SUBMISSION NO. 8

Submission to the Joint Select Committee on Cyber-safety Inquiry into Cybercrime Legislation Amendment Bill 2011

Introduction

Electronic Frontiers Australia Inc. (EFA) is a non-profit national organisation representing Internet users concerned with on-line rights and freedoms. EFA was established in 1994, is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties.

EFA was a founding member of the Global Internet Liberty Campaign (GILC), an international coalition of online civil liberties groups, which made representation to the working group drafting the Convention, and so EFA has been party to opposition to some of the articles of the Convention since the drafting stage[1]. EFA is on record as having argued against many of the proposals in the Convention since the drafting stage, and still feels that the Convention is very problematic. This legislative draft has confirmed that opinion.

We remain concerned about the combination of a lack of mutual criminality proceedings, and feel that we need strong protection against foreign request for assistance in regards to offences with political elements. We appreciate that the assent of the Attorney General is required, but we believe that issues remain.

Our major concerns, however, are with the strong expansion of applicability of the offences under the Criminal Code. The minimum amendments have been made to allow the necessary coverage required by the Convention, but we feel this expands the applicability of the offences far too widely.

Criminal Code Revisions

We are extremely concerned about revisions to the Criminal Code. It appears that minimal revisions to the text of the Criminal Code have been made to satisfy the requirements of the treaty, but these minimal textual changes (a short series of deletions) have had a very major effect on the nature of the offences described. In effect, offences that previously applied only to either interference with a Commonwealth computer, or were made via a carriage service provide, now apply to any interference with a computer. This vastly broadens the applicability of these offences. EFA understands that more general offences are required for compliance with the Convention, but does not regard simply removing the existing conditions as an adequate response. Any unauthorised interference with a computer is now a significant criminal offence,

[1] GILC response recorded at http://gilc.org/privacy/coe-letter-1200.html, EFA reasoning at http://www.crime-research.org/library/CoE_Cybercrime.html written by Greg Taylor, board member of EFA at the time.

regardless of circumstances or intent, regardless of content. Actions become a more serious crime purely by virtue of data being stored digitally rather than on paper. We believe strongly that the changes to the Criminal Code should be considered in far more detail, and the parts of the legislation should be significantly revised from the current draft.

If the goal is compliance with the Convention, the conditions previously in place should not simply be removed, but replaced with restrictions more appropriate to the offence. The Convention explicitly allows for the broader (but still significant) restriction that offences apply only 'in relation to a computer system that is connected to another computer system', as permitted by Article 3 and 4, for example. The proposed legislation removes the carrier service, and replaces it with no requirement for connection at all. We strongly advocate replacing the carrier service requirement with legal wording equivalent to connected system requirement permitted by the Convention.

We are particularly concerned with section 477.2 of the Criminal Code, Unauthorised modification of data to cause impairment, section 477.3, Unauthorised impairment of electronic communication, and section 478.1, where the amendments change an offence concerned with modification of a Commonwealth computer or via a carriage service, to an offence concerned with the modification of data on any computer, in any Australian jurisdiction, by any means. This changes the offence to an extremely broad one, without reviewing the applicable penalties. Deleting a message from a modern mobile phone, by hand, would qualify for a several years imprisonment, for example.

Section 478.2 is another example of how the broadening of applicability can be extreme, and result in an unacceptable broadening of the applicability of the offence. The offence in the unamended Criminal Code is to interfere with Commonwealth data. The amended version makes it punishable by 2 years Imprisonment to interfere with authorisation with any data storage device at all, regardless of the owner of the data, the value of the data, or the level of harm resulting!

EFA believe that a change of this nature, that very much broadens the applicability of the offences, should be accompanied by a significant review, and not simply added to comply with the Convention. The changes to the Federal Criminal Code are significant, and not simply a matter of closing some jurisdictional loopholes as implied by the explanatory memorandum. The effect of the changes is to introduce some extraordinary penalties to interference with computer equipment by any means.

In addition to the direct effects of the significant changes, the context of the laws has changed significantly since 1995. Modern smartphones and other personal appliances would clearly qualify as a computer under the act, and without the requirement of the act being committed via a carriage service provider, a very wide range of interaction with it might qualify as Unauthorised access to, or modification of, restricted data (478.1), or even Unauthorised modification of data to cause impairment, 477.2 (especially as actual impairment, or even intent to cause impairment ('reckless' modification is sufficient), which carries a significant penalty of 10 years in prison. Without restrictions (such as the requirement the offence be via a carriage service), and not restricted to Commonwealth computers, the questions of access and authorisation become quite murky, and not straightforward[2]. In some jurisdictions, non-compliance with an End User Licence Agreement has been considered unauthorised use, for example. There is a significant issue of questions of authorisation that should remain matters of civil dispute becoming offences that carry significant criminal penalties.

