Consumer Data Right

Telecommunications sectoral assessment consultation

SUBMISSION

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

EXECUTIVE SUMMARY

Australian Information Security Association (AISA) welcomes the request for submissions from the Treasury in relation to its sectoral assessment. The Australian Government announced that the Consumer Data Right (CDR) will extend to telecommunications datasets, pending sectoral assessment and formal consultation. AISA understands that the associated consultation process seeks to understand the scope of what could be considered as 'telecommunications data', the nature of that data and who holds the data with particular regard to identifying data that could provide value to consumers if made accessible.

AISA champions the development of a robust information security 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, 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 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 and information technology 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 (ACSC), 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 partners such as $(ISC)^2$, ISACA, the Association of Information Security Professionals (AiSP) and over twenty five Universities and TAFEs across Australia.

It is AISA's hope that the Treasury CDR Division will consider our responses to the consultation paper and incorporate recommendations included as part of a holistic drive by the Australian Government to help deliver a safer and more secure cyber world for the people of Australia, both now and well into the future.

THE AISA VIEW OF SECTORAL ASSESSEMENT

The Australian Information Security Association (AISA) welcomes consultation with industry and the broader community on the possible designation of the telecommunications sector under the CDR. AISA supports the fundamental objectives of the CDR.

SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS

AISA wishes to comment on the privacy and security issues associated with designation. AISA therefore focuses its feedback on Question 11 in the consultation paper: *What privacy issues should be taken into account when considering designation of the telecommunications sector to the CDR regime?*

Cumulative privacy and security risk

CDR sectoral assessments are important but, due to their sectoral focus, run the risk of ignoring cumulative privacy risk across CDR sectors. Certain telecommunications datasets may, on their own, appear no more sensitive than datasets already designated in the banking sector. However, as CDR services begin to bring together consumer data from multiple sectors in one place[1] , the privacy and security risks necessarily multiply. These include security risks associated with the creation of data honeypots attractive to cyber-criminals and privacy risks associated with increasingly detailed information about individuals being brought together and analysed. Those risks are not eliminated by the voluntary nature of consumer participation nor by CDR consent requirements. These data honeypots would be of significant interest to hostile nation states with significantly more resources and skills than your typical cyber-criminal, amplifying the likelihood of a data theft event occurring.

Such risks must be treated seriously. AISA recommends that the Treasury consider telecommunications datasets in that wider context when weighing risks of designation. We also suggest that higher security requirements apply to accredited data recipients (ADRs) that wish to handle a consumer's CDR data across multiple sectors. For example, such ADRs could be subject to higher accreditation requirements.

Overreliance on consent to offset privacy and security risk

The consultation paper points out that the CDR offers higher privacy protections than are available under the *Privacy Act 1988* and, in particular, offers a strict consent mechanism to protect consumers and their interests (see p 26 of the Consumer Data Right Sectoral Assessment Telecommunications Consultation paper).

While consent is important, AISA is concerned that too much emphasis is being brought to bear on the role it plays in offsetting privacy and security risk. The thinking appears to be that privacy risk associated with designation of certain datasets is largely alleviated by consent and the consequent choice and control consumers have over CDR participation. For example, the consultation paper implies that consent mitigates privacy and security risks of designating usage data and location data.

In AISA's view, consumers will be ill-equipped to weigh the privacy and security risks inherent in a complex data sharing system like the CDR. Designating 'risky' datasets such as location data and allowing consumers to consent to sharing such data places an unfair burden on the consumer to weigh the risk. AISA believes the system must already be as safe as possible before consumers are asked to participate in, or consent to, CDR data sharing. This includes only designating data that is safe to share regardless of the consumer's risk appetite.

AISA therefore recommends that the existence of CDR consent not be used as a mitigating factor when weighing privacy and security risks associated with dataset designation.

[1] Consumer Data Right Sectoral Assessment Telecommunications Consultation paper (https://treasury.gov.au/sites/default/files/2021-08/c2021-182135-tc.pdf) – Case study 3 page 14

Risks associated with usage data

The consultation paper discusses the possible designation of usage data. According to the paper, such data could include total data usage per period (i.e., monthly), number of calls and voice minutes and number of messages sent. AISA wishes only to emphasise that such data should not include telecommunications metadata of the kind regulated by the *Telecommunications (Interception and Access) Act 1979*. Nor should it include internet browsing information or message content. It appears that such data would not be able to be designated due to restrictions in the Interception Act and *Telecommunications Act 1997*. In AISA's view, the sensitivity of such information outweighs the possible benefits to the consumer of CDR designation.

