FINAL Report: 14 February 2022

The Department of Transport and Main Roads

FOR PUBLICATION

PRIVACY IMPACT ASSESSMENT REPORT AND INDEPENDENT REVIEW – MOBILE PHONE AND SEATBELT TECHNOLOGY (MPST)

IIS Partners

INFORMATION INTEGRITY SOLUTIONS

Contents

Glossary

Abbreviation or term	Expansion or definition
AI	Artificial Intelligence
APPs	Australian Privacy Principles in the *Privacy Act 1988* (Cth).
CDOP	Camera Detected Offence Program
CRN	Customer Reference Number
EMC	Executive Management Committee – Project Board
EMC SIG	EMC – Strategic Implementation Group
HRA	*Human Rights Act 2019* (QLD)
IIS	Information Integrity Solutions Pty Ltd
IP Act	*Information Privacy Act 2009 (QLD)*
IPP	Information Privacy Principles in the IP Act
MPST	Mobile Phone and Seatbelt Technology
PIA	Privacy Impact Assessment
QPS	Queensland Police Service
QRO	Queensland Revenue Office
SPER	The State Penalties Enforcement Registry
TMR	Department of Transport and Main Roads
TORUM	*Transport Operations (Road Use Management) Act 1995* (QLD)
TRAILS	Transport Registration and Integrated Licensing System
WOG SOA	Whole of Government Standing Offer Arrangement

1. Executive summary

The Department of Transport and Main Roads (TMR) engaged IIS Partners (IIS) to:

- Conduct an independent review of its draft Privacy Impact Assessment (PIA) on the Mobile Phone and Seatbelt Technology (MPST) project, and
- Complete a revised PIA that assesses the privacy risks of the MPST program and recommends actions to ensure privacy compliance, risk management and best practice.

The MPST program is part of the Queensland Government's Camera Detected Offence Program (CDOP). It uses camera technology and artificial intelligence (AI) to detect mobile phone and seatbelt offences. The project intends to address a significant public interest issue – the huge hurt and cost resulting from road deaths – and is expected to deliver significant benefits.

The use of 'smart' camera technology to conduct the MPST program carries potential privacy risks. These include broader privacy considerations beyond strict compliance with the law, arising in particular from the surveillance nature of the activity and that it involves the use of AI.

IIS assessed the MPST program as having a high degree of inherent privacy risk. The collection process involves surveillance and uses AI to identify possible offences. Individuals might not be aware of the activity, and there is potential for harm or embarrassment to individuals, particularly if they are wrongly identified as infringing the mobile phone or seat belt rules (false positives).

IIS believes the risks are offset however, by the project's privacy positive features, which include:

- The collection and use of images for the MPST program is authorised by law
- The program avoids one of the major risks from AI – while possible offences are identified by the AI, decisions about offences are not automated, and instead:
  - offences are validated by human review (at three separate points)
  - individuals are given copies of the 'offending' images and have the right to seek a review of the decision or to challenge it in court
  - individuals can provide evidence if they have an exemption from the seatbelt rules or medical exemptions from wearing a seatbelt
- Images are deleted relatively quickly from the cameras and systems, once an offence is ruled out
- TMR has advised that biometric information will not be captured or analysed by the program,[1] and
- TMR has taken privacy into account from the outset, with steps including strong requirements in its contract with the camera and AI provider, a focus on accuracy and transparency in implementation, and its draft PIA.[2]

[1] Biometric information is discussed further in the analysis at 5.2.1.2

[2] Project Plan Camera Enforcement Distraction, Project Definition notes that 'The Queensland community has a reasonable expectation that their privacy will be maintained while travelling in vehicles on the network'

IIS considers that the residual risks for the MPST program (after implementing the above measures) are medium. IIS has identified some areas where it considers TMR should take additional steps to ensure compliance, or to promote better privacy practice. It considers that, subject to implementation of the report recommendations, the MPST program can operate in compliance with the *Information Privacy Act 2009* (IP Act).

IIS has made **22 recommendations** and **3 comments** which address key issues and areas of privacy risk. The recommendations focus on matters of privacy governance – both broadly at TMR and uniquely for the MPST program – and alignment of personal information handling practices with the IPPs.

The table below sets out a summary of our recommendations, as set out in Section 5, and risk treatments proposed by TMR.

IIS Recommendation	TMR Risk treatment
Rec 1: In consultation with the Privacy Team, formalise TMR's policy position on use of AI in decision-making.	
Rec 2: In consultation with the Privacy Team, formalise MPST-specific governance, including specific policies, procedures and accountabilities.	
Rec 3: Monitor decisions about MPST camera placements for patterns that could be construed as responsive to community characteristics (e.g., demographics, socio-economic). Take proactive steps to address related perceptions of program bias, such as through community outreach.	
Rec 4: Report MPST outcomes to the community at regular intervals. In addition, publish findings of any program evaluations undertaken.	
Rec 5: Conduct a further PIA on MPST within one year of commencing the enforcement phase.	
Rec 6: Conduct a PIA where it is proposed to expand the use or functionality of MPST cameras, or where there is a significant departure from the present MPST program specifications.	

IIS Recommendation	TMR Risk treatment
Rec 7: Review TMR's policy position in the context of Recommendations 3 and 4 on: 1) deciding MPST camera locations and 2) monitoring decisions for perceived bias.	
Rec 8: Explore with the Privacy Team opportunities for the MPST adjudication team to receive tailored training about privacy considerations specific to their role.	
Rec 9: Continue to promote the MPST program through various communication channels to ensure community awareness that their personal information may be collected remains high.	
Rec 10: Update TMR Privacy Policy to include reference to camera-enabled offence detection and the collection of relevant images.	
Rec 11: Continue proactive disclosure of information about TMR operations through publication of MPST-specific information on the TMR website.	
Rec 12: Continue training the AI in the MPST cameras to correctly detect mobile phone use and seat belt offences, whereby irrelevant images (those indicating no offence) are not retained for the adjudication process.	
Rec 13: Continue to implement recommendations arising from the TMR Information Security Risk Assessments of the MPST program.	
Rec 14: Routinise the receipt of vendor audit logs associated with the pre-adjudication process.	
Rec 15: Urgently open discussions with the MPST program Board to: 1) communicate a requirement for a secure-access facility accessible only to the MPST adjudication team; and 2) seek resolution to accommodation issues prior to 30 November 2021.	

IIS Recommendation	TMR Risk treatment
Rec 16: Urgently address physical security considerations and operational challenges relating to accommodation.	
Rec 17: Seek urgent advice of the Privacy and Records Management teams as regards secure destruction and management of MPST images and associated records.	
Rec 18: Conduct longitudinal analysis of accuracy of QA adjudicator decisions (with learnings to be incorporated into MPST adjudication processes) and report on findings.	
Rec 19: Where a passenger seatbelt offence **is not** detected by an MPST camera, take steps to limit visibility of (or entirely obscure) passenger images through the further adjudication processes relating to the driver and any subsequent issue of infringement notice.	
Rec 20: Where a passenger seatbelt offence **is** detected, investigate whether passenger face (where visible in whole or in part) can be obscured when generating the infringement notice.	
Rec 21: Where the Regulations do not specify additional permitted **uses** of MPST images and other personal information, follow the overarching privacy governance requirements for MPST.	
Rec 22: Where the Regulations do not specify additional permitted **disclosures** of MPST images and other personal information, follow the overarching privacy governance requirements for MPST.	

The table below further sets out a summary of IIS comments, as set out in Section 5.

IIS Comment
Comment 1: The MPST program has been active in its outreach to the community, including through its use of signage, commercials, social media and 'warning letters' sent as an educative tool prior to the enforcement phase of the program. IIS commends this.
Comment 2: There is ongoing importance of making information about access and amendment of personal information associated with the MPST program easy for the community to find, easy to understand and use, and accurate in terms of the TMR processes a person will be required to engage with – particularly where there is a need to 'set the record straight'.
Comment 3: It is vital for the MPST program to reflect on the Privacy by Design considerations raised by Recommendation 2 in respect of avoiding function creep – not just within the MPST program, but where other areas of TMR may wish to leverage the MPST camera technology or use stored images for other purposes.

2. About the PIA

The Department of Transport and Main Roads (TMR) engaged IIS Partners (IIS) to:

- Undertake an independent review of TMR's draft PIA on the Mobile Phone and Seatbelt Technology (MPST) project, and
- Develop a revised PIA that takes account of developments since the draft PIA; assesses the privacy risks of the MPST program, and recommends actions to ensure privacy compliance, risk management and best practice.

2.1 Scope

The scope for this PIA includes:

1. The implementation of a camera solution designed to detect alleged mobile phone and seatbelt offences
2. The storage and review, use and disclosure of images containing customers and their vehicles
3. The generation of warning letters to customers involved in mobile phone and seatbelt camera detected incidents, and
4. The generation of infringement notices to customers deemed to have committed a mobile phone or seatbelt offence – including the images of the camera detected offence.