Another issue of unintended consequence of the changes is that the very broad applicability of offenses means that sections 478.3 and 478.4 of the Criminal Code, though both are unamended, also became far more broadly applicable in their application (as they refer to other, amended, offences). This may be an issue as regards to the legality of possession of various tools used to penetrate computer security (as such tools are almost by definition unnecessary for authorised access). EFA strongly supports the broad legal availability of such tools, both on principle, and for the very practical reason that such tools are necessary for testing by anyone seeking to confirm or investigate the security of a system.

The committee has already noted the potential constitutional issues raised by cases such as Dickson v The Queen. The proposed Criminal Code amendments would make the Federal Criminal Code computer crime offences to broad, that in almost all situations in which an offence had been committed under State or Territory law, a Federal offence would also have been committed. So the issues raised by Dickson v The Queen would be potentially relevant in the great majority of offences committed under the proposed legislation, potentially significantly complicating prosecution of such offences.

We feel the amendments to the Criminal Code are overly broad, the consequences poorly thought out, and far broader than they need to be for compliance with the Convention. We suggest this section of the proposed legislation should not proceed in its current form.

Mutual Assistance in Criminal Matters Act

We remain concerned about the lack of dual criminality provisions for mutual assistance. The amendments to the Mutual Assistance in Criminal Matters Act 1987 do not contain any exceptions specifically omitting political offences (even though such a specific exemption is explicitly permitted under the Council of Europe Convention on Cybercrime). While we appreciate that authorisation for a stored communications warrant is at the discretion of the Attorney General, we would like to see further safeguards, both legislative and procedural, ensuring that these provisions are not used to investigate dissident activity in repressive states (typically in such states dissident activity can carry harsh criminal penalties, and so qualify under other provisions of the act), or otherwise conduct investigations and surveillance into activities that are not criminal activities in Australia. Besides human rights issues related to dissident activities, it is also a concern that some disputes (such intellectual property rights disputes) that may be civil disputes under Australian law may be criminalised in other

[2] Hacking Offences, Australian Institute of Criminology, http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb005.aspx

jurisdictions, and if they reach $100,000[3] may qualify for a stored communications warrant under the amended act (particularly as notional potential penalties in such cases can often be quite speculative).

We feel that the potential for this legislation to allow communications interceptions warrants intended for serious criminal and intelligence investigation to be pressed into service by foreign agencies to investigate activities that are not illegal under Australian law remains an area that must be examined carefully in the proposed legislation.

We therefore would recommend that section 13 of the proposed Act, which would amend section 116(2) of the Mutual Assistance Act, should include more explicit checks to the extent to which the investigation may constitute criminal activity under Australian Law. That section also includes, in proposed section 2A, the issue of how interference with individual privacy, but does not make explicit what level of privacy violation would be acceptable, leaving a great deal of scope for interpretation. Some explicit guidelines on the level of acceptable privacy violation would be a valuable safeguard here.

In light of our concerns with mutual criminality, we are strongly supportive of Item 21, which amends the Telecommunications Intercept Act to require the Minister to report on the extent to which foreign stored communications warrants meet, or substantially meet, mutual criminality, and we would welcome strengthening of these requirements to include more detail.

Conclusion

There are several areas of the proposed legislation that we have not had the time to discuss fully, due to the short time schedule for comment. We believe that privacy implications in particular have not been adequately addressed in this submission, and deserve further scrutiny.

EFA is very concerned with amendments to the computer crime offences in the Criminal Code, and believe these parts of the current legislation are both deeply problematic, and unnecessary for adherence to the Convention.

We also retain concerns EFA remains concerned about about the human rights implications of no strict requirement for dual criminality, though we acknowledge some valuable reporting requirements within the legislation.

Article 12 of the Universal Declaration of Human Rights states:

> 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

EFA is concerned that some aspects of this legislation can potentially enable arbitrary interference with privacy and correspondence. We believe it should treated with great caution. But worse, we believe the Criminal Code changes would apply serious criminal penalties, up to 10 years imprisonment, on a very broad range of actions, well beyond what is required for the Convention, and for this reason the legislation should be rejected in its current form.

---

[3] Or equivalent allowing for future increase in the value of a penalty unit.

David Cake
Chair
Electronic Frontiers Australia

Addendum: About EFA

Electronic Frontiers Australia Inc. (EFA) is a non-profit national organisation representing Internet users concerned with on-line freedoms and rights. EFA was established in January 1994 and incorporated under the Associations Incorporation Act (S.A.) in May 1994.

EFA is independent of government and commerce and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties.

Our major objectives are to protect and promote the civil liberties of users and operators of computer based communications systems such as the Internet, to advocate the amendment of laws and regulations in Australia and elsewhere (both current and proposed) which restrict free speech and to educate the community at large about the social, political, and civil liberties issues involved in the use of computer based communications systems.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. The EFA board includes members from a range of backgrounds, and EFA is not affiliated with any political party.
