Submission of the

New South Wales Council for Civil Liberties

to the

Commonwealth Attorney-General's Department

on

Australia's proposed accession to the

Council of Europe Convention on Cybercrime

Authors: Alana Maurushat[*]
Renée J Watt

[*] Lecturer, Faculty of Law, University of New South Wales; Academic Co-Director of the Cyberspace Law and Policy Centre, Faculty of Law, University of New South Wales, PhD candidate (in the area of botnets and cyber-crime), Faculty of Law, University of New South Wales.

1 Summary of recommendations.

In relation to Australia's proposed accession to the *Council of Europe Convention on Cybercrime* ('**Convention**'), the New South Wales Council for Civil Liberties ('**CCL**') makes the following recommendations:

(a) the Convention has the potential both to aid law enforcement in combating cyber-crime, and also to significantly undermine civil liberties. If, *and only if*, the Australian Government is able to implement the following safeguards, then, *and only then*, should it accede to the Convention;

(b) mutual assistance must be conditional on:

  (i) dual criminality;

  (ii) a 'mutual assistance warrant' system; and

  (iii) Australia's ability to refuse to cooperate where:

    (A) torture or the death penalty may flow form the assistance;

    (B) there is a danger the information may be disclosed to another state or a non-governmental authority; and

    (C) there is a danger the requesting party may use the information to investigate or prosecute offences that are not among the Convention's substantive offences;

(c) mutual assistance for copyright infringement should only be available for investigations of mass infringement for commercial financial gain;

(d) extradition should be conditional on:

  (i) extradition treaties; and

  (ii) Australia's ability to refuse to cooperate where the extradited person may be subject to torture or the death penalty;

(e) the Convention should not be used in furtherance of existing powers to extradite for copyright offences;

(f) introduction of the 'misuse of a device' offence should:

  (i) be narrowly drafted so as only to catch dangerous behaviour;

  (ii) specifically include botnets as a 'device'; and

  (iii) exempt security researchers;

(g) introduction of any other substantive offences should:

  (i) be narrowly drafted so as only to catch dangerous behaviour; and

  (ii) exempt security researchers;

(h) data interference should not be an offence unless it causes serious harm, and serious harm should include aggregate harm;

(i) the 24/7 network contact should:

  (i) play a purely facilitative role;

  (ii) be the only point of contact for overseas law enforcement agencies seeking to investigate cyber-crime occurring partially within Australia;

(j) data retention and destruction policies should accompany provisions requiring data preservation;

(k) seizure of computers and computer systems should be of limited duration;

(l) trans-border remote searching under a court-issued warrant should be considered;

(m) ISPs should be obliged to notify subscribers that ISPs may share subscribers' personal information with foreign law enforcement;

(n) law enforcement agencies should be obliged to provide statistics on surveillance undertaken or information shared pursuant to the Convention; and

(o) except in cases of mass infringement for commercial financial gain, any extension of domestic investigative powers should be expressly unavailable for the investigation of copyright-related offences.

2 The Convention can help combat cyber-crime, but it can also undermine civil liberties.

2.1 The principle effect of the Convention for Australia will be the sharing of personal information with foreign law enforcement.

At essence, the Convention requires signatories to do three things:

(a) to enact certain substantive offences;

(b) to implement certain procedures for the investigation of cyber-crime; and

(c) to co-operate with other signatories in cyber-crime investigations and prosecutions.

Under the substantive offences, only one change will be required at domestic law: 'misuse of a device' will need to be an offence (see 3.3, below); the other substantive offences are largely already caught at domestic law (but see 4.1, below). The procedural requirements do not mandate any technological capabilities or legal powers that Australian law enforcement does not already enjoy. The principle change therefore is that Australian law enforcement will be sharing the fruits of its investigations with foreign law enforcement.

2.2 The Convention is a potentially powerful tool for investigators and prosecutors.

Cyber-crime is extremely difficult to police. This principally because:

(a) obfuscation renders trace-back almost impossible (see 5.1, below); and

(b) cyber-crime tends to be multi-jurisdictional.

By facilitating international cooperation, the Convention addresses one of the two main obstacles in cyber-crime investigations.

