ACT Government

Mobile Device Detection Cameras

Privacy Impact Assessment (PIA) extract

Introduction

ACT Government takes the management of personal information provided to us seriously and is committed to ensuring adequate security and privacy safeguards are in place to protect customer information.

As recommended by best practice, an initial privacy impact assessment (PIA) was undertaken before the procurement for a suitable Mobile Device Detection Camera (MDDC) system was commenced. A summary of this PIA, and its recommendations are listed below.

Once a suitable MDDC system provider was awarded a contract, a further PIA was undertaken to ensure compliance with the recommendations arising from the initial PIA and to identify further privacy safeguards. A summary of this PIA and its recommendations, and actions taken with regard to the recommendations are also listed below.

2020 Privacy Impact Assessment Executive summary

Introduction

What is a Privacy Impact Assessment?

A privacy impact assessment (PIA) is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

PIAs are an important component in the protection of privacy and are used as part of the overall risk management and planning processes when Governments are considering a project that will involve the handling of personal information.

In developing a possible framework for the use of the mobile device detection cameras in the ACT, the Government will ensure there are appropriate privacy safeguards in place and that the implementation of the cameras does not create an unreasonable limitation on a person's right to privacy.

To achieve this, the Transport Canberra and City Services Directorate (TCCS) has drafted this PIA to ensure all privacy and human rights implications are fully considered and any impacts properly managed. The PIA will be used to guide appropriate amendments to the Territory's road transport laws and to demonstrate to stakeholders, including any organisation seeking to provide the cameras, that the legislative and operational framework will be designed with privacy in mind.

The recommendations in this PIA seek to achieve an appropriate balance between the interests of individuals affected by the project (including measures for minimising privacy intrusions and maximising privacy protection) and the project's road safety benefits for the community.

Privacy Impact Assessment Scope

The scope of this PIA is to analyse the possible privacy impacts on individuals whose personal information will be handled in the implementation of the mobile device detection cameras, by reference to:

1. the information flows described in this PIA; and
2. the *Information Privacy Act 2014* (the Act) including the Territory Privacy Principles (TPPs); and
3. section 12of the *Human Rights Act 2004*.

The Act provides that the TPPs apply to ACT public sector agencies and contracted service providers (including subcontractors) where they perform obligations under a government contract. Section 21 of the Act provides that a public sector agency must not enter into a government contract unless the contract contains appropriate contractual provisions requiring the contracted service provider to comply with both Territory and Commonwealth Privacy laws. Any service provider of the mobile device detection cameras would therefore be subject to the Privacy Act 1988 and the Australian Privacy Principles (APPs).

The TPPs are similar to the Commonwealth APPs, as set out in Schedule 1 of the Privacy Act 1988. There are some differences such as where the Commonwealth APPs are not relevant to the regulation of information privacy by ACT public sector agencies and have therefore not been included in the TPPs. The TPPs also contain minor text differences to the Commonwealth APPs but this does not change the intended meaning of the principles, and ultimately places the same obligations on a service provider.

Noting the similarities between the TPPs and APPs, this PIA focuses its consideration on the TPPs from which a privacy risk could arise from the use of mobile device detection cameras.

This PIA has been drafted prior to the ACT Government approaching suppliers in the market and is based on the assumed framework for the operation of the cameras. The PIA will be updated throughout the project.

Stakeholder Consultation

In drafting this PIA, TCCS has consulted with the following organisations:

- ACT Human Rights Commission;
- Office of the Australian Information Commissioner;
- ACT Policing;
- Office of the Chief Digital Officer;
- Justice and Community Services Directorate; and
- Chief Minister, Treasury and Economic Development Directorate - Access Canberra.

Recommendations

Recommendation 1

Access Canberra, JACS and ACT Policing's Privacy Policies to be reviewed and updated before mobile device detection cameras are implemented.

