Australia’s proposed accession to the Council of Europe Convention on Cybercrime

Comment on public consultation by:

Dr Gregor Urbas
ANU College of Law
The Australian National University
Canberra, Australia
Ph. (02) 6125 4262
Gregor.Urbas@anu.edu.au

Dr Yao-chung Chang
Regulatory Institutions Network
The Australian National University
Canberra, Australia
Ph. (02) 6125 2637
Lennon.Chang@anu.edu.au

14 March 2011
We thank the Attorney-General’s Department for the opportunity to comment on the public consultation on Australia’s proposed accession to the Council of Europe (COE) Convention on Cybercrime. As cybercrime researchers based at the Australian National University (ANU), we are pleased to offer the following observations.

Australia’s Relationship with the Council of Europe Convention on Cybercrime

1. Although Australia is not currently a signatory to the COE Convention on Cybercrime, Australian cybercrime law – particularly at the federal level – has already been significantly influenced by this international agreement. For example, the Cybercrime Act 2001 (Cth), which updated the Commonwealth’s computer offences and enacted them within the Criminal Code Act 1995 (Cth), was shaped by reference to earlier drafts of the COE Convention, which was finalised and opened for signature in November 2001 in Budapest. 1 Although Australia was not directly involved in the COE process, it did co-operate with an Expert Group on Computer and Computer Related Crime convened by the Commonwealth countries which developed a draft model law in November 2001, similarly heavily influenced by the COE Convention. 2 Thus, Australian co-operation with international partners in the development of legal responses to the threat of cybercrime is not a new phenomenon. 3

2. Given that the Cybercrime Act 2001 (Cth) added a comprehensive set of unauthorised access, modification and impairment offences to Part 10.7 of the Criminal Code Act 1995 (Cth), it is not surprising that – as noted in the public consultation document ‘Outline of the articles of the Council of Europe Convention on Cybercrime and Australia’s compliance’) – Australian federal offences already substantially comply with Articles 1-5 of the COE Convention. Moreover, with the enactment of a broad suite of further telecommunications offences in Part 10.6 of the Criminal Code Act 1995 (Cth), added by the Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004 (Cth), Australian federal law now includes child abuse and child pornography offences, child grooming and procuring offences, online hoax, threat and menacing offences etc. and with other offences under Commonwealth law relating to misuse of devices, forgery, fraud and copyright infringement etc. there is substantial compliance also with Articles 6-10 of the COE Convention.

1 Council of Europe, Convention on Cybercrime (CETS No. 185): http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG
3. It is noteworthy that, although the Commonwealth’s legislative power is constitutionally mainly limited to crimes involving telecommunications services – relying on ‘postal, telegraphic, telephonic, and other like services’ under section 51(v) of the Constitution – rather than crimes against or involving computers or computer systems generally, with the rapid adoption of the Internet as a global medium for personal and business communications, the expansion of federal jurisdiction in this sphere has been significant. For example, prosecutions relating to offensive or illegal online content or associated misuses of communications are now routinely based on Commonwealth offences rather than, or in addition to, available State and Territory offences. Indeed, the very broad offences found in s474.14 of the Criminal Code Act 1995 (Cth) – covering the use of a telecommunications service to commit a serious Commonwealth, State, Territory or foreign offence – are arguably sufficient to extend the reach of federal criminal law to all forms of online crime, including computer fraud, online vilification and cyber-terrorism.

4. The provisions in the Criminal Code Act 1995 (Cth) relating to extensions of criminal responsibility – such as attempt, aiding and abetting, conspiracy and incitement, as well as corporate criminal responsibility – and the statutory penalties for the various cybercrime offences, substantially comply with Articles 11-13 of the COE Convention. The recent addition of s11.2A dealing with joint commission enhances the ability to prosecute those who commit offences in combination with others – this is important in the context of cybercrime, where geographically dispersed individuals may co-operate online to commit offences such as child exploitation or copyright piracy. As regards penalties, the statutory penalties for cybercrime offences under the Criminal Code Act 1995 (Cth) are generally set at appropriate levels, though we note that this does not always translate into adequate sentences in individual cases, where judges are often dealing with young offenders with no criminal history.

5. Where Australian federal law may require updating in view of the proposed accession to the COE Convention is in the area of procedural powers. While the Cybercrime Act 2001 (Cth) added a range of new provisions relating to search and seizure to the Crimes Act 1914 (Cth) and the Customs Act 1901 (Cth), it is evident that there are some gaps such as those relating to the expedited preservation of data at the request of a foreign law enforcement agency. If appropriate amendments can be made, in conformity with the general principles operating under Australia’s mutual legal assistance and extradition regimes, it is reasonable to expect that Australian federal law will substantially comply with Articles 14-35 of the COE Convention.

---


The International Status of the Council of Europe Convention on Cybercrime

6. Although the COE Convention is widely considered to be the first international convention on cybercrime, and is accepted as such by the United Nations, some countries regard it as a regional rather than international treaty. In fact, there is only one non-European nation, the United States of America, which has ratified the Convention, although Canada, Japan and South Africa are signatories. The Convention therefore cannot yet be described as being a global agreement. In particular, large countries such as China and Russia have not been involved in development of the COE Convention.

