Privacy impact assessment

Project, programme or system name

Advanced Mobile Location information for the Triple Zero Emergency Call Service

Division/branch

Consumer Safeguards Branch, Infrastructure and Consumer

Delegate approval

Name	Position	Date
Kathleen Silleri	Assistant Secretary	14 May 2019

Description and purpose of project

Background

The Department of Communications and the Arts (the department) is implementing arrangements that will improve the accuracy of location information provided by callers from mobile phones to the Triple Zero Emergency Call Service (managed by Telstra as the Emergency Call Person (ECP)), and subsequently provided to appropriate Emergency Services Organisations (ESOs) (the Police, Fire and Ambulance services of each Australian State and Territory).

The ECP currently receives two types of caller location information from telecommunications carriers.

- Standardised Mobile Service Area data — which indicates a broad geographic region where the mobile call has originated from. This data is sent by the telecommunications carrier with the call to Triple Zero. All calls from fixed-lines also carry SMSA data, but the data simply indicates that the call is a fixed-line call (and the caller's location is looked-up using service address information from the Integrated Public Number Database (IPND) - see further information below).
- Push MoLI data — provided by mobile carriers is more accurate than SMSA data. Push MoLI automatically provides a 'polygon' indicating the probable location of the caller (based on the mobile base station the caller is connected to). In urban areas Push MoLI may be as accurate as a few hundred square metres, but in regional areas it may provide a radius of several hundred square kilometres in which the caller may be based.

For each call made to Triple Zero, the ECP interrogates data contained in the Integrated Public Number Database (IPND). The caller service address or billing address is provided to the ESO that the call is transferred to (providing accurate information for fixed-line calls, but uncertain information for mobile callers as they may not be calling from the service or billing address). The IPND is managed by Telstra under its carrier licence conditions (see the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997).

In May 2016, the Review of the National Triple Zero (000) Operator was released. Recommendation 1.1 of the review recommended that:

> ***'The inclusion of capability to reliably receive and automatically forward more accurate location-based data (coordinates) from mobile emergency callers to the Emergency Service Organisations should be a priority in the development of the Triple Zero service.'***

In response to the review, the Department conducted an Expression of Interest process which identified 'Advanced Mobile Location' (AML) as the Department's preferred solution for delivering improved mobile location information.

The new arrangements are expected to be implemented and operating from May 2020.

How AML works

AML derived location information will be provided to the Triple Zero Emergency Call Service, in addition to the SMSA, Push MoLI and service address information that is currently provided.

AML is a caller location technology that allows a smartphone to send a caller's location directly to emergency services (via the Triple Zero Emergency Call Service). An AML-enabled smartphone will calculate a caller's location based on one of three sources of location data:

- Global Navigation Satellite System (GNSS) — the most commonly used GNSS system in Australia is the Global Positioning System (GPS)
- calculations based on proximity to Wi-Fi base stations, or
- calculations based on proximity to mobile base stations.

An AML-enabled smartphone recognises when an emergency call is made (to either the Triple Zero (000) or 112 numbers in Australia) and, if not already activated, activates the phone's GNSS functions. The handset then assesses the information available to it from the three potential location information sources, and selects the methodology that will provide the most accurate location. For example, if the handset cannot get a 'fix' on the GNSS satellites, it may opt to use the Wi-Fi calculation method instead. Once a location is calculated, the handset then sends an automatic SMS (or data transmission to an https endpoint) to the Triple Zero call centre, before turning off the GNSS (if it was turned off when the call was initiated). The SMS contains the latitude and longitude coordinates of the caller.

The AML service is available on all handsets utilising the Android Operating System (version 2.3 and above with Google Play Services enabled (ninety-nine percent of Android handsets)), and the Apple iOS operating system version 12 and above.

When undertaking the calculation of the caller's location, the handset may interrogate location service databases that assist to either accelerate the calculation of the location, or provide information in regards to the location of Wi-Fi base stations or mobile base stations. For GNSS/GPS purposes, this functionality is known as Assisted-GPS, which accelerates the 'time to first fix' — a measure of the time required by a GPS receiver to acquire satellite signals and calculate a position.

The AML process is automatic, and does not require the caller to do anything — a caller's location is sent in the background as they dial and speak to emergency services. The calculated location data is not stored by the operating system provider — the location data is only sent on to the Triple Zero call centre via an SMS message generated by handset. Mobile carriers may be required to store AML SMS messages for law enforcement purposes, under Section 107G of the Telecommunications

(Interception and Access) Act. AML is not an application that is required to be downloaded, it is part of the operating system of the mobile handset.

