Joint statement urging the Australian government to protect end-to-end encryption in the statutory review process of the Online Safety Act

End-to-end encryption plays a crucial role in ensuring the safety, security and privacy of millions in Australia. However, the statutory review of the Australian Online Safety Act erroneously characterises end-to-end encryption as an obstacle to online safety and law enforcement, instead of recognising that it is essential for online security and weakening it reduces safety for all.

The Online Safety Act risks becoming forever known as the Online 'Un-safety' Act if strong protections for communications and stored information secured by end-to-end encryption are not included in the Act. Without clear protections, the eSafety Commissioner will soon implement industry standards under the Australian Online Safety Act that effectively force service providers to weaken or circumvent end-to-end encryption to monitor and intercept communications.

These measures would weaken the security, confidentiality and integrity of communications while they are transmitted or in storage. A failure to safeguard end-to-end encryption will make all Australians and people around the world less safe, not more.

Further, the addition of a general duty of care to the Act, without safeguarding encryption, suggests compelling service providers to remove or circumvent the confidentiality of end-to-end encryption in order to meet their duty of care obligations. This would pave the way for pervasive surveillance and damage online safety as well as the human rights to privacy and free expression.

End-to-end encryption not only protects children from bad actors harvesting their personal data or intercepting and taking over their communications – it also protects children by preventing their personal data from being used for profiling and advertising.

We urge the Australian government to utilise the Online Safety Act review process to course correct and actively protect and encourage the use of end-to-end encryption. Doing so would benefit people, businesses, and governments and would be crucial to achieving the goal of the Online Safety Act.

Signatories:

Access Now
ARTICLE 19
Assembly Four
Bangladesh NGOs Network for Radio and Communication
Betapersei S.C.
Big Brother Watch

Blacknight Internet Solutions Ltd (Blacknight)
Center for Democracy & Technology
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Connect Rurals
Cybersecurity Advisors Network (CyAN)
cyberstorm.mu
Digispace Africa
Digital Rights Watch
Electronic Frontier Finland
Electronic Frontiers Australia
Encryption Europe
Fight for the Future
Gate 15
Global Partners Digital
Human Rights Journalists Network Nigeria
Inclusive Design Institute / WebQ
Internet Australia
Internet Freedom Foundation
Internet Governance Project
Internet Society
Internet Society Ethiopia Chapter
Internet Society Guatemala Chapter
Internet Society Tanzania Chapter
Internet Society UK England Chapter
JCA-NET(Japan)
Keexle
LGBT Tech
Mozilla
Myntex
New America’s Open Technology Institute
OpenMedia
Organization for Digital Africa
Parsec
Phoenix R&D GmbH
Privacy & Access Council of Canada
Proton
Quilibrium, Inc.
SecureCrypt
SeeZam S.A.
Software Freedom Law Center India (SFLC.IN)
Surfshark
Tech for Good Asia
The Tor Project
Three Steps Data

Tuta
West Africa ICT Action Network
West African Digital Rights Defenders coalition