Waka Kotahi (NZ Transport Agency)

NZ Roading Network – CCTV, Automated Compliance and General Management System

A Privacy Impact Assessment

August 2022

Contents

CONTENTS **2**

EXECUTIVE SUMMARY **4**

1. BACKGROUND **6**

1.1 What is a Privacy Impact Assessment? 6
1.2 Scope of this PIA 6
1.3 Privacy Principles 8
1.4 Privacy by Design 8
1.5 Algorithms – Fair, Ethical and Transparent Use of Data 9

2. CAMERA SCRUTINY OF THE ROADING SYSTEM **11**

2.1 Key Objectives 11
Speed *11*
Distracted Drivers *11*
2.2 Camera Systems 12
Fixed Speed Cameras *12*
Mobile Speed Cameras *12*
Red Light Cameras *12*
Distracted Driver Cameras *12*
Special Vehicle Lanes Cameras *12*
Dual Red Light and Speed Cameras *13*
Average Speed Cameras *13*
2.3 What personal information is processed by Roading Management Cameras? 13
2.4 System Requirements 14

3. ANALYSIS OF POTENTIAL RISKS **15**

3.1 Governance, Accountability and Control 16
3.2 Internal Privacy Reporting 17
3.3 Privacy Policy 18
3.4 Collection Practices 19
Lawful Purpose *19*
Practical Purpose *20*
Necessity - Data minimisation *21*
Transparency *22*
3.5 Security and Storage 24
Technical Security *26*
Controls on Access to Personal Information *27*
Audit Capability *27*
3rd Party Relationships *28*
Guidance and Training *28*
3.6 Data breach handling 29
3.7 Integrity of Personal Information 30
3.8 Retention 32
3.9 Use, Disclosure, and Other Access 33
Disclosure Generally *34*
Individual's Requests *35*
Requests for Voluntary Release of Personal Information *36*
Regulatory Context *37*
Lifecycle of Information Context *38*
Risks *39*

4. CONCLUSION....41
ANNEXURE 1 – INHERENT AND RESIDUAL RISK MATRIX....43
ANNEXURE 2 - CANTERBURY NORTH CORRIDOR TRIAL....44
ANNEXURE 3 - DISTRACTED DRIVER / SEAT BELT COMPLIANCE TRIAL....46
ANNEXURE 4 - AUTOMATION OF VERIFICATION BUSINESS RULES. 49
ANNEXURE 5 – STAGE 2 SAFETY CAMERA ROLLOUT....57
ANNEXURE X – TEMPLATE....63XX

Executive summary

This report, a Privacy Impact Assessment (PIA), is an assessment of the privacy risks associated with the prospect of the New Zealand Transport Agency (*Waka Kotahi*) deploying an operating system, a variety of CCTV cameras and related tools to manage the NZ Roading Network from a safety, compliance and a general management oversight perspective.

The assessment focuses on a number of fundamental issues that may raise privacy concerns. These include privacy risk within the context of the obligations *Waka Kotahi* has under the Privacy Act 2020, including the Information Privacy Principles (IPPs), as well as globally accepted best business privacy practice such as expressed in the Privacy by Design principles.

After assessing the tools that might potentially be or have been deployed, the conclusion is that there are areas of risk that ought to be addressed. The report focuses on the system that will be engaged to manage roading management cameras, the personal information that they gather and the administrative processes that are required from research analysis to compliance. It also analyses the risks that arise for specific camera platforms that are or may become a part of *Waka Kotahi* road management strategy. Annexures have been added to the end of the report highlighting specific relevant issues that apply to a camera project. PIAs ought to be living document's that are capable of alteration to accommodate business or technical changes or advances that occur over time. PIAs should not be set in stone. This report aims to provide *Waka Kotahi* with a business artifact that can grow with the future deployment of roading managing camera systems and equipment over time.

The key points in the assessment are –

- Overall governance supported by established and regular assurance reporting is a prudent business process to ensure that the systems are controlled, remain controlled over time and protect both *Waka Kotahi,* staff and the public. It is recommended that *Waka Kotahi* views the roading management camera deployments as a national system that requires national senior management oversight.

- Defining *purpose* early in a project is a key enabler to define the extent or limits of the system and how the personal information collected can be subsequently used.

- Roading management cameras should only be deployed in a way that minimizes the extent of data required and collected.

- A strategy is required to ensure that good transparency exists around the overall deployment of roading management cameras. The areas of communication in this regard ought to include advice on the *Waka Kotahi* public website.

- Being transparent also requires consultation with key stakeholders in addition to the public. The Privacy Commissioner is a potential important contributor to the project on behalf of the community at large. Likewise, on a no surprises basis the Minister of Transport is an important stakeholder.

- Appropriate storage of the camera data will enhance the security of the personal information collected. Centralised *Waka Kotahi* infrastructure is desirable along with end to end and at rest encryption. Centralised storage will enable effective governance including audit and assurance reporting of the system.

- The personal information collected by the camera system is likely to be held in 3rd party systems for processing by *Waka Kotahi* staff. The personal information is not legally shared with the 3rd party and legally remains the sole responsibility of *Waka Kotahi*. Contractual terms with the 3rd parties must clearly reflect the responsibilities of *Waka Kotahi.*

- Training the staff involved in managing the data and the subsequent uses of the personal information, is an important aspect of deploying the systems, particularly in the context of using, sharing and disclosing information.

- Retention is an important consideration. The longer information is retained the more it potentially is exposed to risk. Retaining information unnecessarily also exposes *Waka Kotahi* the management burden.

1. Background

1.1 What is a Privacy Impact Assessment?

A PIA examines a change, project or system to evaluate how, and to what extent, it might impact on individual privacy. It is about identifying risks to the personal information that may flow through a system, business process or tool. This report identifies inherent risks pertinent to the *Waka Kotahi* circumstances. The assessment is about designing privacy into a project, to ensure that risks are identified early and processes, products and safeguards are designed with privacy in mind from the outset. It's about setting the right course early.

This assessment will help to avoid privacy pitfalls when deploying technology on the roading network, in particular CCTV and safety cameras, their related technical tools such as ANPR, and the system that will manage and store the information. Camera technology is deployed to enable *Waka Kotahi* to manage the roading system including operational, administrative and compliance activities.

This assessment should also be viewed as a living document, which ought to be revisited when new uses for cameras are contemplated, and when existing deployments are altered or used in different ways. This report includes assessment of risks associated with using a 3rd party technology systems to manage the information that is collected by the cameras.

The risks, recommendations and controls in this report ought to be considered in regular assurance reporting to evaluate if risks are managed and that controls remain effective. It ought to be a base line document for an appropriate governance group to regularly measure current deployment and practice and have confidence that the business continues to effectively manage the personal information that flows through the systems.

In the context of a 'living document' it has been created as a report that *Waka Kotahi* can use over time. Firstly, the report assesses roading management cameras and the system in a general way attempting to embrace all the potential issues that may arise from a privacy perspective. Secondly annexures are attached that focus on specific camera projects and identify risks in the report that are relevant or not for the camera systems. Where appropriate additional risks are identified.

Over time *Waka Kotahi* can amend this report to adjust its content according to changes in thinking, or new products that introduce new risk, or new camera tools by simply adding a further annexure.

1.2 Scope of this PIA

As a part of the Government's road safety strategy *"Road to Zero 2020-2030",* road safety cameras (roading management cameras) are deployed or will be deployed to deter excessive speed, inattentive driving and non-compliant use of the roading system. Roading management cameras with various aims are effective in keeping roads safe and enabling effective management of the roading system. Currently being used or under consideration are cameras that detect excessive speed or vehicles driving through red lights; point to point cameras that determine average speed over distance; cameras that detect vehicles using roads that are limited for example special transit lanes; and cameras that identify distracted drivers, for example those using mobile phones while driving.

This assessment analyses the *general* use of roading management cameras within the public spaces of the roading system and examines the risks inherent in their deployment. It also addresses the risks

associated with using 3rd party technology to store and process the information that flows from the cameras, acknowledging that at present a preferred provider has not been chosen.

Additionally, it recommends controls or mitigations that will eliminate or reduce the risks. This is the focus of the main assessment within the report. Building on the risks, recommendations and controls, examined in the general assessment we have assessed their further applicability to key projects. These are detailed within annexures to the report.

The assessment also considered the personal information issues that may arise for road users and *Waka Kotahi* . Risks are identified and quantified by reference to the *Waka Kotahi* risk matrix. In using its risk matrix we have attempted to be objective. We recommend that the project staff revisit our assumptions and bring an agency view to the risk assessment.

Recommendation 1: Undertake an agency risk workshop to qualify the risk assumptions made within this assessment.

Technical Security

This is not a review of the technical information security aspects. While information security is an important part of any privacy framework, it is a specialised part that requires separate and detailed consideration by information technology security experts. We understand that *Waka Kotahi* will conduct separate security assessments before systems are deployed.

To prepare this PIA we reviewed information provided by *Waka Kotahi*, including earlier risk assessments; business case documents; specification documents applicable to camera systems; system requirements documents, and *Waka Kotahi* risk guidance and matrix. Workshop meetings were completed with IT, legal staff and various project staff involved in the deployment of cameras and a camera system. We also reviewed *Waka Kotahi* corporate documents including the *Statement of Intent;* strategic documents and commentary about road safety and the Government's *Road to Zero 2020-2030* strategic aims. We also researched a range of international guidance for general principles relating to deployment and administration of the collected information.

Please note: In preparing this assessment, Simply Privacy has relied upon information, statements and representations provided to it by or on behalf of the *Waka Kotahi*. Simply Privacy provides no warranty of completeness, accuracy or reliability in relation to this information, these statements or these representations. Further the contents of this assessment are not legal advice, and should not be taken as such.

1.3 Privacy Principles

A PIA reviews a project through the lens of the Information Privacy Principles (IPPs) outlined in the Privacy Act 2020[1]. The IPPs regulate how agencies may collect, store, provide access to, use and disclose personal information. They provide agencies with a flexible roadmap for good privacy practice. They are designed to ensure that an agency can use personal information to achieve its lawful purposes efficiently and effectively, while protecting the privacy rights of the individuals the information is about. Although sourced from the Privacy Act, these IPPs reflect globally accepted best privacy practice, and provide an effective framework through which to assess privacy issues in the context of *Waka Kotahi* 's contemplated deployment of roading management cameras.

Summary of IPPs:

1. Collect only 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 and lawful particularly when children or young persons are the subjects
5. Take reasonable steps to keep personal information safe and secure
6. Enable individuals to access information about them
7. Enable individuals to correct their information if it is wrong
8. Take reasonable steps to ensure that 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 for defined purpose or where an exception applies
12. Take care when disclosing personal information outside New Zealand
13. Take care with unique identifiers

1.4 Privacy by Design

The Privacy Act and IPPs are complimented by the seven principles of Privacy by Design[2]. These aim to build privacy controls into systems, technologies and processes. If implemented correctly, individuals should not have to take any action to protect their privacy – the system's design achieves this by default. For *Waka Kotahi* , these principles can helpfully inform a process that facilitates good privacy outcomes, when deploying systems on the roading network. The principles are;

1. Privacy measures should be proactive not reactive.
2. Privacy should be the default setting.
3. Privacy should be embedded into design.
4. Aim for full functionality rather than viewing privacy in opposition to other interests.
5. Ensure end-to-end information security.
6. Promote visibility and transparency of risks and solutions, and
7. Make sure systems are user centric.

[1] Note that on 1 December 2020 the new Privacy Act 2020 came into effect.

[2] Privacy by Design – The 7 Foundation Principles https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

1.5 Algorithms – Fair, Ethical and Transparent Use of Data

Lastly in the context of heightened use of advanced technologies and the use of Artificial Intelligence, it is appropriate to consider the safe, fair and ethical use of technologies that process data. Where processes inform decision making and may have an impact on individuals, for example where road management cameras capture non-compliance that results in a sanction, it is appropriate to consider a set of principles that will inform the deployment.

At the encouragement of the Government a set of principles were jointly developed by the Chief Government Data Steward and the Privacy Commissioner to support safe and effective use of data and analytics[3]. These principles are reflected in a subsequent report delivered by Internal Affairs and Stats NZ in October 2018 - *Algorithm Assessment Report.*[4] *Waka Kotahi* is a signatory to the Algorithm Charter.

In summary the principles reflected in the Algorithm Charter recommend that the use of data and analytics:

- Must deliver clear public benefit – particularly where they support decision making
- Ensure data is fit for purpose – including accuracy and completeness
- Have a focus on people – recognising that deploying data analytics to process data and support decision making can have real-life impacts
- Maintain transparency – taking into account the views of stakeholders and ensuring that the deployment, use and management of the data and analytics are explained to the public, simply and clearly
- Understanding the limitations – avoiding bias, unfair or discriminatory outcomes
- Retaining human oversight – ensuring human judgement and evaluation remain an integral part of the decision making

Together the three frameworks provide legal and best practice guidance on the issues to be considered when creating and deploying systems that collect and use personal information. They have been paramount in this assessment and analysis of the general and specific deployment of roading management camera systems on the roading network.

The assessments covers the deployment of roading management cameras in the context of the lifecycle of personal information that will be generated within the various options available to *Waka Kotahi* . Key considerations are,

- ***Governance*** of the ongoing deployment and management of roading management cameras and the technical system

[3] *Privacy Commissioner and Stas NZ – May 2018* - 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

[4] https://www.data.govt.nz/assets/Uploads/Algorithm-Assessment-Report-Oct-2018.pdf

- Examination of collection practices including the ***purpose***, ***transparency*** and ***fairness*** of the collection (IPPs 1-4)
- General ***Security and storage*** of the personal information including appropriate guidance and training (IPP 5)
- Individuals' ***access*** to the information about them (IPP 6)
- Information is **accurate, complete and not misleading** before it is used or disclosed (IPP 8)
- ***Retention*** of the information (IPP 9)
- General ***use and disclosure,*** statutory and ***other access*** requests for the information (IPP 10 & 11)

2. Camera Scrutiny of the Roading System

2.1 Key Objectives

A safe roading system is an essential focus for the Government's road safety strategy *"Road to Zero 2020-2030".* It aims to meet the Government's vision to have a roading system in which there are no deaths or serious injuries (DSIs) on the roads. Launched in 2019 it aspires to influence 5 areas including speed management. Introducing automated oversight of the roading system is an aspect of the *Waka Kotahi* strategy and includes deploying or exploring the potential to deploy roading management cameras to effectively manage limited use roads such as 'transit lanes' for vehicles with more than 1 occupant; speed and red light cameras; cameras that detect point to point average speed between two points; and, cameras that detect potential distracted drivers, for example those using mobile phones while driving.

