



Open Source Risk Management, Inc.  
2530 Meridian Parkway  
Third Floor  
Durham, NC 27713

## Open Source Software IP Risk Audits: The Emerging Due Diligence Standard for Technology M&A Transactions

By Daniel Egger, CEO, Open Source Risk Management, Inc.  
and Matthew Hogg, Underwriter, Kiln plc

An abridged version of this article was first published by  
Financier Worldwide, Issue 44, August 2006.

Open Source now provides much of the essential infrastructure of the world's global IT economy. At least 75% of global companies use Open Source, and few software companies could distribute their latest products without incorporating or relying upon at least some Open Source third-party components.

Open Source software is ubiquitous. Free and Open Source includes the Linux operating system that runs most of the world's business applications; the Apache web server that supports more than 50% of the world's web sites; the Firefox Web Browser used more than 100 million people; and the Open Office productivity suite that competes directly against Microsoft office and offers comparable functionality at no charge. Many of the most popular electronic devices contain and run on embedded Open Source software, including for example most new mobile phones from Motorola, Cisco Routers, Tivo and Lodgenet set-top boxes, and more than 20 Sony products.

It is difficult to build commercially competitive software today that does not contain or rely on Open Source at least in some areas. The C libraries, Java, the Perl and PHP scripting languages, and the MySQL and Postgres databases, among the most important building blocks that software engineers use and combine to create new computer applications and systems, are all partially or completely Open Source.

The first Open Source license, the GNU General Public License (GPL), was developed to prevent vendors capturing Open Source software and promoting proprietary versions of that same technology. Called "Copyleft," the GPL works as follows: the authors of Copyleft software retain all copyrights, but grant limited, revocable permission to use and distribute their software to those who comply with the license. Violation of the license results in

automatic revocation, requiring the infringer to cease use immediately. The GPL extends its Copyleft requirement to any later derivative works of the original. Copyleft places on those who distribute a derivative work the requirement that they will provide the source code to the derivative work to all downstream users under the same provisions through which they received the original work.

Copyleft is a powerful force for cooperation, but holds significant dangers for companies that are not careful to isolate their own proprietary intellectual property from the Copyleft code. Unwary developers have found that their own technology, combined with or relying upon slightly modified Copyleft code, is “claimed” by one or more Open Source copyright holders as a derivative work that must be made freely available. Understandable hesitancy to “open source” proprietary code under pressure from Open Source developers has led to more than 60 disputes in the last three years.

Copyleft disputes generally lead to one of the following outcomes:

- Release of the proprietary source code under a Copyleft Open Source license;
- Re-engineering of the product to eliminate the Open Source code or change the way it is accessed so that the proprietary code is no longer considered a derivative work of the Open Source; or
- The plaintiffs obtain an injunction or settlement forcing removal of the combined work from the market altogether, preventing its use or sale.

Obviously, if a company is forced to make its product available in source code form without restrictions on further redistribution it can largely destroy the commercial value of that product.

One of the most well-known examples of the financial impacts of Copyleft enforcement actions comes from Cisco and Linksys. Cisco acquired Linksys, a network equipment manufacturer, for approximately \$500 million. After the acquisition was complete, the Free Software Foundation ([www.fsf.org](http://www.fsf.org)) determined that a Linksys toolkit contained FSF-copyrighted code licensed under the GPL. FSF contacted Cisco, and Cisco determined that it would be cost prohibitive to reengineer the product to replace all Open Source code. Cisco therefore released the toolkit’s source code under the GPL. As a result, software that Cisco considered to be proprietary at the time it acquired Linksys became freely available at no cost.

It is interesting to consider the “chain of commerce” through which the GPL-licensed code ended up in the Cisco’s product. Linksys routers relied upon programmable chips supplied by Broadcom. Broadcom outsourced development of some of its chip programming tools to an overseas contractor, which provided the FSF software to Broadcom without proper acknowledgment. Neither Broadcom, nor Linksys, nor Cisco was a knowing infringer of the FSF Copyrights. The overseas contractor may also have been acting in good faith. Nevertheless, Cisco faced a stark – and expensive – choice: the programming toolkit product needed to be pulled from the market or the source code for it released without charge.

Note that through use of automated code-scanning systems designed to detect Open Source, such as OSRM's Silhouette™ Scanning technology, the Copyleft code in the Linksys product could have been identified easily at any step in the value chain through a simple audit process: by Broadcom when it purchased the code, by Linksys when it accepted the Broadcom tools, or by Cisco when it acquired Linksys.

The Cisco-Linksys settlement demonstrated to M&A professionals the potential financial impact of Open Source license violations. Sophisticated buyers of technology companies now routinely evaluate Open Source compliance risk in every piece of software they buy. The cost of such an audit is perhaps 1/1,000 the cost of a forced interruption in selling the product in future.

A second example of the financial impacts of Open Source enforcement comes from Fortinet, a UK-based maker of firewall software and devices used to provide security against intrusion for web sites and internal corporate networks. Fortinet devices run on the Copyleft Linux operating system. Fortinet developers allegedly made modifications and additions to Linux as part of its firewall offering, but failed to make the source code for this derivative work available without charge. GPL-violations.org ([www.gpl-violations.org](http://www.gpl-violations.org)), a non-profit organization charged with enforcing Copyleft in Europe, successfully sued in German courts and obtained a temporary injunction barring all sales of the disputed product in Germany. Fortinet settled the case by releasing source code to that product without charge under the GPL. The Fortinet case demonstrated that German courts will support aggressive enforcement of the GPL, and as a result no product can be safely marketed in Europe if it is likely to face challenge as a potential derivative work of Open Source code licensed under the GPL.

Acquirers need to ask not *whether* there is Open Source in the technologies they are acquiring – there almost certainly is, and a blanket refusal to accept Open Source is self-defeating – but *how* that Open Source is used by the proprietary code in the product. Some forms of use are almost certainly “derivative use” while others are clearly not. Buyers should routinely assess the business risk of one or more Open Source copyright holders bringing a future compliance action, the risk that such an action would prevail, the portion of the product's value as a proprietary offering that would be lost, and the possibility and cost of re-engineering the product at that future time to eliminate the issue and provide customers with a non-infringing substitute.

All of the above can be accomplished through a detailed Open Source audit in which automated source code scanning tools such as OSRM's Silhouette™ are combined with expert engineering and risk analysis to produce a risk profile of the target acquisition that identifies likely risk scenarios, outcomes, and corrective actions. The acquirer can then make an informed decision as to the risk that they may acquire, the necessity (or lack thereof) for remediation, and the potential financial impact of both.

Given the near total lack of case law on the meaning of “software derivative work,” the courts will be facing a large number of cases over the next five to ten years, and tens, or hundreds of millions of dollars will turn on their determination as to whether Copyleft licenses apply.

Insurance becomes appropriate when a commercial software product mixes Open Source and proprietary code in a manner not addressed by previous case law. Insurance addresses

the financial risk that new rules will emerge that define a fact-pattern as impermissible. By hedging away this risk now, and pricing in the cost of the business interruption insurance geared specifically to this contingency, commercial software developers can use Open Source freely – except in situations that would clearly constitute a violation under current case law – and make business, marketing, and capital investment decisions exactly as if they had no Open Source risk whatsoever.

Kiln, a leading managing agent at Lloyd’s of London, and OSRM have developed an insurance policy specifically for the business interruption risks associated with acquiring software assets or entire software companies. This insurance is what is called “first-party” coverage; it offers a business that in the future needs to withdraw a product from the market, re-engineer it, or release some or all of its source code in response to new legal rulings compensation for the resulting loss in revenues or loss in profits. This insurance is particularly valuable in facilitating M&A transactions, where a buyer may otherwise get cold feet upon discovering potential future problems with a product it is acquiring. With the ability to hedge away this risk at reasonable cost, inadvertent use of Open Source, when identified in a risk-audit, need not and should not lead to forced abandonment of the deal.

Open Source risk is not to be feared, but to be managed. With these facts in mind, wise sellers should consider performing their own Open Source risk-audit – and obtaining a multi-year term insurance policy where appropriate – before they put their assets up for sale. Likewise, as the saying goes, buyers beware.

## **About the Authors**

Matthew R. Hogg is an underwriter at Kiln, a managing agency at Lloyd’s of London. As part of the Risk Solutions team, he is Kiln’s specialist in the field of Intellectual Property insurance and first-party cover.

Voice: +44 (2078) 869 000  
e-Mail: [Matthew.hogg@kilnplc.com](mailto:Matthew.hogg@kilnplc.com)  
Website: [www.kiln.co.uk](http://www.kiln.co.uk)

Founder and CEO of Open Source Risk Management, Daniel Egger is a serial entrepreneur and lawyer and is well-versed in both the engineering and legal aspects surrounding open source use.

Voice: 919-680-4511  
e-Mail: [degger@osriskmanagement.com](mailto:degger@osriskmanagement.com)  
Website: [www.osriskmanagement.com](http://www.osriskmanagement.com)