# TELSTRA TRANSPARENCY REPORT

1 July -31 December 2013

IT'S HOW WE CONNECT

# TELSTRA TRANSPARENCY REPORT

## INTRODUCTION

Millions of Australians trust Telstra to provide their telecommunications services. As part of honouring this trust, we have produced our first Transparency Report.

Telstra is bound by Australian privacy law which protects the personal information of our customers.

We are also required, like all telecommunications companies that provide services in Australia, to assist Australian national security and law enforcement agencies. This assistance may involve disclosing customer information.

This assistance is provided for specific reasons, such as enforcing criminal law, protecting public revenue and safeguarding national security. We also provide assistance to emergency services agencies in response to life threatening situations and Triple Zero emergency calls.

We only disclose customer information in accordance with the law. This is a non-negotiable part of the way we operate. We assess any request for information to ensure it complies with the law. When acting on these lawful requests, we seek to never interfere with our customers' legitimate use and enjoyment of our services.

The Telstra Transparency Report aims to keep our customers informed of the requests we have received for access to information from Government agencies in line with our legal obligations both in Australia and overseas.

Our report is the first of its kind in Australia, but is aligned with recent international reporting and builds on existing reporting in Australia undertaken by the Attorney General's Department and the Australian Communications and Media Authority.

We believe complying with the law is an important part of being a responsible corporate citizen. Equally, being open and upfront with our customers about the legal obligations that come with being a telecommunications company helps build confidence in our products and services.

As digital technology continues to evolve rapidly, law enforcement issues are likely to continue to be the subject of significant discussion in the community. We hope the Telstra Transparency Report makes a meaningful contribution to these discussions and helps our customers understand our obligations under law.

This inaugural Telstra Transparency Report provides figures for the six months ending 31 December 2013. Future Transparency Reports will be published annually at the end of the financial year.

Kate Hughes
Chief Risk Officer

# TELSTRA TRANSPARENCY REPORT

## SCOPE

For our business in Australia, the report relates to activities by law enforcement agencies as well as regulatory bodies and emergency services organisations (the 'agencies'). It does not include figures on requests for information by national security bodies. Our understanding of the Attorney-General's Department's position on requests by national security agencies is that reporting on these figures is prohibited under the *Telecommunications (Interception and Access) Act 1979*.

## LAWFUL ORDERS

Like all telecommunications companies that provide services in Australia, we are required by law to assist Australian Government agencies for defined purposes such as enforcing criminal law and protecting public revenue. Part of our obligation is to act on requests under law for our customer information and carriage service records, and warrants for communications travelling over or held in our network. Between 1 July and 31 December 2013, across a base of more than 26 million active retail services, Telstra received approximately 40,000 requests for customer information.

## LAW ENFORCEMENT REQUESTS

1 July – 31 December 2013[1]

| | |
|---|---|
| Telstra customer information, carriage service records and pre-warrant checks | 36,053 |
| Life threatening situations and Triple Zero emergency calls | 2,871 |
| Court orders | 270 |
| Warrants for interception or access to stored communications | 1,450 |
| **Total** | **40,644** |

**Notes:**
1. These figures do not include requests by national security agencies.

## TYPE OF REQUESTS

### Customer information

Customer information refers to details that appear on a phone bill, such as the customer's name, address, service number and connection dates. It can include other information we may hold such as a customer's date of birth and previous address.

Carriage service records relate to use of telecommunications services, including call records, SMS records, and internet records. These records include information such as details of a called party, and the date, time and duration of a call. Internet session information includes the date, time and duration of internet sessions as well as email logs from Bigpond addresses.

A pre-warrant check confirms that telecommunication services of interest are still active with Telstra.

### Life threatening situations

Telecommunications carriers act on requests from authorised emergency service agencies (e.g. police, fire, ambulance) where the release of customer information could prevent or lessen an imminent threat to the life or health of a person. Information may also be requested by law enforcement agencies where calls to emergency service numbers (i.e. 000, 112 and 106) have taken place.

### Court orders

Court orders such as subpoenas and coronial requests issued by a court or judge require us to provide customer information and carriage service records. Typically, court orders involve a civil dispute that involves individuals or organisations and related telecommunications data is required by the court to adjudicate on the matter.

### Warrants

A warrant is required for an agency to access the content of a communication. Warrants require us to provide the relevant agency with real time access to communications as they are carried over our network (e.g. a lawful interception). Warrants may also compel us to supply the content of communications after it has been delivered.

## OTHER TYPES OF DISCLOSURES

### Integrated Public Number Database

The Integrated Public Number Database (IPND) is a centralised database of all Australian telephone numbers including the service and directory addresses provided by the customer. The database is managed by Telstra, as required under our carrier licence issued by the Australia Government, and contains numbers from all telecommunications service providers in Australia.

The IPND is used most critically for the operation of the Triple Zero emergency call service and for law enforcement and national security purposes. Relevant agencies are able to access certain information, in particular the name and address associated with a particular phone number. The IPND Code and Telecommunications Act 1997 contain strict provisions on how information on the IPND can be accessed and used.