Speed

Waka Kotahi reports that the single biggest road safety issue in New Zealand today is speed – drivers travelling too fast for the conditions. Speed affects all crashes. It can be a factor in causing them and it has a direct effect on the damage done in a crash. It is clear from the crash statistics that many people underestimate how changing conditions, such as wet weather, can increase road risk. In 2019, speeding was a contributing factor in 73 fatal crashes, 408 serious injury crashes and 1,457 minor injury crashes[5].

Studies reveal that the number of crashes is substantially reduced when speed cameras are used. A study of crash data in the 20 months following the introduction of speed cameras in New Zealand in 1993 found a 23% reduction in fatal and serious crashes at urban speed camera sites and an 11% reduction in fatal and serious crashes at rural speed camera sites.

International experience shows that speed cameras are a highly cost-effective speed management tool. This means they save a lot of lives for the cost of putting them in place and operating them. In consultation with roading stakeholders speed cameras are sited on stretches of road with a number of risks factors to road users.

Distracted Drivers

Waka Kotahi also reports that driver distraction can significantly increase the likelihood of a crash or near-crash. Distraction occurs when a driver's attention is diverted away from concentrating on driving, towards competing events, objects or people.

In 2019, driver distraction was a contributing factor in 10 fatal crashes, 133 serious injury crashes and 918 minor injury crashes.

[5] Waka Kotahi website

2.2 Camera Systems

There are a range of road safety cameras currently in use by Police and regional authorities. They include -

Fixed Speed Cameras

Fixed speed cameras are a familiar deployment on the roading system and currently managed by Police. They are used to measure the speed of vehicles at a specific location (travelling to or away from the camera), identify which lane they are travelling in and differentiate between vehicles such as heavy trucks and cars which have different speed limits. An infrared flash enables number plate information to be captured in the dark.

Mobile Speed Cameras

Mobile speed cameras are currently deployed by Police and can be housed inside a van and/or trailer, allowing the cameras to be mobilised to roading areas of risk. They work in a similar fashion to fixed safety cameras but due to their lower deployment costs and ability to rotate around sites, they are suited to address a wider range of risks, including seasonal and temporary risks. Police currently manually transfer data into their system but the future state for *Waka Kotahi* is likely to be automated.

Red Light Cameras

These static cameras are used to capture vehicles running a red light. Vehicles are tracked as they approach the intersection. If a vehicle crosses the stop line during a red-light phase, a camera photographs the rear of the vehicle. These are currently deployed by local authorities and Police in urban areas. The cameras also record vehicle speed near and at the controlled intersection, recording still and video images.

Future camera options may include –

Distracted Driver Cameras

A specialised set of cameras that captures high-resolution images of the vehicle, driver and registration plate. The images can be used to provide evidence that a driver is using a mobile phone.

Special Vehicle Lanes Cameras

Special Vehicle Lanes (SVL) are designed to encourage road users to either defer to public transport or pool their private vehicles so that travel is undertaken with multiple occupants, that is a High Occupancy Vehicle (HOV). Dedicated lanes are provided for HOVs only. Road management cameras can be deployed on these lanes to ensure that road users are complying with the permitted use of the particular lane. The lanes may be bus only lanes or limited to use by vehicles that have a specified minimum occupancy.

Similar to the distracted driver cameras a high-resolution image will be taken of vehicles providing potential evidence of a vehicle in the wrong lane or a vehicle that has less than the minimum occupants. The aim is to monitor SVL to improve network performance and encourage road user

compliance. The monitoring may be accompanied by an enforcement regime that infringes drivers using a HOV lane without the requisite number of passengers.

Dual Red Light and Speed Cameras

in addition to red-light running, the speed of vehicles travelling through the intersection is also captured, enabling speed offences to be issued irrespective of the light phase. Dual red-light/speed safety cameras have a higher reported effectiveness at reducing deaths and serious injuries at intersections than red-light safety cameras alone.

Average Speed Cameras

Average speed cameras (sometimes called a point-to-point camera) calculate and record a vehicle's average speed between two points along a stretch of road, providing an accurate reading of whether drivers are speeding over a sustained distance. Infringements are only issued if the average speed over that entire distance exceeds the legal limit.

Overseas experience shows a significant reduction in the number of infringements issued where these cameras are deployed, along with sustained safer speeds on the road network. They have a track record of saving lives in Australia, the UK and Europe. A UK study found fatal crashes on targeted roads reduced by 46% in three years after implementation.

Waka Kotahi believes these cameras are potentially a very effective way to improve safety in areas where speed driving puts others at particular risk. Identifying sections of the roading network marked as average speed zones and publicity about the zoning, gives road users the opportunity to moderate their speed, avoid fines and overall contribute to safer roads.

2.3 What personal information is processed by Roading Management Cameras?

It is useful to understand the nature of the personal information that will be acquired and used in any new project. More sensitive or intrusive information will require more careful management. Under the Privacy Act, personal information is defined as 'information about an identifiable individual'. This is an expansive definition and encompasses information which on the face of it may not be immediately identify a specific individual, but which, if combined with other pieces of data, may result in the identification of an individual.

Broadly considered, roading management cameras, the speed recording device, the optical character recognition software commonly referred to as Automatic Number Plate Recognition (ANPR) and the contiguous business system, collects and stores personal information about road users' behaviour in public spaces on the roading system. The potential types of personal information include:

- still photos and video footage of a vehicle that captures an aspect of the driver and/or passenger that may identify that person, the colour and potentially the type of vehicle plus the number plate information for the vehicle
- images of the registration number of the vehicle which may lead to identifying the registered owner of the vehicle
- images that capture the side of the vehicle and displays the occupants in sufficient detail to enable a count of occupants

- images that display the thermal images of occupants within vehicles
- images that identify behaviour of an individual such as use of a telephone or the absence of a seat belt
- meta data that includes time, date and location of images and direction of travel

Where the system is used to enforce road laws, such as speed or other contraventions, the original images form the basis of the evidence that may be produced in court. In these circumstances the original recorded images are stored digitally and cannot be overwritten or altered. All images and relevant information (such as time, date and location) are encrypted.

Although cameras and recording devices are ubiquitous in our society, these tools are viewed as intrusive and potentially generate emotive commentary alleging unwarranted surveillance systems. In addition, compliance cameras may result in a detriment to individuals. Consequently, people may feel uncomfortable at the prospect of their images or behaviour being captured by video and other means despite the information being acquired in public places where the expectation of privacy is significantly reduced.

Considering the Privacy Act wide definition of personal information, it will be very difficult to argue that the information collected through camera surveillance in a public place, involving the use of people's motor vehicles is not personal information. It would also be difficult to argue against potential public perception that *Waka Kotahi* is collecting information about them. Semantic and competing legal views and arguments aside we encourage *Waka Kotahi* to view information acquired in the road management camera system as 'personal information" and subject to the Privacy Act.

2.4 System Requirements

Following a Cabinet decision to transfer the existing road safety camera system from NZ Police to *Waka Kotahi,* a new technology system will be required to enable *Waka Kotahi* to both absorb the existing road safety camera structure from NZ Police and accommodate new structure introduced by *Waka Kotahi*. Over the next 10 years it is intended to expand the road safety camera system to approximately 800 fixed site and mobile cameras. Cameras will be more visible, with fixed cameras clearly signed, and mobile cameras used in a more covert, general deterrence mode. High-risk sites will be chosen based on historical data about harm and modelling of underlying risk factors.

Waka Kotahi will deploy and manage the operation of the cameras including the processing of offences. The stated strategy for the deployment of roading options includes to educate, engage and where appropriate enforce using a regulatory style that aims to reduce 'death and serious injury' events on the roading system.

Waka Kotahi estimates by 2030 it will be processing around 3 million infringements annually, and their processes and technology will be capable of issuing these infringements close to real-time. Prosecutions are likely to increase to around 3300 annually. An estimated 400+ full time staff will be required to manage the system and its information flows from collection through to prosecution.

Waka Kotahi intends to acquire appropriate 'as a service' technology platforms that maximises efficiency and automation and meets security and privacy standards. Camera management will be automated, with images transmitted securely through the mobile and physical data networks. While aiming where possible for incident verification that is largely automated through the use artificial intelligence, *Waka Kotahi* acknowledges the need to strike a balance between efficiencies and maintaining the public's trust and confidence in the system. This will mean a balance between automation and maintaining viable human oversight. At the time this assessment has been made a technology platform and provider had not been engaged.

As part of its obligation under the Privacy Act to inform people about the use of road safety cameras and the collection of personal information *Waka Kotahi* intends targeted campaigns explaining the purpose and promoting the role of safety cameras. The public advice will be supported by the Road to Zero public awareness campaign that aims to increase awareness and understanding of the Safe System approach underpinning Road to Zero. In time *Waka Kotahi* aims to achieve a recognisable social licence for safe system interventions.

Sharing data from the road safety camera system will be a necessary and appropriate function of the new system. For example providing the Ministry of Justice with relevant information to complete the justice process for infringement notices, the collection of unpaid infringement fines and engage in prosecutions.

Road policing activities will continue to be coordinated through the Road Safety Partnership with NZ Police. It is intended through timely sharing of information from roading management cameras e.g. verified infringements/traffic charges, high risk driving events, police officers would continue to have a connected view of the roading system to enable effective roadside conversations and decision making about driver compliance.

3. Analysis of Potential Risks

As mentioned earlier this assessment is undertaken by reference to the general requirements of the information privacy principles (IPPs) in the Privacy Act, as well as Privacy by Design and data analytics principles. This has resulted in the identification of a number of inherent privacy risks. The assessment is completed in the context of a preferred system provider not yet determined and not all camera options available or deployed. In the main part of the report, we have detailed recommendations for action and suggested controls that will reduce inherent risk for a potential technology system and all camera systems in general. The recommendations will assist with the technical configuration and controls and contractual terms and conditions with any potential software or service provider.

3.1 Governance, Accountability and Control

The *Waka Kotahi* national roading management camera systems must be governed in a way that ensures effective privacy oversight, clear accountability and ownership and real control over personal information.

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

Effective governance is also a requirement within the Government's expectations articulated within the *Privacy Maturity Assessment Framework (the Framework)* which *Waka Kotahi* reports on annually. The *Framework* measures agency performance against core expectations which are influenced by the *Data Protection and Use Policy*[6]. Performance is characterised ranging from a low 'informal" approach through "foundational" to "managed". Among the core expectations is a Leadership section which expects privacy risk management to be integrated and include monitoring and reporting to a governance group that is "reasonably confident" that the agency's privacy risk is managed. Adequate governance performance is unlikely to be achieved without effective risk and assurance processes and reporting within a '3 lines of defence' reporting model[7].

When privacy issues are taken seriously and championed at senior levels, frontline staff are more likely to recognise and if necessary escalate privacy concerns. Establishing and promoting a strong privacy governance framework for the information system forms part of an agency's wider risk management culture.

Recommendation 2: Identify a national governance and assurance structure for the national deployment of roading management cameras that includes regular oversight and assurance reporting.

Not unusually in both the public and private sector the practice of creating and deploying digital frameworks often falls to the IT capability within the agency. Following deployment there is often a

[6] See Digital.Govt.NZ commentary at https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/data-protection-and-use-policy-dpup/

[7] The Controller & Auditor General's view can be found here https://oag.govt.nz/good-practice/audit-committees/what-works/three-lines-of-defence
See the views of the Institute of Internal Auditors here https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

vacuum around agency oversight of the business process and information flows that are created as a result of the technical solution. Technical staff continue to maintain the effectiveness of the technical tool and by default may also be expected to manage the data that flows within the system, although not specifically tasked to that role and responsibility. In our view this is a critical fault in the management of data, in this case personal information.

In addition, in agencies that have national footprints, projects are often delivered on a regional basis with little connection between deployments that are the same or similar.

In discussions with *Waka Kotahi* staff during the assessment of roading management camera systems in general it became apparent that there is little or no national oversight of the camera systems. Evidence of that is apparent in the disassociated manner in which various road management camera products have been viewed and assessed. For example there have been separate 'privacy impact assessments' and 'privacy threshold assessments' for a range of deployments including; ANPR to monitor special lanes (2017); ANPR Weigh Right for commercial vehicle compliance (2018); ANPR journey time calculations on the Christchurch Northern Corridor (2020); and ANPR to detect distracted drivers (2020). There are likely others. These projects and deployments are remarkable for their similarities rather than their differences. Each of these efforts essentially recreates the wheel in terms of risk and mitigation and while there is no criticism of the assessments they are a duplication of effort and likely a product of a lack of centralised senior oversight.

In the context of creating both a 3rd party technical system to manage the information gathered from roading management cameras and deploying various camera systems, it is crucial that *Waka Kotahi* has adequate governance in place to create the best oversight of what will become a significant work stream.

Waka Kotahi must identify a national governance group to take responsibility for data governance in the roading management cameras context and setting the related privacy policy. The governance group should be accountable for assessing the effectiveness of the privacy controls in place around the system and camera deployment by establishing risk assessment expectations and regular assurance reporting. The assurance reporting should at least include post deployment reviews that show that recommendations made to reduce risk are accepted (or not) and controls are established. Overtime the reporting should provide assurance both to *Waka Kotahi* management and the public that the systems remain safe and the controls continue to be effective.

An effective governance group, and clearly assigned accountabilities will be crucial in ensuring proper privacy protections are in place around the growing roading management camera deployments along with the growing responsibility to manage the personal information that flows through them.

Privacy is everyone's responsibility. Both governance and operational users of the systems should take on information practices and responsibilities that reflect the nature of the relationships involved and the amount of strategic or operational influence they hold. At the top level, privacy responsibilities focus on setting tone and direction and ensuring overall accountability for risk. At the end user level, privacy responsibilities focus on day-to-day risk identification and management. Between these levels, strong communication (assurance reporting) is important – with risk and breach reporting being communicated up the chain and guidance and expectations moving down the chain.

3.2 Internal Privacy Reporting

Recommendation 3: Develop a privacy reporting agenda for the roading management camera system Business Owner and service providers to report regularly to the governance group.

To ensure strong accountability, privacy must be a regular topic of discussion at the strategic and/or executive level. An active three lines of defence assurance model would require both the Business Owner, operational group and the 3rd party service providers, report regularly to the governance group about privacy matters. A regular reporting agenda, covering areas of significant privacy risks, would ensure that those matters remained highlighted as governance priorities. It should be noted that there is likely to be significant overlap between areas of privacy and security priority.

