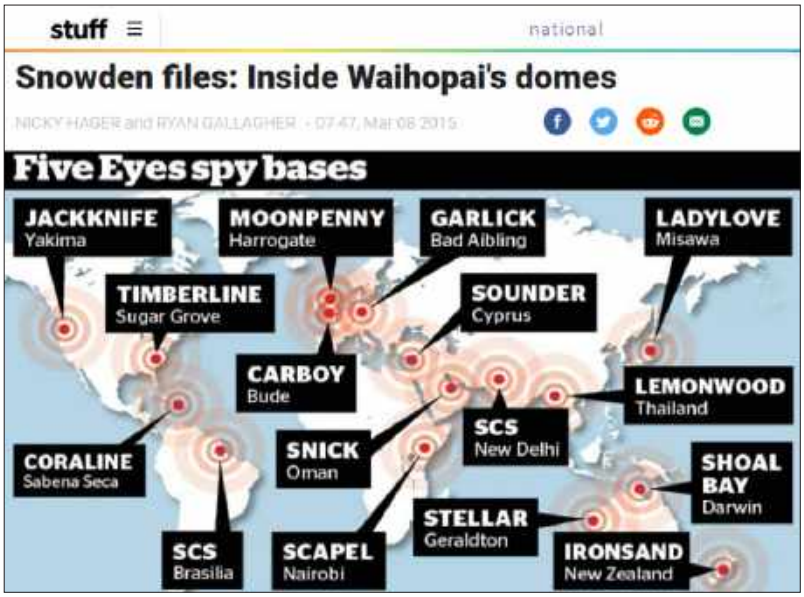
Five Eyes 'national security' blob absorbs competition regulator

By Richard Bardon

Like the titular alien amoeba in the classic 1958 horror film *The Blob*, which grows to monstrous proportions as it engulfs and devours every living creature it touches, the Anglo-American Empire's overarching "Five Eyes" intelligence apparatus is busily absorbing every aspect of Australia's administrative and policy-making institutions it can reach. The latest is the Australian Competition and Consumer Commission (ACCC), the independent statutory authority within the Department of the Treasury which regulates the nation's markets and critical infrastructure. Since its inception the Morrison government, even more so than its predecessors, has used every excuse it could find to expand the powers of Canberra's intelligence agencies in the name of protecting "national security", a process it has accelerated markedly under cover of the COVID-19 pandemic. Co-opting the ACCC—whose bland bureaucratic façade belies extraordinary, in some cases almost dictatorial powers—into the Five Eyes intelligence-sharing arrangement, along with its counterpart agencies in the other member states (Canada, New Zealand, the UK and the USA), removes several of the remaining legal barriers to its intended universal surveillance. Between that and the new powers planned for Canberra's electronic spying agency the Australian Signals Directorate (ASD), few if any areas of Australia's economy and her citizens' everyday lives will remain off limits to the Five Eyes' prying gaze.



A map from stuff.co.nz showing Five Eyes spy bases around the world, based on NSA information revealed by Edward Snowden. Photo: Screenshot

The ACCC announced its absorption by the Five Eyes blob, albeit not by name, in a 3 September press release. "Competition agencies from five countries including Australia will share intelligence, case theories and investigative techniques to better coordinate investigations across international borders", it stated, thanks to a memorandum of understanding (MoU) signed that week which "includes a template 'Model Agreement' that the agencies can use to establish cooperation arrangements focused on investigative assistance such as the provision of mutual assistance, sharing of confidential information, executing searches and seizures and cross-border evidence-gathering". Dubbed the Multilateral Mutual Assistance and Cooperation Framework for Competition Authorities (MMAC), the agreement was "signed virtually" on 2 September by representatives of the US Department of Justice and Federal Trade Commission; the UK Competition and Markets Authority; the New Zealand Commerce Commission; the Competition Bureau Canada; and the ACCC. It came into effect the same day. Ostensibly the MMAC is directed towards improving cooperation on matters such as the misuse of market power by large digital platforms (upon several of which, notably Facebook and Google, the ACCC has had a particular focus of late), in a manner similar to that in which the ACCC "has already been cooperating closely with other competition agencies within the framework of the OECD and International Competition Network for over 20 years" on such matters as international shipping cartels. ACCC Chairman Rod Sims is quoted saying that the MMAC merely "complements our existing formal and informal cooperation agreements with competition agencies in the US, Canada and NZ … [and] will improve the effectiveness and efficiency of competition investigations that span multiple jurisdictions." A close reading of the MMAC itself, however, reveals glaring and therefore presumably deliberate loopholes that might be exploited to extend the already pervasive surveillance powers of the signatory nations' intelligence agencies.

