setting out the applicable thresholds for exceptions to the requirement to inform the individual. In relation to the maintenance of the law exception, that requires a reasonably held belief that not complying with IPP 3 is necessary to avoid prejudice to the maintenance of the law; (d) the circumstances that require the consent of the individual, to ensure that photographing the individual is fair and does not intrude to an unreasonable extent on the personal affairs of the individual concerned. For example: <ul style="list-style-type: none"> (i) if an officer is engaging with an individual and informing them of the reason and purpose of the photograph, it will generally be fair to also obtain their consent, particularly if the individual is a youth; or (ii) if seeking the individual's consent would be disproportionately prejudicial to the reason for taking the photograph or to the maintenance of the law, that risk of prejudice can justify proceeding without consent; and (iii) that, if a photograph is taken after the refusal of consent, the individual must be informed that the photograph is mandatory.
6	<p>Police policy should provide clear guidelines for complying with the Privacy Act when taking photographs of youth for investigation purposes including:</p> <ul style="list-style-type: none"> (a) reflecting the youth specific protections in the Oranga Tamariki Act and UNCROC; (b) tailoring the explanation under IPP 3 to the youth in an age-appropriate way; and (c) reflecting the requirements of IPP 4 when officers are deciding whether to proceed with a photograph of a youth and require officers to engage with the youth's family, whanau or caregiver and, in the case of a child or tamariki under the age of 14, to obtain consent from them (or if they are unavailable another appropriate and independent adult), before taking a photograph of the youth.
7	<p>Police policy should require officers to record the circumstances and considerations that they rely upon to justify the collection of personal information for investigation purposes.</p>

	Recommendations
8	Police policy should confirm that Police may take photographs at a crime scene provided that the privacy of those unrelated to the incident is taken into account. This could be addressed by the redaction of images that include individuals who are not relevant to the investigation.

Traffic checkpoints and other traffic stops

	Recommendation
9	<p>Police should prioritise review of training and policy on LTA checkpoints and stops to ensure that:</p> <ul style="list-style-type: none"> (a) policies reflect the current legal constraints, including the application of the privacy principles when taking photographs for non-LTA purposes; (b) checkpoints and other traffic stops are not established for the primary purpose of collecting photographs and personal information for a collateral purpose; (c) information gathered in the course of an LTA checkpoint or stop is not used for other purposes (e.g. general intelligence) unless lawfully collected for that other purpose, or it comes under a valid use exception under the Privacy Act; (d) photographs are taken for identification purposes at traffic checkpoints and other traffic stops when an infringement notice is being issued only when the driver's identity is not able to be ascertained in other way (eg by examination of the driving licence and accompanying photograph); and (e) officers receive regular training on the limits of taking photographs at LTA checkpoints and traffic stops.

Protests and other large gatherings

	Recommendation
10	<p>Police should review the <i>Demonstrations</i> policy to reflect that:</p> <ul style="list-style-type: none"> (a) an appropriate threshold for photography is where the officer believes, based on some articulable facts, that there is a reasonable possibility of disorder occurring; and (b) recording demonstrators for no reason other than their presence in an otherwise lawful and peaceful demonstration, with the aim of identifying them for potential future demonstrations, is not necessary for a lawful Police purpose.

Issuing notices and proof of service

	Recommendation
11	As part of a general review of policy and guidance relating to photographs of members of the public, Police should review and update policies and process relating to proof of service. This should make it clear that officers may photograph individuals holding a summons or

	Recommendation
	infringement notice, as long as officers properly explain the purpose and use of the photograph, take it by fair and reasonable means, and limit the use of the photographs to demonstrating proof of service.

Responding to monitoring by members of the public

	Recommendation
12	As part of a general review of policy and guidance relating to photographs of members of the public, Police should ensure there is guidance about the lawful basis for photographing or video recording members of the public monitoring Police. This should make clear that officers should do so only if the officer has reasonable concerns that the person's behaviour poses a threat or is obstructing them in the performance of their duty.

Interaction with youth in Police stations

	Recommendations
13	Police policy should reflect that "voluntary consent" - whether or not it is informed - does not make the otherwise unlawful or unnecessary collection of personal information lawful or compliant with the Privacy Act
14	Police should cease the practice of taking photographs of youth on a 'voluntary' basis where a youth has been uplifted or detained, except where a photograph is necessary for Police's care and protection role to ensure the safety of the youth.
15	Police should cease the practice of taking biometric prints from youth on a 'voluntary' basis.
16	Police policy should identify: <ul style="list-style-type: none"> (a) the limits on taking 'voluntary' photographs of youth (and adults) present in Police stations on a voluntary basis under IPP 1; and (b) where a youth is concerned, the requirement for a parent, caregiver or other appropriate adult to be present to give informed consent for a 'voluntary' photograph.
17	Police should prioritise training for officers to improve understanding of: <ul style="list-style-type: none"> (a) Police's functions under the Oranga Tamariki Act in the youth justice and care and protection contexts; and (b) the youth-specific protections due to vulnerability.

Use

	Recommendation
18	Police policy should provide clear guidelines on the purposes for which lawfully collected personal information in the form of photographs and videos may be used under the Privacy Act (IPP 10).

Retention

	Recommendations
19	<p>Police policy and guidelines (including any relevant disposal schedule) should be reviewed and amended to ensure the technology policy is fit for purpose to support compliance with Police's obligations under the Privacy Act (and other relevant legislation) and provide guidance for officers routinely using mobile devices for mixed personal and policing purposes including, in particular:</p> <ul style="list-style-type: none">(a) the consistent storage and uploading of images and associated data to secure locations, and minimising the retention of images on individual devices and the duplication of images across Police systems;(b) limits on using individual devices to capture images where other Police devices or technology is specifically set up for that purpose;(c) protocols on handling sensitive or traumatic images;(d) limits on the use and retention of images (and copies) in individual devices and in Police systems;(e) routine review and deletion of images from mobile and desktop devices;(f) protocols for purging and replacing devices.
20	Police should prioritise regular training for all officers on using mobile devices to ensure legal compliance.
21	<p>Police should review systems and implement the ability to audit compliance with:</p> <ul style="list-style-type: none">(a) updated technology policy and the handling of photographs of individuals on mobile devices; and(b) the deletion of identifying particulars in accordance with statutory time limits.

General recommendations

	Recommendations
22	<p>Police should develop a strategy to improve its staff's fundamental understanding of the application of the Privacy Act to the collection and protection of personal information with a particular focus on photographs as sensitive biometric information covering:</p> <ul style="list-style-type: none">(a) policies and processes;(b) training; and

	Recommendations
	(c) methods for updating knowledge and practice on an ongoing basis.
23	<p>In implementing the strategy, Police should establish a rolling programme of reviews and updates of key policies, and develop and deliver agency-wide training to its staff and relevant contractors on:</p> <ul style="list-style-type: none"> (a) the decision-making framework and procedures to be followed to photograph individuals and youth in public; and (b) storage and deletion procedures.

BACKGROUND TO THIS JOINT INQUIRY

84. In December 2020, the Office of the Privacy Commissioner (OPC) and the Independent Police Conduct Authority (IPCA) announced a joint inquiry into Police conduct involving the photographing of members of the public.²⁷ The decision to instigate a joint inquiry followed substantial media publicity about Police taking photographs of Māori young people in Wairarapa in August 2020.²⁸ After the IPCA made direct inquiries with Police, on 24 December 2020 Police formally notified the IPCA of the incidents.
85. Police subsequently provided information to the IPCA about similar incidents where Whanganui Police photographed rangatahi in 2014. In addition, following the announcement of the joint inquiry further similar incidents were reported to the IPCA and OPC through the media and, in some cases, directly by whānau.
86. While the initial Wairarapa complaint and the similar incidents reported to the IPCA and OPC all involved Police photographing of youth, it quickly became clear that the issues these incidents raised had much broader application. Police photographing in public places is a widespread practice that is not limited to youth, and many of the issues and questions arising out of photographing young people apply equally to the photographing of members of the public in general.
87. While a key focus of the joint inquiry is the situation of individuals being photographed in public settings (when not being detained or suspected by Police of committing an offence), the joint inquiry also reviewed situations where Police photographs are taken of youths when they have been detained and taken to Police stations or are there on a so-called voluntary basis, or of youth or adults for intelligence purposes who are stopped at traffic checkpoints or are on private premises during the exercise of a search power.

²⁷ Privacy Commissioner and Independent Police Conduct Authority “[Terms of Reference of joint inquiry into Police photographing of members of the public](#)” (press release, 9 March 2021).

²⁸ See for example Te Aniwa Hurihanganui and Hamish Cardwell “[Questions raised after police officers stop youths to take their photos](#)” *Radio New Zealand* (online ed, 21 December 2020).

88. In addition, other methods Police use to collect personal data raise similar conduct, policy, practice and procedure and privacy issues as those related to taking photographs. In this joint inquiry, we have also inquired into Police taking video recordings of members of the public and the collection of youth fingerprints and palmprints (biometric prints) on a so-called voluntary basis.
89. The context for issues raised about Police photography of members of the public is the rapidly expanding role of mobile technology (mobile devices) in everyday frontline policing.²⁹ The rollout of mobile devices has put a small, easy-to-use camera in the hands of every frontline Police officer. This has exponentially increased the number of photographs or videos Police officers are taking in the course of their work and the ease with which they can share those photographs and videos.
90. Police photographing of members of the public falls into the oversight jurisdiction of both OPC and the IPCA and both agencies had separately decided to inquire into the reported issues. Given the common subject matter, OPC and the IPCA agreed the inquiry should be conducted jointly with each body exercising its respective functions and powers:
- (a) The IPCA brings its powers to investigate complaints under section 12(1)(c) of the Independent Police Conduct Authority Act 1988 (IPCA Act). Additionally, section 12(2) broadens the power to investigate to any Police practice, policy or procedure which relates to the complaint. Following an investigation, the IPCA can make recommendations pursuant to section 27(2) of the IPCA Act.
 - (b) OPC brings both powers of inquiry under section 17(1)(i) of the Privacy Act 2020 (Privacy Act) and the regulatory powers set out in the Privacy Act, including the power to issue one or more compliance notices to remedy identified breaches of the Privacy Act.
91. In December 2021, the Privacy Commissioner issued a compliance notice to Police in relation to non-compliance with information privacy principle (IPP) 9 of the Privacy Act.³⁰ The compliance notice relates to Police retaining photographs and biometric prints in contexts where that personal information could not lawfully be used, and therefore requiring its deletion from Police devices and systems. Police have accepted the actions required by the Privacy Commissioner within the timeframes set out in the compliance notice.

TERMS OF REFERENCE

92. The IPCA and OPC released terms of reference for the joint inquiry in March 2021 (Appendix 1 at B). The terms of reference set out the purpose of the joint inquiry into Police's conduct, practice, policies and procedures as they relate to members of the New Zealand public, including whether Police action, policy or procedure has resulted in the privacy of individuals being infringed. This relates to Police practices around the use of photography in situations where

²⁹Police use the term "mobility device" in internal documents and policies to describe Police-issued smartphones, tablets and other similar portable digital devices used by Police officers. In this report, we use the term "mobile device" to describe those devices.

³⁰See Appendix 1 at C.

individual members of the public are not at the time being detained for or suspected of committing an offence.

93. The terms of reference recognise that Police photographing members of the public who are not being detained for or suspected of committing an offence raises significant Police conduct, policy, practice and procedure and privacy issues.
94. The purpose statement in the terms of reference record that the joint inquiry will incorporate the investigation of reported incidents of Police photographing Māori youth in Wairarapa. The terms of reference affirm that the release of the joint inquiry report and potential compliance action by the Privacy Commissioner do not preclude individuals who feel that their privacy has been infringed being able to make a privacy complaint to the Privacy Commissioner under the Privacy Act.
95. In this report we use the term ‘rangatahi’ to mean young persons who are Māori. We also use the term ‘youth’ as an umbrella term to cover children and young persons (and including rangatahi). The Oranga Tamariki Act 1989 defines a ‘child’ as a person under the age of 14, and a ‘young person’ as a person over the age of 14 but under 18.
96. The terms of reference for the joint inquiry set out the key issues for consideration:
 - (a) To determine whether Police actions with respect to the Wairarapa incidents complied with Police policy, the Privacy Act 1993,³¹ and any other key legislation.
 - (b) To determine if any compliance and enforcement action is required if it is found that Police breached the privacy of the individuals involved.
 - (c) To identify the extent to which, and the reasons why, Police are photographing, video recording, or gathering biometric prints from, members of the public.
 - (d) To identify variations in practices in this respect across Police districts.
 - (e) To determine the extent to which any or all of these practices are consistent with the Privacy Act or any other legislation.
 - (f) To identify what Police policy and practice in this area ought to be, including the extent to which any specific restriction or requirement ought to govern the photography of youths.
97. The terms of reference record that the IPCA had recently concluded an investigation into a complaint about Northland Police staff taking photographs of members of the public at a Police

³¹Although the Privacy Act 2020 has been in force since 1 December 2020, this report covers incidents which took place before that date. Therefore, the Privacy Act 1993 may apply to this report to the extent that the 1993 Act was in force when those incidents took place. However, we do not consider that our analysis would be affected by the enactment of the Privacy Act 2020 due to the principles-based nature of both Acts. In all material aspects, and in particular with respect to the recommendations for Police going forward, we use and apply the Privacy Act 2020 in this report. For further details on transitional matters see Privacy Act 2020, s 5 and sch 1.

checkpoint without the necessary lawful grounds to do so.³² One of the outcomes of the Northland incident was a recommendation that Police review national Police policy to provide clear guidance on when photographs can be taken for intelligence purposes.

98. The terms of reference for this joint inquiry specified a number of outcomes.
- (a) The production of a joint report for Police and the public, providing an assessment of Police's compliance with legislation and policy, and any recommendations for remedial measures that should be taken to improve policy and practice.
 - (b) To the extent that relevant breaches of the Privacy Act by Police were identified, the terms of reference anticipated that the Inquiry may result in compliance and enforcement action being taken by the Privacy Commissioner.

UNCONSCIOUS BIAS

99. Inquiring into unconscious bias was not within the Terms of Reference of the joint inquiry. However, we note the affected youth we spoke to were Māori rangatahi. From available data on intelligence photographs retained by police, over half are Māori. Rangatahi and their whānau interviewed as part of this joint inquiry also consistently raised concerns that their treatment was as the result of their race. Police have instigated a long-term research programme³³ focussed on understanding the role of bias within Police policies, processes and practices entitled *Understanding Policy Delivery*.³⁴

THE ROLE OF THE INDEPENDENT POLICE CONDUCT AUTHORITY | MANA WHANONGA PIRIHIMANA MOTUHAKE

100. Under the IPCA Act, the IPCA has the function of receiving complaints alleging misconduct or neglect of duty by any Police employee, or concerning any practice, policy or procedure of Police affecting the person or body of people making the complaint. The IPCA may then determine what action to take in relation to a complaint, such as to investigate the complaint itself, or refer the matter back to Police for investigation by Police.
101. In addition, the IPCA has entered into a Memorandum of Understanding with Police under which the Commissioner of Police may notify the IPCA of incidents involving criminal offending or serious misconduct by a Police employee, where that matter is of such significance or public interest that it places or is likely to place Police's reputation at risk. The IPCA may act on these notifications in the same manner as a complaint.³⁵

³²Independent Police Conduct Authority "[Photographs taken at Police checkpoint unlawful](#)" (press release, 13 April 2021).

³³NZ Police | Ngā Pirihimana o Aotearoa "[Understanding Policing Delivery](#)" <www.police.govt.nz>.

³⁴ See section 5 of this report – Police actions.

³⁵See Independent Police Conduct Authority "[Legislation and accountability](#)" <www.ipca.govt.nz>.

102. The Privacy Commissioner, an independent Crown Entity, is New Zealand’s privacy regulator.³⁶
103. The Privacy Commissioner has broad functions under the Privacy Act, including those set out at section 17. One of the Commissioner’s functions is to generally inquire into any matter, including any practice or procedure or technical development, if it appears to the Commissioner that the privacy of individuals is being, or may be infringed.³⁷
104. In addition, the Privacy Commissioner has powers under Part 6(2) to issue a compliance notice to organisations or businesses not meeting their obligations under the Privacy Act. A compliance notice requires the organisation or business to do something, or to stop doing something, in order to comply with the Privacy Act.
105. As the Privacy Act applies to Police,³⁸ the Privacy Commissioner has jurisdiction to consider complaints from members of the public about the handling of personal information, and to monitor Police’s compliance with the IPPs and with the Act.
106. In performing functions and duties and exercising powers under the Privacy Act, the Commissioner must have regard to the IPPs in the Privacy Act and the privacy interests of individuals alongside human rights and other interests, including the desirability of a free flow of information and the right of government and business to achieve their objectives in an efficient way. The Commissioner must take account of New Zealand’s international obligations and consider any general international guidelines that are relevant to improved protection of individual privacy.
107. The Privacy Commissioner must also take account of cultural perspectives on privacy pursuant to section 21(c) of the Privacy Act. Tikanga may inform how best to approach a situation in an appropriate way to meet the cultural needs of affected individuals and their whānau. Te Tiriti ō Waitangi / Treaty of Waitangi is considered a founding document of Aotearoa New Zealand and the text(s) and the principles of partnership, active protection and equity help guide the work of OPC. Tikanga is widely accepted by the courts as part of the common law of Aotearoa New Zealand including, recently, by the High Court in *Te Pou Matakana v Attorney-General*.³⁹
108. During the course of this inquiry, the Commissioner has published two papers relevant to the Police conduct reviewed by the joint inquiry: a position paper on biometrics⁴⁰ and guidance on the handling of sensitive personal information under the Privacy Act.⁴¹

³⁶Privacy Commissioner “[Compliance and Regulatory Action Framework](#)” (November 2020).

³⁷Privacy Act 2020, s 17(1)(i).

³⁸Police is a “New Zealand agency”; see Privacy Act 2020, s 8(a)(ii). See also the Privacy Act definitions of “public sector agency” and “organisation”; Privacy Act 2020, s 7(1).

³⁹*Te Pou Matakana v Attorney-General (No 2)* [2021] NZHC 3319 at [27]; see also at [107]–[112] where Gwyn J considered what the decision-maker’s obligations were under Te Tiriti ō Waitangi and what would be required to apply those obligations in a manner consistent with tikanga.

⁴⁰Privacy Commissioner “[Office of the Privacy Commissioner position on the regulation of biometrics](#)” (7 October 2021).

⁴¹Privacy Commissioner “[Sensitive personal information and the Privacy Act 2020](#)” (16 December 2021).

109. Police's core role is the maintenance of law and order. This is reflected in the Police functions listed in the Policing Act 2008: keeping the peace; maintaining public safety; law enforcement; and crime prevention.⁴²
110. Police perform many additional functions including conducting search and rescue operations; education; emergency management; and safeguarding the welfare of youths. Given this multi-functional role, Police are in constant contact with members of the public at any time of day or night and in a wide variety of places and circumstances.
111. To effectively carry out policing functions, Police rely on intelligence gathered by officers in a range of settings that includes the collection of personal information about individuals such as photographs and biometric prints. The interactions Police officers have with members of the public on a daily basis are a common means of gathering intelligence information.
112. Intelligence supports Police by providing timely, accurate and relevant insight and foresight to enhance the organisation's tactical, operational and strategic decision-making. Police's exercise of this intelligence-gathering function when engaging with members of the public and taking photographs on Police mobile devices of individuals who have not been detained, gives rise to the issues discussed in this report.

METHODOLOGY

113. OPC and the IPCA worked together, and with Police, to gather appropriate data to enable us to identify the extent of the collection of photographs and other personal information during encounters with members of the public.
114. We used a multi-pronged approach to gather the data needed:
 - (a) We reviewed existing Police policy relevant to the photographing of, and taking of other personal data from, members of the public.⁴³ We also identified the applicable legal principles through a review of relevant legislation.
 - (b) We sought to gain an understanding of current Police practice by investigating the individual complaints made to the IPCA arising out of incidents in Wairarapa, Whanganui, Hamilton, and Gisborne. The joint inquiry process involved interviewing complainants, their whānau, involved officers and other relevant Police staff. We also reviewed Police files relating to these incidents.
 - (c) We also drew on the IPCA's findings from its investigation into the photographing of people at a Northland checkpoint.⁴⁴

⁴²Policing Act 2008, s 9.

⁴³For a list of Police's policies and procedures that we reviewed, see Appendix 1A.

⁴⁴IPCA press release, above n 32.

- (d) Police National Headquarters (PNHQ) sent questionnaires to each Police district as part of Police's internal review. Police consulted with OPC and the IPCA when developing the questionnaires. The questionnaires requested data on policy, practice and procedure regarding photographing and fingerprinting by district. This data was collated and summarised in a report by PNHQ, which was provided to OPC and the IPCA.
- (e) Analysis of this data enabled us to gain an understanding of Police policy, practice, and procedure; whether there are any inconsistencies across districts; and whether there are any gaps between the legal requirements and Police policy and practice.
- (f) We selected four districts for further analysis: Counties Manukau, Waikato, Wellington, and Southland. These districts were selected to provide a variety of demographic and geographic characteristics, including geographic and population size, geographic location, and both urban and rural settings.
- (g) We interviewed a mix of staff within each district with the aim of understanding what policy and procedure is within each district, as well as how well that policy and procedure is understood and implemented in practice. Staff interviewed ranged from recent graduates from the Royal New Zealand Police College (RNZPC), to senior management and sworn and non-sworn staff with several years' experience. Staff included those with a variety of roles and experiences within Police to draw upon in their interviews. We also sought to gather views from Police staff on whether their experiences and knowledge levels were representative of their colleagues, what they believed policy should be, and where they felt there were any gaps in policy and/or training.
- (h) Throughout the joint inquiry we have also engaged with appropriate staff from PNHQ on an ongoing basis to identify relevant issues and next steps.
- (i) Police provided the joint inquiry team with the summary of its internal review and key findings on a without prejudice basis. This has assisted to establish the key areas of focus for the joint inquiry. The analysis of those issues and the recommendations of the joint inquiry team have been developed independently of Police's internal review.

Limited available data

115. The joint inquiry also sought to analyse Police data relating to the numbers of photographs collected and stored and the characteristics of those individuals photographed. Police have not been able to provide statistical information about the following key issues to the joint inquiry:

- (a) the basis on which prints or photographs have been lawfully obtained and in what circumstances or for what purpose;
- (b) whether the person has been provided with enough information to provide informed consent;
- (c) how many prints or photographs are obtained by officers, where they are stored, length of retention and reasons for retention;

- (d) whether the individuals are adults or youths, the ethnicity of the people printed or photographed or if the photographs are of one person or contain multiple persons.
116. The data Police have been able to provide is limited by the auditability of the OnDuty database and is therefore incomplete. Police officers use a mobile application system called OnDuty when carrying out their policing duties. OnDuty enables frontline officers to access intelligence in the field and to complete formal paperwork (and attach photographs to that paperwork) using their mobile device. OnDuty is directly connected to the National Intelligence Application (NIA) database, which has transformed the way New Zealand's frontline officers collect, access and act on information.⁴⁵ A review of the OnDuty database was carried out in 2021 to identify intelligence (intel) notings with at least one photograph, however that review could not determine if each photograph was of an individual without looking at every photo. The OnDuty database review noted:
- (a) intel notings were linked to 88,553 records collected since January 2018. Of these, 49,816 intel notings had a photograph attached;
 - (b) the intel notings may have had more than one person identity record attached to it. Of these person identity records, 45% had a linked ethnicity recorded as Māori, and 10% Pasifika;
 - (c) 6,153 of the 49,816 intel notings with photographs (12%) were linked to 10,851 individuals aged under 18 years. Some of these notings will have had more than one person identity record attached to it; and
 - (d) 53% of the 10,851 individual figures had a recorded ethnicity of Māori attached to it. 10% were recorded as Pasifika.
117. In addition to the limited auditability of OnDuty, a further caveat to the usefulness of this data is the fact that (as became clear from our interviews with Police staff) only a very small percentage of photographs Police take of individuals in public places actually end up in the OnDuty database.

OVERVIEW OF THE RANGATAHI INCIDENTS

118. As well as examining the systemic issues raised by Police photography, this joint inquiry reviewed a number of specific incidents involving rangatahi being photographed by officers in public settings.
119. This joint inquiry was prompted by reports by whānau of Police photographing their rangatahi in circumstances they considered was unfair or unjustified. Some of the reports resulted in complaint investigations by the IPCA. OPC interviewed whānau as part of this joint inquiry.

⁴⁵NIA is a database used by Police to manage information needed to support operational policing. The database holds records about offences and incidents reported to Police as well as intelligence notings. For further information see Data Quality and Integrity Team [National Recording Standard](#) New Zealand Police (August 2019).

120. Some examples of rangatahi photography were brought to the attention of the inquiry team by way of formal complaints to the IPCA. Others were brought to our attention by Police or the news media and individuals involved in these incidents were interviewed to inform this joint inquiry rather than by way of an individual complaint investigation under the Independent Police Conduct Authority Act or Part 5 of the Privacy Act.
121. Where issues were raised by whānau with the media, the joint inquiry team made contact with the whānau who had agreed to have their personal contact details forwarded onto us.
122. We note that some of the issues are historical. As a result, neither Police nor the IPCA were able to identify the officers involved or to corroborate the events as outlined for all incidents addressed in this joint inquiry. This means that, for some complaints, we are unable to make conclusive findings.
123. Some incidents have been acknowledged by Police and have resulted in letters of apology to whānau. In some cases, Police have offered to meet whānau and resolution processes have not yet concluded.
124. The whānau interviewed or spoken to by the media or the joint inquiry team have spoken of their feelings of whakamā (shame),⁴⁶ embarrassment, frustration and anger they feel from the actions by Police towards their rangatahi and their belief they have been targeted due to racial bias. This has led to many whānau requesting face to face meetings with Police to receive an apology and have a wider discussion on how the actions of Police are continuing the cycle of racial bias experienced by Māori.
125. As noted in the terms of reference, the consideration of these incidents by the IPCA or the joint inquiry does not preclude whānau from raising their concerns with OPC as formal complaints, where particular recent incidents remain unresolved for whānau.
126. The incidents are outlined below and considered in more detail in section 3D of this report.

Rangatahi uplifted and photographed without consent or explanation

127. In 2020, Police officers stopped and spoke to three rangatahi who were out late at night in Wairarapa. The officers were investigating alleged offending that had occurred nearby. The officers took the rangatahi back to the Police station using powers under the Oranga Tamariki Act 1989, as the rangatahi would not provide the officers with the details of their parents or caregivers or home addresses.
128. Back at the station the officers, in the course of asking the rangatahi questions about their home details and the alleged offending, took photographs of each of the rangatahi. It is not clear the extent to which officers sought consent from either the rangatahi or parents or caregivers and what explanation for the photographs was given to any of those involved.

⁴⁶Significant humiliation is one of the recognised grounds for remedies under the Privacy Act for a breach of privacy; see Privacy Act 2020, s 69.

Reports of rangatahi being stopped and photographed without consent

129. We reviewed three incidents involving rangatahi who were stopped and photographed on the street by Police without their consent (two of these being historical incidents).
- (a) In 2020 in Hamilton, two rangatahi were waiting at a bus stop after school. Police officers were responding to a burglary that had been reported about 550 metres from where the rangatahi were spoken to. Neither of the rangatahi matched the description of the reported offenders. The Police officers did not properly seek consent before taking the photograph and provided only a brief explanation to the rangatahi about the photograph being used to eliminate the rangatahi from the inquiry.
 - (b) An incident was reported from 2014 in Whanganui of two rangatahi who were waiting for their koro outside a shop. Police officers reportedly stopped and asked the rangatahi some questions about an alleged burglary. The report was that as they spoke to the rangatahi, the officers took photographs of them but did not explain why they were taking the photographs, nor did the rangatahi consent to having their photographs taken.
 - (c) An incident was reported from some time between 2014 and 2016 in Gisborne of a rangatahi returning home one evening from a local basketball court being stopped by a Police officer who spoke to him about reports of concerns he had heard from neighbouring residents. The report was that an officer took a photograph of the rangatahi during the conversation without telling the rangatahi why it was being taken, what it would be used for, or asking the rangatahi for consent. The officer gave the rangatahi a ride home and reportedly took a further photograph of him at his home despite the rangatahi's mother telling the officer that she did not consent to a photograph being taken.

Rangatahi photographed after he refused consent and explained his rights to Police

130. In early 2021 Police officers observed an animated conversation between rangatahi in a suburban street and stopped to intervene. One of the rangatahi refused to provide details to the officers and asserted that Police were not entitled to that information. During a confrontation with Police, the officers took photographs of the rangatahi, despite members of the group voicing their objection and attempting to impede the photographs from being taken (by holding their arms over their faces).

2 RELEVANT LEGISLATIVE FRAMEWORK

131. The fundamental role of Police is to uphold the law. Police as an organisation and individual Police officers (in their capacity as Police employees) are all subject to applicable statute and common law constraints on the exercise of Police functions and powers.
132. This part of the report sets out an overview of the legislative framework that applies to Police photography of members of the public, depending on the particular policing context in which the photograph is taken.

133. It is important to note that Police take photographs of members of the public in a range of different contexts. The particular legal requirements that apply to Police photography of members of the public depend on the policing context and the circumstances in which photographs are being taken.
134. Particular statutes establish circumstances in which officers may collect identifying personal information, including in some instances taking photographs.⁴⁷ Sometimes these statutes include safeguards and limits on the manner in which personal information may be collected and/or retained.
135. To the extent that Police collection and use of identifying personal information is not governed by a particular statute, the Privacy Act and its principles apply as a constraint on Police photography of members of the public. In particular, the Privacy Act requires that taking photographs of members of the public must be necessary for a lawful policing purpose.⁴⁸
136. The table below provides an overview of key elements of the legislative framework.