Matters for the agenda could include:

- Whether any privacy (or security) breaches had occurred
- Whether internal or service provider system audits had identified any inappropriate access or use of personal information
- Whether security assurance plans are being implemented appropriately
- Outcomes of any independent certification or audits of the service provider
- Confirmation that controls identified to manage privacy and security risks remain in place and fit for purpose.

3.3 Privacy Policy

Recommendation 4: Create a plain English informative privacy policy for the roading management camera system and ensure it is understood by all system users.

The insider human factor is perhaps the greatest risk in any system. With determination, most system protections can be manipulated or bypassed. System protections must therefore be supported by clear privacy policy, which establishes the expectations and obligations on system users.

A plain English privacy policy or system guidance is an essential part of the privacy framework and should provide system users with high-level principles that govern system access and the use and disclosure of information.

The roading management camera system privacy policy should briefly outline:

- The system's primary purpose,
- Staff access limitations - reinforcing that staff may only access, use or disclose information for legitimate role-based purposes.
- Information security requirements - particularly in respect of the transfer of personal information between systems or for reporting purposes.
- Information retention requirements

It is recommended that the system display a summarised privacy policy to staff when accessing the system, by way of a warning or reminder of the obligations when entering and using the system and the information.

A formal privacy policy is valuable in inducting new staff, providing background for third party service provider staff, and informing the governance group.

Without adequate governance *Waka Kotahi* runs the risk of project and deployment risks not being adequately implemented and monitored over time and not being in a position to demonstrate

adequate stewardship of the road management cameras and system. If identified risks within the road management camera systems are not controlled or mitigated it is *likely* that at a national level *Waka Kotahi* will suffer scrutiny and reputational damage. Technology systems such as CCTV and surveillance type systems are of considerable public interest. Risk to personal information that flows through the systems may also result in harm or other detriment to individuals. This may result in limitations or an inability to deploy road management cameras with a resultant negative impact on the Road to Zero programme. Without controls the inherent risk is *high.* Implementing active governance accompanied by a '3 lines of defence' assurance reporting model and effective policy or guidance reduces the likelihood of harm to individuals and to *Waka Kotahi* to *unlikely* and the consequences to *moderate or minor* resulting in a residual risk of *low to medium.*

Governance Risk Profile – R2, R3 & R4
Inherent risk rating – High
Residual risk rating – Low/medium

3.4 Collection Practices

The key risks that arise in collection processes include the requirement to establish a lawful *purpose*, promoting *transparency* and ensuring the collection is *fair*. (See IPPs 1 – 4; and the Principles for the safe and effective use of data and analytics).

The use of roading management cameras and the collection of personal information should have a well-defined purpose at an early stage in project and well before deployment

***Waka Kotahi* must ensure that personal information that is collected within a roading management camera system is:**

Collected for a lawful purpose connected with its functions or activities, and

Only collected when necessary for that purpose; and

Not used to collect individuals identifying information where it is not necessary for the purpose. (IPP 1)

Lawful Purpose

Recommendation 5: Acquire a legal opinion on the lawfulness of collection of personal information in the context of the deployment of roading management cameras.

Purpose is an often overlooked or underdone issue when considering deploying a new system or tool. Collection by an agency is expected to be for a lawful purpose and the manner of collection also needs to be lawful (see IPP 1 & 4).

While roading management cameras are deployed in public spaces, where expectations of privacy are significantly reduced, establishing a lawful basis for their deployment is an important first step in approving the use of the tool. Where the deployment is meeting a statutory obligation to detect, prosecute and deter unlawful behaviour on the roading system the lawfulness of the collection is likely to be legislatively obvious.

In addition, the use of roading management cameras to broadly assess road users' behaviour, conduct research or acquire statistics are also permitted activities under the Privacy Act.

However, where new uses of technology arise it is appropriate to reconsider their lawfulness. For example, establishing the lawfulness of collecting information through the camera system about distracted drivers, seat belt compliance and vehicle registration. There is an inherent risk that someone will *possibly* question the lawfulness of the deployment of a new use of a roading management camera. Without a lawful basis for the deployment the consequences could be *moderate* to *severe.* The inherent risk would be *high* to *critical.* Examples of roading compliance errors have often arisen in the local authority context where roading obligations have not been published in the *Gazette* and therefore not able to be enforced.

We recommend that a legal opinion is acquired, particularly in the deployment of new camera options, to provide assurance to *Waka Kotahi* and if necessary, the public, that the full potential use is lawful. Being able to explain the *Waka Kotahi* lawful use of roading management cameras and using the opinion as the basis for transparency may result in critical questioning being *unlikely.* Establishing lawfulness will avoid potential unnecessary questioning or negative perceptions of surveillance and reduce the consequences to *minor*. The resultant risk would be *low.*

Lawful collection Risk Profile – R5
Inherent risk rating – High
Residual risk rating – Low

Practical Purpose

Recommendation 6: Establish at an early stage the primary and directly related purposes for using a roading management camera system and collecting personal information.

Waka Kotahi has focused on the safety benefits of roading management cameras. This is an entirely defensible and responsible approach to the task of making our roads safer. However, there are other aspects of the collection of personal information that will serve other related purposes. While the collection IPPs require a lawful purpose, the ability to use or disclose information is permitted when the activity is within *the purposes or directly related purposes for collecting the information*. In this context it is appropriate to identify the reasonably foreseeable purposes for which the information will be used. For example, it is highly likely that the ultimate deployment of roading management cameras will result in prosecution actions with the potential for the information and images to be evidence in Court processes or procedures. It is also defensible that the information acquired from the system will be used to continually review the best places to establish cameras or test whether the service delivery around the process is efficient and effective.

In some cases, the deployment of a roading management camera may take the form of a trial or 'proof of concept'. The initial purpose may be to decide whether the technology is viable and beyond that whether it may be deployed to ascertain if there is roading behaviour that needs monitoring. It may be that it is desirable that a lawfully deployed system is capable of a corollary application that enables research into road use.

However, well-defined intentions about purpose at the outset will enable clarity for *Waka Kotahi* when deploying roading management cameras and when considering the limitations on use of the personal information. The exercise of defining purpose at an early stage in the project enables the collected

personal information to be managed appropriately. For example, by contributing to the policy, guidance or assurance reporting around storage, security, use and retention of the personal information.

There is a risk that if the purpose for roading management cameras is not clearly defined at the outset of the project it is *possible* that subsequent uses of the footage may be unlawful or perceived unlawful. It is also *possible* that staff may misunderstand the consequences of using the equipment outside of the expected purpose and the public may not fully comprehend the way in which the information is used and disclosed. The resultant consequences may well be no greater than *moderate* but may mean that the use of roading management cameras becomes untenable due to public perceptions; media attention about their deployment; the safety aspect of their deployment is not achieved; and the trust and confidence in *Waka Kotahi* is impacted. The inherent risk would be *medium*.

The remedy is to clearly define purpose for the collection of personal information at an early stage in the project. An established purpose statement will assist with other aspects of the management of the collected personal information.

Defined purposes for deploying roading management cameras will help demonstrate the *Waka Kotahi* limits on the collection and use of personal information. By establishing a defensible purpose about the deployment and use, the likelihood of unwarranted scrutiny of the project remains *possible* while the consequences are potentially reduced to *minor or insignificant* resulting in a residual risk of *low/medium.*

Practical Purpose Risk Profile – R6
Inherent risk rating – Medium
Residual risk rating – Low/medium

Necessity - Data minimisation

The collection of roading management camera data should be designed to only collect personal information that is necessary and proportionate to the purpose for deploying the system

***Waka Kotahi* must not collect personal information that is:**

Unnecessary and disproportionate to the purpose for the collection.

Identifying data that is not required for the purpose for the collection (IPP 1).

The principles in the Privacy Act also require that personal information is collected only when necessary and proportionate to the purpose (IPP 1). The new Privacy Act 2020 now has an additional provision in IPP 1 prohibiting the collection of individuals' identifying data when it is not required for the lawful purpose. Globally this is frequently referred to as data minimisation, a term borrowed from the language of the European Union's General Data Protection Regulations (GDPR).

Deploying proactive data minimisation practices also reduces the risk to information when it is held in agency systems. Unnecessarily collecting and holding personal information exposes the information to risk that may harm the individuals it is about and affect the reputation of the agency.

Recommendation 7: Establish policy or guidance for each targeted deployment of roading management cameras, that prescribes data minimisation so that collection of unnecessary personal information is eliminated.

In the roading management camera context data minimisation ought to be considered when deciding on the technical and practical controls around what is captured and collected by cameras. It is also an exercise to accommodate a holistic purpose for deploying a roading management camera system for example, speed cameras generally or lane management cameras generally as opposed to individual cameras or individual geographical locations.

In the law enforcement context, a greater level of personal information is required to be collected to support the infringement process. However, in the context of road use analysis, such as establishing journey times within a particular section of the roading system, limited or no personal information may be required to complete the analysis. Policy or guidance ought to prescribe the required and relevant information to accomplish the stated purpose.

Collecting the same level of data for a general roading system analysis as that required for a law enforcement purpose risks acquiring personal information that is unnecessary and disproportionate to the purpose of deploying the roading management camera. Failing to minimize the personal data necessary to achieve the stated purpose of the deployment will result in an *almost certain* unnecessary collection of personal information. The consequences are likely to be *moderate* with potential ongoing media interest, political concerns, and some loss of reputation for the *Waka Kotahi.* The risk may also put the viability of the project at risk. The inherent risk profile is likely to be *high.*

In general, cameras deployed for law enforcement purposes will at least require images and meta data that includes time, date and place of the event, speed of the vehicle accompanied by sufficient detail to prove the identity of the offending vehicle. Number plate, colour of vehicle and perhaps vehicle badges identifying the make of the vehicle may be captured. Collecting this extent of data in the context of general roading analysis would be an over collection of personal information.

In the context of roading management cameras there will be a technical ability to reduce or potentially eliminate the collection of personal information. For example, the collection of 'real-time' journey times for the purpose of advising road users of expected journey times when entering a roading system, can be achieved without the ultimate collection of any personal information by limiting what is collected and anonymizing the data for analysis.

The combination of establishing a clear purpose for the deployment of roading management cameras and setting policy expectations around data minimisation are likely to deliver assurance that personal information will not be over collected. The existence of clear policy and guidance will also assist *Waka Kotahi* in its defence of the use of the technology. It is also likely to ensure that the technology is considered a benefit and reduce actual or perceived systems risks to *unlikely* and the consequences as *minor* resulting in a residual risk to *Waka Kotahi* of *low*.

Necessity/data minimisation Risk Profile – R7
Inherent risk rating – High
Residual risk rating – Low/medium

Transparency

The practice of collecting personal information within the roading management camera data systems should be fully publicly acknowledged unless reasonable grounds exist not to do so

***Waka Kotahi* must ensure that in respect of roading management camera data that is personal information it:**

Takes reasonable steps to make individuals aware that their information is being collected, the purpose of the collection and how it will be used and shared (IPP 3)

Recommendation 8: Implement a transparency strategy to cover the deployment of a roading management camera system including comprehensive advice through appropriate agency channels.

It is noted that the current aims include broad campaigns to advise the public about cameras and their use for detecting non-compliance on the roads; targeted messaging directly to road users and the frontline staff working with customers to educate towards compliance. An important addition to these activities is comprehensive advice on the agency website. *Waka Kotahi* has an exemplar in the Tolling System's public facing advice on the website.

Informing the Public

IPP 3 requires an agency, when collecting personal information, to take reasonable steps to advise an individual client about the circumstances of the collection. The usual focus in this regard, when circumstances permit, is to advise people at the time of collection. Where this is not practicable advice might be provided in corporate documents, publishing guidance and advice on agency websites and in the case of roading management cameras, developing signage on the roading system. While the focus of IPP 3 is on notifying the individual from whom information is collected, good business practice requires a wider consideration of advice to the public in general and consultation with key stakeholders.

There are also exceptions to the transparency requirements that may have a bearing on the deployment of some camera systems. The most relevant are,

- where transparency would result in a prejudice to the prevention, detection, investigation, prosecution and punishment of offences, and
- where the information is to be used in an anonymised way for statistical or research purposes
- being transparent would prejudice the purpose of the collection.

An example of the latter exception would likely arise where a trial to ascertain road user behaviour would be prejudiced by telling the public where a particular camera was deployed or informing of a trial where the fact of the trial would disclose the location of the cameras.

The Privacy Commissioner provides useful advice on best practice to accommodate transparency in the deployment of CCTV.[8] The advice suggests an agency "collection" or "privacy notice" that informs the public of the circumstances of the collection including the purpose and the uses for the personal information. This ought to be at least published on the agency website. It also recommends signage where appropriate along with proactive media strategies around the deployment.

Stakeholders

The public at large is a key stakeholder and transparency can be managed as mentioned above. But there are other key stakeholders that ought to be considered.

[8] https://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf

An important stakeholder is the Office of the Privacy Commissioner. As the public's overseer of privacy issues, consulting with the Privacy Commissioner may potentially elicit additional advice about best practice in the context of technology deployment. Further the Privacy Commissioner may be able to provide public support for the agency's deployment if the project is publicly questioned.

Lastly, it will be important to consult with the Minister of Transport who may also publicly support the project and contribute to the public's trust and confidence in *Waka Kotahi.*

There is risk in not establishing comprehensive transparency processes and advice about a project that deploys roading management cameras and allied technology such as ANPR. In addition, clear advice about how the system behind the cameras works will contribute to trust and confidence that the whole system is integrated and has a defined and established purpose. In the absence of robust community advice, it is *likely* that the project will be called into question by the media, the public and potentially the Privacy Commissioner. There is a current heightened public and media interest in new technologies, particularly when deployed by public sector agencies. Of particular interest is the deployment of technology that incorporates artificial intelligence, machine learning or algorithms. The public attention is likely to result in complaints to the Privacy Commissioner, and potentially negative or inaccurate media coverage. The impact is likely to be at least *moderate* with the inherent risk sitting at *high.*

Initiating a comprehensive transparency strategy around roading management camera use is likely to get ahead of negative public comment or perceptions and reduce the risk to *unlikely but possible* providing *Waka Kotahi* introduces comprehensive advice and consultation about the project and its later deployment. With adequate attention to transparency requirements the impact of the deployment of roading management cameras is not likely to exceed *moderate* but more likely to be a *minor* impact with a residual risk profile of *low/medium.*

Transparency Risk Profile – R8
Inherent risk rating – High
Residual risk rating – Low/medium

3.5 Security and Storage

The roading management information storage should be designed with strong security protections around its systems and processes to ensure that personal information is used only for its legitimate purpose.

