Open Source Legal Risk Management in the Enterprise, Version 1.2

OPTAROS WHITE PAPER

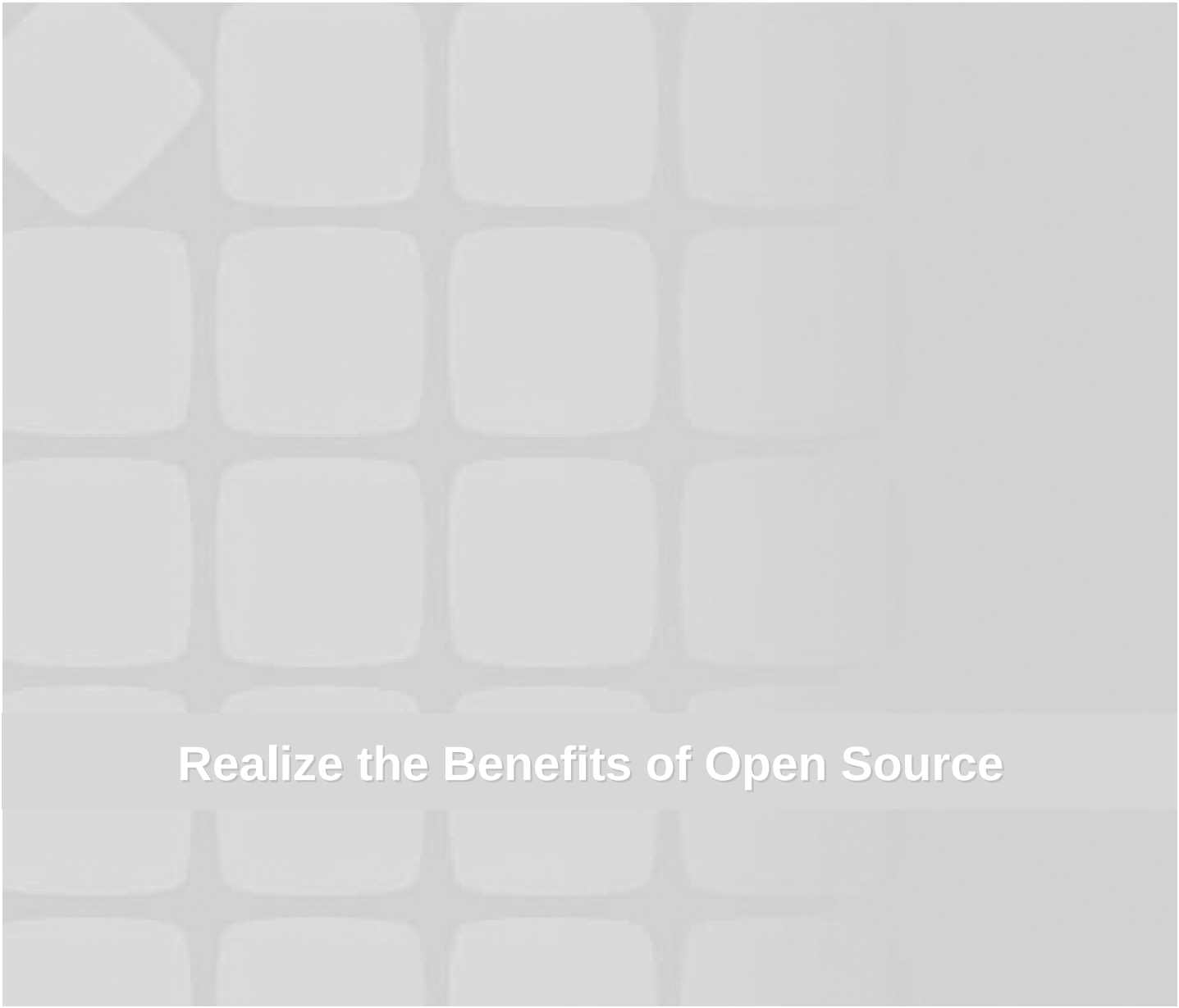

Table of Contents

Introduction

There is sometimes confusion about how legally risky using free and open source software (FOSS) can be in the enterprise. These concerns center around:

- the SCO Group vs. IBM lawsuit,
- issues of FOSS license management and compliance,
- concerns around patent infringement and litigation, and
- insurance and indemnification.

