office of the privacy commissioner
new south wales

Investigation into NSW Roads and Maritime Services use of an expired protocol for release of photographic images to the NSW Police Force

Agency:	Roads and Maritime Services NSW
Report date:	17 June 2015
IPC reference:	IPC14/OM000001
Keywords:	Protocol, audit, compliance, governance, PPIP Act, recommendations

Contents

Privacy Investigation: Roads and Maritime Services NSW

This is a report of the Privacy Commissioner's investigation into privacy matters related to NSW Roads and Maritime Services (RMS) release of photographs or photographic images to the NSW Police Force (NSWPF) in circumstances where the protocol, approved by the Privacy Commissioner and agreed between the two agencies setting out the limits and controls on release, had expired.

Executive summary

1. RMS collects and stores driver licence photographs for road transport purposes and is prohibited from releasing those photographs except in certain prescribed circumstances. Section 57 of the *Road Transport Act 2013* authorises RMS to release photographs or photographic images to the NSWPF. However, RMS must ensure that the authorised release of photographs or photographic images to NSWPF is done in accordance with any protocol approved by the Privacy Commissioner.
2. A protocol was made by RMS and the NSWPF, and approved by the Privacy Commissioner, to meet the requirements of section 57 the *Road Transport Act 2013*. The protocol commenced on 1 April 2008, for a period of five years, and expired on 31 March 2013. The agencies continued to operate as though the 2008 Protocol had not expired.

   Discussions as to the remaking of the protocol occurred from 2010 typically in the context of addressing issues that arose from implementation of the protocol.
3. On two separate occasions in 2013, follow up occurred with RMS to enquire as to the status of the expired protocol and the need to renew or replace these protocols.
4. Upon receipt of the correspondence, the Privacy Commissioner wrote to the RMS on 5 February 2014 seeking advice on the status of the protocol and if a new protocol was to be renewed or remade.
5. On 26 February 2014, RMS advised that it and NSW Police Force had agreed to a retrospective extension of the expired protocol until 31 December 2014.
6. The Privacy Commissioner received correspondence and subsequently advice from the Crown Solicitor that retrospective extension was not available and would have no legal effect. Consequently, the Privacy Commissioner met with RMS and advised that a retrospective extension was not available and a new protocol would be required and should occur as a matter of priority.
7. The Crown Solicitor also raised the possibility that disclosures of photographic images after expiry of the protocol may have constituted an infraction of the *Privacy and Personal Information Protection Act 1998* (PPIP Act). Consequently, the Privacy Commissioner wrote to RMS and NSW Police Force seeking information to enable an investigation as to whether such a breach had occurred.
8. RMS expedited the renewal of the protocol, and the Privacy Commissioner approved it on 6 June 2014. The new protocol is in force until 5 June 2019. RMS advised that it is taking steps to strengthen its governance arrangements for the 2014 Protocol. The Privacy Commissioner was of the view that the photographs or photographic images released by RMS met the definition of personal information under the PPIP Act and that RMS is a public sector agency for the purposes of the PPIP Act. Accordingly, RMS was obliged to comply with the PPIP Act and the information protection principles when releasing photographs or photographic images to NSWPF at all times, in addition to the requirements of the *Road Transport Act 2013*. This obligation to comply with the PPIP Act exists regardless as to whether an approved protocol under the *Road Transport Act* was in force.

9. Specifically, the information protection principle on disclosure of personal information contained in section 18 of the PPIP Act and which provides that public sector agencies must not disclose personal information held unless:
    - it has a person's consent or if the person was told at the time that it would be disclosed,
    - disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or
    - disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.
10. In this matter, RMS could call upon the exemption that a public sector agency is not required to comply with section 18 of the PPIP Act if the disclosure of the information is for a law enforcement purpose. This exemption is contained in section 23 of the PPIP Act. Relevantly, section 4 of both the 2008 Protocol (expired) and the 2014 Protocol, provides that RMS releases photographs and photographic images to the NSWPF for the purposes of the NSWPF investigating major crimes. Accordingly, RMS relies upon the exemption for a law enforcement purpose.
11. The intent of the approved protocol requirements under the *Road Transport Act* appears to be the establishment of parameters for release so as to minimise unnecessary intrusions on the privacy of RMS customers. The approved protocols extend to both RMS and NSWPF a framework within which the authorised release of photographs or photographic images can occur, with appropriate limits and controls on the release process to ensure compliance with relevant laws, including the PPIP Act.
12. While there was a clear and significant failure by RMS to ensure that a protocol was in force as a sound privacy governance mechanism, no breach of the information protection principles appears to have resulted by way of RMS releasing personal information during the period between its expiry (April 2013) and renewal (June 2014), due to the exemption under section 23 of the PPIP Act.
13. In finalising the investigation, the Privacy Commissioner welcomed the RMS commitment to implement more rigorous governance and better communication to ensure that the 2014 Protocol and subsequent renewals are managed efficiently and effectively:
    - considering governance arrangements for all inter-government MOUs within cluster arrangements
    - establishing regular relationship meetings with NSW Police Force
    - inclusion of the protocol in audit and risk processes.
14. The Privacy Commissioner's recommendations recognise the RMS commitment in this regard and focus on ensuring stronger privacy governance through integration in audit and risk arrangements, consultation with Transport for NSW to improve oversight, continuing to work with NSWPF to improve communication and management, and commencing a review and renewal process in January 2019.
15. The Privacy Commissioner's investigation concluded that while there was a significant lapse in sound privacy governance, there appeared to be no breach by the RMS of the information protection principles under the PPIP Act.
16. A response from RMS to the draft report was received by the Privacy Commissioner on 3 August 2015.
17. The Privacy Commissioner thanks RMS and NSW Police Force for their assistance during the course of this investigation.

