

9 December 2022

Phil Pennington  
[Phil.Pennington@rnz.co.nz](mailto:Phil.Pennington@rnz.co.nz)

Dear Phil

***Request for Information***

Thank you for your Official Information Act 1982 (OIA) request dated 30 September 2022, in which you asked for information regarding Police's Automatic Number Plate Recognition (ANPR) systems and privacy assessments.

My response to each of your questions can be found below.

*Pls release in full and in fully searchable format, regarding any and each of the ANPR camera networks systems police access, including SaferCities and also Auror;*

***1. Privacy impact assessments or similar (if there are multiple, then all)***

Police completed a Privacy Impact Assessment (PIA) in August 2017 for a project concerning the collection of information from private ANPR platforms. The full document is withheld under section 9(2)(g)(i) of the OIA, to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any public service agency or organisation in the course of their duty. The executive summary of this PIA can be provided, and you will find a copy enclosed. Of note, this document was prepared in 2017. Since then, clear policy and processes have been put in place regarding the use of technology by NZ Police, including the use of ANPR. Please note some information from this document has been withheld under section 9(2)(g)(i) of the OIA.

Auror and SaferCities have carried out their own PIAs to satisfy their obligations under the Privacy Act (2020) by identifying and mitigating any of the potential risks arising from the collection, use, or handling of personal information. Police sought an understanding from these companies as to their treatment of any potential privacy risks, for which they provided Police with their PIAs.

Information regarding any risks to the platforms that Police use is critical to their safe operation. Information on any risks provided by these companies must therefore be subject to an ongoing obligation of confidence to ensure that information will continue to be proactively provided to Police. Releasing this information could also prejudice their respective commercial positions. The companies' PIAs are therefore withheld with reliance on sections 9(2)(ba) and 9(2)(b(ii)) of the OIA.

**Police National Headquarters**

180 Molesworth Street. PO Box 3017, Wellington 6140, New Zealand.  
Telephone: 04 474 9499. 04 498 7400. [www.police.govt.nz](http://www.police.govt.nz)

2. *Any report, doc, response or similar arising directly from any and each of these PIAs*

There are no reports or documents arising directly from any PIA. Police consulted with the OPC on the proposed trial of additional functionalities within the Auror platform. OPC provided its response via email on 2 August 2021. The feedback from the OPC on Police's ANPR policies has been considered and where appropriate incorporated into the updated policy.

The full email is withheld in full under section 9(2)(g)(i) of the OIA, to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any public service agency or organisation in the course of their duty.

3. *The latest two of any separate risk assessments.*


Security Risk Assessments are maintained for services provided by Auror and SaferCities. These documents are withheld in full under section 9(2)(b)(ii) of the OIA in that the making available of this information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information, and section 9(2)(ba) of the OIA to protect information which is subject to an obligation of confidence.

You have the right to ask the Ombudsman to review my decision if you are not satisfied with the response to your request. Information about how to make a complaint is available at: [www.ombudsman.parliament.nz](http://www.ombudsman.parliament.nz).

Yours sincerely



Carla Gilmore  
Manager Emergent Technology



## **Automatic Number Plate Recognition – Privacy Impact Assessment**

Abstract: A review of the Counties Manukau Project to acquire and use Number Plate Information (NPI) from private Automatic Number Plate Recognition (ANPR) platforms

## 2.0 Executive summary

---

### 2.1 – The Project

The Project is an endeavour by the Counties Manukau District to acquire data about motor vehicles from existing privately operated (non-police) CCTV systems using ANPR software. The NPI data will be stored and available in a database known as the Vehicle Identification Broadcast Engine (VIBE), supplied by SecuroGroup, a private software company.

There is a growing use of ANPR private operators. ANPR software has become more affordable and effective. Groups of retailers, owners of large car parking complexes and local authorities are all tapping into the security benefits of the tool. Government entities such as NZTA are exploring the possibility of using ANPR for roading use intelligence. Figures on how many ANPR platforms there might be New Zealand wide are not available. Auckland Police continue to be approached by Community Partners wanting to provide NPI to Police. It is a safe assumption that if this project were to become a nationally owned crime tool in the future, the potential number ANPR sites connected to Police could be significant.

Recent information suggested that in the Northland region there are 3 Northland towns keen to supply NPI data, their contribution arising from up to 700 cameras. It is a safe assumption that nationally the potential ANPR platforms number in the many 1000s.

ANPR ought to be viewed as a forerunner to the wider use of other CCTV platform options such as 'facial recognition'. Already another Police district is contemplating the opportunity provided by retailers who have deployed 'facial recognition' software.

