Commonwealth OMBUDSMAN

Submission by the Commonwealth Ombudsman

INQUIRY INTO THE CYBERCRIME LEGISLATION AMENDMENT BILL 2011

Submission by the Commonwealth Ombudsman, Allan Asher

July 2011

1 INTRODUCTION

On 25 June 2011, the House of Representatives Selection Committee referred the Cybercrime Legislation Amendment Bill 2011 (the Bill) to the Joint Select Committee on Cyber-Safety (the Committee) for inquiry and report. The Committee has invited submissions on the Bill by 26 July 2011.

The main purpose of the Bill is to make amendments necessary to facilitate Australia's accession to the Council of Europe Convention on Cybercrime (the Convention)[1]. The Bill amends the *Telecommunications (Interception and Access) Act 1979* (the Act) to, among other things, require carriers and carriage service providers[2] to preserve stored communications (and telecommunications data) for specific persons when requested by certain agencies. The submission focuses on this aspect of the Bill.

We request that Appendix A to the submission be provided on a **confidential** basis.

2 BACKGROUND

The Commonwealth Ombudsman safeguards the community in its dealings with Australian Government agencies by:

- correcting administrative deficiencies through independent review of complaints about Australian Government administrative action
- fostering good public administration that is accountable, lawful, fair, transparent and responsive
- assisting people to resolve complaints about government administrative action
- developing policies and principles for accountability, and
- reviewing statutory compliance by law enforcement agencies with record keeping requirements applying to telephone interception, electronic surveillance and like powers.

Since the introduction of the regime in 2006, this office has inspected the records of 17 different enforcement agencies in relation to stored communications access to ensure compliance with the Act.[3] The Ombudsman is also responsible for the inspection of telecommunications interception records of certain Commonwealth agencies[4] under the Act. The Ombudsman reports to the Commonwealth Attorney-General annually on the Ombudsman's activities.

[1] Explanatory Memorandum, Cybercrime Legislation Amendment Bill 2011 (Cth).
[2] Collectively referred to as 'carriers' in this submission.
[3] The agencies are: Australian Federal Police, Australian Crime Commission, Australian Customs and Border Protection Service, Australian Competition and Consumer Commission (to be inspected during 2011-12), Australian Securities and Investments Commission, the police forces of each State and Northern Territory, Corruption and Crime Commission (WA), Crime and Misconduct Commission (QLD), Office of Police Integrity (VIC), New South Wales Crime Commission, and Police Integrity Commission (NSW).
[4] The Commonwealth agencies are: Australian Federal Police, Australian Crime Commission and Australian Commission for Law Enforcement Integrity.

Amongst other things, the Bill introduces a preservation mechanism under Chapter 3 of the Act with respect to the access to stored communications by enforcement agencies. The Bill provides a legislative basis for arrangements currently in place between enforcement agencies and carriers to preserve stored communications to prevent them from being deleted from the carriers' systems as a matter of routine system administration.

The 'preservation notices' will allow certain agencies to request that carriers preserve stored communications (not only those that are already stored on a carrier's system, but also those that may come into existence in the future) to prevent them from being deleted. A requesting agency can then apply for a warrant under Chapter 3 of the Act to access the stored communications.

3 COMMENTS ON THE PRESERVATION MECHANISM

The submission is informed by the Ombudsman's understanding of the operation of the Act in relation to both access to stored communications and the interception of telecommunications, gained from numerous inspections of agencies' records.

Whilst acknowledging the purpose and the benefits of the amendments as outlined in the Explanatory Memorandum, we have several concerns with the practical operation of the preservation notices scheme.

3.1 See Appendix A

3.2 Unlimited number of preservation notices

The Bill introduces two types of domestic preservation notices – historic (which covers stored communications held by the carrier on a particular day) and ongoing (which covers stored communications held by the carrier in a particular 30-day period).

There are no limits on the number of domestic preservation notices that may be issued in relation to the same person or telecommunications service. Although an ongoing preservation notice in relation to the same person or service can only be issued one at a time, it does not prevent an agency from issuing another ongoing preservation notice after its expiry or revocation if the conditions for giving these notices have been satisfied (proposed s 107J).

This aspect of the Bill can potentially lead to ongoing preservation of stored communications for a long period of time. This effectively amounts to telecommunications interception, which is regulated by a separate part of the Act (Part 2-5).

