EXPLANATORY STATEMENT

Select Legislative Instrument 2013 No. 28

Issued by the Authority of the Attorney-General

Telecommunications (Interception and Access) Act 1979

Telecommunications (Interception and Access) Amendment Regulation 2013 (No. 1)

The *Telecommunications (Interception and Access) Act 1979* (Cth) ('the TIA Act') prohibits interception of communications passing over telecommunications networks.

There are exceptions to the prohibition of interception of communications under the TIA Act where law enforcement agencies obtain interception warrants for the investigation of defined *serious offences*, including offences relating to *criminal organisations.* Section 5 of the TIA Act further defines a *criminal organisation* as an organisation that is:

(a) a declared organisation within the meaning of:
  (i) the *Crimes (Criminal Organisations Control) Act 2009* of New South Wales; or
  (ii) the *Serious and Organised Crime (Control) Act 2008* of South Australia; or

(b) an organisation of a kind specified by or under, or described or mentioned in, a prescribed provision of a law of a State or Territory.

Section 300 of the TIA Act provides that the Governor-General may make regulations, not inconsistent with the Act, prescribing matters either required or permitted by this Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

Accordingly, sections 5 and 300 of the TIA Act enable the Governor-General to make Regulations prescribing the relevant provisions of a law of a State or Territory in the TIA Act's definition of *criminal organisation.*

This Regulation amends the *Telecommunications (Interception and Access) Regulations 1987* ('the Principal Regulations') to prescribe *declared organisations* within the meaning of section 7 of the *Serious Crime Control Act* (NT) ('the SCC Act') as *criminal organisations* within the definition of section 5 of the TIA Act.

The SCC Act provides that the Supreme Court of the Northern Territory may declare an organisation to be a *declared organisation* for the purposes of the SCC Act. The Court may make such a declaration where it is satisfied that the members of the organisation associate for the purposes of serious criminal activity and the organisation represents a risk to public safety and order. Once an organisation is

'declared,' the SCC Act provides a number of mechanisms to regulate and restrict the actions of its members.

The amended changes provide that intercepted telecommunications can be used during investigations into *declared organisations* under the SCC Act. The Regulation thus allows an interception agency, such as the Northern Territory Police, to apply for an interception warrant to assist with their investigations into breaches of control orders under the SCC Act. The amendments reflect government policy that telecommunications interception should be available to assist in the investigation of offences arising from the actions of organised criminal enterprise.

The Commonwealth Attorney-General's Department has consulted with the Northern Territory Attorney-General and Minister for Justice regarding the measures in the *Telecommunications (Interception and Access) Amendment Regulation 2013* and the provisions of the SCC Act.

The accompanying Regulation is a legislative instrument for the purposes of the *Legislative Instruments Act 2003*.

Financial Impact Statement

The *Telecommunications (Interception and Access) Amendment Regulation 2013 (No. 1)* will not have any direct financial impact on the Commonwealth. The costs associated with the use of telecommunications interception for investigations into breaches of control orders under the SCC Act will be borne by the Northern Territory.

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

This legislative instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Legislative Instrument

The Telecommunications (Interception and Access) Amendment Regulation 2013 (Cth) ('the Regulation') is made by the Governor-General under section 300 of the *Telecommunications (Interception and Access) Act 1979* (Cth) ('the TIA Act').

The Regulation amends the Telecommunications (Interception and Access) Regulations 1987 (Cth). The amendment under the Regulation provides that a '*declared organisation*' within the meaning of section 7 of the *Serious Crime Control Act* (NT) ('the SCC Act') is prescribed as a '*criminal organisation*' within the definition of section 5 of the TIA Act.

This amendment under the Regulation will enable an interception agency such as the Northern Territory Police to intercept telecommunications under an interception warrant to assist with investigations of offences under the SCC Act in relation to *declared organisations*.

