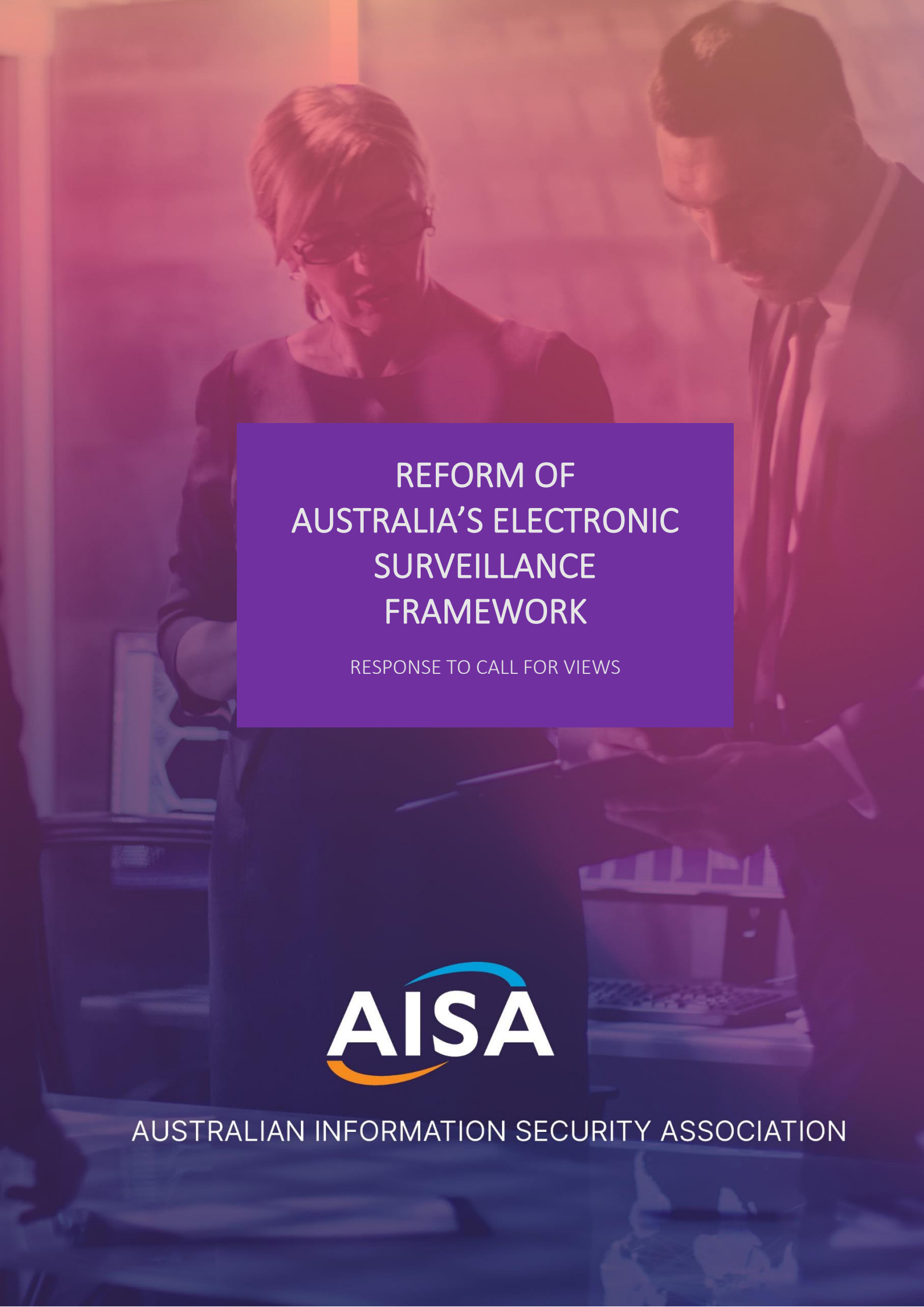


REFORM OF AUSTRALIA'S ELECTRONIC SURVEILLANCE FRAMEWORK

RESPONSE TO CALL FOR VIEWS

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

EXECUTIVE SUMMARY

The Australian Information Security Association (AISA) welcomes the request for the call for views from the Australian Government's Department of Home Affairs in relation to reforming Australia's Electronic Surveillance framework.

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, 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 7,500 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 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 Centre for Cyber Safety and Education, ISACA, IAPP, the Association of Information Security Professionals (AiSP), the IoT Security Institute (IoTSI) and over twenty-five Universities and TAFEs across Australia.

It is AISA's hope that the Department of Home Affairs will consider our responses to the call for views 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.

Australian Information Security Association
ABN 181 719 35 959

Level 8, 65 York Street,
SYDNEY NSW 2000
AUSTRALIA

Phone: (02) 8076 6012
Email: info@aisa.org.au

TABLE OF CONTENTS

AISA Response to the Reform of Australia's Electronic Surveillance Framework Discussion Paper.

Australia's cyber security ecosystem relies upon adherence to high standards of privacy, security, risk management and resilience. AISA supports all measures to facilitate and maintain a safe and secure cyber ecosystem.

