AUSTRALIA

Joint Submission to the United Nations Human Rights Council
Twenty-third Session of the Universal Periodic Review Working Group
November 2015

Surveillance in Australia: Breaching the Rights to Privacy, Freedom of Expression, and an Effective Remedy

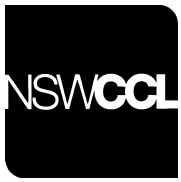
Submitted by:

Center for Democracy & Technology

Australian Privacy Foundation

New South Wales Council for Civil Liberties

Privacy International



*The **Center for Democracy & Technology (CDT)** is a champion of global online civil liberties and human rights. For more than 20 years, CDT has been driving policy outcomes that keep the Internet open, innovative and free.*

*The **Australian Privacy Foundation (APF)** is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians, and to defend the right of individuals to control their personal information and be free of excessive intrusions.*

*The **New South Wales Council for Civil Liberties (NSWCCL)** was founded in 1963 with the aim of protecting the rights and liberties of persons in Australia and its Territories. It is now one of Australia's leading human rights and civil liberties organizations.*

***Privacy International** was founded in 1990 and was the first organization to campaign at an international level on privacy issues. Privacy International is committed to fighting for the right to privacy across the world.*

Contact: Sarah St.Vincent ◆ sstvincent@cdt.org ◆ +1 202 407 8835

I. Introduction and executive summary

1. The Australian Privacy Foundation, New South Wales Council for Civil Liberties, Privacy International, and the Center for Democracy & Technology are pleased to make this submission to the UN Human Rights Council in preparation for the second cycle of the Universal Periodic Review ("UPR") of the Commonwealth of Australia. The lead author of this document is the Center for Democracy & Technology.

2. Our organizations are writing to draw attention to several aspects of Australia's secret surveillance practices that we believe do not comply with the State's obligations under the Universal Declaration of Human Rights ("UDHR") or the International Covenant on Civil and Political Rights ("ICCPR").

3. Our submission addresses five key issues, including:

    - **The extraordinarily broad powers of Australian law enforcement, intelligence, and administrative bodies to intercept and otherwise gain access to private data;**

    - **In particular, the ease and arbitrariness with which the authorities can and do gain access to highly sensitive communications "metadata," which can reveal many details of personal relationships, practices, and beliefs;**

    - **The virtually limitless powers the authorities have to share private data with one another and with the intelligence services of other nations, such as the United States' National Security Agency and the United Kingdom's Government Communications Headquarters;**

    - **The criminalization of individuals' efforts to ensure the privacy of their communications; and**

    - **The adoption of criminal penalties designed to prevent disclosures about secret surveillance practices by journalists or their sources.**

4. Our concerns about the incompatibility of Australia's surveillance practices with the international human rights instruments extend beyond these five issues. However, we believe these aspects of Australia's surveillance regime merit special attention from the Human Rights Council and the Member States, as they have particularly grave implications for the ability to maintain a fully democratic society and prevent gross imbalances of power between the authorities and the governed. We are especially—although not exclusively—troubled by the negative implications these practices may have for religious and ethnic minority groups in Australia who may have pre-existing vulnerabilities to overreaching by law enforcement or other abuses.

5. It is our view that these aspects of Australia's surveillance activities violate the right to freedom from arbitrary or unlawful interference with **privacy and correspondence**, as guaranteed in Article 12 of the UDHR and Article 17 of the ICCPR, as well as the right to **freedom of expression**, as guaranteed in Article 19 of the UDHR and Article 19 of the ICCPR. We believe Australia has also failed to respect the right to an **effective remedy** for violations of the rights listed above (Article 8 of the UDHR and Article 2(3) of the ICCPR).

6. We observe that during the first cycle of the UPR, Australia accepted several recommendations concerning the need to ensure that its counterterrorism legislation and

activities conformed to its human rights obligations.[1] The Human Rights Committee has also previously stressed that Australia "should ensure that its counterterrorism legislation and practices are in full conformity with the Covenant."[2]

7. We urge Australia to implement the Committee's recommendation and adhere to its treaty obligations, including by adopting the recommendations listed in Part IV below.

