ASIO/AFP clown show foreshadows further crackdown on online privacy

7 May—The Australian government, the national security establishment and their media propagandists continue to exploit last month's stabbing attacks in Sydney, and another incident last weekend in Perth, to advance their campaign to destroy fundamental civil liberties in the name of protecting their self-serving pretence of democracy. As the *Australian Alert Service* reported last week,[1] the Albanese government seized upon the Sydney incidents, and the social media discourse about them, as pretexts upon which to expedite the passage of its "Combatting Misinformation and Disinformation Bill" to end free speech on the internet, which Communications Minister Michelle Rowland has announced she will introduce to Parliament before the end of this year.

Guardian journalist Paul Karp asking the heads of the AFP (left) and ASIO (right) why they aren't using the powers they already have. Photos: Screenshot, AFP

The heads of domestic spying agency the Australian Security Intelligence Organisation (ASIO) and Australia Federal Police (AFP), meanwhile, have used one of those incidents in particular—the (non-fatal) attack on Assyrian Orthodox Bishop Mar Mari Emmanuel by a mentally disturbed 16-year-old Muslim boy—effectively to demand the abolition of online privacy, by calling upon social media companies and other online messaging services to restrict or remove users' access to end-to-end encryption which makes intercepted communications harder to read. According to ASIO Director-General Michael Burgess and AFP Commissioner Reece Kershaw, speaking 24 April at the National Press Club in Canberra, "voluntary" compliance with this and related requests is urgently necessary to their agencies' efforts to "keep Australians safe" from terrorism, child sexual exploitation and all manner of other evils.

The problem with their story, however, is that they have in fact had practically unlimited authority to compel compliance from any and all providers of electronic communications services ever since the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* was rushed through Parliament on a similarly "urgent" basis almost six years ago—but which, as one sharpeyed journalist at the NPC event pointed out, they have *never actually used*. From which, combined with the spurious nature of the "terrorism" charges laid against the attacker's juvenile alleged associates following hugely over-the-top police raids on their family homes the same day, it would seem that as they have been caught doing before, the AFP and ASIO are at best grossly exaggerating and at worst have simply fabricated a threat, to justify yet another grab for power over the people they are supposed to serve.

Be afraid, be very afraid

Burgess opened proceedings by listing what he called the "dynamic tensions between security and technology", of whose resolution he and his fellows are bidding to be anointed the unquestioned arbiters. "The internet is a transformative information source—and the world's most potent incubator of extremism", he said. "The smart phone is a brilliant communication tool—and an all-in-one surveillance device, listening when you're not on the phone, tracking your movements and recording your browsing. Social media is a convenient way to connect with family, friends and the world—and a convenient way for scammers, criminals and spies to connect with you. *Encryption protects our privacy and enables our economy—and creates safe spaces for violent extremists to operate, network and recruit.* [And] depending on who you speak to, at one extreme, artificial intelligence [AI] will save humanity—and at the other extreme, it will destroy it." (Emphasis added.)

Whilst he had interesting (and deceptive) things to say on all those subjects, the main thrust of Burgess's remarks was that "terrorists and spies … [have been] early adopters" of end-to-end encryption, which therefore is and shall remain a dire threat to our so-called democracy—unless, presumably, ASIO is allowed to dictate when and by whom it can be used. "In recent years, tech companies have significantly expanded and extended their use of encryption", he said, "and from what the industry is saying, they plan on expanding its use even further. Encryption is clearly a good thing, a positive for our democracy and our economy. It protects privacy, it enables communications and transactions. But at the same time *it also protects terrorists, spies, saboteurs and the abhorrent criminals Reece will talk about*." (Emphasis added.) Even ASIO's most unsophisticated targets, he added, "routinely use secure messaging apps and virtual private networks to avoid detection and hide their activities", such that they now "damage intelligence coverage" in "virtually 100 per cent" of counterterrorism and espionage cases, up from 97 per cent in 2021.

Burgess insisted that he was "not calling for an end to end-to-end encryption", nor asking for new laws or powers, nor even more resources. Indeed, he said, "I am not asking the government to do anything." Rather, "I am asking the tech companies to do more. I'm asking them to give effect to

the **existing** powers and to uphold **existing** laws. Without their help *in very limited and strictly controlled circumstances*, encryption is unaccountable … like building a safe room for terrorists and spies, a secure place where they can plot and plan." (Bold emphasis in original; italic emphasis added.) There is already a "very clear and well established legal framework that allows ASIO to seek warrants to access communications", he acknowledged—namely (though he did not name it) under the aforementioned *Assistance and Access Act 2018*. Burgess claimed however that "even when the warrant allows us to lawfully intercept an encrypted communication, we cannot actually read it without the assistance of the company that owns and operates the app. *The company has to be willing and able to give effect to our warrant.*" (Emphasis added.)

Kershaw, citing the distribution of child abuse material and radicalisation of young people via encrypted chats, accused social media companies in particular of "pouring accelerant on the flames" of "social combustion" through their "indifference and defiance" to the legitimate needs and requests of Australian authorities to remove offending materials and, he implied, to help them break encryption. "Numerous law enforcement agencies, including the AFP, have appealed to social media companies and other electronic service providers to work with us to keep our kids safe. … [And] if a judicial officer decides there is reasonable suspicion that a serious crime has been committed, and it is necessary for law enforcement to access information to investigate that serious crime, *tech companies should respect the rule of law and the order of a court, or independent judicial authority*, and provide that information." (Emphasis added.)

Everything quoted above from both men is the exact literal truth. By its construction, and most importantly by what it omits, it is the biggest lie you will hear today.

Busted

In the Q & A session that followed, most of the journalists present took Burgess and Kershaw's comments at face value. Not so *Guardian* chief political correspondent Paul Karp, who brought the whole propaganda charade undone with one incisive question.

"More than five years ago, Parliament passed the supposedly urgent legislation to help law-enforcement agencies break encryption", Karp began. Holding up an A4- size graph, he continued: "I've got the latest data on how many times these new powers have been used, and you'll see that the Technical Assistance Requests, which is the voluntary cooperation from the tech companies, [are] reasonably well used; 66 times last financial year. The compulsory powers, Technical Assistance Notices and Technical Capability Notices—a big fat zero [by] all agencies last financial year, and the year before that. So, my question, please: Why are you asking the tech companies for more cooperation, instead of escalating and using the powers that you *already* have to compel it?" To which the hapless Kershaw replied: "I think you'll see in this financial year a 100 per cent increase on that zero." After some chuckling from the crowd and reminder from Karp that "100 per cent of zero is zero", Kershaw clarified that "what I am aware is that there has already been one [notice] issued".

Which is to say, in case it were not clear, that for all Burgess's implicit accusations that social media and the "tech industry" in general are wilfully enabling terrorism, spying, scams and extremism, and Kershaw's of protecting child abusers as well, the sector has until now done every single thing but one that ASIO, the AFP or anyone else with the authority has asked of it. The rest is all smoke, mirrors and threat-inflation humbuggery. Sure, Burgess and Kershaw are not asking for additional powers—yet. But Kershaw in particular, with his demand that "work[ing] with us to keep our kids safe" must include "not transitioning to end-to-end encryption until they can ensure their technology protects against online crime rather than enabling it", is clearly at least setting the stage for such a request in the near future. One more reason to remain especially vigilant regarding the Albanese upcoming government's mis- and disinformation bill, whose contents are as yet unknown to the public.

Footnotes

1. "Albanese gov renews push for global internet censorship", *AAS*, 1 May 2024.

By Richard Bardon, Australian Alert Service, 8 May 2024