AISA acknowledges the essential roles of the Director-General of Security, the Director-General of the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO) and the Director-General of the Australian Signals Directorate (ASD) in enforcing criminal law, promoting, and protecting Australia's economic and national interests, and maintaining national security.

Any changes to law relating to electronic surveillance implemented as a result of work arising out of the changes proposed in the discussion paper must not erode the privacy of Australian citizens, their confidence in the confidentiality of their communications and protection of proprietary information. Where access is necessary for law enforcement and national security purposes, there must be strong oversight and controls to ensure that compromised agencies and/or corrupt officials do not present a new form of cyber risk to Australian business, to prevent unnecessary or unplanned uses or abuse of lawfully obtained information, and to ensure that powers are not used under political pressure to subvert our democracy, or for the widespread collection and capture of information without a specific target.

AISA does not agree with the premise proposed in the discussion paper that without access to information and data as defined by note[1] in the paper, law enforcement agencies could not prevent and prosecute the most serious criminal activities, such as child sexual abuse, organised crime and cybercrime. This default stance as listed in the discussion paper proposes that those not in support of the legislative changes support organised crime and child abuse, which is both preposterous and offensive to many Australians.

The discussion paper goes on to state that ASIO requires access to this information and data to protect Australia from serious national security threats, such as terrorism or foreign interference with our democratic institutions. This mission should drive the structure of the ASIO's right to access information: i.e., the power to access information should be limited to cases where there is a serious national security threat or a case of foreign interference The discussion paper also misses the largest threat to our democracy from foreign interference, which is primarily through misinformation and disinformation campaigns which are openly spread on social media and therefore occur in plain sight.

AISA supports:

(a) Strengthening of legal protections to protect the security of communications and electronic systems.
(b) Simplifying legislation at both the Commonwealth and State/Territory levels to avoid conflicts, maintain common understanding between agencies and ensure transparent independent oversight by bodies with appropriate experience, resources, scope and powers.
(c) Acknowledging that terminology in the current suite of legislation is outdated and no longer represents the current technological landscape.
(d) Adopting a strategy of technologically agnostic terms that is likely to retain relevance over a longer period.
(e) Increasing transparent oversight, safeguards and public accountability to protect individual privacy of Australian citizens.

[1] The discussion paper uses the phrase 'access to information and data' to refer to the use of electronic or technologically-assisted means to covertly listen to or read a person's conversations or messages, access a person's electronic information or observe a person's activities and movements – collectively, electronic surveillance powers. This includes activities such as intercepting phone calls, remotely accessing a person's computers or using a listening or tracking device. The terms 'information and data' are used to refer to any kinds of information that could be obtained through these methods. There are various methods of accessing information (including electronic information and data) that do not involve electronic surveillance. For example, agencies may be able to access a computer on premises when executing a search warrant. Powers of that kind are not within the scope of the discussion paper.

(f) A framework to protect individuals that provide information to journalists and institutional whistle-blowers to encourage and support public and private reporting of institutional and political wrongdoing and malpractice.
(g) Harmonising legislation relating to the use (including the circumstances) and definition of surveillance devices jointly with state and territory governments.

AISA Response to Call for View Questions

Current State

1. Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day?

AISA supports the existing standing prohibition on the interception of communications (clause 7 of the *Telecommunications (Interception and Access) Act 1979*), the qualified prohibition on carriers and carriage service providers disclosing or using any information relating to the content of a communication, carriage services supplied and the affairs and personal particulars of individuals (Part 13 of the *Telecommunications Act 1997*) and the criminal offences which protect telecommunications and computer systems expressed in Parts 10.6 and 10.7 of the Criminal Code.

AISA recommends the Commonwealth enact legislation to harmonise state and territory surveillance device laws to protection Australian citizens against observing activities, listening to conversations, and tracking a person's movements through the unauthorised use of surveillance devices. Legislation must be co-developed with the state and territory governments in good faith to ensure unintended consequences do not arise and Australian citizens are protected.

2. Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives?

AISA believes that harmonised provisions need to incorporate stringent protection of networks, individual and company information and data from unauthorised access.

AISA recommends the government consider including express exceptions to the existing prohibitions to allow active measures to protect electronic data and the public:

(a) It should be permissible for commercial operators to detect and delete known malware and scam emails from information systems in transit. In our view the legislative framework should support proactive removal of hostile content.
(b) A safe harbour should be legislated to facilitate good faith research regarding third party system vulnerabilities perhaps on the condition that the researcher will
    a. not damage any data or interfere with the functioning of any system; and that
    b. any findings are shared with the system operator or kept confidential.
(c) A safe harbour to allow response to an attack: It should not give rise to a criminal offence for victims of an attack to:
    a. take reasonable steps to identify the source of the attack;
    b. recover lost data from the source of the attack; and/or
    c. where able to identify with reasonable certainty the source of the attack owned or operated by the attacker, take steps to disable the attacker's software or system.