II. Domestic legal framework

8. Unlike many other democratic States, Australia does not have legislation at the national level (such as a Bill of Rights or Human Rights Act) that sets out the fundamental rights of citizens and others within its jurisdiction. Additionally, although it is a party to the ICCPR, the State has not given this treaty effect in its domestic law, meaning that the Covenant is generally not a source of rights upon which individuals can rely in federal or state courts.[3]

9. To a limited extent, some of the rights found in the international human rights treaties are recognized in Australian law or jurisprudence. However, the State does not recognize any general individual right to free expression (notwithstanding an implied freedom of "political communication" that the High Court has read into the Australian Constitution) or freedom from unlawful or arbitrary interferences with privacy in the secret surveillance context.[4]

10. Although Australia has established a national human rights institution, the Australian Human Rights Commission ("AHRC"), this institution does not have the power to issue enforceable rulings or inquire into any activity carried out by an intelligence agency.[5] Similarly, although a Parliamentary Joint Committee on Human Rights was established in 2011 and provides detailed scrutiny of Australian legislation in an effort to promote compliance with human rights, the committee's recommendations are not binding.[6]

11. Where the secret surveillance of communications is concerned, the default assumption in Australian law is that the interception or collection of a private communication is unlawful unless explicitly authorized in legislation.[7] In reality, however, the surveillance powers that are available to Australian authorities at the national, state, and even local levels are extremely broad. As discussed below, this problem is compounded by the far-reaching abilities of law enforcement and intelligence agencies to share the data they collect with one another and with other nations (from which they are also able to receive data). The problem is also likely to be exacerbated by the increasing criminalization of efforts by individual Internet users and journalists to protect and promote the privacy of communications.

12. Where we have quoted statutory language in this submission, we invite the Council and the Member States to consider the vague and expansive nature of terms such as "assist," "facilitate," "in connection with," "in relation to," "activities prejudicial to security," and "in the interests of … Australia's foreign relations or … national economic well-being." We believe such language should be approached with a full appreciation of its potential for abuse.

---

[1] Human Rights Council, *Report of the Working Group on the Universal Periodic Review: Australia*, UN Doc. A/HRC/17/10 (Mar. 24, 2011), ¶¶ 86.137-86.140; Human Rights Council, *Report of the Working Group on the Universal Periodic Review: Australia: Addendum*, UN Doc. A/HRC/17/10/Add.1 (May 31, 2011), p. 10.
[2] Human Rights Committee, *Concluding observations of the Human Rights Committee: Australia*, UN Doc. CCPR/C/AUS/CO/5 (May 7, 2009), ¶ 11.
[3] *See, e.g.*, *Minogue v Williams* [2000] FCA 125, ¶¶ 21-25.
[4] *See, e.g.*, *Lange v Australian Broadcasting Corporation ("Political Free Speech case")* [1997] HCA 25; Privacy Act 1988.
[5] Australian Human Rights Commission Act 1986, § 11. On the Commission's inability to inquire into the acts or practices of the intelligence agencies, see §§ 11(3)-(4).
[6] Human Rights (Parliamentary Scrutiny) Act 2011, §§ 7, 8(5).
[7] *See, e.g.*, Telecommunications (Interception and Access) Act 1979, § 7(1) (hereinafter "TIA").

a. Collecting and obtaining access to data within Australia

i. Law enforcement

13. As the Parliamentary Joint Committee on Intelligence and Security ("PCJIS") has implicitly recognized, the Australian legal regime governing the interception of or access to communications is exceptionally complex, with multiple types of warrants (or, for some types of data, warrantless access) granted based on a variety of different standards.[8] Although some of these warrant regimes are more compliant with human rights than others, many of them give rise to serious concerns in this respect, as discussed in Part III below.

14. Where the content of communications is concerned, Commonwealth law enforcement authorities such as the Australian Federal Police, along with certain approved state authorities, may apply to judges or members of the Administrative Appeals Tribunal ("AAT") for warrants to intercept private communications in their entirety as they pass through communications networks.[9] These "telecommunications service warrants" may be issued as long as the judge or AAT member concludes that the information "would be likely to assist in connection with the investigation of a serious offence": that is, one punishable by a maximum prison sentence of at least seven years.[10]

15. However, if the authorities are unable to meet this standard, they will often simply be able to wait until the communications in question become "stored" communications (i.e., messages that are no longer in the process of transmission—a transformation that, as a technical matter, will occur virtually instantaneously for communications such as e-mails, text messages, and chats).[11] At that point, the authorities will be able to apply for a different type of warrant with significantly less demanding criteria: a judge or AAT member may issue such a warrant if the information would merely be likely to assist in connection with a "serious contravention"—a term expansive enough to include any offense punishable by a maximum of at least three years in prison or a fine reaching a certain level.[12] As the Gilbert + Tobin Centre of Public Law has pointed out in this context, "[m]any offences with a maximum penalty of three years imprisonment capture conduct that is relatively minor in nature" and "may ultimately be punished by only a very short period of imprisonment (if at all)."[13]

16. Meanwhile, no warrant at all is required for law enforcement officers or members of a variety of administrative bodies to obtain communications information other than "content[] or substance."[14] Although the relevant legislation does not employ such a term, these data are often referred to as "metadata." As the Court of Justice of the European Union has highlighted, such information, especially in the aggregate, "may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence,

