

New Zealand Police

Privacy Impact Assessment

Police use of third party ANPR information

17 April 2023

Frith Tweedie & Mike Flahive
Simply Privacy Ltd

Table of contents

1.	Executive Summary	3
2.	About this PIA.....	6
2.1	Scope	6
2.2	Methodology	7
2.3	How this PIA is structured	7
2.4	About us.....	7
3.	Regulatory environment	8
3.1	Privacy Act.....	8
3.2	Data Protection and Use Policy	8
3.3	Privacy by Design	8
3.4	Fair and ethical use of data, analytics and algorithms	9
4.	Background and context	10
5.	Summary of application of IPPs	16
6.	Privacy risk & opportunity assessment.....	18
6.1	Police collection practices	18
6.2	Information sharing.....	21
6.3	Governance, accountability and assurance	24
6.4	Accuracy and reliability of data	29
6.5	Data retention	33
Appendix 1: Glossary		36
Appendix 2: Information gathering		38
Appendix 3: Summary of IPPs		39
Appendix 4: DPUP principles.....		40
Appendix 5: Privacy by Design principles		41
Appendix 6: Algorithm Charter commitments		42

Version	Date	Author	Comments
0.1	23 March 2023	Frith Tweedie & Mike Flahive	First draft for consultation
0.2	11 April 2023	Frith Tweedie	Amended draft
0.3	17 April 2023	Frith Tweedie	Final

1. Executive Summary

This is an independent PIA on the privacy implications of Police use of data collected by Automatic Number Plate Recognition (**ANPR**) cameras owned and operated by a range of organisations such as service stations, retailers, regional councils and public infrastructure owners (**Organisations**). That information may include number plate information, still images, video footage of a vehicle and its occupants, metadata and vehicle make, model and colour (**ANPR data**), which is stored in technology platforms (**Platforms**) owned by Auror Limited (**Auror**) and SaferCities Group Limited (**SaferCities**) (the **Platform Providers**).

ANPR data is “information about an identifiable person” and is therefore personal information subject to the Privacy Act 2020.

This PIA report identifies the high-level privacy risks requiring consideration in this context, applying a risk and principles-based approach to recommendations designed to address those risks.

A defining feature of the Platforms is the way they automate pre-existing processes for Police access to ANPR data, enabling the Police to readily access that data on request or by statutory demand. While this ease of use and access provides numerous benefits to Organisations, the Police and ultimately the communities they serve, it also introduces opportunities for potential misuse.

Key risks include a lack of transparency around Police use of this information, potential improper use of the Platforms and the data on them leading to privacy and other harms, inaccurate data leading to possible misidentifications and perceptions of profiling and surveillance.

While Police have established robust ANPR rules, guidance and policies to encourage appropriate use of the Platforms by Police users, those documents on their own will not remove the potential for misuse. Supporting governance, processes, controls and training are required to ensure legal and policy requirements are satisfied.

In particular, there need to be ways to ensure Police personnel use the Platforms lawfully and appropriately, that any scope for misuse is limited as much as possible and that should misuse in fact occur, it is promptly identified and addressed. That includes implementing effective and proactive processes and controls that identify and prevent inappropriate behaviour *before* access occurs, as well as post-event audits. Doing so will provide assurance that the Platforms are not being misused and will help demonstrate to the public they can have trust and confidence in the Police’s stewardship of their information.

Summary of recommendations

The following recommendations are grouped thematically and presented in summarised form. We encourage you to read each relevant section and associated recommendation in full to understand the context in which each recommendation is made. Please see the **Glossary** in Appendix 1 for explanations of the defined terms used below and throughout this document.

#	Theme	Issue	Recommendation	PIA section
Rec-001	Police collection practices	Purpose, necessity and proportionality	Ensure Police governance, policy, procedures and controls only permit the collection of ANPR data through the Platforms for the purposes stated in the ANPR policy and in ways that are necessary and proportionate to the benefits so as to minimise the risks of unnecessary collection of personal information, particularly where “active detection capability” (ADC) is involved.	6.1.2
Rec-002		Transparency	Implement a transparency strategy to highlight Police engagement with the Platforms, including making the public aware their personal information may be collected by Police via third-party ANPR systems and the reasons for that collection.	6.1.3
Rec-003		Voluntary disclosure requests	Ensure Police requests for the voluntary disclosure of ANPR data by Organisations through the Platforms facilitate and satisfy Organisations’ expectations and obligations for the disclosure of such information.	6.2.1
Rec-004, Rec-009, Rec-010, Rec-011	Governance, accountability & assurance	ANPR policy and process	Update the Police ANPR policy and Standard Operating Procedures (SOPs) to: <ul style="list-style-type: none"> ensure the rules and guidelines for Police collection and use of ANPR data on the Platforms are presented in a clear, consistent and concise way that facilitates easy comprehension and implementation by Police staff; 	6.3.1 6.4.1 6.4.2 6.5

			<ul style="list-style-type: none"> require Police users to double check Platform-sourced data before it is relied upon, including drawing attention to the risks associated with “automation bias”; include explicit rules and requirements around the use and expiry of ADC alerts in the Platforms, similar to those currently in place for Police-owned ANPR systems; reflect for how long Police users can access ANPR data in the Platforms, both for where a vehicle is – and is not- considered to be a vehicle of interest for Police purposes. 	
Rec-005		Monitoring and auditing	Ensure both Police systems and the Platforms effectively log access to ANPR data in the Platforms and that regular audits are conducted to understand how the Platforms are being used by Police.	6.3.2
Rec-006		Controls to minimise misuse	Implement manual and/or technical controls to reduce the risk of misuse of the Platforms by Police users <i>before</i> it happens, including enabling real-time monitoring and validation of Police information entered in the Platforms.	6.3.3
Rec-007, Rec-008, Rec-010		Engagement with Platform Providers	Continue to engage with the Platform Providers to explore:	6.3.3
		Accuracy	<ul style="list-style-type: none"> what user interface changes could be made to the Platforms to require Police users to always enter valid information; the incorporation of reminders and “nudges” in Platform user interfaces to encourage Police users to input the correct information; and how appropriate controls could be implemented in the Platforms to ensure ADC alerts always align with the relevant Tracking Authorisations. 	6.3.4 6.4.2
Rec-008		Guidance & Training	Support Police staff to use the Platforms lawfully and appropriately through adequate training, awareness raising exercises and Platform nudges and reminders.	6.3.4
Rec-011		Data retention	Establish a clear position on how long Police can access ANPR data on the Platforms to encourage Platform Providers (and Organisations) not to retain personal information for longer than is needed for Police purposes, noting IPP 9 compliance in the context of ANPR data on the Platforms is the responsibility of the Organisations.	6.5

2. About this PIA

A Privacy Impact Assessment (PIA) is a critical tool to help agencies identify and evaluate the potential privacy impacts of a project, process or change. PIAs give agencies a better understanding of their privacy risks and how best to manage them to help deliver the desired benefits in a way that protects individual privacy.

This report considers the privacy impacts associated with Police collection and use of ANPR data collected by Organisations and stored in the Platforms. We note the Police previously conducted a PIA in 2017 with a more limited scope focused on a Police district-based trial of one of the Platforms.

This PIA should be viewed as a living document that is revisited when material changes are made to Police interaction with the Platforms and the data on them. It could also form the basis for regular assurance reporting to review and determine that identified risks are appropriately managed and controls remain effective. It is a baseline risk document for an appropriate governance group to regularly measure current deployment and practice and maintain confidence that the Police continues to use the Platforms appropriately.

2.1 Scope

In scope	Out of scope
<ul style="list-style-type: none">- Police use of the Platforms to access and collect ANPR data.- Consideration of the above in the context of the Privacy Act 2020 and the broader regulatory environment as at the date of this PIA.	<ul style="list-style-type: none">- ANPR data generated from ANPR cameras owned and operated by the Police or other government agencies not provided to the Platforms.- Personal information collection practices and/or privacy obligations of Organisations or the Platform Providers.- Technical security risks associated with the Platforms or Police systems. While this PIA may identify high-level security risks, it is not a security assessment.- Consideration of whether a "search" has been conducted under the New Zealand Bill of Rights Act 1990 or Police obligations under the Search and Surveillance Act 2012.

This assessment is not legal advice, and its contents should not be taken as legal advice.

In preparing this assessment, Simply Privacy has relied upon information, statements and representations provided to it by or on behalf of the Police. Simply Privacy provides no warranty

of completeness, accuracy or reliability in relation to such information, statements or representations.

This PIA should not be read as providing any endorsement or criticism of either of the Platforms.

2.2 Methodology

We reviewed key Police ANPR policy and operational documentation and interviewed relevant Police staff about their policy, guidance and current use of the Platforms.

A full list of the stakeholders interviewed and the documents reviewed is set out in Appendix 2.

2.3 How this PIA is structured

The PIA contains the following four key sections.

Regulatory environment	Outlines the relevant regulatory and policy contexts within which this PIA is prepared, including the Privacy Act 2020.
Background and context	Outlines Simply Privacy's understanding of how the Platforms operate and are used by the Police.
Summary of application of IPPs	Summarises the application of the Information Privacy Principles (IPPs) to Police use of the Platforms, with a view to identifying areas of risk and opportunity that should be given more detailed consideration.
Privacy risk and opportunity assessment	Assesses the key privacy risks and opportunities identified in relation to Police use of the Platforms and ANPR data.

Our recommendations are highlighted in yellow throughout this PIA and summarised in the Executive Summary.

2.4 About us

Simply Privacy is one of New Zealand's leading privacy consultancies. We provide privacy strategy, risk analysis and consultancy services to public and private sector agencies in New Zealand and around the world. Simply Privacy's principals are experts in their field, having previously held senior privacy roles in-house, with the Office of the Privacy Commissioner and in large legal and consulting firms. Simply Privacy has provided strategic, maturity, risk assessment, advisory and other privacy services to numerous government agencies.

