The Types of Telecommunications Device Identification and Location Approximation Metadata: Under Australia's Warrantless Mandatory Metadata Retention and Disclosure Laws

By Stanley Shanapinda, Ph.D. Candidate, UNSW SEIT (ACCS, UNSW Law, D2D CRC)

INTRODUCTION

This article briefly discusses the legal duties of Australian telecommunications service providers (**Telcos**) to access, use, retain, create and disclose device identification and location information. In this context, the device identification and location information is the relevant metadata. The article also touches on the powers of law enforcement and national security agencies (**the Agencies**) to authorise the disclosure, access and use of the device identification and location metadata. It provides a brief description of the types of identification and location metadata Telcos are legally compelled to retain, create and disclose. The intention of this article is to describe to lawyers, who practise in the areas of communications and privacy law, six of the methods that may be used to identify and approximate the physical or logical location of fixed or mobile telecommunications devices.

COMPELLED ASSISTANCE

Telcos are required to provide such help as is reasonably necessary to the Agencies. Compelled assistance is imposed by subsections 313(3), (4) and (7) of the *Telecommunications Act 1997 (Cth)*. Reasonably necessary assistance means the disclosure of identification and location metadata of telecommunications equipment or a line used in connection with a communication. The duty to retain the metadata prior to its disclosure is set out in subsection 187A and subsection 187AA (1) of the *Telecommunications Interception and Access Act 1979 (Cth)* (**TIA Act**), in Items 2, 3 and 6 of the data set specifically. Identification and location metadata are required to be retained for a period of two years or more, in terms of section 187C of the TIA Act. In judge and jury fashion, the device identification and location metadata must be disclosed upon authorisation by the very same Agencies, without requiring a judicial warrant. Under the TIA Act, the device identification and location metadata may be historical or prospective.

METHODS FOR DEVICE IDENTIFICATION AND LOCATION APPROXIMATION

The identification and detection of the approximated location of telecommunications devices may be done in any of the six methods, briefly described below. The devices may be mobile (wireless), fixed, or fixed-wireless.

Mobile wireless devices may include Wi-Fi routers and modems; tablets; dumb phones and smartphones. Fixed devices may include fixed-line telephone devices and ADSL. Fixed-mobile devices include WiMAX and HFC cable networks, such as those offered by the NBN Co.

Other devices and equipment include the Base Transceiver Station (**BTS**) housed close to a cell tower and the physical location of the actual physical tower. Identification and location detection may be done by both or either of the parties. This may depend on whether raw location data is retained and disclosed, that may require triangulation.[1]

Using GNSS (Global Navigation Satellite System)

As the name suggests, GNSS includes all the satellite systems of the world. It includes GPS, the American system; Galileo, the EU system that is currently being deployed; and the Russian system GLONASS; but not limited thereto. There is no telling which system a device is using. Apple uses Assisted GPS and GLONASS. The location is approximated in terms of latitude, longitude and possibly altitude, and may have an accuracy of between 15m to 1m. It is never precise, and even less so in urban areas, than in an open field.[2]

[1] ACMA. (2010). *Mobile location information Location assisted response alternatives*. Retrieved from Canberra http://www.acma.gov.au/webwr/_assets/main/lib311840/mobile_location_information_location_assisted_response_alternatives.pdf.

[2] Forensics, C. M. (Producer). (2015, 14 May 2016). Understanding Location Information Extracted From Mobile Devices Professor David Last. Retrieved from https://www.youtube.com/watch?v=6rm4wixUPzk&feature=youtu.be&elqTrackId=6AE31B9C63C526AA355016A1D00F; and Apple. (2016). iPhone 6. Retrieved from http://www.apple.com/au/iphone-6/specs/.

[3] Brandis, G. (2015). *Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2015 Revised Explanatory Memorandum*. Canberra: THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA Retrieved from http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c%22; p.50.