2.3 The Convention also has potential to powerfully undermine civil liberties.

The key effect of the Convention for Australians will be the sharing of personal information with foreign law enforcement. This prompts grave concerns.

Chief among these concerns is that some signatories employ torture and the death penalty. Extradition or mutual assistance that results in a person being subject to torture or the death penalty is under no circumstances acceptable.

A second significant worry is that covert surveillance of a suspect already comes at the cost of privacy; sharing that information with overseas law enforcement significantly increases the breach of privacy this represents, especially where a regime has comparatively lax standards of privacy or is prone to abuse personal information.

2.4 Australia should accede to the Convention *only if* it is able to enact adequate safeguards to civil liberties.

Because of the Convention's potential to significantly undermine basic rights (privacy, freedom from torture, right to life, and others explored below in Part 3), the Australian Government should only accede to the Convention if it is able to adequately protect against these possible abuses. Specific measures Australia must adopt if it is to accede to the Convention are considered at Part 3, below.

3 The CCL recommends that Australia accede to the Convention if, *and only if*, it implements the following safeguards to civil liberties.

3.1 Mutual assistance must be conditional.

The Convention provides for mutual assistance between signatories that are investigating cyber-crime. Australia should *not* provide assistance to foreign law enforcement *unless* the following conditions are met.

(a) The Convention specifically allows for signatories to make dual criminality a precondition for mutual assistance. This is plainly imperative.

Except where preservation orders are concerned (see 1.10 (a), below), the Convention specifically allows for signatories to make mutual assistance conditional on the existence of dual criminality. Australia should without question adopt dual criminality as a precondition for mutual assistance under the Convention.

(b) Mutual assistance should be subject to a court-issued 'mutual assistance warrant'.

The Convention expressly preserves any domestic civil liberties safeguards in relation to mutual assistance. This means foreign law enforcement will only be able to access Australian information pursuant to the Australian warrant system. However, where *foreign* law enforcement wishes to access information from Australian authorities, a separate warrant should be required.

A 'mutual assistance warrant' will enable an independent Australian body (the courts) to examine requests for assistance on a case-by-case basis. So as not to place political decisions into the hands of the judiciary, the legislature should list the circumstances to which the court may have regard when deciding whether to issue a 'mutual assistance warrant'. These should include:

(i) whether the applicant has a history of misuse of personal information, such that it seems possible that information collected under the warrant may be:

(A) used to prosecute the suspect for an offence unrelated to the substantive offences the Convention proscribes;

(B) disclosed either to a third country, regardless of whether that country is a signatory to the Convention, or to a non-governmental authority; or

(C) used for any purpose not specified in the application for the warrant;

(ii) whether the applicant employs torture or the death penalty; and

(iii) whether the applicant otherwise has a history of human rights abuses (which concept may require further elucidation).

A 'mutual assistance warrant' should only be required in order for overseas law enforcement to *access* information. In the interests of the timely preservation of volatile evidence, a 'mutual assistance warrant' should not be needed for preservation orders (discussed below at 4.2).

(c) Mutual assistance should only be available where foreign law enforcement undertakes not to use the information in prosecutions that may result in torture or the death penalty.

Australia should not provide assistance to foreign law enforcement where the suspect may consequently be subject to torture or the death penalty. Where a signatory employs torture or the death penalty for certain offences, Australia should only provide assistance on the undertaking that any information it provides will not be used in a prosecution from which torture or the death penalty may flow. Where under a particular regime torture appears to occur haphazardly, or where Australia does not trust a regime to respect its undertaking, Australia should reserve the right to refuse all assistance.

Picking and choosing with which signatories Australia will cooperate may appear to defeat the Convention's purpose of facilitating international cooperation in policing cyber-crime. But the Convention cannot come at the cost of basic rights and freedoms. If acceding to the Convention means that Australians will be subject to torture and the death penalty then Australia must not accede. If however it is possible to carve out exceptions to the Convention, so that Australia is able to participate more effectively in combating cyber-crime *without sacrificing basic rights*, then this is the preferred path.

(d) Mutual assistance must not be available unless the requesting state undertakes not to disclose the information to other states or any non-governmental authority.

