Australian
Privacy
Foundation

e m a i l: enquiries@privacy.org.au
w e b : www.privacy.org.au

11 March 2010

Supplementary Submission to the Senate Standing Committee on Legal and Constitutional Affairs regarding the inquiry into the Crimes Legislation Amendment (Sexual Offences Against Children) Bill 2010

Supplementary Submission by the Australian Privacy Foundation

1. We are grateful for having had the opportunity to provide you with our written submission (Submission 5), and for having had the opportunity to speak to that submission at the Senate hearing held 9 March.

2. We acknowledge that we were offered the opportunity to amend our submission at the hearing and did not do so.

3. For the benefit of the Standing Committee, we would nevertheless like to offer the following additional observations.

Inadequate defences for innocent receivers of prohibited content

4. Bearing in mind that a person has limited possibilities of controlling what type of content one receives, the issue of possessing child pornography deserves some further attention.

5. Imagine that a person receives a MMS or an e-mail containing underage sexting images. Imagine further that the recipient does not check the inbox on a regular basis or, for some other reason (other than a desire to keep the content), does not delete the images (for example, because the person is in the habit of retaining all emails in a personal or business archive, or an attempt to delete the content is made, but fails).

6. In such an instance, the recipient should typically not be considered guilty of any child pornography offence. However, it is not entirely clear to us how such a person is protected under the current legislation and the Bill.

7. A number of additional circumstances exist, beyond attachments that are 'pushed' into a person's electronic mailbox. These include:

a) downloads that are pulled down to the device by some other user;
b) downloads that are pulled down to the device by the user, intentionally, but unwitting as to the content of the file. In some cases, the file's contents may be displayed, in which case the person may become aware that they have infringing content on their device. As the draft law is currently phrased, that in itself may be sufficient to create an offence, even if the person is horrified, and immediately deletes the file. On the other hand, not all files that are downloaded are ever opened, in which case the person may remain unaware that they have infringing content on their device; and
c) malware of various kinds, including peer-to-peer (P2P) software, may utilise a person's device as a waystation, or storage-device-of-convenience, without the person intentionally acquiring a copy of the infringing material, and without the person being aware that the infringing material is on the device.

8. Perhaps, an innocent recipient can rely on defences outlined in Division 9 of the *Criminal Code Act 1995* (Cth). However, in our view, it may be preferable to include a more specific defence.

9. It is of course crucial that such a defence does not become a loophole for genuine offenders, so care must be taken in the drafting. Perhaps inspiration can be found in how the matter is addressed in the *Crimes Act 1900* (NSW). More specifically, s. 91H(5) states that:

> "It is a defence to a charge for an offence under subsection (2) not involving the production or dissemination of child pornography that the material concerned came into the defendant's possession unsolicited and the defendant, as soon as he or she became aware of its pornographic nature, took reasonable steps to get rid of it."

Inadequate defences for intending reporters of prohibited content

10. Furthermore, it is also important here to review how the proposal impacts on those wishing not to just 'get rid of it' but to assist law enforcement and investigation aimed at the real perpetrators, by reporting the unsolicited receipt of such material, or its discovery on a server or storage or similar device under the administrative control of the

individual. This includes both individual citizens, and those such as system administrators or network technicians who have a role in inspecting the entire contents of a system whose content they do not initiate or normally control. From a public policy perspective the reports that similar provisions elsewhere have resulted in practice in a reduction in willingness to report and deal with the worst material are disturbing, as this can lead to its longer persistence in the online environment (compared to more innocuous, less criminalised deprecated content), and failure to pursue enforcement action against the material's deliberate initiators and distributors. This gives support to the observation that well-intentioned but insufficiently targeted extension of criminal sanctions and responsibility may in such cases have paradoxical unintended consequences contrary to the interests of those the legislation aims to protect. The risk of this should be addressed in more detail before the draft proceeds.

11. As an example, see s273.9 Defences to offences against this Division

(1) A person is not criminally responsible for an offence against section 273.5 or 273.6 because of engaging in particular conduct if the conduct:

(a) is of public benefit; and

(b) does not extend beyond what is of public benefit.

In determining whether the person is, under this subsection, not criminally responsible for the offence, the question whether the conduct is of public benefit is a question of fact and the person's motives in engaging in the conduct are irrelevant.

Note: A defendant bears an evidential burden in relation to the matter in this subsection, see subsection 13.3(3).

(2) For the purposes of subsection (1), conduct is of public benefit if, and only if, the conduct is necessary for or of assistance in:

(a) enforcing a law of the Commonwealth, a State or Territory, or a foreign country; or

(b) monitoring compliance with, or investigating a contravention of, a law of the Commonwealth, a State or Territory or a foreign country; or

(c) the administration of justice (whether within or outside Australia); or

(d) conducting scientific, medical or educational research.