Human Rights Implications

The legislative instrument engages the following human rights:

- arbitrary and unlawful interference with privacy – Article 17 of the International Covenant on Civil and Political Rights (ICCPR), and
- freedom of expression – Article 19 of the ICCPR

Unlawful or arbitrary interference with a person's privacy or correspondence

Article 17 of the ICCPR prohibits arbitrary or unlawful interference with a person's privacy, family, home or correspondence. Interferences with privacy may be permissible, provided that they are authorised by law and not arbitrary. In order for an interference with the right to privacy not to be 'arbitrary', the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' in this context to imply that 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.

Interceptions of telecommunications will limit the right to protection from arbitrary and unlawful interference with privacy in Article 17 of the ICCPR. This limitation is for a legitimate objective, namely protecting public order by ensuring that law enforcement agencies can effectively investigate serious crimes committed by members of criminal organisations under the SCC Act.

The Legislative Assembly of the Northern Territory enacted the SCC Act to strengthen the Northern Territory's anti-crime legislation regime in order to disrupt and restrict the actions of known criminal organisations. Where there is a relationship between an organisation and serious criminal activity, the SCC Act provides that the Commissioner of Police may apply to the Northern Territory Supreme Court to make a declaration that the organisation is a *declared organisation*. Upon this declaration, the Commissioner may then seek a '*control order*' from the Supreme Court against particular individual members of that organisation which restricts these particular individuals from associating with other members of the *declared organisation* or other persons who have engaged in serious criminal activity.

At the time of enacting the SCC Act, the Legislative Assembly recognised that the Northern Territory was home to local groups or chapters of criminal organisations which in turn belonged to larger interstate groups. Police intelligence noted that Northern Territory-based criminal organisations had been involved in drug trafficking and intimidation of trial witnesses and juries, while the interstate groups to which they belonged were suspected of a range of serious offences ranging from murder and serious assault to drug importation, money laundering and firearms offences. While the Legislative Assembly particularly noted the value of the SCC Act in dealing with outlaw motorcycle clubs, they noted that the SCC Act had the capacity to restrict the actions of other organised crime groups involved in serious criminal activity.

The TIA Act provides that telecommunications may be lawfully intercepted in order to detect, investigate and prosecute persons involved in serious offences, including offences carried out in furtherance of a criminal organisation. The ability for investigators to intercept the telecommunications of suspected members of criminal organisations is necessary because these communications, whether wholly within the Northern Territory or interstate, can provide evidence that these members are associating for the purposes of criminal activity. In particular, telecommunications between a person the subject of a *control order* under the SCC Act and another member of the *declared organisation* would provide strong evidence that the first person is in breach of their *control order*. In the absence of telecommunications interception, investigators may otherwise have to undertake direct physical surveillance of suspects, which is more intrusive, resource-intensive and poses a higher risk to personal safety. These measures support the goals of the SCC Act in disrupting the activities of criminal organisations and thus meet the legitimate aim of protecting public order.

This legislative instrument is therefore necessary to enable this highly effective investigative technique available for the investigation of criminal organisations in the Northern Territory under the SCC Act.

Therefore, the limitation on the right in Article 17 is made to address the pressing and substantial concern as to the capacity of the police to investigate organised crime under the SCC Act via telecommunications interception. This limitation is intended to achieve the legitimate objective of protecting public order.

The measures in the legislative instrument are also rationally connected to this legitimate objective of protecting public order via the investigation of serious crimes committed by a *declared organisation* under the SCC Act. In the circumstances dealt with under the SCC Act, members of a *declared organisation* may communicate via

the telecommunications network for the purposes of planning or involvement in criminal offences. Those members who have engaged in serious criminal activity may also continue to associate with other members via the telecommunications network after the Northern Territory Supreme Court has issued a *control order* prohibiting such associations. Lawfully intercepting the telecommunications of those suspected of criminal activity assists with gathering evidence of suspected criminality which may be used in subsequent criminal prosecutions. These investigations also have the capacity to discover further networks of criminality, and may also have the effect of exculpating ultimately innocent persons or excluding persons from an investigation.

