Digital Rights Watch

Submission to United Nations Special Rapporteur on the protection of the right to freedom of opinion and expression

Study on freedom of expression in the telecommunications and Internet access sector

30 October 2016

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 Special Rapporteur's initiative in soliciting submissions for his study on freedom of expression in the telecommunications and internet access sector. DRW sees a fundamental connection between freedom of expression, digital privacy and a free and open internet. We have set out a number of areas in which these values are compromised in laws and practices in Australia.

1. **Data retention regime**
2. **Copyright website blocking regime**
3. **Executive powers over the telecommunications industry**
4. **Removal of content at the request of the eSafety Commissioner**
5. **Privacy principles - potential remedies for undue access to customer data**
6. **Digital divide - promotion or enhancement of internet accessibility or connectivity**
7. **Standards and governance**

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

1. Data retention regime

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

The Australian government recently passed a legislative data retention regime - one 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 relevant Bill amending the *Telecommunications (Interception and Access) Act 1979* received Royal Assent on 13 April 2015. The laws came into force on 15 October 2015 but many providers have until 13 April 2017 to comply with these changes. The requirement to retain data applies to all licensed carriers, carriage service providers and internet service providers.[1] Some services are specifically excluded, such as broadcasting.

The types of data which must be retained are listed in the legislation.[2] This includes subscriber information and telecommunications data from customers, but not content. 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, and location of communications equipment.

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.[3] The legislations does 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 agencies have requested that they be added to the list, but to date none has been.[4] Reporting requirements by the Attorney-General are minimal.

There are some reporting requirements which form part of the bigger picture of regulation of the Telcos and ISPs, one of which is the role of the Australian Communication and Media Authority (ACMA). The data retention regime came into force in a general context where carriers and ISPs are required to keep customer data confidential. Part 13 of the *Telecommunications Act 1997* creates offences for the use or disclosure of any information or document which comes into their possession in the course of business, where the information relates to customer communications and other personal information. However there are exceptions to this, including an exception for providing telecommunications data to enforcement agencies. The ACMA is required under paragraph 57(2)(f) of the ACMA Act to include in its annual report information on disclosures of customer information made during the reporting year.[5] However, carriers and

---

[1] Section 187A of the *Telecommunications (Interception and Access) Act 1979.*
[2] *Id*.
[3] Sections 110A and 176A of the *Telecommunications (Interception and Access) Act 1979.*
[4] 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.
[5] Australian Communications and Media Authority, Fact Sheet: Disclosure requirements under Part 13 of the Telecommunications Act,

ISPs cannot report requests for data they get from the Australian Security and Intelligence Organisation. In short, there is very little by way of notification to customers or public disclosure of requests made or actions taken to provide or facilitate access to customer data.

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 the Australian Security Intelligence Organisation (ASIO), including their processes for accessing telecommunications data. The Privacy Commissioner assesses industry's compliance with the Australian Privacy Principles and also monitors industry's non-disclosure obligations under the Telecommunications Act.[6]

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.[7] There has been significant criticism of the regime as a result.[8]

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.[9] 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.[10] The relevance 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.

In summary, Australia's data retention regime permits authorities access to the extraordinary 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

---

http://www.acma.gov.au/theACMA/disclosure-requirements-under-part-13-of-the-telecommunications-act.

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

[7] 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/.

[8] 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/.

[9] 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.

[10] 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.

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.

2. Copyright law and copyright website blocking regime

Australian copyright law, both common law and legislation, has compromised the privacy of customers and has undermined the ability of Telcos and ISPs to respect human rights.

In 2012, the High Court of Australia held that iiNet, an ISP, had no legal duty to police what its subscribers did with their internet connections.[11] The litigation was brought by a coalition of rights-holders seeking to enforce their copyright by holding the ISP responsible for alleged customer infringements. The court found that ISPs are under no obligation to take measures against subscribers based only on the strength of copyright infringement allegations made by rights-holders.

In a later application, a rights-holder did eventually succeed, at least partially: a court has since required an ISP to hand over data about customers whose households are alleged to have infringed copyright, subject to the rights-holder satisfying the court that it would not use this information to engage in speculative invoicing.[12] Ultimately that never happened.[13] The subsequent responsibility for dealing with the infringements with this customer data fell to rights-holders.