---

[8] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013), ¶¶ 2.100 *et seq*., available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm (hereinafter "PJCIS 2013 report").
[9] TIA, *supra* n. 7, § 46.
[10] *Ibid.* at §§ 5D, 46(1)(d).
[11] *Ibid.* at § 110.
[12] *Ibid.* at §§ 5E, 116(1)(d).
[13] Gilbert + Tobin Centre of Public Law, "Inquiry into potential reforms of National Security Legislation: Submission No 36" (2013), available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm.
[14] TIA, *supra* n. 7, §§ 172, 177-180.

daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[15]

17. Law enforcement bodies are permitted to seek metadata as long as they believe such an action is "reasonably necessary" for the enforcement of criminal law, the protection of public revenue, or the location of missing persons.[16] In order to obtain the data, the authorities simply "authorise" the company or other entity that holds it to disclose it; the holder of the data is then obligated to comply.[17]

18. In addition to law enforcement, 41 other government departments, including such entities as city councils, the Australian Fisheries Management Authority, the Department of Health and Aging, the Taxi Services Commission, and the Royal Society for the Prevention of Cruelty to Animals, also presently enjoy warrantless access to private metadata in Australia (although pending legislation may reduce this number).[18]

ii. Intelligence agencies

19. Where the intelligence agencies are concerned, the Australian Security Intelligence Organisation ("ASIO") is empowered to obtain a warrant for the interception of communications (including content) from the Attorney-General whenever a communications service is being used by someone who is "reasonably suspected" of being "likely" to engage in "activities prejudicial to security," insofar as the interception will "assist the Organisation in carrying out its function of obtaining intelligence relating to security" (a set of phrases that includes a number of potentially broad terms).[19] These ministerial (i.e., non-judicial) warrants allow ASIO to intercept communications as they are transmitted and also to collect stored communications.[20] An additional type of warrant, the "named person warrant," is issued under the same standard and is designed to allow ASIO to intercept communications made via multiple services by a single person; however, this type of warrant also allows the intelligence agency to enter any premises—including private homes—in secret in order to install interception equipment.[21]

20. Like law enforcement authorities, ASIO may also obtain metadata without a warrant simply by authorizing the entity that holds the data to make a disclosure, as long as the person authorizing the disclosure believes that it "would be in connection with the performance by the Organisation of its functions."[22] The data holder is required to turn over the relevant metadata upon being authorized to do so.[23]

21. Where physical searches of devices are concerned, ASIO may obtain a ministerial warrant to search any computer (or network of computers) as long as there are reasonable grounds for believing that the agency's access to the data stored in the device "will substantially assist the

---

[15] *Digital Rights Ireland* (Judgment of the Court) [2014] EUECJ C-293/12 (Apr. 8, 2014), ¶ 27.
[16] TIA, *supra* n. 7, §§ 178-179.
[17] *Ibid.*; Telecommunications Act 1997, § 313; *cf.* Vodafone, *Law Enforcement Disclosure Report: Legal Annexe* (2014), pp. 9-10, available at http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf (hereinafter "Vodafone report").
[18] *See* Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979: Annual Report 2012-13*, pp. 44 *et seq*., available at http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf (hereinafter "Attorney-General's report").
[19] TIA, *supra* n. 7, § 9.
[20] *Ibid.* at § 9(1A).
[21] *Ibid.* at §§ 9A, 9B(2)(b).
[22] *Ibid.* at §§ 175-176.
[23] Telecommunications Act 1997, § 313; Vodafone report, *supra* n. 17.

collection of intelligence" in respect of a matter that is "important in relation to security."[24] These "computer access warrants" further empower ASIO to enter premises to view, copy, add, alter, or delete data (which the agency may also obtain permission to do remotely).[25] Through an additional type of ministerial warrant, ASIO may also secretly install surveillance devices that "listen to, record, observe or monitor the words, sounds or signals communicated to or by" a person.[26]

22. Two other Australian intelligence agencies, the Australian Secret Intelligence Service ("ASIS") and the Australian Signals Directorate ("ASD"), have the mission of obtaining "foreign intelligence": that is, "intelligence about the capabilities, intentions or activities of people or organisations outside Australia."[27] Both agencies have the power to provide "assistance" to domestic law enforcement bodies; where ASD is concerned, the law provides that this "assistance" may relate to such broad matters as "cryptography" or "communication and computer technologies."[28] As discussed below, in practical terms this assistance may take the form of intelligence sharing.

b. Data retention and preservation

23. As of the date of this submission, the proposed Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 remains pending. If adopted, however, the legislation is expected to require communications service providers in Australia to retain all non-content communications data (i.e., metadata) for two years.[29] As presently drafted, the bill will also require communications service providers to create certain types of metadata for the purpose of retaining them if the service offered does not normally result in the creation or recording of those items of data (for example, subscriber information).[30] The bill has been highly controversial within Australia, primarily due to concerns about privacy and press freedom as well as a perceived failure on the part of the government to explain its rationale for selecting a two-year retention period.[31] If the legislation is passed in its current form, both ASIO and law enforcement will be able to obtain access to the retained metadata without a warrant (although amendments made to the bill immediately before the date of this submission would impose a warrant requirement when the authorities wish to obtain journalists' metadata in order to identify a source).[32]