3. Regulatory environment

This section looks at the legislation, policies and principles that provide legal and best practice guidance on the issues to be considered when using platforms and systems that collect, store and share personal information.

The following forms of regulation complement each other and have guided this assessment and our analysis of Police collection of ANPR data from the Platforms. This PIA takes a risk-based approach, consistent with the general principles of Privacy by Design (discussed below). It does not look for outcomes that protect privacy at the total expense of other risks but aims to recognise that privacy is one of many considerations faced by the Police.

3.1 Privacy Act

A PIA reviews a project through the lens of the Information Privacy Principles (**IPPs**) in the Privacy Act 2020 (the **Privacy Act**). The IPPs govern how agencies may collect, store, provide access to, use and disclose personal information.

The IPPs (summarised in Appendix 3) are designed to ensure that agencies such as the Police can use personal information to achieve their lawful purposes efficiently and effectively, while protecting the privacy rights of the individuals the information is about. They provide agencies with a flexible roadmap for managing the personal information lifecycle, from collection through to destruction.

Privacy is not an absolute right. The application of the IPPs is subject to any other law that specifically regulates when and how personal information may be collected, made available, used or disclosed. This includes Police powers under the Search and Surveillance Act 2012 (**Search and Surveillance Act**).

3.2 Data Protection and Use Policy

The New Zealand Government has developed a Data Protection and Use Policy (**DPUP**) that describes what “doing the right thing” looks like when government agencies collect or use personal information. Though not mandatory, agencies are encouraged to adopt DPUP in a way that makes sense for their work and their communities. Police performance against the DPUP is self-assessed and then reviewed annually by the Government Chief Privacy Officer.

The DPUP complements the requirements in the Privacy Act by providing a shared set of rules for the respectful, trusted and transparent use of personal information. It also recommends certain practices that go beyond the law – for example, by including a focus on groups and communities as well as individuals. The five key principles of the DPUP are set out in Appendix 4.

3.3 Privacy by Design

The Privacy Act and the IPPs are complemented by the seven principles of Privacy by Design (**PbD**), a well-established methodology to ensure that privacy is managed effectively within project processes and procedures. The PbD principles are set out in Appendix 5.

By embedding privacy from the beginning of a project, the PbD approach enables a proactive approach to privacy management. It also ensures a more meaningful risk management process by requiring engagement with an agency's privacy function throughout the project lifecycle, including in relation to the design and implementation of governance and control measures.

3.4 Fair and ethical use of data, analytics and algorithms

The Algorithm Charter for Aotearoa New Zealand (the **Algorithm Charter**) is a commitment by government agencies to manage their use of algorithms in a fair, ethical, and transparent way. The Algorithm Charter Commitments are set out in Appendix 6.

The Algorithm Charter builds on the "Principles for safe and effective use of data and analytics"¹ (**Principles**), which set out six key principles intended to help agencies involved in data analytics activities, including algorithmic decision-making.

The Algorithm Charter and the Principles each align with the Privacy Act, providing additional guidance on the fair and ethical use of data, data analytics tools and algorithms. They are relevant to this PIA in the context of the algorithms that power ANPR systems, particularly in respect of accuracy considerations.

¹ See <https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance3.pdf> published by the Privacy Commissioner and the Government Chief Data Steward in 2018.

4. Background and context

This section explores the background and context to Police use of the Platforms, including consideration of how the Platforms work, how Police use them, what data is involved and overviews of the potential risks and the legal framework for sharing data in New Zealand.

4.1 What is ANPR?

Automatic Number Plate Recognition (**ANPR**) involves the use of cameras to capture still or video imagery that is then processed using Optical Character Recognition (**OCR**) and image processing software to automatically recognise and read vehicle alpha-numeric data. The information captured by ANPR systems may include number plate information (**NPI**), still images, video footage of the vehicle and its occupants, metadata (including a time and date stamp and the location of the vehicle in question) and vehicle details such as the make, model and colour (together, the **ANPR data**).

For the purposes of this PIA, this information is collected when an individual drives a vehicle into the operating sphere of an Organisation's camera that forms part of an ANPR system, such as a shopping centre car park or a service station forecourt. Vehicles involved in incidents such as suspected theft are recorded by Organisations in the Platforms as "vehicles of interest" to Organisations, with staff subsequently receiving alerts from the Platforms if one of those vehicles re-enters their premises.

4.2 Overview of the Platforms

From a Police perspective, the two Platforms are broadly similar in that they provide Police access to ANPR data sourced from the likes of private companies, local councils and public infrastructure owners (referred to in this PIA as "Organisations" for ease of reference) that own and operate ANPR networks.

The Auror platform focuses on enabling Organisations to report and log incidents occurring on their premises (which may range from theft to harassment and violence), manage and investigate cases and surface insights to help prevent and identify criminal activity in retail environments. Organisations who are Auror customers may choose to share their ANPR data with other Platform customers and the Police via the Platform.

The SaferCities "vGRID ANPR" platform is a video convergence platform that enables Police to view video streams from Police-owned and community ANPR cameras, such as those located in public spaces and on local council-owned buildings, including gantry and stadium cameras. It also enables the sharing of ANPR data with the Police, emergency services and other trusted partners.

Each Platform provides Police with access to two types of ANPR data.

4.2.1 Historic/retained data

Accessed using the “Find a Vehicle” function in the Auror platform and “ANPR detection” or “Quick Searches” in the SaferCities platform, this is ANPR data collected by Organisations. Police can retrospectively access and review such data in the Platforms to look for historic vehicle detections in the following circumstances:

- to investigate offences involving the use of motor vehicles after an offence has taken place;
- to investigate past offences that are suspected of being committed by someone who owns or uses a vehicle; and
- for intelligence gathering purposes in respect of vehicles linked to a person under investigation for an offence or a vehicle linked to an offence for which a suspect has not been identified.

While the Police are not required to obtain a warrant to access this information, the Police ANPR policy and SOPs set out various rules applicable to the levels of authorisation and information required for Police staff to access such data.

4.2.2 “Active detection capability”

The Police may also use the Platforms to collect real-time information about stolen vehicles and, in certain limited circumstances, other specific vehicles of interest to Police. This is referred to in the ANPR policy as “active detection capability”, with the Platforms referring to it as “Track a Vehicle” (Auror) and “Plates of Interest” (SaferCities). For the sake of consistency, we have used the Police term “active detection capability” or “ADC” throughout this PIA.

1) *Stolen vehicle list alerts*

The Police can receive automatic alerts from the Platforms of stolen vehicles detected by Organisations’ ANPR systems. To facilitate those alerts, the Police provide the Platforms with a list of stolen vehicles every 20–30 minutes, following the rules set out in the ANPR policy on page 9. This list is also published on the Police’s externally accessible website. This list is updated three times a day.

2) *Individual VOI Tracking*

Police staff can also create manual entries in each Platform to generate an alert and obtain the real-time location details of individual vehicles of interest (VOIs) when the specified vehicle is detected by a camera on the relevant ANPR network (**Individual VOI Tracking**). Individual VOI Tracking can only be used in the following limited circumstances (discussed further in section 6.2).

- Pursuant to a warrant obtained under the Search and Surveillance Act authorising the tracking of a particular vehicle or a person using a particular vehicle.
- Pursuant to emergency powers under section 48 of the Search and Surveillance Act.
- In circumstances where there is insufficient information to suspect an offence but Police reasonably believe there is a serious threat to the life or safety of any person or a serious threat to public health or public safety. This includes persons who are considered to be at risk of self-harm or harm by other individuals. In these circumstances, ADC can be used in respect of any

specific vehicle(s) suspected to be linked to the incident. We understand this scenario is based on an exception to IPP 2, which allows the Police to collect personal information from someone other than the individual concerned where that is “to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual” (IPP 2(e)(v)). This supports the function of the Police set out in the Policing Act 2008, which include “maintaining public safety”, “community support and reassurance” and “emergency management”.

The ANPR policy details the access and approval processes (page 12) and the SOPs set out what information is required to be entered in the Platforms (page 18) when conducting Individual VOI Tracking. Issues relating to the expiry of Platform alerts connected to Individual VOI Tracking are discussed in section 6.4.2.

4.3 Police use of the Platforms

The Police have used CCTV cameras and ANPR for some time to identify VOIs and investigate crimes involving motor vehicles. Prior to their access to the Platforms, the process used by Police to legally access information from Organisations was manual and time consuming. For example, in the context of a stolen vehicle, this would typically involve Police officers physically attending a store location to take witness statements and search the Organisation’s systems for information on the relevant vehicle.

The Platforms automate many of these processes by directly ingesting ANPR data from Organisations and enabling Police to readily access that data on request or by statutory demand. A defining feature of each Platform from a Police perspective is that the requests by Police are managed in an automated way.

Information obtained by the Police from the Platforms may be used in investigations and can be included in an investigation file as a permanent record.

Police use of the Platforms has grown significantly since access was first established, averaging in the range of 10-15,000 queries per month. Use of ADC functions and automated alerting is much less frequent (though also trending up), averaging fewer than 200 requests per month.

ANPR data sourced from the Platforms and elsewhere is used by the Police to investigate a range of issues in addition to motor vehicle theft. The ANPR policy includes various examples of how ANPR data may be used, including using ADC to generate real-time alerts for a vehicle where a suicidal teenager has gone missing in the family car or using a tracking device warrant to receive real-time alerts for a suspect in a vehicle involved in a shooting in a public place.

