Political police will hack into computers

Wide new powers for Australian spy agency

Mike Head
27 March 1999

Australia's political intelligence agency will be able to hack into computers via the Internet, plant tracking devices on people and obtain emergency warrants to enter and search premises under a new Bill introduced by the Howard government on Thursday. These provisions have serious implications for free speech and the right to political discussion, particularly in relation to use of the Internet.

The Australian Security Intelligence Organisation (ASIO) Legislation Amendment Bill contains other sweeping provisions as well. Introduced with little publicity, it provides for the greatest expansion of ASIO's power since the ASIO Act was first passed in 1979. For the first time, ASIO--the federal government's internal political spy force--will have authority to collect foreign intelligence, intercept articles delivered by private couriers as well as Australia Post, and access taxation files.

Some of these measures were first mooted last year, when a leaked Australian Federal Police document indicated that the government was planning to use the Sydney 2000 Olympic Games as a pretext for boosting ASIO. The revamped Bill makes it plain that ASIO's capacity to conduct pervasive surveillance will be permanent, not specifically tied to the Olympics.

In the name of protecting the "national security", the Bill gives ASIO far-reaching powers to retrieve and alter information from any computer or computer system, including an Internet service provider, regardless of any state or federal law.

ASIO officers will be empowered to seize data obtained by "remote access"--commonly referred to as hacking--or by direct physical access to a computer system under an entry and search warrant. They will be authorised to crack and modify password control systems and encryption programs, opening the way for the sabotage of web sites, e-mail facilities and internal communications systems.

The explanatory memorandum circulated by Attorney-General Daryl Williams states: "The computer provisions permit the Minister to authorise ASIO to add, delete or alter data for the purpose of gaining access to data in a target computer and to do things that are reasonably necessary to conceal that anything has been done under the warrant. This would include modifying access control and encryption systems."

Since it was formed by a Labor government in 1949 to crackdown on post-war political unrest, ASIO has been notorious for harassment, dirty tricks and frame-ups directed against government opponents and political dissidents, including socialists. Official hackers will now be in a position to extend these activities via the Internet.

In an unprecedented move, ASIO will be authorised to install tracking devices--electronic beacons or even chemical substances--on people or in vehicles, with or without consent. This opens the possibility of ASIO maintaining around-the-clock surveillance of targetted individuals.

Other provisions give the ASIO Director General or his delegated officers power to issue warrants--whether for search and entry, tracking devices or "remote access" to computers--in so-called emergencies. In the past the Minister had to approve ASIO search warrants. The new emergency warrants will last up to 48 hours.

In addition, warrants issued by the Minister will last for an extended period--28 days, instead of the current 7 days. No other policing agency can obtain such open-ended warrants. Williams commented: "Unlike law enforcement agencies, most search warrants issued to ASIO need to be executed covertly and it may take time for a suitable opportunity to arise."

No one's banking and tax records will anymore be free from political monitoring. ASIO will be able to request and use individual and business taxation and financial transactions data from the Tax Office and the Australian Transaction Reports and Analysis Centre.

Williams' memorandum reveals that the Sydney Olympics and the subsequent Paralympics are likely to see a great many people placed under federal and state surveillance. The Bill will enable ASIO to provide security assessments directly to state authorities, such as the political police of Special Branch (now known as the Protective Security Group in New South Wales), rather than via the federal police. According to Williams, the change will "simplify administrative processes in the expectation that State authorities responsible for security arrangements for the Sydney 2000 Games and Paralympics are likely to request large numbers of security assessments".

Being able to gather foreign intelligence within Australia will widen ASIO's operations considerably. Until now, it has only been authorised to do so under special warrants. Foreign intelligence has been the province of the Australian Secret Intelligence Service (ASIS), the Office of National Assessments (ONA), the military's Joint Intelligence Office (JIO) and the electronic eavesdropping agency, the Defence Signals Directorate (DSD).

The penalties for obstructing or interfering with the operations of ASIO will also be strengthened, by giving courts the power to impose heavy fines as well as jail terms of up to five years.

By seeking unfettered power to crack open and modify e-mail encryption codes, the Australian government is going further than its British and American counterparts. They have sought to use export controls to prevent the distribution of encryption software, unless national intelligence agencies were able to read the codes. Some companies, including the makers of Pretty Good Privacy (PGP), have refused to comply on the grounds that the First Amendment of the US Constitution outlaws restrictions on free speech.

The actions of the Howard government are on a par with those of the most repressive regimes in the world, which have sought to restrict access to the Internet or develop new techniques to identify and monitor users of the World Wide Web. Among them is the Stalinist government in China, which recently placed an Internet provider on trial for "inciting the subversion of state authority" for supplying Internet addresses to a US-based dissident publication.

ASIO already has the power to bug phones, instal listening devices in offices and homes, intercept telecommunications and open people's mail. The new bid to monitor Internet use underscores the political establishment's unabiding fear of free and democratic discussion on an international scale.