***Waka Kotahi* must ensure that in respect of roading management camera system data it:**

Takes reasonable steps to protect the personal information it collects against loss, misuse and unauthorised access, use and disclosure (principle 5)

Uses personal information only for the purposes for which it was collected (principle 10)

Does not disclose personal information unless it was collected for the purpose of that disclosure or an exception applies (principle 11)

The camera system data held in the various digital storage arrangements will include personal information. *Waka Kotahi* should implement a suite of measures to ensure that where ever

information is held whether on premises or in a cloud solution, it is held securely and protected against misuse.

The adoption of a camera system and the use of 3rd party service providers for software and storage, requires *Waka Kotahi* to share capability for and control over the systems and information with its subcontractors.

The Privacy Act provides that an agency may disclose personal information to a foreign person or entity only if it has reasonable grounds to believe that the information will be subject to safeguards comparable to those required by the Privacy Act[9]. In the context of the road management camera system the transfer of information to a service provider and cloud service will not involve a disclosure or sharing as neither will be using the information for their own purposes but holding and processing on behalf of *Waka Kotahi.*

However, the Privacy Act is clear that where an agency engages 3rd parties to store and process personal information on its behalf, the agency remains solely responsible for the personal information involved[10]. This will be the nature of the relationship that *Waka Kotahi* is likely to have with a 3rd party service provider. Clear expectations with 3rd parties will be needed to ensure that they do not use or disclose information for their own purposes; that they report privacy breaches to *Waka Kotahi* promptly; and, that they provide levels of security commensurate with the expectations of *Waka Kotahi.* In essence all of the security controls that *Waka Kotahi* ought to require, ought also to apply to the 3rd party including limits on its staff access to personal information. *Waka Kotahi* must ensure that it is satisfied with a 3rd parties management of its information, including:

- clearly articulating its requirements for the handling of information, and
- entering into appropriate agreements outlining respective responsibilities

The potential for a cloud services provider to be based in an overseas jurisdiction requires consideration of the risks that might arise in that jurisdiction if personal information is stored there. The jurisdictional risks arise where personal information is subject to the laws of the country where a cloud service provider stores, processes or transmits information and issues may arise that are harmful to New Zealand's national interests or inconsistent with New Zealand's laws. It is not possible to fully contract out of the laws of another country.

The following section focuses on recommended measures that will enable *Waka Kotahi* to satisfy itself that personal information is as well or better protected in 3rd parties' control as if it was held internally.

IPP 5 of the Privacy Act requires an agency to implement reasonable security safeguards in respect of personal information it holds. The usual focus falls to ensuring that the information is secured in a range of settings including –

- security of physical or technical storage both while in the technology platform and in transit to any subsequent storage platform,
- practical management of the data while it is held,
- appropriate operational only access to the data or system,
- audit of the access and activity within the storage system and data,
- policy, protocols or guidance for staff use of the system,
- and, governance.

[9] IPP 12
[10] Section 11 Privacy Act 2020

Technical Security

Recommendation 9: Establish technical security within a roading management camera system and storage that is commensurate with the agency's responsibility for security

The future intention is to grow the roading management camera use to encourage compliance on the roading system and create safer roads. It is anticipated that within the next 10 years there could be as many as 800 cameras deployed on the roading system. This will mean that the volume of data retained within storage will be significant over time. Early contemplation about how *Waka Kotahi* will manage the various deployed cameras and the technical management systems will be of significant benefit long term.

A PIA is not the total tool to review the cameras and technical systems information security. However, privacy and technical security are very closely allied. Technical information security is an important part of the overall privacy framework, but it is a specialised pursuit that requires separate and detailed consideration by information security experts.

As with privacy by design, security by design relies on early involvement in a project, to ensure that security is built in from the start of the project. This requires early engagement with ICT security experts to participate in the design and construction of the storage facilities. In the 'cloud' context it will require consultation with the system service provider to ensure that the level of security required by *Waka Kotahi* is provided within the technical system and within the contractual arrangements with the provider.

Technical solutions would at least require encryption in transit and at rest; access and activity logs and audit capability.

Whether the storage solution is on premises within the *Waka Kotahi* IT infrastructure or in the 'cloud', it is desirable to deploy a solution that enhances access to the data and increase effective management through centralised oversight. This may enhance audit options, provide ease of agency access to locate data in the context of requests for access to it; and the options for security controls over one accumulated set of information is potentially easier to deploy and manage.

Storage arrangements with 3rd party providers requires transferring the responsibilities of *Waka Kotahi* to the 3rd party through clear and accurate contractual expectations.

The absence of centralised storage of the roading management camera system is *unlikely* to result in an immediate risk but over time the consequences may be *moderate* if the management of the systems is disparate and inconsistent, with changes resulting in additional costs and the potential for *Waka Kotahi* management of the cameras being called into question with a resultant loss of reputation. The inherent risk profile would be no greater than *medium.*

A technically secure solution is likely to enhance the management of roading management cameras reducing the risk consequences to *insignificant/minor* with a residual risk of *low.*

Technical Security Risk Profile – R9
Inherent risk rating – Medium
Residual risk rating – Low/medium

Controls on Access to Personal Information

Recommendation 10: Develop a carefully designed set of user roles for access to retained information, ensuring that access to personal information is limited to the appropriate staff.

Good privacy practise requires an agency to control access to systems containing personal information. Greater sensitivity of information typically requires correspondingly more limitations on access.

There are a range of activities that will require access to the data, from involvement in the infringement process, analysis of data acquired for research into roading activity through to responding to requests by individuals and external 3rd parties. *Waka Kotahi* believes that around 400+ staff may be involved in managing the personal information within the system

In order to provide adequate privacy protections for personal information, it is therefore essential that the system tightly limits the information different types of users can access and/or edit and limits groups or individuals range of activity within the system.

The various business needs to access the personal information ought to be defined and access permissions managed centrally to ensure that access is granted and removed according to the particular staff members' role and employment. This will require *Waka Kotahi* to closely monitor account activation and deactivation, as staff arrive, leave or change roles within the organisation.

The risk analysis for this aspect is included within the commentary on audit capability and 3rd party relationships.

Audit Capability

Recommendation 11: Ensure the system logs access to and activity within the roading management camera data and the log is audited.

Access limitation rules are one way to protect personal information from unauthorised access, use or disclosure. However, system constraints and policy can be bypassed. It is essential that the system is capable of effective audit to monitor access to and activity within the personal information. This applies whether in onsite storage or within a 'cloud' solution. Effective audit capability will allow *Waka Kotahi* to meaningfully reassure the business and regulators that its security safeguards are effective.

The future substantial volume of personal information to be captured by the camera systems and managed in the single technical system, means that comprehensive audit facilities should be preferred. An ideal system would create metadata of staff interactions within the road management camera data including:

- Name and role of a user who views it
- Dates, times and nature of information accessed
- Details of downloaded/printed data occurrences
- Details of changes made to records

Dealing with audit capacity in a 3rd party 'cloud' solution is different to the options available onsite. *Waka Kotahi* should aim for audit capability within a 'cloud' service that is commensurate with expected internal capability. This will require clear contractual obligations of the 3rd party provider.

In addition it is appropriate to consider proactive audit of some form as opposed to reactive auditing. Reactive auditing will apprehend reported unlawful behaviour but a better deterrent is proactive auditing activity that leverages off technical tools and captures highly unusual or abnormal behaviour within data storage systems. Behaviour that is likely to have a detrimental impact on customers is usually detectable through reactive audit but harm will have already manifested. Proactive audit is more likely to deter and detect harmful behaviour before it manifests for customers.

3rd Party Relationships

Recommendation 12: Ensure that accountabilities and responsibilities are reflected and passed onto 3rd parties who undertake technical storage facilities or business processes on behalf of *Waka Kotahi*

The Privacy Act is clear that responsibility remains with the agency that uses 3rd parties to store or process personal information on its behalf.[11] In the case of a provider that provides a storage and information management system, the accountability and governance remains with *Waka Kotahi*.

As previously mentioned this will require clear expectations with 3rd parties to ensure that they do not use or disclose information for their own purposes; that they report privacy breaches to the principal agency promptly; and, that they provide levels of security to the expectations of *Waka Kotahi* . In essence all of the security controls that apply to the principal agency ought to apply to the 3rd party including limits on its staff access to personal information.

Risks arise where personal information is accessible to an unknown or undefined number of staff. Limiting access to only those who require access to information along with proactive audit are in combination, valuable controls. In addition, knowledge by staff that these controls exist is an effective deterrent to most employee browsing or unlawful access. Allowing unfettered and unobserved access to personal information is a significant risk which would *almost certainly* result in unlawful behaviour by staff. Reputational damage to *Waka Kotahi* would be a reality along with potentially serious harm to individuals who were subject to unlawful access to their information. The inherent risks in leaving data both open and unaudited would be *critical.*

Introducing controls such as active and effective activation and deactivation of staff access to system information along with proactive audit would introduce significant deterrence to staff and 3rd party unlawful behaviour and provide appropriate agency oversight of the use of the information. This will reduce the chances of aberrant behaviour to *unlikely* although if it were to occur the consequences are likely to remain *severe* particularly in light of the nature of the information that resides in the system. The resultant risk is likely to move to *medium.*

Access Controls and Audit Capability Risk Profile – R10, R11 & R12
Inherent risk rating – Critical
Residual risk rating – Medium

Guidance and Training

[11] See Section 11 of the Privacy Act 2020

Recommendation 13: Support staff to use the roading management camera data appropriately through adequate guidance and/or training.

Privacy is about people and processes as much as systems. A robust 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.

Waka Kotahi should develop training materials and deliver training for all staff who will use the roading management camera system and data. Training should emphasise privacy responsibilities as well as technical knowledge required to use the system.

Staff who are not advised and unsupported around their use of an agency's personal data and who are not aware of the controls and oversight the agency has over personal information are *likely* to stumble into incorrect behaviours or exploit the opportunity to act unlawfully. The consequences are likely to be *moderate* to *severe* resulting in reputational damage to *Waka Kotahi* and potentially significant harm to customers. The inherent risk rating would at least be *high.*

Introducing training and guidance for new staff who engage with the road management camera system along with regular updates for existing staff will reduce the risk of aberrant or inadvertent behaviour. Issues may be reduced to *possible* with the consequences remaining at *moderate* to *severe* and the resultant risk rating reduced to *medium.*

Guidance and Training Risk Profile – R13 Inherent risk rating – High Residual risk rating – Medium

3.6 Data breach handling

Recommendation 14: Take steps to ensure that 3rd parties recognise and report any data breach including near misses

Despite the best risk controls and mitigations, a privacy breach is a likely occurrence in any organisation or business system. If a 3rd party experiences a data breach or a near miss, timely identification and reporting of the incident are crucial to resolving the breach and minimising harm. This is an important consideration in the context of the Privacy Act 2020 notifiable privacy breach regime which requires both the Privacy Commissioner and affected individuals to be notified of a breach that may cause or has caused serious harm. What constitutes serious harm is defined in the Act.

Notifying the Privacy Commissioner is not legislatively bound by time except that it should be completed as soon as practicable. The Privacy Commissioner has intimated that notice should occur within 72 hours of the breach being viewed as causing or may cause serious harm. In the relationship with 3rd parties and the context of the roading management camera system *Waka Kotahi* will be responsible for the reporting obligations in the notifiable privacy breach context.

Therefore, successful data breach handling relies on both 3rd party staff recognising a privacy breach; and 3rd parties reporting to *Waka Kotahi* immediately of a privacy breach event that occurs at any point where data is in its control.

Recognising a privacy breach is not always obvious or easy. Determining whether a privacy breach is notifiable is difficult. As with many other aspects of privacy risk management, recognition relies on staff training and experience. For this reason, *Waka Kotahi* should consider requiring 3rd party staff to

complete privacy training, including focusing on identifying and handling privacy breaches, or at least have confidence that the 3rd party delivers adequate training to its employees.

Recommendation 15: Require 3rd parties to provide all information necessary to investigate, manage and resolve a data breach

Once a privacy breach is notified, it is critical that *Waka Kotahi* can implement its data breach processes. These rely on accessing all the information it needs to investigate and contain the breach, report notifiable privacy breaches, and mitigate any resulting harm to individuals whose information is involved.

A data breach incident is a *possibility* particularly in a 3rd party relationship involving a significant system and substantial volume of information. The consequences would at least be *moderate* to *severe* depending on the resultant harm to an individual or a cohort of individuals. The inherent risk would be at least *medium* and potentially *high.* Active co-operation and the timely release of all information necessary to investigate, manage and resolve a data breach is an important obligation that ought to be part of 3rd party contractual relationships. A proactive and co-operative relationship with a 3rd party has the potential of reducing harm from data breaches to *unlikely* resulting in a residual risk of *medium.*

Integrity of personal information Risk Profile – R14 and R15
Inherent risk rating – Medium
Residual risk rating – Medium

3.7 Integrity of Personal Information

Waka Kotahi must incorporate robust safeguards to ensure the integrity and reliability of personal information.

Personal information within the roading management camera system must be processed by *Waka Kotahi* to ensure that it:

Does not intrude unreasonably into the personal affairs of the individuals (IPP 4)

Takes reasonable steps to check that information is accurate, complete, relevant, up to date and not misleading before use or disclosure (IPP 8)

Recommendation 16: Create business processes that provide assurance that the technical system is accurate and reliable.

Recommendation 17: Create business processes that provides for human oversight of roading management camera data that contributes to decision making.

In addition to the requirements of IPP 8, additional relevant expectations are set out in the guidance promoted by the Chief Government Data Steward and the Privacy Commissioner on the safe and effective use of data and analytics.[12]

Waka Kotahi will potentially deploy systems that use algorithms to detect activity by individual road users such as using a mobile telephone while driving, not wearing a seat belt through to assessment of

[12] https://www.privacy.org.nz/assets/Uploads/Principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance3.pdf

speeds or road position in the context of red light running. Some of these deployments will inevitably result in decisions to infringe or prosecute a driver for a roading offence.

Other systems will be deployed to enable research and statistical analysis of road user behaviour such as journey times, vehicle occupancy and general road user compliance with the road rules.