Investigation

18. The Privacy Commissioner, in accordance with her function under section 36(2)(l) of the PPIP Act, initiated an investigation into the privacy matters related to the release of photographic images by RMS to the NSWPF in the absence of an approved protocol under the *Road Transport Act*.
19. This investigation concerns the RMS as the agency responsible for releasing the photographic images; however, as NSWPF was a party to the 2008 Protocol (expired), the Privacy Commissioner requested it to provide information to assist the investigation.
20. The investigation was conducted in accordance with section 39 of the PPIP Act, which provides that the Privacy Commissioner may determine the procedures to be followed in exercising her functions under the PIPP Act.
21. On 14 April 2014, the Privacy Commissioner wrote to RMS and to the NSWPF advising of the investigation and requesting information to understand whether and to what extent any breach of information privacy principles under the PPIP Act may have occurred. The information privacy principles are at Appendix A.
22. On 28 April 2014, RMS provided an initial response, followed by provision of a more detailed response on 12 May 2014.
23. On 27 May 2014, NSWPF wrote to the Privacy Commissioner with information detailing its access to photographic images released by RMS.
24. The Privacy Commissioner considered the information provided by RMS and NSWPF to make the findings and conclusions set out in this report.

25. On 17 June 2015, a draft of the report was provided to RMS for their consideration and response. A response to the report was received on 3 August 2015 from RMS. The Privacy Commissioner has considered the response from RMS and this has been incorporated into the final report.

26. This report is made as a public statement of the Privacy Commissioner in accordance with section 36(2)(h) of the PPIP Act.

Application of the PPIP Act – public sector agency, personal information and disclosure

27. RMS is a public sector agency within the definition of section 3 of the PPIP Act.

28. Section 4 of the PPIP Act defines personal information to mean "information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity it apparent or can reasonably be ascertained from the information or opinion.

29. The information that is contained within the image includes the photographic image of the individual and the identity of the individual. The photographic image is the personal information of the individual whose identity is apparent or can be reasonably ascertained and therefore falls within the definition of section 4 of the PPIP Act.[1]

30. Section 18 of the PPIP Act provides limitations on disclosure of personal information. Specifically, it provides:

> *(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:*
>
> *(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or*
>
> *(b) the individual concerned is reasonably likely to have been aware, or has been aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or*
>
> *(c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.*
>
> *(2) If personal information is disclosed in accordance with subsection (1) to a person or a body that is a public sector agency, that agency must not disclose the information for a purpose other than the person for which the information was given to it.*

31. RMS is a public sector agency that holds personal information in the form of photographs and photographic images. The RMS disclosed that personal information to NSWPF. As there is no evidence to suggest that the disclosure was in circumstances contemplated by section 18, it may be in breach of the information protection principle unless a relevant exemption under the PPIP Act applies.

Application of the PPIP Act – exemptions

32. Section 27 of the PPIP Act provides NSWPF with an exemption from complying with the information protection principles, except in connection with the exercise of its administrative and educative function. This exemption is specific to the NSWPF and does not extend to include the RMS.

33. RMS seeks to rely upon the exemption available at section 23 of the PPIP Act. Section 23 (5) of the PPIP Act provides as follows:

> ***Exemptions relating to law enforcement and related matters***
>
> *(5) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 18 if the disclosure of the information concerned:*
>
> *(a) Is made in connection with proceedings for an offence or for law enforcement purposes (including the exercising of functions under or in connection with the Confiscation of Proceeds Crime Act 1989 or the Criminal Assets Recovery Act 1990), or*
>
> *(b) Is to a law enforcement agency (or for such other purpose or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or*

1 The Administrative Decisions Tribunal held that photographs of a person are personal information as defined in s4 of the PPIP Act SW v NSW Forests [2006] NSWADT 74, at 31.

(c) *Is authorised or required by subpoena or by search warrant or other statutory instrument, or*

(d) *Is reasonably necessary:*

(i) *For the protection of the public revenue, or*

(i) *In order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed.*

34. Section 23(5) applies to any public sector agency regardless of whether they are a law enforcement agency, including RMS.