Each of these issues has received wide media coverage. Each of these issues appears reasonable at first glance, and no enterprise executive would dismiss these concerns. The reality, however, is somewhat tied to the positions of vendors with vested interests to defend and the perception of risk to the enterprise can be overcome with knowledge.

In this paper, we will look at each these issues and dispel the fear, uncertainty, and doubt surrounding them.

SCO Group vs. IBM

SCO Group vs. IBM is a lawsuit about copyright misappropriation between two vendors. SCO Group claims IBM used SCO Group property in its contributions to the Linux operating system. SCO Group needs to establish that its property has been used and establish that it couldn't be used through the contracts in place at the time between the companies. The Canopy Group, the parent company of SCO Group when the lawsuit began, has litigated against vendors in the past. [1,2]

SCO Group sent letters to a very large number of Linux customers threatening to sue them, then attempted to sue Autozone and Daimler-Chrysler (March 2004).[3] They were attempting to put pressure on IBM to settle. So far the tactic has failed.

In a more general discussion around open source and legal risk to the enterprise, an enterprise should evaluate the risk in relation to risks around other software contract areas:

- A company stands a larger risk of being sued over license counting issues from a commercial software vendor than they do over intellectual property issues associated with open source.

1 “CA Announces Settlement of Canopy Group/Center 7 Litigation,” (Computer Associates International, Inc., 2003), Press release.
2 “Devicelogics Signs New OEM Agreements,” (DRDOS, Inc., 2003), Press release.
3 Stephen Shankland. “SCO suits target two big Linux users,” *C|Net News.com*, (3 March, 2004), http://news.com.com/SCO+suits+target+two+big+Linux+users/2100-1014_3-5168921.html, (accessed 12 May, 2006).

License management and counting users and systems is a notoriously difficult space. There is no good way to manage user license counting across diverse vendors and products. Vendors regularly litigate in these spaces and some wield the Business Software Alliance (BSA)[4] and call for audits.[5] Open source licensing reduces this type of risk.

- The only known lawsuit to date is the SCO vs. IBM suit. It is not considered to be seminal — but rather, is an aberration based on one company's actions. In a multi-billion dollar marketplace, Linux has been in active deployment for ten years, MySQL for five years, and Apache for fifteen years. This is the only known lawsuit in which a customer was threatened with legal action.
- In a very few other cases, the inappropriate use of software licensed under the GNU General Public License (GPL) has been an issue between two vendors or between the vendor and the project. In every case, the vendor has respected the license, and either published their modifications or modified the project code to stop the inappropriate use of the software covered by the GPL. There have been no major law suits or major damages awarded.

License Management and Compliance

From a software development perspective, there is concern of late over whether or not software development efforts have been somehow "tainted" with "viral" code and therefore would need to be published at large — and concern over what sort of software development tools and practices need to be put in place to prevent such risk. Ideas around free and open source license compliance tracking have been raised. Again, one needs to consider the risks in context.

- While developers may not be copyright lawyers, most understand that copying code without checking the associated license can lead to consequences affecting the company's ability to ship its product. This concern does not apply only to free and open source software. It also applies to code samples found in books and developer network portals (e.g. MSDN with its once confusing array of copyright statements), as well as to third party licensed software (e.g. C++ library and framework source code from companies like Oracle and RogueWave).
- The requirement that software source code be published and licensed under an open source license such as the GPL (or the software withdrawn) is triggered on distribution of the software. This is very relevant to a software development company, but not to an enterprise that is deploying the software internally. Licenses such as the Apache license or BSD license do not require publication or re-licensing of the software source code at all. Even software development companies have demonstrated that they can ship products based on free and open source licenses such as the GPL without "risking their businesses," gaining very different benefits that outweigh the risks of publishing the source code.
- Source code scanning tools are only as good as their fingerprint databases and the software engineering process in which they are used. The fingerprint databases will always be incomplete with respect to all the non-open source software to which a development team may be exposed, as well as some open source projects that may not be covered. Such tool sets may not be effective depending upon the rigor of the software development process. Relying on a tool

4 David Becker. "Newsmaker: Rockin' on without Microsoft," *C|Net News.com*, (20 August, 2003), http://news.com.com/2008-1082_3-5065859.html?tag=lh, (accessed 12 May, 2006).
5 "Houston firms settle software piracy claims with BSA." *Houston Business Journal,* (27 November, 2001), http://www.bizjournals.com/houston/stories/2001/11/26/daily16.html, (accessed 12 May, 2006).

rather than developer education may lead to missed problems and a false sense of security. Invest in better software development tools for testing, debugging, and release and configuration management to improve software quality and reduce software maintenance costs before detecting code taint from specific open source projects. The risks don't merit the expense in context. Remember that such scanning tools will never cover all the other potential sources of third party code taint. Understand that no scanning tool can detect patent infringement.

Patents and Property

There is much discussion about FOSS and intellectual property (IP) and the patent infringement risk inherent in large enterprises using FOSS. The rhetoric follows the logic:

- FOSS developers may be trespassing on all sorts of patents
- FOSS developers obviously (sic) don't care about intellectual property
- Customers using FOSS therefore run the risk of patent infringement suits

This logic is inaccurate for two very fundamental reasons. First, developers may be infringing on the claims of other people's patents every day. This risk does not specifically pertain to open source development methods or licensing. It is a fact of software development and the way software patents are developed. Second, patents are a vendor-to-vendor discussion. Vendors typically don't sue customers over broadly applicable issues like patent infringement, because it would send the wrong signal to their other customers. Let's look at both these issues more closely.

Intellectual property is distinct from the asset it protects, so it is important to establish a few definitions. Intellectual property (IP) law refers to a set of legal tools that one uses to protect an asset. IP law typically covers the ground of trade secret (how one legally protects an idea as a secret), patent (how one publishes an idea in a legally protected way so others cannot build it for a period of time), copyright (how one controls the use of the "written" representation), and trademark (protecting the way one identifies the asset). Companies develop assets that are packaged into products for sale to customers. These assets may be real works of invention and innovation, or merely represent some subjectively "better" level of business execution, packaging, and service to the customer. Not every idea, process, and asset a company develops is necessarily "property" in a legal sense.[6]

The lag between application and issue of the patent in the U.S. is now approximately 36 months.[7] This means it is quite possible to ship a product and not know for quite some time whether or not it has infringed on the claims of someone else's patents. As a product becomes successful, it becomes visible and a potential target for litigation. The patent holder may want a percentage of the proceeds, or if the patent holder is a competitor, they simply may want to prevent the "making" and "distributing" of wares. Software products

[6] Some vendors are very advanced in their IP strategy. It is not simply the case where "more patents faster" is a rule. A patent can be costly considering patent attorney fees and the defense of the patent over its life. So one might want to choose how to apply patent protection to selected assets that make up a product for sale. Indeed one might choose to aggressively publish some ideas to ensure no one else patents in that space. In the end, patents are business decisions and not technical issues. The top ten list of patent award winners was published for 2004 from the U.S. Patent and Trademark Office (USPTO). IBM tops the list with more than 3,000 patents. At an estimated US$15,000.00 per patent for the application and legal fees, this means that IBM spent more than US$45,000,000.00 just obtaining the patents. IBM also recently "released" 500 patents for open source use. This is a good example of patent protection being a business decision.

[7] "Innovation and its enemies," *The Economist*, (12 January, 2006).

certainly fall into this window of risk with the speed that concept to shipping a product happens in the computing industry.

No developer can actually be aware of software patent infringement. There are seldom published warnings about pending patents. With patents written in legal language and targeted as broadly as possible, it would be almost impossible for a developer to track all of the patents relevant to their work. And of course the lag problem still exists, meaning even if the developer had the time and training to review patents in their area of expertise, they cannot know whether or not their work infringes someone's patent claims in any meaningful time frame. And if it looks like a developer may have attempted to study the problem, and perhaps misread or misinterpreted a patent's broad claims, then they may be construed as having “willfully” infringed a patent's claims by the court and that brings additional financial damages in the U.S.

The more important thing to realize is that vendors typically don’t sue customers over IP issues. IP is a vendor-to-vendor discussion. While technically a vendor could sue anyone that infringes their property, including a customer using another vendor’s product that infringes, it makes no sense for that first vendor to do so.

