Australian Labor government threatens Signal encrypted messaging system

Mike Head
28 July 2025

Meredith Whittaker, the president of the foundation for widely-used global Signal encrypted messaging app, has said it will shut down the system in Australia if forced to hand over its users' encrypted data to the country's political surveillance agency, the Australian Security Intelligence Organisation (ASIO).

Whittaker gave an interview to the *Australian* newspaper today, clearly responding to demands by ASIO and the Albanese Labor government for the not-for-profit Signal Foundation to first create, and then provide, a so-called "backdoor" mechanism for them to access the data of users.

This push by the Labor government was first revealed publicly in April last year. That month, Prime Minister Anthony Albanese held a joint media conference with ASIO chief Mike Burgess and Australian Federal Police (AFP) Commissioner Reece Kershaw to accuse social media companies of refusing to "snuff out" supposed "extremist poison" by handing over access to their users' data.

The Labor government's moves are now threatening the existence of a vital encrypted communications platform. Signal, a free, open-source service, is used by millions of people worldwide to protect their privacy and free speech, shielding their communications from government, spy agency and corporate surveillance and data collection.

Whittaker told the *Australian* that Signal, which is funded largely by donations and grants, is relied upon by "millions of people in Australia" alone.

She said Signal would take the "drastic step" of leaving any market where a government compelled it to provide a means of accessing its data, saying that would create a vulnerability that hackers and authoritative regimes could exploit, undermining Signal's "reason for existing."

The Signal Foundation's stated mission is to protect free expression and secure global communication through open-source privacy technology. Its value, as an end-to-end encrypted service, is that it collects virtually no user data and makes it difficult to discover others on the platform.

Whitakers explained that Signal has no "backdoor" means of accessing its users' communications. "You could come to my house, put a gun to my head, saying, 'give me the data.' I could not give you the data. You would have to shoot because I don't have it. I don't have access to it," she said.

"Our commitment to end-to-end encryption, maintaining robust, technically guaranteed privacy for everyone who uses Signal never wavers. That's the reason we exist. Our ability to make good on that commitment, for the people of Australia who depend on our services—often for very high stakes communication where there is real risk involved—does face threats from legislation."

Whittaker said the forced creation of any "backdoor" would make Australia a "gangrenous foot" for Signal globally. "If you undermine it in Australia—the human rights workers, the journalists, anyone using Signal in Australia—it suddenly creates a weakness for anyone else they are talking to…

"It is very serious, because a backdoor in one part of a network that is interconnected across the world undermines the entire network that becomes the vector through which the privacy of people's communications can be attacked.

"And for many people, private communication is the difference between life and death. A regime that has power over you and can see what you're talking about—can see what you're co-ordinating with your fellow dissidents, can see materials that you are

planning to blow the whistle about, the stakes could not be higher."

Whittaker said government and intelligence use of AI increased the danger. "Ultimately, we're talking about the ability to sustain fundamental human rights in the face of industrial and government pressure that has metastasised surveillance across our core infrastructures over the last few decades."

ASIO and the other Australian intelligence agencies, with their US, UK, Canadian and New Zealand partners, operate as part of the global "Five Eyes" mass surveillance network. This worldwide web is now focussed on the Trump administration's aggressive trade and military confrontations, especially with China, which Washington regards as the major threat to US hegemony.

As the thousands of secret US documents published by US National Security Agency (NSA) whistle-blower Edward Snowden and by Julian Assange via WikiLeaks showed, the Five Eyes partners intercept the communications of millions of people around the globe, routinely exchange data about each others' citizens, and also supply cyber warfare facilities and targeting information to their militaries.

Snowden and Assange also revealed how the US and its allies carry out coups, organise regime-change operations, orchestrate military interventions, assassinate people and initiate public disinformation campaigns.

In 2020, at the behest of the first Trump administration, Australia's previous Liberal-National Coalition government introduced legislation to expand the powers of the country's intelligence network to obtain and share encrypted communications with the "Five Eyes."

That was in addition to the anti-democratic Assistance and Access Act coming into effect that year, with the Labor Party's support. That Act allows intelligence and police agencies to issue "technical assistance notices" or "capability notices" to compel cooperation from technology companies in building in "backdoor" access.

Such measures are invariably portrayed by governments and the media as efforts to crack down on "terrorists" and "child sex predators," yet those activities are already closely monitored by international police agencies, which also have vast interception powers.

The real overriding fear in ruling circles is that working people worldwide use encrypted messages to discuss and organise, free of government eavesdropping, amid mounting anti-genocide and anti-war opposition, social unrest and political disaffection.

The Albanese government is now escalating this offensive, together with the Trump administration. Last week, on the first business day of parliament after the May 3 election, the Labor government also introduced legislation to make permanent and significantly expand ASIO's police-state compulsory interrogation powers.

Unprecedented powers to forcibly question people were first handed to ASIO in 2003 during the supposed "war on terrorism." Under Labor's proposed amendments to the ASIO Act, these powers will be extended and broadened indefinitely to cover four new war-related fields: "sabotage," "promoting communal violence," "attacking defence facilities" and "threatening border security."

If anyone fails to comply or hand over material, or provides misleading information, they face up to five years' imprisonment. Those interrogated also face five years' jail if they tell anyone, except an ASIO-vetted lawyer, over the next two years what has happened to them, thus helping to keep ASIO's operations shielded from public scrutiny.

Albanese revamped his ministry straight after winning the May 3 election, in which Labor only obtained just over a third of the primary vote. One revealing move was to place a key minister, Tony Burke, in charge of ASIO, as well as the AFP and the Australian Border Force, creating what amounts to a repressive Home Affairs super-ministry.