Access to information will be strictly controlled

3. Are there any additional agencies that should have powers to access particular information and data to perform their functions? If so, which agencies and why?

AISA is of the opinion that electronic surveillance and access to information should be strictly limited to agencies who are:

(a) Investigating serious crimes, and have the assessment capabilities to establish the necessary and proportionate gravity of the matter under investigation
(b) Have the right governance, oversight, safeguards and skills to deal with such matters; and
(c) Capable to assess and limit breach of privacy for an individual.

4. Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?

AISA contends that the use of covert electronic surveillance should be regarded as a measure of last resort, rather than a substitute for conventional evidence gathering. AISA forms the view that additional agencies may be included in the existing list of permitted agencies on the basis that access to electronic surveillance is the only possible means of acquiring evidence; where the subject matter of the investigation is sufficiently serious by reason of the amount of revenue involved; the alleged or suspected crime is of a gravity and magnitude which dictates covert surveillance as a necessity; there is a serious and immediate risk to individuals; and where a judge issued warrant is granted.

If extra surveillance powers are being given to agencies, it is necessary to give extra protections to Australians to protect against misuse. This can take the form of a specific named protection for the citizen, but could also be an added form of oversight from another agency.

Agencies requiring additional surveillance capability need to have a corresponding independent entity that is both capable and equipped to perform an oversight function.

5. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?

AISA believes the definition of 'communication' used to protect communications from unauthorised access and misuse should be different from the definition used to define the information that may be accessed for national security or law enforcement purposes. The definition used to protect communications should be wide. Whereas the definition used to identify information that might be accessed by various means for national security or law enforcement purposes should be drafted according to the sensitive (privacy intrusive) nature of the relevant data.

AISA considers the following categories of data should be highly protected and accessed only under warrant where reasonable grounds exist to suspect the information will assist with the prosecution of a serious offence or assist to prevent a terrorist attack:

- Metadata – For example, a location, call history (and associated details), and person's activities on the internet. This also includes web-browsing history, URLs visited by a person and a person's use of non-messaging applications on their smartphone.
- Data that is not transmitted – This includes electronic documents, files, images, or other content created by a person, regardless of whether they are transmitted to another person. This includes documents or images a person saves on their computer or uploads to a cloud storage service such as Dropbox or Google Drive.
- Interactions between a person and a machine – This includes instant messages between a person and an automated system, such as a customer service chat-bot.
- Interactions/signalling information between a machine and another machine – This includes interactions

between devices on the Internet of Things, for example, data generated by connected or autonomous vehicles, or smart home security systems.
- Emerging technologies, such as artificial intelligence and information derived from quantum computing.

Under the proposed new definition of 'communication', any device or item connected to the Internet, regardless of whether it is used by an individual under surveillance, becomes in scope. AISA considers that this proposed definition is too generic, and instead contends that the focus be only on communications generated by the individual to other individuals. AISA believes that this change would ensure that the legislation would remain true to form in relation to subverting serious organised crime and child sexual abuse, rather than mass surveillance of the Australian public which the proposed form lends itself towards.

7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?

The framework should support the use of encryption to protect private messages and systems. AISA notes that the recent success of Operation Ironside was dependent on persuading the targets that the devices with which they had been supplied were secure and could not be hacked. AISA recommend that the Australian Government adopt a position on the use of encryption analogous to that of the German government, namely, that it supports widespread, strong and unregulated encryption.

There are a plethora of methods security agencies can use to conduct targeted remote hacking.[2]

AI and advanced information analytics offer the prospect of law enforcement agencies taking large volumes of data from computers or mobile phones and using the data to identify criminal operations and/or specific offenders. The new framework must address the power, risks and uses of surveillance and these new tools directly by recognising that:

- Metadata is often more useful and privacy intrusive than 'content'.
- Metadata over a short period and in small volumes is likely to be less privacy intrusive than metadata relating to long periods and large volumes which can be highly privacy intrusive, particularly when subject to formal analysis.
- The Privacy Act and Consumer Data Right frameworks treat information related to individuals as being owned by and subject to control by that individual. It is contrary to the principles driving those frameworks to engage in covert collection and analysis of data relating to individuals without their knowledge or permission. Accordingly, such activities need to be highly regulated, and subject to third party oversight and clear public reporting.

8. What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information?

The distinction between 'content' and 'non-content' is meaningless. The important issue is the extent to which collection and use of the information is privacy intrusive. An individual who has not been knowingly accompanied by a law enforcement officer does not expect his or her movements over any period, who he or she spoke to, when and for how long, to be shared with government agencies in the absence of a warrant, as is currently permitted by the mandatory data retention framework. This 'non-content' information is more privacy intrusive than the content of many telephone conversations and should be regulated in the same manner.

9. Would adopting a definition of 'content' similar to the UK be appropriate, or have any other countries adopted definitions that achieve the desired outcome?

[2] https://carnegieendowment.org/2021/03/31/encryption-debate-in-germany-2021-update-pub-84216.

