HUMAN RIGHTS IN THE DIGITAL ERA

An International Perspective on Australia

accessnow

We defend and extend the digital rights of users at risk around the world

accessnow.org

TABLE OF CONTENTS

INTRODUCTION

Australia's role as a leading political and economic force in its region and around the world means it carries a critical responsibility in establishing and maintaining protections for human rights. Historically, Australia was a founding member of the United Nations and was significantly involved with drafting the Universal Declaration on Human Rights.[1] Australia acts as a geopolitical democratic stronghold in the Indo-Pacific region and a global economic leader,[2] and also ranks high internationally in terms of education and investment.[3] Australia has in many respects a unique position in the global security order, including as a member of the "Five Eyes" intelligence partnership, along with Canada, New Zealand, the United Kingdom, and the United States.[4]

Accordingly, Australia should be a global leader in serving as a champion for human rights, such as the right to privacy and rights to freedoms of expression and association.

Unfortunately, Australia has taken actions that indicate the nation is willing to undermine human rights as it adapts to the challenges of the digital era. It may be that in fact, Australia has expanded its surveillance laws and practices more since 9/11 than any other nation.[5] It is undoubtedly true that there are security threats created or facilitated by the existence of technology, including the internet, and, as in the physical world, responding to these threats is the responsibility of government. However, government is also responsible for recognizing and taking action to protect human rights, just as it was before the rise of modern technologies.

As the digital world continues to develop and technology increasingly becomes an intimate part of our daily lives — including through the growth in the use of artificial intelligence and Internet of Things devices — Australians are facing a choice. The country can either continue to be a testing ground for policies that undermine privacy and security in the digital era, or it can be a champion for human rights in the digital age, leveraging its relationships in the world to raise the standards for the next generation.

In this memorandum, we examine actions that Australia has taken that influence human rights in the digital age, nationally, regionally, and globally, and make recommendations for ways Australia can set a positive human rights agenda for the world to follow.

ABOUT ACCESS NOW

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon,[6] we fight for human rights in the digital age.

As part of this mission we operate a global Digital Security Helpline for users at risk to mitigate specific technical threats. We work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those who are most vulnerable. We serve on the European Commission Expert Group on the application of the General Data Protection Regulation, we are accredited with the United Nations Economic and Social Council, and we host RightsCon, the world's leading conference on human rights in the digital age.

We also work closely with a network of Australian digital rights and human rights organizations that understand the critical nature of these issues.[7] We coordinate frequently with academics, technologists, and the private sector to ensure Australia's human rights compliance in the digital age.

[1] https://www.humanrights.gov.au/publications/australia-and-universal-declaration-human-rights.

[2] Australia has one the highest Gross Domestic Products (GDPs) as a measure of its strength in the international economy. http://databank.worldbank.org/data/download/GDP.pdf. From 2017-2019, Australia is expected to rank 7th in terms of contributions to growth of the global GDP. https://www.weforum.org/agenda/2018/04/the-worlds-biggest-economies-in-2018/.

[3] *See* https://www.usnews.com/news/best-countries/australia; *see also* https://www.ft.com/content/e9fd9d6a-cf9f-11e5-986a-62c79fcbcead.

[4] The partnership facilitates the distribution of information and communications, as well as analysis and determinations, acquired through surveillance operations. https://ispydoc.com/select.

[5] https://www.theguardian.com/australia-news/ng-interactive/2015/oct/19/all-of-australias-national-security-changes-since-911-in-a-timeline.

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

[7] Many of these current issues are laid out here: https://digitalrightswatch.org.au/2018/05/14/the-state-of-digital-rights/.

ISSUE ONE: DIGITAL SECURITY AND ENCRYPTION

In July 2017, Prime Minister Malcolm Turnbull announced plans for legislation to compel device manufacturers and service providers to assist law enforcement in accessing encrypted information.[8] Foreign Minister Julie Bishop echoed this request a few months later, declaring Australia would want to work "with communications service providers to prevent terrorists from using encryption to hide online."[9] In May 2018, the Minister for Law Enforcement and Cybersecurity, Angus Taylor, stated that decryption legislation remained a top priority.

To some in law enforcement, encryption presents challenges in obtaining data from criminal suspects. However, encryption is not simply used by criminals, but by all internet users. Because of its reliability, encryption is often described as the best-known method for protecting digital information for financial services, journalism, human rights activism, and commercial privacy.