The European Telecommunications Standards Institute (ETSI) reports that AML has the potential to provide location precision down to 5 metres for outdoor locations and around a 25-metre radius for indoor locations[1].

AML has been implemented in a number of countries such as New Zealand, the United Kingdom, Finland, Ireland, Lithuania, Belgium, Slovenia and Estonia.

Legislative and contractual framework

The Telecommunications Act 1997 (Telco Act), the Telecommunications (Consumer Protection and Service Standards) Act 1999 (TCPSS Act), and the Telecommunications (Emergency Call Service) Determination 2009 (ECS Determination) provide the legislative and regulatory framework for the provision of the ECS.

The Telecommunications Act 1997

Section 276 of the Telco Act prohibits an eligible person (defined in section 271 as a carrier, carriage service provider, their employees or contractors) to disclose or use information that relates to the contents or substance of communications carried by their service. However section 286 of the Telco Act permits disclosure to an ESO or ECP of information (such as name, phone number, address, location, matters raised during call) gained during an emergency call, for the purposes of dealing with the matters raised during call. It is the department's view that section 286 adequately provides a legislative basis for the provision of AML location data to the ECP, and subsequent provision to the relevant ESO.

Part 13 of the Telco Act provides additional coverage for the disclosure of location information through AML-enabled handsets as follows:

- Section 287 of the Telco Act provides additional assurance, allowing disclosure or use of information or a document if the information relates to the affairs or personal particulars of another person, and the first person believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious and imminent threat to the life or health of a person
- Section 288 allows disclosure or use of information if the disclosure is reasonably necessary for the preservation of human life at sea, or relates to the location of a vessel at sea
- Section 289 allows disclosure or use if the caller is likely or reasonably likely to have been aware or made aware that information of that kind is usually disclosed or used in the circumstances concerned
- Section 290 allows disclosure of information if having regard to all the relevant circumstances, it might reasonably be expected that the sender and the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use.

[1] ETSI Technical Report — ETSI TR 103 393 v1.1.1 (2016-03) — Emergency Communications (EMTEL); Advanced Mobile Location for emergency calls. Downloaded from http://www.etsi.org/standards-search.

The TCPSS Act and the Telecommunications (Emergency Call Service) Determination 2009

Section 147 of the TCPSS Act requires the Australian Communications and Media Authority to make a Determination that imposes requirements on carriers, carriage service providers and emergency call persons in relation to the emergency call service. The importance of location information is identified in section 147 (2)(i) of the TCPSS Act which states that the Determination must have:

> ***'the objective that carriage services used to make calls to an emergency service number should, as far as practicable, provide the emergency call person concerned with automatic information about:***
>
> ***(i) the location of the caller, and***
> ***(ii) the identity of the customer of the service being used by the caller'.***

This requirement is reflected in section 49(3) of the ECS Determination, which requires calls made on a mobile to provide all the relevant information that is available about the caller's approximate location in accordance with an industry guideline published by the Communications Alliance Ltd (as in force from time to time). The current version of the industry guideline is G557 Location Information for Emergency Calls. The Communications Alliance (www.commsalliance.com.au — an industry forum) is currently working to implement a new part to the guideline to reflect the arrangements for Advanced Mobile Location for handset-derived location information.

Section 52(A) of the ECS Determination requires mobile carriers to provide the most precise mobile location information available about the location of the customer equipment from which an emergency call from a mobile phone was made, when a request from an ESO is received. This process is known in the industry as Pull MoLI (as it is undertaken on request from an ESO). The department does not intend for similar arrangements to be implemented for AML, as AML does not allow Pull requests of data from a handset. Arrangements are being implemented however, for an ESO to request the AML-derived location information from the ECP (not the mobile carrier) if the AML data has not been provided when the call is transferred to an ESO (this may occur where the location information was not able to be provided to the ESO due to a delay in the handset deriving and sending the location data).

Personal information involved

AML is a caller location technology that allows a smartphone to send a caller's location directly to emergency services.