Deploying systems that create automated reports about individual's behaviour and actions, require careful oversight. It is important to ensure that subsequent decisions or processes that are predicated on machine reports are accurate and not misleading, particularly where the decisions may be detrimental to individuals' rights and freedoms. The Government's data and analytics principles include that the technology deployed,

- Must deliver clear public benefit – particularly where it supports decision making
- Ensure data is fit for purpose – including accuracy and completeness
- Have a focus on people – recognising that deploying data analytics to process data and support decision making can have real-life impacts
- Maintain transparency – taking into account the views of stakeholders and ensuring that the deployment, use and management of the data and analytics are explained to the public, simply and clearly
- Understanding the limitations – avoiding bias, unfair or discriminatory outcomes
- Retaining human oversight – ensuring human judgement and evaluation remain an integral part of the decision making

Some of these are covered elsewhere for example, delivering a clear public benefit which is necessarily a consideration of the lawfulness and purpose aspects of collecting personal information. However, human oversight, judgment and the application of discretion are attributes that must accompany the deployment of automated technology. Without them there is a risk of bias or unfairness in decisions that may have a marked detrimental impact on individuals and the business of *Waka Kotahi.*

Appropriate controls include to build human oversight into the systems at crucial points to ensure that it technically functions appropriately and that decisions based on the system's product are defensible. This will mean establishing a business process to regularly review that the technology is deployed appropriately and is reliable. And secondly by establishing a business process that ensures that before information acquired from the system is used in a decision, it is checked for its integrity.

Deploying technology without ensuring its functional accuracy and relying totally or predominately on its outputs for decision making is *almost certain* to raise issues that result in consequences that are *moderate* to *severe*. *Waka Kotahi* would likely come under the scrutiny of media and the public in general. There is a heightened public awareness and concern about the use of algorithms and machine learning resulting in greater scrutiny of public sector deployments. The inherent risk rating is likely to be at least *high.*

By introducing human oversight of road management camera outputs which are only used to assist with decision making rather than relying on them totally, along with regular reviews of the accuracy of the systems outputs the likelihood of unwarranted adverse consequences for individuals will be reduced to *unlikely.* Issues that arise remain likely to result in *moderate* to *severe* consequences with the resultant risk reducing to *medium*.

Waka Kotahi will need to strike a balance between total automation and total reliance on human oversight. The system must incorporate a sensible reliance on automation with sufficient human oversight both at the decision-making point of the system and with subsequent activity around the use of the data. The aim would be to arrive at a practice that gives both *Waka Kotahi* and the public, confidence that the used data is accurate and not misleading particularly when the decision outcome may result in a detriment for individuals.

Integrity of personal information Risk Profile – R16 and 17
Inherent risk rating – High
Residual risk rating – Medium

3.8 Retention

Waka Kotahi must not retain personal information longer than necessary.

Personal information collected by the *Waka Kotahi* roading management camera system must not be:

Retained longer than it is required for the purposes for which it may be lawfully used (IPP 9)

Recommendation 18: Set retention periods for personal information collected by individual roading management camera systems.

A growing set of data may become challenging to administratively manage and holding personal information for longer than necessary introduces more opportunity for misuse of the content. Accordingly, it is appropriate to create policy and guidance detailing how long personal information is to be retained. Conversely it is equally appropriate to define which personal information is capable of early deletion. Data minimisation, mentioned earlier in the report, contributes positively to the retention exercises.

Clearly stated purposes for collecting and using roading management camera personal information will contribute to establishing lawful and rational reasons for specific retention periods. The Public Records Act and any authority for disposal agreed with the Chief Archivist will be important contributions to the policy adopted by *Waka Kotahi.* Clarity around retention will also contribute to the level of the administrative burden. For example, if certain footage and related data is only kept for a short period of time, the obligations to administratively account for it and provide access to it will dissolve.

There will be reasons for keeping information for lengthy periods or indefinitely such as information that contributes to decision making about offending. Conversely personal information that is used in a research or evaluation manner, to inform business decisions may be able to be destroyed or deleted within short periods of time or retained in a de-identified form.

The uncertainty around the nature of the data that emanates from the various camera options means that decisions about retention must be made in the context of the purpose for the camera deployment. As discussed in the earlier commentary around purpose, and the later commentary about voluntary disclosure, retention should be influenced by the lawful and necessary purpose for collecting personal information. For example, data collected from a passing vehicle that is aimed at detecting distraction should not be retained beyond a very short period if distraction is not detected. This suspicionless data should not be retained, in an identifying way, for reasons that are unrelated to the aim of catching distracted drivers.

Retaining personal information for longer than necessary introduces *possible* risk to the information. The information may be used for purposes outside of its original purpose or simply at risk by its presence in the agency's holdings. The consequences may at least be *moderate* resulting in an inherent risk value of *medium.*

Introducing clear guidance and policy about what information will be retained and for how long reduces overall risk to the agency. Deleting data that is not required for one of the camera purposes means that data is not put at risk. It also reduces or avoids consequences to individuals in the event of an incident. Retention policy wisely linked to the purpose of the collection of personal information may reduce the likelihood of incidents arising to *unlikely* and while the consequences may remain *moderate,* they may also be *minor* with a residual risk of *low.*

Waka Kotahi will also need to be cognizant of the possibility of the over collection and retention of personal information resulting in perceptions that the agency is engaged in mass surveillance of NZ citizens. Given the potential numbers of cameras that will be deployed and the range of roading issues that they will be aimed at, the volume of data is likely to be extensive, but could be viewed as unnecessarily if substantial amounts of data are retained for unrelated or undefined future uses.

Retention of personal information Risk Profile – R18
Inherent risk rating – Medium
Residual risk rating – Low

3.9 Use, Disclosure, and Other Access

Managing the personal information acquired within the roading management camera system requires trained and knowledgeable decisions makers.

Waka Kotahi while being transparent about collecting personal information within the roading management camera systems, must adequately resource the task of enabling access and correction rights.

Waka Kotahi must ensure that:

When disclosing or sharing personal information it complies with the expectations set out in IPP 10 and IPP 11 of the Privacy Act 2020 or other lawful provisions

Road users have the ability to access personal information about them (principle 6)

Road users have the ability to correct personal information about them (principle 7)

Recommendation 19: Establish a business process that administers the various requests that will be made for roading management camera data/personal information.

Recommendation 20: Establish comprehensive guidance and training for staff and a business process that provides oversight of the way roading management camera data is managed and used.

Use and disclosure of personal information are often perceived by staff to be the most difficult aspect of managing personal information. These difficulties often arise out of inadequate business statements about the purposes or directly related purposes for which the information was acquired. Further, the perceptions are often compounded by an absence of guidance and training about the appropriate factors that are required to be taken into account when using or disclosing information.

The earlier commentary and recommendations about purpose (see 3.4) will contribute to managing the risks around use and disclosure. Understanding the purposes and directly related purposes for using personal information is a good start to safe practice but the task also requires an understanding of the application of the exceptions within IPP 10 and IPP 11 that enable extended uses, and ensuring that only sufficient information is used or disclosed to meet the request. In addition the responsibilities to respond to Privacy Act "access requests" and Official Information Act requests for information are time consuming and potentially onerous.

Disclosure Generally

With a potential growth in the use of roading management cameras and allied technology it is likely that other agencies will seek to take advantage of the collected information. For example law enforcement agencies may seek access to information informally or through a statutory demand or court order. The latter is a mandatory disclosure by law. But otherwise, personal information held within the roading management camera data holdings should only be disclosed to external agencies in accordance with the exceptions to IPP 11 of the Privacy Act (or where appropriate the like provisions of the Official Information Act). The most relevant exceptions are likely to be:

- To avoid prejudice to maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences (11(e)(i));
- For the conduct of proceedings before any court or tribunal 11(e)(iv);
- To prevent or lessen a serious threat to public safety 11(f)(i) or the life or health of the individual concerned or another individual 11(f)(ii)
- To enable an intelligence and security agency to perform any of its functions (11(g))

Waka Kotahi must develop robust business processes for staff to follow when making decisions about whether to disclose under principle 11. This process should ensure that:

- criteria are applied consistently, and
- information decisions, such as which exception is relied upon for disclosure, are thoroughly documented.

A robust business process and well documented decision-making criteria would enable *Waka Kotahi* to demonstrate that it has meaningful privacy protections in place when deciding whether to disclose personal information. In the face of a request for data a simple decision tree might look something like,

⇒ Is the required response discretionary or compelled?

⇒ Does the request seek the use or disclosure of personal information for one of the purposes or directly related purposes for which it was acquired?

⇒ If the answer is 'no' – does one of the exceptions in IPP 10 or 11, depending on the request, apply? For example, action is necessary for a law enforcement reason; the information is required for proceedings in a court or tribunal.

⇒ If the answer to either of the above is 'yes', ensure that the minimum amount of relevant information is released or used to meet the request.

The last step is a requirement to only release or use information that is necessary and proportionate to the identified need for the information – a data minimisation requirement. In a non-statutory request situation the obligations fall on the holding agency and arise under IPP 11 – the responsibility and discretion is to release only information necessary and proportionate to the reason why the information is sought.

Individual's Requests

Along with 3rd party requests it is inevitable that *Waka Kotahi* will receive requests from individuals seeking information about themselves that they believe has been captured by the roading management camera systems – Privacy Act access requests. Additionally, there will likely be requests made under the Official Information Act and responsibilities to disclose information under the Criminal Disclosure Act (in respect of infringement offences). These may take the form of either:

- broadly worded requests that encompass information contained in the system; or
- Specific requests for access to camera information, as the system receives public attention; or
- Access to information about a registered person's car driven by someone else.

While we are not aware of the current *Waka Kotahi* system for dealing with Privacy Act requests, roading management camera personal data should be included in a robust process for responding to access requests including the following general stages:

- **Assessing** whether the request information is held within the system.
- **Compiling** the information from the system
- **Reviewing** the information to determine what should be released and whether any information should be withheld
- **Releasing** the data to the requestor

An additional criminal offence within the new Privacy Act 2020 provides for significant fines for destroying information which is the subject of a Privacy Act access request. Destruction of personal information before a response to an access request may result in a criminal conviction and also an interference with the individual's privacy resulting in a civil damages. The liability may be triggered by circumstances where after receipt of the request and before a response is made, an agency allows a system to automatically delete or destroy the target information. There will be a need for those dealing with Privacy Act requests to be aware of this possibility and to take prompt action to preserve the required information.

Waka Kotahi must ensure that its business processes are adequate to comply with the procedural steps set out in Part 4 of the Privacy Act if it receives an access or correction request. Requirements would include -

- Steps must be taken to verify the identity of the requester.
- Assistance to a requester to ensure that the request is understood.
- A decision must be made on a request, and conveyed to the requester, within 20 working days.
- Where a requester has good reason to make an urgent request, a decision should be made as soon as reasonably practicable.
- The information requested should be provided in the way preferred by the requester.
- The requester must be advised of any information that has been withheld, or redacted, from the information released.
- The information must be provided to the requester without undue delay.
- If a correction request is refused, the customer must be given the opportunity to attach their request to the disputed information as a statement of correction.

While the camera system requirements seemed to have focused on providing a copy of a photograph, registered owners of vehicles could request all information pertaining to an infringement event, history or account transactions and allied data. The development of a new back-office system for managing road management camera data is an ideal opportunity to build in a process that enables staff to quickly respond to requests. It is desirable to include the ability to redact or pixelate image or video information where required.

There is an inherent risk in managing information in the face of demands or requests to use the information for reasons other than the original purpose or not within lawful exceptions. There are also risks around complying with the obligations within the Privacy Act to provide individuals with access to their information. It is *likely* that even with the best guidance in place information will be released or withheld in error and the consequences may range from *minor* to *severe.* The inherent risk is likely to be in the *medium* to *high* category.

By providing adequately trained and informed resource to the task of managing information releases the occurrence of error is likely to reduce to *unlikely* The consequences of mistakes will unlikely change meaning the resultant risk will remain at *medium.*

Use, disclosure and access of personal information Risk Profile – R19 and 20
Inherent risk rating – High
Residual risk rating – Medium

Requests for Voluntary Release of Personal Information

Recommendation 21: Create policy that defines the limited purposes for which the road management camera system collects personal information and reflect the limited purposes in *Waka Kotahi* retention, use, and disclosure rules.

This section covers the potential for other agencies to seek access to personal information that has been collected by *Waka Kotahi* through its road management camera system. The commentary is separate to considerations of statutory requests such as those resulting from a search warrant or production order, or those arising out of other statutory authority including the Official Information or the Privacy Acts or *Waka Kotahi* enabling legislations.

The information collected by point to point cameras is a relevant collection activity on which to focus this analysis. It generally involves two types of data – data about compliant and non-compliant vehicles and drivers. Respectively referred to as suspicion-less and prosecution or infringement personal information. In a camera system like the point to point technology the volume of suspicion-less personal information will be substantially higher than infringement information. It will be information about people going about their daily routines or travel that is legal and potentially has an element of expected privacy. Anonymized and de-identified information may be used to generate public advice about road use peak times. *Waka Kotahi* may decide that there are allied uses for the data. For this assessment it is assumed that point to point speed cameras will only be used for detecting excess speed.

Regulatory Context

There is a regulatory context that needs to be accommodated. The information collected will be personal information about the movements and travel of people and the Privacy Act will apply. The Privacy Act focusses on the life-cycle of information expecting that an agency will apply rules to the collection and use of personal information that it collects.

Mentioned previously in this report, collecting information for a *lawful purpose* is the first and paramount consideration. Establishing a primary purpose enables best practice to be defined for the remaining data life-cycle activities of collection, retention, storage, use and disclosure. Relevant to this discussion, disclosure is allowable for the primary purpose for which the collection was achieved, and may include,

- When disclosure is directly related to the primary purpose
- To avoid prejudice to the maintenance of the law
- To prevent or lessen a serious threat to the life or health of a person.

These are permitted activities and commonly referred to as exceptions to the general rules around dealing with personal information. They are to be applied when there is reasonable grounds to believe that the disclosure is necessary. The permitted activities are viewed as applicable to one off situations and not bulk transfers of data between agencies particularly in the public sector. For that reason Part 7 of the Act provides mechanisms to facilitate bulk or ongoing transfers between agencies of data such as,

- Approved Information Sharing Agreements (AISAs)
- Regulatory mechanisms reflected in Schedules to the Act authorising access to regular supply of personal information between agencies to enable identity verification – see s 165 and s 168 of the Act and Schedule 3
- Authorising agencies to have access to law enforcement information held by other agencies – see s 172 & 173 and Schedule 4.

