# STATE OF DIGITAL RIGHTS

KEY RECOMMENDATIONS

**Digital rights are inherent human rights.** And just as other human rights are far from inalienable, digital rights must be fought for, solidified into social normality and ultimately protected and upheld if we are to maintain our humanity in digital spaces.

Upholding digital rights requires us to find the balance between the opportunity the internet provides us to live better, brighter and more interconnected lives, and the threat, posed by trolls, corporations and government. Ideally it will involve law making that includes educated community participation and generates nuanced public debate.

*The State of Digital Rights* report analyses a select few of the key digital rights issues facing Australians today - the full list of recommendations from the report listed here. A critical step towards upholding our human rights in a technological age is to understand that digital rights are human rights that are expressed online. We must protect these rights, whatever the cost.

**Repealing metadata retention**

- The Australian Government should immediately repeal the metadata retention regime or introduce significant amendments to existing legislation to put in place proper safeguards consistent with the rights to privacy and freedom of expression.

**Protecting privacy**

- The Australian Government should introduce legislation that respects and upholds the right to digital privacy and to data protection.
- Investigate the creation of a similar body to the European Data Protection Authorities and task this body with upholding and monitory privacy protections, including digital rights in the workplace.
- Explore the possibility of a 'right to disconnect' that would regulate employer's use of digital tools to make sure that this does not encroach on statutory periods of rest and holidays of employees.
- Privacy, data protection, anti-discrimination, right to explanation, and review and appeal regulatory structures and policy frameworks should be considered in localised contexts, prior to implementation of big data policing and algorithmic profiling.
- Implement the 2014 Australian Law Reform Commission recommendations for the introduction of a Commonwealth statutory civil cause of action for serious invasions of privacy, including digital privacy.
- Expand the definition of sensitive information under the Privacy Act to specifically include behavioural biometrics.
- Increase measures to educate private businesses and other entities of their responsibilities under the Privacy Act regarding behavioural biometrics, and the right to pseudonymity.
- Investigate the development of a free and easily accessible national data and movement-tracking opt-out register for people who do not want their sensitive data to be collected for commercial uses.
- Introduce a compulsory register of entities that collect static and behavioural biometric data, to provide the public with information about the entities that are collecting biometric data and for what purpose.

**Intelligence sharing operations**

- The loopholes opened with the 2011 reform of the FOI laws should be closed by returning ASD, ASIO, ASIS and other intelligence agencies to the ambit of the FOI Act, with the interpretation of national security as a ground for refusal of FOI requests being reviewed and narrowed.
- A new agreement negotiated among the Five Eyes governments that any information held by the United States on nationals of the other countries

be stored only within the borders of that country and unless directly related to a national security operation or criminal trial, be accessible only with the approval of the home government, with an annual report of how many requests for access have been made.

- A complete cessation of commercial espionage conducted by the Australian Signals Directorate.
- Expansion of powers of the Joint Parliamentary Committee on Intelligence and Security to initiate its own reviews into operational matters.

**Protecting encryption**

- The Australian Government should not weaken encryption protocols through any method as a matter of principle.
- The government should focus on the reform of Mutual Legal Assistance Treaties instead of weakening encryption to purportedly improve law enforcement process.

**Computer network operations**

- There is a need for greater clarity and specificity in law that allow for CNOs in order to comply with democratic norms such as proportionality and rule of law;
- Standards and procedures should be implemented to ensure clarity and transparency in the conduct of extraterritorial investigations, including those involving honeypot or CNOs, with specific regard to ensuring basic standards for determining the admissibility of evidence from remote forms of police surveillance;
- Attempts should be made to improve communications between government agencies under Mutual Legal Assistance Treaties (MLAT) processes, rather than removing these requirements, and the due process procedural safeguards they promote, which has been done via the CLOUD Act

**Copyright reform**

- The Australian Government should ensure that copyright laws that are flexible, transparent and provide due process to users, through:
  - Include proper due process and privacy safeguards in the website blocking regime.
  - Extension of a safe harbour provisions to all Australian online service providers.
  - Inclusion of a broad, general purpose, 'fair use style' exception to infringement in the Copyright Act 1968.

**Content moderation**

- Telecommunications providers and internet platforms must develop processes to increase transparency in content moderation by clearly explaining:
  - what content has been removed or triggered an account suspension,
  - who was responsible for making a decision to remove a user's content or suspend their account.
  - why a decision was made (including the specific rule that has been breached).
  - how the moderation system was triggered, including a description of the role of algorithms, other users, law enforcement agencies, other third parties, and internal decision-makers in flagging, detecting, or evaluating prohibited content.

**Protecting children online**

- Ensure that Australian policy and practice community address all three dimensions of children's rights in relation to the digital world: a) children's access to digital media; b) their rights in online spaces, and how digital media can be harnessed to deliver on a broad range of children's rights.
- Australian research, policy and practice must endeavour to minimise the potential harms and maximise the benefits of online engagement for Australian children. and to adopt a child rights approach to governance, research and program delivery in relation to children's use of digital media.
- Actively engage children and young people in developing responses that protect their rights to provision, protection and participation in the digital age, and develop child-centred measures of impact.
- The rights of disadvantaged children must be centred more consistently across Australian research, policy and practice interventions of online engagement, including investment into research that examines both the potential harms and benefits of children's digital media use.
- Continued support for the eSafety Commissioner's Office and further mechanisms to support cross-sector knowledge sharing; ongoing research; policy development; and evidence-based programmatic responses.
- The Australian Government should lend support to the Case for a General Comment on Children and Digital Media to guide states, NGOs and corporations in their interpretation of the Convention on the Rights of the Child.

*The State of Digital Rights Report 2018* was coordinated and produced by Digital Rights Watch, a charity organisation founded in 2016 whose mission is to ensure that Australian citizens are equipped, empowered and enabled to uphold their digital rights. The full report can be found at digitalrightswatch.org.au