Submission No 120

Inquiry into potential reforms of National Security Legislation

Organisation: Australian Taxation Office

Australian Taxation Office

Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into potential reforms of national security legislation

Introduction

The Australian Taxation Office (ATO) manages the tax crime risk in Australia. We work with other law enforcement agencies, through targeted and coordinated joint agency and taskforce approaches, to combat tax crime including direct and indirect attacks on Australia's tax and superannuation systems.

The ATO is included in the Commonwealth's Organised Crime Strategic Framework as an agency with shared responsibility for addressing the impact on Australia of serious and organised crime. The Commissioner of Taxation is a member of the Australian Crime Commission (ACC) Board and of the Heads of Commonwealth Operations Law Enforcement Agencies (HOCOLEA). The ATO is a member of the Serious and Organised Crime Coordination Committee (SOCCC) and represented on groups that fall under the SOCCC which have high level representation across law enforcement agencies, including Joint Management Groups and Joint Operations Groups.

In 2010-11 the total of all our active compliance activities raised $11.3 billion in liabilities. Our ability to raise liabilities from active compliance activities relies upon our access to information including telecommunications content.

Now more than ever, those who attempt to commit crime, including tax crime, do so electronically. We are facing increasingly sophisticated attempts to systematically defraud our electronic lodgement and processing systems. The ATO's continued ability to access telecommunications information is crucial in allowing us to respond to these threats and to prevent them in the future.

The ATO's current powers under the *Telecommunications (Interception and Access) Act 1979* (TIA Act)

The Telecommunications (Interception and Access) Act 1979 (TIA Act) distinguishes between access to historical telecommunications data (data that is already in existence at the time of the request) and prospective data (data that is collected as it is created and forwarded to the agency in near real time). There are separate provisions for those agencies defined as criminal law-enforcement agencies as opposed to those defined as civil penalty-enforcement and public revenue bodies.

Under the TIA Act, the ATO can only access historical telecommunications data in accordance with our classification as an enforcement agency as our functions include administering laws imposing pecuniary penalties and administering laws relating to the protection of the public revenue. Agencies that can access prospective or real time data include those defined as criminal law-enforcement agencies (such as state police and the Australian Federal Police) and those prescribed as criminal law-enforcement agencies pursuant to the regulations (the Australian Customs Service).

In accordance with sections 178 and 179 of the TIA Act, telecommunications providers can supply information to the ATO including:

- telephone numbers, both land-based and mobile, listed and unlisted,
- name and address details,

- specific itemised call records and reverse call charge records where available,
- information on identification documents supplied by clients when applying for telecommunication services, and
- subscriber information relating to internet address searches.

The ATO is also able to apply to an issuing authority for a stored communications warrant under the TIA Act.

The safeguards and privacy protection currently in place
The ATO has developed strict policies and procedures governing access and use of telecommunications information. We have a clear policy, in a Corporate Management Practice Statement, regarding authorisation processes to be followed when requesting information from telecommunications providers. Further, we have developed a Practice Note to provide direction to our authorised investigators on the use of powers relating to stored communications warrants.

In addition, the ATO is bound by strict secrecy provisions for the protection of information obtained by ATO employees in the course of their duties.

We report annually to the Attorney-General regarding access and use of our powers. This information, including the number of requests to access information, can be provided to the Committee upon request.

The ATO's need to access telecommunications information
The ATO is facing increasingly sophisticated attempts, particularly through identity theft, to systematically defraud our electronic lodgement and processing systems. The scale and frequency of instances of identity fraud are increasing, and are expected to continue to increase. The ATO's ability to access telecommunications information is crucial in enabling our capacity to respond to these criminal actions, work effectively with other law enforcement agencies and ultimately maintain the integrity of Australia's tax and superannuation systems.

However, a major limitation with our current powers under the TIA Act is our inability to access prospective or real time telecommunications information. As the ATO can only access historical telecommunications information, we often face time delays in obtaining critical information to identify offenders and, when working with other law enforcement agencies, to apprehend them. In addition, there is a risk that historical information may not always be retained by telecommunications carriers for a period of time that enables the ATO time to identify its importance and apply for access to it.

The discussion paper *Equipping Australia Against Emerging and Evolving Threats*, prepared by the Attorney-General's Department, discusses the importance of access to real time content in investigating offences committed using a computer or involving telecommunications networks, at page 24:

> Real time content based warrants are available to 17 Commonwealth and State and Territory agencies… The AFP and State and Territory police forces have access to interception powers as part of a nationally consistent approach to combating serious crime. The remaining agencies are a mix of agencies whose functions relate to investigating police integrity, anti-corruption and serious and organised crime.

> While traditionally limited to an offence that carries a penalty of at least 7 years' imprisonment (a 'serious offence'), over time numerous legislative amendments have confused the policy in relation to the circumstances in which interception is available. There are occasions where the general penalty threshold is too high to cover a range of offences for which it is already recognised that general community standards would expect interception to be available. For example, child exploitation offences and offences that can only be effectively investigated by accessing the relevant networks (including offences committed using a computer or involving telecommunications networks) do not meet the general 7 year imprisonment policy threshold.