Recommendation 2

Mobile device detection camera technology operating in the ACT must have the technical capability to:

- ensure that all images captured by the cameras that do not contain evidence of an offence are rapidly and permanently deleted;
- automatically analyse images and identify those that are likely to show a driver using a mobile phone within a set timeframe;

- only retain the minimum amount of data required to detect and enforce offences;
- pixilate images of front seat passengers, and not record any image of a front seat passenger; and
- blur out parts of the vehicle or the image if required or requested.

The camera technology must not be able to view or record any image of the rest of the inside of the car.

Recommendation 3

Existing security and privacy safeguards for road safety cameras will be applied to the operation of mobile device detection cameras, where appropriate.

Recommendation 4

Amendments to the Territory's road transport legislation to be drafted in a way that:

- confirms that the *Information Privacy Act 2014 and Privacy Act 1988 (Cth)* applies to the handling of personal information, and is in accordance with the *Human Rights Act 2004*;
- identifies (as far as possible) the specific kinds of personal information that may be collected, used and disclosed;
- ensures that there is a clearly defined scope of the proposed permitted collections, uses and disclosures of personal information by the mobile device detection camera system operator, Access Canberra and anyone else authorised to access the information;
- clearly articulates the purpose(s) for which personal information may be collected, used and disclosed;
- clearly provides a legally binding obligation for the mobile device detection camera system operator to permanently delete images that do not contain evidence of an offence; and
- clearly provides a contractually binding obligation for the mobile device detection camera system operator to comply with the TPPs and the *Privacy Act 1988 (Cth)* as required.

Recommendation 5

Contractual arrangements should be implemented that:

- confirm that the *Information Privacy Act 2014, Human Rights Act 2004 and Privacy Act 1988 (Cth)* applies to the handling of personal information and what legislation applies in what circumstances;
- identifies (as far as possible) the specific kinds of personal information that may be collected, used and disclosed;
- ensures that the scope of the proposed permitted collections, uses and disclosures of personal information by the mobile device detection camera system operator, Access Canberra and anyone else authorised to access the information are in accordance with the *Information Privacy Act 2014, Human Rights Act 2004 and Privacy Act 1988 (Cth)*;
- clearly articulates the purpose(s) for which personal information may be collected, used and disclosed; and
- clearly provides a legally binding obligation for the MDDCS operator to permanently delete images that do not contain evidence of an offence.

Recommendation 6

Where a decision is made to include mobile device detection cameras in the ACT's Road Safety Camera Program, a public awareness campaign should be undertaken advising of the privacy and information security protections in place.

Recommendation 7

The decision-making process to determine whether there is evidence of a mobile phone offence or if an image should be deleted during the review process must be traceable and auditable through the mobile device detection camera system.

Recommendation 8

To protect the security of personal information, mobile phone detection camera technology operating in the ACT must ensure the system has the technical capability to ensure that:

- the person reviewing images not ruled out by the artificial intelligence is only provided with a view of the driver; and
- no information about the camera, location, vehicle or time of day are provided to a person reviewing the offence.

Recommendation 9

The contractual agreement between the Territory and the mobile device detection camera system operator should require that appropriate vetting and training of staff occurs, and that this is clearly documented.

Recommendation 10

Appropriate controls over physical access to the camera sites and the mobile device detection camera system should be established.

2023 Privacy Impact Assessment Executive summary

Introduction

Mobile device use while driving is a road safety concern due to the increased risk of accidents resulting from driver distraction. It is an offence under road transport legislation for a driver to use a mobile device while the vehicle is moving, or is stationary but not parked (subject to certain exceptions).

The ACT Government has introduced mobile device detection cameras (MDDCs) as part of the ACT Road Safety Camera Program. The aim is to reduce road safety risks associated with driver distraction by encouraging drivers not to use mobile devices while driving. MDDCs in the field have been in a test phase since February 2023. Issuing of infringement notices will not commence before 1 February 2024, with a minimum 3-month warning phase.

The Chief Minister, Treasury and Economic Development Directorate (CMTEDD), and in particular Access Canberra, is responsible for the proposed MDDC System and related information and communications technology (ICT) systems. The MDDC System itself is being provided by Acusensus Australia Pty Ltd (Acusensus), and will integrate with:

- Xilium (the Adjudication System) delivered by Sensys Gatso Australia Pty Ltd (Gatso);

- the Rego.ACT System; and
- the Access Canberra web portal.