Table 1: Types personal information collected

Information	Collection	Visibility	Use
Caller mobile number	ECP — number is visible (including unlisted)	ECP ESOs	ECP ESOs
Location information — latitude, longitude, altitude, IMEI, IMSI	Handset Operating System activates AML functionality when an emergency call is made and calculates location using either GPS, Wi-Fi or mobile base station location information. Location information is sent automatically by SMS to the ECP's SMS gateway, which accepts the location data, and matches it to the voice call received. The location information is provided to the relevant ESO that the ECP transfers the call to.	ECP accepts data and transfers to ESOs (ECP call-takers do not have visibility of AML caller location information). ESO call-takers receive location with transferred calls, or may request location data that the ECP has received if that location data was unable to be provided to the ECP when the call was first transferred.	ECP ESOs

Stakeholder consultation undertaken

The department continues to work with the following stakeholders:

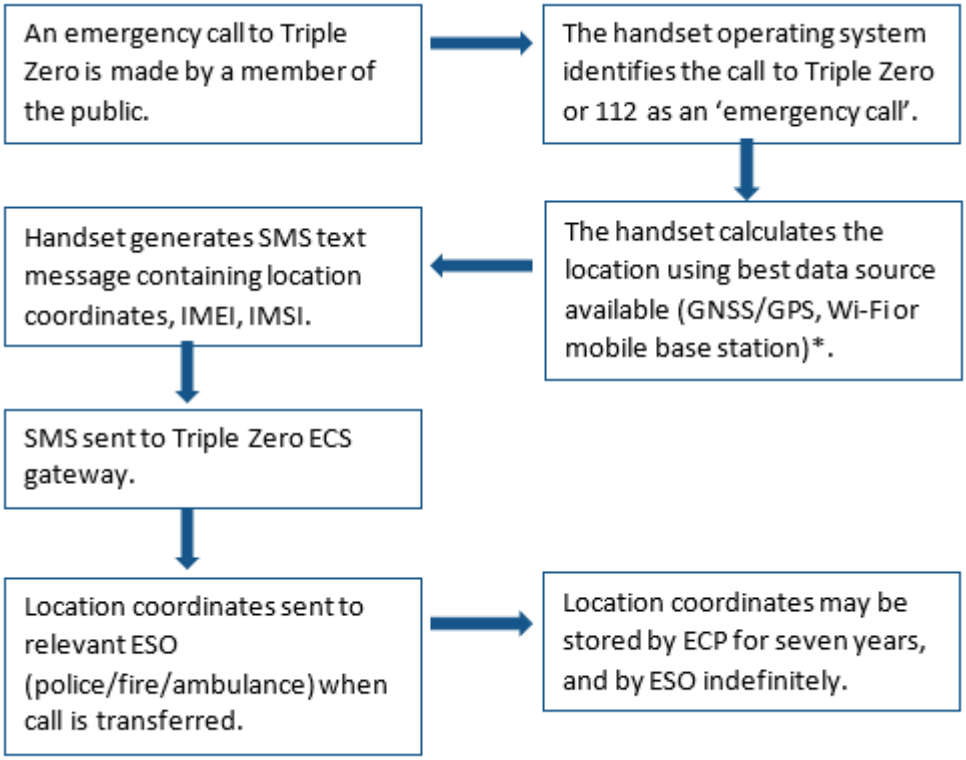
- Telstra (in its role as ECP)
- ESOs (the Police, Fire and Ambulance services of each Australian State and Territory)
- Mobile operating system providers (Apple and Google)
    - Apple and Google have agreed to implement the necessary technical changes to the iOS and Android operating systems for Australian users. This is through the implementation of the European Technical Standard Institute (ETSI) Technical Standard EMTEL-00035.
- Mobile carriers

The department and mobile operating system providers will not handle AML data or store it. Under Section 107G of the Telecommunications (Interception and Access) Act, mobile carriers may be required by a law enforcement agency to retain SMS messages, including SMS messages containing AML data.

AML data will be stored by Telstra (in its role as ECP) and ESOs. All stakeholders will comply with the Australian Privacy Principles, the Privacy Act 1988 and relevant State/Territory based legislative, regulatory or code obligations applying to public service organisations.

Map of personal information flows

Figure 1: Map of personal information flows



Privacy impact analysis and compliance check

As previously stated:

- The department will not handle AML data or store it.
- The data will not be stored by the operating system provider.
- Mobile carriers may be required to store SMS messages, including those containing AML data, for law enforcement purposes under section 107G of the Telecommunications (Interception and Access) Act 1979.