While this PIA focuses on current Police use of the Auror and SaferCities platforms, the ANPR policy and SOPs have a broader focus. Page 9 of the ANPR policy recognises that the Platform Providers are the only currently approved operators of ANPR-related platforms and sets out an approval process for any additional ANPR-platform operators with whom the Police may wish to engage.

4.4 ANPR data is personal information

The Privacy Act defines personal information as “information about an identifiable person”. That definition only requires the information to be about an identifiable individual, not that the individual is in fact identified in the information. Moreover, if an agency can link such information with other information to identify the individual(s) to which it relates, then the information will clearly be considered personal information and subject to the Privacy Act.

ANPR data provides a significant record of a vehicle’s – and by extension the owner/driver’s – whereabouts at a given time or over time. If a sufficient number of ANPR cameras are in operation, the combination of ANPR data from those cameras could lead to a comprehensive picture of a particular motor vehicle or individual’s movements and location. The grouping of information from multiple ANPR sites therefore has the potential to provide a wide-ranging log of vehicle movements.

Both Platform Providers also offer “automatic video retrieval” services, whereby the Police can use the Platforms to automatically retrieve video footage of vehicles – and their occupants – from ANPR sites on request.

Police use the Platforms to compare ANPR data collected from Organisations’ cameras with their own data held in various Police databases, including the National Intelligence Application (NIA) and Waka Kotahi’s Motor Vehicle and Driver Licence Registers. Police therefore have access to a range of data sources that in various combinations provide information that is demonstrably information about individuals and is therefore personal information subject to the requirements of the Privacy Act.

4.5 Legal framework for sharing ANPR data

An important feature of defining privacy risk and responsibility is clarifying who “holds” or is responsible for the personal information in question. The Privacy Act makes clear that where an agency (referred to as the **processor** in this PIA) holds or processes personal information solely on behalf of another agency (the **controller**), the controller is deemed to “hold” that information and is liable for it under the Privacy Act.²

In the current context, each Organisation is a controller who collects ANPR data directly from individuals and determines how that information is to be used, stored and shared. Under the Privacy Act, Organisations are considered to “hold” that information, even when it is stored on their behalf by processors like the Platform Providers. Organisations have the primary responsibility to ensure the processing of personal information complies with the IPPs.

As processors, the Platform Providers store and process personal information collected by Organisations on their behalf. They cannot process the information for their own purposes but they must take reasonable steps to ensure the ANPR data is secure (IPP 5).

² The terms “controller” and “processor” are borrowed from the EU General Data Protection Regulation as they provide a more useful shorthand to refer to the various parties in a service provider relationship. Section 11 of the Privacy Act sets out this agency relationship in a New Zealand context.

Organisations may choose to use the automated sharing functionality provided by the Platforms to disclose ANPR data to the Police. If they elect to do so, then as controllers they must ensure they comply with the disclosure requirements set out in IPP 11 in relation to Police requests for the voluntary release of ANPR data by Organisations to assist with Police operations. This is discussed in more detail in section 6.2.1.

In turn, when the Police access ANPR data disclosed by Organisations via the Platforms, they are considered to be “collecting” that information, requiring them to comply with Privacy Act requirements around purpose, transparency and lawfulness.

4.6 Potential risks associated with ANPR

Use of ANPR technology by law enforcement agencies has not been without controversy, particularly in the US and the UK.

4.6.1 US context

Civil liberties groups such as the American Civil Liberties Union (**ACLU**), the Electronic Frontier Foundation (**EFF**) and the Brennan Centre for Justice have for some time expressed concerns that ANPR poses a fundamental risk to privacy because aggregated data can reveal sensitive information about an individual's activities. Police use of ANPR systems in the US has raised concerns around mass surveillance, inaccurate results, improper data retention and usage (including increased enforcement and disparate racial, ethnic and socio-economic impacts), inadequate protection of data collected by ANPR cameras and a lack of regulation.

Lobbying by those groups³ led to the adoption of legislation expressly addressing the use of ANPR in 17 US states. Typically, those laws are focused on the use of ANPR by law enforcement and incorporate rules around data retention time frames, individual access to information held about them and restrictions on sharing ANPR data with third parties.

4.6.2 United Kingdom

Both CCTV and ANPR are widely used in the UK, with the former UK Information Commissioner calling the country a “surveillance state” in 2006. Various pieces of legislation have been implemented to regulate surveillance camera and ANPR usage in the UK, including the Data Protection Act 2018 (the UK’s implementation of the General Data Protection Regulation), the Regulation of Investigatory Powers Act 2000 and the Protection of Freedoms Act 2012, which applies to publicly-owned systems and those controlled by the police.

A Surveillance Camera Code of Practice and the appointment of a Surveillance Camera Commissioner were established in 2013 under the Protection of Freedoms Act 2012 with the intention

³ See the 2012 ACLU report and related campaign entitled “You Are Being Tracked” – <https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked?redirect=feature/you-are-being-tracked>

of securing public confidence in the use of surveillance cameras as a crime detection tool. The Code sets out guiding principles that apply to “all surveillance cameras in public spaces” and sits alongside the ICO’s CCTV Code of Practice (2008).

The Code has twelve guiding principles for CCTV and ANPR and introduces a philosophy of “surveillance by consent”, meaning the public can be confident that the cameras are not there to spy on them, but to protect them and help in the fight against crime.

In February 2022, the Surveillance Camera Commissioner became the Biometrics and Surveillance Camera Commissioner whose role is to encourage compliance with the Surveillance Camera Code of Practice as well as focusing on biometric issues.⁴

4.6.3 New Zealand

Unlike the US and the UK, New Zealand does not currently have any legislation specifically targeted at CCTV or ANPR usage. Furthermore, guidelines issued by the Office of the Privacy Commissioner in 2009 entitled “Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations” do not reference ANPR.




Key concerns associated with ANPR in a New Zealand context include mass surveillance and Police misuse of ANPR data and systems⁵.


⁴ <https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner>







⁵ <https://www.nzherald.co.nz/nz/crime/police-used-false-information-to-access-powerful-network-of-surveillance-cameras/BEVYOQHF3N5VAED3CD7LXSPTAU/>

5. Summary of application of IPPs

This section summarises the application of the IPPs to Police collection and use of ANPR data from the Platforms, with a view to identifying risks that should be given more detailed consideration in section 6. It should be noted that risks and solutions can impact several IPPs simultaneously.

-  No issue
-  Relevant, but not serious
-  Must be given serious consideration

IPP	Status	Comments
1. Collect only personal information that is necessary for a lawful purpose		When collecting ANPR data from the Platforms, the Police must have a lawful purpose for their collection and must not collect more than is necessary for that purpose. See the further discussion in section 6.1.1.
2. Collect personal information directly from the person concerned		The Police may rely on an exception to IPP 2 enabling them to collect information indirectly (i.e. from Organisations via the Platforms) where that is necessary to avoid prejudice to the maintenance of the law, including to the prevention, investigation, prosecution and punishment of offences (IPP 2(2)(e)(i)). See the further discussion in section 6.1.2.
3. Tell people why personal information is required, how it will be used, and who it may be shared with		The Organisations collect ANPR data directly from the individuals concerned so they need to take reasonable steps to communicate such collection to the public. We encourage the Police to also take a broader view of its transparency obligations, as discussed in section 6.1.3.
4. Collect personal information lawfully, fairly and not in unreasonably intrusive ways		Police collection of ANPR data from the Platforms must be necessary and proportionate as discussed in section 6.1.2.
5. Take reasonable steps to keep personal information safe and secure		The Police already have a range of security and access controls in place around staff use of sensitive systems, including NIA. Controls around how Police specifically access ANPR data in the Platforms is discussed in more detail in section 6.3.
6. & 7. Let people access and correct their personal information		The Police already have policy and processes in place to address rights of individual access to and correction of personal information.

IPP	Status	Comments
8. Take reasonable steps to check personal information is accurate before using it		Ensuring ANPR data is accurate before Police staff rely on it in their investigations is critical to avoid the risk of misidentification. This is addressed in more detail in section 6.4.
9. Don't retain personal information for longer than it's needed for a lawful purpose		It is important Organisations and Platform Providers do not retain ANPR data for longer than is required for the Organisations' lawful purposes. The Police have a role to play in supporting both groups to comply with IPP 9, as discussed in section 6.5.
10. Use personal information only for the purposes it was collected		<p>The Police must ensure they only use ANPR data for the purposes specified in the ANPR policy (see pages 4-5).</p> <p>If necessary, they may be able to rely on an exception enabling them to use personal information for a different purpose where they reasonably believe that is necessary to avoid prejudice to the maintenance of the law, including the prevention, investigation, prosecution and punishment of offences (IPP 10(1)(e)(i)).</p>
11. Don't disclose personal information, unless an exception applies		<p>Disclosure of ANPR data to the Police is a key consideration for Organisations under IPP 11. The actions Police should take to support Organisations' compliance is discussed in section 6.2.</p> <p>In addition, the Police cannot disclose ANPR data to a third party unless an exception applies, including where they reasonably believe disclosure is necessary to avoid prejudice to the maintenance of the law, including the prevention, investigation, prosecution and punishment of offences (IPP 11(1)(e)(i)).</p>
12. Only disclose personal information to overseas third parties if it is subject to comparable privacy safeguards		IPP 12 is not directly relevant as the Police do not disclose ANPR data outside New Zealand.
13. Only assign unique identifiers if you need to, and don't assign another agency's unique identifier		Unique identifiers are not relevant in this PIA.

6. Privacy risk & opportunity assessment

This section discusses the Police's key privacy risks and opportunities arising from its collection of ANPR data from the Platforms, including the critical need for appropriate governance and accountability in any systems collecting personal information like ANPR data.

6.1 Police collection practices

From a privacy perspective, Police "collect" personal information when staff members access and use ANPR data on the Platforms.