Accordingly, officers will be able to more effectively investigate whether members of the *declared organisation* are associating for the purposes of a criminal enterprise using the techniques permitted by the legislative instrument. Use of these techniques in accordance with the law meets the legitimate aim of protecting public order.

To the extent that the measures in the legislative instrument may limit the right to protection from arbitrary and unlawful interference with privacy in Article 17 of the ICCPR, the limitation is proportionate to the legitimate objective.

The capacity to lawfully intercept telecommunications is of particular value to investigations involving criminal organisations, as correspondence between members of these organisations may provide evidence of criminal offences. The ability to investigate members of *declared organisations* under the SCC Act will be enhanced by the capacity to lawfully intercept these communications, and supports the legitimate aim of protecting public order and the safety of the Australian community.

The following safeguards on access to telecommunications within the TIA Act aim to ensure that any limitations on the right to privacy under the Regulation are reasonable and proportionate, and are not unlawful or arbitrary. Access to telecommunications for the investigation of offences under the SCC Act will be subject to the safeguards contained in the TIA Act. These safeguards ensure that the limitation on the right to privacy in Article 17 is minimised to the extent that the legitimate objective of public order may be achieved, and proportionate to the nature of the criminal conduct investigated:

- *Prohibition on unlawful access to telecommunications:* The TIA Act continues to advance privacy protections for users of the Australian telecommunications network by prohibiting unlawful access to the private telecommunications of its users.

- *Access to telecommunications content under a warrant:* The TIA Act establishes a process of authorisation under law for access to the private communications of users of the telecommunications system by requiring interception agencies to obtain a warrant from a nominated Judge or Administrative Appeals Tribunal Member ('issuing authorities') to access the content of these communications. The authorisation process requires issuing authorities to consider the need for access to this information on a case-by-case basis in accordance with a prescriptive legal framework.

  This framework provides that interception warrants may only be issued when likely to assist in connection with the investigation by a law enforcement agency of a serious offence. This framework also requires issuing authorities to consider

how much the privacy of any person or persons would be likely to be interfered with by the intercepting of communications in deciding whether to issue a warrant.

Telecommunications interception warrants are targeted towards the telecommunications services or identities of persons suspected of serious criminal offences. Issuing authorities may issue a warrant for a particular telecommunications service that a suspect is likely to use, or may issue a warrant which identifies the suspect and allows for interception of telecommunications services the suspect is likely to be using (which are known as 'named person warrants'). An issuing authority is only entitled to issue a named person warrant in circumstances where the issuing authority is either satisfied that there are no other practicable methods for the investigating agency to identify the telecommunications services used by the suspect, or are satisfied that it is not practicable to intercept the known telecommunications services of the suspect. These warrants are used less in comparison to telecommunications service warrants due to the higher potential impact on privacy that results in the use of a named person warrant. In exceptional circumstances, an issuing authority may issue an interception warrant for the telecommunications service of a third party where the suspect is likely to use that third party's telecommunications service. In a similar manner to named person warrants, an issuing authority is only entitled to issue a warrant for interception of the telecommunications of a third party in circumstances where the issuing authority is either satisfied that the investigating agency has exhausted all practicable methods of identifying the telecommunications services used by the suspect, or are satisfied that it is not possible to intercept any telecommunications services of the suspect.

The TIA Act further provides that issuing authorities must consider the extent to which methods of investigating the offence that do not involve accessing intercepted material have been used by or are available to the agency. The legislation underpinning the warrant process in the TIA Act has been subject to public scrutiny and debate in Parliament.

- *Oversight and accountability framework:* The TIA Act establishes an oversight and accountability framework for interception agencies' use of telecommunications interception powers. Interception agencies are obliged to keep records of the use of interception for inspection by oversight authorities under Part 2-7 of the TIA Act. In addition, interception agencies are required to give a detailed report to the Minister on the use of telecommunications interception for each reporting year under the reporting regime provided for in Part 2-8 of the TIA Act. These oversight and accountability regimes have been established to ensure that the investigation of serious offences via telecommunications interception is proportionate to the limitations on the right to privacy of those affected by the interception.