According to the revised Explanatory Memorandum submitted with the *Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2015*, the Telcos are not required to keep the continuous GPS location of a device.[3]

The intention of this article is to describe to lawyers, who practise in the areas of communications and privacy law, six of the methods that may be used to identify and approximate the physical or logical location of fixed or mobile telecommunications devices

Using the Subscriber's Address

The simplest method is using the subscriber's residential and/or business address.[4]

It is for this reason subscribers of either fixed, mobile or fixed-mobile telecommunications services are required to submit identity and residential documentation. Prepaid mobile subscribers have been legally compelled to do so since 1997. Telcos are forbidden to activate any pre-paid mobile services for which no identity documentation is submitted. No subscriber will be rendered a service and no Universal Integrated Circuit Card (**UICC**) will be activated in respect of that subscriber, unless the identification requirements have been met. These are requirements in terms of the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013*.[5] The subscriber may be required to notify the Telco of any address changes, or if and when the UICC is lost or stolen.

Using the Telco's Network

Using the UICC

The UICC is a smart card, the IC (Integrated Card). It is commonly referred to as the SIM-card. The UICC has an Integrated Circuit Card Identifier (ICCID) that consists of the number 89, representing the telecommunications industry, the country code, and the MNC, e.g. 03 and a 14 digit code. The location area of the device is stored on the SIMs.

The smart card contains the SIM-card or the USIM-card software applications (Project, 2015). These in turn contain the IMSI (International Mobile Subscriber Identity). Without the IMSI no cellular phone service can technically be provided to the subscriber. It is used to identify and authenticate the subscriber to use the cellular network. The IMSI differentiates the subscriber from all other users of the network.[6]

The IMSI consists of three fields, i.e. the mobile country code (**MCC**), the mobile network code (**MNC**), and the mobile subscription identification number (**MSIN**) or mobile identification number (**MIN**). Australia's MCC is 505 and Telstra's network code is 01, for example. The MSIN is a 10-digit number that uniquely identifies a subscriber. It is issued by the Telco to register the subscriber, to authenticate the handset for use, to retrieve any subscription data and for billing purposes.[7]

The MSIN and the Mobile Station ISDN (MSISDN) are associated to identify the subscriber.[8]

The MSISDN comprises the CC (Country Code) and the National (significant) mobile number. The National (significant) mobile number in turn comprises the NDC (National Destination Code) and the Subscriber Number (SN).[9] Australia's CC is 61.[10]

This may be what makes IMSI-catchers or cell site simulators, branded as StingRay amongst others, popular with American agencies such as the FBI and the NSA.

Using BTS

Telcos are also required to retain and disclose the location of the BTS.[11] The device can use the Base Station Identify Code (BSIC) to differentiate between two BTSs. This is a 6 bit color code.[12]

To approximate the location of a mobile cellular device, the unique ID of the cell within the Telco's network must be determined. This unique ID is called the Cell Global Identification (**CGI**). The CGI is in turn identified from the Location Area Identification (**LAI**) and the Cell Identity (CI).[13]

[4] Attorney General's Department (2015). *DATA RETENTION Frequently Asked Questions for Industry*. Canberra: Attorney General Department Retrieved from https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionIndustryFAQS.pdf; p22.

[5] *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013* (Cth), section 2.3.

[6] ITU. (2011). List Of ITU-T Recommendation E.164 Assigned Country Codes ITU, p.1.

[7] ITU. (2008). The international identification plan for public networks and subscriptions *SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS* (pp. 1). Geneva: ITU-T; p.2.

[8] ETSI. (2016), Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (pp. 22, 24, 25). Sophia Antipolis Cedex - FRANCE: ETSI; pp. 16, 22.

[9] Ibid.

[10] ITU, (2011).

[11] Brandis, G. (2015); p. 50.

[12] ETSI. (2016), Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (pp. 22, 24, 25). Sophia Antipolis Cedex - FRANCE: ETSI; p. 25.

[13] Ibid.

