Australian Computer Society Inc. (ACT)
ARBN 160 325 931

National Secretariat
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

To the Australian Government Department of Home Affairs,

ACS response to the Reform of Australia's electronic surveillance framework discussion paper

4 February 2022

Dear Sir or Madam

Thank you for the opportunity to contribute to this critical discussion.

The Australian Computer Society (ACS) is the peak professional association for Australia's information and communications technology (ICT) sector, with over 43,000 members.

We're very happy to see that the Australian Government is undertaking this critical review and seeking comments from industry and professionals. For IT and telecommunications professionals, compliance with surveillance frameworks has been challenging, and has often been at odds with the need to ensure general customer security and privacy. There has also been an increasing desire by agencies to "deputise" IT companies (and the professionals that work in such) that we believe represents both a danger to the Australian IT industry and the Australian public. We hope this review can resolve some of those issues and deliver a framework that finds a proper balance of public interests.

In the following pages you will find comments on many of the questions asked in the paper. We hope these are useful for understanding the current concerns of IT professionals.

Thank you so much again for your time and the opportunity to comment on this work, and we'd be delighted to discuss this response and its proposals with you further. If you'd like to discuss any part of this response or simply seek further clarification or input, please feel free to contact myself by email at troy.steer@acs.org.au or by phone on 0417 173 740.

Yours sincerely

Troy Steer
Director of Corporate Affairs and Public Policy
Australian Computer Society

Part 1: Who can access information under the new framework?	
1. Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day? **a) If so, which aspects are working well?** **b) If not, which aspects are not working well and how could the new prohibition and/or offences be crafted to ensure that information and data is adequately protected?**	An important issue is the inconsistency of state and territory legislation. This hinders and may even prevent certain investigations. The planned approach to harmonise legislation should ensure a consistent and level planning field across Australia. This would not only provide equitable approaches across the nation but would also allow vendors and other organisations to have a consistent understanding of obligations, regardless of jurisdiction.
2. Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives, e.g. cyber security of networks, online safety or scam protection/reduction?	
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?	ACS members are sometimes called upon and expert witnesses for a range of criminal activity, both as experts for their employers as well as independent experts. Given that in their expert capacity ACS members might be called by either the prosecution of defendants, a common observation is there should be a mechanism for defendants to access telecommunications evidence without having to request it from the prosecuting agency, effectively "tipping them off" to their defence strategy. It is also a common observation that the officer in charge of an investigation does not have the necessary technical expertise and either misrepresents or under plays the need for the defendant's access to telecommunications evidence, resulting in the request being denied. Another way to put this, is that if the officer in charge had appreciated the need for access, they should have requested the telecommunications evidence already.
4. Do you agree with the	The government's consideration of access is based on the threshold

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?	question of serious criminal activity. ACS members believe there are categories of civil and administrative offences that merit access to telecommunications evidence. Access should be provided to State and Territory anti-corruption agencies who are responsible for investigating and prosecuting serious corruption. The current circumstances require anti-corruption agencies to request access through an authorised agency and ACS members have seen first-hand examples where requests have been denied, frustrated and delayed so that the information is no longer useful. One common observation for rejected requests is that the threshold for Police commencing a corruption investigation is different from ICAC commencing a criminal investigation.

Part 2: What information can be accessed?	
5. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?	The UK definition relies on "telecommunication" and it is unclear whether and when video conferencing and videos fall into the category of communication or of content. ACS members have observed an emerging theme across employers who are foregoing telephony and only implementing video-conferencing services. They are also replacing traditional voicemail with video-clip messages. It is not clear whether or when video conferencing and video-clip messages will be disclosed as communications or protected as content.
6. Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?	Currently there are two categories: Communications and Content. A third category is becoming increasing relevant: Decisions. Ultimately, criminal investigation is about attributing accountability for actions, and actions are the outcome of decisions. It would be grossly unfair to hold a human user accountable for the decisions made for them by another party. Attached to a Decision is the concept of Confidence. Confidence is a measure of the reliability of that decision. If Decisions are to be disclosed, then the confidence of that decision should also be disclosed. With regards to video content, providers are adding data that may or may not be considered system data. If it were system data, it is unclear whether it would be disclosed under the UK definition. For example, the following data might be automatically added to video content by a provider's software (system data): • transcription of audio or audio description for hearing impaired • location • object recognition • algorithmic assertions about people (eg. age, sex, ethnicity, socioeconomics, mood) In essence, it is the broad scope of "system data" that is a cause for concern. The framework is silent on what an agency might do with the collected surveillance data (apart from to whom they may disclose it).

