Chapter 1[1]

New and continuing matters

1.1 This chapter provides assessments of the human rights compatibility of:

- bills introduced into the Parliament between 24 February and 5 March 2020;
- legislative instruments registered on the Federal Register of Legislation between 6 February and 4 March 2020.[2]

1 This section can be cited as Parliamentary Joint Committee on Human Rights, New and continuing matters, *Report 4 of 2020*; [2020] AUPJCHR 43.

2 The committee examines all legislative instruments registered in the relevant period, as listed on the Federal Register of Legislation. To identify all of the legislative instruments scrutinised by the committee during this period, select 'legislative instruments' as the relevant type of legislation, select the event as 'assent/making', and input the relevant registration date range in the Federal Register of Legislation's advanced search function, available at: https://www.legislation.gov.au/AdvancedSearch.

Response required

1.2 The committee seeks a response from the relevant minister with respect to the following bill and legislative instruments.

Census and Statistics Amendment (Statistical Information) Regulations 2020 [F2020L00109][1]

Purpose	This instrument amends the Census and Statistics Regulation 2016 to update the list of topics in relation to which the Statistician shall collect statistical information
Portfolio	Treasury
Authorising legislation	*Census and Statistics Act 1905*
Last day to disallow	15 sitting days after tabling (tabled in the House of Representatives on 11 February 2020 and in the Senate on 12 February 2020. Notice of motion to disallow must be given by 12 May 2020 in the House of Representatives and by 17 June 2020 in the Senate[2]
Right	Privacy
Status	Seeking additional information

Collection of personal information

1.3 Schedule 1 of the regulations updates the list of statistical information to be collected by the Census in the *Census and Statistics Regulation 2016*, to insert topics relating to 'health conditions as diagnosed by a doctor or a nurse' and service in the Australian Defence Force (ADF). It also removes a topic relating to access to the internet at the dwelling.

Preliminary international human rights legal advice

Right to privacy

1.4 Requiring the statistician to collect personal information about respondents' diagnosed health conditions engages the right to privacy.[3] The right to privacy

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Census and Statistics Amendment (Statistical Information) Regulations 2020, Report 4 of 2020; [2020] AUPJCHR 44.

2 In the event of any change to the Senate or House's sitting days, the last day for the notice would change accordingly.

3 International Covenant on Civil and Political Rights (ICCPR), article 17.

encompasses respect for informational privacy, including the right to respect for private information and private life, particularly in relation to the storing, use, and sharing of personal information.[4] The right may be subject to permissible limitations which are prescribed by law and are not arbitrary. In order for a limitation not to be arbitrary, it must pursue a legitimate objective, be rationally connected to that objective, and be a proportionate means of achieving that objective.[5]

1.5 The statement of compatibility acknowledges that the regulations engage the right to privacy, but states that any limitation on privacy is in pursuit of a legitimate objective, because 'all levels of government in Australia need information about Australia's population to inform their decisions and policy making'.[6] The statement of compatibility further explains that due to Australia's aging population health services in many states are coming under pressure, and that while extensive information is collected at the national and broad state and territory levels, there is currently no information available to policy-makers on the prevalence of diagnosed health conditions for small population groups, and at small geographical areas'.[7] The collection of statistical data for the adequate provision of health services is likely to be considered to be a legitimate objective for the purposes of international human rights law.

1.6 The statement of compatibility also states that there is a rational connection between the regulations and the legitimate objective, as 'if the Government did not have access to the information collected on Census night, it would be unable to make informed decisions that balance Australia's future needs and ensure our scarce resources are appropriately allocated'.[8] However, in assessing if a measure is rationally connected to its stated objectives it is necessary to consider whether the relevant measure is likely to be effective in achieving the objectives being sought. As a result of these regulations the census will now collect statistical information on the number of 'health conditions diagnosed by a doctor or a nurse'. This appears to be broad in scope, as acknowledged in the statement of compatibility, which states that 'respondents only need to identify whether they have diagnosed health conditions and they do not need to provide any specifics about their medical condition or

4 See, UN Human Rights Committee, *General Comment No. 16: Article 17* (1988) [10]; and *General Comment No. 34 (Freedom of opinion and expression)* (2011) [18].

5 See, for example, *Leyla Sahin v Turkey,* European Court of Human Rights (Grand Chamber) Application No. 44774/98 (2005); *Al-Adsani v United Kingdom*, European Court of Human Rights (Grand Chamber) Application No. 35763/97 (2001) [53] - [55]; *Manoussakis and Others v Greece*, European Court of Human Rights, Application No. 18748/91 (1996) [36] - [53]. See also the reasoning applied by the High Court of Australia with respect to the proportionality test in *Lange v Australian Broadcasting Corporation* [1997] HCA 25.

6 Statement of compatibility, p. 3.

7 Statement of compatibility, pp. 3-4.

8 Statement of compatibility, p. 4.

treatment'.[9] However, without any details of what the medical conditions are, it is not clear how having such information will assist with government planning for the provision of services, when the nature of the service provision required is unknown.

1.7 In relation to the proportionality of the measure, the statement of compatibility argues that the limitation on the right to privacy is reasonable, necessary and sufficiently precise, and that 'the Regulations do not impose obligations on persons to provide personal information'.[10] However, section 14 of the *Census and Statistics Act 1905* (Census Act) makes it a criminal offence[11] for a person not to fill in their census form, or answer the questions on the form. This offence is subject to strict liability, meaning there is no need for the prosecution to prove fault. Therefore, as a result of these regulations, respondents will be obligated to disclose if they have a diagnosed medical condition, and it will be a criminal offence to refuse to answer. Whether the limitation on the right to privacy can be justified as being proportionate to the objective being sought is thus unclear.

1.8 The statement of compatibility also states there are safeguards to ensure personal information is appropriately safeguarded, used and handled, noting that section 19 of the Census Act makes it an offence for officers to disclose census information to third parties. However, no information is provided as to whether the information is securely held and how long identifiable information is retained.

