Sweeping security law would have computer users surrender privacy

September 18 2014, by Keiran Hardy

So broad is the amendment bill's definition of computer that a warrant could arguably give ASIO access to all computers connected via the internet. Credit: AAP/Dan Peled

Parliament is about to consider a range of changes to Australia's security laws introduced by the Abbott government during its last sitting. The most controversial measures in the National Security Legislation Amendment Bill 2014 (Cth) include stronger anti-whistleblower provisions and a "special intelligence operations" regime that would

grant ASIO officers immunity from civil and criminal liability.

Less attention has been paid to proposals to expand ASIO's powers to collect intelligence held on computers and computer networks. Like the government's proposals to require the retention of metadata, these measures suggest the power of intelligence agencies to invade Australians' privacy will dramatically expand.

Flinging open the door to computer access

Section 25A of the Australian Security Intelligence Organisation Act 1979 (Cth) (ASIO Act) currently allows the attorney-general to issue a computer access warrant when requested by the director-general of security (the head of ASIO). The warrant may be issued if the attorney-general believes on reasonable grounds that access to data "held in a particular computer" would substantially assist the collection of intelligence that is important for security.

ASIO officers may then undertake activities to obtain that data. These include entering private premises and doing any other thing necessary to conceal their actions.

"Computer" is defined in the Act as "a computer, computer system or part of a computer system". This means that a computer access warrant gives ASIO access to only a single computer.

The government proposes to amend the statutory definition of computer so that a single access warrant may apply to multiple computers and networks. The ASIO Act would then define "computer" as:

a) one or more computers;

b) one or more computer systems;

c) one or more computer networks;

d) any combination of the above.

What this means is that wherever the word "computer" (singular) appears in the ASIO Act this should be understood as referring to any number of computers or computer networks (plural). Importantly, the legislation does not attempt to define computer network. In a peculiar feat of legislative drafting, a singular noun would refer to a potentially limitless number of electronic and telecommunication systems.

The only effective limitation is that the warrant must specify a particular computer, a computer located on particular premises, or a computer associated with or likely to be used by a particular person. Again, these should be read as plural. This means that ASIO could, for example, specify multiple computer networks located at a university, or other computer networks to which a person has access.

The Bill would also allow access to data through computers owned by third parties (friends, relatives, co-workers). This would be allowed where it is "reasonable in all the circumstances to do so". ASIO officers would be empowered to cause material interference with computers or computer networks if necessary to execute the warrant, so long as this does not cause material loss or damage.

Everyone's privacy is at stake

The government's metadata proposals have attracted far more attention, but these other changes will also dramatically expand ASIO's ability to invade the privacy of Australian citizens.

At its broadest, access to multiple computer networks could plausibly entail access to all computers connected to the internet. The internet is a

network of computer networks, so there is no reason why this would not fall within the scope of the legislation. The internet is certainly "likely to be used" by the person of security interest, as the legislation requires.

This is not likely the intended meaning of the provision, but it shows just how little thought the government has put into placing some sensible restrictions on the warrant provisions.

A more realistic scenario is that ASIO would be able to access all computers located at a university where a person of security interest is studying, or at the person's workplace. Even if the government abides by this "narrower" interpretation, the legislation will still expose large numbers of innocent persons to potentially severe invasions of their privacy.

One way to restrict the potential impact of these provisions would be to define "computer network" so that it encompasses only those computers located on a particular premises or associated with a particular person. This language is already contained in the Bill, although it does not restrict the scope of the powers to this degree.

Another method would be to specify that ASIO can only access parts of a computer or computer network where doing so is reasonably necessary to collect relevant intelligence. Yet another would be to specify that ASIO can access multiple computers only after it has exhausted other methods of obtaining the intelligence.

These are all viable ways to limit the potential impact of the warrant provisions. They would still allow ASIO significant scope to access data held on multiple computers. The government, however, has made no effort to include such limiting factors in the legislation.

Good law should be clearly stated

The lack of any clear limits on these provisions is not merely the result of the government's attempts to expand ASIO's powers. The government faces an incredibly difficult task of drafting legal language in such a way that it accurately describes and accounts for new and emerging technologies.

The government has approached this challenge by avoiding clear definitions of key terms in the Bill. On one possible view, this is a sensible solution. It gives intelligence agencies sufficient power to collect intelligence without being confined by statutory definitions that are likely to be superseded by further advances in computer technology.

But in doing so the government is granting ill-defined powers to intelligence agencies when the privacy of all Australian citizens is at stake. The law should be stated clearly in advance. Vagueness and overreach are not adequate responses to difficulties in legislative drafting.

When Parliament considers the amendments, it should take the time to ensure that the computer access warrant powers are clearly defined and that any invasions of privacy are kept to the minimum necessary. If the period of law-making after September 11 taught the country anything, it is that laws enacted hastily in response to security threats are often poorly drafted and overly broad.

Parliament should also be careful that debate on the amendments is not overshadowed by the government's next tranche of national security reforms. The threat to security posed by returning foreign fighters and the threat to privacy posed by data retention are certainly important issues. But granting ASIO these powers of access in their current form also poses a real threat, particularly to the privacy of individuals in workplaces and universities.

The National Security Legislation Amendment Bill (No. 1) 2014 has been referred to the Parliamentary Joint Committee on Intelligence and Security, which will present its report during the week of the parliamentary sitting beginning September 22.

Source: The Conversation