Many governments have, however, looked for a way to weaken encryption. Yet encryption is based on the fundamentals of mathematics, and technologists and cryptographers have consistently made clear that it is not possible to undermine encryption without having significant, serious impacts on the security of everyday communications and transactions, including transactions with banks, hospitals, and retail enterprises, among others.[10]

In 2016, Access Now formed a global coalition to call on government leaders around the world to support encryption.[11] We explained how encryption not only protects our global economy and prevents crime, but also protects human rights, citing the United Nations Special Rapporteur for Freedom of Expression, who observes, "encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age."[12] Today, there are more than 400 named organizations, experts, and companies who have joined that coalition, hailing from more than 60 countries around the world.

While Australian officials, including Law Enforcement and Cybersecurity Minister Angus Taylor, continue to clamor for a legal regime for limiting access to and use of encryption,[13] leading digital rights groups across Australia, including FutureWise, Electronic Frontiers Australia, Digital Rights Watch, and the Australian Privacy Foundation, have launched a petition asking Members of Parliament to publicly affirm support for strong encryption.[14] Shortly after the petition was launched, the Australian Senate passed a motion calling for Australia to support development and use of strong encryption, resist other governments' demands to weaken encryption, and "work with law enforcement to develop alternative avenues to obtain information through warrants and targeted surveillance that does not put every Australian at greater risk of identity theft."[15]

RECOMMENDATIONS

In July 2018, Access Now led a coalition of 76 organizations, companies, and experts from across Australia and the world in a letter to Members of Parliament, explaining, "in order to fully realize the benefits of the digital space, Australia must fully and unequivocally commit to a strong foundation for digital security."[16] Accordingly, Access Now calls on Australia to:

- **Act as a global leader in decisively ending the government's pursuit of legislation to undermine encryption or force developers to modify their products to ensure law enforcement or intelligence access**;
- **Establish a vulnerabilities disclosure process and protect security research;**
- **Prioritize digital security for Australians, including through support for the development and use of strong encryption both domestically and on the international stage; and**
- **Invest in research and development on encryption and digital security to protect Australians and people around the world.**

[8] https://www.gizmodo.com.au/2017/07/everything-that-went-down-at-malcolm-turnbulls-encryption-law-announcement/.
[9] http://www.zdnet.com/article/australia-looks-to-deny-encryption-to-terrorists/.
[10] https://www.accessnow.org/cms/assets/uploads/2018/01/Crypto-Australia-Memo.pdf.
[11] https://www.accessnow.org/announcing-a-global-coalition-demanding-security-for-all/.
[12] securetheinternet.org.
[13] http://minister.homeaffairs.gov.au/angustaylor/Pages/speech-sydney-institute.aspx.
[14] https://secureaustralia.org.au/.
[15] https://www.theregister.co.uk/2018/03/28/australian_senate_passes_motion_saying_encryption_is_very_useful/
[16] *See* https://www.accessnow.org/global-coalition-calls-on-australias-government-to-reject-plans-to-undermine-encryption/

ISSUE TWO: GOVERNMENT SURVEILLANCE IN THE DIGITAL AGE

Australia has one of the most extensive surveillance legal schemes in the world. Laws to facilitate surveillance include the Telecommunications (Interception) Act 1979,[17] the Telecommunications Act 1997,[18] the Surveillance Devices Act 2004,[19] and the so-called terror laws of 2014-2015,[20] including the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.[21]

Australia is also a member of the "Five Eyes," an intelligence sharing partnership that facilitates the distribution of information and communications, as well as analysis and determinations acquired through surveillance operations. As a Five Eyes member, Australia is expected to host the next Five Eyes Ministerial meeting in August 2018. Through the Five Eyes partnership, Australia's surveillance regime has an impact far beyond its domestic borders, with information collected under these authorities frequently being handed over to authorities in other governments with a history of overreach and abuse.

Australia is not a stranger to misuse of surveillance authorities. In fact, investigative reporter Glenn Greenwald has said Australia is "one of the most aggressive countries that engage in mass surveillance as a member of the Five Eyes Partnership."[22] Documents have detailed Australia's programs aimed at surveillance of other nations in the Indo-Pacific region, including to gain an advantage in trade negotiations with East Timor.[23]

In the past, Reporters Without Borders has listed Australia as a "country under surveillance," alongside 13 other countries, including Egypt, Kazakhstan, India, Russia, and Turkey.[24]

In recent years, Australia has continued to pursue invasive surveillance programs, introducing government hacking tools,[25] high-tech surveillance drones,[26] and persistent location tracking,[27] all without the necessary and proper legal safeguards in place.