6.1.1 Purpose

The New Zealand Police Manual (known as the "Police Instructions") sets out instructions and guidance to Police on the administrative and operational aspects of policing, including nationally consistent standard operating principles, practices, policies and procedures.

Included in the Police Instructions is a chapter on ANPR, which includes the ANPR policy and the SOPs. They describe the Police's purposes for using ANPR technology as being for a "range of enforcement, staff safety and public safety purposes" as follows (page 4).

- *The use of real-time (or as near to real time as possible) ANPR data for crime prevention, staff safety and immediate response activities, including in relation to vehicles with a "stolen" alert identified by third-party ANPR networks; and*
- *The use of retained (i.e. historical) NPI for investigative, evidentiary and intelligence purposes for the investigation of offences (together the Purpose).*

We consider those purpose statements are sufficient for IPP 1 and do not introduce further risk.

"Function creep" refers to the gradual widening of the use of a technology or system – and the data on it – beyond the purpose for which it was originally intended, especially when this leads to potential privacy issues. To minimise the risk of function creep, the Police will need to ensure appropriate governance, controls and audit processes are implemented, as discussed further in section 6.3 below.

6.1.2 Lawfulness, necessity and proportionality

IPPs 1 and 4 require consideration of whether the collection of ANPR data by the Police is necessary to fulfil the Purpose, whether the Police's collection methods are lawful and fair, whether they are the best or only way to capture the information and whether the privacy impacts on individuals are outweighed by the public interest in the Police having this information.

An assessment of whether those potential privacy impacts are proportionate to the benefits of Police use of ANPR involves consideration of the scale of the risks and benefits. If the benefit is relatively minor, then the loss of privacy is less likely to be considered appropriate and proportionate.

In terms of the potential benefits of Police use of the Platforms to access ANPR data, there is ample evidence that stolen vehicles and crime in general are significant problems. ANPR data benefits the Police and the public by facilitating crime detection and prevention and the maintenance of public safety, including by helping to identify the locations of those suspected of criminal offences as well as those who may be missing or at risk of harm. Access to ANPR data – particularly in real time – saves Police time and resources in obtaining that information, including by enabling the fast deployment of Police vehicles for investigation purposes. An additional benefit of systems that involve CCTV and ANPR is likely to be the deterrent effect this may have on potential offenders.

While the Police are still able to access similar information via more manual methods, the ability to access ANPR data in a centralised platform is a significant time and resource saver, which can be critical in high-risk or urgent situations. In addition, by providing better visibility of suspects, the Police may be better placed to take appropriate and preventative action, including where there is violent and/or aggressive behaviour.

However, those benefits need to be balanced against the potential privacy impacts of Police use of ANPR data. They include a lack of transparency, inaccurate data leading to misidentifications, unreasonable use and/or disclosure and perceptions (real or otherwise) of profiling and surveillance. Media reporting suggests public concern around the potential for Police surveillance given the Platforms contain substantial ANPR data about ordinary citizens going about their daily lives, including video footage of potentially both drivers and passengers. The ANPR Policy itself states that “The vast majority of NPI is of no interest to Police as it will not be matched to a VOI”.

To address these privacy risks and concerns, the Police need to have robust governance, policies, processes and controls in place that ensure Police engagement with the Platforms is appropriate and lawful and the potential for misuse is limited as much as possible. This includes the following.

- Given its privacy-invasive nature, Police should ensure the use of ADC functionality in the Platforms is proportionate to the Purpose, including by limiting Police access to ANPR data for ADC purposes to clearly defined circumstances with supporting operational guidance and technical controls in place to ensure access is only possible in those limited circumstances. See the discussion in section 6.3 for more detail.
- Incorporating data minimisation principles into Police processes to ensure there is only targeted access to ANPR data focused on specific queries. Police should not have unfettered access to all of the data in the Platforms. This is currently the case – the Police are only able to make targeted queries within the Platforms, rather than having wholesale access to all of the information contained in those environments.
- Deleting ANPR data not used for real-time “hits” identifying stolen vehicles from the Platforms as soon as possible, while acknowledging the need to retain “hit” data for investigation and prosecution purposes and processes. If non-“hit” data is retained for further search purposes, the proportionality argument needs to be supported by evidence that the retention is beneficial to Police functions and that the collection benefits the public.
- Helping Organisations to meet their disclosure obligations under IPP 11 of the Privacy Act as discussed in section 6.2.1.

- Having appropriate governance and controls in place to ensure all Police staff are using the Platforms correctly and lawfully, as discussed in section 6.3.

Rec-001: Ensure Police governance, policy, procedures and controls only permit the collection of ANPR data through the Platforms for the Purpose and in a way that is necessary and proportionate to the benefits so as to minimise the risks of unnecessary collection of personal information, particularly where ADC is used.

6.1.3 Transparency

When collecting personal information directly from individuals, IPP 3 requires an agency to take reasonable steps to advise affected individuals of the circumstances of the collection, ideally at the time of collection.

Organisations collect ANPR data directly from the individuals concerned and therefore have to comply with the transparency obligations in IPP 3. That could be done by Organisations clearly communicating their collection activities using prominent signage and statements to explain that the Organisation is collecting and sharing ANPR data both with other Organisations and the Police and that this may include video footage of drivers and passengers. We acknowledge the Police has no ability to require Organisations to do so but note they may be able to influence Organisation activity in this space.

The Police collects ANPR data indirectly from Organisations via the Platforms rather than directly from individuals, so strictly speaking is not required to comply with IPP 3 at this stage.⁶ However, given the Police's law enforcement role in New Zealand there is an argument that it has wider transparency obligations to the general public in relation to how it collects and uses ANPR data. In our view, Police transparency around its use of ANPR data is likely to enhance public trust in Police efforts, ultimately supporting notions of "policing by consent", as well as potentially providing a general deterrence to those who commit crime.

This is supported by DPUP, where the "Transparency and Choice Guideline" describes an approach that focuses on transparency and openness as the foundation of improved trust. In particular, it emphasises that people who use agency services (including those provided by the Police) want a good understanding of why their information is needed, pointing out that they can experience anxiety if agencies are unclear about the purposes of collection, especially if their current situation is already a difficult one.

It is therefore appropriate that the SOPs state in section 4.1 that the Police's ANPR governance group, the Organisational Culture Governance Group, will approve annual public transparency reporting on Police use of ANPR technology. To support this reporting, we recommend the Police develops a strategy for ensuring appropriate transparency on its collection and use of ANPR data from the

⁶ We note that possible changes to IPP 2 in relation to the indirect collection of personal information are currently under consideration by the Ministry of Justice, which may impact the Police in this context if introduced. See the Ministry of Justice's Summary of Engagement on "Possible changes to notification rules under the Privacy Act 2020"
<https://www.justice.govt.nz/assets/Summary-of-Submissions-notification-rules-Privacy-Act-2020-FINAL.pdf>

Platforms, including the fact that ANPR data may include video footage featuring a vehicle's driver and passengers.

Information about the Police's ANPR activities should be published in an easily locatable section of the Police's public-facing website. It should include information about the Purpose, the controls in place around access to and use of ANPR data on the Platforms and a summary of governance and audit practices. The Police has indicated it may proactively publish usage statistics and summaries of audit findings on the Police's public-facing website, which we encourage. The Police should also consider making this PIA available to the public to confirm that privacy issues have been considered.

Transparency reporting also presents the Police with an opportunity to communicate the public benefits associated with Police use of ANPR data, not only in terms of the investigation and prevention of criminal activity but also in relation to public safety and emergency response activity.

Rec-002: Implement a transparency strategy to highlight Police engagement with the Platforms, including making the public aware their personal information may be collected by Police via third-party ANPR systems and the reasons for that collection.

6.2 Information sharing

When it comes to ANPR data in the Platforms, the key disclosure of personal information is that made by Organisations to the Police via the Platforms. Police may obtain ANPR data for law enforcement purposes either by making a request for the voluntary disclosure of personal information or pursuant to powers granted under the Search and Surveillance Act, as follows. Police may only demand information if they have a lawful power to do so.

- **Voluntary disclosure requests:** The Privacy Act applies to Police requests for the voluntary disclosure of personal information by Organisations, which may be made without a warrant or other statutory demand where an investigation would otherwise be prejudiced. This is referred to in the ANPR Policy as a "Request for Information" (RFI). Compliance with a Police request for personal information is not mandatory and the Police have no power to compel Organisations to disclose personal information.
- **Production orders:** Section 71 of the Search and Surveillance Act enables the Police to issue production orders, which require the custodian of documents to make those documents available within a specified period. An agency served with a production order must comply with the order, which overrides the Privacy Act.
- **Search warrants:** Section 46 of the Search and Surveillance Act provides for the use of surveillance device warrants, which cover tracking devices (defined as any device that can be used to ascertain the location of a thing or a person). Except in very limited circumstances, the Police may only use tracking devices with a surveillance device warrant issued by a judge. A warrant must specify the period for which it is in force, which cannot exceed 60 days.
- **Emergency situations:** Under section 48 of the Search and Surveillance Act, a surveillance device warrant is not required in some emergency situations, including where there are

reasonable grounds to suspect a serious offence has been or is being committed (punishable by a term of imprisonment of 14 years or more) or there is risk to the life or safety of any person requiring an emergency response and the use of a surveillance device. The use of tracking devices without a warrant is only permitted for a maximum of 48 hours.

6.2.1 Voluntary disclosure requests under the Privacy Act

The Privacy Act requires both disclosers and recipients/collectors of personal information to establish a lawful basis for their actions. In the current context, this means that Organisations – as disclosers of personal information – must establish they can rely on an exception to the general prohibition on disclosure in IPP 11 to enable them to disclose ANPR data to the Police. Similarly, the Police must be able to establish that an exception applies to the general requirement in IPP 2 that personal information is collected directly from the person concerned when collecting ANPR data from Organisations via the Platforms.