The Convention allows signatories to make mutual assistance conditional on confidentiality and 'limited use'. Many countries are party to information-sharing agreements and networks, whose scope lies well beyond anything the Convention anticipates. Australia should only provide mutual assistance if the state to whom the information is to be provided undertakes not to disclose the information to:

(i) any other state; or

(ii) any non-governmental authority, except a court of the requesting state.

Where Australia does not trust a regime to respect its undertaking, Australia should reserve the right to refuse all assistance.

(e) Mutual assistance should only be provided where the requesting party undertakes to use the information for the sole purpose of investigating and prosecuting cyber-crime.

The Convention only requires signatories to participate in mutual assistance for the purpose of policing cyber-crime. To avoid the abuse of personal information in the hands of foreign states, Australia should only provide mutual assistance where the requesting state undertakes to use the information it receives for the sole purpose of investigating and prosecuting the Convention's substantive offences. The information should not be used for the investigation or prosecution of other offences, including computer-related offences that do not fall within the purview of the Convention's substantive offences.

(f) Mutual assistance for copyright infringement should only be available for investigations of mass infringement for commercial financial gain.

The international sharing of personal information comes at a very high price for privacy. The Australian Government should only wear such a cost in respect of the most extreme offences. Copyright infringement only meets this threshold in cases of mass infringement for commercial financial gain. In such circumstances, mutual assistance should be available, but in no other case does copyright infringement justify mutual assistance.

Article 25(4) stipulates that signatories cannot exclude mutual assistance simply because they consider an offence to be merely 'fiscal'. If this means Australia cannot limit mutual assistance regarding copyright infringement to cases of mass infringement by for commercial financial gain, *Australia should not accede to the Convention*.

3.2 Extradition should be conditional on extradition treaties and should not lead to torture or the death penalty.

(a) Extradition must be conditional on extradition treaties.

The Convention stipulates that where signatories have signed extradition treaties, they must include the Convention's substantive offences as extraditable offences. Where parties do not have an extradition treaty, the Convention may form the basis of the power to extradite. This is not acceptable. Australia must not extradite any person absent an extradition treaty between itself and the state requesting the extradition.

(b) Extradition not available for copyright infringement.

The Convention stipulates that all its substantive offences are extraditable. These include copyright offences. Although Australia already has extradition arrangements in relation to copyright infringement, the Convention should not be used to inflate those powers. Where foreign law enforcement suspects copyright violation in Australia, it should refer its intelligence to Australian law enforcement, who can investigate the matter locally.

(c) Australia must not extradite anyone who will as a result be subject to torture or the death penalty.

As with mutual assistance, Australia should not extradite anyone who may consequently be subject to torture or the death penalty. Where a signatory employs torture or the death penalty for certain offences, Australia should only extradite a person on the undertaking that the person will not be subject to those punishments. Where torture appears to occur haphazardly, or where Australia does not trust a regime to respect its undertaking, Australia should reserve the right to refuse to extradite anyone.

3.3 Introduction of the 'misuse of a device' offence should be narrowly construed, specifically include botnets as a 'device' and exempt security researchers.

There is significant overlap between the substantive offences the Convention requires signatories to enact and offences already extant under Australian law. An exception is Article 6 of the Convention, which requires signatories to make 'misuse of a device' an offence.

(a) The offence must not criminalise behaviour that is not dangerous.

On its face, an offence relating to 'misuse of a device' leaves ample scope for over-criminalisation. Take for example Australia's recent spate of identity theft offences.

These criminalise the use of publicly available personal information coupled with a criminal intent, such that possession of a street directory and a vague notion that robbing a bank might be fun is actually a crime:[1] over-broad criminalisation is a live concern.

The offence that Article 6 captures is appropriately narrow. Production or distribution of a device is only an offence where the device is designed or adapted for the purposes of committing any of the other substantive offences in the Convention (all of which are arguably already offences under domestic law) *and* where the producer or distributor intends that the device be used for the purpose of committing any of those offences. Article 6 also proscribes the production or distribution of data by which a computer system is accessed where the producer or distributor intends that data to be used in committing the Convention's other substantive offences. In these ways, Article 6 draws a strong connection between the offense and actual dangerousness (unlike Australia's identity theft offences). Should Australia accede to the Convention, it must similarly limit any offence relating to the 'misuse of a device'.