Bulk disclosure or regular feeds of bulk information are not enabled by the exemption provisions of the IPP 11. They are designed for a case by case examination of a one off need to disclose or share specific information. In the absence of a provision under Part 7 of the Privacy Act or specified lawful sharing of personal information in other primary legislation, bulk or regular sharing is not permitted. An example of permitted bulk sharing exists in the Customs and Excise Act 2018 Sections 314 to 316. Without similar enabling provisions *Waka Kotahi* would have to rely on exercising its discretion under IPP 11 on a case by case basis.

Requesting personal information be disclosed in a voluntary way is not prohibited. However, the agency disclosing information in response to a request is obliged to apply the provisions of the Privacy Act in particular IPP 11 and exercise its discretion to release or not release information.

Failing to factor in the responsibilities in responding to requests not based on a statutory authority is a risk for *Waka Kotahi* . The risks are amplified in a Privacy Act complaint between the journalist Nicky Hagar and the Westpac Bank[13]. Police made a request to Westpac for the voluntary release of personal information about Hagar. Westpac supplied personal information without asking Police for information sufficient to enable Westpac's discretion to be properly applied. They weren't informed and did not ask how the disclosure of the information would avoid prejudice to a criminal investigation. In a similar vein the Supreme Court in *R v Alsford* affirmed the responsibilities of agencies when dealing with law enforcement requests[14]. While both these scenarios dealt with the application of the law enforcement exception, the responsibilities would apply to any of the discretionary exceptions under IPP 11 when an agency is responding to a request to voluntarily release personal information.

Lifecycle of Information Context

The first consideration for *Waka* an *Kotahi* is to clearly define the lawful, necessary and proportionate purpose that enables it to collect personal information in the context of the road management camera system. That purpose informs the public of the what, how, when and why their information is being collected. Broadly speaking from discussions with *Waka Kotahi* project staff, the various camera options are either collecting data that enables monitoring of road use and behaviour, to infringe or prosecute non-compliance, or collect tolling information. These are road transport reasons and purposes.

In the case of tolling information there is a specific legislative bar on the tolling information being used for any other purpose other than tolling. The law provides an exception within IPP 11 – maintenance of the law which as previously stated is to be exercised on a case by case basis in response to a request. In the context of the tolling provisions in the Land Transport Act the Privacy Commissioner expressed concern of wider uses of the information saying –

> *When the Land Transport Management Act was put in place it contained several provisions to* ***ensure that modern tolling systems would not unnecessarily infringe on New Zealanders' privacy****. The requirement to have an anonymous method of payment in section 51(3) was central to these protections. This Bill proposes repealing this section.*
>
> *My view is that removing the section will leave New Zealanders at risk, unless the Bill puts in place alternative statutory safeguards.* ***This is because mass collection of travel information about New Zealanders creates risks of surveillance that could have serious effects on rights of privacy and freedom of movement.*** *Current privacy rules are insufficient to protect against those risks.*

By analogy it will be wise to view these comments as relevant to other forms of substantial data collection involving other CCTV camera imperatives. The comments are particularly relevant in the context of suspicion-less data for example personal information collected to inform about road behaviour or collected as a corollary to determining non-compliance.

Defining purpose will avoid extraneous rationale for retaining or using information. It avoids function creep – the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy[15]. For example if the deployment of point-to-point speed cameras is to detect road users who are speeding it would be appropriate to use the data to further that purpose and as is applicable currently for Police, share information with the Courts and *Waka Kotahi* as permitted by Schedule 4 of the Privacy Act. There would be no justification or necessity for keeping data that did not detect a speed event for any period beyond

[13] https://www.privacy.org.nz/publications/statements-media-releases/privacy-commissioner-welcomes-westpac-privacy-breach-settlement/

[14] https://www.privacy.org.nz/blog/supreme-courts-alsford-decision-affirms-role-of-the-privacy-act/

[15] Collins English Dictionary

verification of excessive speed. Retaining it for the possibility that it might be useful for the investigation of other offences and criminal behaviour, not a function of *Waka Kotahi* , is not likely lawful and at least unnecessary and disproportionate to the main purpose – to apprehend speeding drivers. However, it does not mean that suspicion-less data cannot be retained in a de-identified way to enable road use analysis. This is a permitted exception within IPP 10 and 11.

A clear purpose will limit the information that needs to be collected and retained. The retention of personal information beyond a defined purpose, poses a risk to *Waka Kotahi* .

Risks

The social licence aspects of *Waka Kotahi* collecting personal information are likely to be confined to a public acceptance that the agency manages the roading network and is entitled to enforce applicable regulations. It is unlikely that *Waka Kotahi* would be seen by the public as a general law enforcement agency involved in the investigation of criminal offences.

In the context of data stewardship and privacy, 'social licence' is an important concept where an agency's ability to carry out its business is based on the confidence society has that it will behave legitimately, with accountability and in a socially and environmentally responsible way[16]. For a public sector agency terms such as acting lawfully, demonstrating best practice and fostering trust and confidence through practice are appropriate.

Collecting personal information that is not necessary for the purposes of the agency and retaining it on the assumption that another agency might make use of it may result in an *almost certain* withdrawal of social licence and a loss of trust and confidence in *Waka Kotahi* . It is also likely that the collection and retention of unnecessary personal information is unlawful. The consequences are likely to be *moderate* to *severe* and include a lot of effort to regain general trust and confidence. Individuals may also suffer significant detriment as a result of the use of their information about them going about their lawful activities. The inherent risk is likely to be *high* or possibly *critical.*

Not retaining suspicion-less data or establishing enabling regulation that permits the collection, retention and use of the data will result in a residual risk where the likelihood is *rare or unlikely* and the consequences are *insignificant or minor.*

Requests for Voluntary Release of Personal Information – R21
Inherent risk rating – High
Residual risk rating – Minor

[16] A Social Licence to Operate Paper – NZ Sustainable Business Council
https://www.sbc.org.nz/__data/assets/pdf_file/0005/99437/Social-Licence-to-Operate-Paper.pdf

4. Conclusion

This review has highlighted potential risks that may apply to the deployment of a roading management cameras and a technical management system and has made recommendations to manage them. It is acknowledged that some camera systems already in use by *Waka Kotahi* may have adequate controls. The report is designed to enable a review of existing camera systems along with providing input into new systems that are in contemplation. It also provides recommendations to manage risks that may arise in the acquisition and deployment of technical system that will manage the camera data.

The PIA makes the following recommendations to assist the *Waka Kotahi* to mitigate the identified privacy risks and meet its privacy objectives:

Summary Table of PIA Recommendations	
Recommendation 1	Undertake an agency risk workshop to qualify the risk assumptions made within this assessment.
Recommendation 2	Identify a national governance sand assurance structure for the national deployment of roading management cameras that includes regular oversight and assurance reporting.
Recommendation 3	Develop a privacy reporting agenda for the roading management camera system Business Owner and service providers to report regularly to the governance group.
Recommendation 4	Create a plain English informative privacy policy for the roading management camera system and ensure it is understood by all system users.
Recommendation 5	Acquire a legal opinion on the lawfulness of collection of personal information in the context of the deployment of roading management cameras
Recommendation 6	Establish at an early stage the primary and directly related purposes for using a roading management camera system and collecting personal information.
Recommendation 7	Establish policy or guidance for each targeted deployment of roading management cameras, that prescribes the expectations of data minimisation so that collection of unnecessary personal information is eliminated.
Recommendation 8	Implement a transparency strategy to cover the deployment of a roading management camera system including comprehensive advice through appropriate agency channels.
Recommendation 9	Establish technical security within the roading management camera system and storage that is commensurate with the agency's responsibility for security
Recommendation 10	Develop a carefully designed set of user roles for access to retained information, ensuring that access to personal information is limited to the appropriate staff.
Recommendation 11	Ensure the system logs access to and activity within the roading management camera data and the log is audited.
Recommendation 12	Ensure that accountabilities and responsibilities are reflected and passed onto 3rd parties who undertake technical storage facilities or business processes on behalf of *Waka Kotahi*
Recommendation 13	Support staff to use the roading management camera data appropriately through adequate guidance and/or training.
Recommendation 14	Take steps to ensure that 3rd parties recognise and report any data breach including near misses
Recommendation 15	Require 3rd parties to provide all information necessary to investigate, manage and resolve a data breach

Recommendation 16	Create business processes that provide assurance that the technical system is accurate and reliable.
Recommendation 17	Create business processes that provides for human oversight of roading management camera data that contributes to decision making.
Recommendation 18	Set retention periods for personal information collected by individual roading management camera systems.
Recommendation 19	Establish a business process that administers the various requests that will be made for roading management camera data/personal information.
Recommendation 20	Establish comprehensive guidance and training for staff and a business process that provides oversight of the way roading management camera data is managed and used.
Recommendation 21	Create policy that defines the limited purposes for which the road management camera system collects personal information and reflect the limited purposes in *Waka Kotahi* retention, use, and disclosure rules.

The recommendations align with the identified risks and are shown on the Risk Matrix "Heat Maps" at *Appendix 1* showing the inherent risk and with controls and treatments, the residual or remaining risk.

There is no hierarchy of importance in the way the risks are highlighted. They are arranged according to the lifecycle of information that will be acquired and held by *Waka Kotahi.* It would be prudent to accommodate the recommendations into deliberations about any potential system provider, factor them into contractual negotiations to establish desired terms and conditions, and to establish clear business processes early in deploying any camera options or camera system. In this way *Waka Kotahi* will be building a clear pathway for a project which will be easier to consult upon when the time comes to reach out to the public, the Privacy Commissioner, and the Minister of Transport.

Lastly, as stated earlier, this assessment should be viewed as a living document, capable of review and alteration depending on milestone decisions that occur during the future deployment of cameras and allied systems on the roading network. We have provided a main report that ought to remain relevant over time. Additional camera projects can be added to the report by adding an Annexure for the system and applying the relevant main recommendations to the project.

The Annexures highlight individual projects and set out the recommendations that are applicable to the project. The recommendations are set out in a project timeline way rather than the information lifecycle context used in the report.

Annexure 1 – Inherent and Residual Risk Matrix

Inherent Risk Position (with no controls in place)

	Insignificant	Minor	Moderate	Severe	Extreme
Almost Certain	Low	Medium	High **R5;R7; R16; R17**	Critical **R10;R11; R12;R21;**	Critical
Likely	Low	Medium	High **R2; R3; R4; R8; R13; R19; R20;**	Critical	Critical
Possible	Low	Medium	Medium **R6; R14; R15; R18;**	High	Critical
Unlikely	Low	Low	Medium **R9;**	Medium	High
Rare	Low	Low	Low	Low	High

Residual Risk Position (with controls in place)

	Insignificant	Minor	Moderate	Severe	Extreme
Almost Certain	Low	Medium	High	Critical	Critical
Likely	Low	Medium	High	Critical	Critical
Possible	Low	Medium **R6;**	Medium **R13;**	High	Critical
Unlikely	Low	Low **R2; R3;R4 R5; R7; R9;**	Medium **R8; R14; R15; R16; R17; R19; R20**	Medium **R10; R11; R12;**	High
Rare	Low	Low **R18; R21**	Low **R3**	Low	High

Annexure 2 - Canterbury North Corridor trial

This project involves monitoring of a south bound 'special vehicle lane' which will operate between 6am and 9am weekdays only. During those times only High Occupancy Vehicles (HOVs) will be permitted to use the lane. An HOV is a vehicle carrying more than one occupant. The aim is encourage road users to either use public transport or car pool.

To monitor the use of the special vehicle lane *Waka Kotahi* will strategically install 8 high definition cameras on the lane with a forward and side facing focus to provide a view capable of counting the number of occupants. This will enable *Waka Kotahi* staff to periodically view the traffic flow to determine the level of compliant use of the lane.

The existence of the cameras may also provide a deterrent to road user's non-compliant use of the special vehicle lane.

Personal Information

The personal information collected will be video imaging of vehicles passing the cameras sufficient to count occupants. The images will also enable identification of some people and capture the make and registration of the vehicle.

The personal information will be used in a research and statistics in ways that individuals will not be identified.

In view of the short retention period it is unlikely that 3rd party or individuals will be able to request information before it is deleted

Intended Controls

- The video imaging will be streamed to a secure server within the *Waka Kotahi* IT infrastructure and made available at the Wellington Transport Operations Centre (WTOC).
- It will be encrypted during travel and at rest.
- The imagery will only be available to small number of analysts for periodic analysis of road user compliance and reporting to the stakeholders who have responsibility of the roading system. Reports will be about volumes, aggregated and anonymised, and not individual road users.
- All imagery will be deleted from the servers 5 days after uploading to the server.
- Access and limited activity logs are kept for audit purposes
- A transparency strategy will include roadway signage, website commentary and media statements.

Recommendations specific to CNC Special Lane Project	Recommendation Reference	Date • Accepted • Implemented
Establish at an early stage the primary and directly related purposes for this deployment of roading management cameras to inform system design and use	R6	
Introduce policy or guidance that minimises the data required so that unnecessary personal data is not collected; define retention to the minimum time required to meet the purpose of establishing general compliance	R7; R18	

Consider the requirements for technical security within the roading management camera system and storage that is commensurate with the *Waka Kotahi* responsibility for security	R9	
Ensure the system logs access to and activity within the camera data and the log is audited.	R11	
Establish assurance reporting about the technical and analytical aspects of the system	R16	
Create user roles for the appropriate staff to use the data.	R10	
Devise a strategy for advising the public and other stakeholders about the project	R8	
Designate a responsible governance structure for oversight and assurance reporting post the technical deployment	R2;R3	
Consider the need to accommodate requests for information that arises within the anticipated short retention period	R19	

Annexure 3 - Distracted Driver / seat belt compliance trial

This trial involves the deployment of three roading management cameras to detect the incidence of distracted driving. Using a mobile phone while driving is the predominant cause of distracted driving while other activities may also be relevant, such as reading printed material and consuming food.

In addition the camera system is capable of determining whether the front seat occupants are wearing a seat belt. The camera will be deployed to provide analysis of this behaviour.

Waka Kotahi is trialling a camera system provided by Acusensus Pty Ltd of Australia, the *Acusensus Heads-Up Solution*. The system is designed to detect illegal mobile phone use by drivers. Using artificial intelligence the camera system detects drivers whose hands are not both on the steering wheel of the vehicle and are potentially otherwise occupied with a mobile phone. The system is also able to detect if front seat occupants are wearing seatbelts. A wide front of vehicle still photo image is captured along with an additional zoomed in close up still image of the driver.