1.9 Therefore, more information is required in order to assess the compatibility of this measure with the right to privacy, in particular:

- how collecting information as to people's diagnosed medical conditions can assist with government planning for the provision of services (noting that the nature of the medical condition is unknown and could capture a range of conditions, including those that require no provision of services);
- whether the measure is sufficiently circumscribed; in particular why it is appropriate that a person who does not disclose a diagnosed health condition would be subject to a criminal penalty; and
- what other safeguards would protect the privacy of personal information which respondents would be compelled to provide, including whether the information is securely held and how long identifiable information is retained.

Committee view

1.10 The committee notes that these regulations will require all Australians on census night to disclose if they have a diagnosed health condition. The committee

9 Statement of compatibility, p. 4.

10 Statement of compatibility, p. 4.

11 Subject to one penalty unit, currently $210 (*Crimes Act 1914*, section 4AA).

notes the legal advice that the measures engage and limit the right to privacy. In order to assess the compatibility of this measure with the right to privacy, the committee seeks the Assistant Treasurer's advice as to the matters set out at paragraph [1.9].

Defence Amendment (2020 Measures No. 1) Regulations 2020 [F2020L00120][1]

Purpose	This instrument sets out the circumstances when written notice is not required before a decision is made to terminate an Australian Defence Force member's service
Portfolio	Veterans Affairs
Authorising legislation	Defence Act 1903
Last day to disallow	15 sitting days after tabling (tabled in the House of Representatives 13 February 2020 and in the Senate on 24 February 2020). Notice of motion to disallow must be given by 14 May 2020 in the House of Representatives and 11 August 2020 in the Senate[2]
Right	Work
Status	Seeking additional information

Terminating without notice the service of an Australian Defence Force member

1.11 These regulations amend section 24 of the Defence Regulation 2016 to establish two new grounds on which the employment of a member of the Australian Defence Force (ADF) may be terminated without written notice. These grounds are where the member has been imprisoned for an offence; or where they have pleaded guilty to, or been convicted of, an offence and the Chief of the Defence Force is satisfied that it is not in the interests of the defence force for notice to be given to them.[3]

1.12 The regulations also remake what currently exists in section 24, to provide that a member's employment may be terminated without written notice where: the appointment or enlistment is subject to a probationary period; they have failed to

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Defence Amendment (2020 Measures No. 1) Regulations 2020 [F2020L00120], *Report 4 of 2020*; [2020] AUPJCHR 45.

2 In the event of any change to the Senate or House's sitting days, the last day for the notice would change accordingly.

3 Schedule 1, Item 5, subsection 24(3). The reasons for something being or not being in the interests of the defence force are set out at subsection 6(2) of the regulations, and expanded by this instrument to include a member's failure to meet one or more conditions of the member's enlistment, appointment or promotion. See, Schedule 1, Item 1, subsection 6(2)(c).

meet a condition of their appointment or enlistment; or they have been absent without leave for a continuous period of three months or more.

Preliminary international human rights legal advice

Right to work

1.13 Providing that an ADF member's employment may be terminated without notice to them, for reasons related to their conduct or performance, engages and may limit the right to work. The right to work includes a right not to be unfairly deprived of work.[4] A person's employment must not be terminated for reasons related to their conduct or performance before they are provided an opportunity to defend themselves against the allegations made, unless the employer cannot reasonably be expected to provide this opportunity.[5] Any decision to terminate employment should be 'preceded by dialogue and reflection between the parties'.[6]

1.14 The right to work may be limited, provided limitations are prescribed by law, pursue a legitimate objective, are rationally connected to (that is, effective to achieve) that objective, and are a proportionate means of achieving that objective.[7]

1.15 The statement of compatibility recognises that the regulations could be seen as limiting the right to work, however, it states that any limitation is reasonable, necessary and proportionate in pursuit of a legitimate objective. It notes that service in the ADF differs from civilian employment in that ADF members face combat, and must follow all lawful commands, making discipline and a system of command essential.[8] It also states that an ADF member who fails to attend duty may be charged with an offence and liable to imprisonment, and states that section 24 enhances the rights of ADF members at work by providing specific grounds for termination, and a process which must be followed before deciding to terminate a person's service.[9]

1.16 The statement of compatibility gives a detailed explanation as to why the two new bases on which employment can be terminated without notice are

4 See, International Covenant on Economic, Social and Cultural Rights, articles 6-7.

5 International Labour Organization (ILO) Convention 158 , article 7 and ILO, *Protection against Unjustified Dismissal*, [146].

6 ILO, *Protection against Unjustified Dismissal*, [148].

7 See, for example, *Leyla Sahin v Turkey,* European Court of Human Rights (Grand Chamber) Application No. 44774/98 (2005); *Al-Adsani v United Kingdom*, European Court of Human Rights (Grand Chamber) Application No. 35763/97 (2001) [53] - [55]; *Manoussakis and Others v Greece*, European Court of Human Rights, Application No. 18748/91 (1996) [36] - [53]. See also the reasoning applied by the High Court of Australia with respect to the proportionality test in *Lange v Australian Broadcasting Corporation* [1997] HCA 25.

8 Statement of compatibility, p. 5.

9 Statement of compatibility, p. 5.

reasonable and necessary. However, the regulations also remake the existing bases on which employment can be terminated without notice. As such, it is necessary to examine the entirety of these regulations and any limitation on the right to work.

1.17 It is unclear whether terminating a member's employment without notice where they have failed to meet a condition of their appointment or enlistment, or where they have been absent without leave for three months or longer is a permissible limitation. In particular, it is noted that the ability to terminate without notice could apply for a failure to meet *any* condition of a member's employment. It is unclear why a member should not be notified of a decision to terminate their employment in such circumstances.

1.18 In order to assess the compatibility of the entirety of the measure with the right to work, further information is required as to:

- whether terminating the employment of an ADF member for failure to meet a condition of their employment or enlistment, or being absent without leave, without notifying them of the decision, is compatible with the right to work; and
- in the absence of notification, what opportunities ADF members would have to respond to allegations related to a failure to meet a condition of their employment or service, or to an absence without leave, prior to their employment being terminated.

Committee view

1.19 The committee notes that the regulations sets out the circumstances in which written notice is not required before a decision is made to terminate an Australian Defence Force member's service. The committee notes the legal advice that the measure engages and may limit the right to work. In order to assess compatibility with the right to work the committee seeks the minister's advice as to the matters set out at paragraph [1.18].

