ONLINE SAFETY ACT

EXPOSURE DRAFT SUBMISSION

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

EXECUTIVE SUMMARY

AISA welcomes the request for submissions from the Australian Government's Department of Infrastructure, Transport, Regional Development and Communications in relation to the Exposure Draft for the proposed Online Safety Bill, a Bill that seeks to enhance the existing protections contained within the *Enhancing Online Safety Act 2015* (Cth).

The Australian Information Security Association (AISA) champions the development of a robust information security and privacy sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. Established in 1999 as a nationally recognised and independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security, safety and privacy in Australia. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA's vision is a world where all people, businesses and governments are educated about the risks and dangers of invasion of privacy, cyber-attack, and data theft and to enable them to take all reasonable precautions to protect themselves. AISA was created to provide leadership for the development, promotion, and improvement of our profession, and AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education, and organisational excellence.

This response offered by AISA represents the collective views of over 7,000 cyber security, information technology and privacy professionals, allied professionals in industries such as the legal, regulatory, financial and prudential sector, as well as cyber and IT enthusiasts and students around Australia. AISA members are tasked with protecting and securing public and private sector organisations including national, state and local governments, ASX listed companies, large enterprises, NGO's as well as SME/SMBs across all industries, verticals and sectors.

AISA proactively works to achieve its mission along with its strategic partners. These include the Australian Cyber Security Centre, AustCyber, Cyrise, the Risk Management Institute of Australia (RMIA), the Australian Strategic Policy Institute (ASPI), the Australian Institute of Company Directors (AICD), the Oceania Cyber Security Centre (OCSC), the Australian Security Industry Association Limited (ASIAL) as well as international partner associations such as $(ISC)^2$, the Center for Cyber Safety and Education, ISACA and the Association of Information Security Professionals (AiSP).

It is AISA's hope that the Department of Infrastructure, Transport, Regional Development and Communications will consider our responses to the exposure draft for the proposed Online Safety Bill to ensure privacy settings and online safety protections empower consumers, protect their data and best serve the interests of all Australians.

TABLE OF CONTENTS

EXECUTIVE SUMMARY **1**

TABLE OF CONTENTS **2**

1. BASIC ONLINE SAFETY EXPECTATIONS **4**

DEFINITION 4
CORE BASIC ONLINE SAFETY EXPECTATIONS 4
REPORTING 4
COMPLIANCE AND ENFORCEMENT 4
PUBLIC DISCLOSURE 4

2. CYBER-BULLYING SCHEME **5**

DEFINITION 5
COMPLAINTS 5
REMOVAL NOTICES 5
COMPLIANCE AND ENFORCEMENT 5
PUBLIC DISCLOSURE 5

3. ADULT CYBER-ABUSE SCHEME **6**

DEFINITION 6
COMPLAINTS 6
REMOVAL NOTICES 6
COMPLIANCE AND ENFORCEMENT 6
PUBLIC DISCLOSURE 6

4. IMAGE-BASED ABUSE SCHEME **7**

DEFINITION 7
COMPLAINTS 7
REMOVAL NOTICES 7
COMPLIANCE AND ENFORCEMENT 7
PUBLIC DISCLOSURE 7

5. ONLINE CONTENT SCHEME **8**

CLASS 1 MATERIALS **8**
DEFINITION 8
COMPLAINTS 8
REMOVAL NOTICES 8
COMPLIANCE AND ENFORCEMENT 8
FEDERAL COURT ORDER 8
CLASS 2 MATERIALS **9**

Definition 9
Complaints 9
Removal Notices 9
Compliance and Enforcement 9
Federal Court Order 9
Industry Codes, Standards, Etc 10
Definition 10
Complaints 10
Directions 10
Compliance and Enforcement 10
Federal Court Orders 10

6. ABHORRENT VIOLENT MATERIAL BLOCKING SCHEME 11

Definition 11
Complaints 11
Blocking Request and Blocking Notice 11
Compliance and Enforcement 11
Limitations and Exemptions 11

7. GOVERNANCE ARRANGEMENTS 12

ABOUT THE LEAD AUTHOR 13

1. Basic Online Safety Expectations

Definition
AISA supports the definition contained under ss 45-47 of the proposed Bill.

Core Basic Online Safety Expectations
AISA supports the Core Basic Online Safety Expectations contained under ss 45-46 of the proposed Bill.

Reporting
AISA supports the reporting requirements placed on service providers and classes of service providers as specified under ss 49, 52, 56, 59 on the basis that reporting requirements are reasonable in nature and do not place an unreasonable burden on service providers. AISA recommends that the Department consider some form of scheme that allows a service provider to seek government assistance and support for costs associated with extensive reporting requirements which may place an onerous burden on a service provider.