As part of the Organised Crime Strategic Framework, the ATO plays a significant role in the fight against serious and organised crime. Further the ATO is constantly faced with "offences that can only be effectively investigated by accessing relevant networks (including offences committed using a computer or involving telecommunications networks)" such as refund and credit fraud committed through identity theft. Revenue agencies worldwide are being subjected to increasing attacks on their tax administration systems and the ATO can upon request, provide the Committee with further detail evidencing the attacks on our system.

The ATO's inability to access real time content limits our ability to rapidly respond to these types of threats to the system. Access to real time telecommunications data would enable our investigators to quickly identify those involved in suspected fraud, establish an association between two or more people, prove that two or more people have communicated at a particular time and by what means, or show that a person was at a location at a particular time. Without such access, our investigators will continue to be limited to accessing historical information and hampered in their ability to respond rapidly. The consequences can be significant, as illustrated by the below example:

> A major person of interest in an identity fraud investigation was moving frequently to different parts of Australia, and investigators were unable to identify a place of abode, through the use of surveillance, in order to execute search/arrest warrants on him. The person of interest was enabling the electronic lodgement of income tax returns, prepared using the Tax File Numbers of foreign students and itinerant workers. In some cases the lodgements were being initiated from computers based overseas, particularly in Malaysia.
>
> The logistics of getting surveillance in the same place as the person of interest for sufficient time to make the necessary observations was proving difficult due to the turnaround time of multiple days for the historical telecommunications data the ATO had access to.
>
> The person of interest was subsequently apprehended by the Department of Immigration and Citizenship (DIAC) and deported to Malaysia, before the ATO investigators could execute a warrant on him. The three day delay for receipt of the telecommunications data on his phone, in the week prior to his detention and subsequent deportation prevented the ATO from acting sooner. The result being that the person of interest remained free in Malaysia to continue his attacks on our system and co-ordinate others to do the same.

In the above case, the use of real time telecommunications information by the ATO would have enabled our investigators and surveillance teams to rapidly respond to locate the person of interest and seek to have search and arrest warrants executed. This is the type of pro-active, real time investigative work that the ATO needs to undertake to maintain and strengthen the integrity of the tax and superannuation systems.

ATO reform proposals

At a minimum the ATO recommends that our current powers under the TIA Act and *Telecommunications Act 1997* should remain. Any further limitations imposed on the ATO could jeopardise our ability to manage Australia's tax crime risk and the effectiveness of our active compliance activities. We further recommend that in order for the ATO to more effectively respond to tax crime, particularly to attacks on our electronic lodgement and processing systems, the Committee should give consideration to the following three proposals:

Proposal 1: Implementing Recommendation 7 from the Parliamentary Joint Committee on Law Enforcement's inquiry into Commonwealth unexplained wealth legislation and arrangements

On 19 March 2012 the Parliamentary Joint Committee on Law Enforcement completed its inquiry into Commonwealth unexplained wealth legislation and arrangements. Recommendation 7 of the report was to amend the TIA Act so as to allow the ATO to use information gained by intercept agencies such as the Australian Crime Commission (ACC) and Australian Federal Police (AFP) through telecommunications interception, in the course of joint investigations by taskforces. Law enforcement agencies have advised the ATO that some of the intercept information held by them could be of particular benefit in combating serious and organised crime where the ACC or AFP does not have the requisite evidence to refer the matter for criminal prosecution. Tax responses are now seen as a key treatment strategy in removing the profit from serious criminal activity. These include enforcing lodgement of taxation returns, criminal investigations undertaken by the ATO, audits, application of penalties and recovery of debts. Allowing the ATO to use intercept information that has already been collected by agencies such as the ACC and AFP would enhance our effectiveness in combating serious and organised crime. The ATO is currently liaising with the Attorney-General's Department in relation to this recommendation.

Proposal 2: Including the ATO as a prescribed authority pursuant to the TIA Act to allow access to real time telecommunications data

Access to real time telecommunications data for our investigators will enable the ATO to respond more effectively to attempts to defraud the Commonwealth through credit and refund fraud. The Australian Customs and Border Protection Service is currently the only agency prescribed by regulation as a criminal law-enforcement agency under the TIA Act. In light of the continuing attacks on our electronic lodgement and processing systems, the ATO recommends that it also be prescribed by regulation as a criminal law-enforcement agency and given the ability to access real time telecommunications data to help maintain the integrity of our tax and superannuation systems.

Proposal 3: Retention of communications data for at least two years

The terms of reference note that the Committee will consider whether communications data should be retained for up to two years. This proposal would be consistent with that imposed by the European Union Data Retention Directive. As discussed previously, the availability of this data can be crucial to the effectiveness of investigations, and a minimum retention period would ensure the availability of this data for a set period of time. The ATO supports a minimum data retention period of at least two years.