**Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs**

**Copyright Amendment (Digital Agenda) Bill 1999**

Dated 1 October 1999

Leif Gamertsfelder
17/33 Lagonda Street
Annerley Qld 4103
leif.gamertsfelder@dgj.com.au

## 1.0 Item 4 – "circumvention device"

1.1 The word "device" should be defined for the purpose of this item. The word is not relevantly defined in either the *Copyright Act 1968* or in the *Acts Interpretation Act* 1901. Accordingly, the courts may refer to the Macquarie Dictionary when determining the meaning of the word "device". The Macquarie Dictionary defines "device" to mean:

> "...a plan or a scheme for effecting a purpose..."

1.2 It is arguable that any writing setting out how to circumvent an effective technological protection measure (whether or not for legitimate purposes such as education) could be caught by this definition. The Bill should at the very least make it clear that writings for bona fide education purposes will not fall within this definition.

## 2.0 Item 5 – "circumvention service"

2.1 The word "service" is not defined in the Bill or in the Acts Interpretation Act. The Macquarie Dictionary defines "service" as:

> "...the supplying or supplier of any articles, commodities, activities, etc, required or demanded..."

2.2 It is not unlikely that a court could consider any information which facilitates the act of circumventing an effective technological protection device could fall within this definition (whether such information was delivered as part of a university course on security testing or some other legitimate purpose) and therefore trigger the prohibitions in Item 116A of the Bill. Accordingly, the scope of the definition should be limited.

## 3.0 Bill will hinder security on the Internet

3.1 The Bill will hinder Internet security because it does not facilitate a pro-active approach to system and network security. Items 116A(3) and 132(5) promote a reactive regime. That is, they do not permit a supplier of circumvention devices, remedial programs or fault detection devices to supply end users with such products prior to a "declaration" being made. Obviously, a declaration will usually only be made *after* the end user becomes aware of a problem. This could be well after a virus has been introduced into a system and loss or damage is suffered.

3.2 On the other hand, a pro-active entity in the security testing or error correction industry would generally learn of a problem well in advance of an ordinary consumer of software products. That entity could adopt an economic loss minimisation strategy by sending unsolicited analytical and remedial tools

(including circumvention devices) to an end user to ensure that they detect and remediate the problem before loss or damage is suffered. In fact, this type of pro-active approach is not only adopted by security testing institutions, it also happens on a smaller scale within groups of companies. This type of loss minimisation strategy is adopted on an ad hoc basis by individual companies in a group of companies that discover a security problem, remediate the problem and then supply the relevant circumvention devices (if necessary) and programs to a related body corporate *without* requesting a written "declaration" of the type contemplated by items 116A(3) and 132(5G). A declaration requirement is counter to best practice in this area.

3.3 In summary, it would appear that the better approach on this point would be to dispose of the declaration requirement in items 116A(3) and 132(5). This will ensure a more efficient approach in this crucial area.

## 4.0 Item 116A(3) – "declaration"

4.1 Under this item it is unclear whether the drafters are referring to a statutory declaration or a mere notice. A court may decide that the word declaration connotes something more formal than a notice, eg, a statutory declaration.[1] This could place a huge obstacle to the efficient operation of this legislation if Item 116A(3) becomes law. I believe the word "declaration" should be omitted wherever it appears in the Bill and substituted with the words "written notice". This would ensure that e-mail notices would satisfy this requirement when legislation in the form of the *Electronic Transaction Bill* comes in to effect.[2]

4.2 Further, the need to retain declarations under Item 116A and related items for, at least, a period in excess of the limitation period for civil actions, ie, 6 years, seems to be a huge burden on the suppliers of circumvention devices. Indeed, this burden becomes quite extraordinary when one considers that prosecution for criminal offences are not subject to a limitation period and suppliers would be well-advised to keep "declarations" in infinitum.

4.3 Further, the declaration requirement would create manifest absurdity when one considers how security testing is ordinarily performed. If, for instance, there were to be another virus scare of the magnitude of the Melissa virus earlier this year and a person or entity that were to provide a circumvention device on-line for a network, operating system or Internet server program may expect to receive over 1,000,000 hits to their website in one day. If that supplier were compelled to receive a signed declaration (which could include large encrypted e-mail files) prior to supply of the circumvention device, the receipt of 1,000,000 declarations

[1] While this might be an unlikely outcome, it is possible. The drafters should take the opportunity to make their intentions clear.

[2] Items 9 and 10 of the *Electronic Transactions* Bill provide will recognise a broad range of electronic writings and signatures.

would cause that website to fail. This is not a situation that will have a positive influence on the development of e-commerce.

4.4 In my opinion, the declaration requirement provided in Item 116A(3) and related items should be removed. The limited scope of the permitted purposes should provide enough protection for copyright owners. If however the requirement is introduced, the amendments proposed in paragraph 4.1 above should be implemented.

4.5 Further, the Bill attaches far too much weight to obtaining permission of a consumer in the context of security testing. The focus in this context should be on the actual activities of the person or persons conducting security testing activities. If their activities are bona fide, there should be no need to have a provision providing for declarations of the type contemplated by items 116A(3) and 132(5G).

4.6 The need for authorisation in a different context is also contained in items 116A(7) and 132(5J), provisions which define the term "permitted purpose". By reference to s 47F of the *Copyright Act 1968*[3] a permitted purpose will be, among other things, the reproduction or adaptation of computer programs for security testing purposes. The scope of the protection provided by these items is therefore dependent on the scope of the protection provided in s 47F.