Both IPP 2 and IPP 11 contain “maintenance of the law” exceptions that facilitate information sharing needed to “avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences”. Organisations and the Police must demonstrate a reasonable belief in their ability to rely on the maintenance of the law exceptions to enable the sharing of personal information in compliance with the Privacy Act when the Police request the voluntary disclosure of personal information by an Organisation.

The Platforms facilitate Police requests for ANPR data from Organisations by automating the Police request and collection processes as well as the Organisation’s disclosure processes. This means an Organisation does not consider each individual Police request for access to their ANPR data as they did prior to the advent of the Platforms. Rather, each Platform receives and automatically processes Police requests on behalf of Organisations, saving both the Police and the Organisations time and resources. Participants in the sharing of ANPR data via the Platforms therefore need to be mindful of the following points, based on case law and commentary from the Office of the Privacy Commissioner.

- The agency seeking to rely on an IPP exception bears the burden of establishing that reasonable grounds exist to rely on that exception. So where an Organisation is asked by the Police to share ANPR data, the Organisation must be able to satisfy itself that it is reasonable to believe the maintenance of the law exception applies to permit the disclosure.
- Any voluntary request by the Police needs to contain sufficient information to enable the recipient (such as an Organisation) to form a reasonable view as to whether there is a proper basis for disclosure⁷. If an Organisation is not satisfied that the grounds for release have been satisfied, it will not have a legal basis under the Privacy Act to release the information and the Police request should be declined.

⁷ *R v Alsford* [2017] NZSC 42, at para 33. The Supreme Court stated that a requesting agency must provide a holding agency with sufficient information to enable it to reach a reasonably-based view on whether or not requested information is required for an authorised purpose. See also the Privacy Commissioner’s commentary on that case in the context of voluntary requests for personal information by law enforcement agencies: <https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/May-2018-Alsford-commentary-for-external-use2.pdf>

- An agency relying on a “maintenance of the law” exception only needs “reasonable grounds” to believe the exception applies – it does not have to be absolutely certain that it does. Reasonable belief has been held to mean “an actual belief based on a proper consideration of the relevant circumstances”⁸.

Organisations therefore need to have confidence that any automated voluntary requests for ANPR data from the Police received through the Platforms contain enough information to enable them to form a reasonable belief they can rely on the maintenance of the law exception. Guidance from the Office of the Privacy Commissioner⁹ provides that whether there is a reasonable basis will depend on what the Organisation knows and what it has been told by the Police about why the information is required. If a Police request does not provide sufficient detail to demonstrate that the ANPR data is necessary for the investigation in question, then the disclosure by the Organisation will not be lawful. This would also mean the Police would be unable to rely on the information as evidence in any prosecution.

Accordingly, it is critical the Police clearly indicate the following in relation to every voluntary disclosure request made using the Platforms.

- **Why they are requesting the ANPR data.** Police users must describe the relevant circumstances that provide reasonable grounds for Organisations to believe the maintenance of the law exception applies. Police are not required to outline the course of the investigation in detail and do not have to meet the same standard as for a production order or search warrant.¹⁰
- **The link between the ANPR data being requested and the offence.** Without adequate detail from the Police, Organisations cannot be satisfied that the maintenance of the law exception applies.

This requires the Police to have suitable policies and procedures in place to ensure their requests for ANPR data meet Organisation expectations and obligations for disclosing that information. In particular, there need to be ways to ensure Police personnel use the Platforms appropriately, enter the necessary information and that any scope for misuse is limited as much as possible. In addition, the Platforms automating this information sharing need to be designed to facilitate the appropriate input of the necessary information by Police. These issues are discussed in more detail in the following section on “Governance, accountability and assurance”.

We note that automation of voluntary requests for disclosure has not yet been tested by the courts. Accordingly, it is possible that judicial interpretation of the application of IPP 11 to how the Platforms automate the disclosure of ANPR data by Organisations to the Police might consider that an Organisation’s reasonable belief must be based on proper consideration of the relevant

⁸ *Geary v Accident Compensation Corporation* [2013] NZHRRT 34.

⁹ See www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/October-2017-Final-Guidance-on-releasing-personal-information-to-Police-and-law-enforcement-agencies-Principle-11f-and-ei.pdf

¹⁰ See <https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/May-2018-Alsford-commentary-for-external-use2.pdf>, including page 3: “At an early stage of an investigation, the Police may not be able to say much more than a particular offence is being investigated and the information requested is relevant to that offence, with some indication of why it is relevant.”

circumstances in each individual situation and cannot be automated to the extent provided by the Platforms. Overall, we consider that provided Police staff provide sufficient information in support of their requests to enable Organisations to form the necessary reasonable beliefs, then the maintenance of the law exception remains available through use of the Platforms.

Rec-003: Ensure Police requests for the voluntary disclosure of ANPR data by Organisations through the Platforms facilitate and satisfy Organisations' expectations and obligations for the disclosure of such information.

6.3 Governance, accountability and assurance

Good privacy practice relies on robust governance, ownership and accountability. Where agencies collect and manage significant quantities of personal information, governance is a critical element of ensuring that the information is well managed and that there is clear ownership of - and accountability for - the risks inherent in gathering and using personal information.

Effective governance is a requirement of the Privacy Maturity Assessment Framework (**PMAF**), which the Police is required to report on annually. The ANPR policy and SOPs also acknowledge the importance of governance and assurance, with page 19 of the SOPs stating that "maintaining good assurance practices regarding Police engagement with the platform holders is crucial to good governance and oversight."

The Police established what is now known as the Organisational Culture Governance Group (**OCGG**) in 2020. This group has primary oversight and governance of the ANPR policy and is responsible for overseeing the Police ANPR programme on a national level, including ensuring regular audits are conducted, that ANPR data is deleted from Police-controlled storage facilities at the end of relevant retention periods, appropriate training is provided and compliance with applicable laws, policies and procedures is maintained.

The ease with which ANPR data may be accessed and collected by the Police on the Platforms brings with it a risk of misuse. While appropriate ANPR rules, guidance and policies will help to encourage best practice use of the Platforms by Police staff, they are unlikely to entirely remove the potential for misuse. As well as appropriate policy settings, Police need to implement supporting processes and controls to ensure legal and policy requirements are followed. In particular, there need to be ways to ensure Police personnel use the Platforms lawfully and appropriately, that any scope for misuse is limited as much as possible and that should misuse in fact occur, it is promptly identified and addressed.

6.3.1 Police policies and procedures

Good governance requires clear rules, policies and procedures around how an organisation collects, uses, stores and shares personal information. For example, and as discussed above in the context of voluntary disclosure requests under IPP 11, it is critical Police clearly indicate why they are requesting access to ANPR data in the Platforms and how that information is relevant to the offence being investigated. This in turn requires the Police to have suitable policies detailing what information must be entered in the Platforms, as well as supporting processes and controls to ensure this happens.

The ANPR policy and SOPs set out how Police personnel are expected to access and use ANPR data on the Platforms. While those documents provide appropriate rules and guidelines on how Police personnel must engage with the Platforms, we query the ease with which frontline Police staff are likely to be able to make sense of the large volume of reasonably complex information in the ANPR policy. That includes details of the different legal bases for accessing ANPR data (i.e. under a search warrant, under s 48 of the Search and Surveillance Act or pursuant to a voluntary disclosure request), rules around authorisation levels required to access information depending on the legal basis and further rules in the SOPs around information that must be entered in the Platforms for assurance purposes.

In addition to the current content, the inclusion of tables or diagrams that collate some of this material and present it in more accessible ways may help to ensure Police staff understand and abide by the various requirements.

Rec-004: Refresh the ANPR policy and SOPs to ensure the rules and guidelines are presented in a clear, consistent and accessible way that facilitates easy comprehension and implementation by Police staff.

6.3.2 Police audits

Each of the Platforms maintains audit logs of Police use of that Platform, which are available to the Police. The ANPR policy sets out the audit functions provided by each Platform¹¹, which include keeping logs that capture data on user access, reviews completed by individual users and all Tracking requests.

The SOPs provide that Police auditing of staff access to the Platforms is important in demonstrating appropriate use by Police of those Platforms, as well as having a deterrent effect. The SOPs specify that audits will be completed every three months.

We understand that the OCGG/ANPR Steering Group will determine the frequency of ongoing audits and any further controls that may need to be implemented. Audits of Police use of the Platforms are likely to be factored into Police's rolling programme of internal audit and assurance work and audit results will be shared with scrutiny and governance groups, such as the Police's independent Assurance and Risk Committee. It is also intended they will be made available on request to oversight and regulatory bodies, such as the Office of the Privacy Commissioner. Audits of Police use of the Platforms will be conducted by specialists based in the Police's central Assurance Group.

In late 2022, the Police commissioned a baseline-setting audit of Police use of the Platforms (**Data Audit**). The Data Audit examined the logs maintained by the Platform Providers as well as Police records associated with ANPR data in NIA and other relevant Police systems. Examples of some of the issues identified in the Data Audit include the following.

- While the Platforms enable users to input Police file numbers, search warrant numbers and the reasons for undertaking a search, they are unable to validate the authenticity of that

¹¹ See Appendices B (Auror) and C (SaferCities) of the ANPR policy.

information against Police systems for security reasons. For example, the Platforms cannot validate whether a valid or accurate search warrant number has been included.

