

INTELLECTUAL PROPERTY

Why businesses need 'clean IP software certificates'

The software industry has matured, and software development nowadays is largely an assembly of components — pieces of code (files) being put together to constitute the final product, much as for hard products. Some software components may be created by product developers, while most of the others are obtained from third party sources: commercial vendors, outsourced developers and, more and more, open source repositories. Software components are easily accessible over the web and sometimes they may appear to be free of cost, but they are not free of licensing or copyright obligations.

Such obligations may end up haunting the hapless company attempting to distribute a software-intensive product without an understanding of the legal implications of doing so. The same is true for a company that acquires a software product without ensuring that it comes with a clean "bill of obligations."

There are sufficiently many legal precedents for people to start asking for a "certificate of software intellectual property (IP) cleanliness" every time there is a commercial transaction involved (see M. Morgan and S. Cohn-Sfetcu's article in *Intellectual Property and Technology Law Journal*, December 2008). The alternative is to impose heavy indemnity coverage and that is expensive as well inefficient in a fast-paced business environment.

So, how does one ascertain that software is free of legal obligations? The usual approach is to go through a process of due diligence. Traditionally,



**MAHSHAD
KOOHGOLI**

**SORIN
COHN-
SFETCU**



this has been done manually, by hiring software and legal experts to check the software and make sure that it meets all necessary obligations, but this is expensive and time consuming.

Fortunately, there are now several commercial software tools to undertake code analysis and attempt to identify its components and determine their pedigrees. This is done by scanning the software, decomposing it into meaningful pieces, and then checking them against large databases of known software code.

The accuracy of the analysis depends on the complexity of the software and the completeness of the available databases. And still, there will be pieces of code that are not fully identified and need to be checked manually. Even worse, if there are any pieces of software that do not have clean IP obligations, the company will have to redevelop them, which is onerous both in terms of development costs as well as delayed time to market.

The best approach is to insist that record keeping and IP management are treated as an integral part of the

software development and quality assurance process. Some companies have done this by attempting to educate their developers in IP matters and imposing certain rules concerning use of third-party software in their products. This may be expensive as it requires constant legal training of software developers (a tough task in its own right), and there still wouldn't be any guarantee that the company rules are fully followed in the development process.

Automatic tools and processes for software IP management can ensure greater efficiency. Such tools and processes cover the spectrum of requirements necessary to deliver a certificate of software IP cleanliness. They include:

- Definition, dissemination and enforcement of an organization software IP policy commensurate with corporate business goals. Such a policy needs to specify what is allowed and what is restricted, what are acceptable external content license attributes, what to do if a piece of code is unknown or has an unacceptable license and what the potential restrictions in distribution due to export controls are;
- Analysis of the enterprise legacy code and the creation of an associated pedigree database;
- A full understanding of the existing software status in relation to the organization's IP policy;
- Real-time gathering of software records for all new source code created or brought into the organization by its developers;
- Preventive analysis of each new software component to ensure that it meets the corporate IP policy;

Alerting the developer that code brought into the project does not meet corporate IP policy, with instructions on what to do in order to alleviate the situation;

■ Completion of a "software bill of materials," which contains information on all components, including their origin, licensing obligations, supplier history, version and all other pertinent information for proper lifetime management.

This software bill of materials is the basis for a certificate of software IP cleanliness, which should be required for any software that changes corporate hands.

Legal counsel should get involved with software managers to help them institute appropriate software IP policies and establish the

necessary processes for ensuring IP compliance, while enabling constructive use and adoption of competitive software components. They should insist that any software acquired by the company comes with a clean IP certificate and enable their clients to provide such certificates to their own customers. ■

Mahshad Koohgoli is CEO of Protecode, Inc., based in Ottawa. He has more than 25 years of experience in the telecommunications industry and specializes in technology start-up businesses. Sorin Cohn-Sfetcu has 30 years of international business and technology experience. He holds several patents in web services, wireless and digital signal processing.

CHART YOUR OWN COURSE.

Power through dispute, investigative and regulatory challenges.

Navigant Consulting Canada.

Turn to us for direction[s].

