

SAGE-AU

The System Administrators Guild of Australia

(ARBN 082 497 792)

27th September, 1999

House of Representatives
Standing Committee on Legal and Constitutional Affairs
Parliament House
Canberra ACT 2600

Dear Members

Re: Request for comments – Proposed Amendments to the Copyright Act (“the Act”)

Further to our earlier phone call with Marie Kawaja, the **System Administrators Guild of Australia Inc (SAGE-AU)** makes the following submission detailing relevant issues and concerns with regard to aspects of the proposed Copyright Amendment (Digital Agenda) Bill 1999 (“the Bill”).

As per our discussions with Ms. Kawaja, we confirm our interest in being granted the opportunity to elaborate on our submission by presenting to the Committee at a public hearing. If a public hearing is to be held in Melbourne, then that would be our preference; otherwise a Canberra timeslot would be appreciated.

Background

In the context of the computer industry, a System Administrator is defined as:

“A person who is responsible for the management of one or more computer systems on behalf of the organisation for which they are employed.”

System Administrators are the people responsible for managing the computing operations and information assets of corporations. These people are directly affected by and intimately involved in the implementation of government policy and legislation such as the Act on a day to day basis.

The Systems Administrators Guild of Australia (SAGE-AU) is the professional society for practising System Administrators. We are therefore in a unique position to comment on the Bill, as it will affect those who must implement the legislation and ensure a corporation’s ongoing compliance with it.

Our review has identified a number of concerns with the Bill in its present form. At the outset, however, we wish to state that we agree with the legislative intention underpinning the Bill and consider that the Bill goes a long way towards addressing a number of outstanding concerns and recognising pragmatic problems with the Act in its present form.

Comments on the Bill

The Bill in its present form would directly impact upon practitioners of Systems Administration in a number of ways that we believe are contrary to the legislative intent underpinning the Bill and the Act itself. This includes the ability of those practitioners to perform their normal duties as Systems Administrators, and their ability to develop and communicate security information and security tools.

SAGE-AU

The System Administrators Guild of Australia

(ARBN 082 497 792)

Normal Systems Administration Activities

The current version of the Bill has what we consider to be an unintended effect of personally exposing System Administrators to the possibility of both civil and criminal liability simply for carrying out their normal duties in the course of meeting their professional responsibilities. Moreover, the System Administrator would unreasonably be required to bear the burden and expense associated with defending civil and possibly criminal proceedings, even in circumstances where they were only performing their duties as directed.

System Administrators are the people charged with the responsibility for maintaining the integrity and security of the computing environments for which they are responsible. This, as a matter of course, involves trouble-shooting problems within those environments, conducting security audits (which often involve attempting to breach security in order to identify holes), and often includes use of higher levels of privilege in the course of those maintenance activities.

These systems which are being managed contain material and/or files and programs that are copyright works. Some of these may be owned by third parties other than the owner or operator of the system under scrutiny.

Under the existing drafting of the Bill, it may be possible for a user of such a system to issue legal proceedings against a System Administrator on the grounds that the System Administrator used a circumvention device or provided circumvention services, even though the System Administrator lacked the requisite “*intent to infringe*”. This would place an unreasonable burden on the System Administrator, who would be required to prove lack of such intention.

By way of example, a System Administrator’s tasks would often include copying and/or inspecting a user’s e-mail files to determine the cause of a mail delivery problem. Under the current version of the Bill, a user whose mail was checked in this manner in order to determine and resolve a problem might have the right to issue proceedings against the System Administrator for merely performing that function, with no requirement that an actual breach of copyright has occurred.

There is also a lack of clarity regarding the definition of what amounts to an “*effective technological protection measure*”. For instance, there is the possibility that a Court might interpret a mechanism as simple as file permissions as constituting such a measure, and in those circumstances, any administrative function which side steps those permissions might be found to constitute a breach. This would effectively expose System Administrators to the risk of legal proceedings when carrying out almost every maintenance activity.

