Australian Human Rights Commission

Review of the mandatory data retention regime

AUSTRALIAN HUMAN RIGHTS COMMISSION
SUBMISSION TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

1 July 2019

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
Complaints info line 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

Table of Contents

1 Executive Summary

1. The Australian Human Rights Commission makes this submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in relation to its review of the mandatory data retention regime contained in Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act). This review is required by s 187N of the TIA Act.

2. In January 2015, the Commission provided a submission[1] to the PJCIS Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill), which introduced the mandatory data retention regime. In that submission, the Commission raised a number of concerns about the potential impact of the Bill on human rights and made a number of recommendations.

3. As outlined in the Commission's 2015 submission and acknowledged by the Government at the time of its introduction,[2] a mandatory data retention regime impacts on human rights—in particular the rights to privacy and freedom of expression. These rights, reflected in articles 17 and 19 of the *International Covenant on Civil and Political Rights* (ICCPR),[3] may be limited by proportionate measures to achieve a legitimate aim if those measures include safeguards and appropriate oversight.

4. In that submission, and here, the Commission refers extensively to the consideration of relevant issues by European courts and authorities. While, of course, Australia is not bound by laws and treaties that apply solely to European countries, the material referred to by the Commission addresses laws that are very similar to the international and domestic laws applicable in Australia, and so it would be common for Australian courts to consider such material in Australian proceedings that deal with such issues. The Commission also notes the Terms of Reference for this PJCIS review expressly include 'developments in international jurisdictions since the passage of the Bill'.

5. Some of the concerns raised by the Commission in its 2015 submission were addressed by changes made to the Bill before it was passed into law. However, some of our recommendations were not adopted, and the Commission remains concerned about certain aspects of the regime — particularly its broad scope, especially when compared with developments in international jurisdictions.

6. As noted in our 2015 submission, '[h]uman rights law provides significant scope for [police and security] agencies to have expansive powers to

investigate criminal activity as well as to protect our national security, even where they limit individual rights and freedoms. Such limitations must, however, be clearly expressed, unambiguous in their terms, and legitimate and proportionate responses to potential harms.'

7. The Commission considers that the mandatory data retention regime goes beyond what can be reasonably justified.

8. This submission is directed at the following aspects of the PJCIS Terms of Reference for this inquiry: the continued effectiveness of the scheme, the appropriateness of the dataset retention period, any potential improvements to oversight, and developments in international jurisdictions since the passage of the Bill.

9. Recent developments in Europe highlight the problems with mandatory and indiscriminate data retention schemes. It is difficult to justify the breadth of these schemes, given their serious encroachments on privacy and their indirect impacts on freedom of expression. The Court of Justice of the European Union (CJEU) has held that European Union law does not permit national legislation which:

    a. mandates general and indiscriminate data retention

    b. grants access to data in circumstances where access is not solely for the purpose of fighting serious crime, and where access is not subject to prior review by a court or an independent administrative authority.[4]

10. The Commission's recommendations are aimed at ensuring that the data retention regime is more closely tailored to the purpose of fighting serious crime and is subject to appropriate safeguards and oversight.

2 Recommendations

11. The Commission makes the following recommendations:

Recommendation 1

The Commission recommends that the TIA Act be amended to include a definition of the terms 'contents' and 'substance' as they appear in ss 172 and 187A(4)(a).

Recommendation 2

The Commission recommends that the two year retention period for communications data be significantly reduced or, alternatively, tailored retention periods be adopted.

Recommendation 3

The Commission recommends that retained communications data is only able to be accessed by enforcement agencies for the investigation of defined, sufficiently serious crimes.

Recommendation 4

The Commission recommends that a warrant or authorisation system by a court or administrative body be implemented for access to retained communications data.

3 Human rights framework

3.1 Article 17 — the right to privacy

12. Article 17 of the ICCPR provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

13. The right to privacy in article 17 encompasses a right against unlawful or arbitrary collection of personal information by others, including government. The United Nations Human Rights Committee (UN HR Committee) has concluded that the capture of communications data amounts to a *prima facie* interference with privacy:

> [A]ny capture of communications data is potentially an interference with privacy and, further… the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.[5]

14. Any limitation on privacy must be lawful.[6] Further, any interference with the right to privacy must not be arbitrary. This 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.[7] Reasonable in this context means any limitation must be proportionate and necessary to achieve a legitimate objective.[8]

