Public Consultation on ‘Consolidated Industry Codes of Practice for the Online Industry’

SUBMISSION

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

COVERING LETTER

2.10.2022

Industry Associations Steering Group
E-submission via www.onlinesafety.org.au

Dear Industry Associations Steering Group,

Re: Public Consultation on 'Consolidated Industry Codes of Practice for the Online Industry'

We have attached a submission on the Public Consultation on 'Consolidated Industry Codes of Practice for the Online Industry' from our perspective as the peak professional body for information security and cyber security in the region.

We have no objection to the publication of this submission, and no redactions are required prior to publication.

Thank you for the opportunity to contribute our views. Please do not hesitate to contact Nicole Stephensen, Michael Trovato or myself if you would like clarification of any of the comments made in this submission.

Sincerely,

Damien Manuel
Chairperson, AISA

Email: damien.manuel@aisa.org.au
Mobile: +61 439 319 603

EXECUTIVE SUMMARY

The Australian Information Security Association (AISA) champions the development of a robust information security and privacy sector by building the capacity of professionals and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. We welcome the request for submissions in response to Public Consultation on 'Consolidated Industry Codes of Practice for the Online Industry'.

Established in 1999 as an independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security and security-related privacy matters 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 for 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. AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education and organisational excellence.

This submission represents the collective views of over 9,500 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 Institute of Company Directors (AICD); the Australian Security Industry Association Limited (ASIAL); Australian Women in Security Network (AWSN); Cyrise; grok academy; International Association of Privacy Professionals (IAPP); the Risk Management Institute of Australia (RMIA); the Oceania Cyber Security Centre (OCSC); untapped; as well as international partner associations such as ISACA; $(ISC)^2$; and the Association of Information Security Professionals (AISP). AISA also works closely with both federal and state / territory governments to ensure a robust and safe sector.

In this submission, we have covered matters of particular interest to AISA at this stage of the consultation, noting that our submission is in support of the IIS Partners submission along with the additional items noted below.

It is AISA's hope that our views will be considered alongside those of our esteemed colleagues, as collectively we are working to ensure enhancements to Consolidated Industry Codes of Practice for the Online Industry to support online safety.

TABLE OF CONTENTS

Introduction

AISA welcomes the opportunity to provide feedback on the draft 'Consolidated Industry Codes of Practice for the Online Industry'. We offer our perspective as a members-based association, and as advocates for responsible digital and information security policy and other initiatives that improve online safety, protect children and young people (and other vulnerable groups) and elevate community awareness.

The eSafety Commissioner did not create the Codes upon which we are commenting and has not yet endorsed these as satisfying the statutory imperatives set out in the Online Safety Act 2021 (Online Safety Act). AISA previously offered a submission to 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 sought to enhance the existing protections contained within the Enhancing Online Safety Act 2015 (Cth) which passed both Houses on 23 Jun 2021.

The Online Safety Act 2021 is new legislation that retains and replicates certain provisions in the Enhancing Online Safety Act 2015 and otherwise expands and enhances online safety requirements in Australia. It includes the non-consensual sharing of intimate images scheme; specifies basic online safety expectations; establishes an online content scheme for the removal of certain material; creates a complaints-based removal notice scheme for cyber-abuse being perpetrated against an Australian adult; broadens the cyber-bullying scheme to capture harms occurring on services other than social media; reduces the timeframe for service providers to respond to a removal notice from the eSafety Commissioner; brings providers of app distribution services and internet search engine services into the remit of the new online content scheme; and establishes a power for the eSafety Commissioner to request or require internet service providers to disable access to material depicting, promoting, inciting or instructing in abhorrent violent conduct for time-limited periods in crisis situations.

The eSafety Commissioner's recent press release encourages Australians to contribute to this important consultation on the draft Codes, and AISA makes our submission in support of this vital area of regulation.

Complementary areas of public policy

AISA agrees with IIS's consideration "that (in a manner analogous to a three-legged stool) online safety is intrinsically linked to the Australian public policy imperatives of privacy and information security. To illustrate,

- Privacy (leg one) is about the protection of personal information in accordance with the law and community expectations. Privacy rules apply to much of the Online Industry (including the services, platforms and apps that are proposed to be subject to the Codes), including placing limits on their collection and handling of personal information and any transborder flows of such information – that is, where personal information ends up, where and how it is stored and by whom it is accessed.

- Information security (leg two) is about the protection of information (including, but not limited to, that which is personal) and information infrastructure from unauthorised access, use, disclosure, loss or destruction. In digital or online contexts, this is often referred to as cyber security.

- Safety is when a person is protected from danger, risk, or injury. eSafety (leg three) is the protection of a person from danger, risk, or injury in electronic and online environments."