35. The 2008 Protocol (expired) described the purposes to which access to the DRIVES database was to be provided.

36. One purpose was the investigation of a missing person, for which section 23 (5)(b) provides a specific exemption. In this regard any disclosure of photographs or photographic images to NSWPF by RMS that related to the investigation of a missing person would appear to be exempt under section 23(5)(b) of the PPIP Act, and not a breach of the section 18 disclosure information protection principle.

37. A second purpose was the investigation of major crime. In considering whether investigating major crime is a law enforcement purpose within the meaning of section 23(5)(a), guidance is available in the decision of GA v Department of Education and Training and NSW Police (No 3) [2005] NSWADT 70.

38. In that matter, the Tribunal adopted the definition of "law enforcement" as determined by the Tribunal in JD v Director General, NSW Department of Health (No. 2) [2004] NSWADT 227at paragraph 79, which said:

"In my opinion, the term "law enforcement" should be given its ordinary meaning and it should not be narrowly construed...

39. The Tribunal noted at paragraph 73 of the decision in GA, that the test in section 23(5)(a) is directed for the purpose of the disclosure, "The statutory test is not directed to the quality or relevance of the information". Application of the test is a question of fact.

40. The purpose for the disclosure by RMS to NSWPF is clear from the purpose of the 2008 Protocol (expired); to assist with police investigations into major crime. Accordingly, disclosures made for this purpose of law enforcement may be sufficient to attract the section 23(5)(a) exemption to the disclosure of photographs or photographic images to NSWPF by RMS under the 2008 Protocol when it was in force and following its expiry.

The Protocol

41. The protocol for the release of photographs and photographic images by RMS to NSWPF is a requirement of section 57 of the *Road Transport Act*. Section 57 provides that RMS must ensure that a photograph to which the section applies and any photographic image or other matter contained in any database of such photographs is not released except to, amongst others, the NSWPF and that any authorised release must be in accordance with any protocol approved by the Privacy Commissioner.

42. The protocol operates in concert with the PPIP Act to provide an authorising environment.

43. Section 23(5) of the PPIP Act permits the disclosure of "personal information" about an individual for "law enforcement purposes" or for "the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person".

44. A protocol in accordance with section 57 of the *Road Transport Act* was in place between the RMS and NSWPF, and approved by the Privacy Commissioner, from 1 April 2008 until 31 March 2013, at which time the protocol expired.

45. RMS and NSWPF continued to operate as though the 2008 Protocol had not expired, with RMS providing photographic images to NSWPF from its DRIVES database.

46. NSWPF accesses the images from RMS for the purposes of investigating major crimes. Under the 2008 Protocol (expired), investigation " means an investigation of a major crime, or an investigation for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person and referred to the Missing Persons Unit within the OIA".

47. Major crime is then defined at paragraph 1(f) as:

The commission or attempted commission of any one or more of the following offences:

(i) *homicide;*

(ii) *child abuse;*

(iii) *extortion;*

(iv) *kidnapping/abduction;*

(v) *bombings;*

(vi) *money laundering;*

(vii) *arson;*

(viii) *terrorist offences;*

(ix) *serious violent crime;*

(x) *drug trafficking;*

(xi) *complex fraud;*

(xii) *serial armed fraud;*

(xiii) *any other crime or incident which, due to its organisation or other special circumstances, is designated as a "major crime" by the Commissioner or the Commissioner's delegated officer.*

48. RMS expedited the renewal of the protocol, and the Privacy Commissioner approved it on 6 June 2014. The new protocol is in force until 5 June 2019.

Releases following the expiry of the 2008 Protocol

49. RMS advised the Privacy Commissioner, in correspondence dated 12 May 2014, that subsequent to the expiry of the protocol a total of 3,282 images were released to NSW Police Force in the period 1 April 2013 and 31 March 2014.

50. NSWPF advised the Privacy Commissioner, in correspondence dated 27 May 2014, that 3,568 images were accessed.

51. A review of the advice provided identified that the difference in the data reported by RMS and NSWPF arises due to the agencies using different time periods for the data captures. In the case of NSWPF, the data related to a longer period of time, being up to 27 May 2014. In this context it would be reasonable to expect that the numbers reported by NSWPF would be higher.

52. On 17 April 2014, NSWPF suspended access to the images other than in an emergency and only subject to approval from the Commander of the Operational Information Agency, pending the making of a new protocol.

Complaints about releases in the absence of a Protocol

53. RMS advised that no complaints were received by it relating to the release of photographs or photographic images to NSWPF during the period following the expiry of the 2008 Protocol.

54. RMS proposed that should complaints be received, they will be dealt with in accordance with usual RMS complaint procedures. RMS proposed also that a complaint provision would be included in the new protocol to replace the 2008 Protocol. Section 10 of the 2014 Protocol contains privacy complaint provisions.