The right to freedom of expression

Article 19 of the ICCPR provides that all persons shall have the right to freedom of expression. This right includes the freedom to seek, receive and impart information and ideas of all kinds, through any media of a person's choice. Article 19(3) provides that such rights may be subject to restrictions for specified purposes provided in the right, including the protection of national security or public order where such restrictions are provided by law and are necessary.

Enabling interception agencies to intercept communications may indirectly limit the right to freedom of expression in that some persons may be more reluctant to use telecommunications services to seek, receive and impart information if they believe that their communications are being intercepted. To the extent that the measures in the legislative instrument have the effect of limiting the right to freedom of expression, the limitation is designed for the legitimate objective of protecting public order by enabling law enforcement agencies to investigate serious crimes committed by criminal organisations.

As raised above, the legislative instrument gives effect to the policy that telecommunications interception should be available to assist in the investigation of criminal organisations under the SCC Act. While the interception of telecommunications arising from the legislative instrument may have the indirect effect of limiting the right to freedom of expression contained in Article 19, the limitation is made for the legitimate objective of protecting public order.

Additionally, the limitation of the right to freedom of expression is rationally connected with the legitimate objective of investigating serious and organised criminal conduct. As discussed above, any indirect limitation on the right to freedom of expression resulting from the lawful interception of specific telecommunications is associated with the need to investigate organised crime through the interception of these communications in order to protect public order.

To the extent that the measures in the legislative instrument limit the right to freedom of expression, the limitation is proportionate to the legitimate objective. Investigations into criminal organisations require lawful access to the telecommunications of suspects for the investigations to be viable. Suspects' communications made over a telecommunications network may provide evidence of planning or conduct of a criminal enterprise. Intercepting the telecommunications of those suspected of committing offences under the SCC Act will allow investigators to discover and utilise evidence of serious criminality arising from communications over the telecommunications network.

As discussed in further detail regarding the right to privacy under Article 17 above, the TIA Act contains a number of safeguards aimed at ensuring that the telecommunications interception regime is compatible with Australia's human rights obligations. In that regard, these safeguards ensure that any need to lawfully intercept telecommunications is proportionate to the indirect limitation on the right to freedom of expression contained in Article 19. In summary, the safeguards contained in the TIA Act relevant to Article 19 include:

- A process of independent judicial authorisation for interception warrants by requiring interception agencies to obtain a warrant from a nominated Judge or Administrative Appeals Tribunal Member in order to have access to telecommunications.
- A limitation that interception warrants may only be issued when likely to assist in connection with the investigation by a law enforcement agency of a serious offence.
- Issuing authorities for law enforcement warrants must consider the extent to which methods of investigating the offence that do not involve accessing intercepted material have been used by or are available to the agency.
- That intercept warrants are targeted at the specific telecommunications services or identity of a suspect of a serious offence and, in exceptional circumstances where a warrant is required for the telecommunications services of a third party connected to the suspect, that the investigating agency must have exhausted all other possible avenues of locating the telecommunications services of the suspect.
- Interception of communications is subject to an oversight and accountability framework to ensure that investigations involving the interception of telecommunications are lawful and appropriate.

The interaction between the legislative instrument and the TIA Act provides that interception agencies will only be able to access a person's communication for the purpose of investigating offences under the SCC Act regarding members of deemed criminal organisations.

These safeguards on the use of telecommunications interception ensure that it is only used in circumstances where it is likely to assist in investigating persons suspected of serious offences, and is conducted upon very specific and targeted services or individuals after the issuing of a warrant by an issuing authority. This ensures that any indirect limitation on the right to freedom of expression in Article 19 is minimised where possible. Such a limitation is also proportionate to the serious nature of the organised crime being investigated under the SCC Act, and is made in furtherance of the legitimate aim of protecting public order and the safety of the Australian community.

Conclusion

The Regulation is compatible with human rights as to the extent that it limits any human rights, those impacts are reasonable, necessary and proportionate.

The Hon Mark Dreyfus QC MP
Attorney-General
Minister for Emergency Management