- Both Platforms allow certain free text entries for inputting necessary information. However, the Data Audit found instances of these not being completed or unhelpful/unclear information being entered.
- It is not uncommon for more than one Police user to share the same login for computer hardware when accessing the Platforms, making it difficult to identify which individual user has done what on the Platforms.
- Email addresses of authorising officers are not always included as required by the ANPR policy and, in some instances, the email requesting authorisation was sent to the officer making the original request.
- A small number of Police employees searched the Platforms for vehicles where their name matches a registered owner. Examples were also found of searches for a vehicle jointly owned by another person with the same surname.

Of the 350,000+ transactions reviewed in the audit, only four cases (0.0001%) were assessed as warranting specific follow up by the Police's National Integrity Unit. Accordingly, these apparent cases of misuse are limited in the context of overall Police usage and appropriate follow-up action appears to have been taken by the Police.

Nonetheless, it is important to recognise that Police misuse of ANPR data could occur, with the potential to cause a range of harms to affected individuals.

Rec-005: Ensure both Police systems and the Platforms effectively log Police user access to ANPR data in the Platforms and that regular audits are conducted to understand how the Platforms are being used.

6.3.3 Real-time monitoring and validation

Historically, audit logs were used to provide visibility of data security risks, including access to and activity within a database. Organisations would typically react to reports of suspicious or anomalous behaviour by scrutinising historical audit logs for evidence of inappropriate or unlawful behaviour.

The problem with reactive audits, however, is that they only occur after harm may have already occurred. Good data stewardship requires appropriate controls to manage how personal information is accessed and used and to minimise the risk of misuse in the first place. This will also deter unlawful behaviour and provide assurance to programme governance that the system is not being abused.

This perspective was emphasised by the Privacy Commissioner in relation to a complaint about the disclosure by two employees of personal information obtained from the Department of Correction's (Corrections) intelligence database¹². The Privacy Commissioner was critical of Correction's

¹² Case note 289320 [2019] NZPriv Cmr 3: Corrections employee accessed complainant's record and disclosed information.

approach: "In our view, it was not sufficient just to have policies to safeguard information against unauthorised access. Agencies should also have processes in place to ensure that those policies were being followed."

In the context of Police access to the Platforms, the aim should be to have effective and proactive processes and controls in place that identify and prevent inappropriate behaviour *before* access occurs, as well as post-event audit. This will provide assurance to Police governance that the Platforms are not being misused and will help demonstrate to the public that they can have trust and confidence in the Police's stewardship of their information.

We recommend this is done by enabling real-time monitoring and validation of the information entered by Police users before they are granted access to ANPR data on the Platforms. Items to be reviewed and validated include the following.

- Whether a valid Police record or warrant number has been entered.
- An indication of the type of Police activity by selecting from a drop-down menu (e.g. drugs, homicide, violent crime etc.).-
- A suitable explanation in the free-text box as to why ANPR data is needed and how it connects to Police activity for IPP 11(1)(e) requests.
- Whether the appropriate authorisations are in place, ensuring system arrangements limit the ability to send approval requests to yourself or a peer. This could take the form of an automatically-populated form designed to ensure it could not be completed unless sent to the relevant supervisor, working from a drop- down list of approved supervisors.
- A supervisor's verification of the request, including that a valid file number and reason are in place.

This real-time validation could be achieved through either manual checking of requests for ANPR data or by using technical solutions.

A **manual solution** could involve all requests for access to ANPR data first being sent to a supervisor to check whether the request is lawful and meets the relevant requirements, including that the necessary information has been provided, is valid and is sufficient for the purposes of the request. If a request does not meet the relevant specifications, it would be declined and would not be sent through to the Platforms. Similarly, such requests could go to an internal Police group tasked with centralised oversight and review of ANPR requests.

A further "manual"-style option to provide assurance and confidence that the Platforms are being used appropriately would be to limit the number of staff who can access the Platforms in the first place. Rather than all Police staff being able to request access to ANPR data in the Platforms, access could be limited to a select group of trained staff.

A **technical solution** could be preferable to a manual one from an operational and Police resourcing perspective but would need to adequately ensure the Platforms were able to properly identify and validate the information provided in relation to the request. For example, determining that a valid file or warrant number has been entered and declining the request if not. From a practical perspective,

this is more challenging given the Platforms are not able to integrate with Police systems for security reasons. However, a technical solution could involve Police infrastructure that manages and stores ANPR data requests before they are sent to the Platforms. This approach would have the added advantage of being centralised and auditable by Police internally, without having to rely on the Platforms for audit purposes.

Whether a manual solution, a technical solution or some combination of the two is selected, real-time monitoring and validation is likely to have a strong deterrent effect. If Police users know that any misuse will be identified in near real-time, then this will address both possible misuse and a natural human instinct to follow the path of least resistance and avoid what could be perceived as the “unnecessary admin” of entering the necessary information when using the Platforms.

Rec-006: Implement manual and/or technical controls to reduce the risk of misuse of the Platforms by Police users *before it happens*, including enabling real-time monitoring and validation of Police information entered in the Platforms.

We understand the Police are already engaging with the Platform Providers to explore what design and user interface changes could be made to the Platform to strengthen controls around the entry of necessary information. In particular, a workshop with the Platform Providers has been scheduled with the aim of identifying opportunities to design the user experience to help Police ensure their requests for ANPR data are lawful, appropriate and in compliance with the ANPR policy.

Topics for exploration include developing and implementing an effective control for self-approval of access requests, the creation of a curated list of authorising email details to function as a pre-set list of individuals able to authorise ADC activities and options for verification that warrant numbers, Police file numbers and other references are valid.

We encourage and endorse this approach because user interface changes can be a powerful way to enforce appropriate usage and actions.

Rec-007: Continue to engage with the Platform Providers to explore what user interface changes could be made to the Platforms to require Police users to always enter valid information.

6.3.4 Guidance and Training

Privacy is about people and processes as much as systems. A robust policy framework and technical infrastructure is still vulnerable to privacy risks if the people using it are inadequately prepared, trained or supported. Staff training is therefore a crucial element of privacy preparedness when implementing a new system.

The official Police position is that access to ANPR data is only permitted in accordance with the ANPR policy and SOPs, with those documents providing guidance on appropriate use of the Platforms. Page 21 of the SOPs provides requirements around completing formal training before ANPR equipment is operated by Police staff. However, this only appears to apply to Police-owned ANPR systems.

We understand that training is currently underway in relation to appropriate log-ins to Police systems and devices, which will include reminders not to use group or team email addresses. However, we are not aware of the Police providing any formal training to users of the Platforms.

In terms of awareness raising, we understand the following ANPR-related communications have been issued by the Police.

- A staff notice went out through “Ten-One” on 28 September 2022 reminding Police staff to view the refreshed ANPR Policy before using ANPR to generate real-time notifications.
- A notice was sent to District Commanders and Directors in November 2022 to draw attention to appropriate use of ADC functions in the Platforms and the importance of recording file numbers in query functions.
- On 27 February 2023 the ANPR Steering Group actioned further reinforcement of expectations around the use of ANPR capabilities with the Investigations Governance Group for cascading to Crime Managers and District Commanders.

In addition, registered Police users of the Platforms are required to agree to Platform terms and conditions that prohibit misuse and reinforce that the Platforms must only be used for the Purpose in accordance with Police policies.

Training of Police staff on appropriate use of the Platforms and requests for ANPR data is key to ensuring Police have a clear understanding of the rules and expectations surrounding that usage. That is particularly so given the complexity of the rules around ADC and the volume of rules surrounding approvals and necessary information inputs to justify Police requests for ANPR data. Formal Police-provided training should focus on lawful and appropriate use of the Platforms that is aligned with the ANPR policy. Updated training should also be provided at appropriate intervals to remind Police staff how they should be using the Platforms and why.

Incorporating reminders and “nudges” into the user interface of the Platforms is another useful way to encourage Police users to input the correct information. A “nudge” is a concept rooted in behavioural science whereby minor changes in product design can be used to affect user behaviour. For example, nudges could be used in the Platforms to remind Police staff of the information that needs to be entered in free text boxes in relation to voluntary disclosure requests.

Rec-008: Support Police staff to use the Platforms lawfully and appropriately through adequate training, awareness raising exercises and Platform nudges and reminders.

6.4 Accuracy and reliability of data

6.4.1 Importance of checking ANPR data

IPP 8 requires agencies not to use or disclose personal information without taking reasonable steps to ensure the information is accurate, up to date, complete, relevant and not misleading. Similarly, the

Algorithm Charter specifies that signatories must “make sure data is fit for purpose by understanding its limitations”.

Privacy harms are likely to arise if inaccurate ANPR data is relied upon by the Police. This includes the potential for misidentification and false accusations of criminal activity, which has the potential to have a significant impact on the falsely accused individual. For example, if an ANPR camera were to misread a vehicle number plate and this information prompted an alert that, without verification, led to the arrest of someone not connected to the actual vehicle in question. This is a real risk that has played out in various scenarios in the US, where incorrect license plate readings have led to unreasonable detentions.

These risks can occur due to poor image quality, including where the quality or positioning of ANPR cameras and/or lighting variations result in the capture of low-quality images. The ANPR policy notes on page 26 that OCR software may occasionally misread similar-shaped characters such as a “1” as an “l” or an “O” as a “Q”. It advises that the ANPR operator must compare the photograph of the captured plate with the OCR-produced reading to determine if the plate has been read correctly.

Human oversight and judgment and the application of discretion must therefore accompany the deployment of automated technology like ANPR systems, requiring Police staff to double check the accuracy of ANPR outputs before relying upon them.

We understand there are established Police processes to make sure ANPR data and other information relevant to an investigation is reliable and can be trusted. For example, staff at the Police command centre check that ANPR data received from a Platform alert matches Police stolen vehicle data, including a match for the make, model and colour of the vehicle. The patrol officers who then attend where the stolen vehicle was identified are required to do a further check on arrival at the location of the vehicle.