Compliance and Enforcement
AISA supports the compliance and enforcement mechanisms contained within ss 50, 53, 57, 60, 163 of the proposed Bill.

Public Disclosure
AISA supports the public disclosure arrangements contained under ss 48, 55, 62 of the proposed Bill.

2. Cyber-bullying Scheme

Definition
AISA supports the definition contained under s 6 of the proposed Bill.

Complaints
AISA supports the provisions detailed in ss 30, 31, 65 of the proposed Bill in relation to how to receive, investigate and action complaints from a victim of cyber bullying.

Removal Notices
AISA supports the general provisions detailed in ss 65, 66, 70 of the proposed Bill in relation to the removal of materials deemed to constitute cyber-bullying.

Compliance and Enforcement
AISA considers that the civil penalty for non-compliance by service providers is appropriate (500 penalty units defined under s 67) as well as measures contained under s 69. AISA supports the civil penalty provisions for service providers contained under Part 10 of the proposed Bill.

AISA supports the provision for end-users to comply with a removal notice and respects the consideration placed on the avoidance of civil penalties given that the perpetrator is often a minor in cyber-bullying cases. AISA notes and supports s 71 and its enforceability under the *Regulatory Powers Act.* AISA is of the view that where a perpetrator is in fact an adult, cases of cyber-bullying deemed to be egregious by the Commissioner or where there is wilful non-compliance by the perpetrator may warrant the addition of a civil penalty. AISA recommends the inclusion of such a provision.

Public Disclosure
AISA supports the public disclosure arrangements contained under ss 69, 73.

3. Adult Cyber-abuse Scheme

Definition
AISA supports the definition contained under s 7 of the proposed Bill.

Complaints
AISA supports the provisions detailed in ss 36, 37, 88 of the proposed Bill in relation to how to receive, investigate and action complaints from a victim of adult cyber-abuse.

Removal Notices
AISA supports the general provisions detailed in ss 88, 89, 90, 93 of the proposed Bill in relation to the removal of materials by social media services, electronic services, internet services, hosting services and end-users deemed to constitute adult cyber-abuse.

Compliance and Enforcement
AISA considers that the civil penalty for non-compliance by service providers is appropriate (500 penalty units defined under s 91) as well as measures contained under ss 92, 163, 164, 165. AISA supports the civil penalty provisions for service providers contained under Part 10 of the proposed Bill.

Public Disclosure
AISA generally supports the public disclosure arrangements relating to adult cyber-abuse. However, under s 93. AISA contends that the threshold of two or more occasions over a 12-month period to qualify for public disclosure will almost certainly result in large and well recognised social media providers where there is a history of cases of cyber-abuse potentially being named. AISA recommends that this provision should explicitly incorporate elements that recognise when social media providers, electronic service providers or internet service providers fully and promptly cooperate with the Commissioners removal notices and where the service can demonstrate a sustained, concerted, proactive and prompt effort to restrict and/or remove materials deemed to constitute adult cyber-abuse as soon as practicable.

4. Image-based Abuse Scheme

Definition

AISA supports the definitions of 'intimate image' contained under s 15, 'non-consensual intimate image of a person' under s 16 of the proposed Bill.

AISA supports the definition of 'posting an intimate image' as defined under s 75 and supports the inclusion of a consent clause (s 75(2)). AISA is of the view that it may be prudent to address the issue of withdrawal of consent as a separate clause under s 75 should an individual who earlier consented to such an image being posted decides at a later time to withdraw that consent

Complaints

AISA supports the provisions detailed in ss 32-5 of the proposed Bill in relation to how to receive, investigate and action complaints from a victim of image-based abuse. AISA supports the right of direct access by a person to the Commissioner.

Removal Notices

AISA supports the general provisions detailed in ss 77-9 of the proposed Bill in relation to the removal of materials by social media services, electronic services, internet services, hosting services and end-users deemed to constitute image-based abuse.

AISA supports the inclusion of a remedial direction for perpetrators of image-based abuse under s 83.

Compliance and Enforcement

AISA considers that the civil penalty for non-compliance by service providers and end-users is appropriate (500 penalty units defined under s 80) as well as measures contained under ss 81, 84, 163, 164, 165. AISA supports the civil penalty provisions for service providers contained under Part 10 of the proposed Bill.

Public Disclosure

AISA generally supports the public disclosure arrangements relating to image-based abuse. However, under s 85. AISA contends that the threshold of two or more occasions over a 12-month period to qualify for public disclosure will almost certainly result in large and well recognised social media providers where there is a history of cases of image-based abuse potentially being named. AISA recommends that this provision should explicitly incorporate elements that recognise when social media providers, electronic service providers or internet service providers fully and promptly cooperate with the Commissioners removal notices and where the service can demonstrate a sustained, concerted, proactive and prompt effort to restrict and/or remove materials deemed to constitute image-based abuse as soon as practicable.