(b) The offence must capture botnets.

Botnets, explored below at 5.1, are the principle technology to enable cyber-crime. There is no specific mention of botnets either in the Convention or at domestic law, and they are covered only obliquely by the *Criminal Code Act 1995* (Cth).[2] In order for this new provision to be of any use, it must be absolutely clear that botnets (a collection of compromised computers) constitute a 'device'.

(c) Security researchers must be exempt from criminality.

Article 6(2) allows for an exemption to criminality where the 'misuse' pertains to security research. It cannot be stressed enough how important this exception is. Currently, security researchers in Australia are not exempt from the computer provisions of the *Criminal Code Act 1995* (Cth). Nonetheless, it is security researchers (university computer science departments, technology companies) that are the primary forces behind tackling botnets and other forms of obfuscation crime tools. There has yet to be a single takedown of a botnet or prosecution of a botnet master that did not involve security researchers.[3] Cyber-crime prosecution cannot occur without their help and they must be free from legal sanction, rather than discouraged from participation.

3.4 The 24/7 network contact should be very tightly controlled.

(a) The 24/7 network contact should play a purely facilitative role.

The Convention mandates that signatories designate a point of contact that is available 24/7 *either* in order to facilitate immediate assistance to other signatories in respect of cyber-crime investigations, *or* to carry out such assistance directly. It is imperative that Australia's 24/7 network contact plays a purely facilitative role and does *not* carry out the investigative assistance directly.

---

[1] Alex Steel, 'The True Identify of Australian Identify Theft Offences: A Measured Response or an Unjustified Status Offence?' (2010) 16(1) *University of New South Wales Law Journal Forum: Cyberlaw* 48.
[2] Alana Maurushat, 'Australia's Accession to the *Cybercrime Convention*: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?' (2010) 16(1) *University of New South Wales Law Journal Forum: Cyberlaw*, 5, 13.
[3] Ibid.

The creation of a new body with actual investigative powers is either pointless or dangerous. Either that body will be subject to all of the safeguards that exist to protect suspects in covert operations (for example, court-issued warrants), in which case why establish the new body if it has no new powers; or that body will *not* be subject to such restrictions, which would be a savage departure from the systems that have been implemented in order to protect civil rights.

The departure from these protections for the purpose of passing information into foreign hands is particularly vicious, as the suspect is then potentially subject to foreign prosecution, which may or may not offer the kinds of protections Australia deems necessary.

(b) The 24/7 network contact should be the only point of contact for overseas law enforcement seeking to investigate cyber-crime in Australia.

Digital evidence is inherently volatile and so time is of the essence when investigating cyber-crime. A single point of contact for international cooperation may therefore be highly useful. On the other hand, the creation of a new point of contact duplicates previous Interpol and Group of Eight initiatives. Multiple points of contact may be confusing, ineffective and time-wasting. The mandate of any new point of contact should be carefully prescribed, with particular attention on its interaction with similar international bodies. In particular, to avoid duplication, the 24/7 network contact should be the only point of contact for foreign law enforcement bodies looking to investigate cyber-crime occurring partially in Australia.

3.5 If other substantive offences are enacted, they should be similarly narrow and should exempt security researchers.

Apart from 'misuse of a device', the offences the Convention mandates signatories enact are arguably already offences under Australian law. If however the Australian Parliament seeks to update these offences in light of the Convention, it should be wary that any new offences do not over-criminalise.

As above in 3.3(c), security researchers should, where appropriate, be exempted from criminal sanction, as their participation is crucial in cyber-crime investigations.

3.6 Data retention and destruction policies should accompany provisions requiring data preservation.

Although the Convention compels ISPs to preserve a potentially large amount of data, it does not address the security that ought attach to this data. A vast data repository makes fertile ground for data theft. Australian legislators should specify security standards attaching to preservation orders. Data retention and destruction policies are essential.

3.7 Data interference should not be an offence unless it causes serious harm; serious harm should include aggregate harm.

