Access Now and Digital Rights Watch Joint Submission to the United Nations Human Rights Council on the Universal Periodic Review 37th Session
Third Cycle for Australia

9 July 2020

About Access Now

Access Now is an international organisation that works to defend and extend the digital rights of users at risk around the world. Through representation around the world, including Australia, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions and convenings such as RightsCon, we fight for human rights in the digital age. As an ECOSOC accredited organisation, Access Now routinely engages with the United Nations in support of our mission to extend and defend human rights in the digital age.[1]

About Digital Rights Watch

Digital Rights Watch strategically defends digital rights in Australia. Digital Rights Watch exists to ensure fairness, freedoms and fundamental rights for all people who engage in the digital world.[2]

Introduction

1. Access Now and Digital Rights Watch welcome this opportunity to contribute to Australia's third UPR review cycle. Australia has participated in two UPR review cycles: 27 January 2011 and 9 November 2015 respectively.[3]
2. This submission addresses the state of digital rights including the right to privacy and freedom of expression and access to information in Australia. The right to privacy and freedom of expression and access to information remain priority issues for Australia.

Domestic and international human rights obligations

3. Australia is a signatory to the Universal Declaration of Human Rights (UDHR). Australia has signed and ratified the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), but not the ICESCR's Optional Protocol.[4]

[1] Access Now, Access Now About Us.
[2] Digital Rights Watch, About Us.
[3] OHCHR, Universal Periodic Review - Australia.
[4] OHCHR, Status of Ratification: Interactive Dashboard.

4. The Australian Constitution does not explicitly protect freedom of expression or the right to privacy. However, the High Court has inferred freedom of political communication in sections 7 and 24 of the Constitution.[5]
5. Human rights, including freedom of expression, access to information and the right to privacy are affirmed and protected at the State and Territorial levels in Australia, but not the federal level.[6]

Developments of digital rights in Australia

6. In response to the increased threat of terrorism, and to tackle serious crime, Australia introduced a metadata retention scheme, the Telecommunications (Interception and Access) Amendment (Data Retention) Act, in March 2015. The Act has given way to a data retention grant program to compensate telecommunications providers for costs of retaining data.[7]
7. The metadata retention scheme raises serious concerns for journalists, who have the ethical obligation to protect the identity of their confidential sources.[8] On one hand, the Act conditions the access to journalists' metadata on the granting of a Journalist Information Warrant, thus limiting the grounds on which journalists' metadata would be disclosed. On the other hand, the warrant can be obtained by at least 21 government agencies, and can serve as a tool to identify and pursue journalists' confidential sources.[9] Worryingly, the warrant is also to be granted in secret, without notice to the journalist, and cannot be challenged by those targeted.[10]
8. In 2019, a review of the Act was launched, giving light to extensive overbroad overuse of the powers by law enforcement agencies.[11] The review is expected to be completed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in the second half of this year.
9. In December 2018, the Telecommunications and Other Legislative Amendments (Assistance and Access) Act (TOLA) was rushed through the Parliament in spite of extensive objections by global experts that the legislation poses a threat to the integrity of the Internet's infrastructure and the human rights of individuals.
10. For instance, TOLA poses additional threats to press freedom and expression, by facilitating access to journalists' metadata. By exempting government agencies from pursuing the Journalist Information Warrant to access journalists' metadata, TOLA further undermines the warrant system created by the Telecommunications (Interception and Access) Amendment (Data Retention) Act.[12] TOLA expands the agencies' access to journalists' sources and withdraws the requirement for a warrant and, consequently, of judicial oversight.

[5] *Australian Capital Television Pty Limited v Commonwealth* (1992) 177 CLR 106; *Coleman v Power* (2004) 220 CLR 1.
[6] *See* Human Rights Act 2004 (ACT), s 16 (expression) and s 12 (privacy); the Charter of Human Rights and Responsibilities Act 2006 (Vic), s 15 (expression) and s 13 (privacy).
[7] See Australia Government Department of Home Affairs, Data Retention Industry Grants Programme
[8] Press Freedom, Journalist Information Warrants, (1 May 2019).
[9] *Id.*
[10] For more details, please visit Press Freedom, Journalist Information Warrants, (1 May 2019).
[11] Josh Taylor, Web browsing histories are being given to Australian police under data retention powers The Guardian, 6 February 2020.
[12] Human Rights Law Centre; Digital Rights Watch, Submission to the Independent National Security Legislation Monitor - review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, (13 September 2019).

