

Risks Associated with Using Open Source Software and Need for Internal Open Source Compliance Programs

Law Seminars International:
Current Issues in Complex IP Licensing

Phoenix, Arizona
March 6, 2008

Presenter

Frank X. Curci, Member
Technology, Intellectual Property
and Biotechnology Practice Areas

Jennings, Strouss & Salmon
Promenade Corporate Center
16427 N. Scottsdale Road, Suite 300
Scottsdale, AZ 85254-1597
Tel: 480.663.2179
Email: fcurci@jsslaw.com

PART I

Introduction

Introduction

- Olliance Group's 2004 Report entitled "*Open Source IP and License Compliance: A Survey & Analysis of Industry Best Practices*" makes it clear that:
 - ◆ as adoption of open source software accelerates
 - ◆ the need for corporate developers and other users of open source to proactively manage open source software usage has increased in importance

Introduction

(cont.)

- **Forrester Research Inc's 2007 Report entitled "Topic Overview: Open Source" warns:**
 - ◆ while open source software is continuing to gain acceptance with IT decision-makers throughout North America and Europe
 - ◆ having "**sound open source strategies and policies**" in place within your company is an essential key to successful use of open source software

PART II

First Step Is To Recognize Key Risks Associated
With Using Open Source Software

Key Risks Using Open Source Software

(cont.)

- Federal Financial Institutions Examination Council (FFIEC), which is part of the Office of Thrift Supervision in the US Department of Treasury, issued a report in 2004 entitled "*Risk Management of Free and Open Source Software*" (the "FFIEC Report") (web site link: <http://www.ots.treas.gov/docs/7/77445.html>)
- The FFIEC Report's purpose is to:
 - ◆ "raise awareness . . . of risks and risk management practices applicable to the use of free and open source software"

Key Risks Using Open Source Software

(cont.)

- **The FFIEC Report's identifies three key "risks" that could result from the use of open source software:**
 - ◆ Strategic Risks
 - ◆ Operational Risks
 - ◆ Legal Risks
- **The FFIEC Report's Strategic Risks include:**
 - ◆ Ability to Customize Risk:
 - need to consider your company's internal technical ability to modify and maintain the code for your customized purposes

Key Risks Using Open Source Software

(cont.)

- ◆ Compatibility & Interoperability Risk:
 - proprietary software products from industry -recognized vendors are typically more compatible/interoperable
 - the compatibility and interoperability of open source software with other software products:
 - may be unknown
 - not yet certified to be compatible / interoperable
- ◆ Maturity Risk:
 - mature proprietary software products usually present fewer risks
 - newer open source software:
 - may be less mature
 - unknown security record
 - less overall support

Key Risks Using Open Source Software

(cont.)

- ◆ Forking Risk:
 - “fork” could occur in the open source development community over the future path of the open source software resulting in:
 - halt to further development
 - a technical direction that no longer meets your company’s needs
- ◆ Systems Integration & Support Risk:
 - must evaluate ability to effectively integrate the open source software application into your company’s larger overall systems
 - can you do this internally?
 - are there third parties that can provide this support?

Key Risks Using Open Source Software

(cont.)

- ◆ Total Cost of Ownership Risk:
 - many assume use of open source software is cost-effective
 - However, indirect costs of use of open source software may be higher than associated with proprietary software:
 - more training costs?
 - outside vendor costs could be higher?

Key Risks Using Open Source Software

(cont.)

- **The FFIEC Report's Operational Risks include:**
 - ◆ **Code Integrity Risk:**
 - need to develop internal standards to:
 - make sure you are acquiring the software "from a trustworthy party"
 - "verify the integrity of the code" received from that source
 - ◆ **Documentation Risk:**
 - documentation that accompanies open source software may be "less comprehensive" than documentation accompanying proprietary software because of the diversity of the open source development community

Key Risks Using Open Source Software

(cont.)

- ◆ Contingency Planning Risk:
 - continued viability of the open source software is “largely dependent” on the applicable open source software community developing that code
 - if that development community goes away, you may end up with “dead-end software”
- ◆ External Support Risk:
 - While external support for such open source software as the LINUX operating system is becoming more robust
 - You must always evaluate the availability of independent vendors that can provide needed support and maintenance.

Key Risks Using Open Source Software

(cont.)

■ The FFIEC Report's Legal Risks include:

- ◆ Must identify and consider the legal risks associated with the use of open source prior to deployment or development
- ◆ Licensing Risk:
 - Understand the full legal consequences of the open source software license
 - Certain OS licenses state that:
 - any release or distribution
 - of modified software/derivative of the OS software
 - must be accompanied by an offer to provide the source code of your code
 - You can easily be bound to an OS license:
 - many OS licenses are NOT “traditional written contracts”
 - instead, the mere downloading or mere use of the OS software could bind you to the OS license

Key Risks Using Open Source Software

(cont.)