Telecommunications Legislation Amendment (International Production Orders) Bill 2020[1]

Purpose	The bill seeks to amend the *Telecommunications (Interception and Access) Act 1979* to establish a new framework for international production orders to provide Australian agencies access to overseas communications data for law enforcement and national security purposes
Portfolio	Home Affairs
Introduced	House of Representatives, 5 March 2020
Right[s]	Life; prohibition against torture, cruel, inhuman or degrading treatment or punishment; privacy; and effective remedy
Status	Seeking additional information

International Production Orders to access personal telecommunications data

1.20 The bill seeks to provide the legislative framework for Australia to give effect to future bilateral and multilateral agreements for cross-border access to electronic information and communications data.[2] To do so, the bill seeks to introduce International Production Orders (IPOs). Such orders would allow Commonwealth, state and territory law enforcement and national security agencies to acquire data held in a foreign country by a designated communications provider, and to allow foreign governments to access private communications data.[3]

1.21 Proposed new Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* (Interception Act) sets out the scheme, and proposes the introduction of three new types of IPOs, relating to:

- the interception of telecommunications data for up to 90 days;
- accessing stored communications and telecommunication data (for example, stored messages, voice mails, video calls); and
- telecommunications data (being information about the communication, but not including the substance of the communication).

1.22 IPOs can be issued for three different purposes:

1 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Telecommunications Legislation Amendment (International Production Orders) Bill 2020, *Report 4 of 2020*; [2020] AUPJCHR 46.

2 Explanatory memorandum, p. 1.

3 Statement of compatibility, [3] and [8].

- to enforce a number of serious offences or offences punishable by imprisonment of at least seven years (for intercepted material) or three years (for stored communications data and telecommunications data); [4]
- in connection with the monitoring of a person subject to a control order; [5] and
- in connection with the carrying out of the Australian Security and Intelligence Organisation's (ASIO) functions.[6]

1.23 IPOs to enforce the criminal law or monitor a person subject to a control order can be issued by a judge (or in some cases a magistrate) or a nominated member of the AAT. IPOs that relate to the carrying out of ASIO's functions can be issued by a nominated AAT Security Division member.

1.24 It would appear that once an IPO is granted, foreign communications providers, subject to there being an agreement between Australia and that country, would then be able to provide Australian law enforcement agencies and ASIO with access to private communications data.[7]

Preliminary international human rights legal advice

Right to privacy

1.25 The interception and disclosure of personal telecommunications data which reveals a person's conversations and messages engages and limits the right to privacy. The right to privacy includes respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information.[8] It also includes the right to control the dissemination of information about one's private life. The right to privacy may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1.26 The statement of compatibility acknowledges that the bill limits the right to privacy. It states that the objective of the bill is to protect national security, public

4 See Schedule 1, item 43, proposed new Schedule 1, Part 2.

5 See Schedule 1, item 43, proposed new Schedule 1, Part 3.

6 See Schedule 1, item 43, proposed new Schedule 1, Part 4.

7 Statement of compatibility, [8].

8 International Covenant on Civil and Political Rights, article 17. Every person should be able to ascertain which public authorities or private individuals or bodies control or may control their files and, if such files contain incorrect personal data or have been processed contrary to legal provisions, every person should be able to request rectification or elimination. UN Human Rights Committee, *General Comment No. 16: Article 17* (1988) [10]. See also, *General Comment No. 34 (Freedom of opinion and expression)* (2011), [18].

safety, address crime and terrorism and protect the rights and freedoms of individuals by providing law enforcement and national security agencies with the tools they need to keep Australia safe. Such objectives would appear to constitute legitimate objectives for the purposes of international human rights law, and the measure appears to be rationally connected to this objective.

1.27 The question is whether the measures in the bill are proportionate to achieving the stated objective, in particular whether the measures are sufficiently circumscribed and whether there are sufficient safeguards in place.

1.28 The statement of compatibility details a number of safeguards that exist in the bill that must be considered before an IPO can be granted (depending on the purpose for which the IPO is granted). These include requiring the judge or AAT member to consider:

- how much the privacy of any person would be likely to be interfered with by issuing the order;
- the gravity of the conduct being investigated;
- how much the information to be gathered would be likely to assist with the investigation; and
- to what extent methods of investigation that do not involve accessing such data exist, and how much these would be likely to assist, or prejudice, the investigation.

1.29 Further, where an interception IPO would allow an innocent third party's communications to be intercepted (for example, third party phone calls are intercepted because it is thought that the suspect will be in touch with that person), the bill additionally provides that the order will be for 45 days or three months (instead of 90 days or six months) and the judge or AAT member must not issue the IPO unless satisfied that:

- the interception agency has exhausted all other practicable methods of identifying the carriage services used, or likely to be used, by the suspect; and
- interception of the suspect's communications would not otherwise be possible. [9]

1.30 In addition, where Victorian and Queensland law enforcement agencies make an application for an IPO, the Public Interest Monitors that exist in those states can appear at hearings of IPO applications to test the content and sufficiency of the information relied on, can question any person giving information, and can make submissions as to the appropriateness of granting the application, which must be considered by the judge or AAT member when deciding whether to grant an IPO.

9 See Schedule 1, item 43, proposed new subsections 30(6), 60(7) and (8), 89(6) and (7).

1.31 The statement of compatibility therefore states that in light of these statutory safeguards to ensure the decision maker evaluates the individual circumstances of each application before issuing an IPO, any limitation on the right to privacy is reasonable, necessary and proportionate. These are important safeguards and assist when evaluating the proportionality of the IPOs. However, there are a number of questions as to whether these safeguards are sufficient in all circumstances.

Public Interest Monitors

1.32 As set out in the statement of compatibility, Public Interest Monitors strengthen the protections in the bill against arbitrary and unlawful interference with privacy.[10] As the suspect is not able to be personally represented at the application for the IPO, having an independent expert to appear at the hearing to test the content and sufficiency of the information relied on, to question any person giving information, and to make submissions as to the appropriateness of granting the application, is an important safeguard to protect the rights of the affected person. As the European Court of Human Rights has held:

> the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his rights.[11]

1.33 However, the bill only applies this important safeguard when the law enforcement agency making the request is located in Victoria or Queensland. The statement of compatibility provides that 'there is scope to accommodate similar oversight bodies in the framework, should they be established in other jurisdictions in the future'.[12] However, there is nothing in the legislation to this effect, and as currently drafted, the majority of jurisdictions in Australia would have no such protection. It is not clear why this bill could not itself establish Public Interest Monitors that apply to jurisdictions that do not otherwise have them, and if Public Interest Monitors are established in these jurisdictions, to ensure these bodies will automatically be able to appear at hearings of IPO applications.