The LAI comprises the MCC, the MNC and the Location Area Code (LAC). The LAC is a hexadecimal number issued by the system.[14]

These identifiers are used to triangulate the position of the device in question.[15]

Triangulation algorithms

Triangulation algorithms are used to locate mobile devices. The two methods are the Cell ID (CID)-RTT (Round Trip Time) and the Radio Frequency (RF) pattern matching method.[16]

In the Cell ID-RTT method the distance from the corresponding cell to the device is calculated, using the Timing Advance (TA).[17] Every RTT measurement is used to calculate the distance. The intersection of the RTT circles is taken to be the location of the device. With the RF pattern matching method, in addition to using the CellID RTT method, a comparison of the radio signal strengths is used.[18]

However, Telcos are not required to conduct additional processing or triangulation. Telcos can simply provide the RTT measurements and the database of the signal strengths, if available from the network.[19]

Using the Handset

Whereas the IMSI is used to identify the user, the International Mobile Station Equipment Identity (**IMEI**) is used to identify the mobile handset. The IMEI contains the origin, model and serial number of the handset.[20]

The IMEI can be retrieved by typing the Unstructured Supplementary Service Data (USSD) code *#06# into the keypad of most mobile phones.

Using the WLAN (Wireless Local Area Network)

Each mobile device has a Media Access Control (**MAC**) address assigned to it by the manufacturer. The MAC address is required to be stored and disclosed.[21] This number was generally static but may be dynamically assigned, by the likes of Apple. MAC addresses are used for billing purposes to uniquely identify the subscriber. It consists of six groups of two hexadecimal digits, with six octets.[22]

When a Wi-Fi router or smart phone detects a WLAN, it will determine if the MAC address is white-listed to use its services. If it is, it will be authenticated, after the correct password is entered and accepted, if required. The MAC address is filtered in this manner.[23] The MAC address is defined as a telecommunications number in section 5 of the TIA Act and must be retained and disclosed, under that legislation.

Using the Hybrid Method

Telcos and the Agencies may generally use a combination of the above methods. These include cell tower signal strength, wireless signal strengths for internet connectivity, Bluetooth sensors and IP addresses.

CONCLUSION

As one can readily see, there are many methods by which a telecommunications device, whether fixed or mobile, can be identified. Through those processes, it is also possible to identify the person registered to operate that device (although not necessarily the person using the device at any particular time), in relation to a criminal investigation, a cybercrime investigation or intelligence gathering for national security purposes. The types of location information and the approximation methods described are by no means a closed list of location metadata.

No doubt, the techniques used to locate and identify end users will evolve as the technology does

No doubt, the techniques used to locate and identify end users will evolve as the technology does. Lawyers advising telecommunications companies and their customers, or security or law enforcement agencies, will need to familiarise themselves with some of the internal architecture of the telecommunications devices that have become a defining feature of the modern digital economy.

[14] Ibid., p. 24.

[15] ACMA. (2010); p.7.

[16] ETSI. (2010). Universal Mobile Telecommunications System (UMTS); Evaluation of the inclusion of path loss based location technology in the UTRAN (3GPP TR 25.907 version 9.0.1 Release 9) p.14; Clarke, R., & Wigan, M. (2011). You are where you've been: the privacy implications of location and tracking technologies. *Journal of Location Based Services, 5*(3-4), 138–155. doi:10.1080/17489725.2011.637969; p,144; ACMA (2010), pp. 7, 9, 14.

[17] ETSI. (2016). Digital cellular telecommunications systems (Phase 2+) (GSM) Functional stage 2 description of Location Services (LCS) in GERAN (3GPP TS 43.059 version 13.1.0 Release 13) (pp. 8,10, 11,12,13,14). Sophia Antipolis Cedex – FRANCE; p.12.

[18] ETSI (2010), p. 14.

[19] Attorney General's Department, p. 15.

[20] ETSI. (2009). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; International Mobile station Equipment Identities (IMEI) (Release 9) (pp. 5). Sophia Antipolis Valbonne - FRANCE: ETSI; p.5.

[21] Attorney General's Department, p. 14.

[22] IEEE. (2016). Guidelines for 64-bit Global Identifier (EUI-64). Retrieved from https://standards.ieee.org/develop/regauth/tut/eui64.pdf.

[23] Huawei Technologies Co, L. (2012). WLAN Access Security Technical White Paper(2), 3. Retrieved from http://e.huawei.com/en website: http://e.huawei.com/uk/marketing-material/onLineView?MaterialID=%7BA944F23F-EF58-43E5-AF55-AC7951B73E83%7D.