15. In our 2015 submission, the Commission highlighted the following comment from the UN HR Committee on data retention schemes:

> Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data 'just in case' it is needed for government purposes. Mandatory third-party data retention—a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access—appears neither necessary nor proportionate.[9]

16. The Commission's 2015 submission referred the PJCIS to the *Digital Rights Ireland* case.[10] In that case, the CJEU had ruled that the EU Data Retention Directive, requiring providers to keep communications data on all users for six months to two years, was incompatible with fundamental rights and therefore void.[11] The Court identified three aspects of the Directive that were particularly problematic:

    a. the collection of personal data was indiscriminate, in that it applied to data of all people regardless of whether or not there was any evidence 'capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime'

    b. the Directive failed to lay down any objective criterion by which to determine the limits of access and use of the data by authorities, to ensure that the data was only accessed and used in relation to the investigation of offences of sufficient gravity to justify the interference with the right to privacy

    c. the retention period failed to distinguish between categories of data based on their potential usefulness in investigating criminal offences.[12]

17. Following the ruling in the *Digital Rights Ireland* case, there was still some discussion and debate about the potential impact of that decision on

national data retention regimes. The CJEU has subsequently resolved this uncertainty by ruling in the *Tele2 Sverige AB* case that EU law must be interpreted as precluding

> national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication … [and]
>
> national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, [and] where access is not subject to prior review by a court or an independent administrative authority.[13]

3.2 Article 19 — freedom of expression

18. Article 19 of the ICCPR provides:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article 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:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

19. As recognised by the Government at the time the Bill was introduced, a mandatory data retention scheme engages and potentially limits the right to freedom of expression. The statement of compatibility with human rights for the Bill noted:

> Requiring providers of telecommunications services to retain telecommunications data about the communications of its subscribers or users as part of a mandatory dataset may indirectly limit the right to freedom of expression, as some persons may be more reluctant to use

> telecommunications services to seek, receive and impart information if they know that data about their communications will be stored and may be subject to lawful access.[14]

20. The only permissible restrictions on freedom of expression are those described in paragraph 3 of article 19.[15] The Bill's statement of compatibility stated that any limitation was 'designed for the legitimate object of protecting public order',[16] which includes 'preventing crime'.[17] In its 2015 submission, the Commission acknowledged that the prevention and detection of crime may be regarded as a legitimate objective.

21. Any limitation on the freedom of expression must be according to law. Laws limiting the freedom must be made accessible to the public, and must provide sufficient guidance both to those executing the laws, and to those whose conduct is being regulated.[18]

22. Further, any limitation on the freedom of expression must be necessary and proportionate to achieve its legitimate objective. As noted by the CJEU in the *Tele2 Sverige AB case*:

> Even if such legislation does not permit retention of the content of a communication … the retention of traffic and location data could nonetheless have an effect on the use of the means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression.[19]

4 Key human rights concerns of the regime

23. The Commission is concerned that the operation of the regime in its current 'catch-all' form is not a proportionate restriction of the right to privacy and freedom of expression.

4.1 Definition of 'contents' and 'substance'

24. Section 187AA of the TIA Act sets out the kinds of information (or documents containing information) that a service provider must keep, including information relating to:

    a. the subscriber of, and accounts, services, telecommunication devices and other relevant services relating to, the relevant service

    b. the source of a communication

    c. the destination of a communication

d. the date, time and duration of a communication

e. the type of communication

f. the location of the equipment or line used in connection with the communication.

25. Section 187A(4)(a) and (b) of the TIA Act explicitly excludes the 'contents' and 'substance' of a communication and a subscriber's web browsing history from the scope of information that may be subject to mandatory data retention. However, there is no definition of 'contents' or 'substance' in the Act.

26. During the course of the previous PJCIS inquiry, concerns were expressed, including by the Commission, the Law Council of Australia and other Parliamentary Committees, that if these terms remained undefined there was a greater potential for data to be retained that does include aspects of content.[20] The submission from the Attorney-General's Department was that, if an attempt were made to define 'content' exhaustively, this may have the effect of unduly limiting the exemption if the ordinary understanding of 'content' expanded over time.[21] One way of addressing this concern is to provide a non-exhaustive definition that still sets out as precisely as possible the current understanding of 'content'. This would have the twin benefits of greater certainty and flexibility.

27. The Commission recommends that the Act be amended to include a definition of 'contents' and 'substance' for the purposes of the regime.