However, it is important to note that human oversight is not itself entirely risk free and can offer false reassurance. “Automation bias” (also known as the “control problem”¹³) arises when people place too much trust in computers and favour the path of least resistance – namely the answer provided by the machine. This can result in them discounting other correct and relevant information.

It is therefore critical to ensure Police officers maintain discretion and awareness of the need to conduct appropriate checks of ANPR data before it is relied upon so they have sufficient confidence they are following reliable leads.

The risks of incorrect information being used after human oversight lie with the Police. For example, if data results in an individual being prosecuted wrongly, an action of an interference with the individual’s privacy could be mounted in addition to the Courts dismissing the prosecution. Police would be responsible for rectifying the incident and potentially paying damages.

We note that page 26 of the SOPs includes a diagram illustrating the procedure to be followed by ANPR operators when a VOI is detected, which is reproduced below.

¹³ See for example Babuta, A. and Oswald, M. (2019) Briefing paper: Data Analytics and Algorithmic Bias in Policing, at p.15 and Zerilli, J., Knott, A., MacLaurin, J. and Gavaghan, C. (2019) Algorithmic Decision-Making and the Control Problem. *Minds and Machines* 29: 555–578.

VOI alerts - ANPR operators

ANPR operators must follow the procedure in figure 1 below when a VOI is detected.

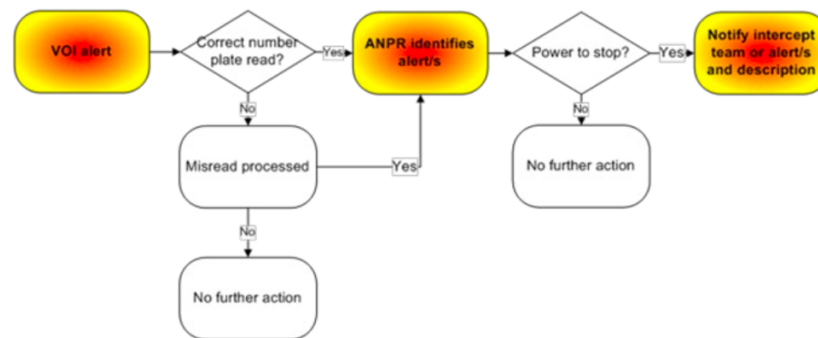


Figure 1: ANPR operators' decision chart

However, this diagram appears to only relate to the operation of Police-owned ANPR systems and there is no equivalent version in the ANPR policy that is applicable to use of the Platforms.

Rec-009: Provide clear guidance on the need to double check Platform-sourced ANPR data before it is relied on, including updating the ANPR policy with guidance focused on accessing ANPR data through the Platforms. This guidance should also call attention to risks associated with automation bias.

6.4.2 Expiry of ADC alerts

ADC and alert data, particularly when used for Individual VOI Tracking, must be up-to-date with appropriate expiry dates to maintain the Police's lawful basis for such activities and avoid the risk of privacy harms.

Individual VOI Tracking

As discussed previously in section 4.2.2, the Police may use the Platforms to generate alerts to conduct Individual VOI Tracking in the following circumstances.

- Where a surveillance device warrant is issued by a judge pursuant to the Search and Surveillance Act, which will specify the applicable time frame for the authorised tracking of a particular vehicle or a person using a particular vehicle. This kind of warrant can be in place for up to 60 days, with the possibility of the Police asking the court to grant an extension to that time frame.
- Pursuant to the emergency powers authorised by section 48 of the Search and Surveillance Act for up to 48 hours without a surveillance device warrant.
- In circumstances where there is insufficient information to suspect an offence but Police reasonably believe there is a serious threat to the life or safety of any person or a serious threat to public health or public safety. The legal basis for this form of Individual VOI Tracking appears

to be an exception to IPP 2 ¹⁴, which supports the functions of the Police detailed in the Policing Act 2008, including “maintaining public safety”, “community support and reassurance” and “emergency management”. We understand the Police typically sets this form of ADC alert for an initial 48-hour period, with a subsequent review as to whether a further 48-hour period is justified.

Together these are referred to in this PIA as **Tracking Authorisations**).

Each of the Platforms has a different approach to the expiry of ADC alerts.

- The user interface of one of the Platforms provides buttons to set an ADC alert duration for either 48 hours, 30 days or 60 days (depending on the Tracking Authorisation). Platform ADC alerts commence upon clicking the button and automatically expire at the end of the selected duration. In addition, the original requestor may cease ADC activity at an earlier time by navigating to a “Stop Track” button in the Platform. This Platform also provides a user dashboard that enables Police users to see all current tracks they have initiated, though a search is required to find and stop any particular instance of Tracking.
- The other Platform enables Police users to create an ADC alert in the Platform and then to set it as “inactive” so as not to trigger alerts. Police users can also delete an alert. This process is not automated so it is up to the individual Police user to take the appropriate action and cancel an alert.

We understand the Police are currently in discussions with the Platform Providers to explore appropriate controls to restrict the duration of ADC alerts in the Platforms so they are in line with the relevant Tracking Authorisation. Ideally, the user interfaces of both Platforms would support Police users to:

- always enter the correct expiry dates as a default at the time the alert is created;
- ensure ADC alerts are kept up to date and stopped or deleted in line with the relevant Tracking Authorisation. It would be preferable if the Platforms could do this automatically rather than Police staff having to manually stop or delete those alerts. This would help minimise potential risks of Police staff forgetting or omitting to do so for whatever reason, resulting in potential unlawful tracking and privacy harms; and
- clearly understand how to set and delete ADC alerts in each Platform.

Stolen vehicle alerts

ADC alerts are also used in relation to the stolen vehicle list alerts referenced on page 10 of the ANPR policy. In this scenario, the Police receive automatic alerts from the Platforms when stolen vehicles are detected by Organisations’ ANPR systems.

¹⁴ IPP 2(e)(v) allows the Police to collect personal information from someone other than the individual concerned where that is “to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual”.

When a stolen vehicle is recovered, Police staff complete a form to cancel the stolen vehicle alert in NIA. We understand this cancellation then automatically feeds through and cancels the equivalent alert(s) in the Platforms.

ANPR policy position

At present there is nothing in the ANPR policy or SOPs that specifically addresses the expiry of ADC alerts in the context of the Platforms and the need to clear such alerts when they are no longer active.

While this is addressed in the context of Police-owned ANPR systems¹⁵, there is no similar guidance in the ANPR policy on ADC alert expiry dates in relation to the Platforms, even though expiry dates are equally as important in that context and particularly where Individual VOI Tracking is underway.

We recommend amending the ANPR policy to clarify that when using the Platforms, Police staff must always enter the correct Tracking Authorisation time frame when an alert is created in a Platform and that they are responsible for ensuring active ADC alerts remain valid in line with Tracking Authorisations and are cancelled upon expiry of the applicable authorisation, particularly until such time as suitable controls are established in both Platforms.

We also recommend updating the ANPR policy to clarify the legal basis underpinning the ability for Police to use ADC where there is a serious threat to life or health. We understand the legal basis to be an exception to IPP 2 in the Privacy Act, working in concert with the Police's defined functions in the Policing Act, but note this is not clear in the ANPR policy.

Rec-010: Continue discussions with the Platform Providers around implementing appropriate controls in the Platforms to ensure ADC alerts always align with the relevant Tracking Authorisations and update the ANPR policy to include explicit rules and requirements around the use of ADC alerts in the Platforms.

6.5 Data retention

IPP 9 states that agencies cannot keep personal information for longer than is required for the purpose for which it may lawfully be used. This is important to help reduce the risk of personal information becoming irrelevant, excessive, inaccurate or out of date. Good deletion practices also help minimise the risks of damaging data breaches. The Privacy Act does not, however, set out or infer any specific time limits for retaining personal information.

In the current circumstances, the IPP 9 data retention obligations apply to the relevant parties as follows.

¹⁵ Page 6 of the ANPR policy provides the following in relation to Police-owned ANPR systems only: *"For the subset of VOI alerts that form part of the VOI extract file exported daily for download to Police ANPR units as the basis for ANPR 'hits', expiry dates are critical to effective use of ANPR and mobile queries. VOI alerts that could trigger a real-time response must be kept up to date. It is important to clear VOI alerts when they are no longer active e.g., stolen vehicle recovered; offender apprehended etc. As a default, an appropriate expiry date for VOI alerts should be entered at the time the entry is made"* (emphasis added).

- **Organisations** are solely responsible for complying with IPP 9 in relation to ANPR data in the Platforms. As controllers of the data, they determine for how long such data may lawfully be retained in the Platforms.
- **The Platform Providers** – as processors – may only retain and delete such data in accordance with Organisations' instructions, including as detailed in their contractual arrangements.
- **The Police** are not responsible for determining when ANPR data hosted in the Platforms should be deleted. They are only responsible for complying with IPP 9 in relation to ANPR data collected from the Platforms and held within their own systems (e.g. NIA), which is outside the scope of this PIA.

Even so, we note that Police influence is likely to be significant in the context of both the Organisations' and the Platform Providers' ANPR data retention policy positions. As such, Police requests for access to ANPR data must recognise the need for retention limits overall.

The ANPR policy currently specifies the following retention limits in relation to Police access to ANPR data in the Platforms.

- Auror retains ANPR data in accordance with each Organisation's own privacy policies. "Any NPI retained by Auror is deleted after 60 days" (Appendix B). This appears to relate only to vehicles that are not VOIs.
- SaferCities similarly retains ANPR data in accordance with each Organisations' own privacy policies and such data is "currently retained for a period of 6 months" (Appendix C). Again, this appears to relate only to vehicles that are not VOIs.
- Police will not request any Organisation to retain NPI for longer than 12 months (p. 9). Presumably this is to tie in with the Police access and approvals process on page 10 of the policy, which provides a maximum time frame of 12 months.
 - We note the upper limit of the access and approvals process on page 10 of the ANPR policy (relating to offences that occurred 6 – 12 months ago) contradicts the position of the Platform Providers on deletion. If the Platform Providers do in fact delete ANPR data after 60 days/6 months, it is unclear how there can be any ANPR data available to access in relation to offences occurring in the past 6-12 months.

