

Public Consultations Team
White Paper Task Force
Department of Foreign Affairs and Trade
RG Casey Building
John McEwan Crescent
Barton ACT 0221
Australia

February 27, 2017

Re: Comments on the Department of Foreign Affairs and Trade Foreign Policy White Paper

Access Now welcomes the opportunity to contribute to the development of the Department of Foreign Affairs and Trade (DFAT) foreign policy White Paper.¹

Context:

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world, including in the Indo-Pacific region. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. The organization, co-founded by an Australian in 2009, is located across the world with 40 staff engaged in a range of policy, advocacy and technology initiatives.

The call for public submissions on the White Paper raises a number of important and interrelated questions regarding internet freedom and digital rights that impact Australia's strategic interests and foreign policy priorities, including:

1. How Australia's values should underpin its foreign policy?
2. Which global trends, such as developments in technology, are likely to affect Australia's security and prosperity?
3. How Australia should use its influence in regional and international organisations to support and shape them?
4. How Australia's foreign policy can support a more prosperous, peaceful and stable region?

There can be no discussion about the future of Australia's foreign policy and the nation's engagement with the world without deeply incorporating, engaging with and anticipating the impact that technology has on every element of external relations, trade, growth and security.

In a December 2016 speech, the Minister for Foreign Affairs, the Hon. Julie Bishop MP, referred to 'worrying developments and persistent trends undermining support and respect for human rights' in our region, drawing particular attention to the fact that

¹ <https://www.accessnow.org/>

‘internet freedom is under pressure’.² Indeed it is.

Given the fundamental role of the internet in our lives – from the delivery of innovative healthcare and education services, to facilitating full participation in civil society and global economic opportunity, to the changing nature of diplomatic relations between states – it is essential to enshrine human rights values into the democratic institutions charged with maintaining a free and open internet, and to incorporate new technology considerations into all levels of foreign policy.

In outlining its candidacy for a seat on the United Nations Human Rights Council (2018-2020), DFAT highlights the active role Australia has played in promoting Human Rights Council resolutions on human rights and the internet, and its commitment to ensuring individuals are able to enjoy the same human rights online as they enjoy offline.³ Access Now played an important role in that resolution, and in its predecessors, and we would very much like to acknowledge the role that the Australian government played in achieving such a significant resolution.

Australia’s foreign policy in this area should be designed to counter any threats to digital rights, in the Indo-Pacific region and beyond. **Access Now encourages DFAT to affirm its overarching commitment to digital rights in the White Paper, with a particular focus on key policy issues including freedom of expression and privacy in the digital age.** We also recommend that the Australian government take full advantage of its membership of the Freedom Online Coalition,⁴ and play a more active role in its work.

Freedom of expression:

We note with interest that the Australian government has said that “should Australia become a member of the Human Rights Council [it] would place a heavy emphasis on protecting freedom of expression’ as a key political right”.⁵ Regardless of the outcome of Australia’s UNHRC candidacy, the White Paper should reflect this ongoing commitment.

Freedom of expression online can be undermined in a variety of ways, including censorship laws, limitations on the right to anonymity, blocking access to social media platforms or communications tools, and network shutdowns. The Australian government has already flagged a particular concern in this area. The newly appointed inaugural Ambassador for Cyber Affairs, Dr Tobias Feakin, has been charged with responsibility for ‘advocating against state censorship of the Internet’⁶. There is a rising tide of proposals around the globe seeking to restrict online speech, particularly with respect to the goal of countering violent extremism (CVE).

Access Now has a policy guide - ‘A Digital Rights Approach to Proposals for Preventing

² http://foreignminister.gov.au/speeches/Pages/2016/jb_sp_161212.aspx

³ <http://dfat.gov.au/international-relations/international-organisations/Pages/australias-candidacy-for-the-unhrc-2018-2020.aspx>

⁴ Freedom Online Coalition, Press Release: Australia Joins the Freedom Online Coalition, March 2015
<https://www.freedomonlinecoalition.com/news/australia-joins-the-freedom-online-coalition/>

⁵ Speech by Minister for Foreign Affairs, The Hon. Julie Bishop MP, December 2016

http://foreignminister.gov.au/speeches/Pages/2016/jb_sp_161212.aspx

⁶ http://foreignminister.gov.au/releases/Pages/2016/jb_mr_161110.aspx

or Countering Violent Extremism Online’ - which maps out a set of high-level principles for evaluating CVE proposals and provides specific recommendations based on those principles.⁷ The Australian government should take a leadership role, particularly within the Indo-Pacific region, declaring the importance of directly protecting human rights in all CVE efforts.

Access Now leads an ongoing campaign against internet shutdowns.⁸ Shutdowns are early warning mechanisms for human rights violations and have been used during the most critical moment of the democratic process — elections. These actions also have a detrimental impact on social and economic activity.

In 2015 Access Now urged the government of Nauru to stop the blocking of certain services on the internet. The presence of an immigration detention facility, funded by the Australian government, in the country makes it even more important that the ability to seek, receive, and impart information through the internet is unrestricted. Free expression is vital for the vulnerable asylum seekers on the island. As the world grapples with increased migration flows, the internet will continue to serve as a crucial means to uphold human rights.

As part of its stated commitment to safeguarding freedom of expression and other digital rights, the Australian government should continue to publically and privately condemn measures taken by other governments to disrupt internet access.

Privacy:

The right to privacy is fundamental to the protection of other freedoms including the rights to freedom of expression and association. There are a number of disturbing global trends currently encroaching on this right including the expansion and legitimisation of mass surveillance programs, high profile examples of government hacking of private communications and policies on encryption that undermine security protections of activists and other individuals. Threats to privacy also come from private companies, such as internet service providers, with access to significant amounts of personal data. Global policy debates on these issues are ongoing. Australia’s stance should reflect its deep commitment to protecting the human rights and genuine security of its citizens.

Australia’s membership in the Five Eyes, an intelligence alliance that also includes Canada, New Zealand, the United Kingdom, and the United States, raises additional questions about the government’s commitment to protecting human rights. The details of the partnership, which involves the sharing of surveillance data and programs, are notoriously opaque.⁹ However, what details are known demonstrate that the surveillance programs impact the personal data of broad swaths of the global population with no ability for users to obtain redress nor adequate transparency even if mechanisms were in place.

⁷ <https://www.accessnow.org/beware-countering-violent-extremism-online-risks-human-rights/>

⁸ <https://www.accessnow.org/keepiton/>

⁹ <https://www.privacyinternational.org/node/51>.

Whilst the focus of this submission is foreign policy rather than domestic legislation, Access Now maintains its previously expressed concerns about the implications of Australia's mandatory data retention and surveillance laws.¹⁰ We do not believe the laws represent a necessary and proportionate response to the threats articulated. Australia also has a law to authorize government hacking operations, which have been used both domestically as well as internationally, including a recent investigation that led to the installation of malware on computers in the United States.¹¹

Government hacking operations are even more invasive than traditional methods of surveillance and have severe implications both for targets and non-targets.¹² An ongoing commitment to policies that undermine human rights constrains the effectiveness of Australian leadership on digital rights issues in an international context. We encourage Australia to re-evaluate and reform these programs and authorities to better protect individual rights.

Australia is tipped to be in a leadership role in the Indo-Pacific region with respect to institutionally advancing data protection given the fact of it having statutory frameworks for privacy at the commonwealth level and across several of its states. This focus on helping safeguard the private data of users must form a key focus for the Australian government, at the foreign policy level in addition to further steps on more effective domestic enforcement, building on its recent advancement in passing a commonwealth data breach law.

Regional capacity building:

The new Australian Ambassador for Cyber Affairs will be responsible for supporting 'cyber capacity building in our region'. Whilst acknowledging Australia's role in assisting partner governments to develop the institutional capacity to address legitimate security concerns, Access Now advocates for a strong human rights focus in the development of Australia's International Cyber Engagement Strategy and the implementation of government funded programs such as the 'Cyber Cooperation Program - Building Cyber Capacity in the Indo-Pacific'.¹³ In that particular program references to human rights considerations are made in both the 'advice to applicants' and the assessment criteria, however, there could be greater emphasis on how proposed projects would consolidate Australia's global commitment to digital rights and operate within a human rights anchored framework. Language matters. An overemphasis on the cyber security theme when talking about internet policy initiatives can detract from valuable work being done on other capacity building fronts.

Additionally, the Australian government should seek to expand its networks and capacity building support in the sphere of legal and regulatory institutions dealing with digital rights. The Australian government should support the Office of the Information Commissioner and the privacy regulators from its states in further engaging and

¹⁰ <https://www.accessnow.org/global-state-of-surveillance-australias-terror-laws-set-to-erode-human-righ/>

¹¹ https://motherboard.vice.com/en_us/article/australian-authorities-hacked-computers-in-the-us.

¹² <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>.

¹³

<http://dfat.gov.au/about-us/business-opportunities/tenders/Pages/dfat-cyber-cooperation-program-building-cyber-capacity-in-the-indo-pacific.aspx>

building the capacity for privacy and data protection enforcement across the Indo-Pacific region, a key step in helping provide an environment that allows for safe cross-border transfers of data and the functioning of the digital economy. Additionally, with its common law tradition, Australia should engage with helping build the capacity of judicial and other legal institutions across the Commonwealth of Nations in the sphere of the internet and digital rights, helping advance a positive programme key for the future of all democracies in our digital age.

Developments in technology:

Given the pace and expansive nature of technological change, the specific implications of developments in network architecture, artificial intelligence, the Internet of Things (IoT) or algorithmic accountability, for example, are impossible to predict. Any strategy for the defence and extension of digital rights must be sufficiently flexible and responsive. Given that the ambition of the White Paper is to guide Australia’s international engagement over the next decade, in a fast moving policy area like digital rights the focus should be on the underlying principles, such as transparency, inclusivity and equitable access. It is also crucial that DFAT seeks to continuously engage with stakeholders and external experts in order to more nimbly respond to the pace of changes on issues relating to digital rights and technology policy issues increasingly discussed at the international level.

Access Now encourages DFAT to build an emphatic respect for and commitment to human rights into its ‘roadmap for advancing and protecting Australia’s interests in a dynamic, complex and unpredictable international environment’.

This submission is a broad overview of the relevant issues of particular concern to Access Now. Further detail can provided, as required, as the development of the White Paper progresses.

Contact:
Brett Solomon
Executive Director

[Access Now](#)

