Digital Rights Watch

Submission to United Nations High Commissioner for Human Rights on the right to privacy in the digital age

9 April 2018

Who is Digital Rights Watch?

Digital Rights Watch (DRW) is an Australian non-profit charity that supports, fosters, promotes and highlights the work of Australians standing up for their digital rights. Digital Rights Watch is also a member of the international coalition Keep It On, which aims to educate and advocate against internet shutdowns worldwide.
http://digitalrightswatch.org.au

For more information about this submission please contact Elizabeth O'Shea, Board Member of Digital Rights Watch - lizzie@digitalrightswatch.org.au

Executive Summary

DRW commends the UN High Commissioner for Human Rights' initiative in inviting input from stakeholders on human rights challenges relating to the right to privacy in the digital age, including on principles, standards and best practices with regard to the promotion and protection of the right to privacy. DRW sees a fundamental connection between freedom of expression, digital privacy and a free and open internet. We have set out response to a number of issues raised in the call for input:

1. **Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age.**

2. **Surveilliance and communications interception: government surveillance; role of business enterprises in contributing to, or facilitating government surveillance activities.**

3. **Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.**

4. **Growing reliance on data-driven technology and biometric data: main challenges regarding the impact on the right to privacy and other human rights.**

5. **Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals.**

Should you wish to discuss any of these matters further, please do not hesitate to contact us.

1. Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age.

We note the Department of Foreign Affairs and Trade released a cyber engagement strategy in 2017.[1] This strategy contains encouraging material, particularly concerning advocacy for human rights and democracy in digital spaces. Unfortunately, we remain concerned because the Australian Government could do better at respecting the human rights of citizens back home, including for reasons outlined in this submission.

2. Surveilliance and communications interception: government surveillance; role of business enterprises in contributing to, or facilitating government surveillance activities.

Australia has a mandatory data retention regime in place that facilitates retention of and access to customer data and compromises Australians' privacy rights.

In 2015, the Australian government began implementing a legislative data retention regime that allows law enforcement and security agencies to apply to access telecommunications data and requires Telcos, ISPs to retain certain telecommunications data for two years. The regime has recently come into full force.

The requirement to retain data applies to all licensed carriers, carriage service providers and internet service providers.[2] Some services are specifically excluded, such as broadcasting. The types of data which must be retained are listed in the legislation.[3] Broadly, the law requires that the relevant service providers retain data including source and destination of a communication, the date, time and duration of a communication, communication type, location of communications equipment, but not the content.

The regime permits a range of enforcement agencies to request that these service providers retain data and facilitate access to customer data without a warrant.[4] The legislations lists those specific enforcement agencies that have immediate authority to request data, but this list can also be added to by the Attorney-General with very few procedural hurdles. A further 61

[1] Australia's International Cyber Engagement Strategy, Department of Foreign Affaris and Trade, October 2017 http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_6_human_rights_and_democracy_online.html
[2] Section 187A of the *Telecommunications (Interception and Access) Act 1979.*
[3] *Id*.
[4] Sections 110A and 176A of the *Telecommunications (Interception and Access) Act 1979.*

agencies have requested that they be added to the list, but to date none has been.[5] Reporting requirements by the Attorney-General in this respect are minimal.

There are some reporting requirements. The Australian Communication and Media Authority (ACMA) is required to include in its annual report information on disclosures of customer information made during the reporting year.[6] However, carriers and ISPs cannot report requests for data they get from the Australian Security and Intelligence Organisation (ASIO). In addition to the ACMA, the independent Inspector-General of Intelligence and Security plays a role in the data retention regime, as that Office oversees ASIO, including their processes for accessing telecommunications data. The Privacy Commissioner assesses industry's compliance with the Australian Privacy Principles and other legislation.[7]

From its conception through to its ongoing implementation, the data retention scheme has been controversial. The general justification for the data retention regime provided by government has been that it is necessary to further Australia's national security interests and to assist law enforcement agencies with criminal investigations. However, government officials have notably had difficulty justifying the data regime on this basis, and have struggled to meet concerns about the inappropriate and disproportionate nature of this response to national security and law enforcement concerns.[8] There has been significant criticism of the regime as a result.[9]

Recent journalistic investigations of the data retention regime have revealed that numerous Federal Government departments and other bodies have attempted to obtain access to metadata, despite not being listed as an enforcement agency in the legislation.[10] Some departments have been attempting to circumvent this by requesting the Australian Federal Police to access data on their behalf, as a listed enforcement agency. These departments include, but are not limited to: the Australian Taxation Office, the Department of Foreign Affairs and Trade, the Department of Agriculture, the Department of Education and the Department of Social Services. Applications to access metadata have also been made by organisations as diverse as the National Measurement Institute and Greyhound Racing Victoria.[11] The relevance

---

[5] Benjamin Sveen, 'Data Retention Bill: Government departments ask AFP to access metadata after legislation enacted,' ABC, 3 October 2016 http://www.abc.net.au/news/2016-10-04/government-departments-obtain-metadata-via-afp/7898648.