One example of the expanding use of technology for surveillance in Australia is the government's plans to connect public and private closed-circuit television (CCTV) monitoring systems around Australia to facial recognition databases.[28] The Identity-Matching Services Bill 2018 and the Australian Passports Amendment (Identity-Matching Services) Bill 2018 will allow scans to be run through existing biometric databases in real time, greatly increasing not only potential for abuse of the system, but incentives for massive collection of biometric data.[29] Facial recognition programs are so invasive, and have such a high propensity for error and bias, that some academics have called for them to be banned outright.[30] In July 2018, Microsoft President Brad Smith stated, "Facial recognition technology raises issues that go to the heart of fundamental human rights protections like privacy and freedom of expression."[31]

We live in an era when the cost of conducting invasive surveillance is at an all-time low and the data collected can be stored indefinitely. To protect our right to privacy, experts came together to develop the International Principles on the Application of Human Rights to Communications Surveillance.[32] Now endorsed by over 600 organizations, the Principles provide guidance for ensuring digital surveillance remains consistent with human rights.

[17] https://www.legislation.gov.au/Details/C2018C00201.

[18] https://www.legislation.gov.au/Details/C2018C00161.

[19] https://www.legislation.gov.au/Details/C2018C00188.

[20] https://www.accessnow.org/global-state-of-surveillance-australias-terror-laws-set-to-erode-human-righ/.

[21] https://www.legislation.gov.au/Details/C2015A00039.

[22] https://www.bbc.com/news/world-australia-33017638.

[23] https://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone; https://thediplomat.com/2013/12/east-timor-australia-spying-scandal/.

[24] https://issuu.com/rsf_webmaster/docs/rapport-internet2012_ang?backgroundColor=%2523222222.

[25] https://motherboard.vice.com/en_us/article/4xezgg/australian-dark-web-hacking-campaign-unmasked-hundreds-globally.

[26] https://www.businesstimes.com.sg/government-economy/australia-buys-high-tech-drones-to-monitor-south-china-sea-pacific.

[27] https://theconversation.com/why-electronic-surveillance-monitoring-may-not-reduce-youth-crime-97864.

[28] https://thenewdaily.com.au/news/national/2017/10/15/facial-recognition-video-surveillance/; https://www.zdnet.com/article/please-run-australias-facial-recognition-surveillance-system-on-the-ato-san/.

[29] https://www.zdnet.com/article/legislation-for-australian-automated-facial-recognition-enters-parliament/.

[30] https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facial-recognition-may-be-coming-to-a-police-body-camera-near-you/?utm_term=.1e848ce29fda

[31] https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/.

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

RECOMMENDATIONS

The rapid growth and development of technology accompanied by the falling cost of storing and mining large sets of data makes government surveillance possible at an unprecedented scale. Accordingly, Access Now calls on Australia to:

- **Endorse the International Principles on the Application of Human Rights to Communications Surveillance;[32]**
- **Commit to conducting a full human rights impact assessment of current surveillance laws and practices before any new surveillance authorities or programs are implemented. The Australian Human Rights Commission current inquiry into the impact and opportunities of new technologies to protect and promote our rights and freedoms would be a good opportunity to begin that process.[33]**
- **Update any and all human rights assessments periodically as the technology advances or programs change; and**
- **Encourage other government leaders, including at the upcoming Five Eyes Ministerial Meeting, to pursue a human rights-centered review of the role of technology in the scope and scale of surveillance activities and examine what protections are needed to protect people in the digital age.**
- **Prohibit the use of biometric tools, including facial recognition, for crowd tracking and monitoring. Where biometric information is collected and stored it must be secured, de-centralized, and subject to data protection safeguards, including rights to notice and correct.**

ISSUE THREE: DATA PROTECTION

Australians care deeply about online privacy.[34] A study by the Digital Rights and Governance Project at the University of Sydney found that 80% of Australians want to know how their information is being accessed and by whom, while 67% of Australians affirmatively take steps to protect their privacy online. Notably, only 38% reported actually feeling in control of their online data.