The Convention allows signatories to reserve the right to require that the prescribed data interference offences contain a 'serious harm' element. Australia has indicated that it will not pursue this reservation.

Any criminal offence should begin with a concept of harm. Harm in cyber-crime can often be difficult to quantify. For example, while the aggregate harm is often enormous, each zombie in a botnet suffers minimal individual harm (see Part 5 below for an explanation of botnets). But difficulties in quantifying harm does not render it permissible to criminalise non-harmful

conduct. Serious harm must be retained as an element of the data interference provisions, and should be drafted so as to capture aggregate harm.[4]

3.8 Seizure of computers and computer systems should be of limited duration.

Both the Convention and Australian law permit seizure of computers or computer systems, and both are silent on the duration for which law enforcement may seize these without laying charges. This is plainly inadequate: seizure of personal property must be subject to safeguards.

3.9 Trans-border remote searching under a court-issued warrant should be considered.

Both the Convention and domestic law are silent on the use of trans-border remote searches. Trans-border remote searches occur when law enforcement agencies covertly install key-logging or other 'spying' software onto the computer of a suspect in another jurisdiction. This is a useful tool for combatants of cyber-crime, but, due to its highly invasive nature, one that must be carefully circumscribed.

The Australian legislature should consider if and under what conditions it will allow trans-border remote searching. Trans-border remote searching should only be allowed subject to strict legislative restrictions, and should not be allowed without a court-ordered warrant.

3.10 ISPs should be obliged to notify subscribers that ISPs may share subscribers' personal information with foreign law enforcement.

Technologies of detection and monitoring must respect privacy. Under the Convention, foreign law enforcement, albeit subject to domestic law, could enjoy access to the personal details of any Australian with an internet connection. Because of the implications of this for privacy, it should be mandatory that ISPs notify subscribers of this possibility, by including a warning and explanation in both their terms of service and their privacy policies. ISPs should be required to notify subscribers of what information the ISPs will gather and share, how they will gather it, and the purpose of this collection.

3.11 Law enforcement agencies should be obliged to provide statistics on the surveillance undertaken or information shared pursuant to the Convention.

Australian cyber-crime statistics are patchy at best. This marks an impediment both to law enforcement and civil liberties protections, as it hampers the research of both. When acceding to the Convention, Australia should stipulate that law enforcement agencies release statistics on the number of preservation orders, production orders, requests of real-time traffic data collection, interception of content data requests, and any other similar requests they receive. Like other surveillance statistics, these should be tabled in Parliament.

3.12 Surveillance statistics should be publicly available regardless of accession to the Convention.

Regardless of whether Australia accedes to the Convention it should be mandatory for:

(a) ISPs to disclose to subscribers, in their terms of service and privacy policies, that local law enforcement can, subject to the Australian warrant system, engage in covert investigation of user's browsing habits; and

[4] For a discussion of serious harm in the context of cyber-crime, see Keiran Hardy, 'Operation Titstorm: Hacktivism or Cyber-Terrorism?' (2010) 16(1) *University of New South Wales Law Journal Forum: Cyberlaw*, 31.

(b) local law enforcement to reveal how many and what type of warrants for which they apply.

3.13 Except in cases of mass infringement for commercial financial gain, any extension of domestic investigative powers should be expressly unavailable for the investigation of copyright infringement.

The Convention contemplates highly invasive investigate tools, such as real-time evidence collection and interception of communications. Australian law enforcement largely enjoys these powers already, and so there is little need to expand their scope in furtherance of the Convention. Nonetheless, if Australia decides to widen its investigate powers in this area, these powers should not be available in investigations of copyright infringement, except in cases of mass infringement for commercial financial gain.

Naturally, any extension of domestic law enforcement's investigative tools should remain subject to current safeguards, such as the warrant system.

4 Where the Convention touches old bones of contention regarding domestic law, the CCL has no *new* civil liberties concerns.[5]

Many of the Convention's most contentious provisions expressly preserve domestic law as a bulwark against invasions of civil liberties. Naturally, the CCL entertains concerns over broadly-worded hacking and fraud[6] offences, which already exist at domestic law but which the Convention stipulates must be enacted as local offences. Similarly, the CCL is uncomfortable with the privacy, surveillance and freedom of expression implications of, for example, intercepting communications or collecting data in real time, which the Convention mandates but which can only occur in accordance with domestic law, such as the warrant system. As technology advances and deep packet inspection and other invasive capabilities become more readily available these concerns will only deepen.