- ◆ Infringement Risk:
 - potential for an infringement lawsuit arguably more likely with use of open source because, unlike proprietary software, open source is developed in an open environment where code is shared and modified by numerous unaffiliated parties
 - this code sharing increases the possibility that proprietary code that is not subject to the OS license is inadvertently inserted into the open source at some point during the development process.
- ◆ Warranties/Indemnification Risk
 - proprietary software licenses customarily include an IP warranty and indemnity from the owner
 - open source software is typically “AS IS” without any IP warranty or indemnity

PART III

These Legal and Other Risks Could Negatively Impact a Company's Intellectual Property Rights and the Company's Overall Valuation

Negative Impact on IP Rights and Company Valuation

- **Increasing Legal Concern that by improperly using open source software, your company could**
 - ◆ end up with Copyleft / Viral consequences
 - ◆ which generally means:
 - if you modify OS software that's subject to an OS license (ie: GPL)
 - then release/distribute it within your proprietary product
 - you maximize the potential that the OS license applies to your distributed product
 - and then you could be obligated, under the OS license, to offer to third parties:
 - access to your original source code
 - access to derivatives you made to the OS code
 - all royalty free

Negative Impact on IP Rights and Company Valuation

(cont.)

- This key legal concern, along with many of the other risks, has increased the concern of Investors (i.e.: Venture Capitalist), M&A Acquirers, Auditors/Accountants and Wall Street (in general) that use of open source could inadvertently
 - ◆ impair a company's ability to effectively enforce its IP rights
 - ◆ impair a company's ability to derive meaningful royalties or other revenue from third party use of its IP Rights
 - ◆ all of which can negatively impair the overall valuation of the company
- Investors/M&A Acquirers will expect you to demonstrate that you:
 - ◆ have performed a legal review of open source licenses
 - ◆ have tracked licenses and changes to them through automated or manual means
 - ◆ understand the legal consequences of combining open source and proprietary software
 - ◆ otherwise the valuation of your company may be reduced in a merger/acquisition.

Negative Impact on IP Rights and Company Valuation

(cont.)

■ SEC Reporting:

- ◆ Growing number of companies have statements like the following to dispel concerns they are suing OS:
 - “None of the software in [_____] products, in whole or in part, is subject to the provisions of any public software or other source code license agreement that requires the distribution of source code in connection with the distribution of or otherwise making available such software . . .”
 - “The [_____] software does not contain and have not at any time contained any open source code or materials, nor have any of the [_____] products been derived from any open source code or materials.”

Negative Impact on IP Rights and Company Valuation

(cont.)

- **Auditors' Warning:**
 - ◆ Auditors (such as PWC, KPMG, E&Y) have started to insert warnings about the risk of a company's use of open source software:
 - proprietary risk to company's product lines
 - even risk to company's overall valuation.

PART IV

Open Source Compliance Programs and Audits

Internal Open Source Policies

- **Code Audits Becoming Common:**
 - ◆ Merger and Acquisitions
 - your company acquires code from target software company
 - ◆ Investors
 - before VC will invest money into your company
 - ◆ Internal compliance programs
 - periodic due diligence of work of your internal developers
 - ◆ Often use one of many publicly available audit programs that look for code belonging to other parties

Internal Open Source Policies

(cont.)

- **Company compliance programs seek to address various sources of OS software:**
 - ◆ OS coming from actions of people/sources known to company
 - internal developers
 - your vendors/suppliers
 - your licensees
 - ◆ OS coming from unknown sources
 - internal developers use of unknown third party OS
- **Internal Developers/Employees**
 - ◆ Your company's developers could use open source software and not fully understand the consequences
 - ◆ Key concern is your internal developers get code from external sources they don't know much about:
 - when developers create software they often do not develop from scratch

Internal Open Source Policies

(cont.)

- rather, developers increasingly gather up different existing applications including open source applications
- this ease of access to third party material can easily create open source issues
- ◆ Thus, Companies increasingly have OS compliance programs for internal company use of OS:
 - Manager approval for use
 - Legal department approval for use
 - Periodic audits of code using one of the many publicly available audit programs

Internal Open Source Policies

(cont.)

- **Vendors/Suppliers**
 - ◆ Stronger representations and warranties from your vendors/suppliers concerning their use of any OS
 - ◆ Periodic audits of code using one of the many publicly available audit programs
- **Licensees of your code:**
 - ◆ Stronger provisions restricting their later use of OS that might implicate your proprietary code
 - ◆ Indemnifications

Frank X. Curci, Esq.



If you would like more information or assistance, please contact Frank X. Curci at 480.663.2179 or email him at fcurci@jsslaw.com

Admitted to practice in Arizona, New York and Oregon.

Frank X. Curci is a Member (Partner) in the Technology & Intellectual Property Practice Groups of Jennings, Strouss & Salmon and practices in the firm's Scottsdale office. He represents clients in domestic and international intellectual property and technology matters, including patent, software and other technology licensing, open source software issues, technology standards, research collaborations, other collaborative technology arrangements, technology transfer matters, and the overall use and protection of their intellectual property. Frank advises clients in many technology sectors, including biotechnology, life sciences, medical device, semiconductor, software, and other technology companies, and universities/research institutes. He counsels universities/research institutes and private sector technology companies concerning research collaborations, sponsored research, material transfers, licenses, and other technology transfer matters. He also represents technology companies and other entities in their participation in technology standards setting organizations and other multi-party technology collaborations and consortia . Since 1996 Frank has been an Adjunct Professor of Law teaching intellectual property courses at California, Oregon and Arizona law schools. Admitted to practice in Arizona, New York and Oregon.

This information is intended for general information purposes only and not as specific legal advice. You are urged to consult an attorney concerning your situation and any specific legal questions you may have.

© 2008 Frank X. Curci and Jennings, Strouss & Salmon. All Rights Reserved.