This is of some concern because the range of agencies that can obtain a telecommunications interception warrant[5] is much narrower than those that can

[5] These agencies are referred to as *interception agencies* under s 5 of the Act, which currently consists of the Australian Federal Police, the Australian Crime Commission, the Australian Commission for Law Enforcement Integrity and agencies subject to a Ministerial declaration under s 34 of the Act.

obtain a warrant to access stored communications.[6] Further, a telecommunications interception warrant is used to investigate a *serious offence*, which carries a higher penalty[7] than a *serious contravention* (for which a warrant to access stored communications is issued).[8]

The risk is that an agency, which may not otherwise be able to intercept telecommunications either because of its status under the Act or because the offence being investigated is not a *serious offence*, would effectively be allowed to receive communications over a substantial period of time.

The risk is somewhat alleviated by the proposal that only an *interception agency* can issue ongoing preservation notices. However, *enforcement agencies* can still issue historic preservation notices at regular intervals so as to obtain the communications over a continuous period of time.

3.3 Ongoing domestic preservation notices

The proposed ongoing domestic preservation notices require carriers to preserve stored communications for 29 days after the day the carriers receive the notice.

In our view, an ongoing domestic preservation notice enables agencies to obtain communications passing over a carrier's system for a period in the future (once a 'stored communications access warrant' has been issued under Chapter 3 of the Act). Similar to our concerns in relation to the potential unlimited 'renewal' of preservation notices (see paragraph 3.2), this practice also effectively amounts to telecommunications interception, which is regulated under Part 2-5 of the Act.

Again, this is compounded by the fact that the Bill does not appear to cap the number of times an agency may issue an ongoing preservation notice in relation to the same person once the initial 29-day period has passed. Thus, the period of preservation and access to the product can last for an indeterminate period, as long as a warrant to access the stored communications is obtained before the end of each 29-day period.

As a side, we note that the Convention, which the Bill seeks to implement, does not specifically refer to an ongoing preservation notice of this nature.

3.4 Effective and purposeful oversight

Under the Bill, agencies that have issued preservation notices are required to keep certain records for inspection by the Commonwealth Ombudsman. The records are any preservation notices, revocations and evidentiary certificates issued by the agency (proposed s 150A). The Bill requires that the Ombudsman inspect an agency's records in order to ascertain whether the agency has kept these records.

This new aspect of the Ombudsman's oversight role has been drafted in line with the existing s 152 – which requires the Ombudsman to inspect an agency's records in

[6] These agencies are referred to as *enforcement agencies* under s 5 of the Act, which includes all current *interception agencies* as well as any agency whose function involves administering a law imposing a pecuniary penalty or the protection of public revenue.
[7] Defined under s 5D, a *serious offence* carries a penalty of, for example, a period of at least seven years imprisonment.
[8] Defined under s 5E, a *serious contravention* carries a penalty of, for example, a period of at least three years imprisonment.

order to ascertain compliance with s 150 (whether the agency has kept records of destruction) and s 151 (whether the agency has kept records in relation to the issue of warrants).

If a literal view of the legislation is taken, the Ombudsman would only be required to determine if the agency has kept the records required under ss 150, 151 (and also s 150A under the Bill) rather than the veracity of these records. However, under s 153(3) of the Act, the Ombudsman is empowered to report on agency compliance with a provision of the Act other than ss 150 and 151 (and also s 150A under the Bill).

To enable more effective and purposeful oversight, we have taken a broader view of our role based on the documents available under ss 150 and 151. Our audit criteria also involve checking that:

- warrants are compliant with the Act
- any warrant conditions imposed by issuing officers are adhered to
- lawfully accessed information was only communicated to authorised officers
- warrants are validly executed, and
- the use of stored communications product is in accordance with the Act.

In our view, to remove any doubt, the Act could provide for a broader scope of the Ombudsman's oversight function – to ascertain agency compliance with Chapter 3 of the Act.[9] We have raised this with the Attorney-General's Department in relation to the current legislation, and the same comments would apply to this Bill.

If the Bill is passed in its current form, we would take a similar approach to the inspection of preservation notices. That is, we will not only look for the existence of records relating to preservation, but also assess if agencies have complied with Part 3-1A.

3.4.1 Foreign preservation notices

As the definition of a *preservation notice* includes a foreign preservation notice, the Ombudsman would also be required to ascertain compliance by the Australian Federal Police (AFP) with regards to foreign preservation notices.

