EXPLANATORY STATEMENT

Issued by the Minister for Home Affairs

Telecommunications (Interception and Access) Act 1979

Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021

The *Telecommunications (Interception and Access) Act 1979* (the Act) protects the privacy of, and regulates access to, the content of telecommunications and telecommunications data. It creates a legal framework for intelligence and law-enforcement agencies to access information held by communications providers for the investigation of criminal offences and other activities that threaten safety and security. The Act prohibits the interception of communications and access to stored communications, except in specified circumstances.

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

Section 7 of the Act prohibits the interception of communications, with some exceptions. Section 108 of the Act prohibits access to a stored communication, subject to exceptions. Relevantly, the exceptions in paragraphs 7(2)(a) and 108(2)(d) allow carriers to intercept or access communications in order to properly operate or maintain telecommunications systems.

The Act also requires that the acts or things done in connection with the operation or maintenance of the telecommunications system are 'reasonably necessary' for an employee of a carrier to perform their duties effectively. Subsection 7(2A) of the Act provides that, in determining whether an act or thing done by a person was reasonably necessary under paragraph 7(2)(a), a court is to have regard to such matters (if any) as are specified in, or ascertained in accordance with, the regulations. Similarly, subsection 108(4) of the Act provides that, in determining whether an act or thing done by a person was reasonably necessary under paragraph 108(2)(d), a court is to have regard to such matters (if any) as are specified in, or ascertained in accordance with, the regulations.

The *Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021* (the Regulations) amend the *Telecommunications (Interception and Access) Regulations 2017* to specify, for the purposes of paragraphs 7(2)(a) and 108(2)(d), the matters a court is to have regard to in determining whether an act or thing done by a person for the purposes of identifying and blocking malicious SMS messages was reasonably necessary in order for the person to perform their duties effectively.

Malicious actors are using a range of methods to send harmful text messages at scale, with innovative and ever-changing approaches to trick victims into compromising their devices and data. Scam SMS messages often impersonate well known businesses or government agencies - they 'phish' for personal information or contain links which when accessed install malware or ransomware in devices. The proliferation of scam SMS has undermined public confidence in communications from businesses and government. Government agencies and services such as Scamwatch now routinely advise the public to be cautious about any SMS and instruct the public not to click on links in any message. It is now almost impossible to identify whether a message is a scam or not especially when scammers can spoof telephone numbers or make them appear to be sent from a legitimate and trusted organisation.

This year SMS message and phone (voice based) scam reports and financial loss are double those reported to Scamwatch in 2020. In 190,000 of the 253,000 Scamwatch reports received this year, contact was made by phone or SMS and over $82 million has been lost. Many people are unaware of the impact of a malicious text message that may steal their personal information or result in financial loss at a later point in time. The volume of harmful text messages sent by malicious actors has had an adverse impact on the effective running of telecommunications systems. Not only does it impact the functioning of the system, it also undermines its integrity. The ability to treat or prevent these messages is therefore necessary to ensure the operation and maintenance of these systems. These amendments will help give industry assurance in using tools it can deploy to block malicious scams. When using these tools, industry will need to consider the Australian Privacy Principles including whether a privacy impact assessment would be necessary.

The Regulations commence on the day after they are registered on the Federal Register of Legislation.

A Statement of Compatibility with Human Rights (the Statement) has been completed in accordance with the *Human Rights (Parliamentary Scrutiny) Act 2011*. The overall assessment is that the Regulations are compatible with human rights. A copy of the Statement is at Attachment A.

Details of the Regulations are set out in Attachment B.

The Department of Home Affairs consulted with parts of the telecommunications industry and relevant Government departments and agencies. The consultations undertaken are consistent with the requirements of subsection 17(1) of the *Legislation Act 2003*.

The Office of Best Practice Regulation (the OBPR) has been consulted in relation to the amendments and has advised that a Regulation Impact Statement is not required. The OBPR reference is 01094.