55. RMS has not and does not intend to inform customers whose images have been released, that release occurred in the absence of a protocol. RMS was of the view that a privacy breach had not occurred and that notification to customers may in fact prejudice police investigations concerning major crimes. RMS was also of the view that because RMS operated from 1 April 2013 according to the process in place in the protocol, customers were afforded the same privacy safeguards as though the protocol was actually in force.

Audit of compliance with the Protocol

56. As required by the 2008 Protocol, NSWPF is responsible for conducting audits for compliance with the protocol.

57. RMS did not undertake any specific audits, inquiries or review of compliance with the 2008 Protocol. RMS indicated that subsequent to the receipt of the NSWPF audit reports, RMS considers action in response to any identified non-compliance with the protocol.

58. It is noted that although section 8 of the expired protocol required that within one month of conducting the audits, the results of the audit were to be communicated in writing to the Privacy Commissioner, this had not occurred in recent years. This represents a failure in fulfilling the responsibilities committed to by the RMS and NSWPF in the making of the protocol.

59. The 2014 Protocol contains similar audit provisions in which it is expected that the RMS (and NSWPF) will ensure safeguards are in place to ensure compliance with the audit requirements during the life of the protocol.

Governance of the Protocol

60. RMS identified that the governance of inter-agency arrangements presented challenges for both large and small organisations. In particular for RMS, the management of the renewal of the 2008 Protocol was affected by significant Transport for NSW and RMS corporate restructures.

    While it is accepted that significant corporate restructures can present challenges for an organisation, this case highlights the importance of ensuring that organisational change management plans detail how system and procedures designed to protect personal information will be maintained through periods of transition.

Privacy Investigation: Roads and Maritime Services NSW

Conclusion

61. Although section 57 of the *Road Transport Act* requires the authorised release of photographs and photographic images to the NSWPF to be in accordance with any protocol approved by the Privacy Commissioner, it does not provide the basis for the lawful disclosure of personal information under the PPIP Act. In other words, operation of the PPIP Act is not conditional upon the existence of the protocol or subject to the operation of the *Road Transport Act*. Rather, the protocol acts to facilitate and provides a governance mechanism to establish parameters for release so as to minimise unnecessary intrusions on the privacy of RMS customers.

62. The failure to review and renew the 2008 Protocol prior to its expiry was a significant lapse in sound privacy governance, however there appears to be no breach by the RMS of the information protection principles under the PPIP Act given the PPIP Act's separate and broader authorising provisions for the disclosure of personal information for law enforcement purposes.

Recommendations

63. This investigation highlighted areas where RMS can improve its privacy governance. A number of suggestions were made to RMS during the course of the investigation and received RMS commitment to implement better governance and communication arrangements to ensure that the 2014 Protocol and subsequent renewals are managed efficiently and effectively. The Privacy Commissioner recognises the RMS commitment and recommends that RMS:

    a. provide this report to its Audit and Risk Committee and any oversight committees of Transport for NSW (TfNSW);

    b. include the section 57 Road Transport Act requirements in the agency's risk management arrangements;

    c. consult with Transport for NSW on establishing regular relationship meetings with NSWPF to provide oversight of agreements, including the 2014 Protocol;

    d. continue working with NSWPF to improve communication and management of the 2014 Protocol; and

    e. commence the review of the 2014 Protocol in January 2019 to ensure the Protocol is renewed by 6 June 2019.

64. In response to the draft report, RMS welcomes the Privacy Commissioner's findings that a breach of the PPIP Act had not occurred however recognises that the unintentional lapsing of the Protocol by not having a mechanism or sufficient oversight in place represented a failure in privacy governance.

    The response by RMS to the recommendations is summarised in the table below:

Recommendation	Action
Provide this report to its Audit and Risk Committee and any oversight committees of Transport for NSW (TfNSW).	Arrangements will be made to brief the RMS' Audit and Risk Committee and its Transport for NSW (TfNSW) counterpart.
Include the section 57 Road Transport Act requirements in the agency's risk management arrangements.	RMS will include in briefing to the Audit and Risk Committee for continued oversight.
Consult with Transport for NSW on establishing regular oversight meetings with NSWPF to provide oversight of agreements, including the 2014 Protocol.	RMS will consult with TfNSW and NSWPF to arrange quarterly meetings.
Continue working with NSWPF to improve communication and management of the 2014 Protocol.	RMS will use the same quarterly meetings as above.
Commence the review of the 2014 Protocol in January 2019 to ensure the Protocol is renewed by 6 June 2019.	RMS scheduled a process to manage renewal of NSWPF Protocol in Customer Liaison and Document Verification Unit management system for January 2019.

65. The Privacy Commissioner welcomes the proposed actions by RMS in response to her recommendations.

Appendix A: Information Protection Principles

The 12 Information Protection Principles (IPPs) under the *Privacy and Personal Information Protection Act 1998* (PPIP Act)

Collection

1. Lawful

An agency must only collect personal information for a lawful purpose. It must be directly related to the agency's function or activities and necessary for that purpose.

