we asked

Expert Panel on Emergent Technology – ANPR Policy

In December 2021 Police sought advice from the Expert Panel on Emergent Technology on the refreshed Automatic Number Plate Recognition (ANPR) policy as the current ANPR policy is required to be updated to ensure the appropriate use of ANPR.

Additions have been made to encompass current business needs for operational delivery, staff safety considerations and to reflect the differing processes between Police and third-party Number Plate Information (NPI) providers AUROR and SaferCities.

The Expert Panel were asked to consider the draft *Automatic Number Plate Recognition Technology Policy* and provide advice that would assist Police in ensuring the policy provides clear guidance on the safe and appropriate use of ANPR.

Any general points of feedback were welcome, and Police were particularly interested in the Panel's advice on whether the Policy provides a comprehensive explanation and a robust means of embedding good practice.

Police's intent is to introduce the revised ANPR policy to ensure use of ANPR is guided correctly; provides greater clarity, guidance and assurance of operational use; and clearly identifies the required approvals, controls and auditing to ensure use is appropriate.

The Panel were also provided the opportunity to offer general observations on additional or alternative considerations that ought to inform judgments about the risks posed using ANPR.

they said

EPET 21.5 Automatic Number Plate Recognition Policy (ANPR)

1. The Panel has been asked to provide advice on the proposed new ANPR Policy.

2. Prior to preparing this advice, the Panel sought further clarity from the Police about several aspects of the Policy. Reponses to these were received between 25 January and 22 February. We thank the Police for these responses, which have informed our advice.

3. The Panel generally regards the Policy as helpful. It is less operationally focused than the current policy, with a greater emphasis on matters such as governance and justification of use, and storage and retention of information. In response to our question about content contained in the current policy but absent in the new policy, the Panel was informed that practical guidance contained in the current policy will be moved to the "Patrol Techniques" chapter, which will be updated to include this aspect, and that a link to this effect will be added to the new Policy. This seems like a logical organization of information.

4. The Panel has queried the rationale behind the maximum 12-month retention period. In particular, we raised doubts whether it will be long enough for the investigation of some crimes. We have been informed that the rationale is based partly on the practice of third party NPI providers, and partly on current limitations to storage capacity and control over access, and that this could potentially be revisited were a solution to become available. Insofar as storage solution cannot presently be identified that would guarantee controlled access, the Panel endorses the conservative approach limiting storage to 12 months but with a caveat that some form of compressed file storage might be a short term solution.

5. Pages 6 and 8 have tables setting out procedures for accessing data held respectively by Police and third parties. The Policy states that "Storage, access and review of such information may generally be considered to be an intrusion of privacy and can only be justified if the law enforcement purpose for conducting this analysis outweighs the right to privacy." The Panel endorses the Police intention to maintain high standards of privacy in respect of ANPR data. However, we are less sure about the link between "Period elapsed since offence occurred", "Offence Seriousness" and "Level of authorization Required". For example, it is not obvious to us why, after 6 months, access is available only for offences punishable by 10 years imprisonment or more. The Panel recommends that Police give further consideration to the access criteria.

6. The final level in the charts sets out the position where "there is a need to prevent or lessen a serious threat to someone's life or a serious threat to public health or public safety." In these circumstances, access to all available records is permitted. The Panel wonders whether explanation of "serious threat" may be beneficial. Is the main distinction between this and the preceding class (offences punishable by ten years or more) that the threat is still current/imminent? Otherwise, could anyone suspected of committing a serious offence within the past 12 months be said to constitute a serious threat to public safety? The Panel recommends that further explanation of "serious threat" be added to the Policy.

7. Assuming that there is a good reason to limit access by offence seriousness (see Paragraph 5), the Panel wonders how Offence Seriousness will be determined. The guidance and examples section on page 12 sets out an example wherein “A person pushes an elderly lady over and steals her handbag.” The paragraph then states that “Due to the offence penalty being 7 years imprisonment, a Senior Sergeant can also approve access…” It is not specified what offence has been committed here, but we note that one possibility – robbery – carries a maximum sentence of ten years (Crimes Act, s 234). According to the charts on pages 6 and 8, this would require written approval by Inspector or above. The more serious charge would also have implications for the time period from offence. The Panel recommends that the appropriate approval level should correspond to the most serious charge that could plausibly arise from what is known of the offending.

8. Later on the same page, a paragraph begins with the acronym CHIS. We understand that this stands for Covert Human Intelligence Sources, and while this may also be widely understood by officers consulting the policy, wonder whether it may be better to set this out in full.

9. The Panel recommends that the Policy contains a clearer statement that use of the ANPR tool is only permitted when the terms of the Policy are complied with, including relevant permissions, and that misuse of the tool could result in an employment investigation and potential disciplinary consequences. In response to a query about auditing, retention and access to NPI data, the Panel has been informed that this now falls under DCE Insights and Deployment and has been delegated to Manager Emergent Technology. This seems appropriate. However, the Panel also recommends that Police consider ensuring that the auditing process should specifically monitor any adverse consequences of the current technical storage limitations, and the way that access is defined by offence type and length of time since offence. In the interests of transparency, the Police should also consider making the results of this monitoring publicly available.

10. The Privacy Act 2020 provides Police with broad exceptions to Information Privacy Principles (IPPs) 10 and 11 concerning the use, and disclosure, of personal information respectively. However, the Policy would benefit from clearer articulation of these exceptions. For example, on page 7 it states that "There is no expectation of privacy in respect of stolen vehicles." There doesn't need to be an expectation of privacy for the Privacy Act to apply. The relevant exception to IPP 11, which governs the disclosure of personal information, is a belief, on reasonable grounds, on the part of Police, that the disclosure of the personal information (VOI) is necessary to avoid prejudice to the maintenance of the law or the prevention, detection, investigation, prosecution, and punishment of offences.

Likewise, on page 9, it states "care needs to be taken that individuals' privacy is not compromised." Arguably, an individual's privacy is compromised when their personal information is disclosed however, the issue is that it is disclosed lawfully. It would read better as "care should be taken to ensure all personal information is used and/or disclosed in accordance with the Privacy Act 2020."

we did

The Expert Panel's advice was provided to the Police subject matter experts on Automatic Number Plate Recognition (ANPR) including Legal Section, Privacy Advisor, and the Emergent Technology Group for consideration.

Additional changes were made to the draft policy including making the useful distinction of separation of operational guidance and policy, clarification of the definition of 'serious threat', including an additional paragraph containing a clearer statement when ANPR is permitted to be used in compliance with the policy, and reflecting in the policy the clear alignment with the limits of use and disclosure of personal information under Information Privacy Principles 10 and 11 of the Privacy Act 2020.

The revised draft was reviewed by further external stakeholders and had been published on the Police web page https://www.police.govt.nz/about-us/publication/automatic-number-plate-recognition-police-manual-chapter-0