1.34 In addition, the bill provides that these Monitors only operate in relation to the 'interception' of telecommunications. There is no role for them when an application is made for an IPO for stored communications data or

10 Statement of compatibility, [30].

11 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015), [233].

12 Statement of compatibility, [30].

telecommunications data. Stored communications data would enable agencies to access all existing messages, including text messages and recordings of voice and video messages. It is unclear that the impact on privacy for intercepting telecommunications for a time limited period is that much greater than accessing all stored data in relation to an individual, given the breadth of the data that may be stored. It is therefore unclear why the safeguard of the Public Interest Monitor does not also apply to an application for an IPO to access stored telecommunications data.

Issuing authority

1.35 The bill provides that applications for an IPO in relation to enforcing the criminal law and monitoring a control order are to be made to a judge (or in some cases a magistrate) who has consented to be appointed as an issuing authority, or an AAT member of any level, who has been enrolled as a legal practitioner for at least five years.[13] In relation to applications for an IPO in connection with carrying out ASIO's functions, the application is to be made to a member, of any level, of the Security Division, of the AAT who has been enrolled as a legal practitioner for at least five years.[14]

1.36 However, it is not clear why it is appropriate to enable non-judicial officers, such as a member of the AAT, of any level and with potentially only five years experience as an enrolled legal practitioner, to issue orders that significantly limit the right to privacy. As the European Court of Human Rights has said in relation to interception:

> In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.[15]

Additional safeguards

1.37 The bill currently provides an additional safeguard before an interception IPO can be issued, namely that the judge or AAT member must have regard to whether intercepting communications 'would be the method that is likely to have the least

13 Schedule 1, item 43, proposed new section 16.

14 Schedule 1, item 43, proposed new section 16.

15 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015), [233]. See also *Klass and Others v Germany*, European Court of Human Rights, application no. 5029/71), (6 September 1978) [55]: 'The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure'.

interference with any person's privacy'.[16] This is in addition to considering how much the privacy of any person would be likely to be interfered with. This is an important safeguard to help prevent the arbitrary interference with the right to privacy. However, it only applies to interception IPOs in relation to control orders, and not in relation to the enforcement of the criminal law or in connection with ASIO's activities. Nor does it apply to IPOs in relation to accessing stored communications data or telecommunications data. The statement of compatibility states that this additional protection was considered appropriate noting that the IPO can be issued in connection with the monitoring of a person subject to a control order rather than in connection with the investigation into a specific offence.[17] While it is welcome that this additional protection has been included for this one category of IPOs, it is unclear why such a protection could not apply to all IPOs, to ensure that the decision maker turns their mind to considering whether issuing the IPO would be likely to have the least interference with a person's privacy.

1.38 In addition, the bill provides that an IPO to investigate serious crimes and in connection with ASIO's activities can be issued if to do so would be 'likely to assist' the investigation.[18] However, IPOs in connection with monitoring a person subject to a control order require that the IPO would be likely to 'substantially assist' the investigation.[19] Given the impact on a person's privacy by intercepting and accessing their communications, it is not clear why all IPOs are not restricted to those that will 'substantially' assist in an investigation.

Duration of interception IPO

1.39 The bill provides that an IPO to allow for interception in relation to enforcing the criminal law and monitoring a control order cannot be longer than 90 days in most cases, and 45 days when an innocent third party's communications are intercepted.[20] In relation to IPOs in connection with carrying out ASIO's functions, the order cannot be longer than six months in most cases, and three months where an innocent third party's communications are intercepted.[21] The explanatory materials do not explain why these time periods have been chosen or why interception IPOs in connection with carrying out ASIO's functions are twice as long as other IPOs. The statement of compatibility only states that the period for intercepting innocent third parties is half that of other IPOs, given such interception

16 Schedule 1, item 43, proposed new paragraph 60(5)(f).

17 Schedule 1, item 43, proposed new paragraph 60(5)(f).

18 Schedule 1, item 43, proposed new paragraphs 30(2)(g) and (h), 39(2)(d), 48(2)(d), 89(2)(g) and (h), 98(2)(e).

19 Schedule 1, item 43, proposed new paragraph 60(2)(i) and (j), 69(2)(e) and 78(2)(e)

20 Schedule 1, item 43, proposed subsections 30(4) and 60(4)

21 Schedule 1, item 43, proposed subsection 89(4).

'inherently involves a potential for privacy intrusion of persons who may not be involved in the commission of an offence'.[22] However, it does not explain how this time period is an appropriate time period in all of the circumstances. It is also noted that further interception IPOs may be made, so long as it begins after the other IPO has ended.[23]

1.40 In addition, there does not appear to be anything in the bill to ensure that if the circumstances that lead to the issuing of the IPO have changed, such that the IPO is no longer warranted, that the IPO ceases to have effect. International case law provides that legislation authorising surveillance warrants should set out the circumstances in which it must be cancelled when no longer necessary, and that without this, the law will not contain sufficient guarantees against arbitrary interference with the right to privacy.[24]

Control orders

1.41 The bill provides that IPOs can be issued in order to monitor persons subject to a control order so as to protect the public from a terrorist act, prevent support for terrorist and hostile act overseas and determine whether the control order has been, or is being, complied with. The control order regime itself engages and limits multiple human rights.[25] It is noted that it is already an offence for a person to fail to comply with the conditions of a control order,[26] which is subject to imprisonment of up to five years. As such, it is unclear why it is necessary to enable an IPO to be made simply to determine if the order is being complied with, rather than relying on the IPOs to investigate breaches of the criminal law. It is also noteworthy that unlike IPOs for investigating serious crime, there is no requirement for the judge or AAT member to consider the gravity of the conduct being investigated. It is unclear why it is necessary to enable IPOs to be granted to determine whether a control order is being complied with rather than relying on the other powers to investigate breaches of serious crimes and why the control order IPOs do not require the judge or AAT member to consider the gravity of the conduct being investigated.