[6] Australian Communications and Media Authority, Fact Sheet: Disclosure requirements under Part 13 of the Telecommunications Act, http://www.acma.gov.au/theACMA/disclosure-requirements-under-part-13-of-the-telecommunications-act.

[7] *See* Data Retention, Attorney-General's Department, https://www.ag.gov.au/dataretention.

[8] Nicolas Suzor, Kylie Pappalardo, Natalie McIntosh, 'The passage of Australia's data retention regime: national security, human rights, and media scrutiny,' Internet Policy Review (forthcoming 2016), https://osf.io/6wxmw/.

[9] Clare Reilly, 'Mandatory Data Retention laws pass Australian Parliament,' CNet, 27 March 2015, https://www.cnet.com/au/news/mandatory-data-retention-laws-pass-parliament/.

[10] Benjamin Sveen, 'Data Retention Bill: Government departments ask AFP to access metadata after legislation enacted,' ABC, 3 October 2016 http://www.abc.net.au/news/2016-10-04/government-departments-obtain-metadata-via-afp/7898648.

[11] Stephanie Anderson, 'List of agencies applying for metadata access without warrant released by Government, ABC, 17 January 2016, http://www.abc.net.au/news/2016-01-18/government-releases-list-of-agencies-applying-to-access-metadata/7095836.

of such applications to protecting national security is highly dubious, and is evidence of the risk of 'scope creep' in such an expansive data collection regime.

Relevantly, one issue remained open until relatively recently, namely, access to data retained under the regime for the purposes of civil proceedings. Civil society raised concerns during the consultation process for the regime about access to data for this purpose. As a result, an amendment was due to be implemented to prohibit the disclosure of telecommunications data by service providers in response to orders of a court in connection with civil proceedings, where the data is kept by the service provider solely for the purpose of complying with its data retention obligations. A parliamentary committee was charged with reviewing whether this kind of data should be available for use in the civil justice system, for example, in family law proceedings involving violence or international child abduction cases. On 13 April 2017, the Government tabled a report in Parliament that concluded that sufficient evidence had not been received to sustain a recommendation that regulations be made to allow civil litigants to access the data.[12]

In summary, Australia's data retention regime permits authorities access to the enormous amount of data collected and stored by Telcos and ISPs. There is little transparency around the functioning of the regime, which has very few requirements for public disclosure of requests made or actions taken under this framework. Furthermore there is reason to believe that organisations, including government departments, may be intentionally circumventing privacy protections within the legislation in order to gain access to data which they are not authorised to have. The extensive, intrusive nature of the current data collection regime, in combination with a lack of transparency over which bodies are able to access it and for what purposes, risks creating a chilling effect on freedom of expression in Australia. This is a source of significant concern to civil society organisations.

3. Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.

The Australian government has indicated it intends to introduce legislation designed to weaken encryption, though the details are not yet clear, which would undermine freedom of expression and opinion.

[12] Australian Government, Attorney General's Department, 'Access to telecommunications data in civil proceedings' https://www.ag.gov.au/consultations/pages/access-to-telecommunications-data-in-civil-proceedings.aspx.

Prime Minister Malcolm Turnbull has publicly announced that his government wants to introduce a method for intercepting and reading encrypted messages. In July 2017, he discussed giving law enforcement this power for the purposes of keeping the public safe from terrorism.[13]

It remains unclear what form this will take. Former-Attorney General George Brandis indicated that mandating a backdoor is not the government's plan, however he has also stated in June 2017 that 'if there are encryption keys then those encryption keys have to be put at the disposal of authorities.'[14]

DRW has serious concerns about the implications of this proposal for Australians' freedom of expression and privacy, and believe that it has very serious implications for Australia's economy and digital security.

4. Growing reliance on data-driven technology and biometric data: main challenges regarding the impact on the right to privacy and other human rights

The Australian government has tabled a bill that would facilitate the collection and centralisation of sensitive biometric information and have serious implications for the right to privacy.

In October 2017, the Australian Government introduced proposed legislation to facilitate the collection of biometric data.[15] The bill provides for the exchange of identity information between the Commonwealth, state and territory governments by enabling the Department of Home Affairs to collect, use and disclose identification information. This includes sensitive biometric information, including from individuals who have not been convicted of criminal offences.

In its current form, the bill represents a serious incursion into the privacy of Australian citizens. DRW supports the joint submission made by Futurewise and the Australian Privacy Foundation in response to the tabling of the bill.[16] That submission outlines how the justification for the proposed regime is not coherent and fails to establish, except through direct assertion, that the

[13] Rachel Baxendale, 'Laws could force companies to unlock encrypted messages of terrorists,' The Australian, 14 July 2017 https://www.theaustralian.com.au/national-affairs/laws-could-force-companies-to-unlock-encrypted-messages-of-terrorists/news-story/ed481d29c956dfac9361061a60dcf590

[14] David Wroe, 'How the Turnbull government plans to access encrypted messages,' The Age, 10 June 2017 https://www.smh.com.au/politics/federal/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html

[15] Identity-matching Services Bill 2018 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6031

[16] Futurewise and the Australian Privacy Foundation joint submission, https://www.aph.gov.au/DocumentStore.ashx?id=1894ab93-e3a5-4123-9751-cd28a3a32fab&subId=564411

proposed measures are a legitimate and proportionate. The wording of the bill is so wide such that the effect is that biometric matching might be deployed for almost any purpose. Further, some of the data governance processes and structures applicable to the Department of Home Affairs remain unclear.