Targeted photography of individuals	Public places	Interaction at police station – arrest or detention	Private property
Law	Privacy Act 2020	Policing Act 2008	Search and Surveillance Act 2012
Voluntary or mandatory	Voluntary if based on authorisation, but this will be context dependent	Mandatory	Police power
Threshold	A reasonable possibility that the individual could be relevant to a specific investigation (IPP 1)	In custody & detained for committing offence (s 32) Good cause to suspect committing an offence and detaining (s 33) Youth justice protections ⁴⁹	Reasonable grounds to believe photo relevant to the purpose of lawful entry

⁴⁷ An example of a Police power to collect information is a surveillance device warrant authorised in accordance with the Search and Surveillance Act 2012.

⁴⁸ Privacy Act 2020, s 22 (IPP 1).

⁴⁹ Oranga Tamariki Act 1989, Part 4.

Targeted photography of individuals	Public places	Interaction at police station – arrest or detention	Private property
Notify or inform	Yes, unless justification for an exception (IPP 3)	Youth justice protections ⁵⁰	Youth justice protections. ⁵¹
Based on consent	Yes, unless circumstances justify taking photo without consent (IPP 4)	No	No
Youth protections apply	Yes	Yes	Yes

POLICING ACT 2008

137. The Policing Act provides powers for Police to obtain biometric information such as photographs and biometric prints, in certain circumstances. The specific powers do not cover all circumstances in which Police may collect this information; rather, the Policing Act instead sets out the circumstances where Police have a specific power to obtain that information when a person is detained in custody. The Policing Act recognises that biographical information collected about a person (name, address and date of birth) is intrinsically different from photographs, images and biometric prints. While other identifying particulars collected when a person is in Police custody and is detained for committing an offence may be retained on the Police information recording system indefinitely, photographs, visual images and biometric prints are required to be destroyed as soon as is practicable if a decision is made not to commence criminal proceedings or the outcome is not one that authorises continued storage (e.g. acquittal on charges).
138. Part 3 of the Policing Act governs the taking of identifying particulars of a person when detained in custody and includes the obtaining of biometric information such as biometric prints and photographs, and provisions for storage, retention and destruction.
139. Section 32 enables Police to collect the identifying particulars (including photographs and biometric prints) when a person is in Police custody and is detained for committing an offence.

⁵⁰Oranga Tamariki Act 1989, Part 4.

⁵¹See also provision for notice of exercise of search power under Search and Surveillance Act 2012, s 131.

140. The purpose of section 32 is to enable Police to obtain information that may be used now or in the future by Police for any lawful purpose. This applies if the person is detained either at a Police station, or at any other place being used for Police purposes.

141. The term “identifying particulars” is defined in section 32(5) as including:

- (a) biographical details (for example, name, address and date of birth);
- (b) the person’s photograph or visual image; and
- (c) impression of the person’s fingerprints, palm-prints or footprints.

“Identifying particulars” in relation to a person under the Policing Act also falls under the definition of “personal information” as that term is defined in section 7(1) of the Privacy Act.

142. Section 33 of the Policing Act provides a similar power to obtain identifying particulars in a situation where a constable has grounds to serve a summons on the individual relating to the suspected commission of a criminal offence. The constable may detain a person to take their identifying particulars and failure to comply with a constable’s direction to provide identifying particulars is a criminal offence. The constable must have good cause to suspect the person has committed an offence and must intend to bring proceedings against the person in respect of that offence before detaining a person under this section, and may detain the person only for the period of taking their particulars.

143. Section 34 sets out requirements for the storage and retention of identifying particulars collected by Police under sections 32 or 33 and sets out when that information must be destroyed. Under section 34(1), any photographs, biometric prints or other identifying particulars collected pursuant to sections 32 or 33 must be entered, recorded and stored on a Police information recording system.

144. Section 34(2) requires the destruction of any photographs, visual images or fingerprint, palm-prints or foot-prints as soon as practicable after a decision is made not to commence a prosecution, or the prosecution does not result in a conviction or other outcome that authorises continued storage under Section 34A. Biographical details collected under Section 32 and 33 may be retained indefinitely.

145. Section 34A explains the outcomes of criminal proceedings that authorise the continued storage of identifying particulars including:

- (a) Admission of the offence and completion of a programme of diversion.
- (b) Conviction for the offence.
- (c) Proceedings where the Youth Court makes an order under section 283(a) to (n) of the Oranga Tamariki Act.
- (d) Discharge without conviction under section 106 of the Sentencing Act.

146. Sections 32 to 34 do not apply, however, to situations where a Police officer engages with a member of the public who is not being detained under Police detention powers.

SEARCH AND SURVEILLANCE ACT 2012

147. Police commonly collect photographs and video recordings by way of the exercise of a specific search or surveillance power, with or without warrant, under the Search and Surveillance Act.
148. The Search and Surveillance Act regulates the exercise of intrusive powers by state agencies, including the search and surveillance powers of Police. The purpose of the Act is to “facilitate the monitoring of compliance with the law and the investigation and prosecution of offences in a manner that is consistent with human rights values”, including by “providing rules that recognise the importance of the rights and entitlements affirmed in other enactments, including the New Zealand Bill of Rights Act 1990, the Privacy Act 2020 and the Evidence Act 2006.”⁵²
149. Police powers of entry to private property are regulated by the Search and Surveillance Act and by the law relating to implied licence.⁵³ This Act is not generally engaged when Police officers are photographing individuals in public settings or undertaking surveillance activities in public places.⁵⁴ As the Act regulates Police powers of search and surveillance, however, it is relevant to Police photography and video recording of activities on **private property** and the use of devices to record **private activities** (as those terms are defined in the Act).⁵⁵
150. The Act has an important intersection with section 21 of the New Zealand Bill of Rights Act 1990, which expresses the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.⁵⁶
151. In particular, the Act requires Police to obtain search or surveillance warrants through the courts before undertaking surveillance activities (including photography) that would infringe a reasonable expectation of privacy, a right encapsulated in section 21 of the New Zealand Bill of Rights Act.
152. Where Police are exercising search powers under the Act, section 110 authorises them to take photographs and video recordings of the place or anything found in that place if the officer has reasonable grounds to believe that the photographs or recordings may be relevant to the purposes of the entry and search.
153. The Search and Surveillance Act also regulates Police use of visual surveillance to observe private activity in private premises and the observation of private activity in the curtilage of private

⁵²Search and Surveillance Act 2012, s 5.

⁵³See *Tararo v R* [2010] NZSC 157.

⁵⁴See *Hamed v R* [2011] NZSC 101.

⁵⁵Search and Surveillance Act 2012, s 3(1).

⁵⁶Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC R141, 2018) at [24].

premises (an entry way or area attached to a private house)⁵⁷ and recordings of that activity exceeding certain time limits.

154. Generally, such use is permitted only pursuant to a warrant under section 46, or the exercise of a specific warrantless power under section 48 in specified situations of emergency or urgency. Section 47 provides an exception: a warrant is not required if the officer is lawfully on private premises and records only what he or she observes or hears. However, it should be noted that while Police may observe (and record) items present on the property, that action must be consistent with the purpose for which the officer is lawfully on the premises.⁵⁸

YOUTH-SPECIFIC PROTECTIONS

155. Police interactions with youth are subject to the youth-specific protections set out in both the United Nations Convention on the Rights of the Child (UNCROC) and the Oranga Tamariki Act. Youths are afforded certain protections under the Act in both the care and protection and youth justice contexts.⁵⁹
156. These protections prioritise the interests of the youth to reduce the potential for offending and the impacts of a criminal record on their life outcomes. The youth-specific protections need to be considered by Police in any informal engagements with youth, given that these interactions could lead to the Police's care and protection and youth justice functions being engaged.
157. The New Zealand system explicitly recognises that offending by children and care and protection issues are linked:⁶⁰

It mobilises the resources of the child protection system, the criminal justice system and the child's own networks to create an integrated plan that deals with both the offending and the child's care and protection needs. Even where there is no criminal justice response, measures are nonetheless taken in relation to offending and its causes. Therefore, cases can be diverted away from the courts and the criminal justice system.

158. Protections set out in UNCROC have been incorporated by reference into the Oranga Tamariki Act.⁶¹ Two of those protections are particularly relevant to the issues being considered in this joint inquiry:

⁵⁷The 'curtilage' means the land immediately surrounding a house or building. It defines the boundary within which the owner of a building can have a reasonable expectation of privacy and where common activities take place. In the context of a residential dwelling, the curtilage will include the garden, front or back yard, or lawn belonging to a home.

⁵⁸Law Commission *Search and surveillance powers* (NZLC R97, 2007), at [11.76].

⁵⁹There is cross-over between the care and protection and youth justice contexts. See *NZ Police v LV* [2020] NZYC 117; *NZ Police v JV* [2021] NZYC 248; Judge Becroft "The Youth Courts of New Zealand in ten years time" (paper for the National Youth Advocates/Lay Advocates Conference) July 2015; and Jennifer George, "Crossover Youth Scoping Study" (Henwood Trust) April 2020, noting that crossover youth form a high and growing proportion of youth appearing before the Youth Court and that most are Māori.

⁶⁰Sentencing Advisory Council (Victoria) 'Crossover Kids': Vulnerable Children in the Youth Justice system, report 3 (June 2020).

⁶¹Oranga Tamariki Act 1989, s 5(1)(b)(i). UNCROC was considered in the case *S and Marper v United Kingdom* [2008] ECHR 1581 (Grand Chamber) at 124 where the European Court of Human Rights emphasised the special position of minors in the criminal-justice sphere, and that the retention of unconvicted persons' data may be especially harmful in the case of minors given their special situation and the importance of their development and integration in society. See also *R (on the*

- (a) Article 3 of UNCROC requires that the best interests of the child be a primary consideration in all actions taken in relation to the child; and
- (b) Article 40(2)(vii) requires that every child alleged to have committed an offence shall have their privacy fully respected at all stages of a proceeding.

159. United Nations guidance has been issued about the application of UNCROC including:⁶²

State parties should enact legislation and ensure practices that safeguard children's rights **from the moment of contact** with the [criminal justice] system, including the stopping, warning or arrest stage, while in custody of police or other law enforcement agencies, during transfers to and from police stations, places of detention and courts, and during questioning, searches and the taking of evidentiary samples. Records should be kept on the location and condition of the child in all phases and processes.

160. UNCROC uses the term "child" to refer to those under the age of 18. In the Oranga Tamariki Act, those in this category are defined as "children and young persons". In this report we use the generic term "youth" or "rangatahi".⁶³

161. When exercising powers under Part 4 of the Act (covering youth justice), Police officers must take into account the four primary considerations outlined at section 4A along with the youth justice principles outlined in section 208 of the Act. The four primary considerations in the youth justice context are:⁶⁴

- (a) the well-being and best interests of the youth;
- (b) the public interest (which includes public safety);
- (c) the interests of the victim; and
- (d) the accountability of the youth for their behaviour.

162. These primary considerations have regard to the principles set out in sections 5 and 208. The principles in section 5 include:

- (a) the youth must be encouraged and assisted, wherever practicable, to participate in and express views about any proceedings, process or decision affecting them and their views should be taken into account;

application of RMC) v Metropolitan Police Commissioner [2012] 4 All ER 510 and the risk of stigmatisation of those entitled to the presumption of innocence. See also Isabelle Peart, Josephine Booth and Amy Hancell "[Police photography of children in Queensland: An analysis of police powers and privacy rights](#)" (position paper presented for and on behalf of Caxton Legal Centre's Human Rights and Civil Law Practice, University of Queensland, May 2018) which examines concerns following a Police operation in Mount Isa to reduce crime in the area where children were being stopped and photographed by officers and asked for their name, address and where they were going.

⁶²Committee on the Rights of the Child *General Comment No. 24 (2019) on children's rights in the child justice system* UN Doc CRC/C/GC/24 (18 September 2019) at D.41; considered in *NZ Police v FG* [2020] NZYC 328; *NZ Police v LV* [2020] NZYC 117; *NZ Police v JV* [2021] NZYC 248.

⁶³See paragraph [14] above.

⁶⁴Oranga Tamariki Act 1989, s 4A(1) and (2).

- (b) the wellbeing of the youth must be at the centre of decision making that affects the youth, and in particular, the rights set out in UNCROC must be respected and upheld and the youth must be treated with dignity and respect at all times and protected from harm;
- (c) mana tamaiti (tamariki)⁶⁵ and the youth's wellbeing should be protected by recognising their whakapapa and the whanaungatanga responsibilities of their family, whānau, hapū, iwi, and family group.

163. The youth justice principles in section 208 guide the weighing of the primary considerations when exercising powers under the Act. In particular, the vulnerability of youth entitles them to special protection.

Special protections due to vulnerability

164. The Oranga Tamariki Act recognises that the vulnerability of youths entitles them to special protection during any investigation into possible offending by that youth.⁶⁶ The vulnerability that requires special protection to be provided to young people is based on their developmental immaturity.⁶⁷

As well as having limited life experience, a young person's capacity for consequential thinking is still developing and impulsive behaviour is common.

165. This requires that, among other considerations, the least restrictive response to offending should be preferred and that the youth's family, whānau, hapu, iwi and family group should participate in decision-making.

166. The Oranga Tamariki Act also recognises that the vulnerability of youths who are being investigated by Police in relation to alleged offending means that they should be dealt with in age-appropriate ways and that particular attention must be paid to protecting their well-being and best interests.

167. There are particular requirements under the Oranga Tamariki Act for Police to follow when engaging with youth. Section 48 applies where a youth is found unaccompanied or in a situation in which their physical or mental health is being, or is likely to be, impaired.

168. Section 48 is focussed on the wellbeing of the youth. Under section 48 a Police officer may:

- (a) using such force as may reasonably be necessary, take the youth; and
- (b) with their consent, return the youth to their home or in certain circumstances place the youth in the custody of Oranga Tamariki.

⁶⁵Mana tamaiti is defined as meaning "the intrinsic value and inherent dignity derived from a young person's whakapapa (genealogy) and their belonging to a whānau, hapū and iwi in accordance with tikanga Māori: *NZ Police v LV* [2020] NZYC 117 at [57].

⁶⁶Oranga Tamariki Act 1989, s 208(2)(h).

⁶⁷*NZ Police v FG* [2020] NZYC 328 at [145].

169. Other requirements include section 215, that sets out the warnings that Police officers must give a youth before being questioned; and section 218 that requires Police officers to give explanations to a youth under [section 215](#), [section 215A](#), [section 216](#) or [section 217](#) in a manner and in language that is appropriate to the age and level of understanding of the youth.⁶⁸

Limits on power to arrest

170. Another special protection is the limit in section 214 on the power of Police (as an “enforcement officer” for the purposes of the Act) to arrest a youth without a warrant. The Police Youth Justice policy explains that section 214 of the Oranga Tamariki Act limits Police powers to arrest youths and sets out the particular circumstances in which that section can be relied on.
171. Section 214 specifies that Police can arrest a youth in certain limited circumstances where the officer is satisfied on reasonable grounds that it is necessary to arrest the youth for the purpose of:⁶⁹
- (a) ensuring the appearance of the youth before the court;
 - (b) preventing the youth from committing further offences; or
 - (c) preventing the loss or destruction of evidence relating to an offence committed or preventing interference with a witness.
172. In addition, section 214A sets out the limited circumstances in which a Police officer may arrest a youth for breach of bail conditions.
173. Once a Police officer has arrested a youth in a manner consistent with their obligations under the Oranga Tamariki Act, the officer may then collect that youth’s identifying particulars using Police powers under the Policing Act.
174. Neither the Policing Act nor the Oranga Tamariki Act, however, empower Police to collect identifying particulars of individuals unless the individual is in custody as provided in Part 3 of the Policing Act.⁷⁰ The identifying particulars collected by Police in reliance on the Policing Act remain subject to a requirement that, if Police decide not to charge the individual or the outcome of the charges does not authorise continued storage, Police must destroy the particulars.

PRIVACY ACT 2020

175. Privacy is a human right, and the Privacy Act sets out broad principles to guide agencies in the collection and sharing of personal information. Because of the principles-based nature of the

⁶⁸*NZ Police v FG* [2020] NZYC 328 at [85]-[90].

⁶⁹Oranga Tamariki Act 1989, s 214.

⁷⁰However, Police officers do have powers under the Search and Surveillance Act 2012 to require an individual to provide certain identifying details in particular circumstances, such as during a vehicle stop if a police officer reasonably suspects the person has committed an offence.

Act, this part of the report gives an overview of how the privacy principles specifically apply to the photography of individuals by Police in public settings.

176. The purpose of the Privacy Act is to promote and protect individual privacy by:⁷¹
- (a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account; and
 - (b) giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the International Covenant on Civil and Political Rights.
177. The Privacy Act applies to Police activities that involve the collection, use, disclosure, and retention of personal information about individuals. Police collect personal information about individuals through a range of methods and in a range of different circumstances.
178. This includes the observation of individuals and activities in public spaces, from which Police can gather intelligence by making notes and records of these observations. This activity is apparent (rather than being covert) when a Police officer walks the streets and observes the community. Police officers are also called to incidents in public where they will need to assess situations and collect personal information. To investigate suspected offending, Police may run investigations that involve the observation of individuals on a covert basis, either through human observation or with surveillance devices.
179. Taking a photograph in these circumstances represents the collection of personal information, since personal information is any information about an identifiable individual. The Privacy Act therefore applies whether or not there are reasonable grounds to suspect that the photographed individual has committed an offence. Moreover, 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.⁷² 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.
180. The Privacy Act requires Police to have an appropriate reason (i.e. lawful purpose) for stopping an individual to talk to them when carrying out policing functions and collecting personal information from the individual about their identity, their associations with others and their

⁷¹Privacy Act 2020, s 3.

⁷²"Sensitive personal information and the Privacy Act 2020", above n 41.

activities. This reason or purpose will be relevant to whether it is appropriate to take a photograph of the individual as part of that interaction.

181. While Police may approach individuals and talk to them during their policing duties, the individual generally has the choice about whether to voluntarily provide their personal details or personal information (including photographs) on a lawful and reasonable Police request.
182. This is supported by the scheme of the privacy principles that applies concepts such as purpose and transparency, and embeds an authorisation framework, reflecting that the dignity of the individual is affirmed through individual autonomy and control over their personal information.
183. For example, the OECD collection limitation principle affirms that:⁷³

There should be limits to the collection of data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

184. Similarly, the OECD use limitation principle affirms that:⁷⁴

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except:

(a) with the consent of the data subject; or

(b) by authority of law.

185. These OECD principles are broadly reflected in the 13 privacy principles in the Privacy Act 2020.
186. The Privacy Act does not positively empower Police to take photographs of individuals in public places. Unless there is an express statutory power that over-rides the Privacy Act⁷⁵ (such as the provisions of the Policing Act, or as authorised under the Search and Surveillance Act), it operates only as a constraint on an otherwise lawful activity.
187. It is recognised in New Zealand law that Police have a residual freedom that government officials have to do things without express legal authorisation, except to the extent that the exercise of those powers is circumscribed by statute, would conflict with legislation or the common law or would breach protected rights.⁷⁶ This is referred to as the “third source” of authority and its scope is limited by any conflicting statutory or common law rules that apply.⁷⁷
188. The Privacy Act provides one such set of limits. Where Police photography is not consistent with these limits on collection for a necessary lawful purpose, with the result that Police are collecting

⁷³Privacy Act 2020, sch 6.

⁷⁴Privacy Act 2020, sch 6.

⁷⁵Privacy Act 2020, s 24.

⁷⁶*Review of the Search and Surveillance Act 2012*, above n 56, at [11.9]. In *R v Ngan* [2008] 2 NZLR 48 (SC) at [52] for example, Tipping J held that “If an ordinary citizen can lawfully do something, so can a police officer, **unless that officer is under some statutory or other constraint which does not apply to a private citizen**. Section 21 of the Bill of Rights Act is a good example of such a constraint. It applies to police officers but not to private citizens. Hence a police officer conducting a lawful search or seizure must pass the statutory criterion of reasonableness.”

⁷⁷*Television New Zealand v Rogers* [2008] 2 NZLR 277, at [110] per McGrath J.

information unlawfully (under IPP 1), seeking consent from the subject of collection does not make the collection compliant with the IPPs.

189. Not all Police actions require particular powers to be assigned under statute. Where a Police officer is undertaking their duties, their actions remain subject to a number of statutory and common law rules. These rules are constraints that do not apply to a private citizen. Where a Police officer collects personal information from someone, the Privacy Act places some limits on the officer's actions.
190. Where a Police officer seeks a surveillance warrant from the Court, the privacy impact of implementing that warrant has already been considered by Parliament when it set the terms, in the Search and Surveillance Act 2012, on which a warrant may be sought and granted. Where search and surveillance activities are carried out, lawfully, outside the Search and Surveillance Act, other rights instruments (including the Privacy Act) are still relevant to how those activities are carried out.⁷⁸

Privacy Act principles as constraint on Police action

191. The way in which these general principles⁷⁹ should operate as a constraint in practice depends on the strength of the policing purpose for the photograph and the particular circumstances that Police encounter. The collection principles 1-4 provide transparency and authorisation safeguards to the extent that these are proportionate to the policing purpose. But it also allows some flexibility to depart from these safeguards where necessary (e.g. to enable the Police to undertake covert photography or to take photographs of individuals without their consent where this is justified from the specific context). In every case there must also be a lawful purpose for the photograph, whether or not the person agrees to it being taken.
192. The constraints imposed by the Privacy Act are therefore flexible according to the factual circumstances and are principles-based. In other words, the privacy principles provide a framework for balancing the statutory expectations on Police to carry out effective policing and the public interest in public safety with the privacy interests of the individual. The extent of the Act's constraints on collection practices therefore depends on the nature and purpose of the Police activity and the extent of the intrusion into personal privacy.
193. In relation to Police photography, this includes the extent to which the photography is targeted at particular individuals as a form of intelligence gathering, and the extent of the privacy intrusion resulting from the collection (compared to other methods of collecting personal information). The extent of the privacy intrusion in taking photographs, and correspondingly the threshold for doing so, differs from Police observations and note-taking to record what an officer sees in public places (without approaching an individual), which are not impeded by the Privacy Act where Police have a necessary lawful purpose for doing so (IPP 1). Nor are officers

⁷⁸See Hon Christopher Finlayson [Ministerial Policy Statement: Conducting surveillance in a public place](#) (Minister responsible for the Government Communications Security Service and Minister in charge of the New Zealand Security Intelligence Service, Ministerial Policy Statement, September 2017). The statement notes that GCSB and NZSIS, to whom the MPS applies, are subject to the Privacy Act 2020 in a more limited way than Police.

⁷⁹ Privacy Act 2020, s 22: information privacy principles (referred to in this report as "IPPs").

constrained by the Privacy Act from seeking information from members of the public, informants and witnesses, as individuals are not impeded from providing information to Police to assist with Police enquiries.⁸⁰

194. However, the action of stopping an individual to speak with them and ask them direct questions about themselves and their activities, is a direct collection of personal information and is a more intrusive form of collection, where the individual is being asked to give their own personal information to Police as a law enforcement agency. This requires Police to apply the set of privacy safeguards from the Privacy Act, that are set out below, as to the purpose of the interaction (IPP 1), informing the individual (IPP 3) and ensuring fair manner of collection that is not unreasonably intrusive (IPP 4).
195. The action of taking a photograph of a person who has been stopped as the focus for Police interaction increases the level of intrusion, as the collection of that person's image represents the individual's unique characteristics, and the potential exists for the image to be retained and used to the individual's disadvantage.
196. This "direct" form of photography of the individual is therefore also subject to the Privacy Act's constraints, and departure from those constraints (where an exception to the IPPs applies) needs to be justified on a case by case basis. If a Police officer takes photographs of an individual outside their express powers set out in the Policing Act (or another framework expressly providing powers to Police), the Privacy Act (along with any other relevant rights-based frameworks) will apply.
197. A privacy decision from the English Court of Appeal considered Police photography of an individual following a company's annual general meeting at which Police assessed there was the potential for unlawful activity by a campaign group:⁸¹

But in my judgment it is important to recognise that state action may confront and challenge the individual as it were out of the blue. It may have no patent or obvious contextual explanation, and in that case it is not more apparently rational than arbitrary, nor more apparently justified than unjustified. In this case it consists in the taking and retaining of photographs, though it might consist in other acts. The Metropolitan Police, visibly and with no obvious cause, chose to take and keep photographs of an individual going about his lawful business in the streets of London. This action is a good deal more than the snapping of the shutter. Police are a state authority. And as I have said, the appellant could not and did not know why they were doing it and what use they might make of the pictures.

⁸⁰Note however the Privacy Act 2020 will regulate the collection of personal information by law enforcement from entities who are "agencies" under the Privacy Act 2020, and their disclosure of personal information to law enforcement. In some such cases section 21 of the NZBORA will need to be considered. See Privacy Commissioner [Releasing personal information to Police and law enforcement agencies: Guidance on health and safety and Maintenance of the law exceptions](#) (6 November 2017).

⁸¹*R (on the application of Wood) v Metropolitan Police Commissioner* [2009] EWCA 414 at 45. European judges have found that photography by state agencies to challenge the right to private life – see Jake Goldenfein "Police Photography and Privacy: Identity, Stigma and Reasonable Expectation" (2013) 36(1) UNSW Law Journal 256 at 261.

Collection principles

198. Taking a person's photograph during an interaction engages the collection principles 1-4 under the Privacy Act.⁸²
199. The collection principles require Police to:
- (a) have a lawful purpose for collection (IPP 1(1));
 - (b) consider the necessity of collecting the information and only take a photograph where necessary for a lawful purpose (IPP 1(1));
 - (c) consider whether the lawful purpose requires the collection of a person's identifiers through taking their photograph and only take a photograph if it does so (IPP 1(2));
 - (d) take reasonable steps in the circumstances to inform the individual about the purpose for which the photograph is being taken (IPP 3);
 - (e) ensure that the photograph is taken in a manner that is lawful and fair in the circumstances, particularly where youths are concerned (IPP 4); and
 - (f) ensure that the photograph is taken in a manner that, in the circumstances, does not unreasonably intrude on the individual's personal affairs, particularly where youths are concerned (IPP 4).
200. The collection principles do not act in isolation. Having a necessary lawful purpose (IPP 1) for engaging with an individual does not mean that these additional privacy safeguards (IPPs 3 and 4) can be disregarded when Police are taking photographs of individuals in public settings.
201. Where collection may be permissible under IPP 1, the other collection IPPs provide guidance on how collection should be carried out. In some cases, despite the threshold for collection under IPP 1 being met, it may still not be appropriate for personal information to be collected in the particular circumstances or in a particular way (including by photography, whether on an open basis or a covert basis).
202. Where Police are openly engaging with individuals and wish to take photographs or collect their identifying particulars, they should generally:
- (a) explain the reasons for obtaining a photograph and other personal information to the individual and what the photograph and personal information will be used for in accordance with IPP 3; and then
 - (b) obtain the individual's consent to take the photograph in order to demonstrate compliance with IPP 4's requirement for fair means of collection and protection against unreasonable intrusion, particularly with respect to children and young people.

⁸²See Paul Roth and Blair Stewart *Privacy Law and Practice* (online looseleaf ed, LexisNexis) at [PA7.5(ii)(c)].

203. IPPs 3 and 4 set the presumptive starting point for Police informing the individual and seeking their consent to the photograph being taken as a matter of fairness, although there will be particular circumstances where those steps will not apply. Whether there is a basis for an IPP 3 exception to notification or for limiting IPP 4 safeguards such as obtaining the individual's consent, needs to be considered by Police policy.
204. For example, circumstances where it may not be necessary to inform the individual are set out as exceptions to IPP 3 and include the situation where compliance with IPP 3 would create a risk of prejudice to maintenance of the law by Police as a public law enforcement agency, or would prejudice the purpose of collection, or would not be reasonably practicable in the circumstances. Where an IPP 3 exception applies, this lifts the usual constraint on Police photography that the individual must be informed, and will justify proceeding without doing so, subject to the requirements of IPP 4.
205. Under IPP 4, the assessment of fairness and the protection against unreasonable intrusion is also based on the particular context. This means that relevant factors may weigh against having to obtain the individual's consent under IPP 4 where Police face an urgent situation, there is a situation of risk to an individual or the public, or it is not possible or practicable to obtain the individual's consent without creating a risk of prejudice to a law enforcement investigation. The engagement of one or more of the IPP 3 prejudice exceptions will be relevant indicators that it will not usually be unfair in the circumstances to proceed to photograph without consent.
206. Such circumstances will lift the usual constraint on Police photography without the individual's consent, for example where Police are undertaking necessary covert photography to progress a Police investigation. This recognises that where Police are actively investigating offending, photography or video is an important tool to capture incidents and evidence.
207. For example, a special Police investigation into a trend in youth offending through car ram raids on shops to steal cigarettes, vapes and alcohol,⁸³ would enable Police to collect personal information about suspected and recidivist offenders, including photographs of youths and stolen cars where Police have a basis to suspect that the youth is actively participating in offending. In those circumstances, notification to the youth or their family in real time may be impracticable or prejudice the purpose of collection or the maintenance of the law, depending on the nature of the incident being observed and the stage of the investigation.
208. Obtaining the youth's consent (or their family or whānau) may also be impracticable in the circumstances of an active investigation where there is a close connection of the youth to live offending, and therefore very strong Police suspicion.
209. Nevertheless, the IPPs do not support a blanket approach to photographing individuals with common attributes (such as youth) without considering the particular circumstances at the time the photograph is taken. For example, under IPP 1 the reported increase in ram raids in a district would not justify a Police response involving photographing all youth encountered in cars in a district after 11pm each night.