2. Direct

An agency must only collect personal information directly from you, unless you have authorised collection from someone else, or if you are under the age of 16 and the information has been provided by a parent or guardian.

3. Open

An agency must inform you that the information is being collected, why it is being collected, and who will be storing and using it. You must also be told how you can access and correct your personal information, if the information is required by law or is voluntary, and any consequences that may apply if you decide not to provide it.

4. Relevant

An agency must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

Storage

5. Secure

An agency must store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

Access and accuracy

6. Transparent

An agency must provide you with details regarding the personal information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

An agency must allow you to access your personal information without excessive delay or expense.

8. Correct

An agency must allow you to update, correct or amend your personal information where necessary.

Use

9. Accurate

An agency must ensure that your personal information is relevant, accurate, up to date and complete before using it.

10. Limited

An agency can only use your personal information for the purpose for which it was collected unless you have given consent, or the use is directly related to a purpose that you would expect, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

11. Restricted

An agency can only disclose your information in limited circumstances if you have consented or if you were told at the time they collected it that they would do so. An agency can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

12. Safeguarded

An agency cannot disclose your sensitive personal information without your consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety. quundit atisimet quiae nust velendelit dolor aut voluptaturit

Itaturerunt odi tore, iusam, cus, uteceperum vel ius dolor sunture perunt, odiorum exerum simus nim labores tiande pa i optibus, eos autes ariae at:

Appendix B: Privacy Protocol – Police Access to Photos: Major Crimes & Missing Persons Investigations

Transport Roads & Maritime Services

NSW GOVERNMENT

Privacy Protocol

NSW Police Force

Police Access to Photos

Major Crime & Missing Persons Investigations

Commencement Date:	6th June, 2014
End Date:	5th June, 2019

[redacted]

Privacy Commissioner

6th June 2014

Date Signed

Table of Contents

Background

A. Section 23(5) of the *Privacy and Personal Information Protection Act 1998* permits the Roads and Maritime Services ("RMS") RMS to disclose "personal information" about an individual for "law enforcement purposes" or "for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person."

B. However, Part 3.5 of the Road Transport Act 2013 imposes additional restrictions in relation to the release of driver licence photographs. In particular, s. 57(2) of the Act requires that the release of driver licence photographs to the New South Wales Police Force ("NSW Police Force") must be in accordance with any protocol approved by the Privacy Commissioner.

C. Part 4 of the Photo Card Act 2005 and Part 6 Subdivision 4 of the Road Transport (General) Regulation 2013 make contain similar provisions concerning photo card and mobility parking photos respectively.

D. The purpose of this Privacy Protocol ("the Protocol") is to establish the parameters for the release by RMS of photographs to the NSW Police Force for the purpose of s. 57(2) of the *Road Transport Act 2013*, s. 19(2) of the *Photo Card Act 2005* and clause 109(2) of the *Road Transport (General) Regulation 2013* so to minimise unnecessary intrusion on the privacy of RMS customers.

Operative provisions

1. Definitions and interpretation

1.1 In the Protocol, unless the context otherwise requires:

(a) "**Commencement Date**" means the date shown on the front page.

(b) "**Commissioner of Police**" means the Commissioner of the NSW Police Force as appointed under the *Police Act 1990*".

(c) "**Commissioner's Delegate**" means the member of the NSW Police Force to whom the Commissioner of Police has delegated the Commissioner's functions for the purposes of this Protocol.

(d) "**Driver licence**" means a licence (including a conditional licence, a provisional licence and a learner licence) issued in accordance with the *Road Transport (Driver Licensing) Regulation 1999* authorising the holder to drive one or more classes of motor vehicle on a road or related area.

(e) "**End Date**" means the date shown on the front page, being five (5) years after the Commencement Date.

(f) "**DRIVES database**" means the database or databases on which RMS holds driver licence, photo card and mobility parking permit photographs.

(g) "**Investigation**" means an investigation of:

- a major crime, or
- an investigation for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person.

(h) "**Major crime**" means the commission or attempted commission of any one or more of the following offences:

(i)	homicide;	(vii)	arson;
(ii)	child abuse;	(viii)	terrorist offences;
(iii)	extortion;	(ix)	violent crime;
(iv)	kidnapping/abduction;	(x)	drug trafficking;
(v)	bombings;	(xi)	complex fraud;
(vi)	money laundering;	(xii)	armed hold-up;

(xiii) any other crime or incident which, due to its organisation or other special circumstances, is designated as a "major crime" by the Commissioner of Police, or the Commissioner's Delegate

(i) "**Mobility Parking Permit**" means a mobility parking scheme authority issued by RMS under clause 97 of the *Road Transport (General) Regulation 2013*

(j) "**Operational Information Agency**" or "**OIA**" means the Operational Information Agency within the Operational Communications and Information Group of the NSW Police Force.