After lobbying by rightsholders to amend the law after the iiNet case, in 2015 the *Copyright Amendment (Online Infringement) Bill 2015* was passed, amending the *Copyright Act 1968.* This legislation introduced a website blocking regime which permits rights-holders to apply to the Federal Court for an order to have websites blocked by Telcos and ISPs if those websites are facilitating copyright infringement.

---

[11] *Roadshow Films v. iiNet* (2012) 248 CLR 42 http://eresources.hcourt.gov.au/showCase/2012/HCA/16.
[12] *Dallas Buyers Club LLC v. iiNet* [2015] F.C.A. 317 http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2015/2015fca0317.
[13] *See* Allie Coyne, 'DBC gives up on iiNet piracy case,' IT News, 10 February 2016 http://www.itnews.com.au/news/dbc-gives-up-on-iinet-piracy-case-414920 ('Perram had set a $600,000 bond as a condition of his lifting the stay of the April 2015 preliminary discovery order, which gave DBC LLC access to the account holder details on a conditional basis….He ruled DBC LLC had failed to address his concerns about going after account holders for high damages.')

To obtain an order under the regime, the rights-holder must show that the website infringes, or facilitates an infringement of, copyright and the primary purpose of the website must be to infringe, or to facilitate the infringement of, copyright.[14] If the order is made to block the website, the Telco or ISP must take all reasonable steps to disable access to the website.[15] The regime has some ambiguities contained within it which are currently being adjudicated in court.[16]

There is very little by way of public disclosure of requests made or actions taken to restrict access to websites, other than by voluntary notification by users. There is a current citizen-led campaign underway for internet users to report any sites that are blocked as a result of the regime.[17] Contributing to the lack of transparency in these matters, the only parties to any application under the website blocking regime are the rights-holder and the Telco/ISP. The person who operates the website may make an application to be joined to the proceeding, but has no right to be heard per se. Indeed, there is no requirement even to notify persons running a website that their website is the subject of an application. This effectively sets up a process which is inherently weighted in favour of blocking websites, impinging on both freedom of expression and access to information in Australia.

A draft industry code for copyright infringement was developed by a number of stakeholders. with a draft released in April 2015.[18] The proposed code involved a notice scheme for customers in situations where rights-holders claim that copyright infringement had taken place. It was abandoned after the cost of operating the scheme was found to be too high.[19] There may be some renewed interest in it from industry, but it remains unclear if it will be adopted.[20]

The copyright safe harbour scheme in Australia is deeply flawed, in that it only applies to telecommunications providers, and not all internet intermediaries.[21] The lack of protection for online intermediaries (including general content hosts, search engines, and social media platforms) creates a great deal of uncertainty and regulatory risk in Australian law.[22] The practical outcome is that the speech rights of Australian users are limited because

---

[14] Section 115a(1) of the *Copyright Act 1968.*
[15] Section 115a(2) of the *Copyright Act 1968.*
[16] *See for example* Jake Sturmer, 'Pirate Bay, Torrentz, IsoHunt under spotlight in Australian website-blocking test case,' ABC, 24 June 2016 http://www.abc.net.au/news/2016-06-24/pirate-bay-torrentz-under-fire-in-website-blocking-test-case/7541714.
[17] See https://s115a.com/.
[18] Communications Alliance Ltd, C653:2015– Copyright Notice Scheme Industry Code, http://www.commsalliance.com.au/__data/assets/pdf_file/0005/48551/C653-Copyright-Notice-Scheme-Industry-Code-FINAL.pdf.
[19] Allie Coyne, 'ISPs blindsided by 'shelved' Australian piracy code,' IT News, 18 February 2016 http://www.itnews.com.au/news/isps-blindsided-by-shelved-australian-piracy-code-415324.
[20] Allie Coyne, 'Australian piracy code could reappear in 12 months,' IT News, 4 April 2016 http://www.itnews.com.au/news/australian-piracy-code-could-reappear-in-12-months-417730.
[21] Peter Leonard, 'Safe Harbors in Choppy Waters-Building a Sensible Approach to Liability of Internet Intermediaries in Australia' (2010) 3 *J. Int'l Media & Ent. L.* 221.
[22] Rebecca Giblin, 'The Uncertainties, Baby: Hidden Perils of Australia's Authorisation Law' (2009) 20 *Australian Intellectual Property Journal* 148.