7. Russia has indicated a continuing concern with Article 32, which deals with trans-border access to stored computer data with consent or where the data is publicly available.\(^7\) China has not signed the COE Convention not only because of inconsistency between its domestic laws and the requirements of the Convention, but also because the Chinese Government was not invited to contribute to the drafting process. As a senior police officer has said:\(^8\)

> Actually, the Council of Europe has been in contact with China, trying to persuade China to amend its law to fit the requirements of the Convention. However, China did not care much about this issue then. And, anyway, when they were drafting the convention, they did not invite China to join in the drafting. Now they want us to join, we are not interested.

8. Even within Australia’s more immediate region, the degree of participation in the COE Convention is limited. Japan is so far the only Asian signatory, and most countries in the Pacific have yet to develop their cybercrime laws to the requisite standard.\(^9\) Taiwan, which has more than 15 million Internet users and is ranked very high in terms of bot-infected computers (see below) and spam and as an origin for phishing, is unable to sign due to lack of political recognition as a country. More than 50 per cent of the world’s population, or an estimated 40 per cent of Internet users, are thus not under its auspices.

9. However, it must be conceded that – despite these limitations – the COE Convention is still the most comprehensive and internationally recognised agreement on cybercrime. Until a more inclusive international instrument is developed by the United Nations, for example, it is in Australia’s interests to become a signatory to the COE Convention in the first instance and to play a constructive role in its improvement or eventual replacement. By acceding to this Convention, Australia will be in an enhanced position to contribute to the global response to the threat of cybercrime.\(^10\)

---

\(^8\) Y. C. Chang, *Cybercrime Across the Taiwan Strait -- Regulatory Responses and Crime Prevention* (2010), Unpublished PhD thesis, Australian National University, Canberra. (Interviews were conducted in China, Taiwan and Hong Kong by the second-named author as part of his doctoral research).
\(^9\) Legislative reform work is being undertaken by the International Telecommunications Union (ITU), for example at the Cyber Legislation Workshop, Port Vila, Vanuatu, 2-4 March 2011.
Future Developments in Cybercrime Law

10. Some areas that are not explicitly covered by the COE Convention, and which might therefore require attention in future elaboration of the Convention and/or Australian domestic law, include the following:

11. **Botnets:** The use of botnets is arguably the most significant new type of cybercrime to arise since the original signing of the COE Convention. A botnet is a group of networked computers containing secretly installed programs which allow people to control those computers remotely. A computer infected with a malicious program or malware that allows it to be remotely controlled is bot-infected. A home or office computer may be bot-infected and actively used as part of a botnet without the computer owner’s knowledge. Using large numbers of networked infected-computers, botnet operators can launch highly damaging attacks, including such serious crimes as Distributed Denial of Service (DDoS) attacks. Some large botnets with hundreds of thousands of computers have been discovered by investigating authorities, and these have been employed for purposes of cyber-terrorism and cyber-war. Botnets have been deemed by scholars as the new architecture of cyber-organised crime.\(^\text{11}\)

12. **Cloud computing:** This relatively new architecture brings new concerns in relation to cybersecurity. Cloud computing provides computation, software, data access, and storage services whereby users can store their data at remote storage facilities provided by service companies or use software provided by those companies. Users do not need to physically store their data on their own computer or buy software for themselves. Cloud computing potentially makes computing more convenient and cheaper, and it has been argued that cloud computing may be “the ultimate category of globalization” – convenient to users but this may become a barrier to successful crime investigation.\(^\text{12}\)

13. **Anonymity and encryption:** The relative anonymity with which people conduct themselves online can lend itself to illicit activity. The use of freely available tools to mask IP addresses, locations and identities makes the task of law enforcement more difficult, as does the use of encryption to protect data from third party access. While these tools also have legitimate uses, their easy availability to cyber criminals may need to be addressed in some manner in future developments of cybercrime law. Some countries have specific law enforcement powers to compel the release of encryption keys, for example.

14. **Social networking:** A considerable amount of cybercrime – including online harassment, stalking and child grooming – is made easier through the use of social networking sites such as Myspace and Facebook. Of course, these services are of undoubted benefit in facilitating social contact and business relationships, but they also appear to afford insufficient protections to

---


unsophisticated and vulnerable users such as children. Greater attention to the possibilities for law enforcement monitoring of such sites, assisted by the private sector entities involved, may be required in the interests of public safety. In turn, this may necessitate a regulatory response that connects sex offender and other law enforcement databases and information with social networking facilities in a more systematic way. Counter-arguments based on appeals to privacy usually ignore the privacy and safety rights of victims of cybercrime, and should therefore be subjected to a deal of scrutiny.

15. It should be noted, of course, that any signatory country’s laws may exceed the minimum requirements set out in international agreements such as the COE Convention. Therefore, Australia will not be precluded from its own domestic legislative reform in the areas mentioned by its proposed accession – moreover, in consultation with other member States, Australia may be in a position to promote the international development of the legal response to cybercrime more effectively, consistently with regional and global policies.

16. With these observations made, we offer our support for Australia’s proposed accession to the Council of Europe (COE) Convention on Cybercrime.