	How the surveillance data is to be processed might impact the authorising officer's decision. Examples might be: • processing using free/cheap facial recognition software versus robust facial recognition software • experimenting with AI versus applying a well-tested algorithm and training data
7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?	ACS members see some difficulty in including machine-learning outputs within the data that can be disclosed. Conceptually, the machine-learning data is a thought process guided by the algorithm and may or may not reflect the thought process of the human user. In arriving at an outcome, the thought process needs to be clearly attributed to the entity making the decision at each decision-making step in the process. In providing access to the thought process, any legislation needs to ensure that the "thinker" has been clearly identified for each step in the process. Also see previous comments relating to the need to disclose Confidence along with the Decision. In the example given at (6), each of the elements may have been deduced by a different "thinker" and each would have a different "confidence". Quantum computing issues are also likely to be an emerging factor that this legislation may be too early to capture. The use of quantum technologies, and subsequent usefulness of evidence collection and analysis techniques are too early to usefully define. The biggest challenge will be collecting and preserving evidence in a reliable manner.
8. What kinds of information should be defined as 'content' information? **What kinds of information should be defined as 'non-content' information?**	
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?	Part (b) of the UK definition is: *anything which is systems data is not content*. ACS members foresee a difficulty in this definition when content is duplicated as system data. An example is security software that records passing traffic in a log file. The log file could be interpreted as "systems data". Also, ACS members have seen firsthand numerous examples where the meaning of the content can be deciphered from the metadata. For example, telecommunications records currently display the number of characters for messages. Where the message is a response to a question, the answer "Yes" or "No" could be inferred from the metadata. Members have also seen firsthand where the response "No" has been confused with the response "OK". Such inferences can be the critical where the message is relied upon to demonstrate consent or refusal.
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?	
11. Should the distinction between 'live' and 'stored' communications be maintained in the new framework?	While ACS members agree with the distinction between "live" and "stored" communications, there is some nuance. For example, is a communication that is now stored on a handset waiting to be read a communication or a stored communication? What is the threshold for "read"? Is it: • read by the intended recipient • read by the intended recipient's device • read by someone else (for example on an iPad linked to the intended recipient's iPhone)? What onus is on the investigator to understand these nuances and make decisions on them that have consequences on people's lives? For example, ACS members are aware of numerous drivers being prosecuted for reading SMSs while driving, when they were actually read by someone else.
12. Do each of these kinds of information involve the same intrusion into privacy? **Or should the impact of each be considered differently?**	This really relates to what is considered system data and ends up being disclosed. ACS members expect a workable solution would align this to the definition of Sensitive Information already in the Australian Privacy Act.
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?**	ACS members expect that this is fairly applied across entities servicing Australians, regardless of whether the service provider is "Australian". In considering "fair" there is a balance in the capacity of service providers to store the data and respond to requests for access. A service provider should not be seen to be in breach of assistance orders where they lack the technical or financial resources to implement such requests. ACS members also don't want innovation to be limited due to the threat of compliance. ACS suggests that small suppliers should be given financial or technical support to help them meet any requirements to comply with requests.
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?**	The ability for agencies to access devices and use them as tracking devices is poorly defined. While phones might be well understood, there are other devices that might be used for tracking. For example: • devices carried by a person (eg. smart watch, smart card) • medical devices carried on a person (eg. insulin pump) or implanted in a person • devices within a smart home or office

	• digital personal assistants (eg. Alexa, Siri, Google) • on-board computers in vehicles • personal and asset tracking (eg. Apple Air tag, Tile, Galaxy SmartTag)

Part 3: How can information be accessed?	
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?	While the ACS support the intent of a outcomes-based framework to simplify authorisations, this simplification leaves too much room for agencies to avoid scrutiny of their surveillance actions. An outcomes-based approach suggests that the source of surveillance data will not have to be disclosed, which means assessments of accuracy and reliability will not be able to be made. This will result in those wrongly accused having an increased burden to prove their innocence – likely a burden they will be unable to overcome. If an outcome-based framework were to be adopted, it should be accompanied by a comprehensive list of approved sources, with agencies selecting sources as part of the authorisation process. This implies the need to establish an independent panel to assess and approve data sources.
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?	