⁸³"Social media, thrill seekers drive ram-raid rust – police" *Radio New Zealand* (online ed, Wellington, 13 April 2022).

210. The best interests of the young person and the relevant protections in the youth justice context must also be taken into account when assessing the basis for proceeding without first engaging with the youth and their whānau or family.
211. Where Police take photographs of a group or an individual on a covert basis (where the individuals are not aware of the photograph being taken), this also requires a privacy analysis under the principles as a check on the fairness and justification for the collection of personal information by covert means. Even where the identities of the individuals are not known at the time the photograph is taken, the image will be personal information about the individual where it comprises information from which the individual can subsequently be identified.

IPP 1: purpose of collection of personal information

212. Under the Privacy Act, when photographs or videos are being taken in public places, the starting point is IPP 1. This principle requires the collecting agency to identify why the personal information is being collected.
213. IPP 1(1) states that an agency must not collect personal information unless the information is collected for a **lawful** purpose connected with a function or activity of that agency, and the collection of the information is **necessary** for that purpose. IPP 1(2) further supports this by specifically affirming the limit on the collection of personal information in the form of identifying information (such as photographs) if there is no lawful purpose for collecting it.⁸⁴
214. IPP 1 is a mandatory consideration when collecting personal information through photography. This means that IPP 1 cannot be set aside on the basis of law enforcement imperatives such as efficiency, nor can IPP 1 be met through obtaining an individual's consent to be photographed.
215. If the requirements of IPP 1 are not met, there is no legal basis for the photograph to be taken, regardless of whether an individual consents. Taking a photograph without an adequate basis under IPP 1 can be an "overcollection" of personal information in breach of IPP 1 as the data minimisation principle.
216. To establish a lawful purpose for taking a photograph, Police must demonstrate that the photograph is being taken to support a lawful function of Police such as investigative policing, or associated intelligence gathering. If the lawful purpose does not require the collection of the individual's identifying information (such as a photograph) then the information may not be required to be given in the absence of a power to do so (IPP 1(2)).
217. If IPP 1 is satisfied, then Police must also consider how IPP 3 and IPP 4 apply.

IPP 3: collection of information from subject – informing the individual unless an exception applies

218. Whenever Police take a photograph when interacting with a person in a public setting, they must consider the requirement in IPP 3 to inform the individual, and whether one of the exceptions contained in that principle might apply.

⁸⁴IPP 1(2) was introduced in the Privacy Act 2020.

219. IPP 3 requires an agency to take reasonable steps to ensure the individual is sufficiently aware the information is being collected, and the purpose for collecting it.
220. IPP 3 protects the autonomy of the individual by allowing them to make an informed decision about disclosing their personal information in response to a law enforcement request. By requiring an explanation to be given, it provides the individual with an opportunity to refuse to disclose their personal information (which the individual is generally entitled to do in a situation where they are not being detained by Police) unless an exception applies in the particular circumstances.⁸⁵ It also enables them to exercise their rights under the Privacy Act to seek access to and deletion of the images in the absence of a lawful basis for their retention.
221. The general principle is that when photographing a person in public, Police must therefore take reasonable steps to ensure the individual is aware they are being photographed as part of their interaction with Police, and the purpose for this. An explanation must be provided to the individual before the information is collected (IPP 3(2)) unless it is not practicable to do so, in which case the explanation must be provided as soon as practicable afterwards.
222. One of the relevant circumstances when assessing the reasonableness of the steps to inform the individual is the sensitivity of the information being collected. Under the Privacy Act, there are higher expectations of transparency where the personal information being collected is sensitive.⁸⁶ As noted above, images taken by Police of individuals are sensitive personal information due to the strong link to a person's identity, mana, tapu and autonomy.⁸⁷
223. The open (and not covert) use of a camera will generally indicate to an individual that their picture is being taken, however Police also need to consider informing the individual during their interaction about the purpose for which the photograph is being taken, the individual's rights to access the photograph as personal information, and whether there are any consequences for the individual if the requested information is not provided (for example, if the individual does not provide their consent to the photograph being taken).
224. Exceptions will depend on the particular circumstances. For example, Police may have a good reason not to provide an explanation where they have a reasonable belief that informing the individual would prejudice the maintenance of the law (IPP 3(4)(b)(i), or that compliance would prejudice the purpose of collection (IPP 3(4)(c)), or that an explanation is not reasonably practicable in the circumstances (IPP 3(4)(d)), or that the information will not be used in a form in which the individual concerned will be identified (IPP 3(4)(e)).
225. These exceptions enable Police to carry out necessary and lawful collection of personal information, including covert photography, without informing the individual, provided there is

⁸⁵See [Practice Note on Police Questioning](#) High Court Practice Note [2007] 3 NZLR 297: A member of Police investigating an offence may ask questions of any person from whom it is thought that useful information may be obtained, whether or not that person is a suspect, but must not suggest that it is compulsory for the person questioned to answer.

⁸⁶See "Sensitive personal information and the Privacy Act 2020", above n 41, at 3.

⁸⁷In European privacy cases, the right to protection of one's image is one of the essential components of personal development and one of the characteristics attached to an individual's personality. See for example *Reklos and Davourlis v Greece* (EUHRC application no. 1234/05) which involves the photography of a newborn baby without the parents' consent.

a sufficient justification for the taking of a photograph in connection with the particular function being carried out, such as investigative policing.

226. Where an IPP 3 exception applies, Police will not need to take steps to inform the individual under IPP 3, but Police must also assess the considerations required under IPP 4.

IPP 3 exception where reasonable grounds to believe non-compliance necessary to avoid prejudice to the maintenance of the law

227. The maintenance of the law exception, under IPP 3(4)(b)(i), permits a law enforcement agency to bypass the usual notification requirement which protects the autonomy of the individual. The exception does not provide an explicit power for Police to do so. Rather, the exception provides justification, in particular circumstances, where Police reasonably consider there is a likelihood of prejudice to its proper policing functions.
228. It is not automatic that IPP 3(4)(b)(i) will apply to Police photography of an individual in public as being necessary to avoid prejudice to the maintenance of the law. That exception does not apply to situations simply on the basis of convenience or efficiency. Rather, the maintenance of the law exception requires that Police can articulate, in each case, a **reasonable belief**⁸⁸ that non-compliance with the notification safeguard is necessary.⁸⁹
229. Whether this IPP 3 exception is engaged will depend on the given situation and whether there is a reasonable basis for believing that informing the individual would create a prejudice to relevant policing functions. For example, Police need to consider what the effect would be if the person is informed about the purpose of collection. Would it prevent an investigation commencing or continuing? Is the situation urgent or threatening? Would it create a risk to the safety of the officer engaging with the individual? Can the information be collected from a different source?
230. The decision to rely on this exception in any particular case must be exercised reasonably by Police, by identifying the particular detriment to the maintenance of the law that notification to the individual would create, and with care and attention to the rights being displaced by reliance on the exception.

IPP 4: manner of collecting personal information

231. In addition to the requirements of IPP 1 and IPP 3, IPP 4 is a further mandatory consideration in the collection of any personal information from an individual, including by Police photography. IPP 4 requires the collecting agency to consider how it is collecting personal information, whether its process is **lawful** and **fair** in the circumstances, and, if the collection is **unreasonably**

⁸⁸Police must actually believe that the exception applies and there must be a reasonable basis for that belief. See *Releasing personal information to Police and law enforcement*, above n 80, at 5.

⁸⁹Although this exception has not been tested by the Courts in the context of IPP 3, we note that the “maintenance of the law” exception was considered in the context of IPP 2(2)(d) and IPP 11(e) in *R v Alsford* [2017] NZSC 42. See in particular at [33] and per Elias CJ dissenting at [182]–[184]. At [182] Elias J held that “... necessity is not shown simply by the request for the provision of the information by a law enforcement agency and its linkage with an investigation”.

intrusive on the individual, whether there are less intrusive means to collect personal information.

232. Firstly, IPP 4 requires the collection of personal information to be conducted by lawful means. Where personal information is collected in breach of a statutory prohibition for example, or beyond the scope of an authorising instrument such as a search warrant, an unlawful collection would be a breach of IPP 4(a). Police photography of members of the public in public places does not generally give rise to the need for analysis under IPP 4(a) as photography in public is not an activity that engages the criminal law except in quite specific terms under the Crimes Act or Search and Surveillance Act.
233. Secondly, IPP 4(b) requires that the collection of personal information, such as photographing members of the public, must be both fair and not unreasonably intrusive on the individual's personal affairs. IPP 4(b) of the Privacy Act now emphasises the need to have particular regard to these considerations where personal information such as photographs is being collected from children and young people.
234. IPP 4(b) therefore requires assessment of the fairness and intrusiveness of the collection, and the manner of collection may require adjustment to ensure that these standards are met. Where it is not possible to collect the personal information in a manner that is fair and not unreasonably intrusive, the personal information should not be collected, unless the manner of collection can be adjusted to mitigate that unfairness and intrusion.
235. While there are no specified exceptions to IPP 4,⁹⁰ there is flexibility as to how IPP 4(b) can be complied with in relation to a particular activity such as Police photography. This enables Police to develop policies and procedures that ensure that Police officers are taking photographs of members of the public, in particular rangatahi and other youth, in a manner that is fair and reasonable. This ensures that the action of taking photographs in the exercise of Police functions is proportionate to the specific purpose for collecting personal information about an individual member or members of the public. It is in this context that the consent of an individual can be an important procedural step to ensure that Police comply with IPP 4.

IPP 4 and informed consent

236. When taking photographs of individuals in public places in the absence of a specified power, officers need to routinely consider if obtaining the consent of the individual is necessary to ensure fairness and limits on unreasonable intrusion in the collection of personal information.
237. Even where the individual is informed about the purpose of taking a photograph (IPP 3), the fairness and intrusiveness of doing so also requires particular consideration where an officer is openly interacting with an individual (as distinct from undertaking passive distant observation without speaking to the subject).
238. Firstly, where Police are interacting with members of the public in a context that involves taking photographs, doing so without the individual's consent is presumptively unfair where the

⁹⁰In particular, it is not possible to comply with IPP 4 where the manner of collection is not lawful.

individual cannot lawfully be compelled to provide their personal information and retains a choice about whether to engage in the interaction.

239. Secondly, because interactions between Police and members of the public carry an inherent power imbalance, there is a question of fairness and whether the photograph is unreasonably intrusive. This is acknowledged in Police's Youth Justice policy:

Remember that your actions and the image you project will have exaggerated importance and could have a lifelong effect on the child's or young person's attitude towards Police.

240. Thirdly, the collection of personal information by 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.
241. 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.
242. It will not always be necessary for a Police officer to obtain consent from a subject before taking a photograph, for example, where Police officers have a specified power allowing a photograph to be taken. There will also be particular circumstances where it is not necessarily unfair or intrusive to take a photograph without consent, for example, in an urgent situation or in a situation of evident risk to an individual or the public, or where it is not possible or practicable to obtain consent without creating a disproportionate risk of prejudice to a law enforcement investigation.
243. If the individual does not give their consent on request, the photograph should not be taken unless proceeding without consent is proportionate to the importance of the photograph for an investigation, and outweighs the fairness to the individual, who should be informed that the photograph is mandatory.⁹¹
244. If an individual declines to consent to a photograph, and proceeding without consent is not proportionate, this does not necessarily limit Police from collecting personal information by alternative means, for example, making general enquiries of individuals without taking photographs, and taking notes from those enquiries to the extent that the individual is willing to participate in the interaction with Police.
245. IPP 4 is not limited to situations where the individual is aware of the photography. Covert photography must also be assessed under IPP 4 and whether the collection of personal information is fair (particularly in relation to youth). The IPP 4 analysis of fairness and

⁹¹Privacy Act 2020, IPP 3(1)(e)(ii).

unreasonable intrusion is important as a check on the purpose for taking the photograph and whether a covert manner of collection is justified. This requires articulating the justification for covert collection – and whether it is necessary to do so without the individual’s knowledge or consent.

246. The fact that an individual may not consent to the photography if they knew about it is not an adequate reason to opt to take photographs covertly. The policing imperative must provide an adequate justification for covert photography in public settings.

Youth justice considerations

247. Police processes for collecting personal information from youth must be appropriately tailored to reflect the statutory protections for youth. This emphasis in IPP 4, combined with the additional protections for youth under the Oranga Tamariki Act and UNCROC and the need to consider the youth’s best interests, must be taken into account by Police when engaging with youth, including through photography, and ensuring fairness and appropriate limits on unreasonable intrusion.
248. Where it is necessary to seek the individual’s consent to comply with the IPP 4 standard of fairness, there are particular considerations for the manner of engaging with youth. As this is a particular consideration under IPP 4, Police cannot therefore apply a standard procedure to the collection of personal information from adults and youth or necessarily assume that, because the collection of personal information in a particular context is fair and lawful in relation to adults, it will also be fair and lawful in relation to youth.
249. Under the Oranga Tamariki Act, Police must inform the youth of their rights before the youth is questioned. This includes explaining that the youth is under no obligation to make or give a statement, the right to withdraw consent for a voluntary statement at any time, and the right to consult with a lawyer, family or whānau member or other adult to assist their understanding and to provide support. Explanations must be given in a manner that is understandable for the youth, taking account of their age and level of understanding.
250. To meet the standard of fairness under IPP 4 and to ensure that the substantive youth protections are not undermined, those protections need to be applied to Police interactions with youth involving photography. The Police Youth Justice policy notes that the vulnerability of youth means they require special protection during any investigation and therefore acknowledges that Police will take the purposes and principles of the Oranga Tamariki Act into account when responding to offending by youth, will provide special protection for youth during any investigation and will consider and implement effective and meaningful alternative actions with youth.

Storage, access, retention and use principles

251. In addition to the collection privacy principles 1-4, other privacy principles are relevant to the storage of photographs by Police (IPP 5), access to photographs by the individuals concerned (IPP 6), the period for which the photographs are retained by Police (IPP 9) and the purposes for which the photographs can be used by Police (IPP 10).

IPP 5: storage and retention of personal information

252. IPP 5 requires Police to ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information. Steps such as password protecting files and limiting access to certain types of files can be effective ways of minimising the risks

IPP 6: Access to personal information

253. IPP 6 states that people have a right to ask for access to their own personal information. Generally, an agency must provide access to the personal information it holds about someone if the person in question asks to see it, unless one of the refusal grounds in Part 4 of the Act applies. One refusal ground is where the disclosure of personal information to the requester would be likely to prejudice the maintenance of the law by a public sector agency, including the prevention, investigation and detection of offences and the right to a fair trial.⁹²

IPP 9: Retention of personal information

254. IPP 9 states that an agency should not keep personal information for longer than it is required for the purpose it may lawfully be used.
255. An agency must be satisfied that personal information it holds may be lawfully used in order to meet its obligations under IPP 9. Accordingly, the purpose for which the agency has collected the information will inform the length of time for which the agency can hold and use that information.
256. IPP 9 is incompatible with indefinite retention.⁹³

IPP 10: Use of personal information

257. IPP 10 states that an agency can generally only use personal information for the purpose it was collected.
258. Sometimes other uses will be allowed, for example, if the other use is directly related to the original purpose or if the person in question authorises a different use of their information. It is important for an agency to be clear about the purposes for which it collects information in the first place, in order to ensure that it is consistent in the way that it uses the information later.

⁹²Privacy Act 2020, s 53(c).

⁹³See Privacy Commissioner Case Note 218236 [2011] NZPriv Cmr 4. European case law has also held that blanket retention of biometric information of persons suspected but not convicted of an offence to be a disproportionate interference with the privacy rights; see *S and Marper v United Kingdom*, above, n 61.

3 CONSISTENCY OF POLICE PRACTICE WITH RELEVANT LAW

INTRODUCTION

259. This part of the joint report assesses the consistency of Police practice with relevant law and includes the joint inquiry team's findings about the extent to which Police practice is consistent with the Privacy Act and relevant legislation. It also makes recommendations for improvements to Police policy and practice.
260. As noted above, where Police collect personal information by taking photographs of individuals in public places without any specific statutory authorisation,⁹⁴ or where not regulated by other statutory frameworks such as the Search and Surveillance Act, officers must comply with the Privacy Act and the IPPs.
261. A particular issue for the joint inquiry has been the review of Police practices in different policing contexts and whether or not the individual's consent is obtained for a photograph to be taken. This includes where Police practice has been to obtain the individual's consent in order to overcome limits that otherwise apply. We have also reviewed Police practice of taking photographs in public settings (such as the rangatahi incidents) without obtaining the consent of the individual and whether this is consistent with the constraints in the Privacy Act.
262. In large part, this part of the report is based on information gained from interviews with Police officers and staff regarding their understanding of their legal obligations relating to photography of members of the public and practices relating to the fingerprinting of youths. The joint inquiry team observed during interviews with officers that most officers had a very limited understanding of the Privacy Act. However, a number of officers expressed interest in receiving training on the Privacy Act.
263. The joint inquiry team reviewed the Police policies listed in Appendix 1A. We found that, although Police have many policies that reference photographing, few officers are aware of the existence of any of them apart from those officers in specialist teams such as Youth Aid or the Criminal Investigation Bureau.

Understanding of NZBORA

264. As the result of our interviews and discussions with Police officers and staff it is apparent to us that a significant number of those we spoke to do not have an understanding that the New Zealand Bill of Rights Act 1990 applies to constrain their actions outside the more obvious applications in the policing context (e.g. search and surveillance and arrest).

⁹⁴An example of such an authorisation is under the Policing Act where Police are specifically authorised by statute to take photographs or collect fingerprints from individuals, when an individual has been arrested or when Police intend to prosecute an individual by way of summons. See Policing Act 2008, ss 32 and 33.

265. Sections 21 to 24 are particularly relevant to Police and represent constraints on Police action through protecting the right to be secure from unreasonable search and seizure, the right not to be arbitrarily detained, the rights of persons who are arrested or detained and the rights of persons who are charged.
266. The joint inquiry team noted that some officers interviewed did not demonstrate sound understanding of how the principles contained in sections 21 to 24 apply in practice and how those sections act as a check or restriction on Police actions in this context. For example, some officers told us that section 21 of the Bill of Rights Act gave them **the right** to stop and search individuals, as long as it was not unreasonable. Officers expressed a view that this meant that they could also take photographs when doing so.
267. In addition, some officers did not seem to have an adequate understanding of section 22 of the New Zealand Bill of Rights Act – the right not to be arbitrarily detained. They did not appreciate that stopping people for no particular purpose or for a purpose that did not relate to the statutory authority that they were using to justify stopping a person could be a breach of section 22.

Outline of this section

268. The following discussion and findings cover:
- (a) policing scenarios involving photography of members of the public representing the collection of personal information and, in particular, the collection of photographic images and biometric prints from youth;
 - (b) the use of this personal information once Police have collected it;
 - (c) the storage, security, retention and disposal of this personal information;
 - (d) the application to specific rangatahi complaints; and
 - (e) general findings relating to consistency of Police practice, guidance, training and policies

A ISSUES RELATING TO COLLECTION BY PHOTOGRAPHY AND OTHER IDENTIFYING PERSONAL INFORMATION

269. This section assesses the consistency of Police practice with relevant law with respect to the taking of photographs in different policing scenarios. This includes Police intelligence gathering, investigations, and policing in other particular situations such as protests and gatherings.
270. This section also assesses consistency of Police practice with relevant law with respect to the taking of photographs in different policing scenarios involving interactions with youth. This includes Police practice with respect to informal, casual or voluntary photographs and the application of this practice to youths, as well as the collection of biometric prints.

Introduction and initial observations

Key issues identified

271. The joint inquiry team has identified the following key areas of concern:

- (a) lack of understanding about the role of the Privacy Act and that Police must take the IPPs into consideration when taking photographs of individuals in public places;
- (b) lack of clarity about the threshold under the Privacy Act for taking photographs of a member of the public for both non-crime scene identification and general intelligence gathering ; and
- (c) lack of understanding about the role of consent – both whether (and if so, when) Police need to seek consent from an individual to take their photograph, and whether the provision of consent is a basis for authorising Police to take the photograph.

272. Of concern to the joint inquiry team is the fact that individual officers were not aware of their obligations under the Privacy Act when taking photographs of individuals in public places. The view of the joint inquiry team is that Police need to make a concerted effort to develop policies in this area, and to train officers to understand that Police activities in public places are regulated by the Privacy Act, where those activities involve the gathering of personal information.

273. In addition, most Police officers and staff we interviewed did not fully understand the rights afforded to youth when collecting personal information from them.

Informal, casual and voluntary photographs with consent

274. One key area of concern to the joint inquiry team is the lack of clarity about the threshold Police applies before taking photographs of members of the public.

275. The joint inquiry has observed that it is common for Police officers to take photographs in public situations and a widespread practice has developed within Police where officers routinely take ‘casual’ or ‘informal’ photographs of youth or adults without clearly linking the need to take a photograph to a particular purpose or considering whether the photograph is necessary.

276. The joint inquiry team found that Police were taking photographs in public not only when investigating an offence, but also for other reasons, including what is broadly described as intelligence gathering. These photographs are taken for a variety of reasons, typically to identify a person of interest who may or may not be linked to offending or suspected offending.

277. During interviews the joint inquiry team also noted frequent references to ‘informal photograph’, ‘voluntary photograph,’ or ‘casual photograph’. These terms have entered the Police vocabulary and are used as accepted everyday language to describe the taking of photographs of individuals in public settings or without relying on an express statutory power. These are not official Police terminology or practice, nor taught to recruits at the RNZPC, but our interviews suggest the terminology has become widespread in practice.

278. Casual photographs were reportedly taken in a variety of situations. Typically, this was reported as being for general identification purposes, allowing officers to identify someone for future reference, rather than to link an individual to a specific event. For example, in a number of interviews, we were told of situations where officers would take photographs of people they were trying to identify and then text the casual photographs around to other officers to see if they could identify who they were talking to.
279. Regarding adults, the photographs would be taken as part of canvassing an area, when stopping vehicles, if an officer suspected they were provided with false details, or when issuing a summons, or a trespass or suspension notice.
280. Photographs were also being taken when transporting youths back home, either via a casual car ride offered by Police, or when officers were engaging with youths under section 48 of the Oranga Tamariki Act.
281. The joint inquiry team was particularly concerned about many instances of officers describing taking photographs of people simply because they *“looked out of place”*, whether that be because of age, manner of dress, location or time of day or night, or any behaviour which officers took as a signal that a photograph should or could be taken. This raises a risk that certain individuals may attract Police attention based on informal profiling (raising a risk of unconscious bias) rather than a disciplined and objective analysis of the purpose and necessity for taking a photograph required under the Privacy Act framework.

Lack of consistency of practice

282. Officers commented that taking photographs was encouraged but it was not a directive issued by management. As a result, the joint inquiry team found a lack of consistency in the way in which photographs are taken.
283. Some officers might write in their notebooks, noting that they have taken photographs of the person they were speaking to. Others do not. Photographs are sometimes taken with some level of verbal consent obtained and sometimes without consent, whether done in an obvious or surreptitious manner. There appeared to be differing practices around what exactly adults or youth are told in relation to the collection, purpose and retention of, and the need for them to consent to, the photographs obtained.
284. There were many examples provided to the joint inquiry team of what occurs when an officer wishes to take a photograph of someone. Often, no explanation would be offered to the individual about why the officer was taking a photograph (unless it was to say Police wanted to rule them out of being involved in the recent/nearby offending). Typically, no explanation would be provided by the officer about what would happen to the photograph, for example, how it would be used or how long it would be retained for.
285. One officer told us: *“Your intention for the right outcome dictates how the photograph is taken”*. In other words, if the officer was of the view that the taking of a photograph was justified but the individual was unlikely to give their consent to be photographed regardless of the

information the officer provided, the officer would simply take the photograph without even attempting to obtain informed consent.

286. There was confusion from officers around what ‘informed consent’ meant, when it should be obtained and how to effectively communicate with an individual from whom consent was being sought, i.e., what to tell someone in order to obtain fully informed consent.
287. Over the course of our interviews, officers expressed the belief that they had a common law right to photograph people in public.⁹⁵ As a result, many officers believed that, like any member of the public, they are entitled to photograph anyone in a public place. Comments in interviews suggested that many officers were not aware of any limits, such as the Privacy Act, on their entitlement to photograph people in public.
288. The joint inquiry team observed a general view amongst officers, expressed in interviews, that if members of the public could take photographs or videos of Police performing everyday duties, officers were entitled to film them back.
289. It became clear during the joint inquiry that Police do not have an official policy on the taking of casual or informal photographs. There is also very little policy around the taking of so-called voluntary photographs (relying on a person’s consent).⁹⁶
290. It is of concern to the joint inquiry team that where they exist, Police policies that reference obtaining photographs (or biometric prints such as fingerprints) without a statutory power do not clearly explain the lawful basis for obtaining them, nor do they provide direction to officers on the steps to determine the lawful purpose.
291. Officers did appear to self-regulate to some degree. Most of the officers who told us they believed they had the right to photograph anyone in a public place also told us that, in practice, they would limit the situations in which they take photographs. Many officers instinctively recognised that taking a photograph could be an intrusion on a person’s privacy and spoke in general terms about needing some basis to believe an individual may be linked to some offending. However, officers were generally unable to articulate a consistent threshold for when it would be appropriate to photograph someone for non-crime scene identification.

General policing scenarios involving taking photographs (collection)

292. Here we summarise the different policing scenarios considered by the joint inquiry team together with our findings, under the following categories involving the collection of personal information through taking photographs:

- (a) intelligence gathering scenarios;

⁹⁵The officers’ belief reflects the advice Police give to members of the public about photographs taken (by members of the public) in public spaces. See for example New Zealand Police “[What are the rules around taking photos or filming in a public place?](http://www.police.govt.nz/what-are-the-rules-around-taking-photos-or-filming-in-a-public-place/)” <[www.police.govt.nz/](http://www.police.govt.nz/what-are-the-rules-around-taking-photos-or-filming-in-a-public-place/)>.

⁹⁶This is covered in the Police “Responding to youth offending and related issues” policy in the context of obtaining photographs and biometric prints from youth. However, we address the issues with the Police approach to obtaining this information from youth later in this report.

- (b) specific investigations;
- (c) other specific scenarios such as check points, protests and large gatherings and other interactions with the public; and
- (d) scenarios involving Police engagement with youth (and including so-called voluntary biometric prints).

(a) *Intelligence gathering*

293. The collection of photographs and video recordings as part of general intelligence gathering is widespread and an area we have identified as being of concern. We are concerned that many of the frontline officers interviewed appeared to lack an adequate understanding of how the Privacy Act and other relevant legislation applies in this context.
294. In addition, the joint inquiry team has identified a lack of clear, consistent Police policy guiding officers on the circumstances in which it is appropriate and lawful to collect photographs and video recordings for the purposes of gathering intelligence under the Privacy Act.

(i) *General observations on photography for intelligence gathering*

295. 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. From an investigative perspective, Police believe that the more information they have, the better. However, officers must always keep in mind the relevant legal and policy framework when collecting personal information as part of any investigative exercise.
296. Frontline officers identified intelligence gathering as one of the most common reasons for photographing members of the public. This was consistent across districts, although there were clear differences between individual officers (even within the same district). Officers we interviewed recognise the tension between investigative policing and legal compliance. However, the way individual officers deal with this tension varies widely.
297. While many officers described taking photographs for intelligence purposes as a routine part of their practice, other officers were clear that their preferred method of gathering intelligence was to talk to members of the public and take notes. The joint inquiry team also found that experienced officers – particularly those who had been in Police since before the issuing of smartphones became widespread – were often less likely to rely on taking photographs for intelligence gathering purposes.
298. The observation of the joint inquiry team is that broad surveillance through 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.

299. One reason for this is that unless data such as photographs is linked to a particular investigation, Police lack the systems to organise and categorise them. Further, unless officers take steps to save the photograph somewhere alongside notes on the relevance and significance of the photograph, it is difficult for them or other officers to look back at those photographs and gather any useful information.

(ii) Issues with Police's approach to taking photographs of youth in public for intelligence purposes

300. The joint inquiry team heard that photographs of youth in public places are commonly taken by Police on their mobile devices if officers see a youth who looks 'suspicious' because they are out late at night without any obvious reason, or during school hours in circumstances suggesting they could be truanting.
301. The Inquiry observed that officers interviewed had a limited understanding of the Oranga Tamariki Act. there was widespread belief amongst the officers we interviewed that there was no difference between photographing adults or youth for this purpose, with some officers explicitly stating in their interviews that they did not believe that youth are afforded any extra rights or protection in such circumstances.
302. The joint inquiry team notes that under section 218 of the Oranga Tamariki Act it is not sufficient for Police to simply "inform" a youth of the reasons for collection and use of voluntary photographs. The Oranga Tamariki Act states that Police must "explain" all relevant information in an appropriate manner and language in view of the youth's age and level of understanding. The inquiry team observed from interviews that officers routinely fail to provide any detailed information to youth or their parents or caregivers. Photographs are taken even when the verbal request for consent is refused. Officers are asking to take a photograph as they take the photograph, thus assuming consent from the person. In addition, we were also told that officers discreetly or covertly take photographs when another officer is talking to that person, even when the photograph(s) have been declined or the person has not been informed of the intent to take photographs.
303. A typical approach we found taken by officers when obtaining photographs and requesting consent would be holding out their mobile device (with the camera function on) and taking a photograph of the youth, whilst saying at the same time "You OK if I take a photograph of you?" or "I'm just going to take a photograph of you".
304. The issue with this approach is that it does not meet the collection requirements under the Privacy Act framework, nor does it reflect the principles to be applied when Police are engaging with youth under the youth justice framework.
305. There are particular considerations of fairness when Police are seeking the consent of a youth to be photographed in a public setting, including the need to properly explain the purpose for the photograph and what it will be used for in an understandable way. In cases where consent is being sought for the photograph, the request for consent should not be cursory, but should properly allow the youth and their whānau or family the choice to decline to consent.

(iii) Intelligence gathering and gangs

306. Gathering intelligence on gangs and gang members is an aspect of policing that featured heavily in our interviews with frontline Police staff. Officers see this as an important part of their work, and as a purpose for which photographing members of the public was overwhelmingly seen as necessary and lawful. This view and this practice appeared to be consistent across all Police districts.

307. Officers described taking photographs of gang members as being something they do as a matter of course. We heard that some officers will, wherever possible, photograph anyone they see in gang clothing. As one officer told us:

I have on occasion taken photos of gang members recently because I wasn't sure who they were. They weren't doing anything wrong but I just – it was more of an intelligence gathering thing for me and to find out who they were...

308. The comment above is consistent with the approach described to us by many frontline Police staff we interviewed. The officers we spoke to, described their encounters with gang members as an opportunity to build up intelligence on gangs and explained that taking photographs is the method most often used. Photographs were often taken openly, although some officers prefer to take photographs in a covert manner. Importantly, these photographs were often taken regardless of whether any specific offending was suspected and, in our observation, seemed to be unrelated to a particular investigation.

309. This practice extends to other contexts in which Police are exercising their functions. During the course of the joint inquiry, the IPCA considered a complaint about an incident involving Police gathering of gang intelligence in the course of executing a search warrant on private premises. In this case, Police entered a house under a search warrant, issued under the Search and Surveillance Act. The search warrant related to an allegation of causing harm by posting digital communications (an offence under the Harmful Digital Communications Act). While in the house, Police took photographs of occupants who were not the subject of the warrant, as well as of various other items in the house.

310. When asked for the basis for taking these photographs, Police accepted they were unrelated to the purpose of the search warrant, but said they were for intelligence gathering purposes (as the house was allegedly gang-linked). Police consider that they were authorised to take these photographs by section 47(1)(a)(ii) of the Search and Surveillance Act and section 24(2) of the Privacy Act.⁹⁷

311. As the issue concerns Police authorisation for photography, the IPCA referred the incident to the joint inquiry for comment and a finding in this report. The joint inquiry's finding is that the Search and Surveillance Act does not authorise Police to take these photographs during the execution of a search warrant for purposes of unrelated intelligence-gathering, as there are constraints on Police photography on private premises.

⁹⁷Section 24(2) of the Privacy Act limits the application of the collection privacy principles if an action is authorised or required under New Zealand law, including the Search and Surveillance Act.

312. The relevant constraint here is the principle of legality – that, in order to be lawful, Police action must be consistent with the source of authority (or powers) being exercised to enter private property. Police derive the power or authority to enter private premises from the consent of the occupier, or from the Search and Surveillance Act (to execute a search warrant) or from other statutes.⁹⁸
313. There are also potential issues with Police photography on private premises for intelligence gathering purposes under section 21 of NZBORA (covering unreasonable search and seizure). The nature of the privacy interest in private property, compared to public places, means there are tighter constraints on Police activity in those places.⁹⁹
314. The relevant source of authority to enter will set the limits and constraints for Police actions while present on private premises. For example, under the Search and Surveillance Act, Police can rely on the plain view principle codified in section 123; and Police are entitled to use their powers of observation while lawfully in private premises.
315. Section 47 of the Search and Surveillance Act is an exception to the requirement in section 46 that certain surveillance activities require a surveillance device warrant. However, that exception should not be read as a broad permission for Police to take photographs on private premises for unrelated purposes.
316. The purpose of that provision is to clarify that specific separate authorisation for the use of surveillance devices (such as cameras) is not required when either the use of the devices is otherwise authorised or where Police are exercising the general right to observe and record those observations while lawfully present on private premises. While Police may observe persons and items present on the property, that function should be linked to the purpose of entry, and there is arguably no basis for recording that observation via photography if it is not linked to the basis for the lawful presence.¹⁰⁰
317. Therefore, section 47 should not be considered by Police as a permission to take photographs for unrelated purposes, as that would intensify the intrusion into private places by extending the Police’s search focus in a manner that is inconsistent with the basis for the authority to enter.
318. 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.

⁹⁸See for example inspections under the Arms Act 1983, s 24B.

⁹⁹See Blanchard J in *Hamed v R*, above n 54, citing McGrath J in *R v Ngan* as to a search having the underlying idea of “an examination or investigation for the purpose of obtaining evidence”. But he would also have included “situations where the state undertakes examinations and investigative activities of a kind that significantly intrude physically on private zones albeit for purposes other than gathering evidence”.

¹⁰⁰ *Tararo v R* [2012] 1 NZLR 145 (CA).

(iv) Monitoring suspicious activity and unknown individuals

319. It appears to be common Police practice to photograph individuals involved in activity deemed suspicious. When we asked officers to broadly describe what they would consider to be a “suspicious activity”, we found most were unable to explain with any specificity what would lead them to photograph someone.
320. One of the concerns of the joint inquiry team is that there did not appear to have been sufficient assessment by individual officers, or Police as an organisation, as to when supposedly suspicious activity reaches a threshold where photographing the individual involved is appropriate.
321. Certainly, the practice among individual officers varies. Some officers prefer to speak with members of the public and rarely, if ever, take photographs in this situation. This approach was summed up by one officer who told us:

If I see something I think is suspicious, I generally won't take a photo. I'll go and speak to the person to see what's going on.

322. This approach was not unusual amongst the frontline officers we interviewed. However, for every officer who favoured this approach, another officer would apparently default to photographing people deemed “suspicious”. The following quotes were characteristic of the responses we received when we asked about the practice of photographing suspicious activity:

... anything that was out of the ordinary would be the most general term to describe it. So, out of the ordinary and you thought it might be useful. Grabbing a photo seemed like a good thing to do to try to prevent or later solve a crime.

Circumstances would include if we see some sort of, someone's behaviour like something suspicious and we come across someone and maybe we don't know if we have an offender yet or not. We might take a picture of what they're wearing in case we're wanting to find out later, particularly youth because we've been advised to do that.

323. Officers also described taking photographs not only of individuals involved in “suspicious activity”, but also individuals deemed suspicious because officers did not know who they were. Officers described two different situations in which they would photograph unknown individuals. The first was specific to smaller communities, and arose when officers encountered a person or vehicle they were not familiar with. Some officers in these smaller centres told us they would want to know who the individual was and, ideally, what they were doing in the community. To assist in this, they would sometimes take photographs, whether covertly or while speaking to the individual.
324. The second situation was specific to youth. In this case, many officers told us they would photograph youth they did not recognise who were seen mixing with other youth the officers considered to be active offenders. Officers said they would photograph these unknown youth to get an idea of the make-up of the various groups, and to build up a picture of these new youth with a view to potentially engaging in early intervention before these youth also engage in criminal behaviour.

325. We commonly heard officers use phrases such as things being “*out of the ordinary*” and taking photographs “*in case we’re wanting to find out later*”. This suggests that officers are commonly taking photographs based on an inarticulable suspicion in case they potentially become useful at some undefined point in the future.
326. This was consistent with what officers told us when we asked about their power to take photographs of members of the public. Most officers expressed the view that they are entitled to photograph anyone in public, just as any member of the public is. However, most officers also told us that they do not take photographs indiscriminately, but only when they have “a reason”. The difficulty came when they were asked to explain what they would consider to be a good reason. We were told repeatedly that it would depend on “*time, place, circumstance*”.
327. This is not an adequate threshold to ensure there is a necessary lawful purpose for the photograph to comply with IPP 1. We are therefore concerned that the current approach may be leading officers to take photographs based on hunches alone, without proper assessment of whether the photograph is necessary to support their lawful policing purpose.
328. In these situations, whether photographing individuals considered to be engaged in suspicious activity, or photographing new or unknown faces, the joint inquiry team finds that officers’ lack of understanding of the law and lack of guidance in Police policy has resulted in no clear threshold for the taking of photographs of members of the public. The likelihood is that Police practice will have resulted in the systemic over-collection of personal information in breach of IPP 1.
329. The joint inquiry team considers that it is necessary for officers to turn their minds to the Privacy Act principles and deliberately consider whether the activity they observe or the circumstances in which they encounter an individual are objectively suspicious, such that the taking of a photograph can be justified. At the end of this section, we set out our conclusions about the IPP 1 threshold we consider Police should be applying.

(v) Monitoring known offenders

330. Many officers we spoke to described the practice of taking photographs whenever they encounter “known offenders”. In the words of one officer:

If I see someone that I know...you know, his name’s popped up before in other information or something and then I’m like “Oh...who’s that? Who’s he with or what’s he driving?” and he’s in an area where I can photograph him, yeah, I’ll take a photo because I know it’s in the interests of Police to record what he’s doing or who he’s with and that may feed in somewhere.

331. Many officers expressed the view that keeping tabs on people they label as “known offenders” is an effective way of both deterring offending by these individuals and solving investigations into reported offending. By having a photographic record of where an offender is and what they are wearing at a particular time, officers believe they may be able to later link that individual to reported offending.
332. In terms of who officers considered to be a “known offender”, many officers we spoke to appeared to include individuals who have not been convicted of any offending, but who Police

merely suspect are involved in criminal behaviour. Several officers told us that their superiors or their Youth Aid sections emphasise the value of, whenever possible, photographing youth known or suspected of being involved in offending. These officers told us that, as a result, in practice they photograph youth more frequently than they do adults.

333. However, we were told that there has been some change to this practice over the past year. The media attention arising out of the original complaint from Wairarapa had resulted in officers being discouraged from photographing youth in some Police districts. This seems to be an interim position some districts have adopted until a review of Police policy is completed. As a result, some officers who would previously have taken frequent intelligence photographs of youth offenders are no longer, or very rarely, photographing youth.
334. We consider that Police's approach to monitoring known offenders based on subjective criteria is problematic. If subjective judgements are being made about taking photographs based on the officer's perception of the individual being monitored, rather than on the necessity for taking monitoring photographs based on the particular circumstances, there is a risk that Police photography will have resulted in the systemic over-collection of personal information in breach of IPP 1. Even if focused more narrowly on individuals who have established prior convictions, Police monitoring and photographing known offenders need to comply with the necessity threshold in IPP 1.
335. The reliance by Police on a subjective standard for monitoring individuals, creates the risk of an overly broad exercise of discretion by Police officers as to who they monitor and photograph and the potential for surveillance. This raises issues of unfairness and undue intrusiveness, as it could lead to individuals who have not necessarily been involved in criminal offending finding themselves under increased scrutiny and surveillance by Police in potential breach of IPP 4. In particular, this could increase the risk of bias when determining who Police target for monitoring, with particular groups being disproportionately impacted.
336. We therefore do not consider that it is appropriate for Police to photograph an individual based solely on their presence in a public place and their actual or perceived status as a known offender. When Police encounter a known offender in a public place, whether it is appropriate for Police to photograph that individual will depend upon an assessment of the relevant circumstances. For example, encountering an individual with a recent history of convictions for vehicle theft, late at night in a parking building that has experienced a spate of vehicle thefts, would likely be a situation where the taking of that individual's photograph for intelligence gathering purposes could be justified. On the other hand, photographing an individual who has a conviction for drink driving at the same location during a busy daytime period, without more, would not be.

(vi) Tracking changes in appearance of known offenders

337. Related to this, we also heard that officers would take photographs of "known offenders" they encounter in order to track their changing appearance over time. This reason for taking photographs was cited particularly in relation to youth, as their appearance may change significantly over a relatively short period of time. However, this practice of photographing known offenders to track their changing appearance is not necessarily consistent with the IPPs.

338. While the appearance of a “known offender” who has a criminal record may change (e.g., because of a beard or tattoos), their most recent arrest photograph will be available to Police. Since it should be necessary to monitor a known offender’s appearance for policing purposes only when there is a recent relevant history of offending, the photograph already held by Police should therefore usually provide sufficient information about an individual’s appearance.
339. If that individual has not had any convictions for such an extensive period of time that their appearance is noticeably different from their arrest photograph, we consider Police have no good reason to be tracking their appearance. In addition, for those who have committed serious offences, there is a likelihood that they will be subject to post-release conditions and monitoring by the Department of Corrections.
340. We therefore cannot see the necessity for photographing individuals solely for the purpose of tracking their changing appearance. If other criteria are met – that is, if there are other grounds making the taking of photographs necessary for a lawful Police function – the taking of a photograph may be justified. Tracking changing appearance will not, on its own, suffice.
341. While the practice of taking photographs to monitor known offenders appears to be common across all Police districts, we do note that some districts appear to encourage this practice in relation to youth, in particular.
342. Although the practice of taking photographs to monitor known youth offenders may have currently ceased in some districts, at least in part due to the joint inquiry being conducted, we are concerned that youth appear to have been specifically targeted.
343. As we have outlined, youth are entitled to enhanced protection under the Privacy Act, the Oranga Tamariki Act, and the UNCROC. We would expect that this would result in youth being photographed relatively rarely for the purpose of being monitored as known offenders.

(vii) General Intelligence gathering – conclusions and recommendations

344. The joint inquiry team has identified there is a need for clear, consistent guidance for frontline policing staff on taking photographs or video recordings in compliance with the Privacy Act in any given situation for intelligence gathering purposes.

Findings – IPP 1

345. In relation to IPP 1, we consider that frontline officers need guidelines to help them properly assess the circumstances in which collecting an individual’s personal information by taking their photograph will be necessary for a lawful purpose connected with a Police function. When collecting personal information (including photographs and video recordings) for intelligence gathering purposes, Police must also be able to articulate the specific purpose for which they are collecting that personal information.
346. We consider an appropriate threshold to be that, when photographing or video recording an individual for general intelligence purposes, 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.

347. When taking photographs for general intelligence gathering purposes, officers therefore should give consideration to the following:
- (a) Do the circumstances mean that the person being photographed has a reasonable expectation of privacy?
 - (b) Is there something in the circumstances that warrants further investigation?
 - (c) Is it reasonable for the photograph to be taken without speaking to the person? E.g., would it be risky or intrusive for the officer to approach the person?
 - (d) How will the photograph be used? Is there a reasonable possibility that the photograph will benefit an active investigation at some point?
 - (e) Where will the photograph be stored so that it can be accessed and used for an appropriate purpose later on?
348. We consider this to be a non-exhaustive list of factors officers should turn their minds to before collecting personal information in the form of photographs or video recordings of members of the public.
349. However, it is important that Police officers understand that consent from an individual cannot be used to expand the circumstances in which Police can collect photographs beyond the IPP 1 threshold. If an officer has considered the individual's personal characteristics and the surrounding circumstances and determined that the threshold for taking a photograph for intelligence gathering purposes has been met, we consider it is important for that officer to then properly record the circumstances and considerations that they have relied upon in taking the photograph. It is important that the decision-making process be captured and be capable of later examination or audit.

Findings – IPP 3

350. We consider that frontline officers need guidelines to help them properly assess the requirements of IPP 3 when collecting personal information (including photographs and video recordings in public settings) for intelligence gathering purposes.
351. Police policy should therefore provide guidance about:
- (a) explaining to the individual the reasons for Police taking a photograph and collecting other personal information and what the photograph and personal information will be used for in accordance with IPP 3; and
 - (b) the threshold for applying the IPP 3 exceptions, including where necessary to avoid prejudice to the maintenance of the law, in order to bypass the usual notification requirements.

352. The maintenance of the law exception requires Police to articulate, in each case, a reasonable belief that non-compliance with IPP 3 is necessary **to avoid prejudice to an investigation**.
353. This requires Police to reasonably consider how notifying the individual about the purpose for taking their photograph would prevent an investigation from commencing or progressing. For example, if the person declines to co-operate in being photographed after having the reason for it explained to them, so that the taking of it becomes more difficult, would this be detrimental to a current or potential investigation and, if so, is taking the photograph without complying with IPP 3 necessary to avoid that detriment?
354. When assessing this exception, officers therefore should consider the following:
- (a) how important is it to the investigation to identify the individual through taking a photograph?
 - (b) the quality of the intelligence that would be provided by taking a photograph of the individual and its relevance to the investigation:
 - i. the higher the relevance of a photograph to an investigation (for example, providing relevant evidence of offending or confirming a relevant detail to an investigation that is not otherwise available such as a person's description or an association with another person or with a location), the more likely an investigation may be prejudiced;
 - ii. the lower the relevance of the photograph to the investigation, the less likely an investigation may be prejudiced by informing the individual of the purpose of the photograph;
 - (c) whether the information that a photograph would provide could be collected in another form (for example by note-taking) or from another source (for example a publicly available source);
 - (d) the seriousness of the offending that is being or will be investigated and the strength of the suspicion that the person that is to be photographed is connected with that offending;
 - (e) the behaviour of the individual and whether they are demonstrating a likelihood or potential for offending (such as carrying a weapon) or expressing a capacity for violence or other behaviours relevant to the offending that is the subject of the investigation;
 - (f) other relevant circumstances of the interaction including the urgency of the situation and whether there is a risk to the officer's safety when engaging with the individual.
355. This is a non-exhaustive list of factors to which officers should turn their minds to check if they reasonably believe that departing from IPP 3 is necessary to avoid prejudice to the maintenance of the law.
356. If an officer has determined that the threshold for relying on the maintenance of the law or another exception is met, we consider it is important for that officer to then properly record the

circumstances and considerations that they have relied upon. It is important that the decision-making process be captured and be capable of later examination or audit.

Findings – IPP 4

- 357. We consider that frontline officers need guidelines to help them properly assess the requirements of IPP 4 when collecting personal information (including photographs and video recordings in public settings) for intelligence gathering purposes.
- 358. Police policy should therefore provide guidance about obtaining the individual's consent to take the photograph in order to demonstrate compliance with IPP 4's requirement for fair means of collection and protection against unreasonable intrusion and assessing the justification for taking photographs without the individual's consent.
- 359. The need to obtain the individual's consent for a photograph will depend on the particular circumstances and the individual. While obtaining the consent of the individual should be considered as a starting point, this will depend on whether to do so is practicable in the circumstances, whether it would be prejudicial to a potential or current investigation and, if so, whether that risk of prejudice outweighs the need to demonstrate fairness in collection by obtaining the individual's consent and is therefore disproportionate.
- 360. For example, if the officer has a reasonably held belief under IPP 3 that notification would prejudice the maintenance of the law or the purpose of collection, this will also be relevant for the purposes of assessing fairness under IPP 4. It will not generally be unfair to proceed without consent in these circumstances, due to the risk of prejudice, but subject to taking into account any particular considerations of fairness in relation to a youth.
- 361. Policy should highlight that compliance with IPP 4 will need to reflect the youth justice principles to be applied in Police interactions with youth for intelligence gathering purposes. A youth's age and the special protections that apply to them as a result will be relevant considerations when assessing the means of collection of sensitive personal information from them through targeted photography in a law enforcement context, and whether that collection is fair and not unreasonably intrusive.
- 362. The capacity and maturity to fully understand what is being requested, and the consequences of that request, will be reached at different ages for different individuals. This may be exacerbated by literacy issues, communication disabilities and mental impairments. Police's ability to obtain informed consent from a youth in these circumstances is therefore problematic due to their inherent vulnerability. The inherent power imbalance makes it very difficult for them to exercise their right to refuse to be photographed, or to understand their rights in this respect.
- 363. The wellbeing and best interests of the youth must be considered, and this includes the role of their whānau in Police interaction with the young person. In particular, the role of whānau in Police interaction with rangatahi is a necessary and relevant consideration. Tamariki are taonga

and their whānau play an important role as kaitiaki of whakapapa as well as the mana and tapu of each tamaiti.

364. Many of the officers we interviewed appreciated the inherent power imbalance between a Police officer and a youth and understood that this will often inhibit a youth from refusing an officer's request. However, few officers appeared to have had any guidance in how to deal with this in a way that ensures any consent is fully informed and voluntary.
365. Therefore, Police policy should emphasise the need to engage with family and whānau when interacting with youth and obtain consent for photographing the youth in public, after explaining the purpose and necessity and how the photographs will subsequently be used by Police. In relation to a child (under 14), consent should be sought from the family, whānau or caregiver (or if they are unavailable another appropriate and independent adult) as well as the child, and the purpose of and necessity for the photograph and how it will subsequently be used by Police fully explained to them. Where it is not possible to immediately obtain the consent of their family, whānau, caregiver or appropriate adult, it will be necessary to defer the taking of the photograph until that opportunity is available.
366. In the case of a youth who is at least 14, where it is not possible to provide an opportunity for the engagement of family and whānau, Police will need to take care to ensure that the purpose and necessity for the photograph and how it will be used can be explained to the youth in suitable and understandable terms and with an opportunity to ask questions. This includes an opportunity to decline to give permission to the photograph being taken, where this is an available choice, in the particular circumstances.

RECOMMENDATIONS – TAKING PHOTOGRAPHS FOR INTELLIGENCE PURPOSES

1. Police should develop a consolidated and comprehensive policy covering the use of photography to collect personal information under the Privacy Act for general intelligence-gathering purposes. This policy should develop clear, practical guidelines for complying with the Privacy Act when stopping individuals in public and taking photographs for intelligence collection purposes including:
 - a. setting out an appropriate threshold under the Privacy Act (IPP 1), for the collection of personal information: when turning their minds to their reasons for collection officers must be able to articulate a reasonable possibility, based on more than mere conjecture, that the individual being photographed could be relevant to a particular or likely investigation (the lawful purpose);
 - b. unless an exception applies, informing the individual of the purpose for taking the photograph, the consequences for the individual if the photograph is not provided and other information required under the Privacy Act (IPP 3);
 - c. setting out the applicable thresholds for exceptions to the requirement to inform the individual. In relation to the maintenance of the law exception, that requires a

reasonably held belief that not complying with IPP 3 is necessary to avoid prejudice to the maintenance of the law;

d. the circumstances that require the consent of the individual, to ensure that photographing the individual is fair and does not intrude to an unreasonable extent on their personal affairs. For example:

- i. if an officer is engaging with an individual and informing them of the reason and purpose for the photograph, it will generally be fair to also obtain their consent, particularly if the individual is a youth; or
- ii. if seeking the individual's consent would be disproportionately prejudicial to the reason for taking the photograph or to the maintenance of the law, that risk of prejudice can justify proceeding without consent; and
- iii. that, if a photograph is taken after the refusal of consent, the individual must be informed that the photograph is mandatory.

2. Police policy should provide clear guidelines for complying with the Privacy Act when stopping a youth in public and taking photographs for general intelligence-gathering purposes including:

- a. reflecting the youth specific protections in the Oranga Tamariki Act and UNCROC;
- b. tailoring the explanation under IPP 3 to the youth in an age-appropriate way; and
- c. reflecting the requirements of IPP 4 when officers are deciding whether to proceed with a photograph of a youth and require officers to engage with the youth's family, whānau or caregiver and, in the case of a child or tamariki under the age of 14, to obtain their consent (or if they are unavailable another appropriate and independent adult), before taking a photograph of the youth.

3. Police policy should require officers to record the circumstances and considerations that they rely upon to justify the collection of personal information for purposes of intelligence gathering.

4. 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.

(b) Police Investigations

(i) Non-crime scene identification

367. One of the most problematic situations, and the one which precipitated this joint inquiry, arises when Police are investigating a specific reported incident and come across individuals who they suspect may have been involved. This is a situation in which most Police officers and staff we spoke to believe it would be appropriate to take photographs.

368. In this situation, some officers told the joint inquiry team that they will only take photographs with the suspect's consent, while many other officers said they do not believe consent is required. Police officers reported taking photographs both covertly and openly.

369. Officers told the joint inquiry team that they took photographs of both adults and youth in this situation, although that practice varied. While many officers said that their approach was the same for youth as for adults, some officers were more reluctant to photograph youth. Others said they were more likely to photograph youth suspects, often because they felt this approach was encouraged by their superiors and their Youth Aid sections. However, some officers also told the joint inquiry team that, following the publicity about the Wairarapa incident, they have been discouraged from photographing youth. The approach to photography seemed to vary across Police districts, with some districts taking a much more cautious approach to photographing youth since the Wairarapa incident came to light.
370. The Police officers interviewed explained they took photographs to either confirm a suspect's participation in the offending, or to rule them out. Officers explained that the intention is to capture the suspect and their clothing as they appear at the time, and to show the photographs to an eyewitness or compare to any CCTV footage of the incident.
371. Our interviews with frontline officers revealed that this practice does somewhat vary depending on location. Specifically, in smaller rural centres Police are much less likely to take photographs in these situations. As officers in rural centres pointed out to us, they are much more likely to already know the individual or individuals they may encounter, and so generally did not feel it necessary to take photographs. In larger centres this level of familiarity is not there, resulting in officers more often resorting to taking photographs.
372. Photographing members of the public to either confirm or exclude their involvement in alleged offending is, in theory, a practical and useful Police investigative technique. However, the lack of clarity about the relevant threshold for using this technique means that there is a risk of casting the net too broadly, thus creating inconsistency with the scheme of the IPPs.
373. The joint inquiry team considers that it is not permissible for officers responding to a report of an offence in a particular location to indiscriminately photograph any person who may be in the general vicinity. For example, where Police have descriptions of alleged offenders, we do not consider that it would be appropriate for them, without observing something that potentially links the person to the crime scene, to photograph individuals who clearly do not match the descriptions.
374. Police policy contains no guidance on when it will be appropriate to photograph someone for the purposes of non-crime scene identification. Furthermore, officers themselves do not understand the relevant law and, as a result of their inadequate training, are unclear about where the line should be drawn. We consider that Police policy should clearly address the question of an appropriate threshold for taking photographs or video recordings in this situation.

(ii) Crime scene photographs and videos

375. During our interviews with frontline Police officers and staff throughout the country, officers commonly described crime scene photographs as an instance in which they had taken photographs in public.

376. Crime scene photographs are generally taken for evidential purposes to accurately depict the crime scene and/or evidence that can more easily be presented in court by way of an image, rather than presenting the object itself. Police officers told us that they will generally try to keep members of the public out of crime scene photographs. However, there will be instances when victims or witnesses may be incidentally captured in crime scene photographs.
377. Police's 'Photography (Forensic imaging)' policy covers the taking of crime scene photographs. This policy sets out general circumstances in which it is appropriate for an officer to take crime scene photographs; circumstances in which a Police forensic photographer should be used; the logistics of taking such photographs; and their storage, retention, and disposal. We consider that this policy appropriately covers the taking of crime scene imagery in situations in which members of the public are not captured in the images.
378. We found crime scene photography to be a relatively uncontroversial category of Police photographing and video recording. Despite this, we consider it important that Police take into account the privacy rights of the individuals captured inadvertently in crime scene photographs.
379. If Police do not need to retain the image for any reason connected to the purpose for which it was taken, they must promptly dispose of that image. If Police do intend to retain the image for a legitimate purpose, we consider that any collateral people captured in the image must be cropped out, blurred, or otherwise removed from the image.

(iii) Victims and witnesses and family harm incidents

380. When investigating alleged offending, officers often collect personal information from victims and witnesses. This personal information may include photographs, video recordings and biometric prints.
381. When it comes to photographing or video recording victims or witnesses, there are unique considerations that apply to family harm incidents. In family harm incidents, one or more of the parties will often have injuries either visible at the time, or that become more visible in the hours or days following the incident. In addition, it is not uncommon for victims in family harm incidents to deny or minimise any injuries. For these reasons, the Police 'Family harm' policy states that officers should take photographs at the earliest opportunity, and again after 24-48 hours. This can provide important evidence of any injuries inflicted.
382. In addition, Police will often take video recorded statements from complainants at the scene, or some other location a short time later.
383. The law allows evidence of a family violence complainant to be given by way of a video recording.¹⁰¹ With this in mind, Police policy recommends that statements be taken from victims and witnesses early on, as they can often become reluctant witnesses during the prosecution process. As a result, victims and witnesses will sometimes be video recorded at the scene in

¹⁰¹ Evidence Act 2006, s 106A.

order to capture their physical and emotional condition at the earliest opportunity and avoid losing the opportunity to obtain a statement from them.

(iv) Investigations – conclusions and recommendations

384. The joint inquiry team has identified there is a need for clear, consistent guidance for frontline policing staff on the circumstances in which the taking of photographs or video recordings for investigation purposes will comply with the Privacy Act.
385. We acknowledge that the Police ‘Photography (Forensic imaging)’ policy is largely fit for purpose (although updates are needed to reflect changes in the technology now used).

Findings – IPP 1

386. In relation to IPP 1, we consider that frontline officers need guidelines to help them properly assess the circumstances in which collecting an individual’s personal information by taking their photograph will be necessary for a lawful purpose connected with a Police investigation. Police must also be able to articulate the specific purpose for which they are collecting that personal information.
387. The legal threshold for a Police officer to arrest someone without a warrant is that the officer has “good cause to suspect” the individual has committed an offence.¹⁰² We accept that it would not be appropriate for the threshold for photographing someone in relation to a suspected offence to be the same as, or higher than, the threshold for arrest.
388. To meet the threshold established by IPP 1, however, we consider that officers must be able to articulate a reasonable possibility, based on more than mere conjecture, that the individual being photographed could be relevant to a specific investigation (the lawful purpose). This will require a consideration of the individual’s personal characteristics and the surrounding circumstances.
389. A non-exhaustive list of the types of factors officers should consider are:
- (a) Is there a description of the alleged offender?
 - (b) If so, does the individual concerned match that description?
 - (c) If the individual is found in the vicinity of the reported incident, how close is this in time to the alleged offence? Are there any other people in that vicinity? If so, how many?
 - (d) How does an individual have potential relevance to an investigation – are they one of a small number of people located near a reported incident close in time to the incident, as opposed, for example, to being one of a large number of people encountered in the vicinity after a substantial passage of time.

¹⁰² Crimes Act 1961, s 315(2)(b); and Summary Offences Act 1981, s 39.

- (e) Is there anything else the officer can articulate that is unusual or suspicious about the time, location or circumstances in which the individual is encountered?
- (f) Is the individual known to Police? In particular, is the offender known or suspected by Police to be involved in similar offending to the type being investigated?
- (g) Is the individual in the company of others who have previously been involved in similar offending?

390. If an officer has determined that the threshold for taking a photograph for identification purposes has been met, we recommend that the officer be required to record the circumstances and considerations that they have relied upon in taking the photograph, so that this can be subject to later examination or audit.

Findings – IPPs 3 and 4

391. Consistently with our findings in relation to the collection of personal information by photography for intelligence gathering purposes in the previous section, we consider that frontline officers need guidelines to help them properly assess the requirements of IPPs 3 and 4 when collecting personal information (including photographs and video recordings in public settings) for investigation purposes.

392. Police policy should therefore provide guidance about:

- (a) unless an exception applies, explaining to the individual the reasons for Police taking a photograph and collecting other personal information and what the photograph and personal information will be used for in accordance with IPP 3;
- (b) the threshold for applying the IPP 3 exception where necessary to avoid prejudice to the maintenance of the law in order to bypass the usual notification requirements;¹⁰³
- (c) the circumstances that require the consent of the individual, to ensure that photographing the individual is fair under IPP 4 and does not intrude to an unreasonable extent on the personal affairs of the individual concerned.¹⁰⁴ For example:
 - (i) if an officer is engaging with an individual and informing them of the reason and purpose of the photograph, it will generally be fair to also obtain their consent for the photograph, particularly if the individual is a youth; but
 - (ii) if seeking the individual's consent would be disproportionately prejudicial to the reason for taking the photograph or to the maintenance of the law, that risk of prejudice can justify proceeding without consent;
- (d) the need to engage with family, whānau or caregivers when interacting with youth and obtain their consent for photographing the youth, after explaining the purpose and

¹⁰³ Refer to the non-exhaustive list of factors set out above in relation to intelligence gathering.

¹⁰⁴ Refer to IPP 4 findings above in relation to intelligence gathering.

necessity and how the photographs will subsequently be used by Police. In relation to a child (under 14), consent should be sought from the family, whānau or caregiver (or if they are unavailable another appropriate and independent adult) as well as the child, and the purpose of and necessity for the photograph and how it will subsequently be used by Police fully explained to them. Where it is not possible to immediately obtain the consent of their family, whānau, caregiver or appropriate adult, it will be necessary to defer the taking of the photograph until that opportunity is available; and

- (e) in the case of a youth who is at least 14, where it is not possible to provide an opportunity for the engagement of family and whānau or an appropriate adult, taking care to ensure that the purpose and necessity for the photograph and how it will be used can be explained to the youth in suitable and understandable terms and with an opportunity to ask questions. This includes an opportunity to decline to give permission to the photograph being taken, where this is an available choice, in the particular circumstances.

RECOMMENDATIONS – PHOTOGRAPHY FOR INVESTIGATION PURPOSES

5. Police should develop a consolidated and comprehensive policy covering the use of photography to collect personal information under the Privacy Act for non-crime scene identification. This policy should develop clear, practical guidelines for complying with the Privacy Act when stopping individuals in public and taking photographs for purposes of investigations including:

- a. setting out an appropriate threshold under the Privacy Act (IPP 1), for the collection of personal information: when turning their minds to their reasons for collection officers must be able to articulate a reasonable possibility, based on more than mere conjecture, that the individual being photographed could be relevant to a specific investigation that is currently underway (the lawful purpose);
- b. unless an exception applies, informing the individual of the purpose for taking the photograph, the consequences for the individual if the photograph is not provided and other information required under the Privacy Act (IPP 3);
- c. setting out the applicable thresholds for exceptions to the requirement to inform the individual. In relation to the maintenance of the law exception, that requires a reasonably held belief that not complying with IPP 3 is necessary to avoid prejudice to the maintenance of the law;
- d. the circumstances that require the consent of the individual, to ensure that photographing the individual is fair and does not intrude to an unreasonable extent on the personal affairs of the individual concerned. For example:
 - i. if an officer is engaging with an individual and informing them of the reason and purpose of the photograph, it will generally be fair to also obtain their consent, particularly if the individual is a youth; or

- ii. if seeking the individual's consent would be disproportionately prejudicial to the reason for taking the photograph or to the maintenance of the law, that risk of prejudice can justify proceeding without consent; and
- iii. that, if a photograph is taken after the refusal of consent, the individual must be informed that the photograph is mandatory.

6. Police policy should provide clear guidelines for complying with the Privacy Act when taking photographs of youth for investigation purposes including:

- a. reflecting the youth specific protections in the Oranga Tamariki Act and UNCROC;
- b. tailoring the explanation under IPP 3 to the youth in an age-appropriate way; and
- c. reflecting the requirements of IPP 4 when officers are deciding whether to proceed with a photograph of a youth and require officers to engage with the youth's family, whānau or caregiver and, in the case of a child or tamariki under the age of 14, to obtain consent from them (or if they are unavailable another appropriate and independent adult), before taking a photograph of the youth.

7. Police policy should require officers to record the circumstances and considerations that they rely upon to justify the collection of personal information for investigation purposes.

8. Police policy should confirm that Police may take photographs at a crime scene provided that the privacy of those unrelated to the incident is taken into account. This could be addressed by the redaction of images that include individuals who are not relevant to the investigation.

(c) Photographs in other policing scenarios

(i) Traffic checkpoints and traffic stops

393. The Land Transport Act was a commonly misunderstood area of legislation, with most officers telling us that under the Land Transport Act they had the right to photograph members of the public in motor vehicles. Many officers incorrectly thought that section 114 of this Act gave them this right.

394. Police policy¹⁰⁵ cites a 1987 High Court case as giving Police authority to take photographs of individuals stopped for traffic-related offences.¹⁰⁶ However, that case predates the Privacy Act 1993 and the New Zealand Bill of Rights Act 1990 and only provides authority for taking a photograph where it is needed for the purposes of the Transport Act 1962. The joint inquiry team also notes that the case is not referred to in the current Police guidance on roadblocks, nor does it reflect the IPCA's recent findings in the Northland checkpoint incident.

395. The Land Transport Act does not give Police officers the power to take photographs of members of the public while stopped at a checkpoint (or any other traffic stop). This means that Police must apply the Privacy Act collection principles when taking photographs of individuals stopped

¹⁰⁵ Identifying drivers with face coverings; see Appendix 1A.

¹⁰⁶ *Cunnard v Auckland City Council* (1987) 2 CRNZ 459 (HC).

using powers under the Land Transport Act, including considering whether the photograph is necessary for the purpose of the stop.

- 396. Section 114 enables Police to stop motorists and to set up checkpoints. This provision gives an officer the power to require a driver to stop and give specified particulars such as name, address, date of birth, occupation, and telephone number.
- 397. If a vehicle is stopped under Section 114 the enforcement officer may require a driver to remain stopped on a road for as long as is reasonably necessary to enable them to establish the identity of the driver, but not for longer than 15 minutes. This provision applies only to the driver of the vehicle and not to any passengers.

Checkpoint incidents previously considered

- 398. Both the IPCA and the Privacy Commissioner have previously examined Police checkpoints and have found the collection of personal information by Police at checkpoints to be in breach of the collection principles in the Privacy Act.
- 399. The Privacy Commissioner examined a Police checkpoint incident in 2018 in the context of a breath testing checkpoint targeted at a group of people who attended an Exit International meeting in Lower Hutt. The Privacy Commissioner found that the Exit International checkpoint was unlawful and unfair and the information was therefore collected in breach of IPP 4 of the Privacy Act 1993.¹⁰⁷
- 400. In 2019 the IPCA investigated a Northland complaint about Police checkpoints and made findings that are relevant to this report. A Northland woman who was driving her car away from a ‘fight night’ event in Ruakākā, Whangārei was stopped at a Police checkpoint which had been set up down the road. The woman was breath tested and her warrant and registration checked, and an officer asked for her licence.
- 401. The woman was then asked to pull over to the side of the road where officers took photographs of her licence, and her partner, through the front passenger window. Her warrant and registration were checked again. The woman complained to the IPCA that she had been unlawfully detained, and that Police did not have authority to photograph her, her partner, or her driver’s licence.
- 402. In March 2021, the IPCA concluded the investigation,¹⁰⁸ finding that, while Police were empowered to carry out the initial checkpoint under section 114, they had unlawfully abused that power to obtain personal information for intelligence purposes. It also concluded that by requiring the woman to pull over to the side of the road for this purpose, they had unlawfully detained her, and by photographing her and her partner they had breached IPP 1 and IPP 3 of the Privacy Act.

¹⁰⁷ Privacy Commissioner “[Operation Painter: Findings in privacy investigation](#)” (press release, 15 March 2018).

¹⁰⁸ IPCA press release, above n 32.

403. Police's own review into the checkpoint recommended that Police undertake a review of national Police policy to provide clear guidance on when photographs can be taken for intelligence purposes. That review will be informed by the findings of this joint inquiry.

Joint inquiry's interviews and findings

404. The joint inquiry team found that the practice of using checkpoints in this way has continued, at least to some extent. When describing the circumstances in which they photograph members of the public in the course of their work, one of the most common situations officers mentioned was traffic stops. This included traffic checkpoints, as well as regular traffic stops.
405. From this inquiry it is clear that traffic stops and associated photographs are being taken for a wider array of purposes than section 114 permits.
406. The most common reasons given for taking photographs at checkpoints and other traffic stops were:
- (a) to establish identity when issuing infringement notices; and
 - (b) to gather intelligence, particularly with regard to gang members.
407. If Police rely on the Land Transport Act to take a photograph of a motorist they have stopped, the taking of the photograph must be for a purpose under the Land Transport Act. An example would be taking a photograph of a driver for proof of service of an infringement notice, provided that the driver's identity is not able to be ascertained in other way (eg by examination of the driving licence and accompanying photograph). Police policy should make that explicit.
408. On the other hand, intelligence gathering – whether of gang members or any other member of the public – is not a lawful purpose under the Land Transport Act.
409. In addition, we consider that Police cannot lawfully photograph people for a non-Land Transport Act purpose, even if that purpose would otherwise be lawful, where the traffic stop is simply a pretext to follow up an unrelated and pre-determined line of information.
410. In our view, this is the situation in most, if not all, checkpoints targeting gangs.
411. From our interviews, it became clear that many officers believed they were authorised to take photographs of anyone who has been stopped under the Land Transport Act. They believed this is consistent with Police policy and they were not aware they may be breaching privacy by doing so. However, the Land Transport Act does not provide a general authorisation to photograph anyone who has been stopped pursuant to its authority.
412. It was also clear from speaking to frontline officers that checkpoints are seen by Police as a vital tool in gathering intelligence on gangs. When officers talked about checkpoints, they invariably described them as targeting gangs.
413. In relation to gang intelligence, the reasons officers gave for taking photographs included:

- (a) identifying gang members;
 - (b) linking individual gang members to specific vehicles; and
 - (c) building up a picture of gang structure by establishing who gang members associate with and identifying their rank or position by viewing their unique patches or 'rockers'.
414. The joint inquiry team is concerned that widespread photographing or video recording of any suspected gang members using Police powers to undertake a lawful traffic stop is too broad and is not rationally or reasonably connected to a law enforcement purpose. We consider that there must be some clear and lawful purpose beyond simply building up a picture of gang membership and structure.
415. Many officers said that gang members are very open and happy to be photographed, and so officers often ask them to pose for photographs. If the individuals are reluctant to have their photographs taken, many officers take the photograph covertly, while others openly take photographs regardless of an individual's wishes.
416. Police policy correctly states that the use of Police checkpoints under the Land Transport Act must be for genuine and proper Land Transport Act enforcement purposes.¹⁰⁹ However, the 'Policing Outlaw Motorcycle Gang Runs' policy also makes the intelligence gathering purpose of these checkpoints clear. According to the policy, the data obtained from a checkpoint should consist of:
- (a) a list of motorcycle registrations;
 - (b) a list of members;
- and potentially:
- (c) an image of the motorcycle; and
 - (d) an image of the member; and
 - (e) an image of any insignia.
417. In relation to checkpoints targeted at gang members, Police's express intention to gather the type of information set out in 'Policing Outlaw Motorcycle Gang Runs' along with the presence of Police photographers, shows a pre-determined intention to gather personal information unrelated to Land Transport Act purposes. We consider that this practice is not lawful and that there is a need for clearer guidance in policy in order to avoid continued systemic unlawful collection of this personal information.
418. However, if during a lawful stop conducted under the Land Transport Act, a lawful purpose to record images of a person becomes apparent, Police may be entitled to do so, depending on the

¹⁰⁹ See for example "Use of Police checkpoints and conducting traffic stops" *Road blocks and stopping vehicles for search purposes*; see Appendix 1A.

particular circumstances. Where Police do take photographs or video recordings, whether for a Land Transport Act purpose or another lawful reason, they must also comply with the Privacy Act.

- 419. In particular, collection of the images must be necessary for a lawful purpose connected with a Police function (IPP 1). Unless an IPP 3 exception is engaged, Police must take reasonable steps to ensure that the individual is aware of the fact their image is being recorded, the purpose for which it is being recorded, who will receive and hold the image, the legal basis on which Police have taken the image, and the individual's rights of access and where the photograph will be held (IPP 3).
- 420. The collection of the image must be collected in a manner that is lawful, fair and not unreasonably intrusive in the specific circumstances (IPP 4) and may require the individual's consent before taking the photograph, depending on the nature of the engagement with the individual or particular purpose for taking the photograph.
- 421. Where an exception to IPP 3 based on prejudice to the maintenance of the law or prejudice to the purpose of collection is engaged, it will not generally be unfair or unreasonably intrusive under IPP 4 to proceed to photograph without the individual's consent. However, where the individual is a youth, this should be taken into account when assessing the fairness of photographs at traffic stops for non-LTA purposes and the reasonableness of the intrusion into their personal affairs.
- 422. As mentioned, above, many officers we spoke to said they asked for permission to take photographs of gang members, many of whom appeared to be happy to agree. However, we are concerned that the apparent "voluntary" nature of these photographs leads many officers to ignore the Privacy Act requirements. The collection of photographs, even with consent, must be necessary for a lawful Police purpose, and the officer collecting the image must still take reasonable steps to comply with IPP 3 by providing an explanation to the individual about why the photograph is taken and what it will be used for. Obtaining consent does not serve to provide a lawful basis for collection without meeting the requirements of IPP 1.
- 423. While the Privacy Act may restrict the circumstances in which Police can record images of gang members stopped under the Land Transport Act, this does not preclude officers from taking detailed notes (where there is a necessary lawful purpose for doing so in compliance with IPP 1) to record their observations. We consider that this would capture much of the data Police are seeking without infringing the privacy collection principles.
- 424. We recognise that notes will not capture the same accuracy or detail as a photograph, and that writing notes is more time-consuming than pulling out a Smartphone and taking a photo. However, many officers described their preference for taking notes over photographs. We also recognise that note-taking was *the* standard practice prior to the roll-out of mobile devices. Restrictions on the recording of images need not mean that no useful intelligence can be obtained.

RECOMMENDATIONS – TRAFFIC CHECKPOINTS AND OTHER TRAFFIC STOPS

9. Police should prioritise review of training and policy on LTA checkpoints and stops to ensure that:

- a. policies reflect the current legal constraints, including the application of the privacy principles when taking photographs for non-LTA purposes;
- b. checkpoints and other traffic stops are not established for the primary purpose of collecting photographs and personal information for a collateral purpose;
- c. information gathered in the course of an LTA checkpoint or stop is not used for other purposes (e.g. general intelligence) unless lawfully collected for that other purpose, or it comes under a valid use exception under the Privacy Act;
- d. photographs are taken for identification purposes at traffic checkpoints and other traffic stops when an infringement notice is being issued only when the driver's identity is not able to be ascertained in other way (eg by examination of the driving licence and accompanying photograph); and
- e. officers receive regular training on the limits on taking photographs at LTA checkpoints and traffic stops.

(ii) Protests and other large gatherings

425. In our interviews with frontline officers, demonstrations were identified as another instance in which Police take photographs of members of the public. The extent of this practice is not clear; that is, it is unclear to us whether this practice happens as a matter of course at most or all demonstrations, or whether the decision to photograph or video-record demonstrations is a selective one, depending on the circumstances of the particular gathering.
426. As well as requiring a consideration of IPPs 1 to 4, Police collection of demonstrators' images has implications under the New Zealand Bill of Rights Act 1990 (NZBORA). In particular, Police must give consideration to sections 14 (freedom of expression) and 16 (freedom of peaceful assembly) when considering whether to take photographs or video recordings of protests.
427. Police have policies in place (the *Demonstrations* policy and the *Unlawful Assembly and Riot* policy) setting out guidance and procedures for using video teams and photographers to capture participants' images.
428. Given that riots and unlawful assembly are, by their very definition, unlawful, it is reasonable that Police would utilise video teams and photographers in circumstances where they believe that a gathering is likely to meet that threshold. Under the policy, this type of evidence gathering must be approved by the Operation Commander and may be used to provide evidence; to help identify suspects; to protect against unjustified complaints; and to exert a controlling influence on Police behaviour. We consider these reasons for collecting photographs, as outlined in the Police *Unlawful Assembly and Riot* policy, to be appropriate and necessary for a lawful Police function.

429. The policy also requires Police recorders to record the time, location, numbers involved, identities and descriptions for each image recorded. The policy requires that images be destroyed once the purpose for which they were taken has been served. We consider these requirements to be appropriate.
430. With regards to the recording of people's images at demonstrations other than riots or unlawful assemblies, the *Demonstrations* policy states that Police photographers should be deployed only on the authority of the Operation Commander, and only where the prevailing circumstances indicate "*a probability of disorder*".
431. In contrast, officers we interviewed spoke of photographing protesters for more general intelligence purposes – that is, to enable them to be identified for future events. While only a small number of officers described doing this, we note it as an approach which seems to be at variance with Police policy.
432. We consider the correct approach to photographing protestors as being somewhere in between that set out in the *Demonstrations* policy and that described by those officers. We believe that recording demonstrators for no reason other than their presence in an otherwise lawful and peaceful demonstration, with the aim of identifying them for potential future demonstrations, is not necessary for a lawful Police purpose and impinges on individuals' rights under both the Privacy Act and the NZBORA.
433. On the other hand, we believe that the *Demonstrations* policy sets the bar for capturing demonstrators' images too high. As we have discussed with regards to the recording of images for investigation purposes, our view is that the threshold must be lower than the arrest threshold. A bar that is set at *probability* of disorder is, in our view, unreasonably restrictive.
434. We consider that it would be appropriate for Police to record images of demonstrators in circumstances where they believe, based on some articulable facts, that there is a *reasonable possibility* of disorder occurring. The purposes for which images can be recorded should be the same as for those in riots or unlawful assemblies as we describe above.

RECOMMENDATION – PROTESTS AND OTHER LARGE GATHERINGS

10. Police should review and update the *Demonstrations* policy to reflect that:

- a. an appropriate threshold for photography is where the officer believes, based on some articulable facts, that there is a reasonable possibility of disorder occurring; and
- b. recording demonstrators for no reason other than their presence in an otherwise lawful and peaceful demonstration, with the aim of identifying them for potential future demonstrations, is not necessary for a lawful Police purpose.

(iii) Issuing notices and proof of service

435. Police staff we interviewed commonly cited establishing proof of service as a situation in which they routinely photograph members of the public.

436. When issuing a summons or an infringement notice, or serving a trespass notice, Police frequently take a photograph of the subject of the summons or notice holding that summons or notice. This is done so that if individual later denies being served with the summons or notice, Police will have photographic evidence establishing service.
437. We agree that this is necessary for a lawful Police function, in accordance with IPP 1. As long as Police properly explain the purpose and intended use of the photograph (IPP 3), take the photograph by fair and reasonable means (IPP 4), and limit the use of these photographs to demonstrating proof of service (IPP 10), we do not have concerns with the taking of photographs in these circumstances.

RECOMMENDATION – ISSUING NOTICES AND PROOF OF SERVICE

11. As part of a general review of policy and guidance relating to photographs of members of the public, Police should review and update policies and process relating to proof of service. This should make it clear that officers may photograph individuals holding a summons or infringement notice, as long as officers properly explain the purpose and use of the photograph, take it by fair and reasonable means, and limit the use of the photographs to demonstrating proof of service.

(iv) Responding to monitoring of Police by members of the public

438. Many officers we spoke to described having to deal with members of the public who either photograph or video record them as they perform their Police duties. Their annoyance and frustration with having to deal with this intrusion in the course of their work were often – and understandably – clear. While a member of the public is entitled to photograph or video a Police officer in a public place, we do not doubt that this is an annoyance and distraction for many officers.
439. When we asked officers to describe general situations in which they would photograph or record members of the public, a number of them mentioned turning their own cameras on members of the public who were recording them. These officers’ attitude can be summarised as: “*If they can do it to us, we can do it to them*”. Some officers described how these people did not like having cameras on them and would often then stop their own recording. It was clear that this was the officers’ intention in turning their camera on these members of the public: to get these people to put down their cameras and stop recording them while they try to do their jobs.
440. While only a relatively small number of officers described engaging in this conduct, the practice appeared to occur frequently enough to concern us. The lack of understanding of any boundaries on their rights as Police to photograph members of the public is particularly concerning.
441. When individual Police officers act in their capacity as Police officers, they are more restricted than the general public in what they can do. Fundamental to this is IPP 1: the requirement that their actions in photographing or video recording members of the public must be necessary for a valid policing purpose.

442. Police are justified in recording a member of the public who is recording them if the officer has reasonable concerns the person's behaviour poses a threat or is obstructing them in the performance of their duty.
443. Police are not justified in turning their cameras on someone simply because they find the experience of being photographed or video recorded by a member of the public to be annoying, bothersome, or a distraction. The feeling of annoyance does not provide a lawful basis for Police officers to photograph or video record members of the public.

RECOMMENDATION – RESPONDING TO MONITORING BY MEMBERS OF THE PUBLIC

12. As part of a general review of policy and guidance relating to photographs of members of the public, Police should ensure there is guidance about the lawful basis for photographing or video recording members of the public monitoring Police. This should make clear that officers should do so only if the officer has reasonable concerns that the person's behaviour poses a threat or is obstructing them in the performance of their duty.

(d) Police engagement with youth in police station settings

444. The joint inquiry has reviewed Police interactions with youth in a Police station setting relating to:
- Voluntary photographs and biometric prints where a youth is detained on suspicion of offending;¹¹⁰
 - Voluntary photographs where a youth has been uplifted for care and protection purposes;
 - Voluntary photographs where a youth has attended the Police station on a voluntary basis.
445. A Police station is a stressful environment and Police officers carry significant structural power. There is therefore a high risk that youth in that setting may be unfairly influenced to give consent to the provision of photographs or other biometric information where no lawful purpose exists to collect the information. This may particularly arise because they want to remove themselves from the situation, do not understand whether or not they are required to provide a photograph or other information and think they will not be able to leave until they comply with the request.

(i) Voluntary photographs and biometric prints where the youth has been detained on suspicion of offending

446. During the course of the Inquiry we identified a widespread practice within Police involving the systematic and unlawful collection and retention of so-called "voluntary" duplicate sets of prints and photographs from youth detained on the suspicion of offending.
447. Where a youth (or adult) has been detained for committing an offence and is in Police custody, Police have express powers to take identifying particulars, including photographs and biometric

¹¹⁰ What Police call "voluntary photographs" includes photographs taken in a custodial or Police station setting where consent has been sought for the photograph to be taken.

prints, under section 32 of the Policing Act 2008. Under section 33, Police may also detain a youth (or adult) *for the purpose of* collecting such identifying particulars when they have good cause to suspect the person has committed an offence and they intend to prosecute by way of summons.

448. These powers are subject to the protections set out in section 34 of the Act, which require that such photographs and prints be destroyed as soon as practicable after a decision is made not to commence a prosecution, or the prosecution does not result in a conviction or other outcome that authorises continued storage. Because charges against youth are frequently resolved through the Youth Courts without resulting in a conviction, photographs and prints collected by Police using powers under the Policing Act are generally unable to be retained.
449. However, officers who we interviewed reported that, following arrest or detention, they not only took a formal custodial photograph under section 32 on the custody unit digital camera, but sometimes supplemented this with a duplicate set of “voluntary” photographs on their mobile devices. These would then be retained on the officers’ mobile devices, or uploaded to the cloud or NIA, used for Intel notings, or emailed to the officer’s computer. What was done with the second set of photographs was left to be determined by the officer taking the photograph.
450. We also found that there was a widespread practice of Police obtaining what they referred to as a duplicate ‘voluntary’ set of biometric prints from youth. Police considered that they were allowed to obtain the duplicate “voluntary” set until the youth or their parent or caregiver expressly asked for them to be destroyed, without being subject to the statutory destruction requirement that applies to the compulsory set.
451. The process for Police obtaining “voluntary prints and photographs” was formalised in Police practice through the “Voluntary biometric prints and photographs consent form for children and young people” (known as the “POL545”). This form is required to be completed whenever so-called voluntary photographs or biometric prints are obtained from a youth. The POL545 is supposed to be used in conjunction with the POL545A, which provides an explanation of a youth’s rights in relation to the collection of voluntary prints and photographs and is to be provided to the youth and their parent, guardian or caregiver.
452. While required, use of the POL545 form varied considerably across and within regions. Where it is used the POL545 form is itself problematic, particularly in those cases where youth and their caregivers are simply given the form to read and sign. The form is dense and in small font, and potentially confusing, given it is intended to be used for both biometric prints and photographs. It is not reasonable to assume that a youth or their caregiver would be able to understand what they were being asked to do and why and provide truly informed consent simply by reading the form. Further, given the power imbalance between Police officers and youth, the presence of a youth’s signature on this form cannot be taken as indicating consent is truly voluntary.
453. Almost all officers we interviewed told us they had obtained so-called voluntary biometric prints from youth at some point in their career. Indeed, we were told that the workplace assessment requirements for probationary constables required them to obtain a set of so-called voluntary

biometric prints from youth (or to show proof that they had made at least three efforts to obtain voluntary prints), so that they would typically ask a youth for a set of voluntary prints after they had been arrested and a set of LiveScan prints had already been lawfully obtained under section 32 of the Policing Act. The first set was retained by the National Biometric Information Office (NBIO), unless the charges against that person were withdrawn by Police or they were found not guilty of the charges in Court. Meanwhile the second so-called voluntary set was unlawfully retained indefinitely, or until the person contacted the NBIO to request its deletion.

454. We have a fundamental concern that many Police officers we interviewed mistakenly see consent as allowing them to collect personal information, including photographs and prints, in situations where the law does not otherwise allow them to do so. We reiterate that consent cannot make the otherwise unlawful or unnecessary collection of personal information lawful or compliant with the Privacy Act.
455. We were told that the underlying rationale for taking duplicate photographs and biometric prints is that it has been an important tool in reducing youth offending, in that youth are apparently less likely to offend if they know that their photographs and fingerprints are on file and that they will be able to be identified if they commit a crime. We were provided with no evaluative material to support this claim. Even if such an evidential basis for this rationale exists, that is not a reason for a practice which is clearly not permitted by law; Police should rather undertake policy work and seek an amendment to the Policing Act.
456. We find that the practice of collecting and retaining voluntary prints and photographs from youth who have been detained on the suspicion of offending is unlawful in that it does not comply with Section 34 the Policing Act or the Privacy Act. The Privacy Commissioner issued Police with a compliance notice under IPP 9 (retention of personal information) during the course of this Inquiry, requiring Police to cease the practice of collecting and retaining voluntary prints from detained youth and initiating the identification and deletion of unlawfully collected prints and photographs as an interim step while the Inquiry completed its investigation and considerations.¹¹¹

(ii) Voluntary photographs where the youth has been uplifted for care and protection purposes

457. The statutory powers to take photographs and biometric prints in sections 32 and 33, and the accompanying destruction requirements in section 34, apply only in the context of suspected offending.
458. However, in addition to the youth justice context, Police are often involved with youth for care and protection purposes.¹¹² In the care and protection framework under the Oranga Tamariki Act, the well-being and best interests of the youth are the first and paramount consideration.

¹¹¹ See the terms of the compliance notice issued by the Privacy Commissioner to Police on 22 December 2021 at Appendix 1C.

¹¹² Examples of Police involvement in care and protection under the Oranga Tamariki Act include Police's role in executing warrants to search for and remove a youth in danger of ill-treatment or neglect (ss 39-40); the power to enter and search a location without a warrant when necessary to protect a youth from injury or death (s 42); and the power to take a youth into custody where that youth's physical or mental health is at risk (s 48).