4.7 Unfortunately, the protection provided under s 47F is limited in that protection is only available if security testing is done by or on behalf of the owner or licensee of a computer program. No protection is available under s 47F (and therefore items 116A(3), 116(4), 132(5G) and 132(5H)) if security testing is conducted on an infringing copy of a program.[4] However, in many cases security testing must be done on infringing copies of programs and in many cases it is not known whether a program is an infringing copy until after the event. Accordingly, much of the protection afforded by items 116A(3) and 132(5G) is illusory by virtue of their relationship with s 47F of the *Copyright Act 1968*.

4.8 The Bill should include a provision amending s 47F of the *Copyright Act 1968* to remove the need for security testing to be done by or on behalf of an owner or licensee of a program and provide a non-exhaustive list of factors for courts to consider when considering when security testing is bona fide for the purposes of s 47F. The Committee is also referred to paragraph 17 of the insightful submission made by Ms Anne Fitzgerald on this important issue.

[3] See items 116A(7)(b) and 132(5J)(b).
[4] Section 47F(2), *Copyright Act 1968.*

## 5.0 Exceptions to Copyright

5.1 Although in many cases it is unlikely that a hacker[5] will come forward to pursue a copyright claim, it is not impossible. If a hacker can claim copyright in her creations (including attack programs or log files[6]), a person supplying or making circumvention devices would need to comply with items 116A(3) or 132(5G) of the Bill.

5.2 This should not be the case in relation to hacking programs.[7] The Bill should expressly exempt the conduct of individuals from the operation of items 116A(3) and 132(5G) where the work in question is a hacking program or other similar attack tool. This could be achieved by inserting a provision that confirms that no copyright subsists in any literary work the purpose of which is to facilitate conduct that is an offence under Federal, State or Territory law, eg, Part VIA of the *Crimes Act 1914*.

5.3 If a specific exception is not made, one would have to rely on existing defences to copyright infringement claims. First, if a hacker was claiming equitable relief (such as an injunction to stop a person doing something) the defence of "clean hands" may apply. That is, because the hacker does not have "clean hands" (ie, by engaging in criminal or quasi criminal behaviour), a court may refuse to grant injunctive relief. Therefore, even if copyright does exist in a hacker's work, it is doubtful whether they would be able to secure equitable relief[8] as opposed to general law relief.

5.4 Secondly, there is the public interest defence. Under the public interest defence a court may refuse to enforce copyright on the grounds of public policy. In Australia however it is unclear whether this defence is good law. Mason J assumed in *Commonwealth v Fairfax*,[9] that the defence may be available in copyright cases,[10] but Gummow J stated in *Collier Constructions v Foskett*[11] that:

> "there is no legislative or other warrant for the introduction of such a concept [ie, the public interest test] into the law of this country....I would hold that in this country there is no such defence known at law."[12]

5.5 I am of the opinion that Gummow J's views would not prevail in hacking cases. However, if His Honour's views do prevail in such cases and a hacker successfully brings proceedings for copyright infringement under the

---

[5] Also referred to as "crackers".
[6] Note that in this context copyright may attach to the manner in which information is expressed [ie, in a log file] in the same way it applies to computer programs.
[7] Also referred to as "attack" programs.
[8] See O'Brien v Komesaroff (1982) 150 CLR 310.
[9] (1980) 147 CLR 39.
[10] Ibid at 56-57.
[11] (1990) 19 IPR 44.
[12] Ibid at 54-57.

circumvention provisions, a person will need to have complied with items 116A(3) or 132(5G) if a supply of circumvention devices occurred.

## 6.0 Excluding rights under items 116A & 132

6.1 Currently, the Bill does not ensure that the exceptions provided in items 116A and 132 are mandatory, ie, not able to be excluded by agreement. The following provision should be included in the Bill:

> "An agreement, or a provision of an agreement, that excludes or limits, or has the effect of excluding or limiting, the operation of subsection 116A(3), 116A(4), 132(5G) or 132(5H) has no effect."

6.2 This proposed amendment mirrors s 47H of the *Copyright Act 1968* (Cth)[13] and will ensure that items 116A(3), 116A(4), 132(5G) and 132(5H) are not rendered devoid of content by contractual mechanisms.

## 7.0 Reasonable Portion Test – Item 20

7.1 At a cursory glance, the proposed amendment contained in item 20 appears to achieve its objective. However, on closer analysis it is clear that item 20 will often miss its target. The relational nature of a website and the pervasive use of hyperlinking can often make it extremely difficult to determine where a "work" begins and ends.

7.2 This makes it difficult to determine whether a particular webpage is a part of a literary work for the purposes of the *Copyright Act 1968.* If it is not a part of a literary work, item 20 has no effect. However, if it is a part of a literary work, the nature of the Internet will make it difficult for many people to identify the entire work. This must be done however if the 10% rule is to be applied.

7.3 In my opinion, the Bill should avoid forcing a concept developed for use in the analogue world into the digital world and allow the courts to determine what a reasonable portion is on a case by case basis.

## 8.0 Typographical error

8.1 In item 116A(4)(a) and 132(5H)(a) the colon should be omitted and a semi-colon substituted.

Please let me know if I can assist you with any issue arising from my submissions.

Leif Gamertsfelder

[13] Section 47H was introduced by the *Copyright Amendment (Computer Programs) Act 1999.*