Despite these gaps, Australia has never established a legal right to privacy. Moreover, while most Australian states and territories have their own data protection laws,[35] the patchwork is inadequate to ensure that personal data is actually protected. Some additional protections exist in state and federal laws in specific sectors, but their applications are fairly narrow.[36] The Privacy Act 1988 affords some protections to privacy and data in the form of the "Australian Privacy Principles," but these, too, fall short because they fail to provide affirmative rights or obligations.[37]

RECOMMENDATIONS

Data protection is an urgent matter. Reports indicate that the Australian Privacy Commissioner could seek court-ordered penalties up to $2.1 million against Facebook after allegations of bad data practices.[38] However, this may not be enough to curb ongoing misuse or abuse of user data, nor to mitigate harm or offer redress. Accordingly, Access Now calls on Australia to:

- **Establish clear rights to privacy and data protection in Australian law or within a Bill of Rights,[39] including statutory avenues for seeking remedy and redress;[40]**
- **Pursue a federal data protection law, drafted transparently and with feedback from all stakeholders, which provides clear, affirmative rights for individuals and obligations for all entities that process data; and**
- **Encourage industry to implement a "privacy by design" approach that recognizes and incorporates privacy as a central tenant at all stages of product development.**

[32] https://tech.humanrights.gov.au/our-work

[34] http://digitalrightsusyd.net/research/digital-rights-in-australia-report/.

[35] https://www.dlapiperdataprotection.com/index.html?t=law&c=AU. Exceptions are Western and South Australia.

[36] *Id.*

[37] https://www.legislation.gov.au/Details/C2018C00034. The ambit of the definition of "personal data" was recently called into question in the case of Privacy Commissioner v Telstra Corporation. In this case, it was noted that metadata relating to the operation of a mobile service is not "about an individual" but about a service, it would not qualify as personal information. *See also* https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles; https://digitalrightswatch.org.au/wp-content/uploads/2018/05/State-of-Digital-Rights-Web.pdf.

[38] https://www.news.com.au/technology/online/social/facebook-inquiry-australia-privacy-commissioner-launches-investigation-into-data-scandal/news-story/3331f39671d4e74068031da3c02f4315

[39] https://www.hrlc.org.au/news/five-things-for-our-new-pms-human-rights-to-do-list ("Australia is the only western democratic nation that doesn't have a national Human Rights Charter or a bill of rights. We know from experience that when human rights are not protected in law, they are always in danger of being eroded. ").

[40] *See, e.g.*, https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf. See also https://www.computerworld.com.au/article/643619/imf-bentham-flags-facebook-lawsuit-over-privacy-breaches/.

ISSUE FOUR: CYBERSECURITY

In 2016, 60% of Australian businesses experienced at least one disruptive security breach every month, and between 2016-2017 companies saw a 15% increase in cyber incidents.[41] Social Services Minister Dan Tehan said, "over the course of 2016-17, reports to the ACSC indicated losses of over $20m due to business email compromise." The figures are likely considerably higher than that, and will undoubtedly grow exponentially over time.

In 2017, Australia launched a new International Cyber Engagement Strategy, intended to expand on "how Australia will attain global responsibility and influence in cyberspace."[42] It includes goals in eight subject areas ranging from human rights and democracy to cybersecurity. In response, Access Now wrote to Tobias Feakin, Australia's Ambassador for Cyber Affairs, explaining that while the strategy makes mention of the rights to freedom of expression and association, it fails to show similar regard for privacy, not referring to it as a right and making reference only to "arbitrary interferences" to privacy instead of unlawful, disproportionate, and unnecessary infringements.[43]

Despite its goals, the strategy also fails to recognize that the government's own current actions, including engagement in government hacking and threats to encryption, actually run counter to the commitments in the document.[44] This is an important and significant challenge for Australian public policy that must be addressed.

While Australia's focus on cybersecurity has increased, the impact is not yet clear. The Privacy Amendment (Notifiable Data Breach) Act 2017 obligates companies to notify its users of breaches of data.[45] However, reports suggest that the law may be soft on companies, and may provide too many exemptions.[46] Even so, in only the first six weeks of Act's applicability, companies reported more than 63 data breaches to the Office of the Australian Information Commissioner.[47]

RECOMMENDATIONS

The Australian government is investing heavily in cybersecurity, including a $50 million Cooperative Research Centre to build Australia's cybersecurity capability and deliver solutions to ensure the safety of our businesses and citizens in cyberspace.[48] In response, an industry group has announced its intent to triple the size of the Australian cybersecurity industry.[49] These expansions will make the inclusion of human rights safeguards vital to ensuring that Australian citizens' rights do not become collateral damage. Accordingly, Access Now calls on Australia to:

- **Commit to building cybersecurity policies and practices around central tenets of human rights, including the right to privacy. This includes compliance with the government's own Cyber Engagement Strategy commitments on human rights and democracy;[50]**
- **Evaluate government hacking law and practice with the goal of either ending the practice or, at minimum, codifying statutory safeguards to protect human rights;**
- **Ensure representatives from civil society and the public are meaningfully included in cybersecurity policy-making, including the ability to participate in drafting key documents; and**
- **Strengthen data breach notification in Australia to ensure full compliance by the public and private sectors.**

[41] http://www.abc.net.au/news/2017-06-09/cybersecurity-skills-shortage-putting-australia-at-risk-expert/8601426; https://www.computerweekly.com/news/450428181/Australias-state-of-cyber-security-report-reveals-rise-in-phishing-attacks.

[42] http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_6_human_rights_and_democracy_online.html.

[43] https://www.accessnow.org/cyber-engagement-strategy-australia-overlooks-threats-user-rights/.

[44] *Id.*

[45] https://www.legislation.gov.au/Details/C2017A00012.

[46] https://www.csoonline.com/article/3252091/privacy/mandatory-breach-notification-is-not-a-silver-bullet.html.

[47] https://www.theaustralian.com.au/business/technology/australia-needs-to-do-more-on-data-protection/news-story/1d2abaf1fd4fcef8911fafaaefb2b2b9.

[48] http://minister.industry.gov.au/ministers/craiglaundy/media-releases/50-million-investment-cyber-security-research-and-industry.

[49] https://www.acsgn.com/cyber-security-sector-competitiveness-plan/.

[50] http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_6_human_rights_and_democracy_online.html

ISSUE FIVE: INFRASTRUCTURE AND CONNECTIVITY

Australia currently ranks 56th on the Speedtest Global Index, which provides monthly rankings of mobile and fixed broadband internet speeds.[51] Despite its poor performance, increasing reach and performance of digital networks is not even mentioned in numerous key documents discussing development in Australia.[52] A lack of proper planning for connectivity has reportedly led to so-called foreign interests stepping in to fill the gaps,[53] leading to last-minute interventions by the Australian government.[54]

The UN Sustainable Development Goals, a set of high-level goals and sub-targets on environmental, social, cultural, and economic indicators launched as part of the UN 2030 Agenda for Sustainable Development, cannot be met without broadly expanding open and secure access to the global internet. Existing gaps in internet access for many Indigenous and rural residents adversely impact public health outcomes.[55] In particular, Indigenous communities must be brought to the table in setting broadband and media development agendas and continually consulted throughout project planning and implementation.[56] More affordable and equitable access to both fixed and mobile connections, via innovative last mile solutions, along with digital literacy capacity building, will help bridge gaps and grow the digital economy.[57]

Internet shutdowns, or the deliberate disruption of the internet and mobile apps as ordered by government, are also a growing trend across their region, and have negative impacts on freedom of expression, journalism, emergency services, businesses, human rights defenders, and demonstrators.

Access Now developed the Human Rights Principles for Connectivity and Development[58] to guide stakeholders to equitably and openly extend the benefits of information and communications technologies within a human rights framework. A human rights-based approach to planning, development, and rollout of improved broadband infrastructure requires close consultation with vulnerable communities at every stage. The principles provide key insights to bridge gender and affordability gaps while respecting the human rights to privacy and freedom of expression, as well as procedural steps to ensure transparency and equity.

RECOMMENDATIONS

Internet access could provide significant benefit to populations that are currently unserved or underserved, but it must be developed with human rights in mind. Accordingly, Access Now calls on Australia to:

- **Endorse and implement the Human Rights Principles for Connectivity and Development to ensure all communities have agency over broadband internet access plans;[59]**
- **Unequivocally condemn internet shutdowns, particularly in countries that rely on Australian infrastructure;[60] and**
- **Pursue a clear, proactive plan to provide high speed, affordable, and resilient connectivity to the open internet for un- and underserved populations across Australia and the region, with a particular focus on consultation with and connectivity for Indigenous communities.**

[51] https://www.speedtest.net/global-index#mobile.

[52] *See, e.g.*, http://northernaustralia.gov.au/sites/prod.office-northern-australia.gov.au/files/files/NAWP-FullReport.pdf (not a single mention of the internet or digital network connectivity).

[53] https://www.asia-pacificresearch.com/pushing-chinas-huawei-out-australia-the-solomon-islands-and-the-internet/5628083.

[54] https://www.arnnet.com.au/article/642650/vocus-wins-136m-australian-govt-contract-build-new-subsea-cable.