However, these are problems with Australia's existing domestic civil liberties protections and do not arise by virtue of the proposed accession to the Convention. This submission describes the CCL's response to the Convention, not to Australian civil liberties protections generally.

4.1 Apart from 'misuse of a device', the CCL has no new concerns over the Convention's substantive offences.

Apart from Article 6 ('misuse of a device'), discussed above at 3.3, the substantive offences the Convention requires signatories to enact do not differ from offences already extant under Australian law. Thus, apart from a reticence regarding the possible broadness of a 'misuse of a device' offence (see 3.2 above), the CCL entertains no new concerns over the Convention's substantive offences. Were Australia, in pursuit of compliance with the Convention, to broaden its illegal access, illegal interception, data interference or system interference provisions, the CCL would entertain the same concerns regarding over-criminalisation as exist in relation to the 'misuse of a device' provisions.

4.2 No new concerns over preservation orders.

Where one signatory to the Convention is undertaking an active criminal investigation, that signatory may compel the ISPs of other signatories to preserve computer and traffic data that the ISPs have already stored but that they would otherwise delete. As this only compels preservation - not collection, not production to overseas bodies - the CCL entertains no particular concerns with this provision. Collection and production remain subject to the Australian warrant system.

4.3 No *new* concerns over search and seizure powers, but opportunity exists for Parliament to address pre-existing concerns over duration for which law enforcement may seize a computer.

The Convention's search and seizure provisions do not differ from those already operative at domestic law, and so no new concerns here arise. However, as at 3.6 above, the CCL recommends that Australia specify the duration that its law enforcement agencies may retain computers and computer systems without laying charges.

4.4 No new concerns over interception and real-time evidence collection.

The Convention's provisions relating to the interception of data and the collection of real-time evidence are subject to existing domestic law. In the Australian context, this means law

[5] By 'new' concerns we mean concerns that arise purely by virtue of changes to Australian law as a result of its accession to the Convention.
[6] See, eg, Steel, above n 1.

enforcement agencies can only exercise these powers pursuant to the warrant system already in place. Except where sharing this information with foreign law enforcement is concerned, no *new* concerns arise regarding these potentially invasive powers. When sharing data with overseas entities, the CCL's recommendations in Part 3 above apply.

4.5 ISPs are unlikely to be required to commit additional resources to accommodate interception and real-time evidence collection requirements.

The Convention requires ISPs to have interception and real-time evidence collection capabilities. Australian law already requires ISPs to have interception capabilities. Interception employs similar technology to real-time evidence collection capabilities and so it is likely ISPs already enjoy both capabilities (although there is not much publicly available information in this regard). It is therefore unlikely that ISPs will have to commit significant (if any) additional resources to updating their systems should Australia accede to the Convention.

5 The Convention will have limited effect on the prosecution of sophisticated cyber-criminals.

5.1 Obfuscation renders trace-back almost impossible; the Convention does not alter this.

Since the Convention was drafted in the late 90s, the most significant technological advance for cyber-criminals has been the development of obfuscation tools. As the name suggests, obfuscation renders trace-back to the perpetrator almost impossible.

Botnets are an example of a criminally-deployed technology that makes use of obfuscation. Put simply, a botnet is a network of compromised computers, usually controlled by a chain of decentralised 'command and control' ('C&C') domain name pages. The compromised computers ('bots', or 'zombies') are infected with malicious software ('malware') usually without a user's knowledge. As one commentator has remarked: "Almost every major crime problem on the Net can be traced to them".[7] Botnets are involved in all four categories of substantive offences the Convention proscribes.

