DOJ formalizes request for encryption backdoors

By Malcolm Owen
5 days ago

The US Department of Justice, in conjunction with the "Five Eyes" nations, has issued a statement asking Apple and other tech companies to effectively create backdoors that will weaken encryption strength overall to provide law enforcement access to data.

In a statement released on Sunday by the US Department of Justice, the "International Statement: End-to-End Encryption and Public Safety" is a continuation of the long-running encryption debate. In the latest salvo in the ongoing war, representatives of governments from multiple countries are demanding access to encrypted data for the sake of sexually exploited children.

The lengthy statement demands tech companies "embed the safety of the public in system designs" relating to encryption, to enable companies to "act against illegal content and activity effectively with no reduction to safety," while enabling law enforcement to do its job. This includes enabling law enforcement officials "access to content in a readable and usable format where an authorization is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight."

In effect, the group is asking for access to encrypted data via some form of backdoor meant just for law enforcement, while still keeping it secure to prevent access by hackers and other online criminals.

The group claims it is working with the tech industry to "develop reasonable proposals that will allow technology companies and governments to protect the public and their privacy, defend cyber security and human rights, and support technological innovation."

Though it does agree that "data protection, respect for privacy, and the importance of encryption as technology changes and global Internet standards are developed remain at the forefront of each state's legal framework," it also wants to "challenge the assertion that public safety cannot be protected without compromising privacy or cyber security."

"We strongly believe that approaches protecting each of these important values are possible and strive to work with industry to collaborate on mutually agreeable solutions," the statement concludes.

The statement is signed by US Attorney General William Barr, UK Secretary of State for the Home Department Priti Patel, Australian Minister for Home Affairs Peter Dutton, and other representatives for Canada, India, Japan, and New Zealand.

History repeating itself

The statement is the latest attempt by governments to try and gain access to data that is protected by encryption, which includes versions such as end-to-end encryption that are extremely difficult to monitor. By being able to access encrypted content, investigators would be able to monitor for illegal activity, and potentially gain evidence that could result in the prosecution of criminals.

This has led to a repeated refrain from law enforcement and governments that technology companies should instigate some form of backdoor into their systems to allow access to law enforcement. The same governments also believe it is possible to enable access while keeping encryption secure.

Critics respond by insisting there's no way you can add a backdoor to encryption without weakening encryption itself. The general belief is that bad actors would simply try to attack the backdoor itself to see data instead of trying to beat the encryption directly.

An earlier example of this sort of governmental demand is the UK's MI5 chief Sir Andrew Parker, who urged for more assistance in gaining access to encrypted communications. The February comments by Parker were part of a documentary, which saw the security head tell government ministers it wasn't possible to halt every terror plot, due to a limited capability to see online communications.

The fight against online child sexual abuse angle has previously been deployed by Barr, speaking alongside representatives from Australia, Canada, New Zealand, and the UK in March. That declaration steered clear of mentioning backdoors, but the sentiment to do so was still evident.

For Apple, its use of on-device encryption has led to very public disagreements with the US government, such as presidential demands to unlock iPhones used by criminals, like the Pensacola shooter.

The FBI has also made public calls for Apple to provide backdoors, but following its own breaking of iPhone security, such calls should have ended.

The public fight for encryption and the resistance to break it has led to lawmakers working to introduce laws to force the matter. In June, a Republican bill was introduced to the Senate to try and weaken encryption by ending the use of "warrant-proof" encrypted technology.