No. The UK definition maintains a distinction between 'content' and 'non-content'. Additionally, the UK is currently undertaking a wide review of critical infrastructure cyber measures, with definitions related to organisations such as service providers is currently in the process of industry consultation.[3]

10. Are there benefits in distinguishing between different kinds of non-content information? Are there particular kinds of non-content information that are more or less sensitive than others?

Yes. Non-content information can be highly sensitive, see our comments above. We note that the Privacy Act Review Discussion Paper (October 2021) proposes that location data be included as an example of personal information (recommendation 2.1), for consideration in the definition of 'sensitive information' (page 33), and for 'collection, use or disclosure of location data on a large scale' to be a 'restricted practice' requiring mitigation measures (paragraph 11.1).

Other types of information that can indicate relationships (e.g., call records), timing of movements (e.g., data associated with access systems, GPS data), and health related information are also highly sensitive. The framework should take the position of the individual and regulate collection and use of information from which information relating to an individual can be derived with a focus on the categories of 'sensitive information' defined in the Privacy Act (along with the accompanying review paper).

Is there a real difference between 'live' and 'stored' communications anymore?

11. Should the distinction between 'live' and 'stored' communications be maintained in the new framework?

AISA is of the view that information at rest and in transit should not be generally distinguished; however, there is a difference between having to physically raid a residence to obtain stored data that cannot otherwise be hacked, and interception that is done in transit. One is much more privacy-infringing

While there are different requirements associated with information that is 'live' or 'stored' being intercepted, the controls and protections should be consistent. Stored communications such as emails, texts and messages should be treated with the same level of interception oversight. Both forms should require a warrant, signed by a judge, to access them.

Where the method of access required involves physical entry to a premises, forced or otherwise, there should be a higher threshold of need proven by the investigator.

12. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?

AISA contends that information that is either 'live' or 'stored' will have the same intrusion into the privacy of an individual or company and have the potential to cause serious harm if mishandled or misused.

Australians no longer communicate exclusively using services provided by Australian carriers and carriage service providers

13. What type of Australian communications providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?

AISA forms the view that Australian communications providers such as telecommunication providers are already burdened by numerous sets of legislation and regulation necessitating them to capture and store data. The financial burden of this is almost always passed onto the consumer. This represents a cost overhead that newer, often offshore-based communication organisations do not need to bear, creating an unfair business environment

[3] https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience.

for Australian-based organisations. In some cases, the provider may actively wish to seek a base of operations in a jurisdiction that is not subject to Australian legislation, so that their commercial interests will not be affected. This represents an adverse outcome and one which runs counter to the stated purpose of any future framework.

Regulation of surveillance devices focuses on types of device, not kinds of information

14. What are your thoughts on the above proposed approach? In particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?

Subject to our comments above, in relation to regulation, oversight and transparency:

- AISA supports the introduction to focus on the type of information collected. AISA notes that devices can readily be repurposed or augmented to collect information that was not intended in the original context, e.g., medical data such as electrocardiogram (ECG) data can now be obtained from device data, when what is intended are the messages sent and received.
- AISA recommends conducting a program of information modelling using industry techniques that would assist in explaining and defining the landscape of information that is captured by surveillance and tracking devices:
    i. Using existing information modelling languages (UML, or the Common Information Model) to determine a common information model across agencies and devices.
    ii. Assessing the current information used by devices and perform a gap analysis between the Commonwealth and States/Territories to determine that common model and where possible align.

.

Is a warrant framework that emphasises impact on privacy over method of access the way forward?

15. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants while ensuring appropriate privacy protections are maintained?

AISA identifies the following issues raised by the new framework, where generic warrants for a category (e.g. electronic communications rather than telecommunications intercept) are proposed to be used rather than a specific warrant:

- More data is collected than intended, compromising the privacy of those not under suspicion, as any communication regardless of the intent becomes fair game. Previously only calls made may be captured rather than any communications which may include interactions with any business or individual across any device or medium.
- The burden of defining what is collected and why is reduced, making it too easy for data to be captured which is not the intended focus of the surveillance. This can be abused due to internal corruption, political pressure, or by accident or misadventure unless there is clear control and transparent oversight.

16. What other options could be pursued to simplify the warrant framework for agencies and oversight bodies, while also enabling the framework to withstand rapid technological change?

The discussion paper contends that amendments will be more difficult to address given the pace of technological change and AISA disagrees with this proposition. While AISA acknowledges that there has been considerable technological change since the 1960s, AISA also forms the view that the pace of that change can be anticipated and better adapted to without the need for simplified warrants. AISA further argues that simplification can be achieved by automating processes and systems, without the need to change the warrant framework.

Access to private communications, content data and surveillance information

17. Is it appropriate to harmonise legislative thresholds (as outlined above) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?

AISA believes such a measure is appropriate, however qualifies that the existing basis for access and controls should be reviewed at a scheduled and regular basis to maintain a suitable threshold, clear oversight and public transparency. AISA strongly argues that the underpinning guiding principle at all times should be to protect an individual's privacy, and not risk it being eroded because of a matter being assessed on a threshold measurement basis.

AISA supports the alignment for law enforcement agencies thresholds to increase to a minimum 5 years.

AISA is of the view that as much harmonising thresholds would assist various agencies when seeking authorisation for surveillance and access to information, the gravity of the matter under investigation should be the deciding factor when issuing a warrant and should be defined clearly to provide appropriate guidance to agencies.

Access to information about communications

18. Are there any other changes that should be made to the framework for accessing this type of data?

Please refer to earlier comments regarding the weakness of the existing framework for accessing metadata.

AISA also submits the following:

- A significant weakness in the existing framework is that it applies to any provider that is a carrier or carriage service provider rather than to the individual systems or services that they provide. For example, a cloud service provider or data centre operator might support a webmail or other customer messaging system that is not subject to mandatory data retention obligations. If they offer to resell carriage services to any of their customers, they will become a 'carriage service provider' and the existing webmail and messaging systems is, thereupon, subject to mandatory data retention obligations. This is a disincentive to agile service delivery. The framework should regulate the system and not create disincentives for the provision of other services.
- The current definition of 'communication' forms part of the current metadata retention framework, thereby capturing systems that transfer data and signals. This has the effect of applying mandatory data retention to many IoT and machine-to-machine systems that should not be subject to the mandatory data retention obligation.
- While not specifically listed in the future state, the need for judicial approval of a warrant to access the records relating to journalists is essential in maintaining the freedom of the press.
- A public interest advocate that is independent with the appropriate authority is a critical component of any future framework.

Access to information about a person's location or movements

19. What are your views on the proposed thresholds in relation to access to information about a person's location or movements?

Please refer to earlier comments referencing the Privacy Review Discussion Paper.

AISA contends that location data is highly privacy intrusive. The fact that police may install cameras in a public place without a warrant is in no way comparable to systematic tracing of the location of an individual.

In an environment where so-called 'Big Data' (the ability to correlate large data sets) is common there is significant capability to combine seemingly sets of unrelated information to infer and derive outcomes.

The premise that tracking information may have less impact needs to be weighed against the geolocation information in combination with other larger datasets; it should not be taken at face value to have less impact.

AISA is of the view that the current authorisation framework and thresholds be retained.

Warrants should be directed at a specific target or person in the first instance

20. What are your views on the proposed framework requiring warrants and authorisations to target a person in the first instance (with exceptions for objects and premises where required)?

AISA submits that in most scenarios, cybercriminals will first try to anonymise their identity and often will hide behind a network of compromised subjects. Targeting a person as a primary approach can be difficult and strenuous, and at times can implicate an innocent computer user. The warrants and authorisations to target a person should be carefully considered and apply protection to privacy as the foundational principle when developing the framework.

What about third parties?

21. Is the proposed additional warrant threshold for third parties appropriate?

AISA contends that the additional threshold for third party access is appropriate. While there are benefits to standardising the thresholds and purposes, it will result in a substantive increase in the ability for ASIO (and other agencies) to conduct surveillance on the general population who are not the subject of an investigation.

The additional threshold should also be aligned across the different agencies to avoid ambiguity and potential confusion with the issuing authorities.

What about groups?

22. Is the proposed additional threshold for group warrants appropriate?

AISA notes that no specific higher thresholds for group warrants are specified, only the initial test that warrants to individual persons must be impractical or ineffective. The introduction of the issue of group warrants is a significant step towards social surveillance and should be approached only after detailed consideration and consultation. We suggest exploring the implications and potential operation of the proposed scheme in a separate consultation where more detail is provided regarding why such warrants are required, when they would be used, what would determine who might be in a group, and how the relevant data might be protected and used.

AISA acknowledges that the current framework of legislation has limitations, but the group warrant proposal has a higher risk of mass surveillance on the Australian Public:

- Recommendation 83 outlines that a warrant be issued when a group has engaged in or is reasonably suspected of having engaged in common activities that would justify the warrant; however, there is no threshold to dissuade misuse against political groups.
- The definition of 'group' is vague with potential to overreach the intent and erode public confidence.
- A warrant should be directed to an individual under investigation.

Powers should only be authorised where necessary and proportionate

23. What are your views on the above proposed approach? Are there any other matters that should be considered by an issuing authority when considering necessity and proportionality?

AISA forms the view that in some cases, authorities do need to have information regarding how their target system works, what information it is capable of delivering and how. This can require technical expertise on the part of the issuing authority and, in some cases, consultation with the entity that holds the information. The existing law makes provision for notice and liaison in support of technical capability notices in Part 15 of the *Telecommunications Act 1997* but does not do so for identify and disrupt warrants under the *Surveillance Devices Act 2004* or account takeover warrants in the *Crimes Act 1914*. The new framework should make sure that all surveillance powers requiring technical intervention by third party service provider ensure adequate consultation and technical expertise on the party of the issuing party.

AISA supports the proposed approach as the future state. However, AISA is steadfast in its view that such powers are only authorised when they pass the necessary and proportional test criteria. AISA notes that it is concerned that such requirements can be open to debate and that often assumptions need to be made and can be hard to pass a threshold test. The approach could be further strengthened by testing for any breach or disproportionate undermining of an individual's privacy protection.