The Act specifies no conditions that need to be satisfied before the power to make the Regulations may be exercised.

ATTACHMENT A

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

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

Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021

This Disallowable 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 Disallowable Legislative Instrument

The Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021 (Amendment Regulations) amends the *Telecommunications (Interception and Access) Regulations 2017* (the Regulations) to specify matters a court is to consider in determining whether activities undertaken by industry to identify and block malicious SMS messages is reasonably necessary for the operation or maintenance of a telecommunications system.

There are a range of methods being used by actors to send malicious SMS messages to target Australian individuals and businesses for the purposes of infecting the victim's device. This year SMS message and phone (voice based) scam reports and financial loss are double those reported to Scamwatch in 2020. In 190,000 of the 253,000 Scamwatch reports received this year, contact was made by phone or SMS and over $82 million has been lost. Many people are unaware of the impact of a malicious text message that may steal their personal information or result in financial loss at a later point in time.

The telecommunications industry has developed approaches to block these types of malicious SMS messages before they are received by the intended recipient. One such approach involves electronically scanning SMS content for URL addresses and matching them against trusted URL addresses associated with the SMS message sender. Where the URL addresses do not match, they will not be delivered. In order to verify the accuracy of the process, industry employees may need to sample SMS messages to ensure the process works as intended. This will involve recording communications passing over a telecommunication system, before they are received by the intended recipient. It may also involve reviewing SMS messages held on equipment operated by a carrier after it has been delivered.

There are existing exceptions to the prohibition on intercepting communications and accessing stored communications under the TIA Act that permit actions by carriers that are reasonably necessary in order for their employees to perform duties effectively in connection with the operation or maintenance of a telecommunications system.

The purpose of the Amendment Regulations is to specify matters that courts must have regard to in determining whether the activity is reasonably necessary in order for the person to perform his or her duties effectively.

Human rights implications

This Disallowable Legislative Instrument engages the following human rights under the International Covenant on Civil and Political Rights (ICCPR):

- protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR

- the right to freedom of expression contained in Article 19 of the ICCPR.

Protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR

Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks.

The protection against arbitrary or unlawful interference with the right to privacy under Article 17 of the ICCPR can be permissibly limited in order to achieve a legitimate objective and where the limitations are lawful and not arbitrary. The term 'unlawful' in Article 17 of the ICCPR means that no interference can take place except as authorised under domestic law. The term 'arbitrary' in Article 17(1) of the ICCPR means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' to mean that any limitation must be proportionate and necessary in the circumstances to achieve a legitimate objective.

The Amendment Regulations protect the privacy of the increasingly large number of individuals subject to malicious SMS messages by limiting their susceptibility to scams, which might involve unauthorised access to their private data or financial loss.

To the extent that carriers may intercept communications or access stored communications to achieve this outcome, the Amendment Regulations provide a framework to assist the courts in determining when threat blocking may be reasonably necessary for an employee of a carrier to perform their duties effectively, in connection with the operation or maintenance of a telecommunications system, as authorised under section 7(2) of the TIA Act. To that end, the Amendment Regulations may place limitations on the right to privacy. Those limitations however, are not arbitrary or unlawful. The Amendment Regulations are reasonable, necessary and proportionate to the objective of protecting the public from receiving malicious SMS messages which may involve unauthorised access to their private data or result in financial loss. The Amendment Regulations are limited in scope and directed only to

malicious activities which seek to exploit individuals and expose them to financial or other detriment.

Protection of the right to freedom of expression contained in Article 19 of the ICCPR

Article 19(2) of the ICCPR provides that everyone shall have the right to freedom of expression, including the right 'to seek, receive and impart information and ideas of all kinds and regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'.

Furthermore, Article 19(3) of the ICCPR provides that the exercise of the rights provided for in Article 19(2) carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary for the protection of national security or public order, or of public health or morals.

