Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia-Pacific news

Gabriela Kennedy

Hogan Lovells, Hong Kong

Keywords:
Asia-Pacific
IT/information technology
Communications
Internet
Media
Law

ABSTRACT

This column provides a country by country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Australia

1.1. *Does copyright subsist in relation to electronically generated works?* Acohs v UCorp Pty Ltd *[2012] FCAFC 16*

1.1.1. *Key points*

- The Full Federal Court has largely upheld the Federal Court's decision on the question of whether copyright subsists in relation to electronically generated works, where there was no single identifiable human author and no clear collaboration between persons using the computer program to generate the work.
- This decision illustrates the difficulty in proving that copyright subsists in a body of source code where the code is generated by a computer program.

1.1.2. *Factual background*

Under various legislative regimes in Australia, a manufacturer, importer or supplier (an "MIS") of hazardous substances and dangerous goods must provide a material safety data sheet (an "MSDS") which sets out prescribed categories of information about the product.

The appellant, Acohs and the respondents, UCorp compete in producing MSDSs. The appeal concerned the question of copyright in relation to electronic MSDSs and the underlying source code.

Acohs' MSDSs were generated by Acohs' computer program called Infosafe and could be created by 1 of 3 ways:

(a) "authoring" by Acohs' employees through a process of data entry;
(b) transcription by Acohs' employees; and
(c) modification by Acohs' customers.

Acohs argued that it was the owner of copyright subsisting in each of its MSDSs, and in the source code for each such MSDS, and UCorp had infringed that copyright by copying its MSDSs.

1.1.3. *At trial*

At first instance, Justice Jessup found that copyright did not subsist in the source code or in the MSDSs, except for certain MSDSs that had been authored by Acohs' employees.

His Honour held that while there was no reason to deny a body of source code the status of a literary work for the purposes of the *Copyright Act 1968* (Cth) (the "Act"), the source code generated by Acoh's computer program (Infosafe) could not be described as an original literary work for copyright purposes for the following reasons:

- the source code, as a complete work was not written by any single human author;
- it could not be said that Acohs' programmers who wrote the routines and instruction tags for Infosafe were the authors; and

0267-3649/$ – see front matter
http://dx.doi.org/10.1016/j.clsr.2013.02.003

- the source code for each identified MSDS was not a work of joint authorship because it was artificial to say that the programmers and the employees who created MSDSs using Infosafe had collaborated with each other in writing the relevant source code.

Although His Honour found that the only MSDSs that attracted copyright protection were the ones "authored" by Acohs employees, His Honour found that there was no copyright infringement of these MSDSs as Acohs had impliedly licensed UCorp to reproduce these MSDSs, as UCorp had reproduced these MSDSs for MISs who were Acohs customers and had an implied licence to make or obtain copies of the Acohs MSDSs.

1.1.4. On appeal

The Full Federal Court largely upheld the trial judge's ruling on the status of the source code and other MSDSs as not being original literary works, but ruled in favour of Acohs on the issue of infringement of the Acohs authored MSDSs.

Interestingly, on the issue of copyright in the source code, the Court said it was possible that a routine or even an information tag for a computer program, if original may be sufficiently substantial and functionally separate from the entire program of which it forms a part to constitute a separate copyright work. Unfortunately for Acohs, it did not plead or advance this argument at trial or on appeal.

The MSDSs that UCorp copied were made in response to requests from customers who had the benefit of an implied licence from Acohs. The Court found that these copies fell within the scope of the implied licence and therefore there was no infringement.

However, Ucorp also "trawled" the internet looking for other MSDSs and, when it found ones it did not already have stored, downloaded them to have them readily available in anticipation of customer requests. As these copies were not made in response to an implied licensee's request, but in anticipation of a request which might never be made, these copies fell outside the scope of the implied licence. Ucorp was found liable for infringing the copyright in all those MSDSs which it reproduced without a specific request from a customer before the copy was made.

Maria Marinelli *(Partner), Ashurst, Melbourne (maria.marinelli@ashurst.com) and* **Vern Phang** *(Lawyer), Ashurst, Melbourne (vern.phang@ashurst.com).*

2. China

2.1. *China to strengthen protection of online private information*

On 28 December 2012, the Standing Committee of the National People's Congress of China issued the Decision on Strengthening Protection of Online Information (the "Decision"), effective as of its issue date. The purpose of the Decision is to protect online personal information, online privacy as well as public interests. Below is a brief summary of the Decision.

2.1.1. Scope of protection

Electronic information that may identify an individual or involves personal privacy is protected by the Decision. Stealing, selling or otherwise illegally obtaining/providing such information is strictly prohibited.

2.1.2. Obligations for collecting and using personal electronic information

Such obligations include:

(a) the principles of legality, appropriateness and necessity must be followed;
(b) the purpose, method and scope for the collection and use must be disclosed;
(c) the relevant individual's consent must be obtained in advance; and
(d) the collection and use of the information shall not violate relevant laws and regulations and shall not violate any agreements or contracts with the subjects of the data collection.

2.1.3. Obligations for safeguarding personal data information

The collected information must be kept confidential and shall not be leaked, modified, destroyed, sold or illegally provided to others. Technological measures and other necessary measures must be taken to ensure the safety of the information. If the information has been or will be divulged, damaged or lost, the entity must immediately take remedial measures to correct the situation.

2.1.4. Information management

If an Internet Service Provider discovers information that was prohibited from being released or transmitted, it must immediately cease the transmission, remove the information, keep relevant records, and report to the relevant government authority. An Internet Service Provider that provides access to internet, landlines and cell phones, or that provides platforms for publishing content must require users to provide authentic identity information.

2.1.5. Commercial electronic information

Without explicit consent or request from a recipient, an information provider shall not send commercial electronic information to a recipient's telephone, mobile phone or personal e-mail.

2.1.6. Remedies

If an individual discovers a personal information leak, or dissemination of his/her privacy information, or is harassed by commercial electronic information, he/she has the right to request the Internet Service Provider to take necessary measures to stop it. He/she may also file a complaint to the relevant government authority.

2.1.7. Government obligation

The government authorities must take technical or other necessary measures to prevent stop and deal with illegal and criminal activities relating to online information, including obtaining personal digital information through stealing or other unlawful means, or selling or illegally providing information to others. Government authorities or its agencies must keep personal digital information that is obtained during the