In the six months to 31 December 2013, the IPND was accessed by agencies around 50,000 times, excluding national security agencies. These figures do not relate to information of Telstra customers per se, as the IPND holds data on every phone number from every telecommunications service provider in Australia.

### Emergency Alerts

For the purpose of providing emergency warnings on likely or actual emergencies, such as fire, flood or extreme weather, emergency services agencies can access data from the IPND.

Organisations such as the police, fire and state emergency services can send voice messages to landlines and text messages to mobile phones on all telecommunications carriers' networks through

*Emergency Alert,* the national telephone warning system. This means that the agencies can access phone numbers based on a person's service address or their physical location at any given time, purely for the purpose of providing important community warnings.

Operators of Emergency Alert do not have access to customer names, they only use telephone numbers and service addresses. Information on telephone locations is not retained.

## OTHER ISSUES

### International operations

Telstra is an Australian company with a global footprint. As such, we have presence in many countries around the world. Wherever Telstra operates, we have to comply with the laws of the land.

No law enforcement or national security agencies from other countries have authority in Australia; only Australian authorities can request customer information. We are prevented by Australian law from acting on any direct requests from overseas authorities.

Similarly, in other countries where Telstra operates infrastructure or provides services, only the agencies with jurisdiction in that country can request information from Telstra.

Our international arm, Telstra Global, provides managed network services, international data, voice and satellite services and manages our submarine cable networks and assets. Telstra Global is focused on providing services to large enterprise customers, rather than individual consumers.

Across all the countries in which Telstra Global operates, we received less than 100 requests for customer information in the six months to 31 December 2013.

### Networks and infrastructure

Under Section 313 of the Telecommunications Act 1997, all carriers in Australia are obliged to do their best to prevent their networks and facilities from being used in the commission of a crime.

In addition to giving effect to requests under law, authorisations and warrants, from time to time Telstra receives requests from Government agencies to take actions at an infrastructure level to prevent a crime. For example, Telstra blocks the Interpol generated 'worst of the worst' list of child abuse sites under a Section 313 request.

These network or infrastructure level requests are relatively infrequent and generally do not involve the disclosure of customer information.

## FREQUENTLY ASKED QUESTIONS

### 1. Why does Telstra disclose customer information?

Like all telecommunications companies that provide services in Australia, we are required by law to assist Australian agencies for purposes such as enforcing criminal law, protecting public revenue and safeguarding national security. We also provide assistance to emergency services agencies for reasons such as responding to life threatening situations or dealing with matters relating to Triple Zero emergency calls. We only disclose customer information in accordance with the law and we assess all requests for information to ensure it complies with the law.

### 2. Which agencies have requested customer information?

The relevant legislation in this area prohibits us from providing details of specific requests made by individual agencies for customer information. Additionally, Telstra does not want to do anything that might jeopardise any investigations. The Attorney General's Department and the Australian Communications and Media Authority do produce annual reports that provide details of requests at an industry-wide level.

### 3. Why doesn't the report include figures relating to national security?

Our understanding of the Attorney-General's Department's position on requests by national security agencies is that reporting on these figures is prohibited under the *Telecommunications (Interception and Access) Act, 1979.* Any enquiries on matters of national security should be directed to the Attorney-General's Department.

### 4. Can I find out if my information has been disclosed to a Government agency?

The relevant legislation in this area prohibits us from providing details of specific requests made by individual agencies for customer information. Any enquiries of the activities of Government agencies need to be directed to the agencies themselves.

### 5. What limits are placed on Australian Government agencies in terms of making requests?

The content of communications between individuals is strictly protected by law and if agencies wish to intercept communications to obtain their content or obtain a copy of the content once the communication has been delivered they need a warrant.

For other information an agency does not necessarily require a warrant but must meet the relevant legislative conditions. For example, the agency must have reasonable grounds to believe that disclosure is reasonably necessary for the enforcement of the criminal law as well as consider the privacy implications associated with the disclosure.

### 6. How do these issues relate to privacy law?

Under Australian privacy law personal and sensitive information is strictly protected. Consistent with this law, we can only provide customer information to defined Government agencies when we receive a lawful request to do so.

### 7. Does Telstra ever reject law enforcement requests?

We only disclose customer information in accordance with the law. If a request for information from an agency is invalid or seeks information that can only be obtained via a different process (e.g. requires a warrant and the requester does not have one), we will reject it. One important difference in the law enforcement environment in Australia compared to other countries is that agencies can undertake pre-warrant checks to make sure they are targeting their warrants accurately. This reduces the instances of mistakes leading to a rejection of a warrant.

### 8. Where can I find more information?

Consumers can find out more information from:

- The Attorney-General's Department on issues of national security and telecommunications interception and access arrangements www.ag.gov.au
- The Department of Communications on assistance to agencies under the Telecommunications Act 1997 www.communications.gov.au;
- Information on Australia's privacy regime at the Office of Australian Information Commissioner www.oaic.gov.au.and
- The Australian Communications and Media Authority for information on the IPND www.acma.gov.au and Emergency Alerts www.emergencyalert.gov.au;