National security

1.42 IPOs may be issued in connection with carrying out ASIO's functions. In particular, an IPO to intercept communications or to access stored telecommunications data can be issued if there are reasonable grounds to suspect

22 Statement of compatibility, [38].

23 Schedule 1, item 43, proposed sections 32, 62 and 91.

24 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015), [250]-[252].

25 See Parliamentary Joint Committee on Human Rights, *Report 10 of 2018* (18 September 2019) pp. 21-36.

26 Section 104.27 of the *Criminal Code Act 1995*.

the communications services are being, or are likely to be, used by a person for activities or purposes that are 'prejudicial to security'.[27] There appears to be no definition of what conduct constitutes matters that are 'prejudicial to security', nor an explanation in the explanatory materials accompanying the bill. An IPO in relation to the disclosure of telecommunications data (information about the communication, but not its substance) can be issued simply if it 'would be in connection with the performance by ASIO of its functions'.

1.43 Human rights standards require that interferences with rights must have a clear basis in law (that is, they must be prescribed by law). This principle includes the requirement that laws must satisfy the 'quality of law' test, which means that any measures which interfere with human rights must be sufficiently certain and accessible, such that people understand the legal consequences of their actions or the circumstances under which authorities may restrict the exercise of their rights.[28]

1.44 The United Nations Human Rights Committee has said that relevant legislation must specify in detail the precise circumstances in which any interferences with privacy may be permitted.[29] The European Court of Human Rights has found in relation to interception warrants that this does not go so far as to compel states to detail all conduct that may prompt a decision to subject an individual to secret surveillance on 'national security' grounds, given that threats to national security may vary in character and may be unanticipated or difficult to define in advance. However, in matters affecting fundamental rights 'it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power'.[30] Consequently, the Court has held that the law must indicate the scope of any such discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. This includes some indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering security, and limits on which events or acts constitute a serious enough threat to justify surveillance.[31]

1.45 In this context it is also significant that IPOs issued in connection with ASIO's activities do not require the nominated AAT member (judges or magistrates are not

27 Schedule 1, item 43, proposed subsection 89(2), 98(2)

28 *Pinkney v Canada,* United Nations (UN) Human Rights Communication No.27/1977 (1981), [34].

29 United Nations Human Rights Committee, General Comment 16: Article 17 (Right to Privacy), UN Doc. HRI/GEN/1/Rev.1 (1988) 21, [8].

30 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015), [247]-[248].

31 *Roman Zakharov v Russia*, European Court of Human Rights, Grand Chamber, application no. 47143/06 (4 December 2015), [247]-[248].

involved in such orders) to consider how much the privacy of any person would be likely to be interfered with by issuing the order or the gravity of the conduct being investigated. The statement of compatibility states that while this is not in the legislation, ASIO 'must conduct their security intelligence activities in accordance with Ministerial Guidelines', including that the actions be proportionate to the gravity of the threat posed and the probability of its occurrence and that investigations should be done with as little intrusion into privacy as possible.[32] While this may constitute something of a safeguard it is not clear why these requirements are not set out in the legislation and required to be considered at the point at which the IPO is issued.

Disclosure of protected information

1.46 Proposed new Part 11 provides that it is an offence to use, record or disclose protected information, being information obtained in accordance with an IPO or other information relating to an IPO. However, there are numerous exceptions to this, which would allow such information to be used, recorded, disclosed or used in evidence. These include:

- in investigations or proceedings relating to a serious offence;
- for the performance of the function, or exercise of the powers, of ASIO;
- in relation to control orders, preventative detention order or continuing detention orders;
- certain extradition proceedings or for providing mutual assistance to foreign governments;
- for unexplained wealth proceedings;
- corruption or misconduct proceedings;
- the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue (in relation to telecommunication data).[33]

1.47 Having such a broad range of exceptions raises concerns as to whether the right to privacy is adequately safeguarded. It is unclear why it is necessary or appropriate to allow sensitive personal information obtained as a result of an IPO for a particular stated purpose to be used, recorded or disclosed for other broad purposes. The statement of compatibility does not address the limitation of the right to privacy from these exceptions. Rather it states that the exceptions operate in 'specific limited circumstances', and that it promotes the right to privacy as it does not permit the use of information for a purpose not relevant to achieving a

32 Statement of compatibility, [36].

33 Schedule 1, item 43, proposed sections 153-159.

legitimate purpose of the bill.[34] However, it is not clear that all of the stated purposes are relevant to achieving the stated objective of protecting national security, public safety, address crime and terrorism. For example, it is not clear how disclosing protected information for the purposes of protecting the public revenue could be linked to the objectives of the bill.

Further information required

1.48 In order to fully assess the proportionality of this proposed measure, in particular the adequacy of the safeguards that apply, further information is required as to:

- why the bill does not include provision for Public Interest Monitors to apply nationwide (rather than only in Victoria and Queensland) and why the Monitors have no role in an application for an IPO to access stored telecommunications data;
- whether the interference with the right to privacy is greater for the interception of communications than accessing stored communications data, and if so, why;
- why the power to issue an IPO is conferred on a member of the AAT, of any level and with a minimum of five years experience as an enrolled legal practitioner, and whether this is consistent with the international human rights law requirement that judicial authorities issue surveillance warrants;
- why does the bill not require, in all instances, that before issuing an IPO the decision maker turn their mind to considering whether doing so would be likely to have the least interference with a person's privacy;
- why the bill does not require, in all instances, that IPOs may only be issued where to do so will be likely to 'substantially' assist an investigation (rather than simply being 'likely to assist');
- how the timeframe for the duration of an interception IPO was chosen and why interception IPOs issued in connection with carrying out ASIO's functions are twice as long as those to investigate serious offences;
- why there is no provision in the bill to ensure that if the circumstances that led to the issuing of the IPO have changed, such that the IPO is no longer warranted, that the IPO ceases to have effect;
- why are existing powers to investigate serious crimes insufficient to achieve the objectives of the measure, such that a separate power to issue an IPO in relation to control orders is considered necessary;

34 Statement of compatibility, [59].

- why do the control order IPOs not require the judge or AAT member to consider the gravity of the conduct being investigated;
- what does conduct that is 'prejudicial to security' mean, and is this sufficiently certain to allow people to know what conduct it covers;
- why can an IPO to access telecommunications data be granted if it would be in connection with the performance of ASIO's functions, without any other requirement that there is any alleged prejudice to national security;
- why does the bill not provide that an AAT member when determining whether to issue an IPO must consider how much the privacy of any person would be likely to be interfered with by issuing the order, or the gravity of the conduct being investigated; and
- whether all of the exceptions to the prohibition on the use, recording or disclosure of protected information obtained pursuant to an IPO are appropriate. It would be useful if a justification were provided in relation to each of the exceptions in proposed sections 153-159 and how these are compatible with the right to privacy.