It was out of scope for the PIA to assess existing processes that will not change, including TMR printing and mailing of infringement notices via the TMR Mail House, and the SPER management of infringement notice debt.

2.2 Methodology

IIS took the following steps to carry out the PIA:

- *Planning* with TMR to confirm the approach and deliverable
- *Gathering information* by reading documents and meeting with staff from TMR, and with other stakeholders
- *Analysing* the information against privacy obligations and taking account of possible broader privacy issues, regulator guidance, and privacy best practice
- *Identifying privacy risks* and developing ways to mitigate those risks
- *Drafting the PIA report* and providing this to TMR subject matter experts, the camera and AI provider, and the MPST Board for comment on matter of fact only, and
- *Addressing feedback* and *finalising* the report.

3. Project description

3.1 Background

Driver distraction is a major cause of road crashes and contributes to almost 20% of serious injuries on Queensland roads.[3] Research shows that using a mobile phone while driving quadruples the risk of crashing.[4] Failing to wear a seatbelt also has significant impacts on the outcome of a crash for drivers and passengers. It is estimated that wearing seatbelts can reduce the risk of a serious injury crash by 50 per cent and death by 45 per cent.[5]

The Queensland Government is committed to improving road safety and reducing road trauma, by 1) reducing driver distraction from mobile phones and 2) encouraging correct seatbelt use. To support these actions, the government committed to expanding the Camera Detected Offence Program (CDOP) – which currently involves red light and speed cameras – to include a new capability that will use camera technology including artificial intelligence (AI) to detect mobile phone and seatbelt offences. A trial of the technology detected more than 13,000 drivers using their phones illegally and more than 2,000 drivers and front seat passengers not wearing seatbelts.

The capability is expected to deliver significant benefits to the community. However, the use of the cameras will be a surveillance activity with potential impacts on citizen privacy. AI, if not applied and managed appropriately, can also carry significant privacy risks. Privacy has therefore been a key consideration as the project has developed.

TMR has completed an initial implementation phase, in which possible offenders received a warning letter outlining the offence. The warning letter did not include images and no offence was recorded. The initial implementation phase ended in late October 2021. Following an 'air gap', to ensure all warning letters have been delivered, the MPST enforcement regime commenced on 1 November 2021. This phase will be supported by an extensive community awareness program.

TMR will continue to operate the program until is it bedded down and BAU processes are in place. TMR expects to transfer the management of MPST program infringement notices to the Queensland Revenue Office during 2022. The MPST program team has noted the imperative to revisit (and update where required) this PIA when the transfer to QRO is complete.

3.2 Program participants

The key participants in the MPST program are as follows:

- **TMR** is responsible for the MPST program

[3] https://www.qld.gov.au/transport/safety/fines/cameras

[4] https://www.qld.gov.au/transport/safety/fines/cameras

[5] Statistical statement from US National Highway Traffic Safety Administration (NHTSA), as referenced in https://streetsmarts.initiatives.qld.gov.au/seatbelts-and-restraints/factsheet

- **Camera and AI provider** provides the cameras, AI systems and software for the program and undertakes the initial 'human' adjudication about whether the images indicate a mobile phone or seat belt offence
- **Queensland Police Service (QPS)** works with TMR to develop and implement the program
- **Queensland Revenue Office (QRO)** will take on the MPST program during 2022
- **Community stakeholders** were consulted on the primary Act and Regulation amendments made in July 2020 and July 2021 respectively. Further, members of the community are directly affected by the MPST program, and
- **University of Adelaide** has been engaged to provide an evaluation framework of the mobile phone and seatbelt camera program. The University of Adelaide received statistical and high level data, that was subject to privacy and confidentiality requirements.

3.3 Applicable legislation

3.3.1 Transport Legislation

The primary legislative authority allowing mobile phone and seatbelt offences to be managed under the CDOP is the *Transport Operations (Road Use Management) Act 1995* (TORUM Act), amended by the *Transport and Other Legislation (Road Safety, Technology and Other Matters) Amendment Act 2020,* which commenced on 22 July 2021. The amendments include:

- S 113A(2) which permits linking the camera to the department's systems for the purposes of detecting an offence[6]
- S 113A(4) which states that Regulations can provide information about how an image from a camera-detected offence might be accepted and how images may be deleted if no offence is detected, and
- S 118 which allows someone who is being prosecuted for a camera-detected offence to inspect the image or video.

Regulatory amendments were also needed to support camera enforcement of mobile phone and seatbelt offences. These amendments are contained in the *Transport Legislation (Distracted Driver and other Matters) Amendment Regulation 2021*.

3.3.2 Privacy Legislation

TMR must also comply with the Information Privacy Principles (IPPs) in the *Information Privacy Act 2009* (IP Act). The IP Act applies to personal information, which is 'information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.[7]

[6] S 113A(2) pre-existed amendments, and remains an authorising provision

[7] IP Act s 12

Section 7(2) of the IP Act provides that privacy obligations operate subject to the provisions of other Queensland Acts relevant to the collection, use and disclosure of personal information. Therefore, TMR must comply with both the IP Act and other legislative provisions when managing camera detection footage that contains personal information. Where these above Acts are silent, TMR will comply with the IPPs when managing personal information.

The IP Act also contains requirements relating to the overseas transfer of personal information and contracted service providers.[8]

3.3.3 Human Rights Legislation

Section 25 of the *Human Rights Act 2019* (HRA) protects an individual's right to privacy and reputation. The Parliamentary process to pass the legislative changes to authorise the MPST program included consideration of a Statement of Compatibility of the proposed TORUM changes with the HRA. The Statement concluded that an impact on individual privacy or reputation is minor and justifiable when balanced against the road safety benefits (the right to life) and protections available to the individual and the community.[9]

3.4 MPST program components

3.4.1 Cameras and in camera AI

The camera and AI provider is providing high-definition cameras, that are triggered by radar and take multiple images of every vehicle passing the camera. This includes capturing the registration number plate as well as images of the front seats of the vehicle. There are two types of cameras:

- Fixed cameras – fitted to existing infrastructure and operating 24 hours, 7 days a week, and
- Portable/ mobile cameras – used at approved locations in both urban and regional areas for shorter periods.

TMR determines the mobile locations using a risk-based analysis of crash data, and provides the approved site location information to the camera and AI provider.

The cameras use AI software to filter images and detect possible mobile phone use by the driver, or failure to wear a seatbelt by the driver and/or front seat passenger. The AI software is located within each camera, rather than a central location. The approach is preferable to avoid sending images unless necessary.

The AI system is trained to apply business rules based on the requirements of the Regulations. The AI will use the camera images and translate it to a cropped image if it deems an incident has occurred based on its business rules. The cropped image is a zoomed-in image where the vehicle cannot be identified.

[8] IP Act s 33 and Chapter 2 (Part 4)

[9] The Statement is available at https://www.legislation.qld.gov.au/view/pdf/bill.first.hrc/bill-2018-106. Pages 8 and 9 deal with privacy issues.

3.4.2 Data components

The MPST project collects and handles the following data:

- Images of the front seats of a vehicle and registration number plate
- Metadata including the time, date, location and speed of the vehicle, and the direction the vehicle is facing relative to the camera
- A camera generated incident number
- name and address of the registered operator and Customer Reference Number (CRN) (where required to issue an infringement notice)
- Alternate driver details (where the registered operator nominates an alternative driver), and
- The registered operator's reasons for rejection of the infringement, including that a vehicle has been sold, disposed, stolen or illegally taken (where provided).

3.5 Information flows

IIS has reviewed the information flows associated with the MPST program, from the point at which cameras take images until TMR has issued an infringement notice. The information flow narrative and diagrams are set out in Appendix A.

3.6 Communications strategy

IIS understands that TMR undertook a range of stakeholder consultations as part of preparing the primary Act and Regulation amendments, which included engaging with members of the community; privacy and community advocates; and the Office of the Information Commissioner (OIC).

TMR also undertook a range of communication activities during the grace/ warning letter phase (June to September 2021) to help inform the community about the new MPST rules and enforcement, and has similar activities planned for the enforcement phase from 1 November 2021. The activities include:

- Communications with stakeholder and user groups, and government departments
- Messages on TMR 'assets' including TV content, messages on transaction receipts, webpages, registration and licence renewal notices, and variable message signs
- Social and other Media announcements
- Mass media campaign, including television and radio commercials, outdoor billboards, digital/social media advertising, and a campaign section on the StreetSmarts website, and
- Both StreetSmarts and TMR will announce the campaign/ enforcement phase via their social media platforms.

3.7 OIC consultations

3.7.1 OIC comments to TMR on draft PIA

TMR provided its draft report to the OIC in July 2021. The main concerns the OIC identified were:

- The need for clarity within TMR on the application of the regulatory instruments, in particular in relation to identifying risk and developing controls
- That the AI aspects of the MPST program, including the potential privacy risks, were not addressed in the draft PIA, in particular in relation to accuracy and potential for bias, and
- That the draft PIA did not refer to the trial phase, the issues that arose, benefits and deficits in the technology and how those have been tested and addressed.