As the Amendment Regulations detail matters a court is to consider in determining whether acts or things were reasonably necessary for the person to perform their duties detail how industry can take action to prevent malicious spam SMS, the Amendment Regulations may have the effect of encouraging the use of telecommunications services for legitimate purposes. The Amendment Regulations may positively engage the right to freedom of expression by ensuring the general public can have greater confidence in the use of such telecommunications services for legitimate purposes.

The Amendment Regulations do not alter the existing exceptions to the prohibition on intercepting communications and accessing stored communications under the TIA Act, which include acts or things in the course of duties for operation or maintenance of a telecommunications systems.

To the extent that this may limit the right to freedom of expression by blocking the use of such technologies for illegitimate purposes, being scam messages to exploit people and expose them to financial or other detriment, this is a legitimate limitation of this right. The Amendment Regulations are appropriately targeted to ensure any limitation of this right is reasonable, necessary and proportionate.

Conclusion

The Disallowable Legislative Instrument is compatible with human rights because it promotes the protection of human rights and, to the extent that it limits human rights, those limitations are reasonable, necessary and proportionate.

The Hon Karen Andrews MP

Minister for Home Affairs

ATTACHMENT B

Details of the *Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021*

Section 1 – Name

This section provides that the name of the instrument is the *Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021* (the Regulations).

Section 2 – Commencement

This section provides for the commencement of the instrument.

Subsection 2(1) provides that each provision of the Regulations specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table.

The effect of the table is that the Regulations commence on the day after the Regulations are registered on the Federal Register of Legislation.

Section 3 – Authority

This section provides that the instrument is made under the *Telecommunications (Interception and Access) Act 1979.*

Section 4 – Schedules

This section provides for how the amendments in the Regulations operate.

Schedule 1 – Amendments

Telecommunications (Interception and Access) Regulations 2017

Item [1] – At the end of Part 2

This item adds section 10A to the *Telecommunications (Interception and Access) Regulations 2017*.

Subsections 10A(1) and 10A(2) provides that for the purposes of subsections 7(2A) and 108(4) of the Act respectively, the matters in subsection 10A(3) are specified for the purposes of determining whether an act or thing done by a person for the purposes of identifying and blocking malicious SMS messages was reasonably necessary in order for the person to perform their duties mentioned in paragraphs 7(2)(a) and 108(2)(d) of the Act effectively.

The exceptions to the prohibitions on intercepting communications or accessing stored communications in paragraphs 7(2)(a) and 108(2)(d) allow carriers to intercept communications or access stored communications where reasonably necessary for an employee of a carrier to do an act or thing to operate and maintain telecommunications systems to perform their duties effectively. Subsection 7(2A) and 108(4) of the Act provide that, in determining whether an act or thing done by a person was reasonably necessary under

paragraphs 7(2)(a) or 108(2)(d), a court is to have regard to such matters (if any) as are specified in, or ascertained in accordance with, the regulations.

Subsection 10A(3) specifies matters for subsections 10A(1) and 10A(2). The matters are:

- the impacts of malicious SMS messages, and actions taken by users of telecommunications systems in response to those messages, on the operation and maintenance of telecommunications systems;

- the extent to which the act or thing assist in identifying and blocking malicious SMS messages;

- community expectations that malicious SMS messages should be identified and blocked;

- the financial or psychological harm caused, or likely to be caused, by malicious SMS messages;

- the extent to which the act or thing is done in a way that minimises any impacts on users of telecommunications systems, including any impacts on the privacy of users.

The effect of the amendment is that a court is to consider these matters for the purposes of determining whether an act or thing done by a person for the purposes of identifying and blocking malicious SMS messages was reasonably necessary in order for the person to perform the person's duties mentioned in paragraphs 7(2)(a) and 108(2)(d) of the Act effectively.

The amendment highlights matters that are considered to be significant in determining whether such action is or is not reasonably necessary.