11. The opposition party vowed to conduct an extensive review of the Act after it was passed, and adopt subsequent amendments to fix the deficiencies in the original text. The PJCIS review is on its 4th iteration since the Act has become operational, currently aiming to finalize their review in September 2020. The Committee has also referred the Act for an independent assessment by the Independent National Security Legislation Monitor (INSLM) which is to be delivered in June 2020.[13]
12. In response to the tragic attack on two mosques in Christchurch, New Zealand, Australia introduced a last minute rushed Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019.[14] The amendment, aimed at giving Australian law enforcement agencies additional powers in order to take down violent or "abhorrent" content, was introduced and passed into law within 48 hours in spite of pleas from human rights groups, journalists and industry groups.[15]

Freedom of expression and access to information

13. It is legitimate for the Australian government to protect its citizens from the dissemination of terrorist content online, but the government will do citizens a disservice if it undercuts the most treasured principle of a functioning democracy, freedom of expression, along the way.[16] It can be tempting to shift the blame to online platforms and threaten them into taking action, including threatening individuals with jail time. Platforms can play a key role in addressing complex societal challenges, including the dissemination of terrorist content online, but it is essential to address real-world issues systematically. Progress requires inclusive, open dialogues and evidence-based policy solutions geared toward a healthier environment that would reflect Australian democratic values of respect for human rights, whether online or off.
14. In 2019, the Australian Federal Police conducted two raids targeting journalists and media outlets, which were reported to be grounded on TOLA. One raid was on the ABC, and the other on the home of a journalist from the Daily Telegraph.[17] Both targets had been reporting on national security issues that are of public interest.
15. In recent years, whistleblowers in Australia have also been facing raids, threats and intimidation from Australian authorities.[18] For instance, "Witness K," an operative of the Australian Secret Intelligence Service, and his lawyer, Bernard Collaery, were charged and have been facing prosecution for revealing the bugging of the Government of Timor-Leste by Australia during negotiations concerning the Timor Sea. Other whistleblowers, especially those who hold public service positions have also been subject to prosecution.[19]
16. Similarly, in 2019, the Australian Media Entertainment and Arts Alliance released a survey of journalists demonstrating that "80% of the respondents reported that defamation laws made

[13] Australian Government - Independent National Security Legislation Monitor, INSLM Review of the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018 (TOLA Act).
[14] Access Now, Changes to Australia's criminal code will create a new class of internet censorship, (2 April 2019).
[15] Access Now, Australia's plans for internet regulation: aimed at terrorism, but harming human rights, (26 March 2019).
[16] *Id.*
[17] Human Rights Law Centre; Digital Rights Watch, Submission to the Independent National Security Legislation Monitor - review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, (13 September 2019); Digital Rights Watch, Breaking: press freedom in Australia (18 September 2019).
[18] Christopher Knaues, Witness K and the 'outrageous spy scandal that failed to shame Australia', The Guardian, (9 August 2019).
[19] *Id.*

their jobs more difficult", while a 25% said that "stories they had written were not published due to fears of provoking defamation proceedings".[20]

17. As the survey demonstrates, defamation-related policies and laws create a chilling effect on the Australian press, and therefore, pose serious risks to the exercise of freedom of expression and the right to access to information. As journalists are triggered to censor themselves under fear of charges and prosecution, they end up refraining from reporting and speaking up on matters that are of public interest.
18. The exercise of the rights to freedom of expression and press freedom, both online and offline, are fundamental in a democratic society. By threatening and prosecuting those who speak up, the government of Australia curtails the exercise of these rights, and impairs the public's right to access to information, which is essential as an oversight mechanism on government's conducts.

The right to privacy

19. Several digital rights organisations have urged the Australian Parliament to revise its data retention scheme to restrict the scope and ensure that authorities retain only data that is strictly necessary; to require judicial warrants for access to metadata; to reduce the overall retention period requirement; and to extend protections and safeguards for journalists and whistleblowers who may be impacted by the regime's creeping scope.[21]
20. In March 2020, the Australian Government's Department of Home Affairs referred the draft Telecommunications Legislation Amendment (International Production Orders) Bill 2020 to the PJCIS. The proposed legislation would result in Australia becoming the "weak link" or "back door" to enable the "Five Eyes" governments to increase their surveillance powers.[22] Specifically, the draft bill introduces "a regime for Australian agencies to obtain independently-authorized international production orders for interception, stored communications, and telecommunications data directly to designated communications providers in foreign countries".[23] This would enable Australian law enforcement authorities to issue requests for data to overseas communications providers directly, often circumventing decision-makers in other jurisdictions (which could have better protection for privacy) as well as skipping out on the warrant requirement within Australia.[24] Text in Schedule 1 offers protection against arbitrary or unlawful interferences with privacy, but it is not convincing because the text presents more carve-outs than protections. Furthermore, it is not likely to meet the necessary human rights standards of international agreements such as the U.S. CLOUD Act, even though it is intended to provide a backbone to those agreements. [25]
21. A concerning trend exists towards mission creep and consolidation of authority with regards to intelligence organisations and communications surveillance. The Australian Security Intelligence Organization (ASIO) is seeking to expand its mandate to encompass looking through the communications of Australians domestically, rather than only focusing on

[20] Freedom House, Freedom on the Net 2019 - Australia.
[21] Human Rights Law Centre, Sweeping metadata laws must be scaled back, (19 July 2019).
[22] *See also* Access Now, Global coalition from five nations demands "Five Eyes" respect encryption, (30 June 2017).
[23] Telecommunications Legislation Amendment (International Production Orders) Bill 2020, (2019-2020).
[24] Stilgherrian, Home Affairs report reveals deeper problems with Australia's encryption laws, ZDNet, (29 January 2020).
[25] *Id.*

international communications to gather intelligence about foreign allies and national security threats.[26] The traditional separation of agencies and powers in governments ensures compromise and dialogue between agencies that often have contrary objectives. To grant singular control over the people meant to protect and secure Australia's infrastructure (cybersecurity) and those picking it apart to catch criminals (ASIO or Australian Federal Police) is the snake eating its own tail.