3.7.2 IIS discussions with OIC

IIS met with the OIC while undertaking this PIA. Our PIA takes account of these discussions, and the OIC's earlier feedback to TMR. Indeed, IIS has identified similar issues. However, the views expressed in this report are our own. We are not intending to represent the views of the OIC.

OIC noted that the current approach includes good privacy measures, including, for example, that images are generally taken from the chin down and are not seeking to include faces.

The main areas where the OIC considered risks might remain are:

- The regulatory approach, where the primary legislation gives a broad authorisation for the program, does not specify permitted uses for MPST data, and includes the power to prescribe other offences. In OIC's view this leaves open the potential for function creep, noting:
    - The widening of the program early on, beyond the initial focus on mobile phone texting and other misuse. Seat belt offences were added at a later date. While there is a public interest justification, it also brought the collection of passenger images into scope
    - The possible ways in which the program might expand; for example, the inclusion of images of back seat passengers, adding new 'driver distractions' or adding facial recognition to the camera technology

  The OIC considered that any further expansions to the program would need to be carefully scrutinised to ensure they are justified and proportionate and that privacy is protected
- The application of AI, including the accuracy of the decisions about possible infringements, which could involve false positives or false negatives, and potential for discrimination
- The contracting arrangements, in particular in relation to personnel, where strong control measures and monitoring should be in place, and
- The need for transparency on deployment, including in relation to camera locations, and on outcomes for the program.

3.7.3 OIC feedback on this PIA

Prior to finalisation of this PIA, IIS received additional views of the OIC on risks canvassed within the body of the recommendations. The OIC's views were largely unchanged from those noted in 3.7.2, above. Notably, concerns remained in respect of:

- The application of AI and the ongoing importance of 'human in the loop' decision-making (which IIS notes is a broad public policy issue highlighted by the MPST program context), and
- The regulatory approach taken by TMR, wherein the spectre of function creep (which is discussed at length in our analysis) appears ineffectively dealt with in the Regulations.

4. Approach to risk analysis

In undertaking this PIA IIS considered:

- The draft PIA report TMR prepared
- The IPPs and other legislative requirements
- The OIC-specific advice on the draft PIA report from TMR and the MPST program generally, and
- Privacy best practice stemming from IIS's knowledge and experience.

4.1 Inherent privacy risks

IIS's risk analysis approach begins with identifying the inherent privacy risks, that arise from:

- The nature of the personal information to be collected and managed – for example, its quantity, sensitivity, and the potential for, and consequences of, misuse
- The range of people from whom the information may be collected
- The context in which personal information is handled at TMR – for example, senior management commitment to privacy, staff privacy skills and experience, the technical systems involved and the nature of the project
- The extent to which information is accessed or handled by third parties, and
- The likely community and/or media interest in the privacy aspects of the project.

Considering these points, IIS considers the information collection and sharing mechanisms that underpin the MPST have a high degree of inherent privacy risk because:

- The MPST program is a form of surveillance, which by its nature is privacy intrusive
- The MPST program uses AI as part of its processes; AI if not well implemented carries inherent privacy risks including potential for discrimination or for inaccurate decisions, and which is likely to attract community and media interest and scrutiny
- People might not be aware of the activity, and there is potential for harm or embarrassment to individuals, particularly if they are wrongly identified as infringing the mobile phone or seat belt rules (false positives) or are caught in illicit or embarrassing behaviour
- There is potential for harm to individuals if camera images are misused, lost or mishandled
- The MPST program is a complex new IT project, which is still being bedded down, and
- Cameras and software are provided by a contractor, whose staff also view the image to undertake pre-adjudication.

4.2 Positive privacy aspects

IIS has also identified positive privacy aspects of the MPST:

- The collection and use of images for the MPST program is authorised by law

- The program project avoids the major risks from AI:
  - While possible offences are AI identified, decisions about offences are not automated, rather they are validated by human review (at three separate points)
  - People are also given copies of the 'offending' images and have the right to seek a review of the decision or to challenge it in court. They can also provide evidence beforehand, which is included in TMR systems, if they have an exemption from the seatbelt rules such as those provided for vintage or classic vehicles or medical exemptions from wearing a seatbelt
  - Steps to prevent bias include:
    - AI improvements/training is based on yes/no responses in pre-adjudication and adjudication of incidents based on cropped images with identifying information, including number plates, removed to the extent possible
    - 'Human' quality control reviews by the camera and AI provider and TMR to help ensure decisions are accurate and consistent
- Images are deleted relatively quickly from the cameras, and from the camera and AI provider's systems, once an offence is ruled out,[10] and
- TMR has taken privacy into account from the outset, with steps including strong requirements in its contract with the camera and AI provider, a focus on accuracy, and transparency in implementation, and its draft PIA.[11]

4.3 Residual privacy risk level

IIS considers that that the residual risks for the MPST program is medium. Factors affecting this assessment include that:

- TMR is implementing recommendations from its PIA and security assessments, but there are still some actions to complete
- The cameras might capture sensitive or irrelevant details, including about passengers where there is no seatbelt offence
- AI is still a new technology with inherent risks, which continue to need to be managed with care
- The program is still in its early stages and needs to be monitored closely to ensure arrangements with the camera and AI provider are working as intended, and to ensure any accuracy or security risks are quickly identified and dealt with, and
- The MPST legislative approach, which includes primary legislation which is broadly worded, and specific offences set out in Regulations, means there is potential for 'function creep' where images or technology are used in new ways which may be unexpected or unwelcome to the community.[12]

[10] The Regulations include clear rules for deletion of images where no offence is detected by the MPST cameras.

[11] Project Plan Camera Enforcement Distraction, Project Definition notes that 'The Queensland community has a reasonable expectation that their privacy will be maintained while travelling in vehicles on the network'

[12] TMR's position is that legislative change would be required if MPST cameras are proposed to be used for other functions.

5. Findings and recommendations

IIS considers that the MPST program can be implemented in compliance with the IP Act and its component IPPs. However, this requires measures that provide a high degree of privacy rigour – for example, those associated with the use of camera technology to detect offences, AI-supported decision-making, and handling of personal information (in particular, driver and passenger images) – and ongoing visibility of TMR's commitment to privacy best practice while performing its law enforcement functions.

This section discusses key issues and privacy risks associated with the MPST program. It provides recommendations for TMR to mitigate or otherwise treat the identified risks. IIS has structured its analysis to account for matters of privacy governance, generally, and IPP compliance, specifically.

The risks treated in the recommendations do not represent *all possible risks* associated with the MPST program; rather, they are the risks IIS considers to be most pertinent to privacy and personal information management in the context of the program at this time.

5.1 Privacy by Design and related considerations

The responsibility for privacy compliance within TMR rests with the entire agency, at all levels of seniority and across all functions. To this end, IIS considers that ensuring a well embedded privacy mindset is vital. Importantly, the notion of mindset and the treatment of privacy as an essential consideration – at all organisational levels, across all business functions, for all matters involving personal information and at all stages of the information lifecycle – is reflected in global best practice and legislative frameworks.

Privacy by Design (PbD) is a best practice approach that supports the building of privacy considerations into decision-making and project design elements for camera detected offences, such as those germane to the MPST program. The approach embeds good privacy practices into the end-to-end management of the program, not only to ensure compliance with privacy legislation, but also to meet community expectations regarding the handling of personal information.

PbD has seven foundational principles, set out below:

1. Proactive not reactive, preventative not remedial
2. Privacy as a default setting
3. Privacy embedded into design
4. Full functionality: positive-sum not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open, and
7. Respect for user privacy – keep it user centric.[13]

[13] For more on PbD, see the work of Dr Ann Cavoukian which now exists in some form or permutation in privacy laws and best practice guidance worldwide - https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

PbD reflects the position that privacy must be *designed in* to policies, procedures, processes, projects, products, services and technologies as opposed to being *bolted on* later, after a complaint has been made or a privacy breach event has occurred. In addition, privacy mindedness should be the default position of TMR when dealing with personal information.

Trust, or a lack thereof, is a key consideration for the community when engaging with government – even more so when the community may be negatively impacted by the decisions of government, such as in the case of law enforcement initiatives. PbD imperatives for the MPST program are relevant not only in terms of improving the compliance posture of the program (i.e., compliance with the IPPs and other aspect of the IP Act), but also in terms of building and maintaining community trust in the way TMR collects and handles personal information associated with enforcement of Queensland's road rules.

IIS notes that privacy has been 'designed' into the project from an early stage, and that TMR undertook a PIA and related information security assessments. However, it would have been preferable for IIS to complete this PIA at an earlier stage to allow for issues identified to be addressed before commencement of both the warning letter and enforcement stages of the program.

IIS found the MPST program team (and relevant stakeholder areas of TMR) to be receptive to our review process, and feedback during meetings was that our consultative approach to privacy risk identification and exploration of possible remediations was welcomed.

5.1.1 Governance - TMR

Good privacy management that promotes privacy compliance and best practice depends upon embedding privacy into an agency's practices, procedures and systems (i.e., its 'privacy program').

5.1.1.1 AI – ethics, use, accuracy, decisions made on the basis of AI

Artificial Intelligence (AI) and machine learning are increasingly desirable features of routine data driven activities within government, whereby some or all of a decision-making process may be automated – thus promoting consistency of decisions and reduction of costs associated with human effort. However, a 2020 Australian Human Rights Commission report identifies significant areas of risk associated with AI; in particular, surveillance, facial recognition, potential for bias and discrimination, and impacts on those who are vulnerable in the community.

Through its design, which features an initial AI-informed 'sorting' of images depicting possible offences, followed by three tiers of human adjudication, the MPST program avoids many of the risks. However, IIS considers that the program design did not have the benefit of referencing broader guardrails or requirements of TMR in respect of AI, and that program decisions were supported largely by responsible design on the part of the chosen vendor. While TMR has explored the use of AI for camera detected offences in the context of the MPST program, it does not – from a governance perspective – have a formalised policy position on use of AI in decision-making.

The Australian government's voluntary AI Ethics Principles were designed to prompt governments and organisations to consider the impact of using AI enabled systems before adopting and deploying such technology. The eight principles, at a glance, are as follows:

1. **Human, societal and environmental wellbeing:** AI systems should benefit individuals, society and the environment
2. **Human-centred values:** AI systems should respect human rights, diversity, and the autonomy of individuals
3. **Fairness:** AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups
4. **Privacy protection and security:** AI systems should respect and uphold privacy rights and data protection, and ensure the security of data
5. **Reliability and safety:** AI systems should reliably operate in accordance with their intended purpose
6. **Transparency and explainability:** There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI, and can find out when an AI system is engaging with them
7. **Contestability:** When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system, and
8. **Accountability:** People responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.[14]

In addition to the above, the question of whether (or the extent to which) there is a 'human in the loop' in AI deployments, as well as the relevance of robust harms assessment, feature heavily in AI-related guidance globally.[15] 'Human in the loop' refers to the involvement of a person at key junctures in decision-making that could impact a person, whether positively or negatively. It is a highly relevant consideration where a person may be affected by a decision about their access to services or benefits, or about imposition of a fine or some other penalty.

In commenting on this topic, the OIC referred to the failed Commonwealth 'Robodebt' scheme, which provides valuable learnings about the perils of failing to legislate for robust human oversight of AI-enabled decisions affecting the rights and entitlements of citizens. The OIC affirmed the importance of 'human in the loop' decision-making and noted the legislated requirements for same in respect of the MPST program.

[14] https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles

[15] Singapore's Personal Data Protection Commission has produced extensive guidance on governance considerations associated with AI implementations, here: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

IIS considers that – for TMR's use of AI in the MPST and other programs to be trusted by the community – the privacy, human rights and broader ethical considerations associated with AI should be a matter of 'big picture' governance at TMR, rather than relying on good individual program specifications (which may not, for example, always include legislative controls such as those put in place for the MPST program). Taking a broader governance approach also has the effect of setting the tone for AI-supported decision-making at TMR and serves as a strong example for other government agencies considering same.[16]

Recommendation 1
In consultation with the Privacy Team, formalise TMR's policy position on use of AI in decision-making. Include in particular; 1) TMR's position on ensuring 'human in the loop' decision-making; and 2) associated requirements to consider the probability and severity of privacy (and other relevant) harms.

5.1.1.2 Limiting function creep

The widening of the original use of a technology or system that involves personal information, including the combining of a technology or system with another, has the potential to result in unintended privacy consequences. Likewise, the expanding of uses or disclosures of personal information beyond those the community reasonably expects can be to the detriment of privacy. This is known as 'function creep'.

Aligned with PbD considerations, IIS supports an approach for TMR operations that avoids function creep to the greatest extent possible. As such, where MPST cameras or aspects of the MPST program (or the personal information associated with it) are being explored in the context of expediency or value-add for other TMR objectives or programs, IIS urges caution.

With respect to camera technology, IIS notes the potential for technology ad-ons, including functionalities (such as facial recognition), that may be considered privacy invasive. The arguments for such ad-ons which might otherwise appear persuasive – such as those focused on improved data capture or increasing value for money in an agency's technology spend – may well require caution when privacy is considered.

In commenting on this topic, the OIC expressed a strong view that expanding offences to be detected using the MPST cameras should only occur by legislative amendment. TMR has confirmed that in addition to compliance with the IP Act, any expansion (i.e., inclusion of new) offences within the CDOP program must be listed within s353 of the *Transport Operations (Road Use Management – Road Rules) Regulation 2009*. Further, any subordinate legislation change must pass through standard parliamentary scrutiny processes, including regulatory impact processes.

While cognisant of TMR's advice, IIS considers that the notion of regulatory creep remains relevant, which – as noted in our summary of OIC commentary at 3.7.2 (which is relevant here and later at Recommendation 21) – may enable use or expansion of technologies, or the uses and disclosures of personal information, without the benefit of meaningful privacy debate.

[16] To illustrate, see the Digital NSW policy approach and links to overarching strategy and other considerations, here: https://www.digital.nsw.gov.au/policy/artificial-intelligence-ai/ai-ethics-policy

IIS considers that lack of specificity in the Regulations as regards permitted (and, likewise, not permitted) uses and disclosures of personal information collected via the MPST program may be a harbinger for this form of function creep. The OIC, too, noted that the Regulations do not appear to specifically limit the offenses to be detected via the MPST program. This can be mitigated to some extent through careful application of the IPPs and a privacy-conscious governance environment for the MPST program.

Consultations revealed that TMR has several policies and mechanisms in place that can address function creep. These are well known to TMR's privacy team, however these are not immediately obvious or accessible to the MPST program team. For example, there are specific processes in place that govern lawful access to MPST data by outside persons or agencies, such as the Queensland Police Service. There is likewise a TMR-wide requirement to conduct PIAs for new – or substantially changed – projects that involve personal information, which would include, for example, the expansion of the use of MPST cameras for purposes additional to those currently prescribed for the MPST program.

Consultations confirmed the desirability of having MPST-specific governance, inclusive of policies, procedures, accountabilities and operational guidance, that can be referenced by the MPST program team and across TMR generally to inform decision-making and limit function creep.

Recommendation 2
In consultation with the Privacy Team, formalise MPST-specific governance. Include specific policies, procedures and accountabilities for: 1) expanding offences to be detected using the MPST cameras; 2) combining the camera technology with other technology (e.g., speed detection, facial recognition); and 3) details of the existing TMR processes for managing requests from law enforcement bodies and others to access, use or disclose images for non-MPST purposes.

5.1.1.3 Perception of bias and discrimination in TMR projects

For any initiatives of TMR, managing perceptions of the community relating to unfair or disproportionate targeting is a key consideration.

IIS is satisfied that the AI component of the MPST cameras is limited to identification and 'sorting' of images that contain key attributes – e.g., a mobile phone is detected, a seatbelt is detected – and that assessment of extraneous factors or attributes presenting potential bias, such as race, skin colour, gender, body weight, type of vehicle and GPS coordinates, are not relevant to the AI.

However, IIS considers that MPST program decisions (which are made by humans) about where to place MPST cameras may trigger community concerns about bias (i.e., unfair targeting) – this also speaks to a broader privacy issue of fair collection of personal information.[17] Queensland OIC guidance in relation to the fair collection of personal information states that *'[c]collection of personal information will be fair if the agency **is open and not misleading**, and if the individual is not coerced or intimidated into providing information against their will'* [emphasis added].[18]

[17] IPP 1(2) – An agency must not collect personal information **in a way that is unfair** or unlawful.

[18] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/collection/all-agencies-obligations-when-collecting-personal-information

Decisions about camera placement are made based on relevant TMR data sets – for example, crash statistics. Fixed cameras have been in place throughout the trial period, however consultations confirmed that mobile camera units are re-positioned regularly based on factors such as frequency of crashes at the location and serious injury and fatality rates associated with the location.

There is potential for the question of unfair targeting to be raised where the MPST program consistently places cameras in areas experiencing high crime rates, low employment rates, proportionally high representation of one or more ethnic groups or other community characteristics where the area or the people within it are perceived as 'targeted' by law enforcement.

IIS considers that community perceptions of program bias may be mitigated through open, consistent and targeted communications about the MPST program and, importantly, its outcomes over time – for example, publication of statistics that show a clear correlation between a regularly chosen MPST camera site and reduction of distracted driver crashes over time. This is discussed further in the context of social license, below.

IIS also notes the potential value – for TMR, the community and academic discourse in respect of deployments of this type – of exploring whether, through its monitoring activities, the MPST program could reliably test for types or levels of inadvertent bias in camera placement decisions.

Recommendation 3
Monitor decisions about MPST camera placements for patterns that could be construed as responsive to community characteristics (e.g., demographics, socio-economic). Take proactive steps to address related perceptions of program bias, such as through community outreach and other communications initiatives.

5.1.1.4 Social licence – proportionality and benefit to the community

Social license is about the trust the community gives the government to make laws, conduct programs, provide services and make decisions on its behalf and in its interest. The obligation rests with government to ensure this license is not abused.

The decision-making principles of necessity and proportionality are important considerations in any project – but particularly those involving technologies or techniques that are likely to arouse concerns in the community about government surveillance or other impingements on privacy rights. **Necessity** requires agencies to ask, *'Is the limiting of a person's right to privacy necessary to achieve our purpose?'* **Proportionality** requires agencies to ask, *'Are the anticipated benefits of project outweighed by the detriment to privacy?'*

The question of necessity is properly answered through objective evidence or findings. In the case of the MPST program, TMR has relied on extensive research in relation to distracted driving and failure to wear seatbelts, and the corollary impacts of serious injury and death. Deterring and issuing infringements for non-compliant driver behaviour on Queensland roads through the MPST program, including its camera surveillance component, was considered by TMR (and, ultimately, Parliament) to meet the necessity test.

Proportionality restricts the exercise of government power (to limit the necessary curtailing of privacy rights of the community) through balance – whereby the limiting of privacy to achieve the purpose (on one hand) is balanced by steps to ensure that privacy rights continue to prevail to the greatest extent possible. These steps include ensuring only the minimum personal information required to achieve the purpose is collected and handled, implementing legislative limitations and safeguards for personal information in the context, applying adequate information security controls.

In its proposed changes to the TORUM Act and Regulations to authorise the MPST program, TMR considered Section 25 of the HRA, which relates to protection of an individual's right to privacy and reputation. The Parliamentary process included consideration of a Statement of Compatibility, which involves assessment of necessity and proportionality in the context of human rights of Queenslanders. Statement concluded that an impact on individual privacy or reputation associated with the MPST program is minor and justifiable when balanced against the road safety benefits (the right to life) and protections available to the individual and the community.[19]

TMR also conducted an internal PIA of the MPST program which was responsive to the questions of necessity and proportionality. Following a review of the PIA by the OIC, sought an independent PIA to ensure privacy risks of the program were fully accounted for.

IIS considers that transparency is another important consideration of social license. Transparency in this case is about ensuring the community has access to relevant, complete and accurate information about the MPST program, and that there is awareness generally about the privacy safeguards in place for the program.

IIS commends the steps taken by TMR to inform the community about the MPST program and its purposes and considers that these could be bolstered by additional transparency measures discussed in section 5.2.1 of this report. IIS acknowledges that the MPST program is relatively young, however sees additional transparency benefits (including those relating to reducing perceptions of program bias) in communicating program outcomes to the community on a regular basis – for example, the extent to which the MPST program has achieved its purpose of reducing distracted driver crashes, including those resulting in serious injury and death from improper wearing of seatbelts.

Recommendation 4
Report MPST outcomes to the community at regular intervals. In addition, publish findings of any program evaluations undertaken.

[19] The Statement is available at https://www.legislation.qld.gov.au/view/pdf/bill.first.hrc/bill-2018-106. Pages 8 and 9 deal with privacy issues.

5.1.2 Governance – MPST program

IIS notes that – although supported by the Privacy Team – the TMR privacy program devolves responsibility for privacy management in projects to the relevant business areas. As such, strong privacy governance will be integral to commissioning, operating and monitoring the MPST program in a manner that provides high levels of privacy assurance to both TMR and the community.

5.1.2.1 Conduct further PIAs

A PIA is formal due diligence exercise that examines privacy risk in the context of programs, processes, technologies and other initiatives involving personal information. PIAs are regarded as best practice globally and assist in managing both statutory obligations and community expectations.

Community awareness of and engagement with MPST program objectives is a key part of organisational accountability. One way of promoting this engagement – and to alleviate any community fear or conjecture in relation to privacy – is to publish PIA reports (or summaries of the reports) that have been completed by TMR in relation to the MPST program. Publication of PIA reports is consistent with Queensland OIC best practice advice.[20] IIS notes, and commends, TMR's intention to publish an MPST PIA report.

PIAs are not, however, a 'set and forget' exercise. This is particularly the case for new or pilot programs, where privacy risks associated with community concerns or perceptions, a technology, a vendor, new or changed personal information flows or internal processes may be revealed during initial stages of the program.

IIS expects that further privacy considerations may arise during the months immediately following commencement of the enforcement phase, including those relating to accuracy of infringement decisions (which may be revealed following a sufficient period of review).[21] Likewise, the extent to which the recommendations in this PIA report have been implemented will be important to review.

Completion of an additional PIA within a year of commencing the enforcement phase would demonstrate ongoing privacy best practice.

Recommendation 5
Conduct a further PIA on MPST within one year of commencing the enforcement phase.

Further to the broader recommendation around MPST program governance, and the relevance of this for limiting function creep, the requirement to conduct a new PIA where TMR proposes to expand the use or functionality of MPST cameras, and/ or where there is a significant departure from the present MPST program specifications, should be beyond doubt.

[20] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment

[21] Refer also, Recommendation 19 at 5.2.4

TMR uses the MPST program (and the personal information derived therefrom) for the enforcement of road rules pertaining to mobile phone use while driving and proper wearing of seatbelts. It would be an expansion of use to apply the MPST program to a new purpose (for example, another aspect of enforcement or to analyse road behaviour). Functionality differs from use, and refers to the operations run by the MPST program. Expanding the functionality of the MPST program may include, for example, adding a facial recognition technology functionality.

IIS suggests building the requirement to conduct a PIA where TMR proposes to expand the use of function of the MPST program, into MPST governance proposed at Recommendation 2.

Recommendation 6
Conduct a PIA where it is proposed to expand the use or functionality of MPST cameras, and/ or where there is a significant departure from the present MPST program specifications.

5.1.2.2 Policy for MPST camera placement

While publication of camera sites – through an interactive map or some other tool – may serve to meet a transparency objective, the MPST program has taken a decision not to publish a map of its camera sites. This is largely because of the variable locations of mobile camera sites and resulting administrative burden to ensure mapping is accurate. There are also program concerns that awareness of camera locations may cause drivers to change their routes and behaviours while in the vicinity to avoid detection.

As discussed in section 5.1.1.3, there is potential for the question of unfair targeting to be raised where the MPST program consistently places cameras in locations where the area (e.g., community, suburb) or the people within it are perceived as 'targeted' by law enforcement. A lack of knowledge in the community about a) where cameras are located, b) how often mobile cameras are moved and to where and c) the extent to continuous surveillance is helping achieve benefits for the community can all compound perceptions of bias.

IIS considers that a strong policy position on camera placement – inclusive of the actual factors that inform camera placement decisions, how camera placement decisions are to be monitored, and reporting of MPST program outcomes to the community via various channels – would serve to mitigate community perceptions of bias.

Recommendation 7
Review TMR's policy position in the context of Recommendations 3 and 4 on: 1) deciding MPST camera locations and 2) monitoring decisions for perceived bias.

5.1.2.3 Community outreach

Community outreach offers agencies a meaningful opportunity to raise community awareness – and receive feedback, whether through formal consultations, comments or complaints – about key issues and agency plans to address those issues.

IIS has observed the various communication campaigns of the MPST program in respect of raising community awareness about the purposes of the program and the imminent roll-out of the enforcement phase.

Comment 1
The MPST program has been active in its outreach to the community, including through its use of signage, commercials, social media and 'warning letters' sent as an educative tool prior to the enforcement phase of the program. IIS commends this.

5.1.2.4 Tailored privacy training for MPST program

The Crime and Corruption Commission's Operation Impala report on misuse of confidential information in the public sector (report) highlighted risks associated with authorised staff engaging in unauthorised access to agency systems and information. The report made specific recommendations to Queensland agencies in relation to security controls, privacy culture and training. IIS considers that the MPST program, and in particular the adjudication team, should have heightened awareness of Impala report objectives when conducting their work.

To this end, TMR requires new and existing employees to attend privacy training pertaining to their responsibilities under the IP Act. Employees also receive misconduct training, which addresses the considerations of the Impala report.

Based on specific IPP 4 (information security) considerations raised by IIS in section 5.2.2.1, as well as consultations with the adjudication team, IIS considers that the adjudication team would benefit from additional training about privacy considerations specific to their role – including operational challenges that present privacy risk and strategies to address such risk.

Recommendation 8
Explore with the Privacy Team opportunities for the MPST adjudication team to receive tailored training about privacy considerations specific to their role.

5.2 Application of the IPPs

IIS has reviewed the internal TMR PIA for the MPST program and notes relevant IPP assessment and risk mitigations therein. In this section, IIS does not re-state the internal TMR PIA; rather, we provide additional commentary about application of the IPPs and findings and risk treatments where relevant.

5.2.1 Transparency and Collection

5.2.1.1 IPP 1

Through the MPST program, TMR collects personal information to fulfil its law enforcement functions; in particular, enforcement of road rules pertaining to mobile phone use while driving and the proper wearing of seatbelts. IIS considers that present and projected levels of community outreach offer consistent and transparent communications in relation to the MPST program.

Recommendation 9
Continue to promote the MPST program through various communication channels to ensure community awareness that their personal information may be collected remains high.

5.2.1.2 IPP 2 & IPP 5

IPP 2 relates to the providing of notice prior to collecting personal information from individuals directly. As a 'law enforcement agency', TMR is not required to observe IPP 2 in respect of the MPST program, however IIS notes that being exempt from the notification requirement in this case does not prevent TMR from taking proactive steps to ensure community awareness broadly.[22]

When seeking information about agency programs and personal information handling generally, the community will often consult the agency's privacy policy. A well-crafted policy can give the community information of sufficient detail to allow them to understand the agency's information practices and seek further clarification from the agency's privacy officer if needed.

IIS considers that TMR's privacy policy could be updated to provide greater granularity about TMR programs that involve the collection and management of personal information; in particular, those of interest to the community due to the surveillance component.

Recommendation 10
Update TMR Privacy Policy to include reference to camera-enabled offence detection and the collection of relevant images. Consider direct reference to the MPST program or providing a link to surveillance-related resources.

IPP 5 requires TMR to take all reasonable steps to ensure a person can find out what personal information the agency holds about them and how they can seek access to that information. IIS considers that this presents a broader proactive disclosure opportunity for TMR.

[22] The OIC provides guidance on the operation of section 29 of the IP Act here: https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-law-enforcement-agencies, with reference also to Schedule 5 of the IP Act, which defines 'law enforcement agency' at ***law enforcement agency*** (b)(iv)(A)

Where there is a lack of information in the public domain about a program or initiative, privacy-related concerns of the community may prompt applications for access to information – whether under IPP 6 (e.g., show me the personal information you have about me) or under the state's Right to Information (RTI) regime (e.g., show me what the program is doing/ will do with personal information).

TMR has a statutory obligation to provide access to agency information, including details of the MPST program, unless on balance it is contrary to the public interest to do so. The public interest reflects the value for the community in ensuring the effective, efficient, fair, accountable and transparent operation of government. When considering whether providing access to information is "in the public interest", it is relevant to assess whether disclosure of the information could reasonably be expected to:

- Promote open discussion of public affairs and enhance TMR's accountability
- Contribute to positive and informed debate on important issues or matters of serious interest
- Inform the community of TMR's operations
- Ensure effective oversight of expenditure of public funds, and
- Reveal the reason for a decision made by TMR and any background or contextual information that informed the decision.

Importantly, and in the context of this PIA, it is also relevant to consider whether the disclosure of the information could reasonably be expected to prejudice the protection of a person's privacy (which is generally considered to be a factor **not in favour** of the public interest).

While TMR's manner of responding to access requests is not within scope of this PIA, it is noted that there is potential for TMR to receive an influx of access requests relating to the MPST program. TMR may, for example, receive both informal and formal access requests for:

- General information about the program
- Details of decisions relating to camera placements
- A map of camera sites
- Information about the vendor working with TMR on the program
- General data (e.g., statistics, outcomes) associated with the program,[23] and
- Adjudicated images held by TMR in relation to infringement decisions.

[23] To this end, TMR advised IIS that evaluation of the MPST program will be incorporated into future evaluations of the whole CDOP, which are undertaken annually. CDOP evaluation reports are published.

IIS notes that asking the community (which includes individuals captured in MPST camera footage, other people interested in the program, media organisations, lawyers, insurers and others) to make formal applications for access to information held by TMR should – in accordance with regulatory guidance in Queensland – be treated a 'last resort'.[24] Rather, an attitude of openness and transparency (balanced with privacy considerations for people whose personal information may be captured in camera footage) should be the default position.

IIS encourages ongoing proactive disclosure of information about the MPST program where it is likely to be 'of interest' to the community or a person, and where privacy considerations pertaining to individuals can be appropriately managed. Consideration should be given to using informal means of disclosure – such as a dedicated page on the TMR website, adding to TMR's existing publicly available surveillance-related resources, interactive mapping, public-access digital dashboards, other publications or through some form of administrative release – to allow release of information by TMR without requiring a person to make a formal IPP 6 or RTI application.

In the context of proactive disclosure, defining and consistently using key terminology will be important. To illustrate: in its existing MPST resources, TMR asserts that it 'do[es] not capture or analyse biometric data'.[25] Biometric information is a type of personal information that is derived using different techniques or technologies that identify a person based on their unique characteristics, such as facial image. IIS notes that biometric information can be derived using facial recognition technology (where, put simply, a facial recognition algorithm creates a unique template of a person's face); however, the collection of a person's image does not mean that TMR has deployed facial recognition software for the MPST program or is using biometrics.

An ordinary person in the community may not have a full understanding of what biometric information includes, or indeed how such information can be derived from images and used. As such, TMR should ensure it defines this term and uses it consistently in published MPST information resources available to the community.

Recommendation 11
Continue proactive disclosure of information about TMR operations through publication of MPST-specific information on the TMR website, either on a dedicated webpage or within existing surveillance-related resources. Additionally, ensure the material published about the MPST program is up to date, specific about the personal information collected and handled for MPST purposes and that key terminology is defined to avoid confusion in the community.

5.2.1.3 IPP 3

IPP 3 requires agencies to only collect relevant, complete and up to date personal information and to not intrude unreasonably on an individual's personal affairs.

[24] https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/proactive-disclosure/proactive-disclosure-and-publication-schemes

[25] https://www.qld.gov.au/transport/safety/fines/cameras/About-mobile-phone-and-seatbelt-cameras

As with IPP 2, TMR's designation as a 'law enforcement agency' exempts it from IPP 3 requirements in respect of the MPST program. Nevertheless, IIS considers that (to meet the broader test of proportionality discussed at section 5.1.1.4, TMR should actively avoid collecting personal information that is not relevant for MPST program purposes. Discarding irrelevant images captured by MPST cameras (i.e., those where no offence is detected) prior to the three-part adjudication process involving the camera and AI provider and TMR is one such opportunity.

Recommendation 12
Continue training the AI in the MPST cameras to correctly detect mobile phone use and seat belt offences, whereby irrelevant images (those indicating no offence) are not retained for the adjudication process.

5.2.2 Storage and Security

On security of personal information, IPP 4 requires TMR to take all reasonable steps – including in its relationships with service providers – to ensure the personal information it holds is protected through its lifecycle from unauthorised access, use, modification, disclosure, loss or any other misuse.

Active measures that can be taken by TMR include a blend of **administrative** (i.e., policy, procedure, contract), **technical** (i.e., access controls) and **physical** (i.e., locked assets) **safeguards**. The measures that are appropriate in the circumstance will depend on factors such as the nature, sensitivity and amount of personal information, the location of the information and whether a contracted service provider is involved. IIS notes that Queensland's Information Security Policy (IS18:2018) provides valuable security signposts, including the application of ISO27001 controls, which were referenced in three internal TMR Information Security Risk Assessments for the MPST program conducted by the information security team.[26]

The camera and AI provider for the MPST program is a contracted service provider within the meaning of the IP Act and has been contractually bound to comply with the IPPs. IIS notes the collaborative and positive working relationship between the camera and AI provider and the MPST program team.

Based on IIS's experience with projects of this type and the extensive information provided by TMR in support of this PIA, IIS has made recommendations for strengthening the security posture of the MPST program.

5.2.2.1 IPP 4

Three internal TMR Information Security Risk Assessments for the MPST program have been conducted by the information security team, with each providing recommendations pertaining to the relevant phase of the program. IIS has not interrogated the extent to which TMR has chosen to accept or treat the risks raised, however notes that electing not to take a reasonable step to secure personal information could raise questions of IPP 4 compliance.

[26] ISO/ IEC 27001: Information Security Management - https://www.iso.org/isoiec-27001-information-security.html

Recommendation 13
Continue to implement recommendations arising from the TMR Information Security Risk Assessments of the MPST program.

The scope of this PIA does not include a detailed information security review of the camera and AI provider. IIS does, however, take a 'trust but verify' approach in respect of privacy reviews and both consulted with the vendor and reviewed information supplied by them that was responsive to questions about information security. IIS is satisfied that the security measures employed by the vendor in respect of IPP 4 are adequate and, indeed, highly cognisant of the privacy rigour expected for initiatives of this kind. IIS is also satisfied that related security considerations in respect of section 33 of the IP Act (regarding transfers of personal information) have been addressed.