(3) Paragraph (2)(d) only applies if the person's conduct was, in all the circumstances, reasonable having regard to the purpose mentioned in that paragraph.

(4) ... etc.

12. There apparently remains no defence for a non-government employee seeking to assist reporting and takedown because these defences are framed to avoid most people being able to use them, rather than ensuring they are clearly available in appropriate circumstances. For instance:

- the person's motives are irrelevant: if they intended to assist but do not fall within public benefit subsection (2), they are caught.

- the notions of e.g., "enforcing" or "investigating contravention" of a law in 273.9(2)(a) and (b) are ambiguous. The explicit mention of law enforcement officers in defence (3) may suggest that (2) extends beyond those in these roles, but the fact that (3) covers conduct beyond that in (2) makes this interpretation less certain. The intent could for instance be that you have to have close official connection to for instance law enforcement to use (2), and (3) is merely a catch-all designed to give very wide exemption to enforcement or intelligence agents, not one which implies (2) is available to a 'civilian' whose intention is to help investigate an offence by reporting.

The Explanatory Memo confirms that coverage is extremely limited, not intended for those seeking to assist by reporting. Eg 273.9(2)(b): "This defence will be targeted at officers of government agencies involved in monitoring and investigative activity related to regulatory schemes that they administer." The other defences are similarly directed at protecting officials only.

13. Anyone except an official investigator etc. is thus unprotected, regardless of what they do or their intention. This is a defect of both this Act and the original Act relating to carriage services. It is based on a demonstrably false assumption that the current regime is intended, and is effective in, having abusive overseas sites taken down in the most efficient way (thus removing the material from where it can have any effect). Recent research and experimentation overseas has demonstrated that simple direct action and reporting often works very effectively where law enforcement does not. Law enforcement is apparently often more concerned with convictions than with effective suppression of this content; while this is their role, individuals should not be exposed to criminal liability for reporting material to them, or to the site hosts most able to effectively and immediately remove the material from circulation.

14. 273.9(5)(a) only applies to assisting ACMA's black list, not police. ACMA does not have a role in law enforcement, and there is wide concern about the limited effectiveness of the regulatory model they operate, so an ordinary person would have good reason to consider reporting a criminal site to the police first, yet they are apparently exposed to liability if they do so.

15. It is also a matter of some concern that the Explanatory Memorandum re 273.9(2) actually seems to limit the coverage of the public benefit defence in a way that the legislation's plain language does not. Innocent and well intentioned reporters of material who simply read the Act may find themselves deprived of what they might have

expected to be a defence. The notion of 'public benefit' is thus of potentially confusing application. If the intent is to criminalise well intentioned citizens or technical personnel not employed by government and deprive them of this 'public benefit' defence (by excluding consideration of intention, and by having the second reading speech hint to a judge that such people are not covered) it should say so much more explicitly, and the proponents explain why they are exposing potentially effective means of suppressing this content to liability.

16. There is another issue with the new offences, defining the 'presence' element of 'engage in sexual activity' to include where someone is not present but connected by a communications system.

17. For instance, two people in a relationship but not actually present, one engaging in 'sexual activity', the other not but with a child in proximity, could potentially be liable if connected by a phone or internet link with audio or video. There is a defence of 'not seeking gratification', but the onus lies with the defendant. This could potentially impact on couples living apart in small premises, where their child could wander past. While parents are generally discouraged from real sexual activity in the presence of their children in the real world, in some smaller premises there may be heightened risk of falling foul of the provisions in the case of communications-mediated activity. Wealthy or older people with larger homes are less likely to be at risk here than younger or poorer people in cramped premises where communications privacy is less practical. A malicious complaint and a keen prosecutor could put many such parents at risk in what might otherwise be considered relatively private communications, and relatively innocuous circumstances (how far are breeding parents expected to go to hide the fact that they have sex, or sexual thoughts, from their children? It is certainly discouraged, but query whether it should potentially fall into this category of the most serious offences?).

18. The use of communications devices in ubiquitous/constant contact modes is only just beginning, and it is not clear that these new circumstances are adequately considered. While the teenage sexting practice seems to have been deliberately excluded by limiting the carriage service offences to where one participant is over 18, other situations (such as the one above) have not apparently been adequately considered.

Conclusion

19. We again thank you for your attention.

For further information contact:

Dr Dan Svantesson, (07) 5595 1418
and
David Vaile, 0414 731 249
E-mail: enquiries@privacy.org.au
APF Web site: http://www.privacy.org.au