Telstra, as the ECP and States and Territory ESOs will handle and store AML data in compliance with the Australian Privacy Principles, the Privacy Act 1988 and relevant State/Territory based legislative, regulatory or code obligations applying to public service organisations.

The positive privacy impacts of the project are:

- Information disclosed by individuals will assist Police, Fire and Ambulance services to locate callers to Triple Zero, assisting in:
    - the identification of an accurate location for the dispatch of resources when a caller does not know their location (including search and rescue operations), is unable to speak (due to illness/injury, or threat to their safety), or where a physical street address is not available;
    - confirmation of address or location details provided by a caller;
    - the provision of updated location information where a caller to Triple Zero is moving or in transit when making the call.

The negative privacy impacts of the project are:

- There are no identified negative impacts.

APP 1 — Open and transparent management of personal information

The department and all other parties involved in the implementation and provision of AML are familiar with the Office of the Australian Information Commissioner's privacy information and understand the obligations with regard to dealing with personal information.

Telstra, as the ECP, will, where necessary, develop privacy policies or amend existing policies to capture requirements for the management of personal information.

ESOs and mobile carriers will review their existing privacy policies to determine whether they adequately cover the new location information that will be collected.

APP 2 — Anonymity and pseudonymity

Telstra, as the ECP and ESOs do not ask the caller for their identity and a caller may choose not to verbally disclose his or her name.

Details such as the mobile phone number and the name under which a phone service is registered will be automatically provided to the ECP/ESO along with the voice call (this is existing practice). Given a caller may not be using his or her own phone, this information may not necessarily identify the caller.

APP 3 — Collection of solicited personal information

AML data collected by ESOs is reasonably necessary for the efficient operation of the Triple Zero Emergency Call Service as AML arrangements will improve the accuracy of location information provided by callers from mobile phones. The collection of this information is authorised by Sections 286, 287, 288, 289 and 290 of the Telecommunications Act 1997.

APP 4 — Dealing with unsolicited personal information

The department considers that the personal information collected is solicited information. The collection of this information is authorised by Sections 286, 287, 288, 289 and 290 of the Telecommunications Act 1997. Individuals from the Australian community have a reasonable expectation that their location information is provided to the ECP and an ESO as part of the delivery of the Triple Zero Emergency Call Service to ensure the protection of life and property.

APP 5 — Notification of the collection of personal information

APP 5.2(c) establishes that a notice is not required if authorised by on under an Australian law. The collection of AML information is permitted by Sections 286, 287, 288, 289 and 290 of the Telecommunications Act 1997.

Furthermore, APP5 acknowledges that it may be reasonable for an APP entity to not take any steps to provide a notice or ensure awareness of all or some APP5 matters where notification may pose a serious threat to life, health, or safety of an individual or pose a threat to public health or safety. Given the need for urgent response to all calls to the Triple Zero Emergency Call Service, the Department considers it reasonable not to provide a notice at the point of collection of this information.

Operating system providers will implement AML technology through a system update to mobile handsets. The inclusion of AML on an individual's handset and the information that will be collected will be communicated to the individual in the terms and conditions of the upgrade.

APP 6 — Use or disclosure of personal information

Information will be collected primarily to allow the ECP and ESOs to accurately determine the location of a caller to the Triple Zero Emergency Call Service.

Information may be used for a secondary purpose including for the investigation of a matter by an enforcement body related to the original call to Triple Zero (by a State or Territory police force, or the Australian Federal Police under APP6.2(e). Note these organisations are included in the definition of an enforcement body in the Privacy Act 1988.

APP 7 — Direct marketing

Not applicable for the Department of Communications and Arts or this project.

APP 8 — Cross-border disclosure of personal information

The personal information will not be transferred or stored overseas. However, when the mobile handset derives the location information it may access information technology systems overseas to assist the operating system of the handset to calculate location (through assisted-GNSS or Wi-Fi database lookup).

APP 9 — Adoption, use or disclosure of government related identifiers

Not applicable for the Department of Communications and Arts or this project. The department is not listed in:

(a) Part I of Schedule 2 to the FOI Act, or
(b) the department's acts or practices in respect of the Project relate to a commercial activity of the department that is specified in Part II of Schedule 2 to the FOI Act.

APP 10 — Quality of personal information

AML data is generated by the operating system of the mobile handset, and the department considers that all data will be reasonably accurate, up-to-date and complete to facilitate the primary purpose of enabling an ESO to establish the location of an emergency caller.