Moving forward, it will be important for TMR to regularly confirm that the camera and AI provider is acting in accordance with contract terms. Verification activities need not be onerous, but they should be formalised and relevant documentation kept with the body of information associated with the program. Routinising these activities can provide vital reassurance to TMR as regards risk of (and opportunities to remediate) a privacy breach.

One type of verification that is particularly useful is review of audit logs. Audit logs capture a set of information to reveal detail about when systems and information are accessed, by whom, for how long, for what purpose and whether there was deviation from any business rules. Consultations confirmed that the camera and AI provider keeps detailed audit logs of the pre-adjudication process, which is the first 'human in the loop' interaction with MPST data, and that this information is made available to TMR on request. Consultations also confirmed that TMR has requested to see pre-adjudication audit logs during the warning letter phase of the program, but not with regularity.

IIS considers that ongoing and regular visibility of pre-adjudication audit logs is reasonable in this case.

Recommendation 14
Routinise the receipt of vendor audit logs associated with the pre-adjudication process.

Often, the way program objectives are met by people (that is, how the work is actually done) can highlight areas for improvement. An aspect of the MPST program of particular interest to IIS was how the adjudication process at TMR – adjudication and the quality assurance (QA) of the adjudicator's decision (points two and three of the 'human in the loop' aspect of MPST decision-making) – works on the ground.

IIS requested a 'ride along' to see first-hand the physical space used by MPST adjudicators, the physical and technical security controls in place regarding access to the MPST decision-making premises and portal, how the relevant images are viewed, how adjudication and QA activities occur in practice and the ways privacy rules are applied in practice (whether as deliberate steps or as culturally embedded).

IIS attended TMR's primary corporate location to conduct the 'ride along' and met with both the MPST program team and the adjudication team at this time. IIS quickly formed a view that MPST adjudicators are deeply aware of the sensitivity of their work and the relevance of privacy and information security requirements. The adjudication team was receptive to receiving privacy support in addition to the mandatory TMR training, such as through tailored privacy training specific to the operational realities of their role. This is consistent with the recommendation for same at section 5.1.2.4 of this report.

A considerable portion of the 'ride along' was spent reviewing the location of MPST adjudication operations – that is, the physical space occupied by the adjudication team. Consultations on the day revealed that accommodation of the team (that is, the space or facility allocated to them) was not within scope of the MPST program and, therefore, not a matter negotiated or decided by the MPST program team. Rather, accommodation of the adjudication team is decided by another business area within TMR and communicated to the MPST program team.

The adjudication team is presently located on two separate floors. This separate accommodation is a new circumstance for the adjudication team, with the bulk of the warning letter phase having been spent working together on the same floor. The team is split equally over both floors, with equal numbers of adjudicators and QA officers on each floor and a supporting Manager who moves between the floors to monitor and support decision-making activities.

IIS notes that the adjudication team performs its operations in entirely open-plan office environments, with the placement of the team in high traffic locations on both floors. The screens used to view images of possible offences are visible to passers-by and to other unrelated TMR staff who occupy desks in the same area. This is contrary to best security practice when viewing images of possible offences, which would ordinarily be expected to occur in a secure-access facility (akin to a 'control room'), or at the least, a separate and dedicated workspace designed to limit physical access of unrelated staff.

IIS considers there is a need to revisit the matter of MPST adjudication team accommodation urgently.

Recommendation 15
Urgently open discussions with the MPST program Board to 1) communicate a requirement for a secure-access facility accessible only to the MPST adjudication team and 2) seek resolution to accommodation issues prior to 30 November 2021.

An operational issue directly arising from the split accommodation of the adjudication team is the requirement for the Manager to float between floors to conduct supervision and support activities. It is impossible to be in two places at once, meaning that consistent oversight of adjudication team activities and availability to support them in their decision-making roles is limited.

Likewise, the adjudication team reported a degree of anxiety associated with potential 'over the shoulder' viewing of their workstations and the ability for unrelated TMR staff to hear their conversations.

Recommendation 16
Urgently address physical security considerations and operational challenges relating to accommodation by 1) relocating to the same floor within TMR until a secure-access facility is made available, 2) moving adjudicator desks out of high traffic/ thoroughfare areas, 3) positioning adjudicator desks so that monitors are not able to be viewed 'over the shoulder'.

As adjudicator-to-adjudicator, adjudicator-to-QA officer and whole-of-team conversations about images of possible offences are an important part of the learning and refining of decision-making associated with the MPST program, such conversations occur frequently. The adjudication team confirmed that this aspect of 'teaming' is vital to their operation, however teaming through conversation cannot be done with frequency and consistency across two floors.

During this review, IIS became aware that an operational work-around for the teaming aspect of adjudication. As opposed to being able to view an image together in real time, as they could within a shared workspace, the relevant images were instead shared virtually so that other members of the team could review it and provide support. This had the effects – from a security perspective – of a) moving MPST images outside of the secure portal environment and into a new vendor environment that is not associated with the MPST program and b) potentially creating records of MPST decisions (inclusive of images, adjudication team commentary and offence decisions) within another vendor environment.

IIS considers that this practice – which ceased during the PIA review period immediately upon TMR being apprised of the privacy risk – had the effect of undermining the various and extensive security measures taken by the MPST program. IIS also considers that this practice would not have been in place if the adjudication team was given appropriate accommodation.

Recommendation 17
Seek urgent advice of the Privacy and Records Management teams as regards secure destruction of (or management as 'records' of TMR, if required) any MPST images and associated commentary shared amongst adjudicators within an environment outside of the secure portal.

5.2.3 Access and Correction

IPPs 6 and 7 require TMR to allow individuals to seek access to and correction of their own personal information.

The MPST program includes the ability for a person to access images of camera detected offences through secure login to their 'My TMR Account'. IIS understands that this functionality will be 'live' from the commencement of the enforcement phase. This complements the established Right to Information processes at TMR.

IIS notes the particular obligation under IPP 7 that TMR must ensure the **quality of information it controls**. This includes taking all reasonable steps to ensure that personal information is accurate, directly related to fulfilling the purpose for which it was collected, relevant, complete, up to date and not misleading. This obligation relates directly to a further obligation under IPP 8 for TMR to ensure quality of the personal information it intends to use *before* actually using it. This becomes relevant in respect of the potential for an image to be applied to a person in error, such as where a vehicle is stolen and the image supplied on the infringement notice is of the thief. Consultations confirmed that the statutory declaration process, which can be used to report errors of this type before enforcement of an infringement notice (thus, correcting the personal information TMR holds about the person), addresses this issue.

Comment 2
There is ongoing importance of making information about access and amendment of personal information associated with the MPST program easy for the community to find, easy to understand and use, and accurate in terms of the TMR processes a person will be required to engage with – particularly where there is a need to 'set the record straight'.

5.2.4 Accuracy

IPP 8 requires TMR to ensure quality of the personal information it intends to use *before* actually using it.

Consultations revealed that accuracy of decisions is considered by stakeholders to be an important measure of the MPST program's effectiveness over time, however this has not been a primary focus of the program to date.

Statistics for the NSW program of a similar nature show that the enforcement phase initially had a 4% error reporting rate (such as through the statutory declaration process, or where an 'offender' successfully challenged an offence), which has dropped to less than 1% (with errors converted to learnings and, ultimately, improved decisions). The MPST program team indicated during consultations that similar visibility in relation to accuracy of decisions is desirable for the program going forward.

IIS considers that the accuracy of decision-making – in particular, at the QA stage of adjudication – will be important for reassuring the community that the MPST program's benefits in improving road safety outweigh the surveillance risk (and any potential inconvenience associated with 'correcting the record' as discussed in respect of IPP 7.[27] To this end, analysis of error reporting over time and incorporation of any learnings into MPST adjudication processes are desirable. Additionally, the community should be made aware of the findings through publication of the relevant statistics.

[27] IIS notes that adjudication team members undertaking QA functions undergo rigorous 1:1 training on identifying offences in accordance with business rules. Consultations revealed that adjudication team members are also audited on their accuracy and comprehension of the business rules.

Recommendation 18
Conduct longitudinal analysis of accuracy of QA adjudicator decisions (with learnings to be incorporated into MPST adjudication processes) and report on findings.

5.2.5 Use

IPPs 9 and 10 require that only the personal information required for a particular purpose should be used, and TMR should only use personal information for the purpose for which it was collected, unless certain circumstances apply. IIS explored the topic of 'use' from both operational and broader PbD perspectives.

The OIC guidance says that '*[i]f information is not about an identifiable individual it is not personal information, which means it presents no privacy concerns. De-identifying an individual's information enables it to be shared or made publicly available while still complying with the privacy principles, protecting the privacy of the individual, and ensuring the information remains appropriate for its intended use.*'[28]

From an operational perspective, the images considered throughout the adjudication process and, ultimately, contained in the infringement notice, depict both driver and front-seat passenger. The question of whether the image of the passenger is necessary to be further used where no passenger seatbelt offence was detected by the MPST camera (and was, therefore, not subject to pre-adjudication processes) was raised by both the OIC and IIS during this review.