Right to an effective remedy

1.49 If IPOs are issued inappropriately they may violate a person's right to privacy. The right to an effective remedy requires states parties to ensure access to an effective remedy for violations of human rights.[35] This may take a variety of forms, such as prosecutions of suspected perpetrators or compensation to victims of abuse. While limitations may be placed in particular circumstances on the nature of the remedy provided (judicial or otherwise), state parties must comply with the fundamental obligation to provide a remedy that is effective.[36]

1.50 The statement of compatibility identifies that the right to an effective remedy is engaged by these measures, but states that any limitations on that right are reasonable, necessary and proportionate.[37] It notes that judicial review is not available under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) for decisions made under the Interception Act, and states that this is consistent with other national security and law enforcement decisions. However, it further notes that a decision of a decision-maker or AAT member will be subject to judicial review under the *Judiciary Act 1903*, providing an avenue to challenge unlawful decisions (where there has been a jurisdictional error). The statement of compatibility further

---

35 International Covenant on Civil and Political Rights, article 2(3).

36 See, UN Human Rights Committee, General Comment 29: States of Emergency (Article 4), (2001), [14].

37 Statement of compatibility, p 16.

notes that the general laws of evidence would serve to protect affected persons, as courts retain the discretion to exclude evidence which has been improperly or illegally obtained.[38] Finally, the statement of compatibility notes that the use of these powers would be subject to the oversight of the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security, which would ensure that the powers are used in accordance with the legislation.

1.51 However, while the oversight of the Commonwealth Ombudsman and Inspector-General of Intelligence and Security may serve as a useful safeguard to help ensure decision-makers are complying with the legislation, this would not appear to provide any remedy to individuals. Further, given that IPOs are designed to be sought covertly, it is also unclear how an applicant could practically seek judicial review of a decision of which they are unaware. United Nations bodies and the European Court of Human Rights have provided specific guidance as to what constitutes an effective remedy where personal information is being collected in the context of covert surveillance activities. The United Nations High Commissioner for Human Rights has explained that in the context of violations of privacy through digital surveillance, effective remedies may take a variety of judicial, legislative or administrative forms, but those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated.[39] The European Court of Human Rights has also stated that if an individual is not subsequently notified of surveillance measures which have been used against them, there is 'little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his knowledge and thus able to challenge their legality retrospectively'.[40] The court acknowledged that, in some instances, notification may not be feasible where it would jeopardize long-term surveillance activities.[41] However, it explained that '[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned'.[42]

1.52 It is not clear that a person who has their communications intercepted or accessed would ever be made aware of that fact (if it does not lead to a prosecution),

---

38 See *Evidence Act 1995*, section 138.

39 Report of the Office of the United Nations High Commissioner for Human Rights on The right to privacy in the digital age (A/HRC/27/37, [40].

40 *Roman Zakharov v Russia* (European Court of Human Rights, Grand Chamber, (Application no. 47143/06) 2015,[234]. See also, *Klass and Others v Germany* (European Court of Human Rights, Plenary Court, (Application no. 5029/71) 1978, [57].

41 *Roman Zakharov v Russia* (European Court of Human Rights, Grand Chamber, (Application no. 47143/06) 2015, [287].

42 *Roman Zakharov v Russia* (European Court of Human Rights, Grand Chamber, (Application no. 47143/06) 2015 [287]. See also *Klass and Others*, [58].

and therefore it is not clear how such a person could have access to an effective remedy for any potential violation of their right to privacy.

1.53 In order to assess whether any person whose right to privacy might be violated by the issuance of an IPO would have access to an effective remedy, further information is required as to:

- whether a person who was the subject of an IPO will be made aware of that after the investigation has been completed; and
- if not, how such a person would effectively access a remedy for any violation of their right to privacy.

Committee view

1.54 The committee notes that the bill seeks to introduce International Production Orders to allow Commonwealth, state and territory law enforcement and national security agencies to acquire data held in a foreign country by a designated communications provider.

1.55 The committee notes the legal advice that the measure engages and limits the right to privacy. In order to fully assess whether the measure is proportionate to the important objective of protecting national security and public safety, and addressing crime and terrorism, the committee seeks the minister's advice as to the matters set out at paragraph [1.48].

1.56 The committee also notes the legal advice that the measure engages the right to an effective remedy. In order to fully assess whether the right to an effective remedy is available, the committee seeks the minister's advice as to the matters set out at paragraph [1.53].

Providing communications data to a foreign government

1.57 Schedule 1, item 13 of the bill seeks to amend the *Mutual Assistance in Criminal Matters Act 1987* ('Mutual Assistance Act') to broaden the scope of materials which the Attorney-General may authorise be provided to a foreign country, to include 'protected IPO intercept information', 'protected IPO stored communications information' or 'protected IPO telecommunications data information' relevant to offences punishable by certain periods of imprisonment or the death penalty.[43]

43 The terms 'protected IPO intercept information', 'protected IPO stored communications information', and 'protected IPO telecommunications data information' would be defined in subsection 3(1) of the Act, pursuant to amendments in Schedule 1, Part 1, Item 11.