---

[24] Australian Security Intelligence Organisation Act 1979, §§ 22 (definition of "computer"), 25A (hereinafter "ASIO Act).
[25] *Ibid.* at § 25A(4); *cf.* Privacy International, "Australian government pushing to expand surveillance, hacking powers" (Aug. 15, 2014), https://www.privacyinternational.org/?q=node/437.
[26] ASIO Act, *supra* n. 24, §§ 26, 26B.
[27] TIA, *supra* n. 7, § 5 (definition of "foreign intelligence"); Intelligence Services Act 2001, §§ 6(1)(a), 7(a) (hereinafter "ISA").
[28] ISA, *supra* n. 27, §§ 6(7), 7(e).
[29] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, §§ 187A, 187C (hereinafter "Data Retention Bill").
[30] *Ibid.* at § 187A(6).
[31] *See, e.g.*, Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015), available at http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report; Gilbert + Tobin Centre of Public Law, "Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014" (letter of Dec. 9, 2014), available at http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions); Amanda Meade, "Data retention bill 'far too intrusive', says new Press Council chair David Weisbrot," *The Guardian*, (Mar. 8, 2015), http://www.theguardian.com/technology/2015/mar/09/data-retention-bill-far-too-intrusive-says-new-press-council-chair-david-weisbrot.
[32] Data Retention Bill, *supra* n. 29, §§ 187A, 187C, read together with TIA, *supra* n. 7, §§ 177-180; Lenore Taylor and Daniel Hurst, "Tony Abbott gives ground on access to journalists' metadata," *The Guardian* (Mar. 16, 2015), http://www.theguardian.com/australia-news/2015/mar/16/tony-abbott-gives-ground-access-journalists-metadata.

24. In the interim, Australian law enforcement authorities and ASIO have the power to issue data preservation notices for content and metadata; these notices require communications service providers to preserve stored communications, including on a potentially large scale.[33]

c. Sharing of data between Australian bodies and with other countries

25. Notwithstanding the limitations Australian law imposes (in however vague terms) upon the types of data that the country's intelligence agencies and law enforcement authorities may collect or access, the laws allow extensive data-sharing between these bodies, meaning that an authority that cannot obtain a piece of data directly may nevertheless be able to seek and receive it from another authority. ASIO, ASIS, and ASD (along with the Australian Geospatial-Intelligence Organisation) have the power to assist Commonwealth and state law enforcement in a variety of manners, including the sharing of intelligence, and the agencies also have wide-ranging powers to assist one another.[34]

26. Where sharing with other countries is concerned, Australia is a party to the UKUSA Agreement (also known as the "Five Eyes" agreement), pursuant to which the ASD does or may share virtually all of the raw data it collects with its peer agencies in the United States, United Kingdom, Canada, and New Zealand.[35] Additionally, Australian law provides in expansive terms that the intelligence agencies may "cooperate" with the authorities of other countries, as long as this is "necessary for [an] agency to perform its functions" or otherwise "facilitates" that performance.[36]

d. Oversight and privacy protections

27. The implementation of Australian counter-terrorism laws, including those governing surveillance, are subject to multiple levels of review and oversight. For example, the Inspector-General of Intelligence and Security ("IGIS"), an independent entity, reviews the intelligence agencies' activities in order to ensure, among other things, that the agencies have respected human rights.[37] Australia also has an Independent National Security Legislation Monitor who reviews the implementation of counterterrorism legislation, including by assessing the laws' necessity and proportionality.[38] Meanwhile, the Commonwealth Ombudsman carries out regular scrutiny of, and reporting on, the interception and other records that law enforcement bodies are required to maintain by law (including copies of warrants).[39] The Ombudsman does not, however, inspect any records kept by the intelligence agencies.[40]

28. Where parliamentary oversight is concerned, the PCJIS may examine any matter relating to the intelligence agencies that is referred to it by a minister or Parliament and has recently

---

[33] TIA, *supra* n. 7, §§ 107H-107J.
[34] ASIO Act, *supra* n. 24, §§ 17(1), 19-19A; ISA, *supra* n. 27, §§ 11(2), 13-13A. *See also* TIA, §§ 64, 67-68, 136-137.
[35] UKUSA Agreement (1955), available at https://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf; Privacy International, *Eyes Wide Open* (2013), available at https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf, p. 5.
[36] ISA, *supra* n. 27, § 13; *see also* ASIO Act, *supra* n. 24, § 19; TIA, *supra* n. 7, § 68A.
[37] Inspector-General of Intelligence and Security Act 1986, § 4 (hereinafter "IGIS Act").
[38] Independent National Security Legislation Monitor Act 2010, § 6.
[39] TIA, *supra* n. 7, §§ 83-88, 152-155.
[40] Commonwealth Ombudsman, "Dealing with the Commonwealth Ombudsman's Office – information for agencies" available at http://www.ombudsman.gov.au/pages/publications-and-media/fact-sheets/information-for-agencies.php#RoleoftheOmbudsman.