The ANPR policy does not currently address retention time frames for data relating to vehicles identified as being "of interest" to the Police or Organisations. We understand that one of the Platforms retains such information for two years where it is considered a VOI by either the Police or the Platform Provider's customers. The other platform retains such information indefinitely.

The Police should encourage both Platforms (and by extension Organisations) to develop appropriate retention and deletion time frames for Police access to VOI data, particularly in respect of the Platform that currently retains such data indefinitely. Those time frames should then be referenced in the ANPR policy to provide transparency around how long both VOI and non-VOI detection data is retained in the Platforms and visible to the Police.

Rec-011: Although only Organisations are required to comply with IPP 9 in respect of the retention of ANPR data on the Platforms, the Police should nevertheless establish a clear position around how long Police users can access ANPR data on the Platforms, including to encourage Platform Providers (and by extension Organisations) not to retain personal information for longer than is needed for Police purposes. Such retention time frames for Police users should be clearly reflected in the ANPR policy, both for records where a vehicle is - and is not - considered to be a VOI for Police purposes.

Appendix 1: Glossary

Term	Definition
ADC or Active Detection Capability	Use of the Platforms by the Police to receive real-time notifications of vehicles of interest detected by Organisations' ANPR systems. This functionality is referred to in the ANPR policy as "active detection capability", in the Auror platform as "Track a Vehicle" and in the SaferCities platform as "Plates of Interest".
ANPR	Automated Number Plate Recognition
ANPR data	Data collected by ANPR cameras, including number plate information, still images, video footage of the vehicle and its occupants, metadata (including a time and date stamp and the location of the vehicle in question) and vehicle details such as the make, model and colour.
ANPR policy	The Police ANPR policy that forms part of the Police "Instructions", along with the SOPs.
DPUP	The Government's Data Protection and Use Policy
Individual VOI Tracking	The ability for Police staff to use the Platforms to generate an alert and obtain the real-time location details of individual vehicles of interest (VOIs) in specific circumstances when the specified vehicle is detected by a camera on the relevant ANPR network.
NIA	National Intelligence Application
NPI	Number Plate Information
OCR	Optical Character Recognition, the software that powers ANPR systems.
Organisations	Organisations such as service stations, retailers, regional councils and public infrastructure owners that operate ANPR systems to collect ANPR data, which is then stored in the Platforms and is accessible by Police.
PbD	Privacy by Design
Personal information	Information about an identifiable individual
PIA	Privacy Impact Assessment

Term	Definition
Platforms	The third-party ANPR platforms operated by the Platform Providers
Platform Providers	Auror Limited (Auror) and SaferCities Group Limited (SaferCities)
Police	The New Zealand Police
Privacy Act	The Privacy Act 2020
Search and Surveillance Act	The Search and Surveillance Act 2012
SOPs	The Police Standard Operating Procedures in relation to ANPR data that form part of the Police "Instructions" on ANPR along with the ANPR policy.
Tracking Authorisations	The legal authorisation for any ADC activity, namely under a surveillance device warrant issued pursuant to the Search and Surveillance Act, using emergency powers authorised by section 48 of the Search and Surveillance Act or under an exception to IPP 2 in the Privacy Act where there is a serious threat to the life or health of any person.
VOI	Vehicle of Interest, specifically in this context in relation to stolen vehicles.

Appendix 2: Information gathering

Stakeholders interviewed

- Annabel Fordham, Chief Privacy Officer
 - Carla Gilmore, Manager: Emergent Technology
-

Documents reviewed

- "Automatic Number Plate Recognition – Privacy Impact Assessment", 2017.
 - Police Instructions – "Automatic Number Plate Recognition" (contains ANPR policy and SOPs)
 - vGRID SaferCity Platform – Police User Guide v2.10
 - vGRID SaferCity Platform – Police User Guide Lite – VAULT v2.09
 - Auror NZ Police Guidelines – September 2022
 - Notice to District Commanders and Directors about use of Auror and SaferCities, 22 November 2022
 - TenOne notice "Staff reminded to view refreshed ANPR policy", 28 September 2022
 - Signed Terms of Reference for audit of Police's use of ANPR platforms, 5 October 2022, Police Assurance Group
 - "New Zealand Police use of third-party Automatic Number Plate Recognition (ANPR) systems to search for and track vehicles", 29 November 2022, Crow's Nest Research
 - "Audit of New Zealand Police's use of Automatic Number Plate Recognition (ANPR) platforms, December 2022, NZ Police Assurance Group
 - "Independent privacy review of Auror's advanced ANPR functionality", 2020, Simply Privacy
 - Email correspondence between the Office of the Privacy Commissioner and the Police, dated 28 September; 2, 12 October; 10, 14 March 2023
 - Letter from the Police to the Office of the Privacy Commissioner, "Police use of ANPR – monitoring and auditing of access and use", 12 October 2022
 - Workshop "Using approved ANPR platforms – providing assurance of appropriate use"
 - Written responses from the Police to questions pertinent to this PIA.
-

Appendix 3: Summary of IPPs

IPP	Summary
1	Only collect personal information that is necessary for a lawful purpose
2	Collect personal information directly from the person concerned
3	Tell people why information is required, how it will be used, and who it may be shared with
4	Collect personal information in ways that are fair, lawful and not unreasonably intrusive
5	Take reasonable steps to keep personal information safe and secure
6	Let people access their information
7	Let people correct their information
8	Take reasonable steps to check personal information is accurate before using it
9	Keep personal information only for as long as it is needed
10	Use personal information only for the purposes for which it was collected
11	Disclose personal information only for defined purposes or where an exception applies
12	Take care when disclosing personal information outside New Zealand
13	Take care with unique identifiers

Appendix 4: DPUP principles

The Data Protection and Use Policy is based on following five key principles.

- **He Tāngata** - Focus on improving people's lives – individuals, children and young people, whānau, iwi and communities. This incorporates privacy concepts such as data minimisation, purpose specification, and the creation of positive outcomes from data use.
- **Manaakitanga** - Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information. This incorporates recognition of diverse cultural perspectives about data, and requires meaningful partnership with affected service users.
- **Mana Whakahaere** - Empower people by giving them choice and enabling their access to, and use of, their data and information. This incorporates privacy concepts such as meaningful transparency, consent, and subject access and correction rights.
- **Kaitiakitanga** - Act as a steward in a way people understand and trust. This incorporates privacy concepts such as data protection (security), accountability, and privacy breach notification.
- **Mahitahitanga** - Work as equals to create and share valuable knowledge. This incorporates sharing data in ways that decrease the burden on service users and ensure the best outcomes for people and their communities, and also ensuring that de-identified data can be used for research and evaluation (though note specific open data risks discussed below).

Appendix 5: Privacy by Design principles

The PbD methodology is articulated through seven clear and practical principles, which should underpin the way privacy is managed within any major project or programme ¹⁶.

- 1 Proactive not reactive, preventative not remedial**
Privacy needs to be considered early in the project lifecycle. Privacy considerations should help drive the design rather than being tacked on at the end to remediate apparent privacy risks.
- 2 Privacy as the default**
The default setting of any design should protect individual privacy. This means privacy-protective settings (such as data minimisation and use limitation) should be the starting point, with reductions in privacy protection introduced throughout the project lifecycle risk-assessed and carefully controlled.
- 3 Privacy embedded into design**
Privacy should be an ongoing and foundational element in the design of a product or process and should be so integral to that product or process that it will not function if privacy settings are altered or removed.
- 4 Full functionality – positive sum, not zero-sum**
Privacy requirements should not be delivered at the expense of other core functionality. This is not a trade-off. Instead, privacy requirements should support and enable the delivery of other requirements. The end goal is to achieve the project's objectives in the most privacy-protective way.
- 5 End-to-end security – lifecycle protection**
Data protection should be ensured at every stage of the information lifecycle for a new product or process, including collection, storage, use, disclosure, and disposal.
- 6 Visibility and transparency**
There should be visibility of the privacy risk assessments, design decisions and privacy controls established for a product or process. This will increase trust in the project. Trust is also built by ensuring appropriate, simple, and clear transparency about how personal information will be collected, used, or shared as part of the process.
- 7 Respect for user privacy – keep it user-centric**

¹⁶ Privacy by Design – The 7 Foundation Principles <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/>

Appendix 6: Algorithm Charter commitments

Transparency

Maintain transparency by clearly explaining how decisions are informed by algorithms. This may include:

- Plain English documentation of the algorithm
- Making information about the data and processes available (unless a lawful restriction prevents this)
- Publishing information about how data are collected, secured and stored.

Partnership

Deliver clear public benefit through Treaty commitments by embedding a Te Ao Māori perspective in the development and use of algorithms consistent with the principles of the Treaty of Waitangi.

People

Focus on people by identifying and actively engaging with people, communities and groups who have an interest in algorithms, and consulting with those impacted by their use.

Data

Make sure data is fit for purpose by:

- Understanding its limitations
- Identifying and managing bias.

Privacy, ethics and human rights

Ensure that privacy, ethics and human rights are safeguarded by regularly peer reviewing algorithms to assess for unintended consequences and act on this information.

Human oversight

Retain human oversight by:

- Nominating a point of contact for public inquiries about algorithms
- Providing a channel for challenging or appealing of decisions informed by algorithms
- Clearly explaining the role of humans in decisions informed by algorithms.