The department does not expect to need to review data as the data record captures a location at a point in time, and will not be subject to amendment after the call to Triple Zero has been completed.

APP 11 — Security of personal information

No personal or sensitive information is directly collected, stored, accessed, used or disclosed by the department in the delivery of the ECS. The protection of personal information by each ESO will be the responsibility of each ESO. Nevertheless, as the project leader, the department via the Triple Zero Coordination Committee will work with ESOs to ensure that access to information is limited to those who 'need to know'. This will involve each ESO ensuring that access to location data is restricted to staff on a need to know basis, which for call takers will be only be when a call is actively handled. Each ESO will ensure information is stored securely, receives the correct security classification, and staff who have access are trained in and understand their security responsibilities.

The department will also work with ESOs, mobile carriers and other stakeholders about the appropriate arrangements for destroying or de-identifying personal information. The principle to be applied will be that the ECP must not retain the location information for longer than is required for the primary purpose.

APP 12, APP 13 — Access to and correction of personal information

The AML process is automatic, and does not require the caller to do anything — a caller's location is sent in the background as they dial and speak to emergency services. For legal and reporting purposes, it will not be possible to alter the information after a call to the Triple Zero Emergency Call Service has been made.

Managing privacy impacts

As the project leader, the department via the Triple Zero Coordination Committee will work with ESOs so that appropriate management of privacy impacts are in place.

Circulation of PIA report

Internal: Privacy team

External: Telstra, as the ECP, State and Territory ESOs, mobile carriers.

Future review of PIA

The PIA will be reviewed (and updated as necessary) commencing from the date of the delegate's approval.

Publication of the PIA summary

Under the privacy code, the department is required to maintain and publish a registered summary of all PIAs it conducts. The Privacy Impact Assessment register is published on our external internet and must be updated periodically by the privacy team.

Glossary

Acronyms and initialisms

Table 2: Acronyms and initialism

Acronym	Description
AML	Advanced Mobile Location
APP	Australian Privacy Principle
Department	Department of Communications and the Arts
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment

Definitions

Table 3: Definitions

Acronym	Description
APP Guidelines or Guidelines	The APP Guidelines published by the OAIC at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/. The APP Guidelines outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing an Agency's compliance with the Privacy Act and the APPs.
APP Entity	Has the same meaning given under the Privacy Act 1988 (Cth).
Approved Privacy Code	Means an APP Code, as defined under section 26C of the Privacy Act.
Commonwealth entity	Has the same meaning given under the Public Governance, Performance and Accountability Act 2013 (Cth). This PIA also refers to Commonwealth entities as 'Agencies'.
Organisation	Has the same meaning given under section 6C of the Privacy Act.
Personal information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not, as defined in section 6 of the Privacy Act. Personal Information may, in certain circumstances, include the following: (a) an email address (where that address contains a person's name); (b) an email address (in cases where that address does not contain a person's name, but the identity of the email account holder can be reasonably identified, including by reference to account-related information holdings); (c) a telephone number (in cases where the person associated with the telephone number can be reasonably identified by reference to account-related information holdings); (d) an IP address (in cases where the holder of the IP address can be reasonably identified by reference to account-related information holdings); and (e) a MAC address (in cases where the operator of the network interface can be reasonably identified by reference to account-related information holdings). It is important to note that 'individuals' who are captured by the definition of Personal Information include APS public servants and Privileged Users. In other words, the protections under the Privacy Act that apply to the Personal Information of 'individuals' apply to APS public servant and privileged users.
Privacy Act	The Privacy Act 1988 (Cth).
Privacy Impact Assessment Guide	The OAIC's Guide to Undertaking Privacy Assessments (May 2014), available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments.

Acronym	Description
Sensitive information	means: (a) information or an opinion about an individual's: (i) racial or ethnic origin, or (ii) political opinions, or (iii) membership of a political association, or (iv)religious beliefs or affiliations, or (v) philosophical beliefs, or (vi)membership of a professional or trade association, or (vii) membership of a trade union, or (viii) sexual orientation or practices, or (ix)criminal record; that is also personal information, or (b) health information about an individual, or (c) genetic information about an individual that is not otherwise health information, or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or (e) biometric templates.

Other resources

Table 4: Other resources

Acronym	Description
Australian Privacy Principles	https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles