accessnow

The Hon Julie Bishop MP
Minister for Foreign Affairs
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600
Australia

Dr Tobias Feakin
Ambassador for Cyber Affairs
Department of Foreign Affairs and Trade
RG Casey Building
John McEwen Crescent
Barton ACT 0221
Australia

October 18, 2017

Dear Minister Bishop and Ambassador Feakin,

We write to congratulate you and your team on the launch of Australia's International Cyber Engagement Strategy (the Strategy).[1] We appreciated the opportunities to discuss the most pressing digital rights issues with the Ministry of Foreign Affairs and Trade.[2] To be a global leader, Australia should not only serve to positively influence global practices and norms but also implement stronger user protections, particularly for privacy, in Australia.

While the Strategy recognises many of the threats, the government's current practices do not necessarily live up to the principles of the Strategy. We call for an evaluation of current practices to ensure better protection of human rights, in line with the new Strategy, and also offer the following recommendations to improve the Australian government's cybersecurity approach and implementation going forward.

Access Now believes cybersecurity policies should be user centric, systemic, and anchored in an open and pluralistic process. Strong digital security is necessary to enable the exercise of human rights. There are consistently new and more sophisticated activities that interfere with rights, including phishing schemes, botnet attacks through conscripted Internet of Things devices, and attacks against public utilities and voting systems, all of which cause real-world damage. It may not be possible to totally eliminate many of these dangers, but Australia has an opportunity to lead the international effort to prevent, reduce, and mitigate these threats, consistent with human rights principles.

[1] http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html
[2] https://www.accessnow.org/cms/assets/uploads/2017/02/DFAT-White-Paper-Access-Now-submission.pdf

In recognition of your appreciation for constructive dialogue and partnership with civil society, we offer the following recommendations for the implementation of the Strategy to better engrain necessary protections for human rights.

Human Rights & Democracy Online

The Cyber Engagement Strategy sets forth a principle of international law and a commendable goal: to ensure that human rights apply online as they do offline. It acknowledges a commitment "to advocate to uphold and protect human rights and democratic freedoms online" (6.01). The Strategy mentions the particular relevance online of "the right to freedom of expression, the right to freedom of association, and the protection against arbitrary interference with privacy." The Strategy's emphasis on upholding these values globally is important because restrictions of human rights online as well as cyber-enabled interference in democratic processes are growing threats (6.02). However, the Strategy does not expressly recognise privacy as a right and fails to mention the full range of threats against it, including unnecessary and disproportionate government activity.

Explicit references to censorship and internet shutdowns signify a devotion to upholding protections for freedom of expression and association. In line with the strategy, the Australian government can uphold those values while publically and privately condemning measures used by other governments to disrupt internet access or censor expression. In addition to the human rights consequences, these shutdowns can have significant economic implications, undermining confidence and trust in sustainable and inclusive digital trade.[3]

Stronger protections for the right to privacy are essential not only for the protection of the right itself but as an enabler of other rights. The Australian government should further strengthen and clarify its pledge to protecting this right and addressing threats that arise in Australia and the Indo-Pacific region and beyond. Protections should be based on the principles of human rights as articulated in the International Principles on the Application of Human Rights to Communications Surveillance, including necessity, proportionality, and legality.[4]

To meaningfully protect privacy and other human rights means limiting activities that interfere with these rights, including dragnet surveillance and government hacking. On the latter, and as noted in the submission, government hacking operations implicate a number of user rights, including privacy, and threaten digital security. We commend the recognition of these risks, though we encourage the Australian government to conduct a thorough examination of current hacking operations and authorities to examine scope, scale, and justification. To comply with international law, certain types of hacking operations should be prohibited outright. If the government decides to continue with some hacking operations, they should support codification of protections for human rights. There is a connection between the strength of Australia's own practices in ensuring appropriate user protections with the effectiveness of its

[3] https://www.accessnow.org/keepiton/
[4] https://necessaryandproportionate.org/principles

international leadership, including its role in the establishment of norms of acceptable behaviour (4.02 – 4.04).

In addition to working with regional governments to raise awareness of states' human rights obligations online (6.03) and with law enforcement agencies dealing with cybercrime (3.05), we encourage the Australian government to support initiatives that build users' capacity to understand and improve protections for their own digital security and human rights. Any such initiatives can conform with the proposed cybercrime awareness training and skills development (3.01). This type of capacity building would complement the short term goal of providing 'guidance to ensure that human rights online are protected in Australian aid and non-government projects with digital technology components' (6.05). The development of digital security awareness is an area where civil society, including Access Now, can and do contribute expert advice in crafting guidance.

We welcome Australia's support of non-government organisations defending human rights online (6.04). As per our submission, we commend the Australian government for recognising the value of its membership in the Freedom Online Coalition and encourage a continued active role in its work.

To reiterate, we recommend that the Australian government:

Recommendation 1: Further strengthen and clarify the commitment to protecting privacy and addressing threats that arise in Australia and the Indo-Pacific region and beyond. Protections should be based on the principles of human rights as articulated by the International Principles on the Application of Human Rights to Communications Surveillance, including necessity, proportionality, and legality.[5]

Recommendation 2: Conduct a thorough examination of current hacking operations and authorities to examine scope, scale, and justification. To comply with international law, certain types of hacking operations should be prohibited outright. If the government decides to continue with some hacking operations, they should support codification of protections for human rights.

Recommendation 3: Support initiatives that build users' capacity to understand and improve protections for their own digital security and human rights.

Recommendation 4: Support and play an active role in the Freedom Online Coalition.

[5] https://necessaryandproportionate.org/principles

Internet Governance

Australia’s advocacy for a multi-stakeholder approach to internet governance (5.01) aids in inclusion of civil society in technical and policy discussions to ensure that human rights principles are embedded in the frameworks and institutions responsible for maintaining a free, open, and secure internet. We encourage civil society participation in the proposed community-led Australian internet governance and cooperation forum (5.02). However, it is important for Australian officials to take additional steps to ensure that this participation is meaningful and that civil society actors are not only given full access to conversations and documents in the policy-making process but are able to shape and influence the decisions.

To reiterate, we recommend that the Australian government:

Recommendation 5: Include civil society organisations, such as Access Now, in the creation of the Cyber Affairs Curriculum (8.02), and ensure effective participation in the proposed Advisory Group (8.05) to ensure adherence with human rights principles.

Cybersecurity

The protection of human rights should be at the heart of cybersecurity policy development. Efforts to promote cybersecurity must ensure the functioning of the open internet as a global network that can help realise human rights. The Strategy rightfully recognised the importance of ensuring that domestic operations comply with international law, particularly humanitarian law, to protect users. The Australian government should now articulate where it intends to commit resources to further international conversations and domestic processes that promote norms of international law to protect users.

The Strategy does not deal directly with encryption, either in the context of cybersecurity capabilities or human rights protections. The Australian Prime Minister’s stated plan to introduce legislation limiting the development and use of the strong encryption will undermine cybersecurity globally, harm online economies and digital trade, and infringe upon basic human rights.[6]

Access Now recently worked with a number of civil society organisations to demand respect for encryption from Australia and its Five Eyes allies.[7] If Australia is to claim a leadership role in the cybersecurity arena and to be consistent with its human rights commitments under the new strategy, it should start by publicly declaring its support for the development and use of strong digital security, like encryption.

In addition to security concerns, we suggest adding human rights principles to the list of factors to be taken into consideration during the design and development of ICT products,

[6] https://www.securetheinternet.org/

[7] https://www.accessnow.org/83-organizations-experts-5-nations-demand-five-eyes-respect-strong-encryption/

systems, and services (2.04). Encouraging companies to implement these principles will become even more important as connectivity expands, and internet-connected devices continue to proliferate.

To reiterate, we recommend that the Australian government:

Recommendation 6: Articulate how resources will be used to further international conversations and domestic processes that promote norms of international law to protect users.

Recommendation 7: Declare support for the development and use of strong digital security, like encryption.

Recommendation 8: Add human rights principles to the list of factors to be taken into consideration during the design and development of ICT products, systems, and services.

Cybercrime

The Strategy references the government's active participation in the negotiation of an Additional Protocol to the Budapest Convention on trans-border access to information (3.02). Access Now joined European Digital Rights (EDRi), the Australian Privacy Foundation, and several other civil society organisations to discuss the human rights implications of the proposed process.[8] We recognise the importance of effective police investigations, however, we encourage the Australian Government to use its position during this process to ensure full compliance with human rights principles and requirements.[9]

To reiterate, we recommend that the Australian government:

Recommendation 9: Condition support for the Budapest Convention Additional Protocol and other alternatives to the Mutual Legal Assistance Treaty system on inclusion of human rights protections,

Access Now welcomes opportunities to engage as you work to implement and refine the Strategy to better protect user rights. In addition, we invite you to present on the implementation of the Strategy at RightsCon Toronto in May 2018. Your perspective would be an invaluable and it would provide the opportunity to engage with the broader digital rights community.

We will be in contact with your office to extend an official invitation.

[8] https://www.accessnow.org/cms/assets/uploads/2017/09/CoE_cybercrime_2ndprotocol_globalsubmission_e-evidence.pdf

[9] https://www.accessnow.org/make-mlat-safe-harbor-safe-users/

In addition, we hope to meet with you to discuss these issues at the Global Conference on Cyberspace this November in India.

We look forward to your written response.

Brett Solomon
Executive Director
Access Now
brett@accessnow.org
+1 917 969 6077

Drew Mitnick
Policy Counsel
Access Now
drew@accessnow.org