The MDDC solution is the same technology currently being used in Queensland, New South Wales (NSW) and Western Australia (WA).

This privacy impact assessment (PIA) has been commissioned by Access Canberra within the CMTEDD to identify and assess privacy impacts and compliance risks relating to the implementation and use of MDDCs in the ACT, and ensure that such issues are appropriately managed.

Overall Finding

Overall, the project presents a medium level of privacy risk that can be mitigated by implementing the recommendations made in this PIA report.

Summary of Recommendations

Recommendations made in this PIA to eliminate, reduce or manage negative privacy impacts and compliance risks are summarised below.

These recommendations seek to:

1. achieve an appropriate balance between the interests of individuals whose privacy will be impacted by the project, and the project's objectives in relation to road safety for the benefit of the ACT community; and
2. where appropriate, maximise opportunities for privacy protection and incorporating a 'privacy by design' approach in relation to the project.

Recommendation 1

We recommend that the CMTEDD consult with the Office of the Australian Information Commissioner in relation to the implementation and use of the MDDC System in the ACT, and its proposed privacy management approach.

ACT Government response

Accepted.

Recommendation 2

We recommend the CMTEDD engage with other jurisdictions in which MDDC systems have been implemented, with a view to obtaining insights and 'lessons learned' that can inform the ACT approach to privacy management.

ACT Government response

Accepted.

Recommendation 3

If there are any material changes to the information flows identified in Schedule 1, including any proposed new use cases regarding the use of MDDC System data and images (such as the detection and enforcement of laws relating to offences other than driver mobile device use), we recommend the CMTEDD undertake:

- a privacy threshold assessment; and
- if required, further assessment of privacy impacts and compliance risks (which could be in the form of a supplementary PIA).

ACT Government response

Accepted.

Recommendation 4

We recommend the CMTEDD undertake regular reviews its use of the MDDC System to ensure:

- the functionality is operating as intended;
- any known, new or unanticipated privacy issues are appropriately managed; and
- ongoing compliance with the Territory Privacy Principles (TPPs), including to identify opportunities to refine data handling practices and maximise privacy protection.

Such reviews should be:

- undertaken at regular intervals during the first 12 months, and periodically thereafter as appropriate; and
- informed by public feedback, and any privacy complaints and identified data quality issues, relating to the MDDC System.

ACT Government response

Accepted.

Recommendation 5

We recommend that the CMTEDD engage in proactive contract management in relation to the delivery of services by contracted service providers (currently Acusensus and Gatso), including by:

- establishing processes and procedures for regular monitoring and review of compliance with contractual obligations, from contract commencement to completion/termination; and
- conducting regular audits of systems and processes to ensure the handling of personal information by contracted service providers (and any subcontractors) is, having regard to the volume, nature and sensitivity of the relevant information, sufficiently secure and satisfies all contractual obligations in relation to privacy and data security.

ACT Government response

Accepted.

Recommendation 6

We recommend the CMTEDD seek an appropriate variation to the Traffic Camera Office Adjudication System Agreement with Gatso, so as to clarify that the Contractor's obligations in relation to notification of

'security breaches' and 'other material incidents' in Item 4(2) of Schedule 2, are not limited to unauthorised disclosures of personal information, but can also include:

- loss, destruction or damage to any personal information; and
- access to and use of personal information other than in accordance with the Agreement.

ACT Government response

Accepted.

Recommendation 7

We recommend the CMTEDD review and update its Privacy Policy to:

- make clear that it applies to Access Canberra (as a business unit of the CMTEDD); and
- ensure it addresses the collection, use and disclosure of images and related metadata taken by cameras on ACT public roads (i.e. MDDCs and other cameras, such as speed cameras) for compliance and enforcement purposes in relation to ACT transport and road transport legislation.

ACT Government response

Accepted.