[55] http://www.abc.net.au/news/rural/2016-06-21/almost-half-of-regional-australia-reports-internet-very-poor/7529734; https://ama.com.au/position-statement/better-access-high-speed-broadband-rural-and-remote-health-care-2016.

[56] https://irca.net.au/about/policy

[57] http://broadbandforthebush.com.au/key-messages; see also http://broadbandforthebush.com.au/wp-content/uploads/2018/01/B4BA-NT-Digital-Strategy-final.pdf

[58] https://www.accessnow.org/cms/assets/uploads/2016/10/The-Human-Rights-Principles-for-Connectivity-and-Development.pdf

[59] https://www.accessnow.org/cms/assets/uploads/2016/10/The-Human-Rights-Principles-for-Connectivity-and-Development.pdf.

[60] https://www.accessnow.org/why-is-a-tiny-island-nation-facing-an-internet-shutdown/.

CONCLUSION

Australia, with its long commitment to democratic institutions, is strategically placed to become a beacon for human rights in the digital age. There is significant need for Australian leadership in the Indo-Pacific region. As a leading common law country in the region and a member Commonwealth of Nations, Australia has the opportunity for setting norms at home and across the region that establish a human rights-centric approach to governance and connectivity.

However, Australia also risks turning its back on its ideals. While we commend actions taken by the public and private sectors in Australia — including the periodic publishing of transparency reports[61] — and note the imperatives of national security and protecting citizens, we warn against the steps that both government and corporate actors have taken that would undermine human rights domestically and around the world.

The public policy decisions that are being made right now with regard to the issues raised in this briefing will impact generations to come. It is therefore vital that Australia takes pause, reflects, and then leads in advancing policy that safeguards human rights and sets an example for other countries can follow.

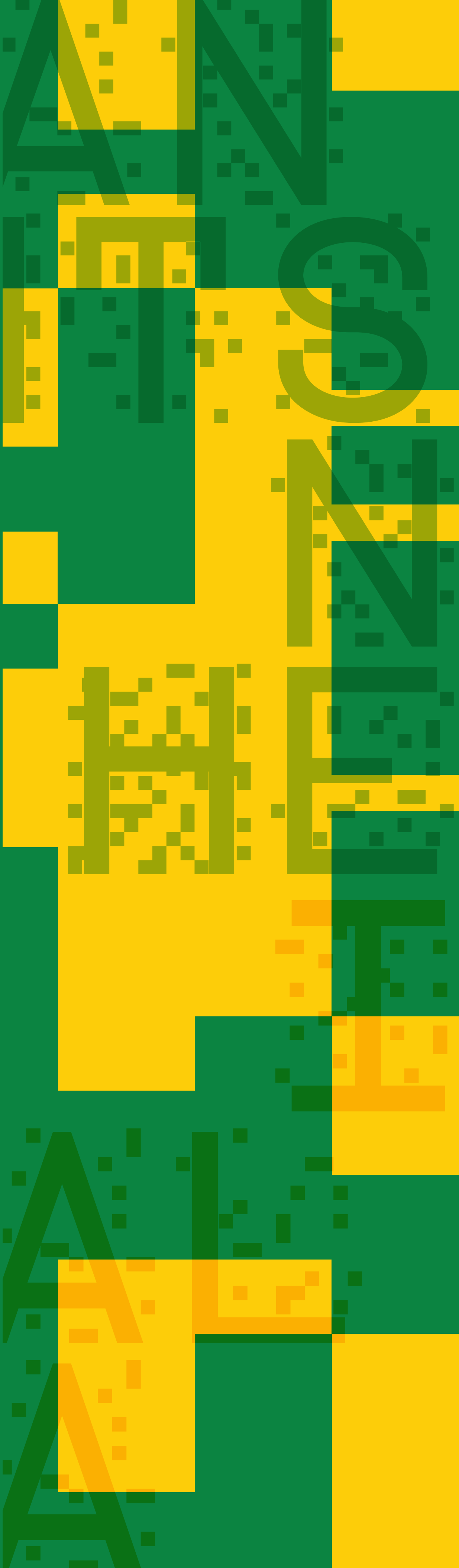
FOR MORE INFORMATION

Brett Solomon | Executive Director
brett@accessnow.org

Amie Stepanovich | Global Policy Counsel
amie@accessnow.org

https://www.accessnow.org

[61] https://www.accessnow.org/australian-telco-telstra-releases-first-transparency-report/.



Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.