First, a court is to have regard to the impact of malicious SMS messages, and actions taken by the users of the telecommunications system in response to those messages, on the operation and maintenance of telecommunications systems. For example, the definition of telecommunications system includes equipment, a line or other facility that is connected to such a network and is within Australia, and includes a telecommunications device. A court should give weight to the adverse impact of malicious SMS messages, on the integrity or effective operation or maintenance of telecommunications systems and devices, when determining whether preventative action to block those messages is reasonably necessary.

Second, a court is to have regard to the extent to which the act or thing assists in identifying and blocking malicious SMS messages. For example, a court should give weight to evidence that acts taken by employees which enable the identification and blocking of malicious SMS messages as supporting a conclusion that the act was reasonably necessary.

Third, a court is to have regard to the community expectations that malicious SMS messages should be identified and blocked. For example, the community may expect that a carrier take steps to protect the network used by the community from content that may cause harm to the community, so long as that action does not unjustifiably intrude on privacy of SMS messages that are not malicious.

Fourth, a court is to have regard to the financial or psychological harm caused, or likely to be caused, by malicious SMS messages. For example, if a person receives a malicious SMS message with a link in it and clicks on that link, it may cause malicious software to be downloaded onto the person's device. This in turn could lead to another person being able to use that software to transfer money from the first person, or for the other person to require the first person to pay them a 'ransom' before the malicious software is removed. In addition to financial harm, exposure to malicious SMS may also result in psychological harm to a person, such as emotional stress from having their identity stolen or due to the loss of access to their accounts or data. This malicious software could also impact the operation of the carrier's network. A court should give weight to the fact that acts to block such malicious SMS messages and prevent financial or psychological harm to individuals, and also protection the operation of networks, in determining whether the acts are reasonably necessary.

Lastly, a court is to have regard to the extent to which the act or thing is done in a way that minimises any impacts on users of telecommunications systems, including any impact on the privacy of users of telecommunications systems. For example, if the act or thing done by the employee is designed in a way that limits any interference with the privacy of the recipient, such as through minimising any access to private SMS messages to the extent absolutely necessary to allow blocking software to operate effectively, then that activity would be more likely to be reasonably necessary.

Subsection 10A(4) confirms that a court may have regard to matters that are not specified in subsection 10A(3). This makes clear the list in subsection 10A(3) is not exhaustive of the matters a court may consider. For example, a court may consider other matters such as how the malicious SMS messages came to the attention of industry, or any advice from regulators that indicates SMS messages from particular sources or which contain particular identifiers are likely to be malicious SMS messages.

Subsection 10A(5) provides a definition of an SMS message. The definition clarifies that an SMS message includes an MMS message (multimedia message service).

Subsection 10A(6) provides a definition of malicious SMS message for the purposes of section 10A. It provides that an SMS message is a malicious SMS message if:

- the SMS message contains a link or telephone number; and
- the purpose, or apparent purpose, of the SMS message is to mislead or deceive a recipient of the SMS message into using the link or telephone number; and
- the recipient would be likely to suffer detriment as a result of using the link or telephone number.

This is intended to cover SMS messages containing links to malware or ransomware. This occurs when a person receives a malicious SMS message with a link in it and clicks on that link, causing malicious software to be downloaded onto the person's device. This in turn could lead to another person being able to use that software to transfer money from the first person, or for the other person to require the first person to pay them a 'ransom' before the malicious software is removed.

This is also intended to cover SMS messages that mislead the recipient into calling a telephone number, which could be spoofed, and result in financial or other harm. For

example, malicious SMS messages may impersonate a government agency which requests the recipient to call a spoofed phone number which leads to a scam.

The inclusion of ‘apparent purpose’ in subsection 10A(6)(b) recognises that it may not be possible to determine the actual purpose of the sender of the SMS message. The intention of ‘apparent purpose’ is to capture SMS messages that are, or are likely to, have the effect of misleading or deceiving the recipient into using the link or telephone number.