provided reviews of current law as well as pending legislation.[41] The Attorney-General also provides mandatory annual reports, including statistics, on the use of interception and data access powers by law enforcement and administrative agencies; these reports are accessible to the public.[42] The Attorney-General's Department has, however, suggested that this reporting regime is "focused on administrative content rather than … ensur[ing] that a particular agency's use of intrusive powers is proportional to the outcomes sought."[43] No similar public reporting requirements are placed upon the intelligence agencies (although the IGIS must report annually to Parliament about her office's inquiries and inspections).[44]

29. Certain elements of Australian law and policy explicitly require the consideration of privacy: for example, the ASD is obligated to adopt a set of privacy rules and has done so, although the rules do not have the force of law and currently provide the agency with extremely wide discretion where the retention and sharing of private data are concerned.[45] Additionally, judges and AAT members must weigh privacy concerns when deciding whether to grant warrants to law enforcement.[46] Law enforcement authorities are also required to consider privacy when seeking disclosures of metadata.[47] However, it is unclear whether a failure to consider privacy adequately (or at all) leads to any consequences for the authority involved.

e. Defeating or criminalizing the use of privacy technologies

30. Notwithstanding the parliamentary, independent, and other ostensible privacy protections described above, the government has adopted laws to defeat or even criminalize the use of privacy technologies. For example, recent amendments to the Crimes Act 1914 empower magistrates to order a person "to provide any information or assistance that is reasonable and necessary" to allow law enforcement authorities to "access data held in, or accessible from, a computer or data storage device." The order can also compel the person to render the data intelligible to the authorities, e.g., by decrypting it. Refusing to comply with such an order can result in a two-year prison sentence.[48]

f. Penalizing journalists

31. Pursuant to recent amendments to the main legislation governing ASIO, the Attorney-General may designate any ASIO operation as a "special intelligence operation" ("SIO"). The effect of such an act is to render the operation's participants immune from criminal or civil liability except in very limited circumstances (for example, where killings or torture occur).[49]

32. By law, anyone, including a journalist, who discloses information that "relates to" an SIO—whether knowingly or not—can be sentenced to five to ten years in prison.[50] The law applies to disclosures both within and outside Australia.[51]

---

[41] ISA, *supra* n. 27, § 29; for recent reviews, *see* Parliamentary Joint Committee on Intelligence and Security, http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security.
[42] *See, e.g.*, Attorney-General's report, *supra* n. 18.
[43] Qtd. in PJCIS 2013 report, *supra* n. 8, ¶ 2.27.
[44] IGIS Act, *supra* n. 37, § 35.
[45] ISA, *supra* n. 27, § 15; *see also* Australian Signals Directorate, "Rules to Protect the Privacy of Australians" (2012), available at http://www.asd.gov.au/publications/dsdbroadcast/20121002-privacy-rules.htm.
[46] TIA, *supra* n. 7, §§ 46-46A, 116.
[47] *Ibid.* at § 180F.
[48] Crimes Act 1914, § 3LA.
[49] ASIO Act, *supra* n. 24, § 35A *et seq.*
[50] *Ibid.* at § 35P.
[51] *Ibid.* at § 35P(4) (referring to Criminal Code Act 1995, § 15.4).

g. Remedies

33. Australian law provides that persons whose communications are unlawfully intercepted (or accessed while stored) are entitled to civil remedies.[52] It does not establish an entitlement to civil remedies for the unlawful accessing of metadata, although violators of the Act's provisions in this respect may be prosecuted.[53]

34. Even where the interception of communications is concerned, the law does not provide for the notification of individuals whose data has been collected illegally, and does not otherwise establish a right to challenge surveillance practices in court. Although ASIO's decisions are technically subject to judicial review, the lack of information available to potential applicants renders this form of redress exceedingly difficult to obtain in practice.[54]

III. Breaches of human rights

a. Right to privacy

35. Although Australia has what appears on the surface to be a comprehensive legal regime governing secret surveillance, we are gravely concerned that the laws' vagueness and overbreadth, as well as the immense powers and discretion they confer on the authorities, may result in serious violations of the right to **freedom from arbitrary or unlawful interference in privacy and correspondence**.

