

Open source software use is still risky

By Andrew S. Nunes with the assistance of Jennifer Sloan

Software developers are increasingly using open source software ("OSS") in the development of software programs, both for their own internal use as well as for external commercialization. By using OSS, developers save time and costs by not "re-inventing the wheel". However, the use of OSS pursuant to the terms of most OSS licences presents a number of risks and uncertainties, which many people in the industry are hoping will be addressed by the new version of the popular GNU licence.

What is OSS?

OSS (a.k.a. "free software") is software for which the right to use, modify and distribute (in its original form and/or as modified) is made freely available to everyone. To enable its modification, the

source code (i.e. human readable form) of the OSS is provided or otherwise made available as part of the distribution. This is in contrast to the traditional distribution model whereby software is made available only as object code (i.e. computer readable form — a.k.a. executable or binary form), which permits the execution of the software but does not permit the software to be modified.

Risks of OSS

One of the risks associated with the use of OSS is the lack of a warranty — users generally receive the product "as is". Another concern is that users are afforded little if any protection against claims for intellectual property infringement.

A third risk is the potential for users to "infect" their own proprietary software. Many OSS licences stipulate that when a user combines open source code in a

certain manner with other software code, then any future distribution of the other software must include distribution of its source code. This is known as a "viral" licence. Therefore, users must be cautious when using OSS in conjunction with software that they wish to retain as proprietary and, in respect of the source code, confidential.

The GNU Licence

Of the over 50 OSS licences, the GNU General Public Licence (GPL) is said to be the most widely used free software licence worldwide. The Free Software Foundation and the Software Freedom Law Center are currently in the process of redrafting the GPL, utilizing an international public review process. The drafters plan to release the final draft of the new version, GPLv3, in early 2007. The second discussion draft of GPLv3 was released on July 27.

Changes to GPLv3

Without going into a detailed discussion of all the changes contemplated in GPLv3, it is worth noting a few changes that are of particular interest when considered in light of certain statutory requirements and the risks associated with the use of OSS.

1. Digital restrictions management

Digital restrictions management (DRM) is the practice of inserting techniques into software programs designed to restrict a user's ability to use or modify the program. DRM is seen as problematic for OSS because it violates the user's "essential freedoms" to fully use and modify the code. The current draft of GPLv3 has been modified in an attempt to prevent users from imposing DRM restrictions on subsequent users of GPL covered software and then forbidding the user from taking them out.

In part, these changes are intended to address the enactment of the *Digital Millennium Copy-*

right Act in the U.S. and similar international directives, which prohibit the circumvention or removal of DRM techniques.

2. Intellectual property infringement claims

Under the current draft of GPLv3, every person who receives a program under the licence also receives a covenant from each author and conveyor of the program that they will not assert any patent claims they may have or acquire over the program against any subsequent users. Arguably, this change does not provide any additional protection over the language in the existing GPL, given that the covenant not to sue is arguably implicit in the general grant of the licence.

The current draft of GPLv3 also requires distributors of the OSS to shield downstream users from patent infringement claims where the distributor knows that the code being distributed relies on a non-sublicensable patent licence

see oss p. 14

Corporate "pretexting" may be morally offensive, but is it illegal?

By Joe L. Lai

Pretexting is an investigative technique used primarily by data brokers and independent contractors to obtain various types of personal information, phone records being a prime target. A pretexter will pose as a customer of a landline or mobile phone company and attempt to dupe a call centre agent into releasing personal information. It is unknown how widespread this practice is although some have suggested that pretexting may be commonly endorsed within the corporate community. Buyers of personal information include law firms, financial institutions, collection agencies, law enforcement agencies, and private investigation and research companies. Such parties may, for example, require certain information to locate debtors or witnesses who are not readily available. How prevalent pretexting is in such cases is unclear, although it has become evident that even large, high-profile organizations can be guilty of this and other questionable investigative methods.

