Submission to the House of Representatives Standing Committee

On Legal and Constitutional Affairs

COPYRIGHT AMENDMENT (DIGITAL AGENDA) BILL 1999

Anne Fitzgerald
Technology Lawyer
PO Box 201
Moorooka Qld 4105
Afitzg@hotmail.com
Phone: (07) 38489374

These submissions deal with the provisions of the Copyright Amendment (Digital Agenda) Bill 1999 (the Digital Agenda Bill) relating to computer security testing. The provisions of the Digital Agenda Bill when read together with existing provisions of the Copyright Act 1968 as amended by the Copyright Amendment (Computer Programs) Act 1999 are too restrictive of bona fide security testing. Consideration should be given to substantially re-drafting these provisions in order to permit bona fide security testing organisations to continue their activities.

It is submitted that:

- **"security testing" should be defined; and**
- **the scope of legitimate security testing activities should be described in a way that does not depend on obtaining the permission of the owner of copyright in the computer program which is being tested.**

1. In the lengthy deliberations that have resulted in the Digital Agenda Bill, there has not previously been any public consideration of the permissible scope of computer security testing activities. This Committee's consideration of the Digital Agenda Bill is the first occasion on which the issue of the appropriate scope of an exception for bona fide computer security testing has arisen for public consideration.

2. Given the increasing importance of ensuring the security of computer networks in the context of the global networked environment of the internet, it is essential that the proposed legislative amendments do not compromise or hinder legitimate security testing activities.

3. The Digital Agenda Bill's precursors include the Copyright Convergence Group's 1994 report *Highways to Change: Copyright in the New Communications Environment*, the joint discussion paper prepared by the Attorney-General's Department and the Department of Communications and the Arts in 1997, *Copyright Reform and the Digital Agenda*, and the draft Digital Agenda Bill and accompanying Explantory Memorandum released for public comment in February 1999. None of these documents deal with the concept of computer security testing. For a general overview of the various reports on copyright law, members of the Committee are referred to Fitzgerald, A. *Intellectual Property Law*, LBC Information Services, Nutshell Series, July 1999, ISBN 0 455 21661 4.

4. Following the release of 1997 Discussion Paper on *Copyright Reform and Digital Agenda*, submissions were made to relevant officers in the Attorney-General's Department and the Department of Communications and the Arts pointing out that it would be necessary to ensure that anti-circumvention provisions were subject to certain exceptions. Attention was drawn to the US experience in implementing the WIPO Copyright Treaty in the Digital Millennium Copyright Act (DMCA) during 1998. As enacted in October 1998, the DMCA provided for exceptions to the anti-circumvention provisions in s1201(a)(1) in order to permit a range of activities, including:

- Reverse engineering (s1201(f));
- Encryption research (s1201(g));
- Protection of personally identifying information (s1201(i)); and
- Security testing (s1201(j)).

5. In February 1999, the Minister for Communications, Information Technology and the Arts and the Attorney General announced that the Copyright Act 1968 would be amended to introduce limited exceptions to permit copying of computer programs for purposes of:

    - Creating interoperable software or hardware;
    - Error correction, including y2k compatability; and
    - Security testing.

6. While the introduction of exceptions for interoperability and error correction had been considered at length and recommended by the Copyright Law Review Committee headed by Mr Justice Sheppard in its 1995 *Computer Software Protection: Final Report*, the issue of security testing had not previously been canvassed. These exceptions were introduced by the Copyright Amendment (Computer Programs) Act 1999. It amended the Copyright Act 1968 by introduce a new Division 4A into Part III which permits limited copying for purposes of interoperability (s47D), error correction (s47E) and security testing (s47F).

7. Submissions on the draft Digital Agenda Bill which was circulated for public comment in February 1999 drew attention to the importance of ensuring that these exceptions were carried across to the anti-circumvention provisions. Unless the anti-circumvention provisions were made subject to such exceptions they would provide overly strong protection to the owner of copyright in materials which have been protected by technological mechanisms. In other words, it would be necessary to adopt a similar approach to that taken in the US in the enactment of the DMCA in 1998 whereby specific uses are excluded from the provisions relating to anti-circumvention devices and services.

8. The Digital Agenda Bill proposes to amend the Copyright Act 1968 by inserting a new s116A and amending s132 to deal with the unauthorised circumvention of effective technological protection measures which have been applied to copyright materials. It is worth noting that these provisions differ from those in the corresponding US legislation, the DMCA, in that that they do not prohibit the circumvention of a technological protection measures *per se.* Rather, they target the manufacture, distribution, importation, exhibition for trade purposes, sale, hiring etc of circumvention devices and the provision of circumvention services: ss116A(1), 132(5B), (5C). These provisions are subject to certain exceptions where the circumvention device or circumvention service is being used for a *permitted purpose* (ss116A(3),(4),(7) and 132(5G), (5H), (5J)). In the case of security testing, the relevant permitted purpose is that set out in s47F of the Copyright Act 1968, as amended by the Copyright Amendment (Computer Programs) Act 1999.