No right to remain silent

It should be noted at the outset that as an MoU between agencies rather than a formal international treaty, the MMAC—as its own text declares—is not legally binding upon any party. As a statement of intent, however, it warrants careful analysis nonetheless, for two reasons. First, history shows that in all five countries, Australia most of all, governments have time and again proved willing to wave whatever enabling legislation the intelligence agencies want through their legislatures unchallenged. And secondly, the ACCC is subject to few constraints on what it can do with the information it gathers in any case.

The MMAC, like the press release announcing it, does not mention the Five Eyes arrangement by name, preferring merely to allude to it with the statement in its opening "recitals" section—that is, the list of principles and precedents upon which it is founded—that the signatories "[recognise] that their respective jurisdictions all have some form of information sharing legislation that allows for sharing of confidential information in certain circumstances". Among the oldest, and certainly the most consequential of these is of course the 1946 "United Kingdom-United States of America Agreement" (UKUSA) regarding cooperation on signals intelligence, which by 1956 had expanded to include Australia, Canada and New Zealand, thereby formalising the Five Eyes.[1] As this news service and others have long maintained, and as US intelligence whistleblower Edward Snowden proved in 2013, the arrangement gives the five countries' intelligence agencies unfettered access to all data collected at home and abroad.

1. G. Peut, A. Isherwood, A. Douglas, "Australia prepares for world war: tragedy, or just plain farce?", *The New Citizen*, June-July 2012.

Often, however, information on those nation's own citizens cannot legally be accessed, since the letter of the law generally does not permit their electronic spying agencies to operate on home soil (p. 14) therefore either some pretext must be found, or a plausible foreign source invented. This is where the ACCC's extraordinary powers could come into play.

As stated on its website, "[the ACCC's] role is to enforce the *Competition and Consumer Act 2010* … and a range of additional legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians." To this end, Section 155 of the *Competition and Consumer Act* (CCA) grants the ACCC compulsory information-gathering powers, including the ability to requisition documents from parties subject to the CCA—which is to say, virtually every business in the country, and anyone involved in running them—and to compel them to give evidence under oath or affirmation. Australian commercial law firm LegalVision states in an overview of the ACCC's powers that as a rule, compliance is mandatory, and that "The consequences of not complying with the ACCC's requests may include fines and in certain situations imprisonment." Not only may the documents or testimony so acquired be used "to assist with making decisions relating to investigations and potential contraventions of the Act … [and] in legal proceedings that arise from the investigation", the overview continues, but "The information you have provided will not be able to be restricted in its use, meaning the ACCC has discretion in the way that it will use the information." It is, however, legally obliged to comply with requests to keep information confidential from third parties, provided said information is "clearly marked confidential … [and not] information that is generally publicly available."

The MMAC, though, includes a loophole that might as well have been designed to bypass such restrictions. "Each Party shall respect its own law with respect to legal rights and privileges when requesting or providing Investigative Information", its Model Framework prescribes, "and shall endeavour not to request or provide Investigative Information that it knows is protected by any legal right or privilege in the other Party's jurisdiction." (Note the equivocal "endeavour not to", rather than a stronger formulation such as "shall not".) But should the Responding Party oh-so-accidentally transmit information "that is later identified as privileged or protected against self-incrimination under its law [the latter of which does not exist under the CAA], the Requesting Party shall ensure that it does not use such information for the purposes of the enforcement of its Competition Laws and shall use all appropriate procedures to limit the disclosure of such information in other contexts".

This last would appear to prevent disclosure to, say, an intelligence agency. But not so fast; because a couple of pages thereafter, Section 11, which deals with confidentiality, explicitly states that "This Agreement does not prevent disclosure of Investigative Information received under this Agreement: a) to Persons that are subject to an enforcement proceeding brought by a Requesting Party if such disclosure is required by its law as determined by the Requesting Party; b) to courts and tribunals in the course of a judicial or administrative proceeding; or c) when the Requesting Party advises the Responding Party it is required to do so under its law." In other words: Whenever we say so! And then to muddy the waters further, Section 12 on "Limitations of Use" states that "Investigative Information provided to the Requesting Party pursuant to this Agreement may be disclosed or used by the Requesting Party solely to administer or enforce its Competition Laws with respect to the investigation specified in the request and for the purpose stated in the request." But two clauses later, it contradicts itself by stating that such Investigative Information *can* be "disclosed or used by the Requesting Party with respect to the *administration and enforcement of laws other than its Competition Laws* with the consent of the Responding Party." (Emphasis added.) Not that it really matters, because Section 12 is qualified by Section 11's "whenever we say so" clause anyway.

Patching the holes in the dragnet?

As the *Australian Alert Service* has reported, the suite of so-called national security laws the Morrison government intends to ram through a pandemic-truncated Parliament by year's end includes a bill to amend the *Security of Critical Infrastructure Act 2018*, so as to broaden dramatically the definition of the "critical infrastructure" which the ASD is authorised to protect from cyber attack.[2] Whereas at present this includes only such things as electricity, gas, water, mass transport, communications and payments systems, changes foreshadowed in a 6 August Department of Home Affairs discussion paper would see it expanded to encompass the *whole banking and finance sector*, universities, the food and grocery industries, and more. The owners and operators of any business or industry so named would thereafter be forced, according to the 6 August *Sydney Morning Herald*, to "pass on information … to the Australian Signals Directorate in real time, and potentially allow the cyber spy agency into their networks to fend off major hacks. … At the lowest level, this would impose an obligation on companies to send the ASD 'signatures'—a file containing a data sequence used to identify an attack on the network—when they are being attacked. Under the approval of Home Affairs Minister Peter Dutton, the ASD could also be given access to the network to monitor and defend against significant cyber attacks." Which is to say, the ASD would be able to intrude into virtually every aspect of Australians' lives on Dutton's or his successors' say-so, on the basis of a cyber attack that could just as well have been instigated by the ASD itself, or by some provocateur in the Five Eyes' employ.

Roping the ACCC and its counterparts into the Five Eyes network, with a focus on digital platforms and online marketplaces, would provide yet another angle from which businesses and, indirectly, the population at large could legally be spied upon via their economic activity, while providing the ASD et al. a plausible source to which they could attribute intelligence gathered illicitly. And given the ACCC's power to disrupt businesses' operations essentially on a whim, to the extent that it can virtually dictate who is and is not allowed to operate in almost any sector, it is no stretch of the imagination to envision it becoming in short order a bludgeon with which the Five Eyes agencies could beat down competition to favoured—and in Australia's case, all foreign—companies which, as Snowden revealed, are often eager accomplices in illegal surveillance of their customers. If such power belongs in any hands at all, it is certainly not those of a supranational spy ring like the Five Eyes. Once again, the Morrison government is ceding to foreign powers the national sovereignty it claims to be protecting.

---

2. "Morrison government's 'national security' hypocrisy exposed", *AAS*, 26 Aug. 2020.