36. We recall that international jurisprudence and commentary suggest that the requirements of this right include the following, among others:

- Any secret surveillance must be done in accordance with international human rights law as well as domestic law;[55]
- The domestic legal regime must be sufficiently clear to give the relevant population an adequate understanding of the types of circumstances that may lead to monitoring;[56]
- Laws permitting surveillance cannot give unfettered discretion to the authorities when ordering or conducting these activities;[57]
- The laws must contain "adequate and effective guarantees against abuse";[58]
- The surveillance activities must be strictly necessary to safeguard the democratic institutions;[59]
- Effective oversight must be provided by bodies that are independent of the entities carrying out the surveillance;[60]
- These requirements apply to the initial interception, collection, or access to data as well as to the later use, storage, or sharing of that data;[61] and

[52] TIA, *supra* n. 7, §§ 107A, 165.
[53] *Ibid.* at § 181A.
[54] *See Church of Scientology v Woodward* [1982] HCA 78; *Parkin v O'Sullivan* [2009] FCA 1096.
[55] *See* Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, UN Doc. A/HRC/27/37 (June 30, 2014), ¶¶ 21-22 (hereinafter "OHCHR report"); UN General Assembly, "The right to privacy in the digital age," UN Doc. A/RES/69/166 (Feb. 10, 2015), operative para. 4(b).
[56] *See Weber and Saravia v. Germany* (dec.) [2006] ECHR 1173, ¶ 93; OHCHR report, *supra* n. 55, ¶¶ 23, 28.
[57] *See Liberty and others v. the United Kingdom* [2008] ECHR 568, ¶¶ 64-70; OHCHR report, *supra* n. 55, ¶ 29.
[58] *See Weber and Saravia*, *supra* n. 56, ¶ 106; OHCHR report, *supra* n. 55, ¶ 28.
[59] *See Klass and others v. Germany* (Plenary) [1978] ECHR 4, ¶ 42; *Rotaru v. Romania* (Grand Chamber) [2000] ECHR 192, ¶ 47.
[60] *See Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* [2007] ECHR 533; ¶¶ 85-89; *cf.* OHCHR report, *supra* n. 55, ¶ 37.

- The treatment of metadata must also comply with these strictures.[62]

37. Based on the foregoing discussion of the domestic laws that govern Australia's secret surveillance practices, we have concluded that Australia is in breach of these aspects of the right to privacy.

38. For the purposes of this submission, we assume that Australia's human rights obligations apply extraterritorially to the extent described by the Office of the High Commissioner for Human Rights ("OHCHR")[63]; however, many of the violations we describe occur, or appear to occur, within Australian territory. We also take the view—as the AHRC, OHCHR, European Court of Human Rights and Court of Justice of the EU have unanimously done—that privacy rights apply to metadata, which (as discussed above) can reveal detailed and highly sensitive aspects of private life.[64]

39. Our foremost concern is that despite its apparent comprehensiveness, Australian law does not give individuals either within or outside Australia a sufficient understanding of the types of circumstances that may lead them to be monitored, and moreover places very few meaningful constraints on the surveilling bodies in this respect.

40. In respect of collection, we observe that both law enforcement and the intelligence agencies have sweeping powers to obtain content as well as metadata. Furthermore, the authorization and oversight mechanisms that are in place—while representing laudable progress—appear to provide few meaningful limits on the authorities' exercise of these powers. Reportedly, the ASD partners with the intelligence agencies of the other "Five Eyes" states to engage in the wholesale interception of transnational communications that pass through undersea cables.[65] Even in the absence of such manifestly arbitrary and excessive activities, however, it is clear that Australian laws, in the aggregate, permit the collection or sharing of virtually any form of electronic correspondence—anytime, anywhere, without adequate standards or oversight.

41. For example, if the Australian law enforcement authorities wish to view the content of a communication, they can obtain a warrant to access it as a stored communication as long as the information would be "likely to assist in connection with" an offense that entails at least a possibility of being punished by three years of imprisonment, and which could be perpetrated by either a party to the communication or a third party.[66] Alternatively, the authorities may simply obtain the communication from ASIO, ASIS, or ASD, all of which have far-reaching powers to collect the content of communications either without a warrant or with only a ministerial warrant, including by secretly entering premises and installing surveillance equipment.[67] The intelligence agencies also enjoy very broad entitlements to obtain the content of communications from one another; in this manner, even those agencies that normally face at least some restrictions when monitoring people within Australia can