Similarly, we would not simply be looking to see whether or not the AFP had kept each foreign preservation notice, revocation or evidentiary certificates. We would also examine the records against ss 107N to 107S of the Bill to determine if the issuance and revocation of foreign preservation notices comply with the Act.

In order to do this, we may require access to certain records such as the written request from a foreign country to the AFP under s 107P(2). Although the Ombudsman may seek access if he determines that the information is relevant to an

[9] Similarly, under the provisions of the Act in relation to telecommunications interception (Part 2-5), the Ombudsman's role is also restricted to ascertaining compliance with ss 79, 80 and 81 – all in relation to record keeping. We have also broadened this view based on s 85 of the Act, which allows the Ombudsman to report on any other contraventions of the Act to the Attorney-General.

inspection,[10] we would prefer a clear mandate to access the documents under the Act. A corresponding obligation should also be placed on the AFP to keep the records.

3.5 When a warrant is not issued following preservation

Under the Bill, a preservation notice ceases to be in force on several grounds, one of which is the issuance of a warrant that authorises access to the preserved product. However, if no warrant was sought, the maximum period a carrier can hold the product under a preservation notice is 90 days.

The Bill is silent on how carriers are to handle the product when the 90-day period expires or when the preservation notice has been revoked by the agency that originally made the request. The lack of obligation on the carrier to destroy the product in such circumstances raises potential security risks.

This is particularly important given the obligation imposed by s 150 of the Act on enforcement agencies to destroy information or records obtained by accessing a stored communication when the information or records are no longer required. If the obligation is imposed on enforcement agencies, then arguably the same obligation should apply to carriers who, if not for the preservation notice, routinely destroy the product.

Further, the security and privacy risk may be compounded by the fact that carriers may make copies of the preserved product. The definition of 'preserve' under the Bill is not only maintaining the integrity of the original communication but also a *copy* of the communication. This means that carriers will be able to make an unlimited number of copies of the original communication, and thus increasing the risk of possible misuse of the product.

However, we recognise that an obligation on carriers to destroy preserved stored communications may be difficult to enforce and audit. Perhaps one solution would be to ask carriers to certify (to the relevant enforcement agency) that any product or copies not 'claimed' under a warrant have been destroyed. This certification should immediately occur after the carrier receives the written notice of revocation under the proposed s 107L(3), or at the end of the 90-day period if the notice has not been revoked.

The Commonwealth Ombudsman should also be responsible for inspecting whether this certification has been kept by enforcement agencies and that it was made in a timely manner.

3.6 Lack of visibility of carriers' actions

Under s 313(3) of the *Telecommunications Act 1997* (Cth), carriers are required to give officers of the Commonwealth and of the States and Territories such help as is reasonably necessary for the enforcement of the criminal law. In this regard, carriers play a vital role in enabling enforcement agencies to obtain stored communications under a warrant. Once a warrant is provided by the agency to a carrier, the carrier is then responsible for accessing stored communications and providing the product to the agency. Likewise, under the proposed amendments, carriers would undertake an important function in assisting agencies to comply with their legislative obligations –

[10] See s 154 of the Act and the *Ombudsman Act 1976* (Cth).

for example, acting in accordance with the preservation notice and not preserving product that is not covered by the notice.

As already noted, where agencies are subject to strict obligations under the Act regarding each step in the process of covertly obtaining stored communications (that is, seeking a warrant, notifying relevant parties of its issue, receiving stored communications from carriers and subsequent use of that information), carriers are not subject to a similar level of scrutiny. There appears to be a *gap in accountability* when carriers' actions are perhaps equally important to those of agencies in giving effect to a stored communications warrant under the Act or preservation notices under the Bill.

The lack of visibility of carriers' actions has affected our recent inspections of enforcement agencies' stored communications records. As carriers are responsible for physically accessing stored communications under a warrant, at times, we were not able to ascertain if stored communications were lawfully accessed when information regarding access is held by carriers.

The Ombudsman's role is to inspect an enforcement agency's records to ensure compliance with the Act. This role does not extend to inspecting the records of carriers. Although the Ombudsman can rely on his coercive powers under s 9 of the *Ombudsman Act 1976* (Cth) to require a carrier to provide its records, these powers would be relied on only to assist the Ombudsman in his inspections of the enforcement agencies. In our view, there needs to be a clear legislative mechanism to hold carriers accountable for their actions in enabling the execution of stored communications warrants.