(k) "**photograph**" means any photograph, including a digitised, electronic or computer generated image, issued by RMS in connection with a driver licence, photo card, mobility parking permit and any other matter contained in any database of such photographs.

(l) **"Photo Card"** means a photo card issued by RMS under *Photo Card Act 2005*.

(m) "**Privacy Commissioner**" means the Privacy Commissioner appointed under the *Privacy and Personal Information Protection Act 1998* or his or her delegate.

(n) "**the Protocol**" means this Privacy Protocol, which includes the attachments that are incorporated into this Protocol by reference, as amended from time to time in accordance with the terms of this Protocol.

(o) "**Term**" means the duration of the Protocol (refer clause 2).

1.2 Except where the context otherwise requires:

(a) **Actions by an agency.** Where there occurs a reference to the doing of anything by an agency including giving any notice, consent, direction or waiver, this may be done by any duly authorised officer of the agency.

(b) **Grammatical forms.** Where a word or phrase is given a defined meaning in the Protocol, any other part of speech or other grammatical form in respect of such word or phrase shall unless the context otherwise requires have a corresponding meaning.

(c) **Headings.** The headings and index in the Protocol are for convenience only and do not affect the interpretation of the Protocol.

(d) **Including.** "Including", "for example" and other similar expressions are not words of limitation.

(e) **References to legislation.** A reference to a statute, regulation, ordinance or by-law ("Law") will be deemed to extend to include a reference to all statutes, regulations, ordinances or by-laws amending, consolidating or replacing that Law from time to time.

(f) **Reconstitution of person, agency or part of agency.** A reference to a person, agency or part of an agency which has ceased to exist or has been reconstituted, amalgamated or merged, or other functions of which have become exercisable by any other person or body in its place, shall be taken to refer to the person or body established or constituted in its place by which its said functions have become exercisable.

(g) **Reasonableness.** Where an agency is required to act reasonably in the performance of the Protocol, that shall be read as a requirement to act as would a party in the position of the agency which is acting reasonably in its own best interests.

(h) **References to groups.** A reference to a group of persons is a reference to all of them collectively and to any two or more of them collectively and to each of them individually.

(i) **References to persons.** Persons will be taken to include any natural or legal person.

(j) **Time Limits.** Where any time limit pursuant to the Protocol falls on a non-business day then that time limit shall be deemed to have expired on the next business day.

2. Term, Suspension, Termination & Review

2.1 The Protocol commences on the Commencement Date and will end five (5) years after the Commencement Date (End Date).

2.2 The Privacy Commissioner may suspend the operation of the Protocol for a fixed period in writing.

2.3 The Privacy Commissioner may amend this Protocol at any time including by extending it.

2.4 The Privacy Commissioner may terminate the Protocol in writing at any time.

2.5 The Privacy Commissioner will inform the Chief Executive Officer of RMS and the Commissioner of Police, in writing at least 3 business days in advance of any suspension or termination or amendment of the Protocol.

2.6 At any time the Privacy Commissioner may (whether at the request of RMS or the NSW Police Force or not) undertake a review of this Protocol in order to consider whether this Protocol should be amended, suspended, terminated or extended and RMS and NSW Police Force must provide such assistance and cooperation as the Privacy Commissioner may require.

2.7 No later than 6 month before the 5th anniversary of the Commencement Date RMS, NSW Police Force and the Privacy Commissioner must commence discussions to review this Protocol.

3. Approval of Protocol

3.1 The Protocol is hereby approved by the Privacy Commissioner for the purpose of s. 57(2) of the *Road Transport Act 2013* and s.19(2) of the *Photo Card Act 2005* and clause 109(2) of the *Road Transport (General) Regulation 2013*.

4. Purpose for which release of photographs is permitted

4.1 Photographs must only be released to the NSW Police Force in relation to an Investigation (as defined in clause 1.1) being conducted by the NSW Police Force.

5. Authorisation process for release of photographs

5.1 All requests by the NSW Police Force for release of photographs must be made through officers deployed within the OIA and authorised by the Commissioner of Police, or the Commissioner's Delegate for this purpose ("Requesting Officers").

5.2 Prior to making any request for release of photographs, Requesting Officers must ensure that an officer holding the rank of Inspector or above has approved the making of the

request and make a record that the requisite approval has been obtained together with the name and rank of the approving officer.

6. Mode of access to photographs

6.1 Requesting Officers must request release of photographs on-line via the DRIVES database by use of operator numbers in combination with passwords.

6.2 The DRIVES database must only permit read-only access to photographs by the NSW Police Force, but may permit photographs to be viewed, exported or printed from the DRIVES database.

7. Security of access to and responsibility for photographs

7.1 Requesting Officers must each be assigned unique operator numbers to be used in combination with unique passwords for the purpose of requesting release of photographs on-line via the DRIVES database.

Requesting Officers must not disclose or share their operator numbers or passwords.