---

[61] *See Weber and Saravia*, *supra* n. 56, ¶ 79; Amann v. Switzerland, [2000] ECHR 88, ¶ 69; OHCHR report, *supra* n. 55, ¶ 20.
[62] *See Digital Rights Ireland*, *supra* n. 15, ¶¶ 27, 34-35; OHCHR report, *supra* n. 55, ¶ 19; *Copland v. the United Kingdom* [2007] ECHR 253, ¶¶ 43-44.
[63] OHCHR report, *supra* n. 55, ¶¶ 34-36.
[64] *Supra* n. 62; Australian Human Rights Commission, "Submission to the Parliamentary Joint Committee on Intelligence and Security" (2015), ¶ 10; *see also* Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, UN Doc. A/HRC/23/40 (Apr. 17, 2013), ¶¶ 41-42 (hereinafter "Special Rapporteur's report").
[65] Philip Dorling, "Australian spies in global deal to tap undersea cables," *Sydney Morning Herald* (Aug. 29, 2013), http://www.smh.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html.
[66] *See* ¶ 15 above.
[67] *See* ¶¶ 19-22, 25 above.

effectively obtain whatever data they like.[68] In respect of ASIO, in particular, civil society organizations have expressed a fear that recent legislative changes mean the agency can now monitor very large computer networks, or even (at least theoretically) the entire Internet, on the basis of a single computer access warrant.[69]

42. Where access to metadata is concerned, the discretion conferred on the authorities is nearly total, and the individuals who may be affected have virtually no means of foreseeing whether their privacy will in fact be subjected to interferences in this manner. As mentioned above, as of the date of this submission, 41 Australian law enforcement and administrative bodies enjoy warrantless access to metadata; the Attorney-General reports that in the 12-month period ending on 30 June 2013, these bodies obtained access to private communications metadata on at least 330,640 occasions.[70] By way of comparison, the population of Australia in 2013 was approximately 23 million, meaning that these authorities issued one metadata authorization for every 70 people in the country (although in literal terms, a single individual may be the subject of multiple authorizations).[71] In illustrating the uses of this metadata, the Attorney-General's report highlighted a city council's use of metadata to resolve a dog-bite case—one that manifestly had no bearing on national security, public order, or public health more broadly.[72] ASIO, too, enjoys warrantless access to this type of data.

43. If the Australian Parliament adopts a mandatory data-retention requirement of two years—one that will require communications service providers to keep or create sensitive personal data that they would not otherwise need—the problem of excessive collection will be seriously exacerbated, in spite of the lack of any concrete demonstration that a scheme of this breadth and length is necessary. In this respect, we note the OHCHR's conclusion that mandatory third-party data retention programs "appear[] neither necessary nor proportionate."[73]

44. Even where a warrant regime exists (i.e., for the collection of content), the issuing authority is often a minister or other senior official who is not fully independent of the entity conducting the surveillance.[74] This is particularly true for ASIO, which is only obligated to obtain ministerial warrants.

45. Aside from the privacy infringements inherent in unnecessarily widespread collection itself, the potential for abuse of this data is clear, given the variety of bodies that may obtain or share it. The warrant regimes and other oversight mechanisms described in this submission do not appear to be capable of preventing such abuses.

46. Additionally, despite its open acknowledgment of its participation in the "Five Eyes" intelligence sharing arrangement and the expansive statutory powers of the intelligence agencies to share data with still other countries (see Part II(c) above), Australia does not appear to have adopted any formal and publicly accessible safeguards to ensure that its transnational data sharing practices comply with human rights. In light of the serious ways in

---

[68] *See* ¶¶ 22, 25 above.
[69] See ¶ 22 above; Gilbert + Tobin Centre of Public Law, "Inquiry into the National Security Legislation Amendment Bill (No 1) 2014" (letter of July 31, 2014), pp. 3-4, available at http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/National_Security_Amendment_Bill_2014/Submissions.
[70] Attorney-General's report, *supra* n. 18.
[71] World Bank, "Population, total," http://data.worldbank.org/indicator/SP.POP.TOTL (last accessed Mar. 18, 2015).
[72] Attorney-General's report, *supra* n. 18, p. 53.
[73] OHCHR report, *supra* n. 55, ¶ 26.
[74] *See* ¶¶ 14-15, 19, 21 above.

which such shared data can potentially be misused by other governments, this shortcoming poses a major threat to privacy rights.[75]

47. Furthermore, we are deeply troubled by Australia's efforts to defeat privacy protections adopted by users, including by compelling providers and individuals to decrypt communications.[76] Forcing providers to weaken their encryption techniques makes users vulnerable to the capture of their information by criminals.[77] Additionally, the ability to communicate anonymously and securely is an indispensable element of the right to privacy (as well as the freedom of expression, which is addressed below).[78] Criminalizing efforts by users and providers to keep their information secure runs contrary to the essence of the right.