All vehicles passing the camera site are photographed. Images that do not identify a distracted driver or an unrestrained occupant are deleted at the camera. Those of an apparently distracted driver or unrestrained occupant are packaged in an encrypted file (described as a *evidential package*) and forwarded to an Acusensus server on the Amazon Web Services Cloud solution in Australia. The decryption key is held only by *Waka Kotahi.* A verification process is undertaken by human resource to determine a valid distracted driver or unrestrained occupant. If the human verification process has not occurred within 48 hours of delivery the images are automatically deleted.

The trial is to ascertain the effectiveness of the *Acusensus Heads-Up Solution* and ascertain the extent of non-compliance over a 6 month period at three sites within the Auckland roading network. *Waka Kotahi* will manually check and adequate sample of the *evidential packages* to

Personal Information

The individual images packages of an incidence of a distracted driver contain limited information. The package will identify the particular site of the camera and therefore the monitored roading space. The vehicle registration plate, passengers and the face of the driver will be automatically blurred prior to becoming part of the *evidential* package.

The evidential packages will be retained in an Acusensus server on AWS Australia.

The verified distracted driver's information will be used in an anonymous manner to determine the statistical efficacy of the *Solution* and establish the volume of non-compliant road user behaviour. This analysis will be carried out by Acusensus who will forward statistics to *Waka Kotahi.* In addition to all data being destroyed and deleted at the end of the trial, auto deleting of data will occur regularly during the trial either on a weekly or monthly basis.

At the completion of the trial all *evidential* packages information will be destroyed.

establish the rate at which the solution positively identifies a distracted driver. No drivers will receive infringement notices, warnings or communication from *Waka Kotahi* as a result of the trial. No searches of the regulatory databases (such as the Motor Vehicle or Driver Licence Registers) are being performed. Public advice about the future advent of the trial is contemplated without disclosing the exact site of each camera deployment to avoid a prejudice to the acquisition of accurate statistics of the rate on driver non-compliance.	

Intended Controls

- Information that does not identify a distracted driver or seat belt not used, will not be retained, and deleted at the camera.
- Information that apparently identifies a distracted driver or lack of seat belt deployed, *evidential packages,* will be delivered to the trial storage server with limited information. Passengers, registration details and the driver's face will all be blurred.
- *Evidential packages* will be assessed by trial staff to provide assurance that the images confirm a distracted driver event.
- *Evidential packages* not analysed within 48 hours will be automatically deleted from the system.
- *Evidential packages* are encrypted from the camera to the storage server at Amazon Web Services in Australia.
- File decryption keys will be held only by *Waka Kotahi.*
- *Evidential packages* information will not be used to the detriment of the non-compliant individuals – no infringement notices, warning or other communications will be issued by *Waka Kotahi* during or because of this trial.
- During and at the completion of the trial all information acquired including *evidential packages* will be deleted and destroyed.

Recommendations specific to the Distracted Driver Proof of Concept Trial	Recommendation Reference	Date • Accepted • Implemented
Designate an appropriate governance group to have oversight of the trial taking into account the overall need to establish adequate governance for the whole of the roading management camera system	R2	
Consider the requirements for technical security within the roading management camera system and storage that is commensurate with the *Waka Kotahi* responsibility for security	R9	
Ensure the AWS system logs access to and activity within the *evidential packages* in the event that an audit of the access to the information is required.	R11	

Ensure that *Waka Kotahi* accountabilities and responsibilities are reflected and passed onto Acusensus in contractual agreements.	R12; R14; R15	
Despite limited personal information and a short trial it is appropriate to designate users for the analysis of the information so that access is limited to defined and appropriate staff	R10	
Establish assurance reporting about the technical and analytical aspects of the system as required in the context of the proof of concept trial	R16	
Devise a strategy for advising the public and other stakeholders about the trial except if there is a reasonable expectation that the trial might be prejudiced if the exact locations of the trial cameras are divulged	R8	

Annexure 4 - Automation of verification business rules.

NOTE: This annexure 4 was drafted by Waka Kotahi. It has been attached to the Simply Privacy PIA for ease of reference, and because the general principles in the PIA will apply.
This note has been added for clarity of authorship.

Overview
This annexure focuses on ensuring the integrity and reliability of personal information in the context of an automated verification process. This involves Waka Kotahi taking reasonable steps to ensure that the information being used in an automated verification process is accurate, complete, relevant, up to date and not misleading.

Appropriate controls to be implemented by Waka Kotahi will ensure that an automated verification process functions appropriately and that decisions based on the process are defensible, particularly if these result in infringement notices being issued or prosecutions taken.

In the context of safety cameras, 'automation' is essentially automating a set of business rules. Automating business rules is the simplest form of algorithm. Rather than a human undertaking a function in compliance with those business rules, an automated process will do this. It is expected that it will do so very quickly, accurately, securely, and consistently, leading to significant increases in productivity and an ability to manage high volumes. Unlike more sophisticated algorithms, automated business rules do not interpret or evaluate large complex data sets to predict future behaviour or risk. Nor do they do so to identify patterns and trends.
Waka Kotahi intends automating the verification process for spot speed and point-to-point offences.

Background

Section 139 of the *Land Transport Act 1998* (LTA) requires an enforcement officer to have reasonable cause to believe an infringement offence has been committed by a person in order for an infringement notice in respect of that offence to be issued to that person by an enforcement officer. NZ Police currently meet this

Personal Information

Refer camera image at the end of this annexure.

This personal information will input into the verification process, whether manual or automated.

statutory requirement through a manual verification process.

Description of the verification process

The proposed Waka Kotahi verification process (whether manual or automated) will involve the following:

1. The speed threshold (amount over the speed limit allowed before an infringement notice would be issued) is triggered by a vehicle as it passes a safety camera
2. The camera will take an image of the offending vehicle and overlay that image with an associated data block (refer image at the end of this annexure).
3. The image will be reviewed and associated meta-data (which may include such things as image quality, target vehicle geo location information, radar signal 'strength' etc) will be used to confirm:
    a. a speeding offence has been committed
    b. the offending vehicle is clearly identifiable (e.g. if there are two or more vehicles in the image, ensuring the offending vehicle is clearly identified, vehicle attributes such as make and model match those in the Motor Vehicle Register (MVR) for that registration plate etc.)
    c. the image quality is sufficient for evidentiary purposes (e.g. no sunbursts, the plate is not blurred, etc).
    d. the vehicle registration plate can be matched to the registered person (owner) in the MVR
    e. there is an address where an infringement offence notice can be sent.
4. If all of these are confirmed Waka Kotahi can have reasonable belief an offence has been committed and an infringement notice can be correctly populated and issued to the registered person for the offending vehicle. The incident data will then progress to the offence processing/issuing stage.
5. The image and associated meta-data are auto-deleted from the camera.
6. If there are any issues with any of the above, for example meta-data may flag image quality as being lower than desired or the target vehicle's geo location information appears to be outside tolerances, the image will go for a 'second opinion' (in the automated process this would be manual verification)
7. There will be a record made in the workflow process of the various verification checks as outlined above.
8. There will also be a record of the decision made in the workflow process – to progress to offence processing, send for further checks, or reject.

9. If the decision is not to issue an infringement notice, the image and incident data will be retained for a few days (exact duration yet to be determined) to allow any Quality Assurance checks to be made retrospectively if required. 10. After this period has expired, the image and associated meta data will be deleted from the verification workflow. If the decision is made to issue an infringement notice, the image and incident data will go to the offence processing part of the system and be used to populate the infringement notice.	

Intended Controls

- Both the manual verification and the automated verification processes will get the same image and associated incident data from the camera.
- The data will be encrypted in transit, and at rest.
- Both manual and automated verification processes will do the same quality assurance checks.
- If there are any issues with any of the above, the image will either be rejected or go for manual verification.
- If there are no issues, the image and incident data will progress to offence processing.
- There will be a log of both automated and manual decisions made for auditing purposes under both processes.
- The same details will be retained under both a manual and automated process - that the image and associated meta data was verified, and a decision made to either progress or not to offence processing.
- If the decision is not to issue an infringement notice the image and incident data will be retained for a few days (exact duration yet to be confirmed) before being deleted.
- If the decision is made to issue an infringement notice the image and incident data will remain in the offence processing part of the system and be used to populate the infringement notice.
- The security of the image and incident data will be the same under both the manual and automated processes.
- Waka Kotahi intends to comprehensively check the accuracy of the incident information by having cameras roadside in 'test' mode capturing incident data and sending it through for manual verification. No infringement or traffic offence notices would be issued during this Quality Assurance initial deployment phase.
- A separate annexure is under development to cover off data retention, deletions and use in this camera 'test' phase.
- Once the offence processing system is in place, manual verification will be used for approximately six months, by which time the automated components of the safety camera system are expected to have been have built. From there, both manual and automated verification processes will operate, with cross-checks undertaken to check the accuracy levels and security of the latter for a further six months.
- Moving to a greater reliance on automation will only occur when Waka Kotahi is confident the automated process is working as expected and automation can satisfy Section 139 of the LTA i.e. the automated process is providing reasonable cause to believe an infringement offence has been committed.
- Waka Kotahi will have an audit programme to regularly audit a percentage (yet to be determined) of images/incident data to ensure the automated process is working as expected.
- Manual verification will remain as a process for those occasions where the automated process:
    - rejects some aspect of the image or associated incident data
    - cannot identify the registered person for a vehicle
    - involves vehicles such as ambulances, fire engines, Police cars etc which have statutory defences in the Land Transport (Road User) Rule 2004 from speeding and red light running.
- Automated verification will initially only be used for offences detected by spot speed and point-to-point cameras (fixed and mobile). Offences detected by red light cameras are unlikely to be verified under an automated process. This is because of the high number of exceptions that can occur due to the many intersections having lanes with different light phases. For example, a lane with a green light for 'straight through' traffic alongside a lane with a red light for turning traffic. Video and manual review will continue to be used for red light offences in the foreseeable future.
- Cameras will be initially calibrated and then re-calibrated annually to ensure they are operating appropriately. Each camera will contain a record of calibration, and an associated certificate of

calibration issued for use as evidence if an infringement is challenged. These certificates will be retained in Waka Kotahi's information management system.

- An assessment of compliance has been undertaken against Government's data and analytics principles, jointly developed by the Privacy Commissioner and the Government Chief Data Steward (refer next section).
- The overall safety camera system will be required to comply with the Waka Kotahi 'Minimum Non-Functional Requirements (NFRs) for Systems'. The expectation is that independently of the system's primary function, information and records captured and managed through the system must be accessible, protected, trustworthy and maintained for as long as required by the business, and by relevant legislation and regulators (e.g. *Public Records Act 2005*, Archives NZ).
- Draft NFRs on collection and data retention have been developed, covering:
    - retention and disposal
    - monitoring
    - audit and logging
    - access control
    - integrity
    - accountability
    - virus protection
    - vulnerability management
    - security event management
    - security testing and review
    - security incident management
    - legislative compliance
    - applicable Standards.

Recommendations specific to Automation	Recommendation Reference	Date • Accepted • Implemented
Create business processes to provide assurance the technical system is accurate and reliable	R16	Will be implemented – initially as manual processes
Create business processes to provide for human oversight of roading management camera data to contribute to decision-making	R17	Will be implemented – initially as manual processes

Principles for the safe and effective use of automated business rules

As outlined in Section 1.5 of the PIA, Government has developed a set of principles to guide the automation of algorithms such as business rules[17]. It is appropriate to apply these to the safety camera system as the business rules will determine whether or not an infringement notice will be issued to the registered person of the offending vehicle.

The principles are automating business rules must:

- deliver clear public benefit – particularly when they involve decision-making
- ensure data is fit-for-purpose – including accuracy and completeness
- have a focus on people – recognising automating the processing of safety camera images to issue (or not) infringement notices will have real-life impacts
- maintain transparency – ensuring business rules automation is explained to the public, simply and clearly
- reflect an understanding of the limitations – avoiding bias, unfair or discriminatory outcomes

[17] ibid

- retain human oversight – ensuring human judgement and evaluation remain an integral part of the decision making

Assessment against these principles

Principle	Assessment
Clear public benefit	The safety camera programme is a key component of the Government's *Road to Zero* strategy to reduce deaths and serious injuries. It is expected automating the business rules around incident verification and infringement issuing will reduce the time to undertake these tasks, resulting in greater productivity and the ability to manage higher volumes as the number of safety cameras increases.
Data is fit-for-purpose (confidence in the data from the cameras is relevant, accurate, consistent)	The HALO cameras have in-built capabilities in the form of 3D high-definition radar beam and target vehicle mapping. When configured for **spot speed**: • The 'raw' evidence files from the HALO cameras include at least two images (the second being used to validate the first) and up to six images, a video file, a summary .pdf file of all images captured, .txt and .xml data files including log files and meta data recording camera activity and data captured. These files are captured and stored unaltered in a separate 'evidence' file repository and are available for future use should an infringement or traffic offence be challenged – unless deleted if a decision is made not to proceed to offence processing. • These raw evidence files are then processed by the 'Extractor', a fully configurable tool that can define which file types, files, and data within those files are copied and then used to process the incident. Waka Kotahi will specify which data elements it needs to have for evidential sufficiency and the 'Extractor' will be configured accordingly. • After the Extractor, the image and video files are available for incident processing. The image files are overlayed with indicators to positively identify the target vehicle has breached the speed threshold for the site's posted speed limit. These indicators include: confirming vehicle direction, comparing vehicle placement between images to confirm distance travelled over time, direction of speed, and a number of other checks (yet to be determined based on what has been configured as available post-Extractor). Site and camera calibration will also be verified. • The HALO camera can map the target vehicle's outline or overall 'shape' as the 3D beam can apply multiple location coordinates to the image. This will enable target vehicle identification to a much higher standard than the current NK-7 cameras operated by NZ Police.