459. The joint inquiry heard that photographs were being taken when transporting youth back home, either via a casual car ride offered by Police, or when officers were engaging with youth under section 48 of the Oranga Tamariki Act. Most officers believed they had a good understanding of section 48, which provides an authority to uplift a youth for their own protection.
460. Officers told us that on occasion they take photographs of youth for care and protection purposes. Specifically, they described the practice of photographing runaways, so that they have a picture for future use if that youth should run away again. We accept that this practice is done with good intentions and with the interests of these runaway youth at heart. However, we do not believe that routinely photographing youth in these circumstances can always be justified under the Privacy Act.
461. Nevertheless, we accept that there will be situations where there are safety or wellness concerns either in the home of a youth or related to the youth themselves. These concerns may justify photographs being taken to allow Police to quickly identify and track down the runaway in order to ensure the safety of the youth and to provide support.
462. This must be considered on a case-by-case basis. When taking and storing any photograph the officer must be mindful of and comply with the collection IPPs, including recording the purpose for which the photograph is being taken to ensure that it is used only for care and protection purposes and not for law enforcement.

(iii) Voluntary photographs where a youth has attended the Police station on a voluntary basis

463. Where a youth is voluntarily present at a Police station, a voluntary photograph should not be taken unless a specific lawful purpose under IPP 1 can be identified. Unless such a lawful purpose exists, officers are not permitted to take photographs of a youth (or an adult) on a voluntary basis. In this respect, they are in the same position as adults.
464. As noted we have a fundamental concern that Police mistakenly see consent as allowing them to collect personal information, including photographs and prints, in situations where the law does not otherwise allow them to do so. We reiterate that consent cannot make the otherwise unlawful or unnecessary collection of personal information lawful or compliant with the Privacy Act.
465. However, the only lawful purpose potentially arising in a Police station setting is either the furtherance of a specific investigation or intelligence gathering. Since the person's identity is already known, it is most unlikely that either lawful purpose under IPP 1 will exist, and if it does, that a photograph will be necessary for that purpose. In our view, therefore, the threshold for taking a photograph in a Police station setting will only be met on an exceptional basis. In particular, a photograph of a youth suspected of committing an offence, but not arrested, should never be taken in a way that effectively circumvents the restrictions in the Policing Act. Examples where there will be a lawful purpose include a voluntary photograph that is necessary for purposes of eliminating the individual (including a suspect) from an investigation, or to verify the identity of a witness or victim for purposes of an investigation (in the absence of other means of verification) or to track the movements of a victim or witness on CCTV footage. If in such exceptional circumstances the threshold is met, the youth specific protections in the Oranga

Tamariki Act apply and strict processes should be followed to inform the youth and the appropriate adult, parent or caregiver about the purpose for the photograph (IPP 3) and to request their informed consent (IPP 4).

RECOMMENDATIONS – INTERACTIONS WITH YOUTH IN POLICE STATIONS

13. Police policy should reflect that “voluntary consent” - whether or not it is informed - does not make the otherwise unlawful or unnecessary collection of personal information lawful or compliant with the Privacy Act.
14. Police should cease the practice of taking photographs of youth on a ‘voluntary’ basis where a youth has been uplifted or detained, except where a photograph is necessary for Police’s care and protection role to ensure the safety of the youth.
15. Police should cease the practice of taking biometric prints from youth on a ‘voluntary’ basis.
16. Police policy should identify:
 - a. the limits on taking ‘voluntary’ photographs of youth (and adults) present in Police stations on a voluntary basis under IPP 1; and
 - b. where a youth is concerned, the requirement for a parent, caregiver or other appropriate adult to be present to give informed consent for a ‘voluntary’ photograph.
17. Police should prioritise training for officers to improve understanding of:
 - a. Police’s functions under the Oranga Tamariki Act in the youth justice and care and protection contexts; and
 - b. the youth-specific protections due to vulnerability.

B POLICE USE OF PHOTOGRAPHS

466. The way in which Police use information is as important as the manner in which it has been collected. While much of the media attention and public discussion has focused on the circumstances of Police collection of photographs and other personal information, attention must also be paid to how that personal information is then used by Police.
467. Current Police policy on the use of personal information is disaggregated across various areas of the Police Instructions. There do not appear to be consistent, overarching policies covering use of this type of personal information. In particular, any analysis of the application of the privacy principles to the use of personal information appears lacking. Police policy should provide clear guidelines on the purposes for which these forms of lawfully collected personal information may be used under the Privacy Act (IPP 10).
468. IPP 10 sets out the limits on the use of personal information. This naturally relates to, and follows on from, IPP 1. As discussed earlier under IPP 1, Police can only collect personal information for

a necessary and lawful policing purpose. Following from that, IPP 10 provides that if personal information is obtained in connection with a particular purpose, it should only be used for that purpose unless an exception applies. One such exception is that personal information may be used for a purpose other than that for which it was collected if that other purpose is necessary to avoid prejudice to the maintenance of the law including for a valid law enforcement purpose.

- 469. As we have already noted, most frontline Police staff we spoke to had little, if any, knowledge or understanding of the Privacy Act in general, the IPPs in particular, or how the Privacy Act impacts upon the collection or use of personal information.
- 470. What IPP 10 means for Police's use of personal information is that once photographs or video recordings have been lawfully collected as necessary for a specific and proper law enforcement purpose, Police can only use those images for that particular purpose, or a directly related purpose, subject to the maintenance of the law and other specific exceptions.
- 471. Once the valid purpose for which the images were collected has been satisfied or no longer exists, or if Police validly collect personal information for a valid purpose but it is never actually used for that purpose, the basis for retaining the information will be spent and Police must securely dispose of that personal information as soon as practicable (IPP 9).
- 472. If the original purpose for which the personal information was collected remains, Police can use that personal information for another purpose as long as that other purpose falls within one of the exceptions to IPP 10.

RECOMMENDATION – USE

- 18. Police policy should provide clear guidelines on the purposes for which lawfully collected personal information in the form of photographs and videos may be used under the Privacy Act (IPP 10).

C ISSUES RELATING TO STORAGE, SECURITY, RETENTION AND DISPOSAL

- 473. The joint inquiry team has identified significant issues relating to the storage, retention and disposal of photographs and prints. The available data indicates that Police hold significant numbers of photographs of individuals – from the review of the OnDuty database, nearly 50,000 intel notings had a photograph attached, and of these 45% were Māori, 10% were Pasifika and 12% were linked to youth. 53% of youth were recorded as Māori. Moreover, the photographs in the OnDuty database are only a small percentage of all photographs taken by officers.
- 474. One of the key themes has been the expanding role of mobile devices (cellphones) and the ease with which photographs can be taken by officers in a range of policing situations. However, there is a lack of comprehensive policy and guidance about the use of mobile devices to take photographs of members of the public, and a lack of process to ensure the consistent storage, retention and deletion of images.

475. In the course of the joint inquiry, OPC identified a significant compliance issue under the Privacy Act (IPP 9)¹¹³ resulting from the retention of photographs and duplicate biometric prints of youth collected by Police in the circumstances being considered by the joint inquiry, including bypassing statutory retention periods.¹¹⁴
476. As a result, the Acting Privacy Commissioner issued a compliance notice to Police in December 2021 (see section 5 and Appendix 1C).
477. The compliance notice required Police to develop practices and procedures to ensure that identifying particulars are not retained for longer than is required for a lawful purpose.

Mobile device issues - storage and retention

478. It is apparent that the rapidly expanding role of mobile technology (devices) in everyday frontline policing is a significant factor in the issues considered in the joint inquiry.
479. Police began the roll-out of mobile devices in 2013¹¹⁵ and now every Police officer has been equipped with a smartphone. Officers are encouraged to keep their police smartphones on them at all times and use them in place of a separate personal device. Police see the use of mobile devices as a vital tool in becoming a world-leading Police service by enabling frontline officers to be better informed, more able to share information quickly, easily and securely and, as a result, more able to make quick evidence and data-based decisions that are most appropriate for each unique situation.¹¹⁶
480. However, Police do not have a policy in place which covers the use of mobile devices when collecting personal information (photographs), nor a comprehensive process for audit and deletion of those photographs. Police officers themselves also do not routinely review and delete the photographs that they collect on their mobile devices, or which they save to other locations and databases. The inquiry team heard that these photographs were routinely retained, culminating in some officers reporting they have thousands of images on their phones. Images include scenes when attending a variety of incidents including vehicular crashes and sudden deaths. There are no apparent guidelines around how long photographs are to be retained on phones or what to do with them.
481. Guidance relating to the use of mobile devices is found in the policy 'Police Instructions – Information and Knowledge Management' for staff. This covers the acceptable use of devices, including the use of information that can be accessed from the devices, as well as personal use.
482. The joint inquiry team often received feedback from the officers that the training provided to staff around the use of mobile devices was not comprehensive. We were told that the training

¹¹³ 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.

¹¹⁴ Policing Act, s 34.

¹¹⁵ New Zealand Police *Police Mobility Action Plan 2016-2021*.

¹¹⁶ *Police Mobility Action Plan 2016-2021*, above, n 115.

provided related more to the professional use of devices, for example, ensuring the mobile device was kept secure and advice on using a strong password.

- 483. The technology policy does not provide clarity for staff on the lawful purpose for which mobile devices can be used for obtaining photographs. There is a lack of guidance for officers around what technology can be used to obtain photographs, how and where that information can be stored, how officers may use that information, or how long Police may retain that information.
- 484. The officers interviewed by the inquiry team reported that both personal and work-related photographs were kept on the same mobile devices. Many officers did not delete photographs held on their work mobile devices, with some officers indicating (when checking during their interview) they had thousands of photographs on their phones.
- 485. During interviews, the majority of officers also admitted they never deleted images from their mobile devices, or only did so after uploading them to their computer desktop, but did not record their existence or nature anywhere. It is unknown how many images are stored on computers and phones that should have been deleted. A number of officers interviewed admitted to having thousands of photographs dating back over 10 years. One officer told the inquiry team they had thousands of photographs stored on their device but that all of those photographs were wiped when they forgot their passcode to their device.
- 486. The lack of a fit-for-purpose technology policy and the existence of multiple storage systems has led to a lack of ability to easily complete audits to determine how many photographs are held, where and of whom.
- 487. Officers were also unsure whether Police had any retention policy regarding photographs held on mobile devices. For example, most officers were not aware of any guidance on how long to retain potentially sensitive photographs of deceased persons or injuries sustained in a traffic incident or as a result of an assault. Many officers were unsure of any process around what to do with the photographs on their devices when exchanging them for a new device. Some officers were prudent and ensured of their own accord that they had uploaded what they required and deleted everything off prior to handing the phone in to exchange it for a new device. However, Police apparently did not provide any formal guidance to officers.

Issues with Police storage systems

- 488. Police have processes in place in the central Police computer system (NIA) to automatically delete photographs in accordance with section 34 of the Policing Act. However, Police do not routinely delete copies of the photographs on Police's desktop computers and mobile devices. We did not find any audit processes by Police to ensure images are maintained, stored or destroyed correctly. This meant that it was impossible to identify how many copies of any image were maintained across the multitude of systems.

489. There are multiple systems available to officers with respect to storing photos (NIA, computer shared and home drives, RIOD,¹¹⁷ OnDuty, IMT,¹¹⁸ Next Cloud¹¹⁹, mobile devices, SharePoint¹²⁰). The joint inquiry team found that many officers stored photographs in multiple locations such as mobile devices, Next cloud, computer hard drives, and IMT folders.
490. The joint inquiry team further noted a lack of training regarding how to use different storage systems such as Next Cloud storage or intelligence notings via the OnDuty application.

Bypassing fixed custody suite camera systems

491. When photographs are being taken of adults in Police custody suites, there is a fixed camera system to ensure that they are automatically upload into NIA and therefore subject to the automated audit and deletion processes in that database.
492. The joint inquiry team found that many officers are instead using their own mobile devices, thus bypassing the NIA-linked system. The joint inquiry team heard from officers who stated they would take photographs on their mobile device which they would keep on their phone indefinitely and typically upload to various storage systems within Police. Officers would typically use email to transfer photographs from their phone to their personal folder on the computer hard drive. This approach creates a trail of storage.

Demonstrations policy – retention period

493. The *Demonstrations* policy currently requires that photographs or video taken at demonstrations be destroyed once the reasons for which they were taken ends. We agree that is appropriate. However, there is the potential for confusion here as, immediately after stating that destruction requirement, the policy refers staff to the NZ Police 'Disposal and Retention Schedule' for timeframes for destruction of photographs. That schedule provides that images taken of public events, including demonstrations, must be held by Police for 10 years from the creation of the image, and thereafter transferred to Archives NZ.
494. Police need to clarify the process for reconciling some limited retention for operational purposes in a way that is consistent with its disposal schedule requirements.¹²¹ Police should ensure that where images are required to be retained for public record purposes, they are archived out of relevant operational systems once the period for using the photos has expired. Police may need

¹¹⁷ RIOD (Real-time Intelligence for Operational Deployment) is an application used by Police since 2011. RIOD is designed for event and emergency management, consolidation and communication of intelligence, prevention activities and deployment, and to facilitate planning and collaboration to support and enable operational staff to deliver services in a co-ordinated fashion.

¹¹⁸ IMT folders are electronic folders within the Police Investigation Management Tool that hold investigation data for particular investigations. Members on the command chart for an operation in IMT have access to the investigation folders and their own staff folders within the IMT system.

¹¹⁹ Next cloud is a cloud-based storage system which allows Police officers to save photographs and videos from their iPhone to a private server within the Police network and onto their Police desktop computer. The photographs or videos can then be saved onto the officer's H: or S: drive, secure folder or uploaded into NIA (for Police work related photographs) or onto a USB memory stick, CD or DVD for personal photographs.

¹²⁰ Sharepoint is a Microsoft software package used by Police to allow groups or teams to share data for processes such as tasking and co-ordination.

¹²¹ For operational purposes we recommend that Police retain photographs only for as long as needed to bring criminal charges, as necessary, or address complaints about Police conduct.

a system to ensure that this is regularly done as a matter of course. As a result of this approach Police will end up with a repository of photos for archival purposes but the process should ensure that they are not accessible beyond the appropriate period.

RECOMMENDATIONS – RETENTION

19. Police policy and guidelines (including any relevant disposal schedule) should be reviewed and amended to ensure the technology policy is fit for purpose to support compliance with Police's obligations under the Privacy Act (and other relevant legislation) and to provide guidance for officers routinely using mobile devices for mixed personal and policing purposes including, in particular:

- a. the consistent storage and uploading of images and associated data to secure locations, and minimising the retention of images on individual devices and the duplication of images across Police systems;
- b. limits on using individual devices to capture images where other Police devices or technology is specifically set up for that purpose;
- c. protocols on handling sensitive or traumatic images;
- d. limits on the use and retention of images (and copies) in individual devices and in Police systems;
- e. routine review and deletion of images from mobile and desktop devices;
- f. protocols for purging and replacing devices.

20. Police should prioritise regular training for all officers on using mobile devices to ensure legal compliance.

21. Police should review systems and implement the ability to audit compliance with:

- a. updated technology policy and the handling of photographs of individuals on mobile devices; and
- b. the deletion of identifying particulars in accordance with statutory time limits.

D APPLICATION TO THE RANGATAHI COMPLAINTS

495. OPC and the IPCA are of the view, based on the evidence reviewed as part of this joint inquiry, that in many instances officers breached their obligations to the rangatahi under the Privacy Act 1993.¹²²

496. Some examples of rangatahi photography were brought to the attention of the inquiry team by way of formal complaints to the IPCA. Others were brought to our attention by Police or the news media and were considered as part of this joint inquiry rather than by way of an individual complaint.

¹²²The Privacy Act 2020 was not in force at the time of this incident. However, the relevant information privacy principles in the Privacy Act 2020 are not materially different to those in the Privacy Act 1993.

497. Where issues were raised by whānau with the media, the joint inquiry team made contact only if the whānau agreed to have their personal contact details forwarded onto the joint inquiry team for the purpose of this inquiry.
498. We note that some of the issues are historical. As a result, neither Police nor the IPCA were able to identify the officers involved or to corroborate the events as outlined for all incidents addressed in this joint inquiry. This means that, for some complaints, we are unable to make conclusive findings.
499. Some incidents have been acknowledged by Police and have resulted in letters of apology to whānau. In some cases, Police have offered to meet whānau and resolution processes have not yet concluded.
500. As noted in the terms of reference, the consideration of these incidents by the IPCA or the joint inquiry does not preclude whānau from raising their concerns with OPC as formal complaints, where particular recent incidents remain unresolved for whānau.

Incident one

501. In 2020 in Wairarapa, Police located three rangatahi late at night and spoke to them about complaints of alleged offending that recently occurred near where the rangatahi were found (**incident one**).
502. After speaking to the rangatahi the officers then detained them using their powers under section 48 of the Oranga Tamariki Act (unaccompanied youth) to return them to their home. Police would usually, as a first choice, return a youth to their parents or caregivers. In this instance the Police officers were unable to do so as the rangatahi did not provide enough details to the officers, so they were taken back to the Police station.
503. At the station the officers made enquiries to determine the parent/guardian details for each rangatahi and confirm their home addresses. The Police officers also questioned the rangatahi about the alleged offending which had taken place near where they were first spoken to. As part of the questioning process the officers took photographs of the group in the Police station custody suite using the officers' mobile devices.
504. The officers took some of these photographs in the general area of the custody suite, while one rangatahi was instructed to stand in the designated area (against the height chart) where official arrest photographs are obtained.
505. It is not clear to us the extent to which Police officers sought consent from either the rangatahi or their parents and caregivers. We were unable to establish what explanation, if any, was provided about the reasons for taking the photographs and what they would be used for.
506. At the time of the incident the rangatahi and their whānau did not make a complaint to Police or the IPCA. The incident was reported to Police and the IPCA after the Wairarapa incident came to light via complaints from whānau representatives to the media. Although in the circumstances outlined it was appropriate for the group to be detained under section 48 of the

Oranga Tamariki Act and returned to the Police station, there was no lawful reason to take photographs.

507. Although the rangatahi were detained (in terms of the Oranga Tamariki Act) they were not arrested for committing an offence. They therefore did not fall within the scope of sections 32 and 33 of the Policing Act (which allows Police to lawfully take “identifying particulars” including photographs where a person is detained for committing an offence).
508. The following IPPs should have been taken into account by Police when engaging with the rangatahi:
- (a) IPP 1 requires that Police collect information for a lawful purpose connected with a function or activity of the agency and that the collection be necessary for that purpose. Section 48 of the Oranga Tamariki Act is focused on the care and protection of an unaccompanied youth and does not specifically authorise Police to take photographs of a youth.
 - (b) IPP 4 requires that Police collect information by lawful means and in a way that is fair and not unreasonably intrusive, particularly where information is collected from youth. The rangatahi were faced with a situation where Police had taken them to the Police station late at night. There was an obvious power imbalance between the rangatahi and Police. The Police officers did not take a record of having sought “consent” from the rangatahi, contrary to Police policy. We have no way of knowing the extent to which the consent process was properly communicated to the rangatahi and their support person. Regardless, even if the consent process had been properly explained, that consent would not have made the photographs lawful.¹²³
509. We consider that the taking of the photographs was not necessary for a lawful purpose under either the Privacy Act 1993 or the Oranga Tamariki Act and was therefore in breach of IPP 1. Accordingly, we find Police actions to have been unlawful.

Incident two

510. In 2020 two rangatahi were waiting at a bus stop after school when stopped by two officers and spoken to in relation to an alleged residential burglary nearby (**incident two**). The Police officers asked the rangatahi several questions and one of the Police officers took a photograph of the teenagers. As the attending officer held their mobile device out and up to the rangatahi, they asked “*Is it OK if I get a photograph?*”, implying or assuming that consent was a foregone conclusion. As the question was posed, the full-length photograph was taken of the teenagers.
511. The Police officer briefly explained to the rangatahi that the photograph would help eliminate the teenagers from their inquiry. The rangatahi were not given an opportunity to object to the photograph and the Police officers did not attempt to contact their parents or guardians before taking the photograph.

¹²³ See discussion above in section 3A(d) – Police engagement with youth in police station settings.

512. The rangatahi and their whānau believe the boys were coerced into complying with the officers' instructions. The rangatahi told us the officers said they would call their parents in relation to being stopped and questioned. The follow-up phone calls to their parents did not occur.
513. The rangatahi were stopped and spoken to by Police 13 minutes after the 111 call made by a witness to the burglary, the location of which was roughly 550 metres away from the place where Police spoke to the rangatahi. Neither rangatahi matched the description given to Police at that time. They did not match the age, build or clothing descriptions provided to the Police by the witness. The witness who made the 111 call identified three suspects while there were only two rangatahi at the bus stop. Three different people were later apprehended for the burglary.
514. The whānau of one of the rangatahi complained formally to the local Police with the support of the whānau of the other rangatahi and the complaint was referred to the IPCA.
515. The attending officers did not recall stating they would contact the parents.
516. The following IPPs should have been taken into account by Police when engaging with the rangatahi:
- (a) IPP 1 requires that Police collect information for a lawful purpose connected with a function or activity of the agency and that the collection be necessary for that purpose. Police were provided with a description of three offenders who carried out an alleged burglary some distance from where the two rangatahi were spoken to. The two rangatahi did not match the description of the three offenders (even setting aside the difference in numbers).
 - (b) IPP 4 requires that Police collect information by lawful means and in a way that is fair and not unreasonably intrusive, particularly where information is collected from youth. The rangatahi were stopped on the street and questioned about a crime that had happened nearby. This would have been confronting for the rangatahi at the time. There was an obvious power imbalance between the rangatahi and Police and no steps were taken by the Police officers to mitigate this by seeking out support from parents or guardians before taking photographs of the rangatahi. Even if consent had been sought, that consent would need to follow Police's explaining the purpose of the collection to the rangatahi and their support person.
517. We consider that, given the overall circumstances (including the inconsistency between the descriptions of the witness and the appearance of the rangatahi), the photographing of the rangatahi in order to rule them out of the Police investigation was not reasonably necessary for a lawful Police purpose and breached IPP 1. Even if it had been lawful, it may have been unfair, without a proper attempt to either obtain informed consent from the rangatahi and their parents or guardians or establish a basis for proceeding without consent.
518. After considering the complaint made by whānau the local Police wrote a letter of apology to the whānau, with Police suggesting a meeting with the officers and whānau could be arranged for a verbal apology.

519. Along with the letter of apology, the local Police stated they understood the importance of ensuring when officers take photographs:
- (a) there is a legal basis for this, and
 - (b) the photographs are deleted from the phone when no longer relevant, or if relevant, attached to the appropriate case for which they were obtained, and then deleted from the officer's phone.
520. Both whānau have advised that they would like Police to meet with them for a 'kanohi ki te kanohi hui' (face to face meeting with a verbal apology). The whānau state their rangatahi are still left feeling uncertain about meeting with the officers concerned. There are two main reasons for this: they still feel the trauma of the interaction; and they remain somewhat mistrusting of what might be said by Police at any kanohi ki te kanohi hui.

Incident three

521. According to media reports and the descriptions provided by the rangatahi and their whānau, in late 2014 officers took photographs of two rangatahi as they waited for their koro one afternoon outside a store (**incident three**). The whānau of the rangatahi told us the city centre was busy with people having lunch, walking in the sunshine or shopping.
522. Two officers reportedly stopped the rangatahi and spoke to them about an alleged burglary nearby. We were told that the officers took photographs of the rangatahi as they spoke to them without giving them any explanation for taking the photographs and without asking for their consent.
523. We were told that the officers continued down the main street, talking to other rangatahi, speaking to them and taking photographs. The rangatahi told us that Pākehā teenagers nearby were not spoken to by Police.
524. We were told that the rangatahi went home with their koro and did not say anything to him about the incident with the Police officers. Later that afternoon a whānau member overheard them crying and enquired as to what the matter was. That whānau member told us the rangatahi were ashamed of what had happened and how the officer spoke to them. The rangatahi told their whānau member that the Police officers had accused them of committing the alleged burglary. The rangatahi appeared fearful as they told their whānau what happened, believing they would be taken to the Police station, arrested and locked up.
525. The whānau told us that after the rangatahi told their story, they went to the local Police station to ask what had happened and why. They told us that the officer who took the photograph was present at the Police station and spoke to the whānau, confirming they had spoken to their rangatahi and that they would delete the photographs from their mobile device.
526. The whānau member told us they later learned from another Police officer (unrelated to the incident) that the offenders involved in the burglary under investigation were Pākehā, not

Māori. According to the whānau members we spoke to, the rangatahi could not have been mistaken for being Pākehā.

527. The joint inquiry team was informed that the officer had no recollection or record of the interaction as described. A check of Police databases showed no record of the interaction nor any photographs held of the rangatahi. Police formed the view they did not discount that the incident may have occurred, however, due to the significant passage of time, the details could not be further corroborated. As a result, the joint inquiry team was unable to make findings based on the evidence available.
528. As **incident three** is historical, the joint inquiry team cannot make any specific findings. However, as a matter of comment we note that IPPs 1, 3 and 4 should be taken into account in this kind of encounter between Police and youth, as well as the youth specific protections under the Oranga Tamariki Act.

Incident four

529. In early 2021, a Police officer was driving down a suburban street in the afternoon when he saw a group of rangatahi having an animated conversation on the street. The officer stopped and got out to speak to them, believing a fight or assault had either taken place or was imminent.
530. The complainant told us the group of youths were either friends or related to each other.
531. One rangatahi's mother told us her son refused to provide the Police officer with his details and that he told Police what he understood to be his rights (based on Community Law advice). The rangatahi's mother told us that the officer responded by telling the rangatahi he would be arrested for refusing to provide his details.
532. The officer who spoke to the rangatahi gave a different account from what we understand to be the rangatahi's account. The officer said that he advised the rangatahi he would be arrested for disorderly behaviour if he continued to refuse to provide his details, as the officer was unable to confirm his identity. The attending officer reported the incident to Police communications and shortly afterwards other units arrived on the scene.
533. We were told by the rangatahi's mother that the Police officers continued to take photographs of the group even after members of the group turned their faces away from the mobile devices or held up their arms in front of their faces to obstruct the images being taken. The attending officer told us it was only one rangatahi who continued to be photographed and that this was due to the rangatahi refusing to keep still and look at the camera.
534. The rangatahi's mother told us that her son continued to refuse to allow his photograph to be taken. The officer told the rangatahi he believed an offence had occurred (fight or assault) which then allowed the officer to take photographs. The police officers did not arrest anyone or give anyone a warning in relation to the incident.
535. The rangatahi's mother told us that her son had been stopped by Police when walking home late one evening a few months prior. When he arrived home after being stopped on that occasion

he told his mother that he was stopped and spoken to in relation to an alleged burglary nearby and that the Police officers had taken a photograph of him. This had sparked a conversation between the rangatahi and his mother about the rights of youth and what they have to tell Police when stopped.

536. The rangatahi's mother told us that she had researched what her son's rights were through the Community Law resources and she told us that she and her son had a discussion prior to the second incident.

The complaint to Police

537. The whānau complained to their local Police station and attended four meetings between the mother and the local Police, one of which included the rangatahi. Following the meetings Police sent a letter of apology to the rangatahi.

The complaint to the IPCA

538. The whānau complained to the IPCA and the complaint was reviewed as part of the joint inquiry alongside OPC.
539. The rangatahi could not be arrested for disorderly behaviour (for declining to provide his personal details) and the officer did not have the legal authority to make this statement. If the officer had reasonable grounds to suspect another offence and intended to proceed by way of summons rather than arrest, the officer could have required the rangatahi to provide his name and address. However, we do not think that the officer had reasonable grounds to suspect any other offence that would have enabled him to proceed in this way.
540. The following IPPs should have been taken into account by Police when engaging with the rangatahi in this incident:
- (a) IPP 1 requires that Police collect information for a lawful purpose connected with a function or activity of the agency and that the collection be necessary for that purpose. It is not clear what the purpose for collection was in this case. While the officers were within their functions by speaking to the rangatahi about the incident that they thought was unfolding it is not clear that the photographs were obtained for any purpose related to that incident (noting that no arrests were made, or warnings given). OPC and the IPCA consider that the officers breached IPP 1.
 - (b) IPP 3 requires that Police must take steps that are, in the circumstances, reasonable to make sure that the individual concerned is aware of the information being collected, the purpose of collection and the consequences of not providing the information. In this case, the Police officers did not provide the rangatahi with an adequate explanation as to why the information was being collected and what would happen if they did not comply with the request. OPC and the IPCA consider that the officers breached IPP 3.
 - (c) IPP 4 requires that Police collect information by lawful means and in a way that is fair and not unreasonably intrusive, particularly where information is collected from youth. In this case the Police officer observed what he considered to be an unfolding incident. However,

the incident seems to have escalated and more Police officers involved after the rangatahi refused to comply with the officer's requests for personal information. The officer did not explain adequately the basis for requesting that information and instead involved more officers to attend the incident. This would have been confronting for the rangatahi at the time. There was an obvious power imbalance between the rangatahi and Police and no steps were taken by the Police officer to mitigate this by seeking out support from parents or guardians before taking photographs of the rangatahi. We do not consider that the means of obtaining the photographs were fair and this was a breach of IPP 4.

