Software Industry Warns of Fallout from Australia’s Passage of New Anti-Encryption Legislation

The software industry is raising concerns about the potential consequences of Australia’s recent passage of legislation to provide law enforcement with expansive new powers to compel the disclosure of encrypted data.

According to **ITPro**, the “Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018” was approved by a 46-11 majority in the Australian parliament last month. As **The Verge** reports, the newly passed legislation grants to law enforcement new notice powers of mandatory technical assistance and technical capability, which “require companies to give access to encrypted data if available, or to build the capacity to provide such access if they are unavailable.” Additionally, as reported by **The Verge**, the legislation grants a voluntary technical assistance request power “that does not have to be publicly reported.” According to **The Verg**e, the fine for noncompliance can be up to $10 million AUD (approximately $7.2 million USD).

The Verge reports that the new law also uniquely enables the Australian government to approach individuals such as key employees in order to compel their cooperation rather than limiting the enforcement powers to merely compelling cooperation by institutions. The penalty for any individual’s failure to cooperate could result in a prison sentence.

As **Wired** has reported, the legislation has been strongly opposed by the tech industry on the grounds that “if Australia compels a company to weaken its product security for law enforcement, that backdoor will exist universally, vulnerable to exploitation by criminals and governments far beyond Australia.” Also, as **Wired** has noted, any company that complies with Australia’s law is likely to then be required to provide the same access to another country. **Fortune** suggests that the legislation is particularly intended to target What’sApp and Signal.

According to **The Verge,** Apple’s position on the legislation has been that “encryption is actually a defense against cyberattacks and terrorism” and that “more of it is needed to make citizens safe, not less.” Apple took its concerns directly to the Australian parliament, according to **Threatpost**, which has posted a **letter** reportedly submitted by Apple to parliament. **Threatpos**t also reports that Cisco and Mozilla have also been vocal in their opposition to the legislation. Commentator and human rights lawyer Lizzie O’Shea also observes to **The Verg**e that “once these [backdoor] tools exist, then it would be easy for Australian authorities to share them with their counterparts in allied nations,” particularly since Australia is part of the Five Eyes intelligence sharing agreement in which Great Britain, Canada, New Zealand and the United States also participate.

The Australian government’s position, according to **The Verge**, is that the powers are necessary to defend citizens against terrorism and crime and that the powers will not introduce a “systemic weakness” into the technology. However, a prevailing criticism has been that “systemic weakness” is not actually defined by the legislation. **Fortune** reports that the Australian Labor Party is already seeking to amend the legislation, particularly to define “systemic weakness.”

Clearly, Australia’s new legislation has the potential to have a far-reaching impact on software companies and individuals working in the software industry.