Digital Identity

22. It is imperative that digital identity systems, particularly those backed by the state's resources and legal powers, are designed around sound principles of governance, data protection, privacy and security. An effective policy framework for a digital ID programme must be supported by an equally strong technology and cybersecurity framework. The collection of large amounts of personal information pertaining to identities – including biometrics – often form tempting targets for criminals and other actors for malicious hacking and cyber intrusion. Additional challenges related to the secure communication of data during authentication must be met through proper encryption.[27]
23. Currently, Australia has two digital identity schemes.[28]The first was built and remains administered centrally by Australia Post at a cost of $30-50 million and is known as Digital iD. The second scheme, GovPass, is developed and run by the Digital Transformation Agency (DTA) at a tallied cost of over $200 million.[29] Neither GovPass nor Digital iD is governed by dedicated legislation so far, beyond existing laws such as the Privacy Act of 1988.
24. Recently, concerns have emerged surrounding the transparency of documentation and processes for accreditation under the GovPass identity system. Under the GovPass system, organisations are required to undergo accreditation to be able to provide digital identity to Australians. When researchers approached the DTA to request for documentation, they were refused. While the DTA has published a lot of documents explaining the rules for accreditation and settings for the digital ID framework, none of the codes behind the scheme or the exchange gateway, or the specifics for each organisations' accreditation have been provided.[30]

Recommendations

25. We therefore urge that freedom of expression, access to information and the right to privacy are prominent issues in the upcoming UPR review cycle. We recommend that the government of Australia:
26. Revise the data retention scheme in order to restrict the scope to retain only data that is strictly necessary, to require judicial warrants for access to metadata, to reduce the overall retention period requirement, and to extend protections and safeguards for journalists and whistleblowers who may be impacted by the creeping scope.[31]

[26] Anthony Galloway, ASIO's counter-terrorism powers to be widened to catch foreign spies, The Sydney Morning Herald, (1 March 2020).
[27] Access Now, National Digital Identity Programmes: What's Next? (May 2018).
[28] Fergus Hanson, Preventing another Australia Card fail, Australia Strategic Policy Institute, (18 October 2018).
[29] Justin Hendry, Australia's digital identity bill tops $200m, Itnews, (19 December 2019).
[30] Denham Sadler, DTA digital ID hit by transparency concerns, Innovation Aus, (22 June 2020).
[31] Human Rights Law Centre, Sweeping metadata laws must be scaled back, (19 July 2019).

27. Support, not undermine, encryption and encrypted communications. The Australian Parliament should repeal the damaging Assistance and Access Act (TOLA) or heavily amend it in order to ensure that individual rights are protected in the day to day functionality of law enforcement agencies and intelligence services.[32]
28. Review national legislation and policies to fully protect the safety and rights of individuals who speak up, including journalists, activists and whistleblowers, so that these actors can pursue their activities freely without undue interference, attacks or intimidation.
29. Update the federal-level Privacy Act, which currently grants little to no actual privacy and data protection for Australian users.[33] Australian lawmakers should refrain from moving away from the objectives of this act as has been done in recent years. Collapsing these complex issues into a one-size-fits-all policy solution is likely to be detrimental for both freedom of expression and privacy going forward.
30. Take the necessary steps to ensure that regulatory bodies related to digital rights and human rights, such as the Office of the Australian Information Commissioner (OAIC), have the necessary resources to develop the appropriate legislative, institutional and policy frameworks to advance the protection of rights, including the right to privacy and freedom of expression.
31. Take steps towards establishing a comprehensive legal framework around its digital identity programmes. These frameworks should evolve from healthy public discussion and such discussions should include important questions related to the purpose of the program, the safeguards for user rights, protections against surveillance, the role of private actors, centralization of identification and authentication mechanisms, and security measures, especially in case of biometrics-based authentication.
32. Legislate human rights protections at the federal level. It is imperative that the Australian government codify these protections so that they are not mere concepts to the Australian public, but a concrete part of the legal system, providing individuals with security and safety.

Conclusion

33. The UPR is an important UN process aimed at addressing human rights issues worldwide. It is a rare mechanism through which citizens around the world get to work with the government to improve human rights and hold them accountable to international law. Access Now and Digital Rights Watch are grateful to make this submission.

For more information, please contact:

Peter Micek | General Counsel, Access Now | peter@accessnow.org

Laura O'Brien | UN Advocacy Officer, Access Now | laura@accessnow.org

Lizzie O'Shea | Co-Founder and Chair, Digital Rights Watch |lizzie@digitalrightswatch.org.au

[32] Access Now, In Australia, major amendments to encryption law are a step in the right direction, (4 December 2019).
[33] Jennifer Duke, Privacy issues 'not exclusive' to tech giants: Google, Facebook lobby group, The Sydney Morning Herald, (24 March 2019).