IIS observed that commentary in relation to complementary areas of public policy – such as discussed in the eSafety Position Paper (Other relevant Australian codes), the Australian Competition & Consumer Commission's (ACCC's) ongoing Digital Platform Services Inquiry, initiatives of the Australian Cyber Security Centre (ACSC), the Australian Information and eSafety Commissioners' involvement in the Digital Platform Regulators Forum, etc. – was largely missing. We agree with IIS' perspective that this omission is a lost opportunity.

IIS considered that the Explanatory Paper for the proposed Codes is a meaningful opportunity for the Code Developers to clarify how key online safety concepts are enmeshed with other Australian public policy imperatives. Additionally, material covered in the Explanatory Paper may – at an appropriate juncture – form the basis for Guidelines (on the operation of the Codes) and other educational materials for industry and the community more broadly.

Recommendation: Discuss the areas of Australian public policy that are complementary to online safety within the explanatory memoranda for the proposed Codes.

Limitations and lawful conduct

In section 6.1 of "Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms" (Limitations), AISA notes:

Nothing in this Code requires any industry participant to:

> (a) implement or build a systematic weakness, or a systematic vulnerability, into a form of encrypted service or other information security measure; Note: Examples of 'other information security measures' include private firewall configurations, VPN tunnels and private networking links, which work directly or complement encryption to protect legitimate cybersecurity and data integrity interests.
>
> (b) build a new decryption capability in relation to encrypted services;
>
> (c) render methods of encryption or other information security measures less effective;
>
> (d) monitor private communications between end-users; Note: In considering whether it would be reasonable for an industry participant to adopt a particular compliance measure under this Code, it will be relevant for the industry participant to take into account the desirability of not intruding upon, and otherwise maintaining the privacy and integrity of, private communications between end-users.

However, where indicated in the Schedule, it may be appropriate for an industry participant to adopt measures that involve analysis of behavioural signals and other data or trends in order to prevent, detect and address harmful activity

AISA is in support of this Limitation with respect to the key online safety objectives and outcomes 1-3.

AISA also notes that "reasonable and proactive steps" with respect to information security to support the Codes, will mean different things to each organisation. As noted in the section above with respect to "Complementary areas of public policy," above, AISA emphasises the need to harmonise the Codes with current and evolving regulation with respect to privacy and information security and notes that weak information security in particular can lead to devastating online safety issues, like use of exploited servers to provide harmful online content or to defeat measures to prevent, detect and address it.

Conclusion

We thank the Industry Associations Steering Group for including us in the consultation process and the opportunity to contribute to this vital work in co-regulation involving the Online Industry and would be pleased to discuss any aspect of our submission.

If you have any questions or need additional information, please do not hesitate to contact us.

About the Lead Authors

Damien Manuel – Chairperson, AISA

As an experienced, results-driven ICT business professional, Damien Manuel has more than 25 years of experience specialising in cyber security, business governance, compliance and risk management.

Damien is the Chairperson of the Australian Information Security Association (AISA), a not-for profit organisation which aims to improve Cyber Security in Australia at a Government, Industry and Community level. Damien also provides advice to several boards both in Australia and internationally. He is a well-known leader in the Australian cyber security sector and works closely with both federal and state / territory governments.

Having recently completed his role at Deakin University as Industry Professor and Director of the Centre for Cyber Security Research & Innovation (CSRI), Damien continues to support the university through his honorary role as Adjunct Professor.

In his former role as the Chief Information Security Officer (CISO) for Symantec Australia and New Zealand, Damien worked with senior executives in the region to align security architectures to industry best practices. He also worked as a senior information security governance manager and later as an enterprise IT and security risk manager at National Australia Bank (NAB), where he was responsible for managing the bank's information security standard globally. He also held senior roles at RSA, Telstra and Melbourne IT and is currently on CompTIA's Executive Advisory Committee.

Damien has supported CompTIA for over 14 years through the development of CompTIA Server+, CompTIA Network+, CompTIA Security+ and more recently the CompTIA Advanced Security Practitioner certification.

Damien's passion for making a difference motivated him to establish Information Technology community resource centres to improve literacy and skills in impoverished and disadvantaged communities in Kenya, Laos, Uganda and Cambodia.

Underpinning his experience is a diverse educational grounding ranging from the highest security, audit and governance certifications complemented by an Executive MBA with an international business focus.

Mr Michael Trovato – Board Member, AISA, Managing Partner & Lead Security Advisor, IIS Partners

Mike Trovato joined IIS in 2018 with over 40 years' experience in consulting and financial services in Australia, Asia Pacific, and the USA. He is a cyber security, privacy and technology risk advisor to boards, board risk committees, and executive management.