During adjudication, where no passenger offence is being considered as part of the decision, the existence of the passenger image becomes surplus to use requirements. Consultations revealed that the passenger image, in such a circumstance, is not considered by the adjudication team.

IIS understands that, together with the camera and AI provider, TMR could create a staging process to effectively remove or obfuscate personal information where there is doubt as to its utility in fulfilling the purpose – that being, completing the adjudication of an image (in order to issue an infringement notice based on a detected offence).

Recommendation 19
Where a passenger seatbelt offence **is not** detected by an MPST camera, take steps to limit visibility of (or entirely obscure) passenger images through the further adjudication processes relating to the driver and any subsequent issue of infringement notice.

[28] https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/proactive-disclosure/proactive-disclosure-and-publication-schemes

During consultations, the rationale for including the passenger image (whereby the inclusion of all or part of the passenger's face renders them identifiable) on the infringement notice was discussed in the context of potentially revealing excessive personal information (about the passenger) to the registered owner of the vehicle who – upon receiving the infringement notice – may not have been the driver and may not have had previous visibility of the passenger. Indeed, and as also noted by the OIC, the very fact of a passenger's existence in a vehicle – including aspects of their physicality, approximate age, gender, manner of dress, tattoos and other markings – triggers privacy considerations.

IIS considers that – leveraging Recommendation 19, above – there is additional opportunity to refine the extent to which passenger images are contained in infringement notices when passenger seatbelt offences **are** detected – to the extent that this does not raise matters regarding evidence of an offence.

TMR has expressed that, while likely possible from a technical perspective, there may be strong rationale for including an identifiable image of the passenger on the infringement notice (rather than just an image of the passenger's offence, with their face blurred or otherwise obscured) – for example, consistency with the contents of other types of camera detected infringement notices, and registered vehicle owners and/ or drivers being able to identify a passenger for the purpose of determining their eligibility for a seatbelt exemption.

Nonetheless, IIS considers there is value in investigating this opportunity further; not least for the purpose of clearly articulating the reasons for including an identifying image of a passenger on infringement notices where a privacy enhancing alternative (such as the blurring of a passenger's face) exists.

Recommendation 20
Where a passenger seatbelt offence **is** detected, investigate whether passenger face (where visible in whole or in part) can be obscured when generating the infringement notice.

The IP Act is subject to other laws, which means the other laws are applied first and the IPPs apply to the extent of any inconsistency – they effectively 'pick up the slack'.

IIS considers that the TORUM Act and associated Regulations could potentially allow for broad additional uses of personal information collected for the purposes of the MPST program, and notes OIC concerns in relation to same. TMR would minimise this risk by making clear its policy position on permitted and anticipated secondary uses.

Comment 3
It is vital for the MPST program to reflect on the Privacy by Design considerations raised by Recommendation 2 in respect of avoiding function creep – not just within the MPST program, but where other areas of TMR may wish to leverage the MPST camera technology or use stored images for other purposes.

Recommendation 21
Where the Regulations do not specify additional permitted **uses** of MPST images and other personal information, follow the overarching privacy governance requirements for MPST. Refer also: Recommendation 2.

5.2.6 Disclosure

IPP 11 place limits on disclosure of personal information to third parties and includes 'exceptions' to the rule where the personal information is necessary to facilitate important processes of government. One such exception is where a disclosure is authorised or required by law, for example the TORUM Act and Regulations.

As with the potential for widening the uses of MPST images and other personal information to the detriment of privacy, IIS notes the same potential in relation to disclosure. Here again, IIS draws attention to OIC concerns in relation to a form of function creep through regulation; that is, the widening of the Regulations (or the interpretation of them) to permit disclosures not currently contemplated for the MPST program.

With respect to the management of third-party requests to disclose personal information, consultations revealed that TMR has formalised procedures in place that would apply to the MPST program – for example, for disclosures to law enforcement agencies and to researchers – however, the MPST program team do not have full visibility of these procedures and did not express confidence in their ability to know which procedures apply in each circumstance.

Recommendation 22
Where the Regulations do not specify additional permitted **disclosures** of MPST images and other personal information, follow the overarching privacy governance requirements for MPST. Refer also: Recommendation 2.

6. Conclusion

In this PIA report, IIS has identified areas where it considers TMR should take additional steps to ensure compliance, or to promote better privacy practice. Our recommendations focus on matters of privacy governance – both broadly at TMR and uniquely for the MPST program – and alignment of personal information handling practices with the IPPs. IIS considers that, subject to implementation of the recommendations, the MPST program can operate in compliance with the IP Act.

7. Appendix A – Information Flow Diagrams

7.1.1 Camera and AI provider information flows

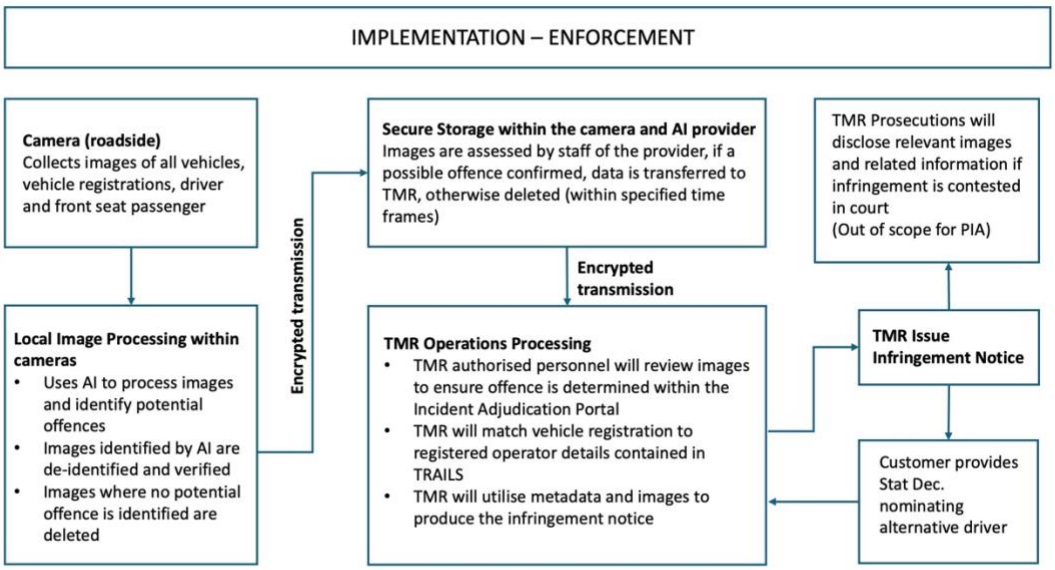
1. The camera and AI provider places mobile or fixed cameras in metropolitan or regional QLD under direction from TMR. Locations are determined using a risk analysis of crash data with the highest risk locations visited more often.
2. Once operational, the camera and AI provider's cameras capture:
    a. Vehicle registration number (image)
    b. Face/lap of drivers and front seat passengers (image)
    c. Location, date and time of image as well as vehicle direction and speed (metadata), and
    d. Camera generated incident number (metadata).
3. The images are processed within the camera using AI:
    a. If no possible offence is detected, the AI system automatically excludes the images from any further analysis and the images are generally deleted within a short period of time.
    b. If a possible offence is detected, the image is cropped to remove any irrelevant material, a data block is prepared, which includes the incident number, the relevant images, and the associated metadata and this is transferred via encrypted channels to the camera and AI provider's database for pre-adjudication.
4. Crops are stored in a database, and downloaded by a camera and AI provider pre-adjudicator throughout their shift. Adjudicators view images for quality and to identify potential offences.
5. Verified images and data will be dispatched to TMR, via encrypted channels, for infringement processing.

7.1.2 TMR information flows

1. TMR stores the data (including images and related metadata) in the stand-alone Incident Adjudication Portal which links to a database.
2. TMR uses information from the image capture and from TRAILS to issue an infringement to the registered operator. Infringement letters will be issued to the TMR Mail House for printing and posting. Printed infringements will be securely stored as per current processes within the TMR Mail House.
3. TMR uses its standard process to maintain security when sending infringement notices to customers identified as protected or suppressed by TMR's Identity Management Unit.
4. The Infringement is recorded against the customer record in TRAILS.
5. TMR might receive communications from the registered operator; the registered operator has the option of nominating an alternative driver, via paper statutory declaration or online nomination of an alternate driver. The infringement might also be challenged for other reasons.

6. TMR Prosecutions will disclose as part of prosecution pack if contested in court and submitted as evidence.

The following diagram gives an overview of the MPST solution design, and the related information flows.



INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: contact@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN 107 611 898

IIS Partners
INFORMATION INTEGRITY SOLUTIONS