541. It is the shared view of OPC and the IPCA that while Police had the right to stop and speak to the group of rangatahi and ask questions, they did not have the right to obtain photographs in the circumstances as described. If the attending officer wishes to obtain photographs, they need to have a particular purpose for doing so and should have then provided further information about the reasons for collecting that personal information to the rangatahi, with informed consent provided by the rangatahi and their parent or guardian to Police. Police accept these findings.

Incident five

542. We were told that sometime between 2014 and 2016, a rangatahi was walking home in the middle of the night after playing basketball at the local school (**incident five**). It was summertime, during school holidays, and on the weekend.
543. The rangatahi described being stopped and spoken to by a Police officer who told him there had been complaints to Police from '*people in the neighbourhood having concerns*'. The rangatahi's mother told us that the Police officer took a photograph during the conversation. The officer reportedly did not give the rangatahi an explanation about why he took the photograph or what it would be used for and did not ask whether he could take the rangatahi's photograph.
544. The rangatahi's mother told us the rangatahi was returned home by the officer who took a further photograph at his residence with his mother present. However, the Police officer did not provide the rangatahi or his mother with an explanation for why he was taking the photograph or ask for consent before doing so. The rangatahi's mother told us that she told the Police officer that she did not consent to the photograph. The mother said that she asked the officer to delete the photographs of her son and he refused.
545. The mother of the rangatahi told us that she complained to the local Police station asking why this incident had occurred. She told us that she was concerned her son was targeted due to generational racism she believes exists in the judicial system.
546. The mother was told by Police at the time that there was no information entered in NIA about the encounter and Police were unable to provide any further information to her. As the officers was not able to be identified by Police, they were unable to confirm whether the photographs had been deleted or not.

The complaint to the IPCA

547. The whānau complained to the IPCA. The IPCA responded to the whānau stating Police did not find any photographs of their rangatahi stored on any Police devices and the rangatahi was not the subject of any investigations. Therefore, the IPCA was unable to determine any wrongdoing by Police at the time and was unable to take any further action on the complaint. As a result, the joint inquiry team was unable to make findings based on the evidence available.
548. In relation to **incident five**, based on the description of the facts provided by the rangatahi's mother (noting that we were unable to substantiate her account), IPPs 1, 3 and 4 should be taken into account by Police when engaging with any rangatahi in this kind of case.

Whānau views

549. The whānau we spoke to told the joint inquiry team about the impact that the incidents had on them and their desire for next steps as follows:

Incident one

550. Whānau representatives expressed concern at how the photographs were taken by officers. They questioned what photographs were retained by Police and what they would be used for. They told us that they are worried the photographs could be used in facial recognition technology.
551. The whānau told us that Police have spoken of wanting to create a better relationship with Māori but they wonder realistically what has been done to achieve that, when they viewed what happened to their rangatahi and heard reports in the media that this has happened to others.
552. Whānau representatives told us that they want Police to better address and understand the power imbalance they have, particularly with youth in Aotearoa. They commented that *"they [rangatahi] will do what is asked of them, without question"* but requests were being made of youth when their fundamental rights were not being adhered to by Police.
553. Whānau spoke of a desire to see better education for Māori to understand their rights in particular around privacy and know how to speak up.

Incident two

554. Whānau told the joint inquiry team that the incident at the bus stop was just one of numerous occasions of their rangatahi and other whanau members being stopped and spoken to by Police. Their rangatahi had clear recollection of the wording and manner in which the Police officers asked their consent to take their photograph. They told us that the officer already had their mobile device poised and there was never an opportunity for the rangatahi to question or refuse the request put to them before the photograph was taken.
555. To bring closure, the whānau have spoken of wanting to see policy or legislative changes brought about to ensure the practice of photographing any tamariki and rangatahi does not continue.

They cite it is important for Police to realise the feelings of whakamā (shame) and upset felt by the whānau.

Incident three

556. Whānau told the joint inquiry team that they are hoping for meaningful change to be brought about by Police in how they perceive rangatahi to be treated and racial biases they believe are prevalent in Police.

Incident four

557. Whānau told the joint inquiry team that the incident was not the only instance of their rangatahi being stopped and spoken to by Police, with photographs obtained of their son. Their wish was to see Police implement formal changes to ensure this did not happen again to rangatahi and they hoped for officers to better understand their obligations to youth and Māori.

Incident five

558. To bring closure, the whānau have advised the joint inquiry team that they would like Police to ‘whakautu’ (respond) by committing to training across the organisation to identify and understand their biases. The whānau believe biases held by Police contribute to the problem of how Māori are perceived by Police.

Consideration of tikanga

559. As this report notes at paragraph 107 above, the Privacy Commissioner must take account of cultural perspectives on privacy pursuant to section 21(c) of the Privacy Act. Tikanga may inform how best to approach a situation in an appropriate way in order to meet the cultural needs of affected individuals and their whānau. OPC is conscious that all of the incidents reported to it and to the IPCA in the course of the joint inquiry are Māori and so this report must reflect this.
560. OPC provides this overview of tikanga to explain the impact of Police’s actions on rangatahi and their whānau and to assist Police with its understanding of the situation and how it may be resolved.
561. During the joint inquiry and subsequent meetings OPC had with the rangatahi and whānau, whānau expressed “their feelings of whakamā (shame),¹²⁴ embarrassment, frustration and anger they feel from the actions by Police towards their rangatahi”.

Whakamā

562. The word whakamā describes the notion of embarrassment and shame.¹²⁵ Whakamā may begin with the individual but the wider group, whānau, hapū and iwi can also be impacted. The feeling of whakamā can be very intense and can cause substantial harm to all concerned. The whakamā can result because of the actions of an individual that then reflects back on themselves or could

¹²⁴Significant humiliation is one of the recognised grounds for remedies under the Privacy Act for a breach of privacy. See Privacy Act 2020, s 69.

¹²⁵Ministry of Justice *He Hīnātore ki te Ao Māori: A glimpse into the Māori world* (2001) at 185.

be caused by the actions of someone else impacting on an innocent party. The latter would be the case in this incident.

Takahi Mana

563. When whakamā is experienced, the result is takahi mana, which describes the trampling on the self-esteem or standing of an individual or group through the actions of someone else. In this case, Police's actions would have had the effect of takahi mana.

Addressing the Whakamā

564. To remain in a state of whakamā can impact significantly on whānau and a process needs to be put in place that can help address the imbalance that individuals or whānau feel. This can be done through karakia, hui, gifting of taonga, koha, or apologies. The important point is that something needs to take place. Those who are in a state of whakamā or have experienced the whakamā need to be empowered to ensure they feel that the whakamā has been lifted and they can return to a state of balance and wellness.
565. This joint inquiry has begun the process by giving voice to rangatahi and whānau. Whānau, through the inquiry process, have provided guidance on how they would like the take, or issue, addressed.
566. Sir Hirini Moko Mead provides a framework that can help return all parties to a state of wellness. It is important to note that not only is this process about the rangatahi and their whānau, but done well, it will support Police in removing the whakamā that they may also experience as a result of their actions.

Take, Utu. Ea¹²⁶

567. The following framework provides a means of identifying the issue, a process for addressing the issue and finding solutions to achieve resolution:
- (a) **Take:** identifying the issue;
 - (b) **Utu:** identifying the form of redress that will most appropriately address the imbalance felt by the whānau; and
 - (c) **Ea:** achieving the desired state where all parties are satisfied with the outcome.
568. It would seem that the first stage of the framework has been completed, *take* – identifying the issue. This report will contribute to the process of addressing the issue and should lead to finding solutions to best achieve the resolution or the state of ea.
569. Key to this framework being utilised successfully is the inclusion and empowerment of the rangatahi and whānau in the process to have their voices heard.

¹²⁶Hirini Moko Mead *Tikanga Māori: Living by Māori Values* (1st ed, Huia Publishers, Wellington, 2003) at 341.

4 GENERAL FINDINGS

570. This section of the report contains the joint inquiry's general findings about:

- (a) gaps in policies and the lack of guidance around the use of mobile technology;
- (b) lack of awareness of the Privacy Act due the lack of training or guidance for staff; and
- (c) the need for an overarching strategy to improve understandings of the Privacy Act to ensure the trust and confidence of communities and whānau.

Gaps in policies and lack of guidance

571. Despite mobile devices being made widely available to Police for use in daily activities since 2013, the technology policy does not provide clear direction for officers on the lawful use and purpose for mobile devices when taking photographs of members of the public, including youth.

572. While Police have embraced mobile devices as an aid to perform various tasks, guidance and training have not been adequately developed and communicated to staff. There is a lack of guidance for officers explaining the circumstances in which mobile devices can be used to obtain photographs, how and where that information can be stored, how it is to be used and how long it should be retained.

573. We consider that Police should ensure that relevant policies (including the technology policy) are made fit for purpose, reflecting the status of digital photographs as sensitive biometric information. These policies should provide guidance to officers about using mobile devices when photographing and videoing members of the public and the relevant procedures for storage and retention to ensure legal compliance.

574. Policy relating to photography is covered in different 'Police Instruction' guidance for taking, downloading and securing images for evidential purposes. The joint inquiry team noted gaps in Police guidance in the following areas:

- (a) the use of mobile devices to obtain, secure and retain photographs in accordance with the policy;
- (b) guidance on images collated from CCTV specific to youth;
- (c) taking voluntary prints using Live Scan;
- (d) the destruction of photographs in accordance with section 34 Policing Act if obtained under sections 32 and 33; and
- (e) storage of these photographs under the Children, Young Persons and their Families Act 1989 (now the Oranga Tamariki Act).

575. Current Police policy regarding photographing and video recording members of the public is fragmented and does not provide adequate guidance on Police authority to obtain photographs

for investigative purposes. Specifically in relation to youth, the current Police Youth Justice policy does not clarify the relationship between the Privacy Act, the Oranga Tamariki Act and UNCROC, and it does not provide any specific guidance for taking photographs of youth in a public place.

- 576. Apart from the fact that Police policies are piecemeal and contain significant gaps, what policy there is can be difficult to find. Many officers we spoke to told us that they had tried to find the relevant Police policy ahead of our interviews but had been unable to locate any. Many officers told us that, when told they would be interviewed, they tried to find the relevant Police policies to make sure they complied with those policies but could not find any.
- 577. Officers were unable to tell OPC what authority they have to take photographs in most circumstances. Officers almost universally described a lack of training or guidance focussed on when it is lawful and appropriate to photograph or video record members of the public for the purpose of non-crime scene identification.
- 578. There is also a lack of instructions or guidelines for Police staff on the practical aspects of taking photographs of youth using mobile devices, and the different situations in which they may be required. For example, the needs of a front-line officer will be different to an officer engaging with their community in a Community Policing or Māori, Pacific and Ethnic Services role, and further still from an Intel Officer role.
- 579. As a priority, we consider that Police should develop and deliver agency-wide training to its staff and relevant contractors on the decision-making framework and procedures to be followed to photograph individuals and youth in public, and related storage and deletion procedures.
- 580. **We find that** policies are not easily accessed, and officers often do not comply with policies that are in place to guide their practice. Even where there is a policy in place the content is often either insufficient or inconsistent with the Privacy Act.

Lack of awareness of the Privacy Act 2020

- 581. The joint inquiry team found that there is a lack of training and guidance on the Privacy Act and its principles provided to Police officers and staff. Many officers did not know that the Privacy Act existed or that it applies to them. This applies to both sworn and unsworn staff, from recruits entering Police College to managers with several years' experience.
- 582. We found that little or no training is being provided by Police (both to new recruits and on an ongoing basis) focussed on compliance with both the Privacy Act and the Policing Act. There is little understanding or appreciation of how the Privacy Act is applicable, or the circumstances of how or when to report privacy breaches to the Privacy Team at PNHQ (or to OPC).
- 583. The lack of training and guidance on privacy has likely led to the systemic overcollection of personal information and the potential mishandling of personal information in the form of photographs of members of the public, including improper storage and retention.

584. **We find that**, overall, Police lack adequate understanding of the Privacy Act and have not developed appropriate training, guidance or policies to enable officers to use their powers and collect information effectively and lawfully. The Police roll out of technology and mobile devices was not accompanied by sufficient training and support and this has resulted in practices that are inconsistent between districts. This is particularly concerning as digital photographs are sensitive biometric information.
585. As a result of this **we find that** Police have been collecting, using and retaining personal information in a way that is at best inconsistent with the Privacy Act and, in some cases, likely unlawful.
586. **We find that**, the manner in which Police collect, use and retain personal information would have likely resulted in systemic breaches under the Privacy Act affecting the rights of individuals.

Trust and confidence

587. As a result of the findings above, we consider that Police should develop a strategy to improve the fundamental understanding within the New Zealand Police of the application of the Privacy Act to the collection and protection of personal information as integral to policing by consent and ensuring the trust and confidence of communities and whānau.
588. Although we examined examples of Police practice affecting both adults and youth, we saw that the Police actions had a disproportionately negative impact on youth and were contrary to the youth protection frameworks in place. We also note that all of the youth who were part of this joint inquiry are Māori and that the incidents have had a significant impact on these rangatahi and their whānau.
589. Police acknowledge that policing by consent carries significant responsibilities and how vital it is for communities and whānau to have trust and confidence in the way that policing is delivered in New Zealand.¹²⁷

GENERAL RECOMMENDATIONS

22. Police should develop a strategy to improve its staff's fundamental understanding of the Privacy Act's application to the collection and protection of personal information with a particular focus on photographs as sensitive biometric information covering:

- a. policies and processes;
- b. training; and
- c. methods for updating knowledge and practice on an ongoing basis.

23. In implementing the strategy, Police should establish a rolling programme of reviews and updates of key policies, and develop and deliver agency-wide training to its staff and relevant contractors on:

¹²⁷New Zealand Police | Ngā Pirihimana o Aotearoa "[Programmes and initiatives: Understanding Policy Delivery](http://www.police.govt.nz)" <www.police.govt.nz>.

- a. the decision-making framework and procedures to be followed to photograph individuals and youth in public; and
- b. storage and deletion procedures.

5 ACTIONS TAKEN DURING JOINT INQUIRY AND NEXT STEPS

COMPLIANCE NOTICE ISSUED TO POLICE

590. In December 2021 the Privacy Commissioner issued Police with a compliance notice. Police was found to be noncompliant with IPP 9 in relation to its retention of identifying particulars of individuals (including the “voluntary collection” of duplicate photographs and biometric prints).
591. A compliance notice requires an agency (in this instance, Police) to do something, or to stop doing something, in order to comply with the Privacy Act. They are drafted and discussed with the organisation with the aim of agreeing on how the issues identified will be rectified by them. The compliance notice is formally issued after this mutually consultative process.
592. The compliance notice issued to Police discussed the systemic retention by Police of the identifying particulars of individuals when in Police custody, and photographs of members of the public who have not been detained.
593. OPC identified these issues in the course of its ongoing joint inquiry with the IPCA.
594. The purpose of the compliance notice was to require Police to remedy the identified breach of the Privacy Act and limit the resulting impact on the individuals concerned from the ongoing retention of their identifying particulars in breach of IPP 9. It requires Police to take a number of steps with respect to photographs and biometric prints including deletion, retention and storage, and changes to collection practices of voluntary photographs and biometric prints of youth in custody.
595. The Privacy Commissioner is pleased with the constructive way in which Police have engaged with OPC thus far on the compliance notice and its requirements, and Police are reporting regularly to OPC on progress towards compliance under IPP 9. Police have indicated that they wish to publicly release their bi-monthly progress reports to OPC. The Privacy Commissioner welcomes this approach and the commitment it signals to openness, transparency and change. The Privacy Commissioner has varied the reporting timeframes in the compliance notice and from 2023 Police will report quarterly on progress towards compliance.

POLICE ACTIONS

596. In addition to responding to the compliance notice, Police have undertaken an internal review of aspects of its practice considered as part of this joint inquiry. That review has resulted in some changes to Police practice as a starting point. We expect that Police will consider its next steps

and review policy and training in light of the findings and recommendations outlined in this joint inquiry report and Police has undertaken to consult quarterly with OPC on this work.

597. The *Understanding Policing Delivery* research programme (UPD) was set up by Police in March 2021 to focus on examining where biases may exist within police policies, processes, and practices.¹²⁸ The Police website states their work will focus on research into understanding whether, where, and to what extent, bias exists at a system-level in Police's operating environment. This work is ongoing and literature reviews and a progress report were released in early June 2022.¹²⁹ As noted, while the existence of bias was not part of our terms of reference we will refer this report to the *Understanding Policing Delivery* Independent Advisory Panel in the hope it will be of assistance in the ongoing research agenda.

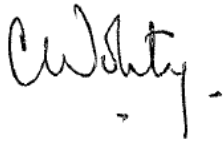
KANOHI KI TE KANOHI AND HUI

598. Whānau indicated during the course of the joint inquiry they would be interested in having hui with Police kanohi ki te kanohi (face to face) to discuss the issues raised in this report.
599. OPC supports the idea of hui taking place to allow rangatahi and their whānau the opportunity to engage with Police following the substantiation of the complaints in incidents 1, 2 and 4 by the inquiry. We hope that this engagement would allow Police to better understand the impact of Police behaviour on the rangatahi and the wider implications of this felt by their whānau and community.
600. The whānau expressed a wish to see and feel the intent of an apology from Police for the impact of the unlawful actions and to have the opportunity for Police to acknowledge the hurt and whakamā (shame and embarrassment) felt by the rangatahi and their whānau.
601. As noted in the terms of reference and as required by section 21(c) of the Privacy Act, the Privacy Commissioner must take account of culture perspectives on privacy. In these particular circumstances the Privacy Commissioner needs to ask the question "what would tikanga require?" It is the Privacy Commissioner's view that it would be appropriate, in the circumstances, for Police to apply Sir Hirini Moko Mead's "Take, Utu, Ea" framework to enable balance to be restored for the rangatahi and their whānau.¹³⁰
602. We note that in at least some of the cases Police have had some engagement with whānau by way of letters of apology and some hui. However, OPC sees this joint inquiry as a starting point and urges Police to continue its work on these issues without leaving the affected rangatahi and their whānau behind.

¹²⁸See "[Understanding Policing Delivery](#)", above n 127; and "[Police launch investigation into 'unconscious bias' against Māori](#)" *Radio New Zealand* (online ed, 16 March 2021).

¹²⁹Kua tīmata Ngā Pirihihihi i te wāhanga hou o te rangahau i te tika me to tōkeke o ngā mahi pirihihihi | Police embark on new phase of research into Fair and Equitable policing ([2 June 2022](#)).

¹³⁰See paragraphs 567 to 569 above; and Mead *Tikanga Māori: Living by Māori Values*, above, n 126.



Judge Colin Doherty

Chair
Independent Police Conduct Authority

8 September 2022



Liz MacPherson

Deputy Privacy Commissioner
Office of the Privacy Commissioner

8 September 2022

APPENDIX 1 – DOCUMENTS

A POLICE POLICIES REVIEWED DURING THE JOINT INQUIRY

Policy	Description/comment
Adult sexual assault investigation (ASAI) policy and procedures	Minimal information around the photographing of victims and storage of images for evidential purposes.
Arrest and detention	Information mainly based around the Policing Act section 32-34 photographing of offenders after arrest.
Assaults and injuries to the person	Minimal information around the photographing of victims and storage of images for evidential purposes.
Child protection investigation policy and procedures	Minimal information around the photographing of victims and storage of images for evidential purposes.
Controlled purchase operations	Minimal mention of photographs in relation to photographic ID and obtaining photographs of the volunteers.
Covert imagery	Mostly around Search and Surveillance Act and warranted powers. Use of video capture.
Disaster victim identification (DVI)	Basic information around the role of the photography coordinator.
Family harm policy and procedures	Minimal information around the photographing of victims and storage of images for evidential purposes.
Fingerprints	Powers covered under section 32 of the Policing Act.
General enquiries in homicide and serious crime investigations	Process for carrying out a photograph line up, how to create and conduct.
Identification of offenders	Process for carrying out a photograph line up, how to create and conduct.
Identifying drivers with face coverings	Mention of section 114 Land Transport Act and the <i>Cunnard v Auckland</i> decision.
Identifying particulars for summons	References section 33 of the Policing Act.
Photography (Forensic imaging)	Comprehensive policy mostly around storage of images and taking of images by forensic photographers. Does not

Policy	Description/comment
	cover general everyday photography by Public Safety Teams.
Police filming and audio recording of operations and events	Refers to types and authority for using different types of recording devices, body worn cameras, Taser cameras etc. Mention made to smartphones and the mobility initiative.
Policing Outlaw Motorcycle Gang Runs	Mention of how and when to obtain images.
Behaviour offences	Power to obtain images after arrest section 32 Policing Act.
Unlawful assembly and rioting	Power to obtain images after arrest section 32 Policing Act.
Demonstrations	Surveillance powers and power to obtain images after arrest section 32 Policing Act.
Mass arrest processing	Power to obtain images after arrest section 32 Policing Act.
Collection of personal information	Refers to IPPs 1, 2, 3 and 4.
Remotely Piloted Aircraft Systems (RPAS)	Reference to the Civil Aviation Act and Search and Surveillance Act sections 46 and 48.
Road blocks and stopping vehicles for search purposes	Outline of the lawful grounds to photograph people.
Categories of surveillance with a device	References to the Search and Surveillance Act and the use of surveillance devices.
TASER (Conducted Electrical Weapons)	Information about the Taser Camera and the recording of information.
Youth Justice – Part 1- Introduction to youth justice	References to the Oranga Tamariki Act and Policing Act sections 32-34.
Youth Justice – Part 2 – Responding to youth offending and related issues	
Youth Justice – Part 3 – Criminal procedure in the Youth Court	

Terms of reference: Independent Police Conduct Authority & Office of the Privacy Commissioner “Joint Inquiry into Police photographing of members of the public” (9 March 2021).

TERMS OF REFERENCE

Independent Police Conduct Authority & Office of the Privacy Commissioner

Joint Inquiry into Police photographing of members of the public

PURPOSE

Joint Inquiry by the Independent Police Conduct Authority (IPCA) and the Office of the Privacy Commissioner (OPC) into New Zealand Police’s conduct, practice, policies and procedures as they relate to the photographing of members of the New Zealand public who are not being detained for or suspected of committing an offence, including whether Police action, policy or procedure has resulted in the privacy of individuals being infringed. The Inquiry will incorporate the investigation of reported incidents of Police photographing Māori youth in Wairarapa in August 2020 who had not committed or been suspected of committing an offence and who had not provided informed consent.

RATIONALE

This Inquiry is being undertaken following substantial media publicity in December 2020 about Police taking photographs of Māori young people in the Wairarapa in August 2020, in the circumstances noted above. After IPCA made direct enquiries with Police, they formally notified IPCA of the incidents on 24 December 2020. Police have subsequently provided information to IPCA about similar matters where Whanganui Police staff were photographing Māori young people in 2014. IPCA has also recently concluded an investigation into a complaint about Northland Police staff taking photographs of other members of the public without the necessary lawful grounds to do so.

Rationale for a Joint IPCA/OPC Review

Police photographing of members of the public who are not being detained for or suspected of committing an offence raises significant Police conduct, policy, practice and procedure and privacy issues. As such this Inquiry falls into the jurisdiction of both IPCA and OPC and both agencies had decided to inquire into the reported issues.

Given this, it has been agreed that the Inquiry is to be a joint project conducted under the powers and authorities of both IPCA and OPC, with the scope and terms of reference for undertaking the Inquiry confirmed following an initial scoping and issue identification exercise.

IPCA and OPC bring different powers and authorities to the Joint Inquiry:

- IPCA brings its powers to investigate complaints under s12(1)(c) of the Independent Police Conduct Authority Act 1988. Additionally, section 12(2) broadens the power to investigate to any Police practice, policy or procedure which relates to the complaint. Following an investigation, IPCA can make recommendations pursuant to s27(2) of the Act.
- OPC brings both powers of inquiry under s17(1)(m) of the Privacy Act 2020 and the new regulatory action powers prescribed in the Privacy Act 2020. These powers include the ability to issue compliance notices should the Inquiry find a relevant breach of the Privacy Act.

KEY ISSUES FOR CONSIDERATION

1. To determine whether Police actions with respect to the Wairarapa incidents complied with Police policy, the Privacy Act 1993, and any other legislation.
2. To determine if any compliance and enforcement action is required if it is found that Police breached the privacy of the individuals involved.
3. To identify the extent to which, and the reasons why, Police are photographing members of the public in public places.
4. To identify variations in practices in this respect across Police Districts.
5. To determine the extent to which any or all of these practices are consistent with the Privacy Act or any other legislation.
6. To identify what Police policy and practice in this area ought to be, including the extent to which any specific restriction or requirement ought to govern the photography of children and young people.

SCOPE/METHODOLOGY

1. Request and review material obtained from Police
2. Conduct interviews with youth involved in the Wairarapa Police photographing activities and any other relevant contacts of the young people including members of their whānau, hāpu or iwi, caregivers and youth aid workers.
3. Conduct interviews with officers involved in the Wairarapa Police photographing activities
4. To the extent necessary, obtain further information about, and if necessary conduct interviews, about Police policy and practice in other Districts
5. Critically examine Police's review and findings
6. Determine preliminary findings and recommendations
7. Draft public report for Police comment.
8. Finalise report in light of submissions received.

Initial scoping exercise

- Review relevant legislation (and subsequently Police’s compliance with same):
 - Privacy Act 1993 & 2020
 - Policing Act 2008
 - Land Transport Act
 - Search & Surveillance Act
 - Oranga Tamariki Act 1989
 - Bill of Rights Act 1990
- Confirm extent of Police policy relating to photographing members of the public
- Review current Police policy (and that which was applicable at the time of the incidents) in relation to the photographing of children and young people.
- Request further information from Police about Wairarapa/Whanganui/Northland incidents and, if necessary, conduct joint interviews with officers to establish what they did and why.
- Request information from Police about all known instances where officers have taken photographs ‘for the purpose of their function’.
- Request information from Police about relevant district practices.
- Determine quality assurance processes within the Police in terms of relevant work practices
- Review documentation relating to requirements re informed consent.

TIMEFRAMES

Draft report completed by end of September 2021

OUTCOMES

The Inquiry will result in a joint report for Police and the public, providing an assessment of Police’s compliance with relevant legislation and policy, and any recommendations for remedial measures that should be taken to improve policy and practice.

To the extent that relevant breaches of the Privacy Act 1993 or 2020 by the Police are identified and confirmed, the Inquiry could also result in compliance and enforcement action being undertaken by OPC.

Neither of these outcomes precludes the ability of individuals who feel that their individual privacy has been infringed to make a complaint under the Privacy Act 2020.

COMMUNICATION

All communication or engagement activity including with the media will be approved through the business owners.

No formal comment on the Inquiry or its findings should be made public without consultation with the other agency.

Privacy Commissioner “Compliance notice: New Zealand Police – Ngā Pirihimana o Aotearoa” (22 December 2021).



Office of the Privacy Commissioner
PO Box 10094, The Terrace, Wellington 6143
Level 11, 215 Lambton Quay
Wellington, New Zealand
P +64 4 474 7590 F +64 4 474 7595
E enquiries@privacy.org.nz
0800 803 909 Enquiries
privacy.org.nz

Compliance notice

New Zealand Police – Ngā Pirihimana O Aotearoa

Table of contents

Authority to issue compliance notice	1
Compliance notice issued.....	1
Scope	1
Background	2
Statutory framework.....	2
Policing Act 2008.....	2
Oranga Tamariki Act 1989	3
Privacy Act 2020	4
Overview of Agency operations and investigation	5
Police information holding and destruction systems	5
Investigation of compliance issues.....	5
Description of identified noncompliance (section 125(1)(b))	8
Decision.....	10
Requirements of section 124(1) prior to making decision.....	10
Decision and reasoning	11
Remedying the breach	11
Steps that the Agency must take to remedy the noncompliance (sections 125(1)(c) and 125(2)(a)).....	11
Timeframes and reporting (section 125(2)(c))	13
Right to appeal (section 125(1)(d)).....	14
Enforcement and publication	14

COMPLIANCE NOTICE

Issued under section 123 of the Privacy Act 2020 (**Privacy Act**)

Agency (section 125(1)(a))	New Zealand Police
Notice number	CN/2021/02
File reference	qA135545

AUTHORITY TO ISSUE COMPLIANCE NOTICE

- A Under Part 6(2) of the Privacy Act, I am empowered to issue a compliance notice if I consider that an agency is not complying with its obligations under the Privacy Act.
- B I have provided the Agency with a reasonable opportunity to comment on a written notice pursuant to section 124(3) of the Privacy Act.

COMPLIANCE NOTICE ISSUED

- 1 I hereby issue this compliance notice to the Agency pursuant to sections 123(1) of the Privacy Act as necessary to require the Agency to remedy its noncompliance with information privacy principle (IPP) 9 as this compliance notice describes in paragraphs 38 and 39.¹
- 2 I now require the Agency to:
- a take the steps set out at paragraphs 45 to 47; and
 - b take each of those steps within the timeframes specified at paragraph 47,
- for the Agency to rectify its noncompliance with IPP 9.

SCOPE

- 3 This compliance notice relates to the systemic retention by the Agency of the identifying particulars of individuals when in police custody, and photographs of members of the public who have not been detained. My Office (OPC) has identified these issues in the course of its ongoing joint inquiry (**Joint Inquiry**) with the Independent Police Conduct Authority (IPCA).²

¹ This compliance notice does not necessarily set out all of the issues with respect to the Agency's noncompliance with the Privacy Act 2020. I reserve my right to issue a compliance notice to the Agency in the future with respect to with IPP 9, any other IPP, or any other aspect of the Privacy Act 2020.