1.58 The bill also provides that all applications for an IPO must nominate a 'designated international agreement'.[44] Proposed section 3[45] provides that if there is an agreement between Australia and a foreign government (or two or more governments) and that agreement is specified in the regulations, it is a 'designated international agreement'. However, it also provides that where one or more offences against the law of the foreign country are punishable by death, the agreement cannot be specified unless the minister has received a written assurance from the foreign government relating to 'the use or non-use', in connection with any proceeding for prosecuting a death penalty offence, of Australian-sourced information obtained in accordance with such an order.[46]

Preliminary international human rights legal advice

Right to life

1.59 Providing that protected IPO intercept information can be shared with a foreign country to investigate or prosecute an offence against the laws of that country that is punishable by the death penalty, engages and may limit the right to life.[47] The right to life imposes an obligation on Australia to protect people from being killed by others or from identified risks. While the International Covenant on Civil and Political Rights does not completely prohibit the imposition of the death penalty, international law prohibits states which have abolished the death penalty (such as Australia) from exposing a person to the death penalty in another state.[48] The provision of information to other countries that may be used to investigate and convict someone of an offence to which the death penalty is also prohibited.[49] In 2009, the UN Human Rights Committee stated its concern that Australia lacks 'a comprehensive prohibition on the providing of international police assistance for the investigation of crimes that may lead to the imposition of the death penalty in another state', and concluded that Australia should take steps to ensure it 'does not provide assistance in the investigation of crimes that may result in the imposition of the death penalty in another State'.[50]

---

44 Schedule 1, item 43, proposed subsections 22(2), 33(2), 42(2), 52(2), 63(2), 72(2), 83(2), 92(2) and 101(2). The order itself must also set out the name of the designated international agreement, see proposed paragraphs 31(3)(d), 40(3)(d), 49(3)(d), 61(3)(d), 70(3)(d), 79(3)(d), 90(3)(c), 99(3)(c), and 108(3)(c).

45 Schedule 1, item 43, proposed section 3.

46 Schedule 1, item 43, proposed subsection 3(2) and (5).

47 International Covenant on Civil and Political Rights, article 6.

48 Second Optional Protocol to the International Covenant on Civil and Political Rights.

49 UN Human Rights Committee, *Concluding observations on the fifth periodic report of Australia*, CCPR/C/AUS/CO/5 (2009), [20].

50 UN Human Rights Committee, *Concluding observations on the fifth periodic report of Australia*, CCPR/C/AUS/CO/5 (2009), [20].

1.60 The Mutual Assistance Act provides that a request by a foreign country for assistance under the Act must be refused if the offence is one in respect of which the death penalty may be imposed.[51] However, the Act qualifies this by saying that this prohibition will not apply if 'the Attorney-General is of the opinion, having regard to the special circumstances of the case, that the assistance requested should be granted'.[52] Consequently, it appears that the Mutual Assistance Act creates a risk of facilitating the exposure of individuals to the death penalty.[53]

1.61 The statement of compatibility notes that the right to life is engaged and 'recognised' by the bill.[54] It notes that Australia opposes the death penalty in all circumstances, and states that 'Requiring governments of foreign countries to provide a written assurance acknowledges the right to life is engaged by the Bill as it does not permit an agreement to be specified where no assurance is given'.[55] It further states that:

> As governments of foreign countries are responsible for their own criminal offences, it may be contemplated that Australia designates an agreement with a foreign country where death is the penalty for certain serious criminal offences and therefore, in accordance with the framework of the Bill, enables communications providers in Australia to provide communications data to that foreign government for the purpose of prosecuting a person for an offence for which the death penalty relates.[56]

1.62 As acknowledged by this statement, the bill does not prevent the sharing of information that may be used to investigate or prosecute a person who may be subject to the death penalty. Rather, it simply requires there be a written assurance relating to the 'use or non-use' of such information. As such, the legislation only requires that a written assurance relating to the death penalty be provided, not that the written assurance state that the relevant information will not be used in death penalty proceedings. While the explanatory memorandum states that the 'policy intention of this provision is to give effect to Australia's long-standing bipartisan opposition to the death penalty in the context of reciprocal cross-border access to communications data', there is nothing in law that would prohibit mutual assistance where it may lead to the imposition of the death penalty. This raises significant concerns as to Australia's international obligations relating to the right to life.

---

51 Subsection 8(1A).

52 Subsection 8(1A).

53 This was previously observed by the Parliamentary Joint Committee on Human Rights in 2013. See, Parliamentary Joint Committee on Human Rights, *Report 6 of 2013*, Mutual Assistance in Criminal Matters (Cybercrime) Regulation 2013, pp. 167-169.

54 Statement of compatibility, p. 15.

55 Statement of compatibility, p. 15.

56 Statement of compatibility, p. 15.

Prohibition against torture, cruel, inhuman or degrading treatment or punishment

1.63 The sharing of information, including personal information, with foreign countries, may, in some circumstances, expose individuals to a risk of torture or other cruel, inhuman or degrading treatment or punishment. International law absolutely prohibits torture and cruel, inhuman or degrading treatment or punishment.[57] There are no circumstances in which it will be permissible to subject this right to any limitations. The statement of compatibility does not identify that the right is engaged, and so no assessment of its engagement is provided.

1.64 The proposed IPO scheme does not contemplate that the provision of information pursuant to a 'designated international agreement', could expose a person to torture or other cruel, inhuman or degrading treatment or punishment. The bill does not require that a designated international agreement not be declared for the purposes of an IPO if there are substantial grounds for believing that, if the request were granted, the person would be in danger of being tortured. Further, in the issuing of an IPO, the bill does not require that a judge or AAT member turn their mind to whether to do so may expose a person to a risk of torture or cruel, inhuman or degrading treatment or punishment. The Mutual Assistance Act requires that a request by a foreign country for assistance must be refused if, in the opinion of the Attorney-General, there are substantial grounds for believing that, if the request was granted, the person would be in danger of being subjected to 'torture'.[58] However, the Act does not also specifically require that the Attorney-General consider whether there is a risk of a person being subjected to cruel, inhuman or other degrading treatment or punishment.

1.65 As the statement of compatibility does not address this right, it is not clear what safeguards, if any, exist to ensure that information which may be shared under the IPO scheme does not lead to a person being tortured, or subjected to cruel, inhuman or degrading treatment or punishment.