48. For the foregoing reasons, we have concluded that Australia's secret surveillance practices are unlawful and arbitrary, and therefore violate the right to privacy.

b. Freedom of expression

49. We recall that the right to freedom of expression may only be subject to restrictions that are set out in law and are necessary either to ensure respect for the rights or reputations of others or to protect national security, public order, public health, or morals.[79] We further recall that "[e]ven the mere possibility of communications information being captured" has a "potential chilling effect" on free-expression rights.[80] This is especially, although by no means exclusively, true for the journalists, lawyers, and watchdog organizations whose work is critical to ensuring the proper functioning of democracy.[81]

50. In light of the extraordinarily expansive powers of the Australian intelligence and law enforcement agencies to intercept, access, and share private data, as well as the frequency with which those powers have been employed (at least where metadata is concerned), we note that individuals both within and outside Australia can never be confident that the Australian authorities are not collecting and viewing their data—even when those individuals have no involvement whatsoever with any criminal activity. We also observe with alarm that a journalist or source can be imprisoned for up to 10 years for disclosing any information about an SIO, even in the absence of any knowledge that the operation was in fact an SIO.[82]

51. For these reasons, we believe the Australian secret surveillance regime places an unnecessary burden on the freedom of expression.

c. Right to a remedy

---

[75] *See* OHCHR report, *supra* n. 55, ¶ 27.
[76] *See* ¶ 30 above.
[77] *See, e.g.*, Nuala O'Connor, "Encryption Makes Us All Safer" (Oct. 8, 2014), https://cdt.org/blog/encryption-makes-us-all-safer/; Center for Democracy & Technology, "Issue Brief: A 'backdoor' to encryption for government surveillance" (Nov. 7, 2014), https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/11/issuebrief-backdoorencryption.pdf.
[78] Special Rapporteur's report, *supra* n. 64, ¶ 23; *see also* Center for Democracy & Technology, "Comments of the Center for Democracy & Technology on the Use of Encryption and Anonymity in Digital Communications" (Feb. 13, 2015), https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/02/CDT-comments-on-the-use-of-encryption-and-anonymity-in-digital-communcations.pdf.
[79] International Covenant on Civil and Political Rights, Art. 19(3).
[80] OHCHR report, *supra* n. 55, ¶ 20.
[81] *See, e.g.*, *Weber and Saravia*, *supra* n. 56, ¶¶ 143-146; *Youth Initiative for Human Rights v. Serbia*, [2013] ECHR 584, ¶¶ 6, 22-26; Human Rights Watch and American Civil Liberties Union, *With Liberty to Monitor All* (2014), *available at* http://www.hrw.org/reports/2014/07/28/liberty-monitor-all.
[82] *See* ¶ 32 above.

52. We observe that although Australian law permits civil actions arising from the unlawful interception of content, the lack of a requirement to provide the victims of such unlawful interception with notice (even *ex post facto*) effectively cancels this ostensible protection. Furthermore, we observe that the legislation does not establish any equivalent remedies for the unlawful collection or use of metadata. We also note that ASIO may exempt participants in its surveillance operations from criminal or civil liability simply by designating an operation as an SIO.[83]

53. Under human rights law, the right to a remedy requires that individuals must have access to effective and enforceable redress for violations of their human rights, including the rights to privacy and free expression. Although governments are permitted to place certain limitations on the remedies that are available for clandestine surveillance activities, they must nevertheless ensure that anyone with at least an arguable claim is able to seek enforceable remedial measures.[84] We believe Australia has failed to meet its obligations in this respect.

IV. Recommendations

54. On the basis of the foregoing analysis, we recommend that Australia should:

- **Adopt legislation giving domestic effect to the ICCPR, or otherwise establishing the rights found in the Covenant in a manner that is clear, effective, and enforceable by individuals and legal persons (both within and outside of Australian territory) before Australian judicial and administrative bodies.**

- **Recognize and take steps to comply with its human rights obligations in respect of persons both within and outside its borders, including by ensuring that any communications surveillance (or sharing of surveillance data) conducted by any government entity is strictly necessary and proportionate, done in accordance with clear laws that promote transparency and the foreseeability of the kinds of circumstances in which surveillance (or sharing) may occur, subject to adequate oversight from all three branches of government as well as independent experts, and susceptible to challenge before bodies capable of upholding the right to an effective remedy;**

- **Protect the free-expression rights of journalists and their sources, including by ensuring that journalistic reporting in the public interest on surveillance or intelligence topics is not, as such, subject to civil or criminal penalties; and**

- **Ensure that the bodies that oversee surveillance conducted by the State have sufficient resources, investigative powers, and enforcement capabilities to prevent, detect, investigate, and address abuses. The scope of the Australian Human Rights Commission's investigative and other powers should be expanded to cover activities carried out by the intelligence agencies, including secret surveillance. The oversight of ASIS, ASD, and ASIO should be as thorough as that of law enforcement and administrative agencies. Oversight entities should be as transparent as possible about their activities and findings.**

[83] *See* ¶ 31 above.
[84] *See Association for European Integration*, *supra* n. 60, ¶ 100; OHCHR report, *supra* n. 55, ¶¶ 39-41; UN General Assembly, *supra* n. 55, operative para. 4(e).