7.2 RMS must allocate a reasonable number of operator numbers and passwords to the NSW Police Force for the purpose of facilitating on-line access to the DRIVES database.

7.3 The Commissioner of Police must maintain a current list of Requesting Officers together with details of their unique operator numbers.

7.4 The NSW Police Force is solely responsible for the use, disclosure and storage of photographs viewed, exported or printed from the DRIVES database pursuant to, or in contravention of, the Protocol, including, but not limited to, the export of any information to third parties or use within the NSW Police Force.

8. Audit of access to photographs

8.1 In so far as concerns on-line requests by NSW Police Force for release of photographs, the DRIVES database must have an audit capability that:

(a) Assigns access rights by reference to unique identification numbers and passwords for each user; and

(b) Generates an audit trail of each and every record accessed by reference to the user's unique identification number and password combination, and IP address, including a record of the sequence of records accessed and functions undertaken, and the date and time of every access.

8.2 The NSW Police Force is responsible for conducting audits to ensure that access is in accordance with the Protocol.

8.3 Audits must be conducted as directed in writing by the Privacy Commissioner following consultation with RMS and the NSW Police Force, but no less than once per financial year and for the first two financial years at least twice per financial year.

8.4 Audits must review a reasonable number of audit trails in relation to photographs accessed via the DRIVES database and verify whether the photographs were viewed, exported or printed for the purposes of an "Investigation," whether the request for access was made and obtained by an officer deployed within the OIA who was authorised by the Commissioner of Police or the Commissioner's delegate for this purpose, and whether the requesting officer obtained approval from an officer holding the rank of Inspector or above prior to making the request.

8.5 The NSW Police Force must inform:

- RMS,
- the NSW Police Force Deputy Commissioner, Specialist Operations;
- the Privacy Commissioner; and
- (unless it provides a written waiver) Ministry of Police & Emergency Services ("MPES")

of the results of each audit in writing in the form of an audit report which must be served no later than 30 September each year in respect of annual audits and no later than 30 March in respect of half-yearly reports. The address for service of audit reports is shown in the Schedule. If MPES provides advises that it waives its right to receive audit reports then NSW Police Force must provide a copy of that waiver to the Privacy Commissioner.

In addition, at any time RMS may require NSW Police Force to undertake a special audit in respect of any period or accesses nominated by RMS and to provide an audit report to RMS within such time as RMS (acting reasonably) may nominate and a copy to the Privacy Commissioner.

RMS must provide a copy of each audit report to its "Audit and Risk Committee" and NSW Police Force must provide a copy to its "Commissioner's Executive Team".

RMS's annual report must report on the most recent audit report.

The report must specify:

(a) The size of the random samples used in the audit and that it is considered statistically robust and appropriate to support the conclusions of the audit report;

(b) The number of on-line requests for the release of photographs made by NSW Police Force users during the audit period by reference to the type of Investigation in relation to which access was sought;

(c) Whether, in all cases, release was in relation to an Investigation within the meaning of the Protocol and, if not, details of each case in which it was not, and why not;

(d) Whether, in all cases, release was sought by an officer deployed within the OIA who was authorised by the Commissioner of Police or the Commissioner's delegate for this purpose and, if not, details of each case in which it was not, and why not;

(e) Whether, in all cases, the Requesting Officer obtained approval from an officer holding the rank of Inspector or above prior to making the request and, if not, details of each case in which it was not, and why not;

(f) Whether the NSW Police Force has any evidence that Requesting Officers have disclosed or shared their operator numbers and passwords and, if so, details of the alleged disclosures and action taken in relation thereto;

(g) Whether any complaints were made during the audit period in relation to the access to, use of, or disclosure of photographs, and the results of the investigation of these complaints.

9. Non-Compliance

9.1 If RMS or NSW Police or the Privacy Commissioner is aware of a material non-compliance with the terms of this Protocol (whether its own or not) it must give written notice to the other parties.

9.2 RMS and NSW Police must also report any material non-compliance with the terms of this Protocol to RMS's "Audit & Risk Committee" and NSW Police Force's "Commissioner's Executive Team" respectively.

9.3 When an alleged non-compliance with this Protocol is notified RMS and NSW Police Force must provide such information as may reasonably be required by the other party or the Privacy Commissioner in relation to the alleged non-compliance (including proposed rectification, mitigation and steps to be taken to prevent any re-occurrence).

10. Privacy Complaints in relation to the release of photographs

10.1 Privacy complaints in relation to the release of photographs by RMS to the NSW Police Force may be made to RMS, the Privacy Commissioner or to the NSW Police Force at the discretion of the complainant.

10.2 The address for service of privacy complaints is shown in the Schedule.

10.3 Subject to all privacy obligations, where privacy complaints are made by a third party to RMS, RMS may, where appropriate and at RMS' discretion, request NSW Police Force to assist RMS in the investigation of such complaint. On receipt of such a request, the NSW Police Force must provide all such reasonable assistance to RMS as is appropriate in the

circumstances (having regard to all the facts and circumstances of the privacy complaint) and investigate the complaint and report to RMS within one month.