Mike focuses on assisting key stakeholders with understanding the obligations and outcomes of effective privacy and cyber security. This includes solving an organisation's issues with respect to regulatory, industry, and company policy compliance and to protect what matters most in terms of availability, loss of value, regulatory sanctions, or brand and reputation impacts balanced with investment.

At IIS, Mike has led over 100 privacy and security governance, risk, and compliance client engagements across government, health care, education, retail, financial services, and technology sectors. He has also advised clients about the direct impact of cyber security on privacy and data protection and how to provide greater resilience to assure better organisational outcomes.

Mike also serves as ICG's Global Cyber Practice Leader and IIS is an ICG Affiliate. Prior to joining IIS, he was the Founder and Managing Partner of Cyber Risk Advisors. Before then, he was Asia Pacific, Oceania and FSO Lead Partner EY Cyber Security; GM Technology Risk and Security for NAB Group; a Partner within Information Risk Management at KPMG in New York; and has held financial services industry roles at Salomon Brothers and Mastercard International. At EY, Mike was responsible for creating the largest, sustained "Big-4" cyber security practice, deploying Privacy and Data Protection solutions, and building the Melbourne Advanced Security Centre (ASC), specialised in attack and penetration testing.

As the NAB's first Group Technology Risk and Security GM, Mike was responsible for risk assessment, strategy, and the security program with a budget of AU$6 million, 11 direct reports and 40+ team members. He focused on enhancing technology risk and security governance, functional security analysis capabilities, and establishing key regulatory and compliance activities.

Mike is a Graduate of the Australian Institute of Company Directors (GAICD), Member Australian Information Security Association (MAISA), an AISA Board Member, ISACA Melbourne Chapter Board Member, Member of National Standing Committee on Digital Trade.

Mike's professional credentials include being a Certified Information Systems Manager (CISM); Certified Data Privacy Solutions Engineer (CDPSE); and Certified Information Systems Auditor (CISA). He is also a member of the International Association of Privacy Professionals (IAPP) and is an ICG Accredited Professional. He has an MBA, Accounting and Finance and BS, Management Science, Computer Science, and Psychology.

Mike is the co-author of The New Governance of Data and Privacy: Moving from compliance to performance, Australian Institute of Company Directors, November 2018.

Contributor

AISA acknowledges the significant contribution of the following individual in this submission:

Nicole Stephensen, FAISA SCCISP – Partner, IIS Partners

Nicole Stephensen is Partner at IIS and leads the privacy strategy and services functions. She was previously Managing Director of Ground Up Consulting Pty Ltd, a boutique firm she established in 2011, which has collaborated extensively with IIS since 2017. With over 20 years in the privacy profession, Nicole believes in building organisational capacity around privacy and embedding best practice into organisational culture.

She has deep public sector privacy expertise, particularly within the privacy regulatory and public policy arenas. Notably, Nicole was asked by the Queensland Department of the Premier and Cabinet to conduct public policy research into and provide drafting instructions for Queensland's first privacy law, the *Information Privacy Act 2009*. She also created and managed the Complaints Management education program at the Queensland Office of the Ombudsman and, while at the Department of Justice at Attorney-General (Queensland's 'lead privacy agency'), was responsible for implementation of the state's early administrative privacy regime under Information Standards 42 and 42A. She has worked for the British Columbia and Alberta privacy regulators and held a principal advisory role at the Queensland Office of the Information Commissioner.

Nicole is a Fellow of AISA (FAISA) and is a recognised leader in privacy acculturation amongst security professionals. She is also a leading member of the International Association of Privacy Professionals (IAPP) and hosts the IAPP's KnowledgeNet Chapter for Queensland. Prior to its incorporation into the larger IAPP in 2019, Nicole was a founding member of the International Association of Privacy Professionals ANZ Chapter (iappANZ) where she sat for three consecutive terms on the Board.

Nicole was the 2020 Smart Cities Council Australia-New Zealand (SCCANZ) Leaderhip Award winner for privacy advocacy and her work building privacy programs for Australian local governments. She is also an Advisory Board member for the SCCANZ Centre for Data Leadership. Nicole held the pro bono position of Executive Director for Privacy and Data Protection at the Internet of Things Security Institute (IoTSI) from its inception until mid-2020 and holds their Smart Cities and Critical Infrastrucure Security Professional (SCCISP) designation.

She is a sought-after international speaker about privacy and the interface between Privacy, Information Security, Risk Management, Ethics and Trust. She is a subject matter expert and Guest Lecturer for the Ducere Global Business School/ University of New England, Queensland University of Technology and the newly-formed Canadian Criminal Justice Academy.

A dual Canadian-Australian citizen, Nicole has lived and worked in Australia since 2003. She holds a Bachelor of Arts (Political Science) degree from the University of Victoria, British Columbia, Canada.