Proposed Amendment to the Bill

We suggest that the Bill be amended to state clearly that where a System Administrator is performing his or her duties as instructed or authorised by the owner or operator of the system under scrutiny or the copyright owner, and is therefore acting in good faith, he or she will not be in breach.

For instance an additional section similar to section 39B (which is intended to protect Carriers acting in good faith) could be inserted in the Bill. This clause would serve to protect System Administrators acting in good faith. We would suggest, at least as a starting point, the following wording:-

SAGE-AU

The System Administrators Guild of Australia

(ARBN 082 497 792)

“A system administrator (or other such person who has been delegated the responsibility of maintaining a computer system by the owner or operator of that computer system) is not taken to have authorised or committed any infringement of copyright in a work merely because they have acted in good faith and in accordance with their instructions or responsibilities in managing a computer system for which they have been engaged or employed to so manage.”

Research into Security Potentially Illegal

The proposed sections 116A, 132(5B) and 132(5C) in the Bill would in our view have the unintended effect of making all research into security related topics, and the creation of security related tools (whether hardware or software) illegal.

The security of the Internet and all major developments in computer security have been the direct result of collaborative and openly communicated efforts amongst System Administrators, system developers and researchers from around the world. Moreover, most experienced System Administrators use and contribute to the tools developed in this open source forum to better understand, examine and improve the security of the computer systems for which they are responsible.

Use of these tools forms an integral part of good System Administration practices, and also forms the core of all assessment activities. These tools are both internally and externally supplied. The use of these tools would appear to be permitted by the Bill as they have a significant purpose other than “*circumvention*”. However, it appears that the actual creation of these same tools would arguably amount to a breach.

The creation of security tools (tools which assist System Administrators to assess and identify security holes) could arguably constitute a breach of the Bill on the grounds that the author could reasonably be expected to know that *some portion* (however small) of the user base would use it to infringe copyright. Under the proposed new section 132(5C):-

“A person must not ... make a circumvention device ... if the person knows ... the device will be used ... to circumvent or facilitate the circumvention of an effective technological measure.”

This proposed section would effectively ban the development of tools in the open forum of the Internet. Of course, this version of the Bill would in our submission only prevent Australian citizens from participating in such forums, placing an unreasonable commercial restriction on Australia’s global competitiveness.

Moreover, it could be argued that clause 132(5B) could be read to prohibit the communication of any information relating to security flaws, including that which is necessary to protect one’s machines from those very flaws. This would serve to make Australian sites vulnerable to attack from malicious hackers, who can readily receive these communications from existing international forums (which Australian sites would be prohibited from participating in).

Proposed Amendment to Bill

We would propose that section 132(5C) be re-drafted to remove this inconsistency and to bring it into line with the intentions of the Bill and the Act.

SAGE-AU

The System Administrators Guild of Australia

(ARBN 082 497 792)

Incidental Backups of Copyright Works Illegal

The draft of the Bill contained a proposed section 43A(1A) which would provide exemption for incidental reproduction of “*computer programs*” (such as where computer programs are stored on backup media in the course of a normal backup regime). This clause was moved into the Copyright Amendment (Computer Programs) Act. This provides effective protection within that narrow scope.

A potential problem arises because many data files (which are copyright works) stored on computers and other storage media might arguably not fall within the definition of “computer program” as defined in the Bill. We submit that this might be addressed by altering the proposed Bill to refer to “copyright work” rather than “computer program”. We believe this is in-line with the original intention of the clause.

In Conclusion

We believe the problems we have identified in this submission could be addressed quite readily in line with the intentions of the Bill, so as to enable System Administrators to meet their professional obligations without concerns about possible exposure to legal liability.

We would be happy to discuss our concerns further with you at your convenience. If you wish to clarify any of the issues presented here, then please telephone us.

Yours sincerely,

Geoff Halprin
SAGE-AU Executive Committee