Who should authorise the use of these powers?

24. Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?

AISA contends that the constitutionally enshrined separation of powers is a powerful and enduring feature of the Australian democratic system. As such, AISA is of the firm belief that the issuance of any warrants should be a function that remains strictly within the judicial arm of government. AISA believes that the Federal Court of Australia and the Supreme Court of each State/Territory are appropriate authorities for the issuing of warrants.

AISA also holds that there should be a consistent approach between law enforcement agencies and other government entities (noting the exclusion of ASIO) in the process required in obtaining a warrant. This process should be principles-based and should focus on the balance between the nature (or category) of the potential harm to the community and that of the individual. AISA maintains that this process should be applied consistently in all cases. The obligation to obtain a warrant should be extended to 'non-content' information where the information collected or capable of being derived is highly privacy intrusive.

AISA acknowledges the outcomes of the PJCIS inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press. AISA is of the steadfast view that access to data held by journalists and media organisations should only be authorised by members of the judiciary, to ensure complete independence and transparency and in the pursuit of the public interest.

AISA supports an expanded role of Public Interest Advocates with a monitoring model to provide greater transparency and accountability. AISA asserts that annual reporting on key metrics should take place, similar to existing models in Victoria and Queensland.

Information must be appropriately protected and only shared with the appropriate authorities

25. What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?

Information use and disclosure should be limited and only be allowed between agencies which are:

- Investigating serious crimes and have the assessment capabilities to establish the necessary and proportionate gravity of the matter under investigation.
- Have the right governance, oversight, safeguards, and skills to deal with such matters.
- Capable to assess and limit breach to privacy for an individual.

AISA also notes that simplification of legislation at both Commonwealth and State level should remove some of the current challenges around sharing information between different agencies, as described in the case study.

The new framework should contain offences for the collection, retention, and misuse of electronic surveillance other than as specifically authorised by law. The new framework should prohibit the use of any information collected for personal gain, political purposes, and identification of the source of a journalist and/or a whistle-blower.

26. When should agencies be required to destroy information obtained under a warrant?

Information retention and destruction policies are vital to balance community security and privacy needs. AISA recommends the application of the following concepts:

- A common metadata standard to simplify the application of any data retention and destruction policy to avoid mishandling or accidental destruction.
- A common records retention format that is focused on the nature and type of information weighted on the risk of disclosure.
- Independent validation of the destruction process with oversight and transparency reporting.
- A common hold process with independent authorisation if the destruction of the information needs to be delayed, again with oversight and transparency reporting.

Warrant requirements should only be relaxed in time-sensitive situations

27. What are your thoughts on the proposed approach to emergency authorisations?

AISA supports the power to issue emergency authorisations provided there is an appropriate threshold, the use of the emergency power is specifically reported to the applicable oversight body, the information regarding use of the power is included in public reporting and emergency authorisations are granted for the shortest possible time period.

A well-founded and tested process should be crafted to support emergency authorisation in rare and/or unprecedented circumstances, including to deal with serious crimes such as terrorism or national security threats.

The process should cater for appropriate documentation and analysis of gravity of the matter to support the decision-making process.

The use of intrusive powers will be strictly limited

28. Are there any additional safeguards that should be considered in the new framework?

As highlighted at Question 24, AISA strongly believes independent authorisation needs to be retained by the Judiciary (noting the exception for ASIO). Where authorisation is sought under another Commonwealth or State/Territory body, this may introduce conflict of interest issues and erode public trust in law enforcement and government agencies.

Information management security and capability within the agencies to ensure basic principles are followed:

- Implementing written policies, procedures, and standards of conduct.
- Designating a compliance officer and internal compliance committee.
- Conducting effective training and education.
- Conducting internal monitoring and auditing.
- Enforcing standards through well-publicised disciplinary guidelines.
- Responding promptly to detected offences, undertaking corrective action, and reporting to the proposed oversight entity (e.g., Ombudsman).

29. Is there a need for statutory protections for legally privileged information (and possible other sensitive information, such as health information)?

AISA supports statutory protections for legally privileged and other sensitive information (e.g., health) to ensure:

- judicial independence and professional conduct rules for legal practitioners is maintained
- procedural fairness in legal matters
- no personal harm is caused through medical record disclosure which is unlikely to be relevant to a warrant

Ensuring powers are exercised in line with the law

30. What are the expectations of the public, including industry, in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?

AISA believes that the public expectation is for government to protect the rights to privacy for individuals who fall under Australian jurisdiction. Understanding that there is a balance that needs to be struck, AISA asserts that unless explicit exemptions of a reasonable nature defined under the Privacy Act are made, or unless the individual explicitly and categorically waives that right to privacy, an individual's right to privacy should always be maintained.

AISA also recognises that there is a balance between the rights of individuals to privacy and the interests of entities to carry out their legitimate functions, including activities being subject to a 'lawfulness' test. At a minimum, the public should expect that entities carrying out data collection, use and disclosure will only do so via a lawful basis.

