Submission No 238

Inquiry into potential reforms of National Security Legislation

Organisation: Telstra

1. **Can you describe Telstra's understanding of what deep packet inspection means?**

Telstra's understanding of Deep Packet inspection (DPI) is as follows: DPI equipment is typically deployed for the purposes of inspecting Internet Protocol (IP) traffic in detail (deep inspection of the IP packets). The results of such an inspection may be used, along with policy enforcement technology, to manage certain types of traffic. Telstra does not currently perform any policy enforcement.

DPI equipment may be deployed either "in-line" to achieve a policy enforcement outcome (manage traffic based on its type or intended use, for example VoIP calls to the emergency call service) or DPI may be deployed "off to the side". Deploying DPI "off to the side" is used when carriers are analysing (but not altering) IP traffic on their networks.

2. **If a data retention regime is put in place, has Telstra developed a model using Deep Packet Inspection?**

If a data retention regime were imposed, Telstra would use a range of technologies and business solutions to meet its obligations. Where existing business tools deliver an appropriate level of coverage (including security and reproducibility) then this would be the first choice. Where additional information was required that does not form part of Telstra's available pool of data then DPI could be one of the mechanisms available to meet these obligations. Telstra will not implement a data retention model prior to the passage of legislation as Telstra currently only retains customer data where there is a clearly identified business need or an existing legislative requirement to do so.

3. **Can you explain the ways that telecommunications service providers can use deep packet inspection to capture and extract data?**

Depending on the configuration of the DPI equipment it would be possible for a carrier to capture and extract specific data using DPI. The technical limits of DPI mean that the volume of data subject to such capture and extraction would need to be constrained. For example, if a carrier was required to capture all Web traffic using DPI, a very significant investment in storage and network infrastructure would be required. The carrier would also be required to secure the captured data to a high degree. At a point, the overall feasibility of such an engineering venture begins to come into question. It would be possible that the costs of implementing such a regime may start to be a significant percentage of the costs of providing the original broadband service. By way of further explanation, it is typical for a

carrier's mobile traffic mix to be up to 50% web traffic. In the last few years, that traffic has approximately doubled YoY.

It is easy to see how such a carrier would be drawn into a cycle of building ever bigger secure data centres as traffic levels rise and the customer base grows.

4. **Can DPI be configured to only capture and extract communications data, and not content?**

DPI is able to be configured to perform in a range of different roles. It may be possible to configure DPI equipment to examine header data without inspecting content. This configuration is highly dependent on the volumes of data and specific meta-data being sought. Again, this is a question of traffic volumes, equipment performance and cost.

5. **Is it possible to extract and store the necessary data and destroy any content captured by the use of deep packet inspection?**

As alluded to above, DPI is able to be configured to perform a number of roles. Extraction and storage of any data is very much dependent on the data required and the related volumes of data to be stored. Some scenarios are infeasible based on current technology. DPI technology is able to be selective *to a degree* in what is collected, again this is limited by volumes and costs.

6. **What data does Telstra currently provide to law enforcement and national security agencies, and under what circumstances (i.e. under an interception warrant and under an authorisation for access to telecommunications data)?**

See attached table below on data disclosures.

Data disclosed to law enforcement and national security agencies

Type of Data Disclosure	Data Classification	Authority for Release
Any telecommunications data or meta data but not the content or substance of a communication. . It may include: • subscriber information (including name, address, date of birth, method of payment and related account transaction details) • telephone numbers of the parties involved in the communication • the date and time of a communication • the duration of a communication • Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication, and • location-based information	Historic data - telecommunications data that is already in existence at the time of the request for access to that data	**TIA Act Section 175(2)** Allows ASIO to access existing information or documents.
		TIA Act Section 177 Disclosures by Telstra to an enforcement agency if the disclosure is reasonably necessary for the enforcement of: • criminal law; or • law imposing a pecuniary penalty or for the protection of public revenue.
		TIA Act Section 178 Allows an authorised officer of an enforcement agency to authorise a telecommunications service provider to disclose historical data if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.
		TIA Act Section 178(A) Allows access to existing information or documents for locating missing persons
		TIA Act Section 179 Allows an authorised officer of an enforcement agency to authorise a telecommunications service provider to disclose historical data if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of a pecuniary penalty or protection of the public revenue.
		Telco Act Section 280 Authorises disclosure by or under law.
		Telco Act Section 284 Dislosure of information or document to assist ACMA, ACCC, TIO, or TUSMA to help them carry out their functions.
		Telco Act Section 286 Allows access to law enforcement agencies of information or documents because of a call to an emergency service number (000).
		Telco Act Section 289 Allows for access and disclosure of information or document relating to the affairs or personal particulars of another person and the person is aware of the usual use or disclosure of such or where they have consented in circumstances concerned.

	Historic ***and*** prospective data	**Telco Act Section 287** Allows for access to existing information or documents where reasonable grounds exist or it is reasonably necessary to prevent or lesson a serious threat to the life or health a person
		Telco Act Section 288 Allows for access to information or document if reasonably necessary for the preservation of human life at sea or if in relation to the location of a vessel at sea and is made for maritime communications purposes.
Anything relating to, but not the content or substance of, a communication. It can include: • telephone numbers of the parties involved in the communication • the date and time of a communication • the duration of a communication • Internet Protocol (IP) addresses and Uniform Resource Locators (URLs) to the extent that they do not identify the content of a communication, and • location-based information	Prospective data - telecommunications data that is collected as it is created and forwarded to the law enforcement agency in near real time as a result of the request for access to that data	**TIA Act Section 176(2)** Allows telecommunications service providers to disclose information or documents that come into existence during the period for which the authorisation is in force (prospective telecommunications data). The authorisation period is 90 days.
		TIA Act Section 180 Allows an authorised officer of a 'criminal law-enforcement agency' to authorise the disclosure of prospective telecommunications data. In making the authorisation, the officer must be satisfied that the disclosure is reasonably necessary for the investigation of a Commonwealth, state or territory offence punishable by more than 3 years. The authorisation period is 90 days.
Communications and information being carried over a telecommunications network	Prospective (real time) communications and interception information	**Interception Warrants** under authority of the TIA Act, received by Telstra, authorising the *Organisation (*ASIO) to intercept telecommunications.
		Interception Warrants under authority of the TIA Act, received by Telstra, authorising *Agencies* to intercept telecommunications.
Stored communications not passing over Telstra's telecommunications network, held on equipment operated by, and in the possession of, Telstra that cannot be accessed on that equipment by a person who is not a party to the communication, without the assistance of Telstra along with some communications data embedded within said communications.	Historic communications and information	**Stored Communications Warrants** under authority of the TIA Act, received by Telstra, authorising access to communications.
		Telco Act Section 290 Allows for the use and disclosure of information or document or substance of a communication if in regard to all relevant circumstances, it might reasonably expected that the sender and the recipient of the communication would have consented to the disclosure if they had been made aware of it.