Pretexting has gained notoriety in recent months thanks mainly to the highly publicized boardroom scandal that has shaken the Hewlett-Packard Company, one of the largest technology companies in the world. In early September, HP admitted that private investigators working on its behalf used pretexting, among other shady

techniques, to acquire the private phone records of several board members and journalists in an effort to ascertain who was leaking corporate information to the press. As a result, on October 4th HP's former chairwoman, Patricia Dunn, HP's former chief ethics officer and senior counsel, Kevin Hunsaker, and three others were charged with four felonies under California statutes, namely fraudulent wire communications, wrongful use of computer data, identity theft, and conspiracy to commit those three crimes. Given the fallout and investigations currently underway by California's attorney general, the Securities and Exchange Commission and the Federal Bureau of Investigation, many have wondered why HP and others did not know pretexting was illegal. In fact, while pretexting for phone records may be unethical, it is *not* specifically illegal in most of the United States or in Canada. Attempts to clarify the law, however, are underway in both countries.

So far in 2006, 15 states have made pretexting illegal, California being the most recent. At the federal level, The *Prevention of Fraudulent Access to Phone Records Act* proposes to allow the U.S. Federal Trade Commission to seek civil penalties from pretexters. Currently, the FTC can only issue injunctions against pretexters and sue for ill-gotten gains. Alter-

natively, The *Telephone Records and Privacy Protection Act* proposes to make pretexting a criminal offense with a penalty of up to 10 years in prison and a fine of up to \$500,000.

In Canada, there are currently no federal or provincial laws directly addressing the problem of pretexting. Some have suggested that Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), or provincial equivalents, would be sufficient to address such activity. PIPEDA, for example, requires every organization to identify the purpose for collecting personal information, and to ensure that such collection is done fairly and lawfully to avoid misleading or deceiving anybody as to the purpose for collection. Despite the relevance of such language PIPEDA may not be a robust enough law to deal with pretexting, enforced mainly by an ombudsman-like body seeking to influence commercial undertakings through non-binding decisions and peaceful resolution. Accordingly, a private member's bill has recently been presented to Parliament allowing for both civil and criminal penalties against pretexting.

Specifically, Bill C-299, introduced by Alberta Conservative James Rajotte, amends the *Criminal Code* by making it illegal to obtain, or counsel another to obtain, personal information by a

false pretence or by fraud, or to sell or disclose such information obtained by similar means. Also, added to the criminal offence of "personation with intent" is fraudulent personation with intent to obtain any record containing personal information about a third party. Second, the Bill amends the *Canada Evidence Act* to prohibit the admission into evidence of any personal information obtained by fraud, false pretence or fraudulent personation. Last, the Bill amends the *Competition Act*, characterizing businesses that fraudulently obtain personal information as illegal trade practices, and further making the promotion of a product that is provided by means of fraud, false pretence or fraudulent personation a false or misleading representation to the public. The Bill also allows victims to recover damages from corporations in Canada affiliated with corporations outside Canada that have obtained personal information from third parties in Canada by fraud, false pretence or personation.

The substance of Bill C-299 arguably speaks to Canada's perception of pretexting as morally blameworthy and offensive to



Joe L. Lai

public and societal sensibilities, requiring either deterrence or compensation for victims. Greater awareness among the Canadian business community, as well as effective legal remedies, may well reduce future incidents of pretexting, at least among reputable organizations.

Joe L. Lai is an associate in the Business Law Department of Fraser Milner Casgrain LLP and a member of the firm's Technology Practice Group in Toronto, specializing in technology-related transactions and intellectual property matters.

ChildView® (coast to coast)

Canada's Gem

Premier software for child and spousal support calculations!

easy to use, intuitive input screens

spousal support tools included in program; no add-ons required

all-inclusive program; no add-ons required

updates included with license

unlimited, toll-free telephone support included with license

Child Support
Spousal Support
Software

www.childview.ca Toll free: 1-800-787-8620