5. Online Content Scheme

Class 1 Materials

Definition

AISA supports the definitions contained under s 106 of the proposed Bill.

Complaints

AISA supports the provisions detailed in ss 38, 39, 42 of the proposed Bill.

Removal Notices

AISA supports the general provisions detailed in ss 109, 110, 124, 128 of the proposed Bill.

Compliance and Enforcement

AISA supports the removal notice measures proposed under ss 111, 125, 129, 163, 164, 165 as well as the formal warning measures detailed under ss 112, 126, 139.

Federal Court Order

AISA supports proposed provisions in relation to the Commissioner having the ability to apply to the Federal Court for an order as detailed under ss 156, 157, 158, 159.

Class 2 Materials

Definition
AISA supports the definitions contained under s 107 of the proposed Bill.

Complaints
AISA supports the provisions detailed in ss 38, 39, 42 of the proposed Bill.

Removal Notices
AISA supports the general provisions detailed in ss 114, 115, 119, 120 of the proposed Bill.

Compliance and Enforcement
AISA supports the removal notice measures proposed under ss 116, 121, 163, 164, 165 as well as the formal warning measures detailed under ss 117, 122.

Federal Court Order
AISA supports proposed provisions in relation to the Commissioner having the ability to apply to the Federal Court for an order as detailed under ss 156, 157, 158, 159.

Industry Codes, Standards, Etc

Definition

AISA supports the definitions and provisions set out under ss 132, 133, 138, 141, 145, 148, 151 of the proposed Bill. AISA is satisfied that sufficient legislative safeguards and community consultation exists within these provisions to ensure proportionality in the achievement of the overall Online Safety goals.

Complaints

AISA supports the provisions detailed in ss 39, 40, 42 of the proposed Bill in relation to how to receive, investigate and action complaints from a person in relation to the breaching of an industry code.

Directions

AISA supports the general provisions detailed in s 143 of the proposed Bill in relation to adherence, compliance and remediation with respect to an industry.

AISA supports the inclusion of a remedial direction for persons who contravene an industry code under s 154.

Compliance and Enforcement

AISA considers that the enforcement provisions contained under ss 143, 146, 154 are reasonable, appropriate and proportionate to the aims of the proposed Bill. AISA supports the introduction of a civil penalty for contravention of directions, standards, rules and remedial directions as defined in the listed sections.

AISA supports the enforcement powers contained under Part 10 of the proposed Bill as well as those contained under ss 163, 164, 165. AISA also endorses the proposal to grant the Commissioner power to issue formal warnings prior to taking enforcement action under ss 144, 147, 155.

Federal Court Orders

AISA supports the powers under ss 156, 157, 158, 159 granted to the Commissioner in relation to the application of Federal Court order in instances where formal and informal attempts to remedy the situation have failed and only in extreme cases and/or cases where a significant community safety risk arises by allowing the continued operation of that service.

6. Abhorrent Violent Material Blocking Scheme

Definition

AISA supports the definitions of 'abhorrent violent material' contained under s 9 and notes its consistency with ss 474.30, 474.31 defined under the *Criminal Code Act 1995* (Cth).

Complaints

AISA supports the provisions detailed in s 27 of the proposed Bill in relation to how to receive, investigate and action complaints relating to abhorrent violent material, and supports the Commissioner having the power to unilaterally act in this regard without a formal complaint. AISA also notes the additional powers under s 95.

Blocking Request and Blocking Notice

AISA supports the general provisions detailed in ss 95, 96, 99, 100 of the proposed Bill in relation to issuing a blocking request and/or a blocking notice. AISA endorses the approach taken by the proposed Bill that in the first instance, the Commissioner would issue a blocking request.

AISA expresses some concern that the statute does not define the length of time by which a service provider must action a blocking notice in relation to the propagation of abhorrent violent material. This is a significant consideration to factor in should a social media provider be utilised by a perpetrator of violent crime in 'livestream mode', as was tragically witnessed in cases such as the Christchurch terrorist attacks.[1]

AISA recommends that a provision be adopted that requires that a Blocking Notice be actioned 'as soon as practicable' and defining an upper time limit in terms of how soon a service provider must action the request by. AISA also recognises the immense difficulty that will be encountered for service providers to adequately monitor any 'real-time' social media posts and recommends that service providers introduce mandatory delays to 'livestream' style social media posts with stringent review procedures for any posts covered by the proposed Bill which may be accessed by a mass audience, in order to mitigate some of the potential issues of this nature occurring in future.

