TELSTRA CORPORATION LIMITED

REVIEW OF THE SURVEILLANCE LEGISLATION AMENDMENT (IDENTIFY AND DISRUPT) BILL 2020

Public submission to the Parliamentary Joint Committee on Intelligence and Security

25 February 2021

01 Introduction

Telstra appreciates the opportunity to make a submission to the review of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (**the Bill**). We are a major builder and supplier of telecommunications networks and services, with a large customer base and a long history of providing lawful assistance to national security and law enforcement agencies. We recognise the need to ensure the tools available to law enforcement agencies remain relevant and appropriate in a rapidly changing social and technological environment but also understand this needs to be balanced against respecting the privacy and confidential information of our customers, their online activities and personal information.

The Bill introduces new law enforcement powers to enhance the ability of the Australian Federal Police (**AFP**) and the Australian Criminal Intelligence Commission (**ACIC**) to combat serious online crime:

- **Data disruption warrants** to enable the AFP and the ACIC to disrupt data by modifying, adding, copying or deleting in order to frustrate the commission of serious offences online.
- **Network activity warrants** to allow agencies to collect intelligence on serious criminal activity being conducted by criminal networks.
- **Account takeover warrants** to provide the AFP and the ACIC with the ability to take control of a person's online account for the purposes of gathering evidence to further a criminal investigation.[1]

These new warrants will expand the range of tools available to fight cybercrime, expanding warrants from collecting evidence to a tool that will facilitate the disruption of criminal activity online. The application of these new warrants will require balancing the use of these intrusive information gathering and disruption powers against the rights and privacy of consumers as well as the technical abilities of some carriers and ISPs. We strongly believe that it is appropriate that the issuing of these new warrants has judicial oversight, with data disruption warrants and network activity warrants requiring the approval of a judge, while the more intrusive account takeover warrants require the approval of a magistrate.

The new warrants represent a significant change to the existing carrier and ISP warrant processes and capabilities. Their introduction will require the development and building of new warrant management processes to enable carriers and ISPs to provide assistance in executing these warrants. We will work with the Government and AFP/ACIC to create a workable framework which strengthens the ability of these law enforcement agencies to serve the new warrants whilst ensuring any new process protects the privacy of third parties and our customers.

Our submission focusses on how the proposed new warrants can be practically implemented and on appropriate protections for those who are not the target of the warrants. In particular, we suggest the legislation should be amended to address:

- A mandatory consultative approach prior to issuing new warrants.
- A requirement to consider and protect the confidential information of non-targets.
- Immunity of organisations responding to warrants in good faith.
- The threshold for a warrant being elevated to serious offences.

[1] Explanatory memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, p. 1.

02 A mandatory consultative approach to implementation

Introducing these new warrant types and the capabilities required to execute them has potentially far reaching consequences for the operation of communications and computer networks. In many cases, especially initially, the capability to execute these warrants by carriers and ISPs may need to be developed. There is also potential for unintended consequences if warrants are not drafted carefully.

We accept that on occasions the need for the warrant might be so urgent that consultation could be seen as an unnecessary delay, particularly if the warrant using a known or previously used capability. However, it is important the warrants are issued in a form that can be executed and that don't have unintended consequences (such as exposing a third party's data). We suggest it would be appropriate to address such circumstances in guidelines on how the AFP and ACIC will interact with those parties whose assistance is required to execute the warrants.

2.1. Where new capability is required, the assistance and access regime should be used

In using these new powers, the AFP and the ACIC will need assistance from carriers and ISPs and potentially others, particularly where capability does not yet exist to meet the warrant requirements. In our view, the 'assistance and access' regime in Part 15 of the *Telecommunications Act 1997* provides what has proven to be a useful mechanism for the development of new capabilities. Part 15 provides a flexible, consultative approach to obtaining assistance and developing capabilities (via technical assistance requests (TARs)) which has proved successful in providing new types of assistance to law enforcement agencies in a co-operative and collaborative way. We believe the use of the TAR process to support the new warrants will allow carriers and ISPs to work with the AFP/ACIC to build capabilities that meet the AFP/ACIC's requirements while ensuring the capability is confined to the particular target of the warrant(s).

If the requested assistance cannot be agreed under Part 15, AFP/ACIC should use compulsory technical capability notices (TCNs) to require carriers and ISPs to develop the specified capacity. The TCN process is also consultative and has appeal mechanisms to ensure the capability is appropriately confined.