Before an overseas body can access information on a botnet's Australian operations pursuant to the Convention, it will first need to navigate the domestic warrant system. Unsurprisingly, this requires investigators to have at least some knowledge concerning the suspect.[8] For example, an applicant for one type of warrant will need information on the botnet's C&C; an applicant for a different type of warrant must first have information regarding which computers are infected. Where a botnet's C&C employs fast-flux to rotate domain names every 20 minutes,[9] or where a botnet comprises hundred of thousands if not millions of bots,[10] law enforcement will struggle to even obtain a warrant. While helpful in that it facilitates international access to the warrant system, the Convention does not render that system any less cumbersome in cyber-crime investigations.[11]

The CCL is *not* advocating the abolition of warrants, which are imperative for the protection of civil liberties. The CCL simply observes that investigation of cyber-crime is inherently difficult and that the Convention does not alter this.

5.2 Production orders only provide information that is already available and not always accurate.

Production orders, which compel ISPs to reveal subscriber information to law enforcement agencies, are of little use where users do not subscribe under their real names. Most cyber-criminals use stolen credit cards to purchase internet services under false credentials. Subscriber information in such cases is not helpful. Further, subscriber information (equally false) is available on the WHOIS database, which is no doubt more easy to navigate than domestic legal procedures. This is not to say that law enforcement should be able to side-step legal procedures; the implication is rather that production orders are fairly pointless.

[7] Scott Berinato, 'Attack of the Bots' (November 2006) *Wired*.
[8] For an examination of which warrants apply in which circumstances, see Maurushat, above n 2, 21 - 24.
[9] See eg the Torpig botnet, described in Maurushat, above n 2, 24.
[10] The Mariposa botnet is said to have had 13 million zombies. See Jim Finkle, 'Spain Bust Hackers for Infection 13 Million PCs' *Wired Threat Level* (2 March 2010).

6 The Convention is a step toward successful cyber-crime investigations.

The chain of events collectively comprising an act of cyber-crime will frequently occur across multiple jurisdictions. This is one of cyber-crime's challenges for law enforcement. Whereas the Convention does not render investigations any more technologically easy (which is the principal challenge for law enforcement), it does, as one would expect of an international treaty, facilitate international cooperation. This is certainly a step toward successful investigations and prosecutions of cyber-criminals.

Because the Convention has the potential to be helpful in an area so difficult to police, it is important for Australia to attempt to accede. But accession must only occur if adequate civil liberties safeguards, such as those outlined in this submission, are implemented. The possibility of catching a cyber-crook must not outweigh the basic rights of every person in Australia with an internet connection.

6.1 International parity is prima facie beneficial.

The Convention dictates elements of substantive and procedural law as it relates to cyber-crime. Of itself, this is beneficial because the greater harmony that exists between Australian provisions and those of other jurisdictions, the easier joint investigations and prosecutions become. Ultimately, the more signatories to the Convention, the fewer legal safe havens will be available to cyber-criminals. However, harmonisation must not come at the price of civil liberties.

6.2 The Convention enhances the collection of real-time evidence, which is essential for botnet-related prosecutions.

Botnet-related crimes leave little evidence after the event. The interception and collection of real-time evidence is of utmost importance for the prosecution of botnet masters. Further, real-time evidence collection allows law enforcement access to encrypted data. This is because real-time evidence collection allows the investigator to examine the communication while the end-user is also examining the data - that is, while the data is unencrypted. This circumvents the need for almost impossible decryption. The ability of law enforcement to collect real-time evidence across jurisdictions is a significant step toward successful botnet-related prosecutions, but again cannot come at the price of civil liberties.

6.3 The Convention will have limited impact on purely local prosecutions.

The Convention stipulates few changes to domestic law. Where a cyber-crime operation occurs purely within Australia, the Convention will have little impact on its investigation.

Nonetheless, if the introduction of the 'misuse of a device' provision catches botnets, which are otherwise only ambiguously caught under Australian offences, there is the possibility for prosecution of a purely local botnet. A purely local botnet however will be rare.

6.4 The less sophisticated the operation, the more useful the Convention.

The less sophisticated a cyber-crime operation, the easier its investigation and prosecution. Where cyber-criminals are unsophisticated, or where they are sophisticated but, being human, make mistakes, and where that operation is trans-national, the Convention may lead to prosecution. It is of course possible that there are as many sloppy cyber-criminals as there are sophisticated ones, in which case the Convention will be very helpful indeed.