Pirate Party Australia

Submission to the Joint Standing Committee on Treaties regarding the proposed accession to the Council of Europe Convention on Cybercrime

Rodney Serkowski

March, 2011

Foreword

First and foremost, we thank the Joint Standing Committee on Treaties for the opportunity to present these submissions. Pirate Party Australia is a forming political and activist organisation that focuses on the freedom and access to information, knowledge and culture, advocating the protection of civil liberties, especially the protection of privacy.

We hope that our observations and reflections assist the Government in its consideration of accession to the Council of Europe Cybercrime Convention ('the Convention').

Australia Should Not Accede to the Cybercrime Convention

There is no doubt, that in order to combat some of the issues mentioned within the treaty text, such as fraud, the manufacture and distribution of child sex abuse material and network security offences, there is a requirement for greater cross border law enforcement co-operation.

However there are serious flaws in the Cybercrime Convention that demand that Australia does not accede to the treaty. It is a fundamentally imbalanced treaty that detracts from the good intentions and benefits that the treaty may carry within it.

We agree with the proposition that law enforcement require a coordinating mechanism to enable those agencies to tackle online criminal elements globally, however we should be very mindful that these mechanisms do not throw fundamental freedoms and respect for individual rights and democratic institutions to the wind. We do not accept that combating cybercrime must lead to erosion of fundamental protections of privacy and the protection of personal data.

Criminal misuse of Internet communications infrastructure does require international understandings and solutions that enable a fluidity for law enforcement, however as per United Nations General Assembly Resolution 55/63,[1] these solutions can and should preserve the capacity of government to fight that misuse by respecting privacy and individual freedoms.

---

[1] *Combating the Criminal Misuse of Information Technologies,* GA Res 55/63, 55th sess, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

Privacy

Whilst it confers on law enforcement agencies powers for search and seizure and provisions to enable government surveillance the Convention contains within it very little by way of specific minimum procedural safeguards and limitations to protect privacy and limit government use of such powers, the provisions which do mention 'human rights and liberties' are vague. With no commensurate safeguards within the Convention, the treaty can and will be abused.

The treaty lacks privacy and civil liberties protections - it contains a single platitude to privacy in the preamble, and no where else in the document. So unlike other law enforcement agreements there is little provision or safeguard to protect an individuals privacy to counterbalance any potential government abuse of these powers.

Surveillance and Data Retention

Article 20/21 of the Convention are very dangerous in that these Articles appear to grant law enforcement agencies power for direct access to entire ISP networks. This effectively mandates mass surveillance - eavesdropping, wire-tapping, interception of private email and any other communication.

Indeed, it was discovered that the Attorney General's Department has been for some time investigating the implementation of a mandatory telecommunications data retention regime, with equivalency to the European Data Retention Directive[2] arguably for the purposes of compliance with the Convention, beyond the expected reservation provided in Article 14(3). However due to the opacity[3] of the Attorney General's Department we are not able to comment on this proposal or the government's intention with any certainty.

---

[2] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications networks and amending Directive 2002/58/EC* [2006] OJ L 105/54

[3] The Attorney General's Department is refusing to release documentation as to what it has asked of ISPs in it's enquiries, citing 'unnecessary debate and could potentially prejudice and impede government decision making' — this is entirely unacceptable for a debate on an issue that potentially will unjustifiably and en masse, invade the privacy of the majority of Australians. The debate on data retention should be open, transparent and evidenced based; Ben Grubb, 'No Minister: 90% of web snoop document censored to stop 'premature unnecessary debate' *The Sydney Morning Herald,* 23 July 2010 <http://www.smh.com.au/technology/technology-news/no-minister-90-of-web-snoop-document-censored-to-stop--premature-unnecessary-debate-20100722-10mxo.html>

There are significant concerns regarding the justifications or evidentiary basis for such regimes of data retention, their inevitable expansion, the actions of subsequent governments, concerns regarding human rights and the collection and analysis of even meta data. We have previously raised these significant concerns with the Senate Standing Committee on Environment, Communications and the Arts and direct the Joint Standing Committee on Treaties to that submission.[4]

No Dual Criminality Requirement

Article 25 of the treaty states that all "Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense."

This means Australia will be called upon to aid other countries in enforcing their laws, however what this treaty fails to do is ensure that the offense is criminal in both jurisdictions. The treaty only requires that the action is a criminal offense in the country where the action was committed. So potentially, this may result in Australian law enforcement agencies conducting investigations in our own jurisdiction, for an action that is not unlawful in Australia.

Copyright & Content

It is not surprising that groups like the RIAA have declared strong support for this treaty due to the inclusion of a mandate to criminalise copyright infringement, and subsequently make it an extraditable offence.[5] However copyright is not stable or uniform globally, and unlike Australia many nations do not have criminal sanctions for copyright infringement and there are differing interpretations of fair use or dealing.

There are other, more appropriate mechanisms and forums for the negotiation and discussion of copyright, and the subsequent co-operation of governments in prosecuting infringement. It is not quite clear or apparent as to why the Convention concerns itself with copyright issues in the first place.

---

[4] https://senate.aph.gov.au/submissions/comittees/viewdocument.aspx?id=c7be6192-ae94-49f2-8f1d-0ce10c03828a

[5] http://www.riaa.com/newsitem.php?id=631D2032-D723-367C-79BA-84809B95AEE7

Treaty is the Result of an Undemocratic Process

The manner in which the Cybercrime Convention was drafted was opaque and undemocratic. There were nineteen drafts prior to the document itself being released, and very little by way of public input and consultation. The Convention was drafted almost exclusively by law enforcement. It is a "wish list", and this is apparent in its disregard for privacy and civil liberties interests within the text.

Even after the release of the draft, and with public consultation, very little substantive change was made to the document and there has been very little in way of acknowledgement to the concerns of privacy and human rights organisations. To submit to a treaty, the draft of which was conducted with such disregard for the democratic and participatory process, condones this process of lawmaking.

UN Solution

Last year there was an attempt made by the UN to begin negotiations over an international Cyber Crime Treaty. The UN recognises that human rights must be central to any criminal justice system that is to be considered fair and humane and this should be the forum for the creation of a truly global standard with commensurate protections. This process was blocked primarily by the EU and US who were in favour of further propagating the CoE Cybercrime Convention as world standard. This treaty does not contain within the minimum protections necessary to ensure an adequate global standard. We continue to advocate a more inclusive, adequately balanced approach through the UN that balances the requirements of law enforcement agencies and civil liberties.