2.2. Service providers should be consulted before warrants are issued

Even if the capability exists, the specifics of the warrant could have consequences unknown to the AFP/ACIC when applying for, and to the judge or nominated AAT member when granting, the warrant. Accordingly, we suggest that the carrier or ISP who has been served the warrant should be consulted on the form and detail of the warrant before it is issued. This will allow the carrier or ISP to suggest any changes that might reasonably be necessary to support the implementation of the warrant and to ensure protection of third-party information and/or non-targets.

While this consultation could be seen as introducing an unnecessary delay in the process of issuing the warrant, we submit it is likely to provide for a more effective and timely execution of the warrant as it will assist in the warrant being issued in a form that can be executed by the carrier or ISP and is appropriately confined to the warrant's target(s).

2.3. There should be an avenue to appeal a warrant

For similar reasons to those set out in section 2.2, there should be a mechanism to appeal the content of a warrant on the grounds that execution is not technically feasible, reasonably practicable or

proportionate. Such a mechanism will be all the more important if consultation before issuing a warrant is not mandatory.

We submit that such an approach should be modelled on the appeal mechanism for TCNs in Part 15 of the *Telecommunications Act 1997*.

2.4. Guidelines outlining the proposed approach to engagement

We believe the new warrants represent a fundamental shift in the way AFP/ACIC will engage with carriers and ISPs in the execution of warrants. Accordingly, we suggest it would be appropriate for the Department of Home Affairs to issue guidelines outlining the way in which AFP/ACIC is to engage with carriers and ISPs to develop capabilities and issue warrants.

This would be similar to the approach taken when Part 15 was introduced.

03 Protections for 'non-targets'

The privacy of our customer's information, data and communications is very important to us and we invest considerable resources in the safeguarding of customers' account data and privacy more generally. We are concerned that in implementing the new warrants the privacy of customers, who are not the target of the warrants need to be protected.

We suggest there should be a requirement for the AFP/ACIC to consider the privacy of 'non-target' third party information and their communications when making an application for one of the new warrants. Similarly, there should be a requirement for the judge or nominated AAT member to be satisfied that issuing the warrant will not result in an undue risk that such an invasion of privacy would occur when accessing third party computers or communications in transit.

04 Immunity of organisations responding to warrants in good faith

We submit the Bill should be amended provide immunity for organisations complying or acting in response to one of the new warrant types in good faith. Such an immunity is provided to an organistation responding to a request for assistance under Part 15 of the *Telecommunications Act 1997*. This immunity has also been reflected in the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and provides entities responding to requests from law enforcement agencies with protection against civil liability when acting in good faith. The Bill should be amended so that a similar immunity is provided to entities responding to a data disruption warrant, network activity warrants and account takeover warrants, particularly given the intrusive nature of the warrants in scope of these reforms. This immunity should extent to both entities and their officers or employees acting in good faith in response to the warrant.

Further to this, proposed section 64B(3) states that it is an offence if a person is subject to an assistance order, is capable of complying with an order and omits to do an act, and will be subject to up to 10 years imprisonment. The Explanatory Memorandum sets out that section 64B ensures that should the AFP or the ACIC issue a data disruption warrant, they will be able to compel assistance in accessing devices, accessing and disrupting data, copying data, and converting documents. The intent of this provision is not to allow law enforcement to compel assistance from industry, but rather from a person with knowledge of a computer to assist in disrupting data (such as a person who uses the computer). However, it is unclear from section 64B or the EM whether a person acting on behalf of an entity subject to an assistance order could be held personally liable where it has knowledge of a computer. Without express immunity, it is unclear whether individual officers could be held personally liable under the Bill.

We submit that the Bill should clarify that individual officers could not be held liable for acting or omitting to act in response to an order.

05 Threshold for a warrant being elevated to a serious offence

We submit the threshold for which the new warrants can be used should be elevated to more accurately reflect the intention of the Bill to address heinous crimes such as child exploitation, terrorism, drug and arms trafficking. The threshold for the offence that a law enforcement officer may apply for the issue of a warrant should be raised so these provisions are only enlivened in the event of a serious offence. This change would be consistent with the intent of the proposed reforms and would also mitigate risks of misuse of the scope and intrusiveness of the warrants in scope under this Bill.