intermediaries do not have the protection of a certain safe harbour scheme.[23] Without an effective notice & takedown scheme, Australian hosts have a strong incentive to remove speech in response to requests from third parties without a clear procedure for evaluating or contesting their validity. The gap in protection in Australian law is due to an unfortunate error in the drafting of legislation implementing the US Australia Free Trade Agreement. New legislation has been drafted and is expected to be introduced to remedy this oversight in coming months.[24]

In summary, Australian copyright law now includes laws that may permit authorities to require Telcos and ISPs to suspend or restrict access to websites, directly impacting on freedom of expression. There are very few requirements for public disclosure of requests made or actions taken for this purpose. Australia has also exhibited a trend in law-making that affects Telcos and ISPs' ability to respect freedom of opinion and expression, through an unequal court process weighted in favour of website blocking. Telcos and ISPs are therefore operating in a legal environment where it may prove difficult to prevent, mitigate or challenge the human rights impact of Australian copyright law as these businesses may be required to provide access to customer data.

3. Executive powers over the telecommunication industry

The government of Australia has a range of powers at its disposal which influence the work of Telcos and ISPs, and effect Australians' right to access an open internet where freedom of expression is respected.

The *Telecommunications Act 1997* contains provisions that allow law enforcement agencies to block websites in order to stop illegal conduct. Telcos and ISPs are required under Section 313 to give officers and authorities such help as is reasonably necessary for the purposes of:

- enforcing the criminal law and laws imposing pecuniary penalties;
- assisting the enforcement of the criminal laws in force in a foreign country;
- protecting the public revenue; and
- safeguarding national security.[25]

This provision applies to Telcos and ISP and includes 'providers of telecommunication networks or facilities.' The law has been in place for fifteen years, but there has been a spike in use since 2012.

---

[23] See generally 'Manila Principles on Intermediary Liability' (2015) https://www.manilaprinciples.org
[24] See Nicolas Suzor, Rachel Choi and Kylie Pappalardo, 'Moments of Flux in Intermediary Liability for Copyright Infringement in Australia' in Mark Perry (ed), *Global Governance of Intellectual Property in the 21st Century* (Springer, 2016) 129 https://eprints.qut.edu.au/91196/
[25] *Telecommunications Act 1997* s 313(3).

Notices issued under this section permit law enforcement agencies to request Telcos and ISPs to block websites if they are believed to be involved in illegal activities. There is almost no transparency on how this provision is used at all.

In 2013, the Australian Securities and Investments Commission inadvertently blocked 250,000 websites after it had attempted to block just 1200 using a Section 313 notice. According to media reports, ASIC later indicated that it was not aware that a single IP address could host multiple website, which lead to the mass take-down.[26]

A bipartisan parliamentary committee was established in the wake of this incident, which found that the use of this provision needed to be 'tightened and made more transparent.'[27] However, the committee maintained that there was an 'indisputable need for government agencies to have access to these powers.'[28] There are a set of proposed guidelines for the use of section 313 currently under review.[29] These guidelines have also been subject to criticism for failing to address concerns around the broad scope of the power and the absence of transparency.[30]

There are a range of other powers which executive government authorities have to impose restrictions on Telcos and ISPs as providers of access to the internet. Licensed telecommunications carriers and nominated carriage service providers are required under the *Telecommunications (Interception and Access) Act 1979* to lodge an annual interception capability plan. An interception capability plan outlines how carriers and nominated carriage service providers can help law enforcement agencies with lawful interception of telecommunications services.

In a similar vein, the Attorney General has released proposed telecommunications sector security reforms. In late 2015, the Attorney General released the *Telecommunications and Other Legislation Amendment Bill*, which is designed 'to strengthen the current framework for managing national security risks to Australia's telecommunications networks.'[31] This includes a legislative regime which allows the Attorney-General to issue carriers and ISPs a direction requiring them to do or refrain from doing a specified thing to manage security risks.