31. What, if any, changes are required to the scope, role and powers of the Commonwealth Ombudsman to ensure effective oversight of law enforcement agencies' use of powers in the new framework?

AISA supports expanding the scope of the Commonwealth Ombudsman (or equivalent) to include oversight on surveillance activities across agencies, with additional powers to report and prosecute wrongdoing, and ensure clear and detailed reporting of information obtained in the discharge of its responsibilities to the Australian public:

- A heightened focus on the legality, propriety, and compliance to human rights so that it aligns with the goals of the Inspector-General of Intelligence and Security (IGIS).
- Ensuring intra-agency sharing, reporting and oversight is transparent and in line with the recommendations to protect journalism and public interest advocacy.
- Enforce or report on compliance with both State/Territory and Commonwealth information management and security requirements (e.g., Information Access, handling, and storage requirements as well as those outlined in Q28).

Reporting and record-keeping requirements

32. How could the new framework streamline the existing record-keeping and reporting obligations to ensure effective and meaningful oversight?

AISA recommends the adoption of a common metadata model and taxonomy across all applicable agencies to assist in unified approaches to storage, reporting, and compliance of records and activities. This creates consistent environments for governing bodies to provide oversight.

33. Are there any additional reporting or record-keeping requirements agencies should have to improve transparency, accountability and oversight?

In combination with oversight and reporting on maintaining strong information protection measures to avoid the potential for abuse:

- Strong access and authorisation models to ensure only those with a clear need have access to the information.
- Clear policies on how long agency members can have access to personal information
- Revocation of access when agencies no longer need immediate access to the information (with the ability to request access in the future if the need arises)
- Reporting and oversight on access to records.

34. How workable is the current framework for providers, including the ability to comply with Government requests?

35. How could the new framework reduce the burden on industry while also ensuring agencies are able to effectively execute warrants to obtain electronic surveillance information?
36. How could the new framework be designed to ensure that agencies and industry are able to work together in a more streamlined way?

Interaction with existing and recent legislation and reviews

37. Do you have views on how the framework could best implement the recommendations of these reviews? In particular:
    a. *What data generated by 'Internet of Things' and other devices should or should not be retained by providers?*

AISA contends that the prevalence and increasing commonality of the 'Internet of Things' represent a significant privacy concern for consumers and companies. AISA has provided a detailed response in respect of this topic in the Department of Home Affairs' recent call for views relating to the strengthening of Australia's cyber security regulations and incentives.[4] AISA notes the fact that IoT devices come from entities with diverse levels of security posture, and developed and manufactured in jurisdictions that have different privacy environments to Australia. Additionally, they often feature cloud-based interfaces making then accessible from anywhere in the world. Given this, questions can be raised in relation to integrity of data held and transmitted from such devices. As an example, many of the control apps for IoT devices are a shared account on middleware that then connects to a provider such as Google or Amazon. This means that any log files generated by these devices may contain data pertaining to multiple households, users and/or families potentially complicating adherence to warrant conditions.

[4] https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/australian-information-security-association-aisa.pdf

b. Are there additional records that agencies should be required to keep or matters that agencies should be required to report on in relation to data retention and to warrants obtained in relation to journalists or media organisations? How can any new reporting requirements be balanced against the need to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed?

AISA recommends that all current reporting required should be completed on time. Further, given the importance of timeliness, agencies should be required to report the cause of any delays in reporting, and the name and agency of the person responsible for authorising the delay. This should be done prior to the reporting date.

A provision should be added that permits media organisations and journalists to seek court orders for the release of any required reporting which agencies have not provided, in the jurisdiction of their choice. The legal threshold for their success in this action should be low.

AISA views the public reporting required around data retention, and related matters such as a warrant, as a vital accountability mechanism. This is not simply statistical reporting. Thus, the information should be reported to the public on time and in full, without excuse. Failure to do so should trigger the opening of legal pathways for the public to seek judicial review.

Actions which extend powers of the State to intercept or seize data, or to break open data (for example, decrypt data), should include new annual or six (6) monthly reporting requirements to the public, again with judicial review if delayed. There are few checks and balances that have been put in place regarding the expanding surveillance powers of the State. Reporting how and when these powers are used to the Parliament and public must be applied and treated with respect.

The reporting to date does not appear to have compromised sensitive investigations. The data is aggregated. The desire to hide capabilities and investigations should not be used as a justification to 'water down' the current level of reporting required, which is already very generalised.

c. Is it appropriate that the Public Interest Advocate framework be expanded only in relation to journalists and media organisations?

AISA recommends that the Public Interest Advocate framework is strengthened to ensure a full briefing, time to consider and an ability to report on issues, processes and outcomes. The coverage of the Public Interest Advocate should be expanded to incorporate new and future media content providers. Within the discussion paper, there are examples given of where there is a clear need to move to technology-agnostic platforms to avoid becoming outdated. This same logic also applies to the media landscape and the ever-shifting landscape in that sector.