Where privacy complaints are made by a third party directly to the NSW Police Force, the NSW Police Force must comply with Part 5 of the *Privacy and Personal Information Protection Act 1998* in dealing with the complaint and have regard to all the facts and circumstances of the complaint.

10.4 If the NSW Police Force or RMS becomes aware of any failures of the audit capabilities of the DRIVES database, or any breaches of paragraph 8.1 of the Protocol ("Audit of Access"), it will immediately refer the matter and details to the Privacy Commissioner for any further action deemed appropriate.

10.5 The NSW Police Force must cooperate with the investigation of any privacy complaint by RMS or the Privacy Commissioner.

10.6 When a privacy complaint is received in relation to this Protocol the Privacy Commissioner must be notified and kept informed throughout the complaint handling process.

11. Protocol to operate concurrently with counter terrorism protocol

11.1 The Protocol operates concurrently with the "Protocol for the access, retrieval and release of photographic images held on the DRIVES database for "counter terrorism purposes" which permits release of photographs to the NSW Police Force and to the New South Wales Crime Commission ("the NSW Crime Commission") for the purpose of counter-terrorism investigations.

12. Requests for release of photographs otherwise than in accordance with an approved protocol

12.1 Any requests for the release of photographs otherwise than in accordance with a protocol approved by the Privacy Commissioner must be made pursuant to a search warrant or as provided for by law.

13. Contact Addresses and Service of Notices

13.1 A notice under this Protocol must be in writing and forwarded to the address, email address or facsimile number of that representative as specified in the Schedule or the address last notified to the sender by the intended recipient.

13.2 Business-as-usual correspondence should be addressed as shown in (1) in the Schedule.

13.3 Audit Reports should be served as shown in (1) in the Schedule.

13.4 Privacy Complaints should be served as shown in (2) in the Schedule.

13.5 Legal notices should be served as shown in (3) in the Schedule.

Privacy Investigation: Appendix B

SCHEDULE

(1) Audit Reports and Business as Usual Issues - Address for Service

RMS	NSW Police Force	Privacy Commissioner	MPES
Manager Customer Liaison & Document Verification, Driver & Vehicle Administration Section, Roads and Maritime Services, Level 4, 99 Phillip Street, Parramatta, NSW 2150 Fax 02 8848 8689	Deputy Commissioner Specialist Operations NSW Police Force, Police Executive Office, Level 15 201 Elizabeth Street Sydney, NSW 2000 Ph: 02 8263 6382 Fax: 02 8263 6541	Information and Privacy Commission, GPO Box 7011, Sydney NSW 2001 Email: ipcinfo@ipc.nsw.gov.au Phone: 1800 472 679 Fax: (02) 8114 3756	Chief Executive Officer, Ministry for Police & Emergency Services, Level 13 Bligh House, 426 Bligh St Sydney NSW 2000 Fax 02 9228 3551 Tel 02 9228 5

(2) Privacy Complaints – Address for Service

RMS	NSW Police Force	Privacy Commissioner
Manager Information & Privacy Unit, Roads & Maritime Services, Locked Bag 928, North Sydney 2059 Phone: 02 8588 4990 Fax: 02 8588 4109	Office of the General Counsel, Privacy Co-ordinator, NSW Police Force PO Box 1678, Woolloomooloo NSW 1335 Phone: (02) 9506 5199	Information and Privacy Commission GPO Box 7011, Sydney NSW 2001 Email: ipcinfo@ipc.nsw.gov.au Phone: 1800 472 679 Fax: (02) 8114 37

(3) Legal Notices - Address for Service

RMS	NSW Police Force	Privacy Commissioner
The Chief Executive Roads & Maritime Services 101 Miller Street North Sydney 2060 Fax: 8588 5991 **Copy to:** Senior Manager Driver & Vehicle Administration, Roads & Maritime Services, Locked Bag 14 Grafton NSW 2460 Tel: 02 6640 2803 Fax: 02 6640 2898	Office of the General Counsel, Privacy Co-ordinator, NSW Police Force PO Box 1678, WOOLLOOMOOLOO NSW 1335 Phone: (02) 9506 5199	Information and Privacy Commission GPO Box 7011, Sydney NSW 2001 Email: ipcinfo@ipc.nsw.gov.au Phone: 1800 472 679 Fax: (02) 8114 3756

Information and Privacy Commission NSW

Level 11, 1 Castlereagh Street, Sydney 2000

GPO Box 7011, Sydney NSW 2001

1800 IPC NSW (1800 472 679)

Fax: (02) 8114 3756

ipcinfo@ipc.nsw.gov.au

www.ipc.nsw.gov.au

Our business hours are 9am to 5pm
Monday to Friday (excluding public holidays)