

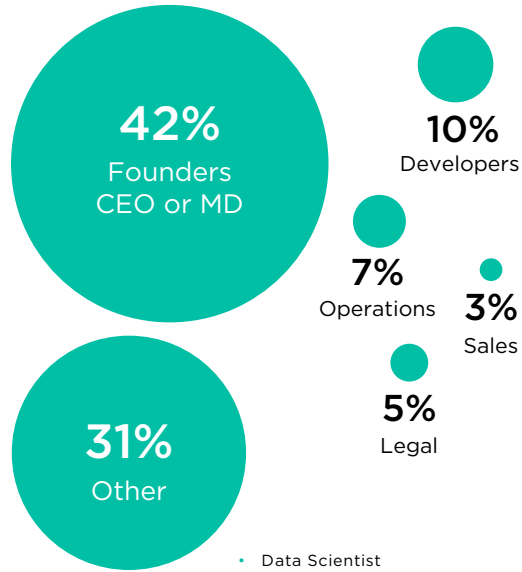


18 DECEMBER 2019

INDUSTRY PULSE | ENCRYPTION LAWS | SURVEY RESULTS

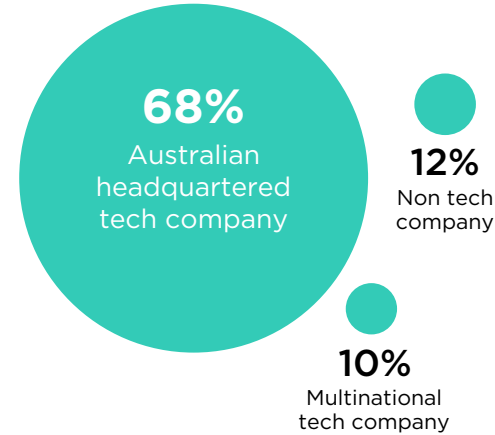


Who did we speak to?



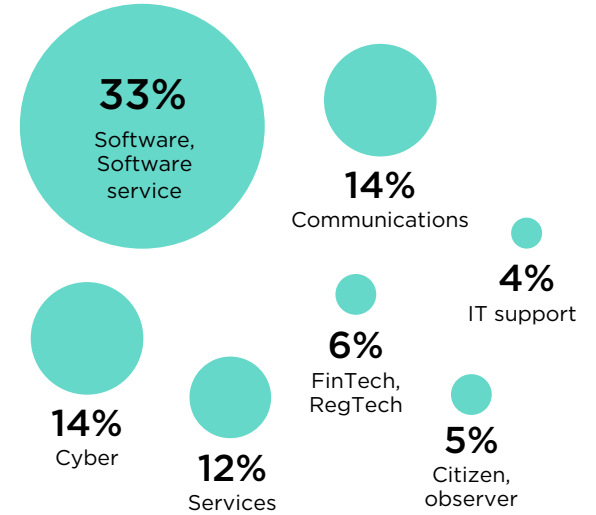
- Complex System Consultant - Security and Governance
- Systems Engineer
- Cloud infrastructure engineering
- Security
- Strategist
- Data Scientist
- Product Management in software
- R&D
- Technology Executive
- Cyber Security Manager
- Product Management
- Consultant
- Board Director

Of what type of businesses?



- Consumer Internet education and Standards development
- Financial services with internal technology services
- University
- Services
- Multinational consulting firm
- Legal services provider (law firm)
- VC

In which industries?



- Assurance, Architecture and compliance services
- Banking, Finance
- Health
- Accounting and Advisory
- IT consulting
- VC
- Cloud

Has your organisation lost sales or other commercial opportunities either domestically or internationally as a direct result of customer concerns about TOLA (Assistance and Access) Act? If so, are you able to quantify the loss?

40% yes

45% no

14% other

- Don't know
- It is hard to be sure, but it seems so
- Still building
- This is difficult to measure
- Unknown
- Too early to tell, but looking that way
- Portfolio companies reporting incidents

It is exactly one year since the TOLA (Assistance and Access) Act was passed by Federal Parliament. Which describes your assessment of the impact of TOLA on the reputation of Australia tech companies in global markets?

51% very negative

44% somewhat negative

3% no impact on reputation

0% somewhat positive

0% very positive

"I expect TOLA to negatively impact the reputation of Australian tech companies based on the assumption that global companies may not be able to trust Australian tech companies"

Have international or domestic customers expressed any concerns about the impact of the TOLA (Assistance and Access) Act on your organisation's products and services?

61% yes

25% no

13% let me explain

"Government customers have yet to really assess possible risks and impacts when cryptographic integrity is weakened."

"Concerns the Australian legislation will be adopted by other nations globally and affect their home countries."

"The threat of requiring decryption will keep anyone away from Australia. It could have severe negative effect on their business elsewhere."

"We produce no products – but fellow mates in [Five Eyes] countries are concerned."

"The industry is losing trust by customers."

"Have had conversations on the risk of holdings client data."

Could the TOLA (Assistance and Access) Act directly affect your business?

50% of respondents said they are directly affected

25% indirectly affected

4% no impact

5% still assessing or having a direct impact on clients

14% citizen observer

Since the passage of the TOLA (Assistance and Access) Act, is your organisation more likely or less likely to perform development operations in Australia?

57% less likely

30% no impact

7% more likely

14% other

- Not yet
- We recommend all our clients to offshore as quickly as possible
- Unknown: consider this a real possibility for some clients
- Too early to comment

For companies with development operations in Australia, since the passage of the TOLA (Assistance and Access) Act, are you more likely or less likely to employ more technical people in these local operations?

51% less likely

4% more likely

40% no change

4% other, don't know or NA

As part of his review, what is the single most important question that Dr James Renwick, the Independent National Security Legislation Monitor, should be asking and to whom?