Recommendation 1

The Commission recommends that the TIA Act be amended to include a definition of the terms 'contents' and 'substance' as they appear in ss 172 and 187A(4)(a).

4.2 Two year retention period

28. Section 187C of the TIA Act requires a service provider to keep relevant information and documents for two years. In our 2015 submission, the Commission expressed concern over the two-year retention period proposed by the Bill. We noted that it was at the upper end of retention periods implemented in comparable jurisdictions and that the Directive requiring EU Member States to establish a data retention regime for between six months and two years had recently been declared invalid by the CJEU.[22]

29. The operation of the Australian regime to date shows that, in the overwhelming majority of cases, the data sought by agencies are less than three months old. Annual reports on the operation of the TIA Act prepared by the Attorney-General's Department for 2015–2016 and 2016–2017 show that:

    a. over 80% of requested data was 0–3 months old; and

    b. less than 7% of requested data was over a year old.[23]

30. This suggests that the data retention period could be reduced in order to address significant privacy concerns without unduly impacting on investigations.

31. In the *Digital Rights Ireland* case, one of the issues of concern for the CJEU was that the EU Data Retention Directive provided for general and indiscriminate data retention. An aspect of the indiscriminate nature of the regime was the blunt data retention period.

32. The Court stated:

> [S]o far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data … on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.
>
> Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.[24]

33. Case law since the last PJCIS inquiry has reinforced this position. In the *Tele2 Sverige AB case*, the CJEU considered the limits on national legislation providing for data retention regimes. It ruled that Member States could adopt legislation

> permitting, as a preventative measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.[25]

34. For data retention legislation to be proportionate, there must be a connection—established by objective criteria—between the data retained and the objective pursued (for example, the threat to public security). This

could be achieved, as suggested by the Court in the *Tele2 Sverige AB case*, by restricting retention to '(i) data pertaining to a particular time period and/or geographical area and/or group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime.'[26]

35. When considered together with the age of data generally being requested under the regime, the Commission recommends the adoption of a shorter retention period or, alternatively, tailoring retention periods to the objective pursued or the person/s concerned.[27]

Recommendation 2

The Commission recommends that the two-year retention period for communications data be significantly reduced or, alternatively, tailored retention periods be adopted.

4.3 Access to retained communications data

36. Access to telecommunications data is regulated by Chapter 4 of the TIA Act. Under the regime, enforcement agencies may access historical communications data in circumstances where it is considered reasonably necessary for:

    a. the enforcement of criminal law;[28]

    b. locating missing persons;[29]

    c. the enforcement of a law imposing a pecuniary penalty;[30] or

    d. the protection of public revenue.[31]

37. Access to prospective communications data, however, may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of a 'serious offence' or an offence with a maximum prison term of at least three years.[32]

38. An earlier inquiry of the PJCIS into national security legislation recommended that the threshold for access to telecommunications data be reviewed, with a focus on reducing the number of agencies able to access telecommunications data by using the gravity of conduct that may be investigated using telecommunications data as the threshold on which access is allowed.[33]

39. A number of recommendations of the PJCIS in its inquiry into the Bill were directed at more clearly identifying the agencies able to access telecommunications data. Among other things, s 176A of the TIA Act was amended to specify that enforcement agencies authorised to access retained telecommunications data be limited to criminal law-enforcement agencies listed in s 110A and other authorities or bodies subject to a declaration by the Minister under s 176A(3).

40. A separate but related issue is whether there should also be a limitation on access to telecommunications data based on the gravity of the conduct being investigated. For example, the Commission recommended that access to telecommunications data should only be permitted for the investigation of defined, sufficiently serious crimes.[34] This recommendation was based on the judgment in the *Digital Rights Ireland* case. The CJEU found that the EU Data Retention Directive was not a proportionate interference with the right to privacy. One of the reasons for this was a failure to limit access to data to purposes that were proportionate to the interference with the privacy.[35] The Court said that the Directive

> fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights … may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.[36]

41. In the PJCIS inquiry into the Bill, the Attorney-General's Department submitted that an access threshold based on gravity of the conduct would be a contravention of the Council of Europe Convention on Cybercrime ratified by Australia in 2012. The Department stated:

> As a party to the Council of Europe Convention on Cybercrime, Australia has international obligations to make access to telecommunications data available for the investigation of all criminal offences. Article 14(2) of the Cybercrime Convention requires parties to ensure that telecommunications data is available for the investigation of any criminal offence, not just serious offences. Accordingly, amendments that reduce the number of agencies that have access to telecommunications data based on the gravity of the conduct in question would contravene Australia's obligations under the Convention.[37]

42. The PJCIS referred to the Attorney-General's Department's submission in its report, as well as to the fact that the then Australian Privacy Commissioner

subsequently revised his initial position (limiting the use and disclosure of telecommunications data to the investigation of serious crimes and national security threats), having noted the Department's advice.[38] The Department's submission appears to have been a significant factor in the PJCIS's recommendation that s 180F of the TIA Act require authorised officers to consider the gravity of the conduct before making an authorisation,[39] rather than introducing an access threshold.

43. Having reviewed the Cybercrime Convention, and Australia's reservations to that Convention, the Commission is of the view that the obligations imposed on Australia are not as broad as the Attorney-General's Department suggested. The Convention aims to facilitate investigations between States in order to combat cybercrime. The article 14 obligation referred to by the Department requires State Parties to implement certain 'powers and procedures'. The powers and procedures that must be adopted by State Parties under the Convention relate to: the *real-time* collection of traffic data (article 20), and the interception of content data (article 21). Both of these powers and procedures relate to active criminal investigations.[40] This is very different from what is required under the mandatory data retention regime in the TIA Act which deals with retention of *historical* communications data regardless of whether or not any crime is being investigated. Article 16 of the Cybercrime Convention does require State Parties to make provision for orders requiring the preservation of stored computer data, but only on a case-by-case basis and for a period of up to 90 days per request.

44. Further, the terms of the Convention and Australia's reservations make it clear that Australia's obligations under article 14 apply only to serious offences.

45. Article 21 requires States Parties to empower authorities to intercept content data only in relation to a range of serious offences to be determined by domestic law. Article 14(3)(a) permits States to make a reservation limiting the application of the article 20 requirement for real-time collection of traffic data to the same range of serious offences. Australia has made a reservation in accordance with article 14(3)(a) in the following form:

> In accordance with Article 42 and Article 14, paragraph 3.a, of the Convention, Australia reserves the right to apply the measures referred to in Article 20 (Real time collection of traffic data) only to offences that are punishable by imprisonment for at least 3 years and any other 'serious offences' as defined under domestic law governing the collection and

> recording of traffic data in real time and the interception of content data. Under Australian law, domestic agencies may only gain access to traffic data collected and recorded in real time in relation to offences that are punishable by imprisonment for at least 3 years and other 'serious offences'. Domestic agencies may only gain access to intercepted content data in relation to 'serious offences'.[41]

46. Amending the TIA Act to limit access to historical communications data for the investigation of defined, sufficiently serious crimes, would not therefore appear to be a contravention of Australia's international obligations under article 14 of the Convention.

47. In response to recommendation 25 of the PJCIS, s 180F of the TIA Act was amended to require that, before authorising the disclosure or use of information or documents under Division 4 or 4A, the authorised officer must be satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate having regard to a number of matters. These matters include the gravity of the conduct, the likely relevance and usefulness of the information or documents, and the reason why disclosure or use concerned is proposed to be authorised.

48. The Commission retains concerns about the scope of the regime. While s 180F properly requires a range of relevant matters to be taken into account, it still permits telecommunications data to be accessed for a range of minor offences. A more human rights compliant regime would also include thresholds based on the objective seriousness of the particular offences being investigated, so that reliance is not placed solely on the opinion of the officer from the enforcement agency responsible for authorising access.

49. The operation of the data retention regime to date shows that telecommunications data has been accessed by law-enforcement agencies for a range of investigations that could not be regarded as the investigation of serious offences. Annual reports on the operation of the TIA Act prepared by the Attorney-General's Department for 2015–2016 and 2016–2017 show that:

    a. thousands of authorisations have been made for the purposes of enforcing pecuniary penalties or protecting public revenue: in 2015/16 1,700 authorisations were made for these purposes, and in 2016/17 this increased to 2,600; and

    b. almost 15% of authorisations made to enforce the criminal law were for offences variously categorised as: Acts — injury,

> Miscellaneous, Justice procedures, Pecuniary penalty, Public revenue, Property damage, Public order offences and Traffic.[42]

50. Since the PJCIS inquiry into the Bill, subsequent case law in Europe has reinforced the concerns expressed in our previous recommendation. In the *Tele2 Sverige AB case*, referred to above, the CJEU stated:

> Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure.[43]

Recommendation 3

The Commission recommends that retained communications data is only able to be accessed by law-enforcement agencies for the investigation of defined, sufficiently serious crimes.