---

[26] Allie Coyne, Labor, 'Coalition unite on controversial website blocking powers,' IT News, 1 June 2015 http://www.itnews.com.au/news/labor-coalition-unite-on-controversial-website-blocking-powers-404669.

[27] Standing Committee on Infrastructure and Communications, Report from inquiry into the use of section 313 of *the Telecommunications Act 1997* by government agencies to disrupt the operation of illegal online services, Balancing Freedom and Protection, 1 June 2015 http://www.aph.gov.au/Parliamentary_Business/Committees/House/Infrastructure_and_Communications/Inquiry_into_the_use_of_section_313_of_the_Telecommunications_Act_to_disrupt_the_operation_of_illegal_online_services/Report.

[28] *Id*.

[29] Department of Communications and the Arts, Guidelines for the lawful disruption of access to online services, https://www.communications.gov.au/have-your-say/guidelines-lawful-disruption-access-online-services.

[30] Bill Birtles, 'Guidelines for website blocking legislation do not address transparency, potential for broad use: lawyer,' ABC, 1 June 2015 http://mobile.abc.net.au/news/2015-06-01/guidelines-for-website-blocking-laws-criticised/6513080.

[31] *See* Telecommunications Sector Security Reforms, Attorney-General's Department https://www.ag.gov.au/Consultations/Pages/Telecommunications-Sector-Security-Reforms.aspx.

In summary, Section 313 notices permit authorities to require Telcos and ISPs to suspend or restrict access to websites for reasons of law enforcement or national security. Transparency around the use of these powers is sorely limited. As an example of a law which regulates the activities of private entities that provide network components or related technical support, it demonstrates the need for greater accountability and transparency over website blocking practices to ensure that freedom of expression is not unduly restricted. Legislative requirements for an interception capability plan and similar proposals are further examples of laws that regulate the activities of private entities that provide network components or related technical support.

4. Removal of content at the request of the eSafety Commissioner

In addition to broad executive powers to direct online intermediaries to remove or block content, Australia has recently introduced an administrative body designed to regulate material that is potentially harmful to children.

The Office of the Children's e-Safety Commissioner (OCeSC) tasked with administering a complaints system for online bullying material targeted at Australian children.[32] While the Office has legal enforcement powers, these are only realistically effective against Australian intermediaries, not the major foreign social media platforms it generally targets. Core to the Office's operation is a voluntary scheme designed to encourage social media platforms to cooperate by developing procedures for the rapid removal of bullying content. The scheme was only recently introduced - its effectiveness to this end remains to be seen.

Worryingly, there is almost no transparency around this function performed by the Commissioner. Requests and responses to requests are not reported. The only insight into how this power is exercised is in the Commissioner's annual report. The most recent annual report states: '[d]uring 2015–16, the Office worked collaboratively with social media services to see cyberbullying material removed from social media platforms, in less than a day in many cases.'[33]

Without adequate transparency, it is impossible to gauge the extent to which social media platforms are removing content in a way that is proportionate and legitimate. There is little accountability to identify when content has been wrongfully removed, and there is no formal system of appeal or due process.

5. Privacy principles

The Australian Privacy Principles, whilst an excellent base level for the protection of privacy, 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 most government agencies, all private and not-for-profit organisations with an annual turnover of more than $3 million, all private health service

---

[32] *Enhancing Online Safety for Children Act 2015* (Cth) s 18.
[33] Office of the Children's eSafety Commissioner - annual report 2015-16, p 124 https://www.esafety.gov.au/about-the-office/corporate-reporting.

providers and some small businesses. They are a set of principles for using, managing and storing personal information.

The Privacy Principles are forward thinking in a number of respects. They ensure that all entities subject to the Privacy Principles have a privacy policy. They require that personal information be managed in an open and transparent way and that individuals be given the option of not identifying themselves, or of using a pseudonym.[34] The also require that personal information collected for a particular purpose not be used or disclosed for a secondary purpose without permission.[35] There is a complaint process for individuals who believe they have had their privacy breached, which is conducted through the Information Commissioner. This can result in a determination by the Information Commissioner and in some cases, the provision of a civil penalty.

The Privacy Principles provide a base level of disclosure about customer 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.