1.66 In order to fully assess the compatibility of the measure with the right to life and the prohibition on torture, cruel, inhuman or other degrading treatment or punishment, further information is required as to:

- why the bill does not provide that an international agreement will not be designated unless there is a written assurance that information provided pursuant to an IPO will not be used in connection with any proceeding by way of a prosecution for an offence against the law of the foreign country that is punishable by death;

57 International Covenant on Civil and Political Rights, article 7, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

58 Subsection 8(1)(ca).

- what safeguards are in place to ensure that information from an IPO would not be shared overseas in circumstances that could expose a person to torture, or cruel, inhuman or degrading treatment or punishment.

1.67 The committee notes that the bill would broaden the scope of Australian sourced information that may be provided to a foreign country, including foreign countries which use the death penalty.

1.68 The committee notes the legal advice that the measures engage and may limit the right to life and the prohibition against cruel, inhuman or degrading treatment or punishment. In order to fully assess the compatibility of the bill with these rights, the committee seeks the minister's advice as to the matters set out at paragraphs [1.66].

Exemptions from existing privacy protections for orders and requests from foreign countries

1.69 The bill also provides that where there is a designated agreement between Australia and a foreign country and the foreign country issues an order or makes a request in accordance with that agreement, then the usual protections in the Interception Act and *Privacy Act 1988* do not apply.[59]

Preliminary international human rights legal advice

Right to privacy

1.70 Removing existing protections designed to prevent the use of surveillance mechanisms without a warrant or order, or the disclosure of personal information, engages and limits the right to privacy. The right to privacy may be subject to permissible limitations where the limitation pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

1.71 The statement of compatibility states that the removal of these provisions is reasonable and necessary in the circumstances as it ensures Australian communications service providers are not prevented from responding to requests for communications data by foreign governments with which Australia has a designated international agreement. As such it appears that the objective is to comply with our reciprocal obligations under such agreements. However, it is not clear that complying with an agreement that itself may limit the right to privacy constitutes a legitimate objective for the purposes of international human rights law. No information is provided as to what safeguards will be in place to ensure that the foreign governments that make such requests or orders do so in a manner that protects the right to privacy. The explanatory memorandum states that it is 'expected' that

59 Schedule 1, item 43, proposed new sections 167 and 168.

consideration of protections and safeguards related to privacy will be a consideration when developing international agreements.[60] However, there is nothing in the legislation to this effect and it is not clear that such agreements will be subject to any form of independent scrutiny. The statement of compatibility states that this Part of the bill 'does not diminish the responsibility of Australian communications providers to comply with privacy obligations in providing information to foreign parties'.[61] However, as the bill removes the existing protections in the *Privacy Act 1988* and the Interception Act in relation to requests and orders made by foreign governments with whom Australia has an agreement, it is unclear how this could be the case.

1.72 In order to more fully assess the compatibility of this measure with the right to privacy, further information is required as to:

- what is the legitimate objective of removing existing privacy protections to allow personal telecommunications data to be intercepted and accessed by foreign governments; and
- what safeguards apply before foreign governments can issue an order or make such a request and what oversight mechanisms are there before such agreements are entered into.

Committee view

1.73 The committee notes the bill would remove all existing privacy protections against intercepting and accessing personal communications data where a foreign government with whom Australia has a designated international agreement makes a request or order to do so.

1.74 The committee notes the legal advice that this engages and limits the right to privacy. In order to fully assess the compatibility of this measure with the right to privacy, the committee seeks the minister's advice as to the matters set out at paragraph [1.72].

60 Explanatory memorandum, [559].

61 Statement of compatibility, [56].

Advice only[1]

1.75 The committee notes that the following private members' bills appear to engage and may limit human rights. Should either of these bills proceed to further stages of debate, the committee may request further information from the legislation proponent as to the human rights compatibility of the bill:

- Foreign Acquisitions and Takeovers Amendment (Strategic Assets) Bill 2020; and
- Representation Amendment (6 Regions Per State, 2 Senators Per Region) Bill 2020.

1 This section can be cited as Parliamentary Joint Committee on Human Rights, Advice Only, *Report 4 of 2020*; [2020] AUPJCHR 47.

Bills and instruments with no committee comment[1]

1.76 The committee has no comment in relation to the following bills which were introduced into the Parliament between 24 February and 5 March 2020. This is on the basis that the bills do not engage, or only marginally engage, human rights; promote human rights; and/or permissibly limit human rights:[2]

- Aged Care Legislation Amendment (Improved Home Care Payment Administration No. 1) Bill 2020;
- Australian Capital Territory (Self-Government) Amendment (ACT Integrity Commission Powers) Bill 2020;
- Australian Education Amendment (Direct Measure of Income) Bill 2020;
- Banking Amendment (Deposits) Bill 2020;
- Climate Emergency Declaration Bill 2020;
- Family Assistance Legislation Amendment (Improving Assistance for Vulnerable and Disadvantaged Families) Bill 2020;
- Health Insurance Amendment (General Practitioners and Quality Assurance) Bill 2020;
- Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020;
- Liability for Climate Change Damage (Make the Polluters Pay) Bill 2020;
- National Greenhouse and Energy Reporting Amendment (Transparency in Carbon Emissions Accounting) Bill 2020
- Therapeutic Goods Amendment (2020 Measures No. 1) Bill 2020.

1.77 The committee has examined the legislative instruments registered on the Federal Register of Legislation between 6 February and 4 March 2020.[3] The

---

1 This section can be cited as Parliamentary Joint Committee on Human Rights, Bills and instruments with no committee comment, *Report 4 of 2020*; [2020] AUPJCHR 48.

2 Inclusion in the list is based on an assessment of the bill and relevant information provided in the statement of compatibility accompanying the bill. The committee may have determined not to comment on a bill notwithstanding that the statement of compatibility accompanying the bill may be inadequate.

3 The committee examines all legislative instruments registered in the relevant period, as listed on the Federal Register of Legislation. To identify all of the legislative instruments scrutinised by the committee during this period, select 'legislative instruments' as the relevant type of legislation, select the event as 'assent/making', and input the relevant registration date range in the Federal Register of Legislation's advanced search function, available at: https://www.legislation.gov.au/AdvancedSearch.

committee has reported on three legislative instruments from this period in this report. The committee has determined not to comment on the remaining instruments from this period on the basis that the instruments do not engage, or only marginally engage, human rights; promote human rights; and/or permissibly limit human rights.