Compliance and Enforcement

AISA considers that the enforcement provisions contained under s 103(1) are reasonable, appropriate and proportionate to the aims of the proposed Bill. AISA supports the introduction of a civil penalty for contravention of a blocking notice, however, is of the view that 500 penalty units may not be a sufficient enough penalty in instances of serious cases of dissemination of abhorrent violent material.

Limitations and Exemptions

AISA generally supports the stated limitations and exemptions defined under ss 95, 96, 99, 100, 104. AISA acknowledges that there is a balance that must be respected between the freedom of individuals to free speech and the need to safeguard and protect the community in relation to materials of an abhorrent violent nature.

[1] Classification Office, New Zealand Government, '*Christchurch Mosque Attack Livestream',* (Web Page) < https://www.classificationoffice.govt.nz/news/featured-classification-decisions/christchurch-mosque-attack-livestream/>.

7. Governance Arrangements

AISA is satisfied with the arrangements defined under the proposed Bill in relation to governance. AISA accepts the need for the evolution of the role and duties of the Office of the eSafety Commissioner.

About the Lead Author

Tony Vizza

Director of the Board
Australian Information Security Association

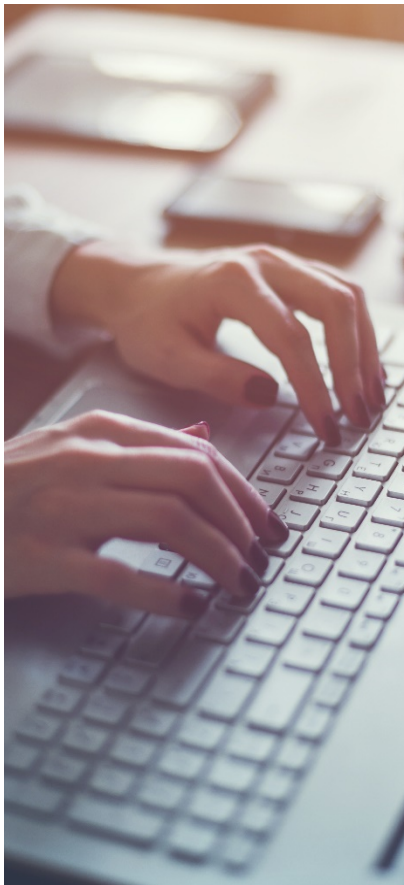
Tony Vizza has been involved in the information technology, information security and privacy fields for more than 25 years.

Tony has completed a Bachelor of Science in Computing Science from the University of Technology, Sydney and a Global Executive MBA from the University of Sydney which included study at Stanford University in the United States, The London School of Economics in the UK and the Indian Institute of Management, Bangalore in India. Tony is currently studying for a Juris Doctor law degree at the University of New South Wales.

Tony's information security credentials include CISSP (Certified Information Systems Security Professional), CCSP (Certified Cloud Security Professional), CIPP/E (Certified Information Privacy Professional / Europe), CRISC (Certified in Risk and Information Systems Controls), CISM (Certified Information Security Manager) and he is a certified ISO/IEC 27001 Senior Lead Auditor.

Tony is a member of the Board of Directors for the Australian Information Security Association (AISA), a Cyber Security Ambassador for the NSW Government, a member of the Cybersecurity Industry Advisory Committee for the NSW Government, a member of the Technology and Business Services Industry Skills Reference Group for NSW TAFE, a member of the Data Security Standards Committee for Blockchain Australia, the co-chair of the $(ISC)^2$ Asia-Pacific Advisory Council and has provided expert services to the United States Government Department of Energy (DoE), the Australian Government's Australian Prudential Regulation Authority (APRA), the Law Society of NSW, the Australian Security Industry Association Limited (ASIAL), the Australian Institute of Project Management (AIPM) as well as numerous boards. Tony works for $(ISC)^2$ as the Director for Cyber Security Advocacy for the Asia-Pacific.

Tony is an expert speaker on information security regularly speaking across the world on information security matters. He has also taught and mentored young and aspiring information security students through Victoria University, TAFE NSW and TAFE Victoria in association with Infoxchange and has lectured cybersecurity students at the University of Technology, Sydney, the University of New South Wales and the University of Queensland. Tony is also a Cyber Ambassador for Untapped, an organisation providing neurodiverse individuals career and life opportunities within the IT sector.



Tony is a regular contributor to numerous cyber security and IT industry publications including CSO Magazine, Infosecurity Magazine, Cyber Today Australia, Security Insider Magazine, Australian Reseller News (ARN), Channel Reseller News (CRN) and Lifehacker, amongst others, regarding information security, business and channel strategy.