Part 4: When will information be accessed?	
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?	ACS members are concerned about the prospect of scope-creep in relation to: *categories of offences that may not meet the recommended five year threshold but cannot be effectively investigated without covert access to communications content*. We do not believe that authorising officers will be able to judge whether or not offences fall into this category and propose that any such addition is supported by a clear framework for deciding how authorising officers can arrive at the decision to allow surveillance in these cases.
18. Are there any other changes that should be made to the framework for accessing this type of data?	
19. What are your views on the proposed thresholds in relation to access to information about a person's	

location or movements?	
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)?	While ACS members support the targeting of specific persons, rather than computers, the onus for such targeting a person and matching devices to that person has to managed be with an agency. Technology suppliers cannot be expected to match devices to persons. Technology suppliers might be expected to assist by tagging devices with personas. If so, there needs to be a clear identity framework governing the reliability of those personas. This is particularly challenging with devices that may have multiple shared users (in an organisational or home context) and with potential for remote access (by authorised users) to share devices more widely.
21. Is the proposed additional warrant threshold for third parties appropriate?	ACS members are concerned about any proposal that creates an onus on technology suppliers to identify the third parties. The onus to identify suspects, including third parties, must be with an agency, with technology suppliers merely acting on an agency's request to provide records relation to specific persons and specific things.
22. Is the proposed additional threshold for group warrants appropriate?	ACS understands why agencies may want to monitor groups. The onus for identifying members of a group should be with an agency and technology providers cannot be expected to identify group members.
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?	The ACS has concerns about collective surveillance of groups merely because they use a specific technology, including hardware or software. Agencies should not be allowed to obtain a warrant to access data for all users or a specific application. Instead, agencies should have to identify specific characteristics that can be used to select specific people that merit surveillance. Again, the onus for selecting specific people, based on characteristics, should be with an agency, not a technology supplier.
24. Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?	The ACS supports requiring independent authorities such as Courts or Tribunals to authorise surveillance. The ACS also strongly supports the proposal that judges, magistrates and tribunal members will need support from suitably qualified experts (ie. public interest advocates) to assist in their deliberations regarding the need for some orders, specifically those requiring technology suppliers to modify commercial and retail software or devices. ACS members have formally and informally assisted judges and tribunal members in these deliberations and have observed first-hand the difficulties faced when they are provided supporting information only from agency-appointed experts. As Australia's peak body for the IT professions, the ACS is well placed to administer a panel of experts as public interest advocates, including assessing the competency of panel members.
25. What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?	

26. When should agencies be required to destroy information obtained under a warrant?	
27. What are your thoughts on the proposed approach to emergency authorisations?	

Part 5: Safeguards and oversight	
28. Are there any additional safeguards that should be considered in the new framework?	
29. Is there a need for statutory protections for legally privileged information (and possible other sensitive information, such as health information)?	While ACS agrees with the need to protect privileged and other particularly sensitive information, the onus for identifying that information should be with an agency. Technology suppliers cannot be expected to identify what information is privileged or particularly sensitive. The ACS also suggest that technology suppliers should not be allowed to not disclose data based on their own assessment of what might be particularly sensitive, including what might be commercially sensitive.
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?	
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?	
32. How could the new framework streamline the existing record-keeping and reporting obligations to ensure effective and meaningful oversight?	

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

Part 6: Working together: Industry and government

34. How workable is the current framework for providers, including the ability to comply with Government requests?	ACS members, in their capacity as expert witnesses, have seen many instances of telecommunications evidence. Unfortunately, they have also seen too many instances where the ultimate product has been erroneous, with errors being introduced by the carrier and/or by the investigators. The ACS suggests that the inputs into the process have so far been overwhelmingly influenced by either an agency, a carrier or a large content provider and suggests that it is well placed to administer a diverse panel of experts to provide an independent lens to the implementation of the framework and of specific operational capabilities.
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?	The ACS rejects the proposal that specific companies could be required to develop "attribute-based" filtering. In essence agencies are trying to shift the cost to companies. Companies might choose to work cooperatively with agencies to build attribute filtering capabilities. If attribute-filtering is used, prosecuting agencies should be able to explain what material has been excluded that might have been exculpatory evidence.
36. How could the new framework be designed to ensure that agencies and industry are able to work together in a more streamlined way?	

Part 7: 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**	ACS members have formally and informally assisted judges and tribunal members in these deliberations and have observed first-hand the difficulties faced when they are provided supporting information only from agency-appointed experts. It is their observation that challenges extend beyond journalists and the media and the provisions relating to public interest advocates should encompass all categories of warrants that require decision-making based on a technology's capability or impact on other consumers of that technology.

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