Principle	Assessment
	• The HALO beam radar can also capture other vehicle attributes such as colour, vehicle type, length and axle counts which could be used with MVR data to further verify target vehicle attributes (e.g. truck vs car) • In addition, the image files have a 'data block' inserted at the top of the image. The data block contains the incident's day of the week, date of offence, time of offence, recorded speed, travel direction indicator, lane indicator, posted speed limit, site code, and unique incident identifier. • The vehicle's registration plate details are inserted into the data block using Optical Character Recognition (OCR) – technology that can identify, capture and return registration plate details When configured for point-to-point (P2P - average speed): • The same camera technology is used as for spot speed but augmented by Alcyon Express (middle ware that sits between the camera and back-office data storage – used to undertake calculations between Camera A and Camera B at either end of the enforcement corridor) which performs P2P target vehicle matching using OCR. • Alcyon Express will match vehicles entering the speed corridor to those exiting it, calculate average speed over distance and identify target vehicles over the average speed threshold, match them, and then generate an incident file. This file will go through the same verification process as spot speed incident files.
People focus	Processes will be put in place to enable infringement notice recipients to query/challenge the infringement notice, and request a copy of the incident image.
Transparency	There will be a comprehensive Communications and Engagement Plan developed and ready leading up the automated process being utilised.

Limitations	Limitations will be mitigated:
	
	• Both the manual verification and the automated verification processes will get the same image and associated incident data from the camera.
	
	• The data will be encrypted.
	
	• Both processes will do the same quality checks.
	  ○ If there are any quality issues, the image will go for manual verification
	  ○ If there are no issues, a decision will be made under both processes to progress to offence processing
	  ○ There will be a log of decisions made for auditing purposes in the workflow under both processes
	  ○ The same details will be retained - that the image and associated was checked, and a decision made.

Principle	Assessment
	○ If the decision is not to issue an infringement notice then the image and incident data will be retained for a few days (exact duration yet to be determined) before being deleted ○ If the decision is made to issue an infringement notice then the image and incident data will remain in the offence processing part of the system and be used to populate the infringement notice. ○ The security of the image and incident data will be the same under both the manual and automated processes. Offences detected by red light cameras are unlikely to be verified through an automated process given the complexity of the circumstances e.g. different lanes with different traffic signals – such as lane 1 with a green light to go straight through, lane 2 with a red light to turn right).
Human oversight	A manual verification process will be retained to deal with exceptions. If, for some reason, the automated verification process fails to perform as expected then the manual verification process can be used instead.

Annexure 5 - Stage 2 Safety Camera Rollout

(June 2023)

NOTE: This annexure 5 was drafted by Waka Kotahi. It has been attached to the Simply Privacy PIA for ease of reference, and because the general principles in the PIA will apply.
This note has been added for clarity of authorship.

This annexure focuses on the activation of Stage 2 of the safety camera rollout programme. This stage involves having a fixed spot speed camera active on the roadside with appropriate safeguards in place, and a Waka Kotahi team capable of manually verifying and determining offences. It is part of the rollout that allows Waka Kotahi to pressure-test systems and processes on a smaller scale between 30 June 2023 – 30 November 2023 before the cameras go live and start enforcing speeding offences.

Stage 2 includes looking at the camera and the core camera management system and how data is captured, processed and verified. It will have a focus on:

- how data is captured by the camera – including, but not limited to, the use of automatic number plate recognition (ANPR) technology
- how this data is transferred, stored and retained in Redflex (camera vendor) and Waka Kotahi systems (including temporary off-shore storage),
- how offences are manually verified, and
- how infringement notices and traffic offence notices are made ready for issuing (but not issued).

Stage 2 will also involve preparations for testing point-to-point (average speed) camera technology in a controlled (off-road) environment before being trialled roadside in Stage 3. Another annexure to the PIA will be completed ahead of the Stage 3 roadside trial taking place.

Stage 2 will not involve:

- sending 'safety notices'
- issuing infringement or traffic offence notices
- point-to-point (average speed) cameras active on the roadside
- use of ANPR technology to collect the vehicle details of every vehicle passing the camera.

.Annexure 5 – Stage 2 Safety Camera Rollout

Waka Kotahi intends to activate a new safety camera network starting with a rollout of new HALO spot speed cameras.

Background

The camera rollout programme comprises four stages:
Stage 1 – testing in a controlled environment
Stage 2 – operating roadside, verifying offences but not enforcing
Stage 3 – operating roadside, enforcing offences
Stage 4 - continue camera expansion, including transfer of camera assets from NZ Police
This annexure covers Stage 2 of the rollout.

Description of Stage 2

In this stage:

- one fixed spot speed safety camera will be installed roadside in Te Tai Tokerau Northland
- it will use technology to capture data on vehicles exceeding the set speed threshold, including ANPR to capture licence plate details.
- an interim data repository process will be developed to enable the use of the offence data for verification and infringement issuing process testing
- this data will be used to test the manual verification process to identify whether:
    - a speeding 'offence' has been committed
    - the 'offending' vehicle is clearly identifiable (e.g. if there are two or more vehicles in the image, ensuring the offending vehicle is clearly identified, vehicle attributes such as make and model match those in the Motor Vehicle Register [MVR] for that registration plate etc.)
    - the image quality is sufficient for evidentiary purposes (e.g. no sunbursts, the plate is not blurred, etc).
    - the vehicle registration plate can be matched to the registered person in the MVR
    - there is an address where an infringement offence notice can be sent.
- The offence issuing system will also be tested in so far as infringement notices will be populated but not issued
- Data will also be collected for research and analytics purposes, such as measuring speeds during the test period

Personal Information

Personal information collected will be:

1. Images of the registration number of the vehicle and other meta data will be captured - which may lead to identifying the registered owner of the vehicle.
2. Meta data that includes time, date and location of images and direction of travel.

Use of ANPR technology to collect registration plate details of 'offending' vehicles

ANPR is image-processing technology that converts an image of a registration plate into decipherable text using optical character recognition software without any human intervention. Such technology is critical to the operation of average speed point-to-point cameras. While it is not necessary to operate the HALO spot speed cameras, Waka Kotahi is taking the opportunity in Stage 2 to test the accuracy and reliability of ANPR.

Testing of ANPR technology will focus on matters such as:

- how well does it recognise plates,
- how well it can recognise the fonts used on NZ plates
- how well it converts the plate image into recognisable characters
- how does it cope with vehicles that have a plate in a non-standard place
- whether it can capture vehicle details if several offending vehicles go past or does it miss offending vehicle plates.

ANPR tends to be controversial. It can create concerns about privacy intrusions and other intrusions into civil liberties. A major concern with ANPR is that networks of cameras are capable not only of tracking individuals across a particular journey, but also that retaining that information may build up a database of vehicle movements over time.

The intended controls outlined below aim to mitigate these concerns.

Stage 2 Safety Camera Rollout (cont)	

• The data flows will involve:
  ○ Offending vehicle details flowing from the Redflex camera into the Redflex camera management system
  ○ A secure network transfer into Waka Kotahi storage, currently sitting with Amazon Web Services (AWS) in Sydney, Australia, for middle office incident file creation
  ○ transitory storage in AWS only
  ○ integration through Azure Sydney to middle office incident file storage location for 30 days, ready for offence verification by Waka Kotahi
  ○ transfer into the New Zealand-based Waka Kotahi verification and offence processing production systems and becoming personal information (by virtue of being linked with registered person details in the MVR) so as to pressure-test the verification/infringement issuing processes prior to enforcing offences in Stage 3.	

Intended Controls

- **Clear purpose for camera use**: The clear purpose of Stage 2 is to have a roadside camera collecting vehicle details in 'test' mode to enable the pressure-testing of the manual verification and infringement issuing processes by Waka Kotahi – without issuing any infringement or traffic offence notices, and not storing personal information for any longer than is necessary to test the verification and infringement issuing processes.

- **Governance**: Safety Camera Programme management will provide oversight and governance to ensure privacy obligations are adhered to throughout Stage 2.

- **No enforcement**: Personal information (in the form of registration plate details that will then be matched to the MVR to identify the registered person for each offending vehicle) will be collected but no enforcement action or infringement notices will be issued.

- **Only critical data will be collected**: only 'offence' data will be captured by ANPR technology. ANPR will not be used to collect and retain the vehicle details of every vehicle that passed the camera. The 'offence' data may include still images and video footage with associated meta-data such as incident day of week, date of offence, time of offence, recorded speed, travel direction indicator, lane indicator, posted speed limit, site code, and a unique incident identifier.
  Non-personal survey data would also be collected for a research and analytics purpose. This will include anonymised data such as vehicle counts, overall speed data, offences detected, and camera performance metrics.

- **Security:** This data will be encrypted in transit, and at rest. The images will be stored digitally and cannot be overwritten or altered.

- **Offshore storage of offence data:** As noted above, offending vehicle details including registration plates will be stored by Waka Kotahi temporarily with AWS and Azure in Sydney, Australia awaiting transferral into the manual verification/offence processing production systems.
  Data sovereignty risks will be mitigated by:
  - such storage being temporary until such time as a storage centre is built in New Zealand (expected to be 2024)
  - Waka Kotahi already stores data with AWS and holds security certification and accreditation for this off-shore storage.
  - the data classification meeting security requirements for storage in Australia (and New Zealand)
  - this temporary storage solution will be reviewed for Stage 3 (and will be outlined in the proposed Stage 3 PIA).

- **Clear 3rd party accountabilities and responsibilities**: Redflex (the camera vendor) and temporary Waka Kotahi data storage providers are contractually required to (among other things):
  - comply at all times with New Zealand privacy laws
  - comply at all times with the Privacy at Waka Kotahi the NZ Transport Agency – A Guide for Suppliers and Service Providers (https://www.nzta.govt.nz/about-us/about-this-site/privacy-guide-for-suppliers-and-service-providers/)
  - meet Waka Kotahi security standards
  - allow for independent security audits and action audit findings
  - take all reasonable steps to prevent security breaches or unauthorised use
  - notify Waka Kotahi if any breaches or unauthorised use occurs and take steps to identify those involved, stop the occurrence and prevent any reoccurrence.

- **Access to camera** will be managed by security protocols built into the camera. On-site and remote access to the camera and the associated camera management system will be protected by a camera/back office unique identifier, a unique password as well as an additional password to coordinate all the various components to detect and create incident files.

- **User access will be logged**: The cameras record audit-related data for access and operational mode changes by user ID. Audit logs are maintained for access and changes made in the camera management system. Access log information is stored and available for auditing in the camera management system. These logs will be regularly reviewed and audited by the Safety Camera Management System Programme.

- **Data minimisation**: Throughout Stage 2 Waka Kotahi staff will have access to the vehicle data collected by the cameras. This is for the purpose of testing and modifying (if required) the end-to-end verification/offence issuing process, performing quality checks, and resolve issues. These staff will be made aware of their privacy obligations.

- **Limited retention period:**
  - Offence data captured by the Redflex camera will be deleted by Redflex as soon as it passes from the camera management system into the Waka Kotahi production system.
  - Vehicle plate detail held by AWS will be transitory in nature and AWS will be instructed not to retain any data once it passes onto Waka Kotahi systems in Azure. Once with Azure, Waka Kotahi will have full control over storage and retention (refer below for retention policy).
  - Offence data collected in Stage 2 will only be retained in the Waka Kotahi production system up until the end of Stage 2 on 30 November 2023 (i.e.) for a maximum of 5 months. Retention during Stage 2 is to enable re-testing of processes using the same offence data. For example, the same offence data could be used to re-test different verification scenarios. At the end of Stage 2, all offence data will be deleted from its systems by Waka Kotahi.
  - A small number of incident files will however be retained for training purposes but the personal information will be altered so as not to identify the offending vehicle or the registered person.
  - Anonymised survey data such as number of vehicles that passed the camera, and vehicle speeds will be retained indefinitely for research and analytic purposes.

- **Public awareness**:
  - Iwi, hapū, and local communities have been consulted on the roadside camera location
  - A public education strategy will support Stage 2. It will provide details on:
    - what's happening
    - why it is happening
    - when it is happening, and
    - what it means for the public/individuals
  - Use will be made of existing Waka Kotahi Customer Service Centre processes, tools and systems to record and respond to requests regarding the personal information collected in Stage 2.

- **Use of data**: as noted above, the data will be used to collect 'offending' vehicle details to enable the testing of the manual verification and offence issuing processes, and to collect anonymised survey data prior to enforcement getting underway in Stage 3.

- **Disclosure of data**: The only 3rd parties that will have access to offending vehicle details will be those listed above. This information will not be shared with 3rd parties such as NZ Police or Ministry of Justice. Such details will solely be used to pressure-test test the manual verification and offence issuing processes prior to the cameras being used for enforcement purposes in Stage 3.

Recommendations specific to Stage 2 (from wider Waka Kotahi roading management camera PIA)	Recommendation Reference	Action • Accepted • Implemented
Establish at an early stage the primary and directly-related purposes for using a roading management camera system and collecting personal information.	R6	Implemented for Stage 2 (refer intended controls)
Establish policy or guidance for each targeted deployment of roading management cameras, that prescribes the expectations of data minimisation so collection of unnecessary personal information is eliminated.	R7	Implemented for Stage 2 (refer intended controls)
Implement a transparency strategy to cover the deployment of a roading management camera system including comprehensive advice through appropriate agency channels.	R8	Implemented for Stage 2 (refer intended controls)
Establish technical security within the roading management camera system and storage that is commensurate with Waka Kotahi responsibility for security	R9	Implemented for Stage 2 (refer intended controls)
Develop a carefully designed set of user roles for access to retained information, ensuring access to personal information is limited to the appropriate staff.	R10	Implemented for Stage 2 (refer intended controls)
Ensure the system logs access to and activity within the roading management camera data and the log is audited	R11	Implemented for Stage 2 (refer intended controls)
Ensure accountabilities and responsibilities are reflected and passed on to 3rd parties who undertake technical storage facilities or business processes on behalf of Waka Kotahi	R12	Implemented for Stage 2 (refer intended controls)
Support staff to use the roading management camera data appropriately through adequate guidance and/or training.	R13	Implemented for Stage 2 (refer intended controls)
Take steps to ensure 3rd parties recognise and report any data breaches including near misses	R14	Implemented for Stage 2 (refer intended controls)
Create business processes to provide assurance the technical system is accurate and reliable.	R16	Implemented for Stage 2 (refer intended controls)
Create business processes providing for human oversight of roading management data that contributes to decision-making	R17	Implemented for Stage 2 (refer intended controls)
Set retention periods for personal information collected by individual roading management camera systems.	R18	Implemented for Stage 2 (refer intended controls)
Create policy defining the limited purposes for which the roading management camera system collects personal information and reflect the limited purposes in Waka Kotahi retention, use, and disclosure rules.	R21	Implemented for Stage 2 (refer intended controls)

Annexure # - Template

Personal Information

Intended Controls •		
Recommendations specific to Point to Point Cameras	Recommendation Reference	Date • Accepted • Implemented