1. When end-to-end technology integrity is weakened through manipulation of cryptographic algorithms and key management, what is the broader societal impacts in loss of digital confidentiality, integrity and availability to Australian Governance, business and society? Math is math and anyone good or bad can use it.
2. (To the general citizenry) Are you prepared for, and do you want, your privacy and security of your communications - your passwords, internet banking credentials, your confidential personal messaging with partners and loved ones - to become openly accessible and no longer confidential, due to measures introduced to try to catch out criminals?
3. With history constantly repeating itself, what could a person like Hitler done with this surveillance machine?
4. The minister(s) who drafted the bill what exactly their technical qualifications are to justify such a draconian policy.
5. What is the bigger purpose when people can easily circumvent our laws by going to other countries?
6. What will be the effect on Australian companies working in the security area internationally? Will foreign suppliers stop doing business in Australia as it will throw suspicion on their products due to unreasonable Australian requirements?
7. When considering National Security, why is economic success and competitiveness not a primary concern? (This question to Hon Peter Dutton MP, Minister for Home Affairs)
8. Who benefits?
9. How does this Act make Australians more secure?
10. To the people who promote these ill-conceived laws, history has proven it is impossible for highly complex systems to be 100% secure, so how can anyone have confidence in the ability of any organisation to keep encryption back doors 100% secure? These laws weaken security for the general population, to the advantage of the criminal actors.

As part of his review, what is the single most important question that Dr James Renwick, the Independent National Security Legislation Monitor, should be asking and to whom?

continued

11. This is a spying bill - it gives the government the right to spy on everything we do. There is no credible reason to need to do this other than control. Can you please ask, why this is really necessary and insist on a non-double speak answer?
12. Does Australia want to be a democracy with rights, freedoms, and a future?
13. Can the enforcers be trusted with backdoors?
14. Is this a Nation that cherishes freedom? (This question to the Fed Government).
15. Why does the government think that opening a back door is the best way to fight cybercrime? Will a backdoor to my home be next?
16. Where economical consequences considered in the making of TOLA?
17. How can you build trust in, maintain and defend a digital democracy when one of its fundamental mainstays has been deliberately sabotaged by government?
18. How will Australia remain competitive in the market for technology products and services?
19. We need to quantify the benefits vs the cost to industry and the economy. This requires transparency.
20. Why make it easier for terrorists and criminals to attack our systems and harder for Australian firms to compete?
21. How does this make us safer to be worth the risk to our liberties and success as international businesses?
22. Dr. Renwick should ask himself; do I have the authority to restrict access to serial abusers of these powers, and if not how do I ensure that these powers exist?
23. How many times will authorities be allowed to abuse these powers before they are taken away from them? Integer answer required.
24. Does this legislation actually do anything at all other than damage the perception of Australian tech companies? I don't see Facebook caving to a TCN any time soon.

As part of his review, what is the single most important question that Dr James Renwick, the Independent National Security Legislation Monitor, should be asking and to whom?

continued

25. Why are the sentencing recommendations set at 10 years for someone who talks about a TCN they have received, this seems unnecessarily high?
26. (To Dutton) What is the timetable for fixes to restore confidence in Australian tech worldwide?
27. How does TOLA balance valid security concerns with human rights (such as, privacy)?
28. When are the proposed amendments supposed to be introduced?
29. How much jurisdiction “shopping” has occurred since the legislation was passed? Ask of technology companies based in Australia looking to sell their software or hosting services internationally.
30. When will it be repealed?
31. The laws cater for the exception, not the rule. In an environment of increasing cyber security threat how does the government guarantee that the outcome of the laws won't be to negate the security features that ordinary Australians rely upon but most likely don't understand?
32. Are you treating symptoms or the cybersecurity disease ?
33. Warrants required and audit trails
34. How can we amend TOLA to reduce the harm to Australia's reputation and drive confidence and investment back into the Australian cyber industry?
35. How can we guarantee to our customers that their data held in Australia is safe?
36. Cost comparison between economic power a cyber secure technology and mitigating what security agencies have not been able to see for the past 10 years anyway?
37. "Are you stupid?" would be a relevant question to ask the Government.
38. Where is the evidence that the risks and negative effects outweigh the positives, if any?
39. When will it be repealed?
40. Did the Govt. consider the impact on Australian IT industry of AA Act's non-judicial mass surveillance of messaging apps and it's weakening of encryption protocols?

As part of his review, what is the single most important question that Dr James Renwick, the Independent National Security Legislation Monitor, should be asking and to whom?

continued

41. How will the encryption law ensure criminals, terrorists etc cannot use encryption that has no backdoor? If it cannot, the law has barely any impact for criminals, yet creates security risks for law abiding citizens.
42. Who watches the watchers?
43. What was the urgency for passing the legislation?
44. We need to secure our digital borders and keep data in Australia. We need to amend this legalisation to keep Australian data in Australia!
45. How we stop data leaving Australia and ensure data sovereignty?
46. Why is it unacceptable for other nations, such as China to force their legally domiciled companies to spy for them - but when the Australian government does it - it's okay?
47. Will US tech companies hire Australian talent if they understand the true potential of TOLA?
48. What is the impact when criminals simply bypass applications that are subject to TOLA?
49. Why does the legislation not have a double lock, like the snooper's act in the UK does?
50. Not sure.

InnovationAus opened the survey to the Australian technology community on 5/12/2019 and closed on 12/12/2019 at midnight. The publication received input from 70 respondents.

For further information,
please contact:

Corrie McLeod

0419 526 848

corrie@innovationaus.com



InnovationAus 20-40 Meagher Street, Chippendale, NSW 2008