AISA contends that contemporary media content creators such as bloggers and podcasters using various means to disseminate their content (such as YouTube, Facebook, TikTok, Spotify and numerous other platforms) also provide public interest content. AISA believes that there is scope for abuse if this ever-changing landscape which represents new media is omitted from the framework. The definition of such media must be widely drafted to include all new forms of citizen journalism, and should certainly cover bloggers as well as others examples listed. The drafting must be so wide as to encompass as-yet-unforeseen new types of journalism born from new technologies.

This broadened definition is for the purposes of the Public Interest Advocate framework, but should equally be applied to all other requirements related to government, agency or private-sector-commissioned-by-government surveillance activities.

A key role of the media in a free and open democracy is to reveal corruption and serious wrong-doing. Increasingly such investigative journalism, which is resource-intensive, is now conducted by specialist bloggers

or other modern media such as podcasters. If they are to fulfil their role our democracy, they must be afforded the same protections and review capabilities as traditional media. To deny this is to remove an important protective element of Australian society that has been enabled by new communication technologies.

d. What would be the impact on reducing the number of officers who may be designated as 'authorised officers' for the purposes of authorising the disclosure of telecommunications data?

Telecommunications interception is a burden on companies and organisations. Larger organisations must often pay highly skilled – and therefore expensive – specialist staff with technical and / or legal knowledge. Given access will at times be necessary, it is important to provide as much flexibility and ease for the organisations on which it imposes as possible. Reducing the number of officers may reduce that flexibility and ease. Therefore, the number of officers who may be designated as authorised officers should not be reduced.

Authors

About the Authors

Joshua Craig – AISA Board Director, MIT, CISM, CISSP, GIA(Cert)

Joshua Craig is a Senior cybersecurity, technology and cloud risk and regulatory professional for ANZ Banking Group. With over 17 years experience in the risk and compliance industry.

Joshua holds a Bachelor of Business, Master in IT as well as industry qualifications such as CRISC, CISM and CISSP, and currently volunteers as a Director and Company Secretary for the Australian Information Security Association. Joshua is also a graduate of the Governance Institute of Australia and standing professional member.

Patrick Fair – Adjunct Professor, Deakin University

Patrick Fair is the principal of Patrick Fair Associates, an Adjunct Professor at the School of Information Technology, Faculty of Science, Engineering and Built Environment at Deakin University and the Chairman of the Communications Security Reference Panel at the Communications Alliance.

Patrick is a member of the IoT Alliance of Australia Security Workstream and General advisor in relation to LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy.

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

Damien Manuel is an Adjunct Professor at 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.

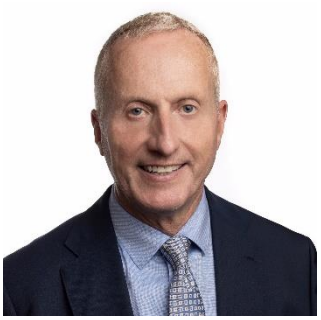
In his former role as the Chief Information Security Officer (CISO) for Symantec Australia and New Zealand, Damien worked with senior executives in the region to align security architectures to industry best practices. Damien also worked as a senior information security governance manager and later as 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, the chair of the ATN Cyber Committee 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.

Michael Trovato – AISA Board Director and Managing Director & Lead Security Advisor of IIS and Research Director ISACA Melbourne Chapter



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.

Tony Vizza – AISA Board Director

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

Tony is a Cyber Security Ambassador for the NSW Government, a member of the Cyber Security 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 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), the Facilities Management Association (FMA) as well as numerous boards.

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, Bengaluru in India. Tony is currently studying 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.

Akash Mittal – AISA Board Director

Akash has over 15 years of IT background in cyber security, compliance, software enhancement, and process optimization. He has worked in various positions across Australian financial and services sector. With a passion towards information security, he is a strong advocate of the importance of cyber awareness.

Akash has over 10 years of experience working within the highly regulated wealth management sector. In his last role at Equity Trustees as General Manager Technology and Security, Akash established a robust cyber security capability and effective governance. Akash has recently joined Trustee Executors as an Executive Technology Officer.

Akash likes solving complex and consequential business problems, and acts as a technology and cyber security advisor to executive management and boards.

Akash holds an MSc in Network Systems, BTech in Computer Systems and is SABSA certified.

Dr Suelette Dreyfus – AISA Board Director

Suelette is a Senior Lecturer in the School of Computing and Information Systems at the University of Melbourne, where she coordinates the flagship undergraduate subject in information security and privacy, and teaches at the Master's level. She has led major research projects in incident reporting in public and private hospitals, in development of free open-source privacy-preserving software and in the international use of secure, anonymous digital dropboxes as anti-corruption tools.

She is a member of the International Council of Transparency International, of the International Council's Academic Sub-Group, and a former board member of Ross House Association.

Prior to entering academia and earning her PhD from Monash University, she worked as a professional journalist, on the staff of *The Herald-Sun*. She then worked on magazines and other publications. She wrote a book about computer hacking that has been translated into seven languages.