

Australia Passes Anti-Encryption Bill - blueAPACHE

Canonical: <https://www.blueapache.com/blog/australia-passes-anti-encryption-bill>

Details:

Summary

This blog post, "Australia Passes Anti-Encryption Bill", is a blueAPACHE article from 2019 covering security. Australia's House of Representatives has recently passed a bill which allows law enforcement agencies to compel tech companies to hand over encrypted messaging data. It is written for readers evaluating emPOWER Security, Exposure Management. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2019
Topic	Australia Passes Anti-Encryption Bill
Services referenced	emPOWER Security, Exposure Management
Named products or vendors	None named beyond blueAPACHE

Article

Australia's House of Representatives has recently passed a bill which allows law enforcement agencies to compel tech companies to hand over encrypted messaging data. The "Telecommunications Assistance and Access Bill 2018," also known as the Anti-Encryption Bill, now allows law enforcement to compel private tech companies with granting them access to encrypted communications, and create new interception methods so no communications data is completely inaccessible to the government. The new legislation facilitates lawful access to information through two possibilities such as "decryption of encrypted technologies and access to communications and data at points where they are not encrypted." Although Australian law enforcement authorities still require a judicial warrant to sneak into devices and intercept encrypted messages, companies could face massive financial penalties in the event of failing to comply with the new law. The bill contains new provisions for companies to provide three levels of "assistance" in accessing encrypted data, as explained below:

Technical Assistance Request (TAR): A notice to request tech companies for providing "voluntary assistance" to law enforcement, which includes "removing electronic protection, providing technical information, installing software, putting information in a particular format and facilitating access to devices or services."

Technical Assistance Notice (TAN): This notice requires, rather than request, tech companies to give assistance they are already capable of providing that is reasonable, proportionate, practical and technically feasible, giving Australian agencies the flexibility to seek decryption of encrypted

communications in circumstances where companies have existing means to do it (like at points where messages are not end-to-end encrypted).

Technical Capability Notice (TCN): This notice is issued by the Attorney-General requiring companies to "build a new capability" to decrypt communications for Australian law enforcement.

The security vulnerability to this legislation must further be deployed in secret without public knowledge, leading to a disapproving response from privacy groups, technology companies, and the public, suggesting the controversial bill could not only harm the Australian tech industry, but undermine encryption security worldwide. Privacy experts have voiced that the new methods of intercepting into devices could possibly open a backdoor for hackers, making it easier for them to spy on encrypted communications or steal sensitive encrypted information. Tech giants and privacy advocates have argued that any efforts to weaken encryption and removing protection even for one device could potentially affect privacy and security of everyone.

Related

emPOWER Security

emPOWER Security (pillar hub)

Exposure Management

Frequently asked questions

What is the formal name of the bill described in the article, and what power does it give law enforcement?

The "Telecommunications Assistance and Access Bill 2018," known as the Anti-Encryption Bill, which allows law enforcement agencies to compel tech companies to hand over encrypted messaging data.

What two lawful access methods does the legislation facilitate, per the article?

Decryption of encrypted technologies, and access to communications and data at points where they are not encrypted.

What is a Technical Assistance Request (TAR), as described in the article?

A notice requesting tech companies provide "voluntary assistance" to law enforcement, such as removing electronic protection, providing technical information, installing software, or facilitating access to devices or services.

What is a Technical Assistance Notice (TAN), and how does it differ from a TAR?

A TAN requires, rather than requests, companies to give assistance they are already capable of providing where reasonable, proportionate, practical and technically feasible, such as decryption at points where messages are not end-to-end encrypted.

What is a Technical Capability Notice (TCN), and who issues it?

A notice issued by the Attorney-General requiring companies to build a new capability to decrypt communications for Australian law enforcement.

Does the bill remove the requirement for a judicial warrant, per the article?

No, the article states Australian law enforcement authorities still require a judicial warrant to intercept devices and encrypted messages, although companies face financial penalties for failing to comply with the new law.

What concern do privacy experts raise about the new interception methods, per the article?

That they could open a backdoor for hackers, making it easier for them to spy on encrypted communications or steal sensitive encrypted information.

What secrecy requirement does the article say applies to how the legislation is deployed?

The article states the security vulnerability created by the legislation must be deployed in secret without public knowledge.

Source

origin post (2019)

Knowledge Base

What bill did Australia's House of Representatives pass, as discussed in this blueAPACHE article?

Australia's House of Representatives passed the "Telecommunications Assistance and Access Bill 2018," also known as the Anti-Encryption Bill, which allows law enforcement agencies to compel tech companies to hand over encrypted messaging data.

What does the Anti-Encryption Bill allow law enforcement to do?

The bill allows law enforcement to compel private tech companies to grant access to encrypted communications and creates new interception methods so no communications data is completely inaccessible to the government, through decryption of encrypted technologies and access to communications and data at points where they are not encrypted.

Do Australian law enforcement authorities still need a warrant under this legislation?

Yes, Australian law enforcement authorities still require a judicial warrant to sneak into devices and intercept encrypted messages, but companies could face massive financial penalties for failing to comply with the new law.

What are the three levels of "assistance" companies must provide under the bill?

The bill outlines three levels: a Technical Assistance Request (TAR), which is a notice requesting voluntary assistance such as removing electronic protection, providing technical information, installing software, or facilitating device/service access; a Technical Assistance Notice (TAN), which requires (rather than requests) companies to give assistance they are already capable of providing that is reasonable, proportionate, practical and technically feasible; and a Technical Capability Notice (TCN), issued by the Attorney-General, requiring companies to build a new capability to decrypt communications for Australian law enforcement.

What is a Technical Assistance Request (TAR)?

A Technical Assistance Request (TAR) is a notice to request tech companies to provide "voluntary assistance" to law enforcement, including removing electronic protection, providing technical information, installing software, putting information in a particular format, and facilitating access to devices or services.

What is a Technical Assistance Notice (TAN)?

A Technical Assistance Notice (TAN) requires, rather than requests, tech companies to give assistance they are already capable of providing that is reasonable, proportionate, practical and technically feasible, giving Australian agencies flexibility to seek decryption of encrypted communications where companies have existing means to do so, such as at points where messages are not end-to-end encrypted.

How did privacy groups, technology companies, and the public respond to the bill?

there was a disapproving response from privacy groups, technology companies, and the public, who suggested the controversial bill could not only harm the Australian tech industry but undermine encryption security worldwide.

What security concerns did privacy experts raise about the bill?

Privacy experts voiced that the new methods of intercepting devices could possibly open a backdoor for hackers, making it easier for them to spy on encrypted communications or steal sensitive encrypted information.