² See Independent Police Conduct Authority and the Office of the Privacy Commissioner *Terms of Reference: Joint Inquiry into Police photographing of members of the public* (9 March 2021) Office of the Privacy Commissioner <<https://privacy.org.nz/publications/commissioner-inquiries/joint-inquiry-into-police-photographing-of-members-of-the-public/>>.

- 4 The purpose of this compliance notice is to require the Agency to remedy the identified breach of the Privacy Act and limit the resulting impact on the individuals concerned from the ongoing retention of their identifying particulars in breach of IPP 9.
- 5 This compliance notice focuses on the retention of particular types of personal information, being “identifying particulars” (as that term is defined in the Policing Act 2008 (**Policing Act**)) in the form of:
 - a photographs; and
 - b fingerprints and palmprints (**Biometric Prints**).
- 6 This compliance notice is the first of a number of compliance notices I am considering issuing to the Agency with respect to systemic compliance issues that OPC has found in the course of the Joint Inquiry.

BACKGROUND

Statutory framework

Policing Act 2008

- 7 The Agency is an “instrument of the Crown” that exists pursuant to section 7(1) of the Policing Act. The Agency’s functions include keeping the peace, law enforcement, crime prevention, and community support and assurance.³
- 8 The Agency has statutory powers to collect sensitive personal information from individuals to carry out its law enforcement activities. The circumstances in which the Agency is empowered to collect and retain personal information is clearly set out in several statutes, including the Policing Act.
- 9 The powers of the Agency to collect and hold identifying particulars are set out in Part 3 of the Policing Act. Section 32 of the Policing Act governs the taking of identifying particulars of a person in custody by the Agency including photographs and Biometric Prints. Section 32 allows the Agency to store identifying particulars in its information systems. In particular:
 - a a constable may take the “identifying particulars”⁴ of a person who is in the lawful custody of the Agency if that person is detained for committing an offence and is at a police station, or at any other place being used for police purposes;⁵

³ Policing Act 2008, s 8.

⁴ See Policing Act 2008, s 32(5). The definition of “identifying particulars” in relation to a person under the Policing Act 2008 also falls under the definition of “personal information” as that term is defined in section 7(1) of the Privacy Act 2020.

⁵ Policing Act 2008, s 32.

- b a constable who has good cause to suspect a person of committing an offence and who intends to bring proceedings against the person in respect of that offence by way of summons:⁶
 - i may detain that person at any place in order to take that person's identifying particulars; and
 - ii must take the person's identifying particulars in a manner that is reasonable in the circumstances.
- 10 Section 34 of the Policing Act governs the storage and destruction of identifying particulars including photographs and Biometric Prints. Photographs or visual images of a person, and impressions of a person's fingerprints, palmprints, or footprints, that are obtained under section 32 or 33 of the Policing Act must be destroyed as soon as practicable after:⁷
- a a decision is made not to commence criminal prosecution proceedings against the person in respect of the offence for which the particulars were taken; or
 - b criminal prosecution proceedings that are commenced against the person in respect of the offence for which the particulars were taken are completed with an outcome (for example, an acquittal) that is not an outcome that authorises continued storage.

Oranga Tamariki Act 1989

- 11 The Children's and Young People's Well-being Act / Oranga Tamariki Act 1989 (OT Act) allows a police officer (in their capacity as an "enforcement officer" under that Act) to, in limited circumstances, arrest a child or young person without a warrant.⁸
- 12 In relation to young persons (as that term is defined in the OT Act) and young Māori (a young person who is Māori being **rangatahi**), section 214 of the OT Act limits the power of the Agency (as an "enforcement officer" for purposes of that Act) to arrest a child or young person without a warrant except in certain limited circumstances where the officer is satisfied on reasonable grounds that it is necessary to arrest the child or young person for the purpose of:⁹
- a ensuring the appearance of the child or young person before the court;
 - b preventing the child or young person from committing further offences; or
 - c preventing the loss or destruction of evidence relating to an offence committed or preventing interference with a witness.

⁶ Policing Act 2008, s 33.

⁷ Policing Act 2008, s 34.

⁸ Oranga Tamariki Act 1989 / Children's and Young People's Well-being Act 1989 (OT Act), ss 214 and 214A.

⁹ OT Act, s 214.

- 13 Once an enforcement officer has arrested a child or young person pursuant to the OT Act, the Agency may collect that child or young person's identifying particulars in accordance with the Policing Act as this compliance notice describes above. Neither the Policing Act nor the OT Act empower the Agency to collect identifying particulars of individuals unless the individual is in custody as provided in Part 3 of the Policing Act.¹⁰ The identifying particulars collected by the Agency in reliance on the Policing Act remain subject to the provision requiring those particulars to be destroyed if a decision is made to not charge the individual or where the outcome of the charges is not one that authorises continued storage.

Privacy Act 2020

- 14 The Privacy Act governs how an agency collects and retains personal information. In the Agency's case, its statutory framework clearly sets out the circumstances and limits it must operate under in collecting and retaining personal information from individuals. The Agency's statutory framework takes into account the role of the Agency and the need to balance that role against the rights and interests of individuals engaging with the Agency.
- 15 To the extent that the Agency may collect and hold information outside its statutory framework, the Privacy Act applies to the Agency and its collection, use and retention of personal information – in particular, IPPs 1, 3, 4 and 9. An agency must collect personal information for a purpose which is clearly linked to a lawful purpose and must collect personal information using means that in all circumstances are lawful, fair and not unreasonably intrusive.¹¹ In addition, where an agency collects sensitive personal information from children or young people, that agency must give particular consideration to its approach in light of the particular vulnerability and more limited agency of those individuals.¹²
- 16 The scope for the Agency to take identifying particulars on a voluntary basis is narrow because there is an express statutory scheme for the taking of identifying particulars in the Policing Act and, in addition, the circumstances in which the Agency takes identifying particulars inhibits the individual's ability to provide informed consent. This is particularly an issue where the individual is a young person, particularly rangatahi, and the voluntary request is made simultaneously with the existing statutory process under the Policing Act for collecting photographs and Biometric Prints.
- 17 The retention of personal information by the Agency, including of identifying particulars pursuant to the Policing Act, engages IPP 9 of the Privacy Act. IPP 9 limits the period for which personal information may be retained and states that:¹³

¹⁰ Powers to require certain identifying details are provided by the Search and Surveillance Act 2012 in certain circumstances such as vehicle stops if a police officer reasonably suspects the person has committed an offence.

¹¹ Privacy Act 2020, s 22 (IPP 4).

¹² Privacy Act 2020, s 22 (IPP 4(b)).

¹³ Privacy Act 2020, s 22 (IPP 9).

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.

- 18 The Agency must be satisfied that personal information it holds may be lawfully used in order to meet its obligations under IPP 9. Accordingly, the purpose for which the Agency has collected the information will inform the length of time for which the Agency can hold and use that information.

Overview of Agency operations and investigation

Police information holding and destruction systems

- 19 The Agency uses a database called the National Intelligence Application (**NIA**) to manage information needed to support operational policing. Most police stations have camera systems and biometric collection forms which are directly linked to NIA and its processing rules (including the requirement to delete the identifying particulars in accordance with section 34 of the Policing Act).
- 20 The fixed camera systems in police station custody suites are set up to ensure that photographs are uploaded into NIA and therefore subject to the automated audit and deletion processes in that database.
- 21 The Agency issues police officers with smartphones for official and personal use. Officers use a mobile application called OnDuty to manually record and submit intel notes, including photographs, directly onto NIA.¹⁴

Investigation of compliance issues

- 22 On 20 January 2021, the Agency admitted that police officers took photos of rangatahi in the Wairarapa region. A police review in August 2020 found that the Agency had taken three photographs, all of rangatahi, in contravention of the Policing Act and OT Act.¹⁵
- 23 On 9 March 2021, OPC and the IPCA announced the terms of reference for the Joint Inquiry. The Joint Inquiry would now focus on the police practice of photographing members of the public in circumstances where individuals are not detained or suspected of committing an offence.
- 24 In the course of the Joint Inquiry, OPC has identified that the Agency may have failed to meet its obligations under IPP 9. I set out my findings as follows.

Casual photographing of rangatahi in public

- 25 As part of the Joint Inquiry, I heard about the general police practice of police officers taking "casual" photographs of individuals in the course of their duties using Agency-

¹⁴ Te Aniwa Hurihanganui "Police using app to photograph innocent youth: 'It's so wrong'" *Radio New Zealand* (online ed, 26 March 2021); "Enabling a game-changing mobile vision." Smudge <www.smudge.com>.

¹⁵ Māni Dunlop "Police launch internal review into policy of taking photos of young people" *Radio New Zealand* (online ed, 20 January 2021).

issued smartphones. After taking a “casual” photograph of an individual, the police officer will often manually load those photographs onto NIA and email a copy of the photograph to themselves from their smartphone. Notably, OPC has seen evidence that police officers have been taking casual photographs of rangatahi who are not engaged in any kind of conduct that would warrant investigation or intervention by the Agency – sometimes by approaching and stopping rangatahi on the street.¹⁶

- 26 OPC has found that the Agency does not have a policy in place which covers the use of smartphones to collect personal information (photographs), nor a comprehensive process for audit and deletion of those photographs. Police officers themselves also do not routinely review and delete the photographs that they collect on their smartphones which are then saved into other locations and databases.
- 27 The Agency does not have a practice or policy in place requiring police officers to delete photographs of people saved on their Agency-issued smartphones once the photographs have been uploaded to NIA. Some of the police officers interviewed by OPC reported retaining thousands of images on their phones. Images retained by police officers include scenes when attending a variety of incidents including vehicular crashes and sudden deaths, along with the officer’s personal photographs.
- 28 OPC has also heard evidence that duplicate photographs are stored in multiple locations by police officers such as on local cellphone storage, cloud storage, computer desktops and other databases which are accessible to employees across the organisation. Therefore, even if an employee deletes a photograph on one device, the same photograph is retained elsewhere in the absence of procedures to ensure comprehensive deletion.

Voluntary Biometric Prints from rangatahi in custody

- 29 OPC has seen evidence that it is common practice within the Agency for police officers to take two sets of Biometric Prints from rangatahi who are taken into custody:

- a **First set (under the Policing Act, subject to automatic destruction)**

The Agency collects a first set of Biometric Prints through a biometric scanning tool called “Live Scan”. Live Scan automatically destroys the Biometric Prints if the Agency withdraws the charges against that person. The Live Scan approach is, as I understand it, consistent with the purposes and mechanisms set out in the Policing Act and enables the Agency to promptly and automatically delete the Biometric Prints in accordance with the requirements in section 34 of the Policing Act and therefore IPP 9.

- b **Second set (voluntary, not subject to automatic destruction)**

¹⁶ OPC has seen evidence of this practice during the Joint Inquiry. I have also seen media coverage of this practice – see for example Hurihanganui, above n 13; and Te Aniwa Hurihanganui and Hamish Cardwell “Questions raised after police officers stop youths to take their photos” *Radio New Zealand* (online ed, 21 December 2020).

Many police officers in stations across Aotearoa also report routinely taking a contemporaneous second and “voluntary” set of the same Biometric Prints using ink on the POL545 and POL545A paper forms. The Agency had retained the Biometric Prints collected in this way far beyond the statutory destruction period set out in the Policing Act.

Police officers that OPC interviewed explained that officers would commonly collect a second set because the Biometric Prints on Live Scan is automatically deleted when the Agency withdraws charges against the person. Charges against rangatahi are commonly withdrawn as the result of rangatahi engagement with Youth Court processes.

The POL545 form states that, if the subject gives the information to the Agency on a voluntary basis, the Agency may use that information “in criminal investigations, to identify [the person] and ... in court as evidence against [the person] at any time in the future”.¹⁷

- 30 Furthermore, OPC has also seen evidence that some police officers had collected a single set of Biometric Prints from rangatahi in custody, again on a voluntary basis in the manner that this compliance notice describes at paragraph 29b above.
- 31 The purpose of collecting Biometric Prints on a voluntary basis (either as a single set or in addition to the set collected in accordance with the Policing Act) is to enable the Agency to retain Biometric Prints for longer than it would otherwise be entitled to under the Policing Act. The Agency considers that the Biometric Prints it collects from rangatahi in custody on a voluntary basis are not subject to the same audit and deletion requirements under the Policing Act, and the Agency retains those Biometric Prints indefinitely.

Photographs of rangatahi in custody

- 32 The genesis of the Joint Inquiry was complaints made by the public about the taking of casual or voluntary photographs of rangatahi in public places. In the course of the Joint Inquiry, however, I had heard that police officers also take photographs of rangatahi at police stations. The Agency has previously stated that if a young person is arrested pursuant to section 214 of the OT Act, the Agency may take the young person's photograph.¹⁸
- 33 The Agency may collect a young person's photograph pursuant to section 32 of the Policing Act if the Agency has detained that person pursuant to section 214 of the OT Act. However, OPC also found evidence that the Agency takes a second set of photographs of rangatahi outside the Policing Act framework, again, on a voluntary basis. The POL545 form (as this compliance notice describes at paragraph 29b above)

¹⁷ New Zealand Police “Voluntary fingerprints and photographs consent form for children and young people (POL545)”.

¹⁸ Dunlop, above n 15.

is a consent form the Agency uses when it takes a second set of photographs of a child or young person on the same voluntary basis.

- 34 OPC has also seen evidence that some police officers had photographed rangatahi in custody solely by relying on the POL545 form – on a voluntary basis outside of the Policing Act framework.

Photographing of adults in custody

- 35 Each police station's custody suite has digital cameras which are linked to NIA. These fixed digital cameras are designed to be used when processing individuals who have been arrested.
- 36 OPC has seen evidence that many police officers bypass the NIA-linked camera systems by using smartphone cameras of individual officers rather than the fixed digital cameras in custody suites. The fixed camera systems are set up to ensure that photographs are automatically upload into NIA and therefore subject to the automated audit and deletion processes in that database.
- 37 By not using the fixed cameras linked to NIA, police officers create multiple copies of the photo across devices (both in cloud storage and in the NIA) without the systematic audit and deletion processes applying to all copies of the photograph.

DESCRIPTION OF IDENTIFIED NONCOMPLIANCE (SECTION 125(1)(b))

- 38 Based on OPC's investigation as part of the Joint Inquiry, I have found that the Agency is failing to comply with IPP 9 in relation to its retention of identifying particulars of individuals (including photographs and Biometric Prints).
- 39 The Agency has failed to comply with IPP 9 (as the case may be) in the following manner:

a Casual photographing of rangatahi in public

I consider that the Agency's practice of photographing rangatahi in the manner that this compliance notice describes at paragraphs 25 to 28 above has directly resulted in the Agency failing to comply with IPP 9. The Agency did not have a lawful purpose for retaining photographs of rangatahi in the circumstances outlined in paragraphs 25 to 28.

Young persons and children, in particular rangatahi, are vulnerable people. I have given due consideration to the inherent power imbalance that exists between police officers and rangatahi, and do not consider it reasonable in the circumstances for the Agency to leverage this relationship to photograph young persons in this way. In the absence of a lawful purpose for retaining such photographs, the Agency should have deleted those photographs under IPP 9.

b Biometric Prints from rangatahi in custody

I consider that the Agency's practice of collecting Biometric Prints on a "voluntary" basis from rangatahi in custody (as this compliance notice describes at paragraphs 29 to 31 above) has resulted in the Agency failing to comply with IPP 9. The Agency's practice of collecting a second set of Biometric Prints on a voluntary basis on paper limits the effectiveness of the destruction of the Live Scan versions and means that the Agency retains Biometric Prints after the statutory retention period expires. I do not consider that the Agency has legal grounds for collecting duplicate sets of Biometric Prints on a voluntary basis outside of the Policing Act and therefore also has no legal grounds for retaining duplicate sets of that those Biometric Prints.

Furthermore, I am concerned about the Agency's practice of collecting a single set of Biometric Prints on a voluntary basis outside the retention and destruction provisions of the Policing Act. It appears that this practice leads to personal information being held by the Agency for longer than is required for the purposes for which the information may lawfully be used.

c Photographs of rangatahi in custody

I consider that the Agency's practice of taking photographs from rangatahi in custody (as this compliance notice describes at paragraphs 32 to 34 above) has resulted in the Agency failing to comply with IPP 9 for the same reasons that this compliance notice sets out at paragraph 39b above.

d Photographing of adults in custody

I consider that the Agency's practice of taking photographs of adults in custody using smartphone cameras (as this compliance notice describes at paragraphs 35 to 37 above) has resulted in the Agency failing to comply with IPP 9. Despite the Agency having camera systems which are designed to automatically delete photographs of adults in custody in accordance with the Policing Act, the Agency's police officers often bypass this process by photographing adults in custody using Agency-issued smartphone devices.

By failing to ensure that it has used the NIA-linked camera systems in a consistent manner, and by failing to have in place a process to ensure that police officers delete smartphone photographs, the Agency has failed to ensure that it will properly delete photographs of adults in custody in accordance with the Policing Act (and therefore meet its obligation under IPP 9).

DECISION

Requirements of section 124(1) prior to making decision

40 Before I issue a compliance notice, I must take into account the factors set out in section 124(1) of the Privacy Act to the extent that they are relevant, and to the extent information about the factors is readily available.

41 My reasoning based on those factors set out in section 124(1) of the Privacy Act is set out as follows:

a whether there is another means under the Privacy Act or another Act for dealing with the noncompliance

OPC has seen media reports and received complaints from individuals with respect to this matter. I am also participating in the Joint Inquiry with the IPCA. In the course of the Joint Inquiry, I have determined that the systemic nature of the Agency's compliance issues in relation to IPP 9 indicate that this compliance notice is the only reasonable means under the Privacy Act to deal with this matter in order to ensure that the Agency promptly addresses this issue.

b the seriousness of the noncompliance

- i OPC has identified that the Agency's processes are a systemic privacy issue across the Agency. I therefore consider that the Agency's noncompliance with IPP 9 to be serious.
- ii When exercising or performing my statutory powers, duties and functions under the Privacy Act, I am required to take account of cultural perspectives on privacy.¹⁹ I have considered the inherent power imbalance between civilians and police officers and have given due consideration to the fact that the Agency's noncompliance has directly affected vulnerable persons such as rangatahi. As a result, I consider that the Agency's noncompliance with IPP 9 is also serious due to such noncompliance likely having a disproportionately detrimental impact on Māori and rangatahi.

c the likelihood of a repeat of the noncompliance

OPC has identified systemic (and therefore ongoing) privacy issues within police practices relating to the taking of casual and voluntary photographs, the systems for taking photographs in custody suites, and the taking of Biometric Prints on a voluntary basis. Therefore, unless the Agency addresses the issues that I have identified in this compliance notice, I consider there is a high likelihood of repeated noncompliance and the risk that further individuals will be affected by the breach.

¹⁹ Privacy Act 2020, s 21(c).

d the number of people who may be or are affected by the noncompliance

I consider that many people may be or are affected by the Agency's noncompliance with the Privacy Act. The Agency itself cannot easily confirm the amount of personal information retained or the number of people affected by the noncompliance. As the result of my investigation into the Agency, I estimate that a significant number people are or may be affected by the Agency's noncompliance with IPP 9.

e whether the Agency has been co-operative in all dealings with OPC

The Agency has been generally co-operative in its dealings with OPC. After having corresponded with OPC, the Agency has indicated its acceptance of its breach of IPP 9. I also understand that the Agency has already taken some steps to address the Agency's noncompliance with the Privacy Act.

f the likely costs to the agency of complying with the notice

I have not quantified the likely costs associated with complying with this notice. I consider that such cost will likely be high and I have taken this into account. On balance, however, I consider it necessary for the Agency to apply appropriate resources in a timely fashion to ensure its compliance with IPP 9.

Decision and reasoning

42 Based on my reasoning above, I have determined that the Agency has failed to comply with IPP 9 of the Privacy Act in the manner set out at paragraphs 38 and 39. In my view, the Agency's continued failure to meet its obligation under IPP 9 is a systemic and ongoing breach of the Privacy Act. Therefore, I have determined that I must issue this compliance notice to the Agency in order for the Agency to rectify its noncompliance with IPP 9 of the Privacy Act.

43 Although I recognise that the Agency has already instigated some work to improve its processes, the systemic nature of the breach means that the Agency will need to adopt a programme of work to ensure that it takes necessary measures to comply with its obligations under IPP 9 on an organisation-wide basis in relation to the retention of photographs and Biometric Prints.

44 I now require the Agency to take the steps and within the timeframes set out in paragraphs 45 to 47 to remedy its noncompliance with IPP 9.

REMEDYING THE BREACH

Steps that the Agency must take to remedy the noncompliance (sections 125(1)(c) and 125(2)(a))

45 The Agency must comply with IPP 9 by ensuring that it has established practices and procedures to delete identifying particulars so that this personal information is not

retained for longer than is required for the purposes for which the information may lawfully be used.

46 I therefore require the Agency to take the following steps to remedy its noncompliance with the Privacy Act:

- a **Delete casual photographs of young persons:** The Agency must:
 - i identify and delete all photographs (and duplicates of such photographs) in the Agency's systems that the Agency has taken in the manner that this compliance notice describes at paragraph 39a above;
 - ii ensure that police officers stop taking casual photographs of rangatahi in public in the manner that this compliance notice describes at paragraph 39a above, to ensure that the Agency does not retain those photographs for longer than is required to meet a lawful purpose; and
 - iii develop and implement a decision-making framework based on objective and lawful criteria which a police officer must follow when deciding whether that police officer can photograph young persons and rangatahi in public, to ensure that the Agency does not retain those photographs for longer than is required to meet a lawful purpose.
- b **Cease collecting Biometric Prints from young persons in custody on a voluntary basis:** The Agency must:
 - i identify and delete all sets of Biometric Prints (and duplicates of such Biometric Prints) in the Agency's systems that the Agency has collected in the manner that this compliance notice describes at paragraph 39b above; and
 - ii ensure that police officers stop collecting Biometric Prints from rangatahi in custody in the manner that this compliance notice describes at paragraph 39b above, to ensure that the Agency does not retain Biometric Prints for longer than is required to meet a lawful purpose.
- c **Cease taking photographs of young persons in custody on a voluntary basis:** The Agency must:
 - i identify and delete all photographs (and duplicates of such photographs) in the Agency's systems that the Agency has collected in the manner that this compliance notice describes at paragraph 39c above; and
 - ii ensure that police officers stop taking photographs of young persons rangatahi in custody in the manner that this compliance notice describes at paragraph 39c above, to ensure that the Agency does not retain those photographs for longer than is required to meet a lawful purpose.

- d **Cease smartphone photography of adults in custody pending procedures and training:** The Agency must:
 - i identify and delete photographs (and duplicates of such photographs) of adults in police custody in the manner that this compliance notice describes at paragraph 39d above; and
 - ii ensure that, until the Agency meets its obligations pursuant to paragraphs 46f and 46g below, police officers stop using devices which are not connected to NIA (including, without limitation, Agency-issued smartphone devices) to take photographs of adults in police custody in the manner that this compliance notice describes at paragraph 39d above, to ensure that the Agency does not retain those photographs for longer than is required to meet a lawful purpose.
- e **Take preventive procedures:** The Agency must develop and implement agency-wide practices and procedures to ensure the practices set out in paragraph 39 above do not continue.
- f **Take deletion procedures:** The Agency must develop and implement agency-wide practices and procedures for the routine and systematic deletion of all identifying particulars, including photographs and Biometric Prints, to ensure that the Agency does not keep any identifying particulars for longer than is required for a lawful purpose.
- g **Undertake training:** The Agency must develop and deliver agency-wide training to its staff and relevant contractors on the practices and procedures that this compliance notice outlines in paragraphs 46aiii, 46e and 46f above.
- h **Undertake audit:** The Agency must develop and implement a system to regularly audit its compliance with its obligation to delete all identifying particulars, including photographs and Biometric Prints, to ensure that the Agency does not keep any identifying particulars for longer than is required for a lawful purpose.
- i **Take all other necessary steps:** The Agency must identify and take all other necessary steps to ensure that its practices set out in paragraph 39 above do not continue.

Timeframes and reporting (section 125(2)(c))

47 The Agency must:

- a remedy its noncompliance with the Privacy Act by:
 - i completing the requirements set out at paragraphs 46aii, 46bii, 46cii and 46dii immediately;

- ii completing the requirements set out at paragraphs 46aiii and 46h on or before 31 December 2022;
 - iii completing the requirements set out at paragraphs 46ai, 46bi, 46ci, 46di, 46e, 46f and 46g on or before 31 December 2023; and
 - iv completing the requirement set out at paragraph 46i as soon as reasonably practicable in each circumstance;
- b provide a two monthly progress report to OPC describing the steps that the Agency has taken to address these matters; and
 - c provide a written report to OPC for each matter set out at paragraph 46 above as soon as reasonably practicable after the Agency has completed that matter (and in any case no later than two months after completing that particular matter).

RIGHT TO APPEAL (SECTION 125(1)(d))

- 48 The Agency has the right to appeal this compliance notice to the Human Rights Review Tribunal under section 131 of the Privacy Act. The Agency may appeal this compliance notice in whole or in part.
- 49 The Human Rights Review Tribunal may allow an appeal for one of the reasons listed in section 131(3) of the Privacy Act. The Agency must lodge an appeal in the Human Rights Review Tribunal within 15 working days from the date of the issue of this notice.

ENFORCEMENT AND PUBLICATION

- 50 If the Agency does not comply with, or appeal, this compliance notice, I may bring proceedings in the Human Rights Review Tribunal to enforce this notice.
- 51 I have the power to publish this compliance notice in accordance with section 129 of the Privacy Act. However, I have determined that I:
- a will not publish the contents of this compliance notice without first giving prior notice to the Agency; but
 - b will publish the existence of this compliance notice in a report on the Joint Inquiry to be published by OPC and the IPCA.

Dated: 22 December 2021

Signed by the Deputy Privacy Commissioner:



Liz MacPherson

APPENDIX 2 – ABOUT

THE INDEPENDENT POLICE CONDUCT AUTHORITY | MANA WHANONGA PIRIHIMANA MOTUHAKE

Who is the Independent Police Conduct Authority?

The Independent Police Conduct Authority is an independent body set up by Parliament to provide civilian oversight of Police conduct.

We are not part of the Police – the law requires us to be fully independent. The Authority is overseen by a Board, which is chaired by Judge Colin Doherty.

Being independent means that the Authority makes its own findings based on the facts and the law. We do not answer to the Police, the Government or anyone else over those findings. In this way, our independence is similar to that of a Court.

The Authority employs highly experienced staff who have worked in a range of law enforcement and related roles in New Zealand and overseas.

What are the Authority's functions?

Under the Independent Police Conduct Authority Act 1988, the Authority receives and may choose to investigate:

- (a) complaints alleging misconduct or neglect of duty by Police;
- (b) complaints about Police practices, policies and procedures affecting the complainant in a personal capacity;
- (c) notifications of incidents in which Police actions have caused or appear to have caused death or serious bodily harm; and
- (d) referrals by Police under a Memorandum of Understanding between the Authority and Police, which covers instances of potential reputational risk to Police (including serious offending by a Police officer or Police actions that may have an element of corruption).

The Authority's investigation may include visiting the scene of the incident, interviewing the officers involved and any witnesses, and reviewing evidence from the Police's investigation.

On completion of an investigation, the Authority must form an opinion about the Police conduct, policy, practice or procedure which was the subject of the complaint. The Authority may make recommendations to the Commissioner.

Who is the Privacy Commissioner?

The Privacy Commissioner has wide ranging functions under the Privacy Act. The Commissioner must have regard to the IPPs in the Privacy Act and the protection of important human rights and social interests that compete with privacy. Competing social interests include the desirability of a free flow of information and the right of government and business to achieve their objectives in an efficient way.

The Commissioner must take account of New Zealand's international obligations and consider any general international guidelines that are relevant to improved protection of individual privacy.

The Privacy Commissioner is an Independent Crown Entity. This means the Commissioner is free from influence by the Executive when investigating complaints, including those against Ministers or their departments. Independence is also important when examining the privacy implications of proposed new laws and information matching programmes.

The Commissioner reports to Parliament through the Minister of Justice and is accountable under the Crown Entities Act 2004.

What are the Commissioner's functions?

As an Independent Crown Entity, the Commissioner is funded by the state but is independent of Government or Ministerial control.

The Commissioner has a wide range of functions, which are listed in section 17 of the Privacy Act .

The Commissioner's key areas of work include:

- making public statements on matters affecting individual privacy;
- investigating complaints about breaches of privacy;
- building and promoting an understanding of the IPPs;
- monitoring and examining the impact that technology has on privacy;
- developing codes of practice for specific industries or sectors;
- examining draft legislation for its possible impact on individual privacy;
- monitoring data matching programmes between government departments;
- inquiring into any matter where it appears that individual privacy may be affected;
- receiving reports of notifiable privacy breaches;
- monitoring and enforcing compliance with the Privacy Act;
- reporting to government on matters affecting privacy, both domestic and international.

ABOUT THIS REPORT

This report is the result of the work of a multi-disciplinary team of investigators, report writers and managers. At significant points in the joint inquiry and in the preparation of the report, the IPCA and Commissioner conducted audits of both process and content.

ACKNOWLEDGEMENT

We would like to thank the Police officers and Police staff members who participated in the inquiry, giving their time, information and insights that contributed to this work.



PO Box 10094, Wellington 6143
Freephone 0800 803 909
www.privacy.org.nz



PO Box 25221, Wellington 6140
Freephone 0800 503 728
www.ipca.govt.nz