6. Digital divide

Australia still experiences a significant digital divide which impacts the human rights of a range of different social groups.

This trend was confirmed in the Digital Inclusion Index, which found problems among older Australians, indigenous people and people with disabilities, among others.[36] The Digital Inclusion Index, which aims to measure the level of digital inclusion across the Australian population, has proven to be a valuable tool to identify the problems with access to the internet and digital literacy.[37] It will also hopefully impact policy proposals also over time.

The Australian government does have some initiatives that are underway to address this. It is currently in the process of rolling out the National Broadband Network (NBN), which is designed to address many of these problems. The purpose of the NBN is to 'deliver Australia's first national wholesale-only, open access broadband network to all Australians.'[38] This project is

---

[34] Australian Privacy Principles 1 and 2, https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.
[35] Australian Privacy Principle 6.
[36] Julian Thomas, Josephine Barraket et al, Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2016, p 5 http://digitalinclusionindex.org.au/wp-content/uploads/2016/08/Australian-Digital-Inclusion-Index-2016.pdf.
[37] *Id.*
[38] *See* NBN, Our Purpose, http://www.nbnco.com.au/corporate-information/about-nbn-co/our-purpose.html.

taking longer than expected, arising from strong differences of political opinion as to the technology choices to roll out the NBN.

The Australian government has also declared 2016 as the 'National Year of Digital Inclusion.' The aim is to 'help Australians to realise their online potential, raise awareness of digital inclusion at all levels of society and celebrate the benefits of digital literacy and digital inclusion through events happening across Australia.'[39]

It is worth noting that competition and consumer laws are arguably important to closing the digital divide. For example, a recent case brought by the Australian Competition and Consumer Commission against a mobile service provider was successful in obtaining damage and injunctive relief and penalties. The provider was found to have engaged in illegal behaviour, including representing to customers 'that mobile phone coverage was available at their home address when it was not, including to customers in remote indigenous communities where no coverage was available.'[40] These cases are necessary because the individual customers are likely to be vulnerable and will probably not have the means to bring a case themselves. Importantly, it shows that groups that do not have access to the internet are keen to find ways to address this. The Government must ensure that the industry is properly regulated to avoid telcos taking advantage of consumers who are seeking to gain access to the internet.

The Government must also ensure that access is guaranteed for those people with special needs, such as those who are blind, deaf or have other disabilities. Australia has adopted a number of both domestic and international instruments to promote inclusion of people with a disability. Australia has had a Disability Discrimination Act[41] in place since 1992 to protect the rights of Australians with a disability; and there is a 10 year National Disability Strategy[42] outlining how people with disability can be further included in Australian economic, social and community participation.

Whilst some of the work being undertaken through the building of the NBN, initiatives such as the National Year of Digital Inclusion, and the work of the ACCC are working to promote or enhance Internet accessibility and connectivity, there continues to be problems of access to much of Australia's networked society for people with a disability, such as cost, literacy and accessibility.

---

[39] *See* Go Digi, National Year of Digital Inclusion, https://www.godigi.org.au/nydi.
[40] Australian Competition and Consumer Commission, 'Court finds Excite Mobile acted unconscionably,' 22 April 2013, https://www.accc.gov.au/media-release/court-finds-excite-mobile-acted-unconscionably.
[41] https://www.comlaw.gov.au/Series/C2004A04426
[42] https://www.dss.gov.au/our-responsibilities/disability-and-carers/program-services/government-international/nationaldisability-strategy

There are many organisations in Australia who are better placed than DRW to comment on the specific needs of people with a disability accessing technology - we merely wish to flag that it remains a concern in relation to equity within Australia.

In summary, the digital divide is a very real concern for large sections of the Australian populace, and only going to grow without significance acknowledgement from the Australian Government that accessing the Internet is a human right and must be available to all its citizens.

7. Standards and governance

The Office of the Information Commissioner (OAIC), a key agency for supervising legal and regulatory standards, has struggled with persistent underfunding and institutional uncertainty.[43]

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.[44] 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.

[43] 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/.
[44] Media Release, Greens Announce Digital Rights Commissioner, 21 June 2016 http://scott-ludlam.greensmps.org.au/articles/greens-announce-digital-rights-commissioner.