4.4 External oversight

51. Presently, the head and deputy head of an enforcement agency or an officer or employee of the agency covered by a written approval from the head of the agency, are all able to authorise access to retained communications data.[44] Other than for information relating to a person working as a journalist (or their employer),[45] all enforcement agencies may access retained communications data without a warrant from an independent body.

52. In its 2015 submission, the Commission noted that the CJEU in the *Digital Rights Ireland* case considered that an independent administrative or judicial body should make decisions regarding access to the retained communications data on the basis of what is strictly necessary.[46] The Court has since repeated and reinforced this position in the *Tele2 Sverige AB case*.

53. In contrast to the position that applies to retained communications data, access to the content of communications requires a warrant. As stated in the 2015 submission, the Commission is of the view that a warrant system is necessary for the access to communications data as well. This is especially the case given the question whether the distinction between content and communications data for the purposes of the right to privacy can be legitimately maintained. The UN HR Committee has stated:

> It has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication does not

> on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as 'metadata' may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.[47]

54. The *International Principles on the Application of Human Rights to Communications Surveillance* (2013) provide that:

> While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications—metadata and other forms of non-content data—may reveal even more about an individual than the content itself, and thus deserves equivalent protection.[48]

55. Contrary to the claims made in the Explanatory Memorandum for the Bill,[49] the Commission considers the retention of and access to communications data may be just as intrusive as retention of and access to content. As recognised by the CJEU:

> [communications] data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them … . In particular, that data provides the means … of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.[50]

56. In the Commission's view, the requirement to store the communications data of each and every customer, just in case that data is needed for law enforcement purposes, is a significant intrusion on the right to privacy and justifies a warrant system for access to it. The fact that there is no specific, identified law-enforcement purpose for the retention of such data further suggests that this might be a disproportionate interference with privacy.

57. The Commission notes the evidence received by the PJCIS from law-enforcement agencies during its inquiry into the Bill, which suggested that a warrant regime would impose an undue administrative burden on their operations.[51] It is true that administrative safeguards against the potential for misuse of compulsory powers require time and effort to comply with.

However, warrants are a familiar part of the existing investigatory process for criminal law-enforcement agencies.

58. Agencies also resisted calls for a warrant regime on the basis that communications data may be required for the investigation of serious offences. However, the fact that an agency is investigating a serious offence does not absolve it of the obligation to satisfy any other existing warrant requirements, for example in relation to access to premises or access to the content of telecommunications.

59. The Commission considers that a warrant regime would apply the appropriate degree of oversight to a regime that has a high impact on privacy. It may also have the effect of rationalising the number of times that retained communications data is accessed. For example, it may be less likely that access would be sought for the purpose of investigating traffic infringements, and more likely that the powers would be reserved for more serious offences. This would limit the potential additional administrative burden on agencies. While the investigation of serious offences may require warrants to be prepared on short notice, this is no different to the requirements that applies in relation to other warrants required for such investigations.

60. While safeguards, such as this three-year PJCIS Review, and the Commonwealth Ombudsman's oversight of the regime, are important checks on the scheme, they are directed at reviewing access powers after they have been exercised. The Commission considers that a warrant or authorisation system for access to retained communications data by a court or administrative body provides a more effective safeguard to ensure that the right to privacy and freedom of expression is only limited where strictly necessary.

Recommendation 4

The Commission recommends that a warrant or authorisation system by a court or independent administrative body, such as a tribunal, be implemented for access to retained communications data.

61. The Commission notes that if recommendations 2 and 3 are not adopted, then recommendation 4 carries much greater importance.

62. As in our earlier submission, the Commission continues to urge that penalties should apply for inappropriate access to and misuse of personal data.