9. Section 47F provides that copyright in a computer program is not infringed by the making of a reproduction or an adaptation of the program for security testing purposes. However, the reproduction or adaptation must be made by or on behalf of the owner or licensee of the copy of the computer program (s47F(1)(a)) and the provision in inapplicable where the reproduction or adaptation is made from an infringing copy of a computer program (s47F(2)).

10. It is submitted that the provisions of ss116A and 132 in their present form in the Digital Agenda Bill would not permit activities which bona fide security testing organisations need to be able to do in order to ascertain and ensure the security of computer programs and networks.

11. Since 47F only applies where the reproduction or adaptation of a computer program is made by or on behalf of the licensee of the original computer program and has no application where the reproduction or adaptation is made from a pirated copy of a computer program, it will not cover many of the activities of security testing organisations. As a result, only a very limited category of security testing activities will fall within the scope of s47F. Thus, in most cases, security testing will not be a permitted purpose constituting an exception to the anti-circumvention provisions.

12. The defect in s47F is thereby carried across to ss116A and 132 which define the permitted purpose for security testing by reference to it.

13. Section 47F and, by incorporation, ss116A and 132 are based on a flawed understanding of what is involved in computer security testing. Members of the Committee are urged to seek further information on technical aspects of computer security testing from acknowledged experts.

14. On a day to day basis, security testing organisations are required to examine:

    - Pirated software;
    - Software developed by a recognised software vendor which has been modified by an intruder to fulfill some other purpose (that is, a trojan horse); and
    - Software developed by an intruder or hacker to exploit a vulnerability in a computer program or system (an attack tool).

    It is important to appreciate that in a typical situation it is not possible for a security testing organisation to know what kind of software it is looking at until it commences the analysis of the software.

    Copying and adaptation of the computer software without the permission of the owner or licensee of the original will frequently be necessary and that reproduction or adaptation will often be made from an infringing copy of the program. Where a security testing organisation is examining a trojan horse or an attack tool, it will have to reproduce or adapt the computer program contrary to the provisions of ss47F(1)(a) and (2).

In the case of an attack tool or a trojan horse developed or adapted by an intruder, the author is typically difficult or impossible to identify, making compliance with s47(1)(a) a practical impossibility.

Security testing is not limited to intruder software, but is often used to identify vulnerabilities in commercial software marketed by major vendors. While security testing organisations usually seek and obtain permission from the copyright owner to carry out the necessary copying, it will not always be possible to do so. Security testing organisations receive software for testing from a variety of sources and it would be impracticable to require them to ensure that every piece of software is not derived from an infringing copy or has been made by the owner or licensee of the original program. Much of the work of security testing organisations is time critical and requiring them to ascertain copyright ownership and obtain permission to copy or adapt the software would impose unreasonable contraints on their activities.

15. Section 47F is deficient in that it creates a security testing exception which comes into operation only where the computer program is copied or adapted by or on behalf of the owner or licensee of the original copy (s47F(1)(a)) and where the copy or adaptation is not made from an infringing copy of the computer program (s47F(2)). When this narrowly defined exception is carried across to the provisions to be introduced into ss116A and 132 by the Digital Agenda Bill, will result in a severely limited security testing exception to the anti-circumvention provisions.

16. In view of the fact that the Digital Agenda Bill proposes to create new civil and criminal copyright infringement provisions (ss116A(5), 132(6B), (6C)) it is important that the scope of permitted exceptions are appropriately delineated and clearly described. The penalties for criminal infringement of the anti-circumvention provisions will be severe: up to five years' imprisonment and fines of up to $60,500 for an individual and $302,500 for a corporation (Copyright Act 1968, s132(6A)). The severity of these penalties will cause security testing organisations to curtail their activities unless the area within which they are permitted to operate is clearly delineated.

17. The legitimacy of security testing should not depend on whether the computer program being tested is a legal copy which is being copied or adapted with the permission of the copyright owner or licensee. Rather, the question of whether security testing is permitted should be determined according to specified criteria. Assistance on the kind of criteria to which reference can be made is found in the DMCA, s1201(j):

> (3) FACTORS IN DETERMINING EXEMPTION- In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include-
>
> (A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

18. “Security testing” should be expressly defined in the Copyright Act 1968, along the lines of s47(1)(b)(i) and (ii), to include:
    - testing in good faith the security of a computer program, or of a computer system or network; or
    - investigating, or correcting, in good faith a security flaw in, or the vulnerability to unauthorised access of, a computer program or of a computer system or network.

    In drafting a definition of security testing, regard should be had to the definition of the term in the DMCA, s1201(j):

    > (1) DEFINITION- For purposes of this subsection, the term `security testing' means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.