Recommendation 8

We recommend that in addition to redacting vehicle passengers from images, Access Canberra should redact other sensitive information (or information of a sensitive nature):

- to the extent that doing so would not unreasonably compromise the quality and integrity of the other parts of the image that are reasonably required for the purposes of enforcing road transport legislation (including the ability to identify and show the driver and offending behaviour, and as evidence in court proceedings)
- subject to the technology capability becoming available to allow it to make such redactions.

ACT Government response

Accepted.

Recommendation 9

We recommend the CMTEDD review and expand its MDDC public awareness campaign to make available information relating to the protection of privacy and data security.

ACT Government response

Accepted.

Recommendation 10

We recommend the CMTEDD develop privacy notices that meet the requirements of TPP 5:

for inclusion in warning letters and infringement notices; and

to be prominently displayed and accessible to individuals who login to the Access Canberra website to check traffic infringement images.

ACT Government response

Accepted.

Recommendation 11

We recommend the CMTEDD review and, as appropriate, update vehicle registration and vehicle registration renewal forms to ensure they each include privacy notices which make individuals aware of the use of their personal information for the purposes of road transport law enforcement.

ACT Government response

Accepted.

Recommendation 12

We recommend the CMTEDD ensure prompt and accurate written records are made of:

- any uses of personal information stored in the Rego.ACT System that are done pursuant to TPP 6.2(e) (law enforcement exception); and
- any disclosures of MDDC images, or other personal information collected and stored in the MDDC System:
    - to the Australian Federal Police or other enforcement bodies made pursuant to TPP 6.2(e); and
    - to other third parties (in accordance with the Information Privacy Act).

ACT Government response

Accepted.

Recommendation 13

To mitigate the risk of unauthorised third parties being able to potentially access personal information via the Access Canberra web portal and improperly deal with it, we recommend the CMTEDD:

- develop and implement a more secure method of enabling individuals to whom an infringement notice has been issued, to access and view MDDC images and related information via the Access Canberra web portal; and
- investigate the feasibility of, and if possible implement, an ICT solution to prevent or at least reduce the risk of images being downloaded, copied or printed from the Access Canberra web portal.

ACT Government response

Accepted.

Recommendation 14

We recommend the CMTEDD undertake, or commission from an external auditor, regular monitoring and review of the MDDC System in relation to data quality and integrity.

ACT Government response

Accepted.

Recommendation 15

We recommend the CMTEDD ensure there is a documented data quality management plan for the MDDC System in place that addresses processes and standards for identifying, assessing, escalating and resolving data quality issues.

ACT Government response

Accepted.

Recommendation 16

We recommend the CMTEDD implement a data retention and destruction plan for the MDDC System to ensure images and other data is only retained for such minimum periods as is:

- required by Access Canberra for the purposes of its road transport law enforcement functions and activities; or
- is otherwise required under the Territory Records Act in relation to the retention of territory records.

ACT Government response

Accepted.

Recommendation 17

We recommend that:

- as soon as possible and prior to the MDDC System becoming operational, the CMTEDD ensure that cyber security assessments (including penetration testing) are completed for all ICT components of the solution (including the MDDC System itself, as well as related integrated ICT systems), as assessed against applicable Australian Government and ACT Government cyber security standards; and
- regular cyber security audits and testing is undertaken thereafter.

ACT Government response

Accepted.

Recommendation 18

We recommend that the CMTEDD ensure it has data breach and cyber incident response plans in respect of, or at least covering, the MDDC System and related ICT systems.

ACT Government response

Accepted.

Conclusion

ACT Government has undertaken due diligence prior to undertaking the reform and implementation of the MDDC system to safeguard the security and privacy of customers.

The steps taken above outline the consideration given to the management of personal information and the actions taken to ensure adequate safeguards are in place to provide the community confidence.

A copy of both PIAs can be requested through [insert link to FOI request page] and will be provided in line with the terms of the *Freedom of Information Act 2016*.

The documents will only be redacted where the information pertains to legal advice received by ACT Government, and to protect Legal Professional Privilege.