[1] Australian Human Rights Commission (Commission), Submission No 42 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions>.
[2] See eg, Statement of Compatibility, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 10 [33]; Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), 28.
[3] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.
[4] *Tele2 Sverige AB (C-203/15) and Secretary of State for the Home Department (C-698/15) v Post-och telestyrelsen and ors* (21 December 2016) ('*Tele2 Sverige AB*').
[5] Office of the United Nations High Commissioner for Human Rights ('OHCHR'), *The Right to Privacy in the Digital Age,* UN Doc A/HRC/27/37 (2014) [20].
[6] That means that any limitations on the right must be provided for by law: see, *Weber and Saravia v Germany*, application no. 54934/00, 29 June 2006.
[7] United Nations Human Rights Committee ('UN HR Committee'), *General Comment 16,* UN Doc HRI/GEN/1/Rev.1 (1988), 21 [3]-[4].
[8] *Toonen v Australia,* UN HR Committee Communication No. 488/1992.
[9] OHCHR, *The Right to Privacy in the Digital Age* [26].
[10] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014) ('*Digital Rights Ireland*').
[11] *Digital Rights Ireland*. See in particular, at [65]: "It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary".
[12] *Digital Rights Ireland* [56]-[64].
[13] *Tele2 Sverige AB* [134].
[14] Explanatory Memorandum, 28.
[15] UN HR Committee, *General Comment 34*, UN Doc CCPR/C/GC/34 (2011) [22].
[16] Explanatory Memorandum, 29.
[17] Explanatory Memorandum, 28.
[18] UN HR Committee, *General Comment 34* [25].
[19] *Tele2 Sverige AB* [101].
[20] Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Advisory report on the Telecommunications (interception and Access) Amendment (Data Retention) Bill 2014* (2015) [3.97]-[3.99].
[21] PJCIS, *Advisory report* [3.100], [3.102].
[22] Commission, Submission No 42 [28]-[32].
[23] Attorney-General's Department ('AGD'), *Telecommunications (Interception and Access) Act: Annual Report 2015-2016*, Commonwealth of Australia, Table 42 (data for 2015/16 is for the period from 13 October 2015 to 30 June 2016); AGD, *Telecommunications (Interception and Access) Act: Annual Report 2016-2017*, Commonwealth of Australia, Table 38.
[24] *Digital Rights Ireland* [63]-[64].
[25] *Tele2 Sverige AB* [108].

[26] *Tele2 Sverige AB* [106].
[27] Retention schemes should distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned: *Digital Rights Ireland* [63].
[28] *Telecommunications (Interception and Access) Act 1979* (Cth) s 178.
[29] *Telecommunications (Interception and Access) Act 1979* (Cth) s 178A.
[30] *Telecommunications (Interception and Access) Act 1979* (Cth) s 179.
[31] *Telecommunications (Interception and Access) Act 1979* (Cth) s 179.
[32] *Telecommunications (Interception and Access) Act 1979* (Cth) s 180(4). 'Serious offence' is defined in s 5D. For ASIO, both historical and prospective authorisations may only be made where the person making the authorisation is 'satisfied that the disclosure would be in connection with the performance by the Organisation of its functions': ss 175 & 176.
[33] PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013), 46.
[34] PJCIS, *Advisory report* [6.177].
[35] *Digital Rights Ireland* [60]-[62].
[36] *Digital Rights Ireland* [60].
[37] AGD, Submission No 27 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015), 44 <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions>.
[38] PJCIS, *Advisory report* [6.184]-[6.185].
[39] PJCIS, *Advisory report* Recommendation 25.
[40] A Maurushat, 'Australia's Accession to the Cybercrime Convention: Is the Convention still relevant in combatting cybercrime in the era of botnets and obfuscation crime tools?' (2010) 33(2) *University of New South Wales Law Journal* 431, 451.
[41] Council of Europe, *Reservations and Declarations for Treaty No. 185 – Convention on Cybercrime*, at <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=ePWWHb3x>.
[42] AGD, *TIA Act Annual Report 2015-2016*, Tables 39, 40; AGD, *TIAA Annual Report 2016-2017*, Tables 35, 36.
[43] *Tele2 Sverige* [102].
[44] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 5, 5AB, 178-180.
[45] *Telecommunications (Interception and Access) Act 1979* (Cth) ss 180G-180X.
[46] *Digital Rights Ireland* [62].
[47] OHCHR, *The Right to Privacy in the Digital Age* [19].
[48] *International Principles on the Application of Human Rights to Communications Surveillance* (2013), 2 <https://en.necessaryandproportionate.org/>.
[49] See eg, Explanatory Memorandum, 3 [10], 5 [5].
[50] *Tele2 Sverige* [99].
[51] PJCIS, *Advisory report* [6.152]-[6.158].