The government has suggested that privacy protections are embedded in the collection process, and that the bill merely facilities centralisation of this data in a 'hub.' This glosses over the implications of government having an enormous amount of data in its control with limited oversight. DRW remains significantly concerned about this bill.

5. Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals

The legal protections of individual Australians' privacy remain weak.

Privacy is not recognised as a constitutional right in Australia and individuals are not able to bring claims directly against organisations which have breached their privacy. Despite numerous recommendations from law reform bodies, no statutory tort of invasion of privacy exists in Australian law.

The Australian Privacy Principles, whilst a good base level for the protection of privacy in respect of government, are inadequate in their ability to deal with the current landscape of privacy issues.

The *Privacy Act 1988* contains a set of principles called the Australian Privacy Principles. The Privacy Principles apply to federal government agencies, all private and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses. They are a set of principles for using, managing and storing personal information.

The Privacy Principles provide a base level of disclosure about consumer privacy for numerous entities, but there are significant exceptions. The complaint process is one path to remediate undue access to customers data by government. But it remains insufficient given the gravity of the issues at stake.

The Office of the Information Commissioner (OAIC), containing the federal Privacy Commissioner, is a key agency for supervising legal and regulatory standards, but it has struggled with persistent underfunding and institutional uncertainty.[17]

[17] Chris Duckett, 'Pilgrim finally gets nod as Australian Information Commissioner,' ZDNet 28 September 2016 http://www.zdnet.com/article/pilgrim-finally-gets-nod-as-australian-information-commissioner/.

The current attitude of the Australian Government towards any kind of independent oversight or advocate on matters of privacy or freedom of expression has been one of clear disdain and active destruction. In the 2014 Federal Budget of 2014, the OAIC was slated for being disbanded and all funding cut. The Senate refused to allow this to occur, and thankfully in 2016, the OAIC was allocated $9.3m to operate. However, the autonomy of the Office has been hampered through changes to the way Freedom of Information requests are now handled, with this responsibility being controlled by the Attorney General's department.

The third largest political party in Australia, the Greens, have announced a plan for an independent human rights commissioner for digital rights.[18] Their role will be to advocate for the online safety, accessibility, privacy and security. DRW supports this initiative as a clear way forward to ensure proper independence for the role of protecting citizens' digital rights.

The Privacy Act contains exemptions for political parties which are a source of concern in light of recent events about data mining for political purposes.

Another deficiency of privacy protection in Australia is the exemption from the *Privacy Act* for registered political parties.[19] This is particularly concerning given the use of personal information in social media sites such as Facebook for political advertising purposes, as has come to light in the current Cambridge Analytica scandal. The Australian federal Privacy Commissioner has announced an investigation into whether Cambridge Analytica and Facebook have handled and utilised Australians' personal information in ways which may constitute infringements of the *Privacy Act*.[20] However, with the exemption for political parties in the *Privacy Act*, Australian political parties engaging in similar conduct may not even be investigated by the federal Privacy Commissioner.

Given the 'datification' of politics and political campaigning, we are concerned that this exemption may facilitate conduct on behalf of Australian political parties which is in breach of Australians' right to privacy. This case also highlights the challenges for national DPAs in investigating transnational tech corporations and forcing their compliance with domestic privacy laws. In neighbouring New Zealand, the Privacy Commissioner there has determined that through this conduct Facebook is in breach of NZ privacy legislation,[21] while Facebook has responded claiming it is not subject to that legislation.[22] We are concerned that even if the Australian federal Privacy Commissioner finds Facebook to be in breach of Australian privacy law, it may not be able to secure Facebook's compliance with it.

---

[18] Media Release, Greens Announce Digital Rights Commissioner, 21 June 2016 http://scott-ludlam.greensmps.org.au/articles/greens-announce-digital-rights-commissioner.

[19] *Privacy Act 1988* (Cth) s 6C(1).

[20] Office of the Australian Information Commissioner, Facebook and Cambridge Analytica https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica#investigation-into-facebook-opened

[21] NZ Privacy Commissioner, Privacy Commissioner: Facebook must comply with NZ Privacy Act, 28 March 2018 https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-facebook-must-comply-with-nz-privacy-act/

[22] Jamie Smyth, 'Regulator says Facebook breached New Zealand privacy act', Financial Times, 28 March 2018 https://www.ft.com/content/dda178ce-3245-11e8-b5bf-23cb17fd1498