Risks associated with location data

The consultation paper implies that location data is under designation consideration. Yet, the paper also implies that such data would not be able to be designated due to the operation of Part 13 of the Telecommunications Act. AISA is therefore uncertain about whether designation of location data is possible or likely. Notwithstanding that uncertainty, we would like to emphasise the sensitivity of location data and the privacy risks inherent in its use and sharing. The existing availability of location data to certain entities is not justification for its wider sharing and use.

Making location data available under the CDR creates room for intentional or inadvertent surveillance of individuals and their movements in time and space. Those risks are particularly acute for cases where the account holder and device user are different people. In such cases, the device user may be unaware that location data is being shared under the CDR, being 'out of the loop' of consent and notice mechanisms that would otherwise apply. AISA recommends careful consideration of the risks before any designation decision about location data.

ABOUT THE LEAD AUTHORS

Michael Trovato – AISA Board Director and Managing Director & Lead Security Advisor of IIS

Mike Trovato is a cyber security and technology risk advisor to boards, board risk committees, and executive management. He 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.

Mike is ICG's Global Cyber Practice Leader. 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.

Mike is a Graduate of the Australian Institute of Company Directors (GAICD), Member Australian Information Security Association (AISA), an AISA Board Member, ISACA Melbourne Chapter Board Member, and 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); Certified Information Systems Auditor (CISA); and PCI DSS Qualified Security Assessor (QSA). 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.

Natasha Roberts – AISA Member and Senior Consultant, IIS

Natasha Roberts is a senior consultant with IIS since 2016 and has been working in privacy law and policy for over fifteen years. At IIS, Natasha has advised a wide range of clients, and has particular experience in digital platforms and identity management, Privacy by Design, health privacy, international privacy law and applying the Australian Privacy Principles in a wide range of contexts.

Natasha led the privacy impact assessment (PIA) work on the administrative data use by the Australian Bureau of Statistics and the data sharing scheme proposed under the Data Availability and Transparency Bill.

In addition to conducting numerous PIAs at IIS, Natasha has also led research on projects examining emerging privacy issues and regulatory responses. This has included options for international privacy regulatory harmonisation for a global digital platform, as well as research on the international regulation of digital platforms for the Office of the Australian Information Commissioner.

Prior to her time at IIS, Natasha worked for a decade at the federal privacy regulator during which time she engaged on a wide range of privacy issues, particularly in relation to new technologies, data analytics, de-identification, electronic health records and APEC privacy enforcement cooperation.

She was a member of the secretariat supporting the Government 2.0 Taskforce. During a secondment to the New Zealand Office of the Privacy Commissioner, Natasha drafted a major research paper and guide on privacy and CCTV. In 2008 she was awarded an Australia Day Achievement Medallion for her work supporting the Australian Privacy Commissioner.

Along with an in-depth knowledge of privacy regulation, Natasha has expertise in information law and policy more generally including freedom of information law and trends in open government.

Natasha holds a Bachelor of Arts (Hons 1) from the University of Sydney. She has also completed training courses on Fundamentals of internal audit; Administrative power and the law; Machinery of Government; and Policy Formulation.

Natasha is a Member of the Australian Information Security Association (MAISA) and the International Association of Privacy Professionals (IAPP).

ABOUT CONTRIBUTING AUTHORS

Damien Manuel – AISA Board Director and Industry Professor / Director of Deakin's Centre for Cyber Security Research and Innovation (CSRI)

Damien Manuel is the Industry Professor and Director of Deakin's Centre for Cyber Security Research & Innovation and 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.

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. Damien 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, Ericsson and Melbourne IT and was on the board of the Oceania Cyber Security Centre (OCSC).

Damien is currently on CompTIA's Executive Advisory Committee in the USA, the Victorian Ombudsman's Audit and Risk Committee, the board of RSA Australia, the chair of Standards Australia's Standards development committee for cyber security and privacy and helps mentor entrepreneurs through CyRise, Australia's only cyber security startup accelerator.

Damien has supported CompTIA for over 18 years through the development of CompTIA Server+, CompTIA Network+, CompTIA Security+ and 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 over 25 years of 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. Damien also has a background in genetic engineering and is passionate about science. He has spoken on a number of podcasts (including with Dr Karl), conference keynotes internationally and locally, radio and TV appearances.