The United Kingdom experience, which is significantly saturated, is a useful case study on appropriate/inappropriate use of NPI. Unlike the VIBE project at hand, the UK Government/Police Forces actively funded the installation of thousands of new ANPR cameras. It now owns and operate over 8000 CCTV/ANPR platforms and acquires 10s of millions of lines of data on a daily basis<sup>6</sup>. Their journey to acceptable use of NPI included a significant public furore, new legislation governing the use of CCTV, the appointment of a Surveillance Camera Commissioner and the creation of a Home Office National ANPR Data Centre. In addition the legislation created a Surveillance Camera Code of Conduct. By all accounts this was a substantial and lengthy process.

There will be much to learn from the UK Police experience and tapping into that experience would be valuable to NZ Police, to assist with the responsible uptake and use of NPI.

In addition to the UK experience, cognisance of the current social climate in New Zealand is important. Section 9(2)(g)(i)

The public debate has drawn in concerns about the security and use of data in the Integrated Data Infrastructure (IDI) administered by Statistics NZ. The public perception is that the State sector is not a trusted steward of citizen's sensitive data.

Without a strong corporate strategy around VIBE, Police acquisition of private NPI data could be characterised as 'mass surveillance' or 'big brother' behaviour. Careful thought and assurance needs be given to the introduction of how the Project is managed, deployed and operated. There is good potential for positive exposure and community benefit from this project. Section 9(2)(g)(i)

Current features of concern with the project include;

### 2.2 Collection of NPI

There is a need for a defensible and thoughtful *purpose* for collecting NPI. That purpose ought to be supported by research about the utility, necessity and proportionality of using NPI for crime detection. In addition it is desirable that the Project is publicly introduced in a transparent manner by briefing the Minister of Police and the Privacy Commissioner.

---

<sup>6</sup> Professional Police Magazine: Future of ANPR, p16 1/12/2016

### *2.3 Security*

Security in a project involving technology and personal information has to be wider than just database and technical security. The considerations around guidance and policy, and physical access to the system and structural security must be connected and complimentary. Being able to determine access and behaviour within the system by any individual is important.

The Project also involves 3<sup>rd</sup> parties who engage with Police in various ways. SecuroGroup and the Fusion Data Centre both supply the technical capability for Police to hold, store and use NPI. They are agents of Police who should operate at a secure and responsible level commensurate with Police's own expectations of itself.

This concept also extends to those parties who are happy to supply NPI from their systems for Police use. They will be seen by the public as acting in tandem or as agents of Police. They will all be using the same NPI data to which Police has access. Having common expectations of this cohort of 3<sup>rd</sup> parties about their level of security around their systems, their uses of the data and their audit capacity are matters that Police should be assessing, before receiving data from them.

### *2.4 Use of personal information*

How NPI will be used and for what is unclear. Linked to the overall purpose of why Police will acquire NPI, clarity around the rules and limits on the use of it are crucial to the integrity of the Project. The thinking about use in general ought to consider the need for limits on disclosure as well.

### *2.5 Retention of Personal Information*

The Project's current thinking about retention periods for NPI data is arbitrary at best. If NPI was to be used simply to detect stolen vehicles in real time, very short periods of retention would be expected. By extending the purpose and use of NPI to include detection of crime, longer periods of retention are potentially defensible. More thought is required about the rationale for stated retention periods.

### *2.6 Governance and Assurance*

In light of the Project potentially becoming a national application, adequate governance and robust assurance are prerequisites for the integrity of the practice. A high level governance group working in tandem with a knowledgeable working group, and a robust '3 lines of defence' model of assurance, perhaps with a 3<sup>rd</sup> line of defence that includes some external independent oversight are very important attributes for the Project. The governance and assurance should be managed from a central executive perspective.

## Recommendations

Collection of NPI	<p><b>Formulate</b> a defensible ‘purpose’ for collecting ANPR</p> <p><b>Conduct</b> research that demonstrates the utility and public benefit of Police use of ANPR for stolen vehicles and crime in general</p> <p><b>Formulate</b> a process for checking on the transparency of 3<sup>rd</sup> party providers on NPI</p> <p><b>Consider</b> political briefings before the Project becomes a national venture</p> <p><b>Consult</b> with the Privacy Commissioner when the Project goals are known, defined and accepted</p>
Security	<p><b>Create</b> clear rules and process about access to NPI in VIBE</p> <p><b>Create</b> a contractual relationship with SecuroGroup/Fusion that includes security requirements for VIBE</p> <p><b>Manage</b> the relationships with 3<sup>rd</sup> party providers of NPI by establishing clear Police expectations of practices in collecting and managing personal information</p>
Use of personal information	<p><b>Establish</b> rules and guidance about how NPI can be used by Police including the limits of use</p>
Retention of personal information	<p><b>Establish</b> retention periods that are commensurate with the various uses or purposes for which NPI will be of value to Police</p>
Governance and Assurance	<p><b>Introduce</b> responsibility for ongoing oversight of the Project to a National Police governance group</p> <p><b>Introduce</b> a robust assurance reporting model that includes consideration of a truly independent 3<sup>rd</sup> line of defence</p>