Once a vendor sues a customer, they have essentially told that customer they never want that customer's business again. That might even be appropriate in a narrow situation where there exists some sort of explicit dispute between exactly the two parties (such as the aforementioned license counting issues). If however the dispute is over something like “patent infringement” that can easily be applied broadly to many customers, then all the vendor's other customers are put on notice that this vendor does not care about the relationship and continued business. New potential customers can see that this is a vendor that may attach law suits to the relationship, and will quickly factor that into the risk analysis on the potential purchase from the vendor. The litigious vendor's top salespeople will discover their phone calls stop getting returned.

The vendor whose product is claimed to be infringing will likely step into the path of the law suit. They don’t want their customer to take the fall for their product and property. They don’t want the customer relationship poisoned. They don’t want a customer to be the first legal line of defense for their product and property.

Intellectual property is important. Cross licenses, patent pools, and simple licenses exist and are business as usual – but between vendors. This is why Eolas Technologies sued Microsoft over their web browser patent and not any of the large corporations that were using Internet Explorer. Similarly, NTP Inc. sued Research In Motion directly over the patents infringed by RIM’s Blackberry devices, rather than any large customers. Between vendors, “Litigation is just another means of discussion.”[8]

Indemnification and Insurance

This leads to the discussion of vendor indemnifications and insurance. As an illustrative example, in the fall 2004, Microsoft made a very public promise of indemnification to Microsoft customers for patent infringement cases against their products to try and differentiate their commercial offering from a generic "open source" threat.”[9] This follows in the wake of the fall, 2003 Novell[10] and HP[11] indemnifications against various IP

8 David McGowan. "SCO What? Rhetoric, Law, and the Future of F/OSS Production" (June 7, 2004). Minnesota Legal Studies Research Paper No. 04-9. Available at SSRN: http://ssrn.com/abstract=555851 or DOI: 10.2139/ssrn.555851

9 Steve Ballmer. "Customer Focus: Comparing Windows with Linux and UNIX," (Microsoft Corporation, 2004), http://www.microsoft.com/mscorp/execmail/2004/10-27platformvalue.asp (accessed 12 May, 2006)

10 “Novell Linux Indemnification Program,” (Novell, Inc.), http://www.novell.com/licensing/indemnity/register/index.html (accessed 12 May, 2006)

11 “HP First Major Vendor to Indemnify Linux Customers,” (Hewlett-Packard Development Company, L.P., 2003), Press release.

infringement suits against Linux if users purchased the systems from them. The Novell and HP statements were in reaction to the SCO Group suit against IBM. IBM loudly did not offer an indemnification around Linux, saying it wasn't necessary.[12]

The vendor promise of indemnification to customers is a legal statement of business reality and is usually redundant to any vendor worth its customers. As was pointed out in the previous section, no vendor wants to be in the situation where customers are being sued with respect to the vendor's property. While in some cases a customer may even have more money than the vendor as a legal target, one can bet that the mainstream vendors will be more than interested in running their own defense case. A vendor would likely want to be named co-defendant, and the primary defense for their own legal property.

In 2005, the idea was suggested that companies could buy insurance to protect against IP lawsuits. The idea that as an enterprise one might want to buy insurance against such risk is interesting. One insures assets, not liabilities. Life and health insurance relates to earning power for the household. As the insured's salary goes up over time, the level of insurance might be increased. Likewise, as the value of a car depreciates over time, the insurance buyer may reduce the replacement value coverage on that asset. All insurance is based on reasonable risk analysis and purchased at rates carefully calculated by the insurance companies based on risk profiles.

Considering that the only known lawsuit to date has been brought forward by the SCO Group, the cost/benefit analysis of obtaining such insurance would be very thin. Until such time as there exists real data in the industry of vendors suing customers over IP (and winning), the cost of such insurance should be considered against all the other investments in your IT infrastructure that could be made for the same amount of money.

Summary

So as FOSS continues to deploy and grow in enterprises, companies will need to consider the source of the technology they use and their vendor relationships, which is no different than any other technology shift in past decades. Concerns over the SCO Group versus IBM lawsuit, FOSS license compliance, patent litigation, indemnification and insurance need to be put in context and considered in terms of the sources of such information.

Free and open source software has been in active deployment in the enterprise and across the Internet for more than twenty years (Sendmail, BIND, Apache, Linux, FreeBSD, MySQL) and there have been no known, valid customer facing lawsuits. Vendor to vendor discussions, negotiations, and litigation may arise from time to time, as they have in the past, but will have little significant impact on the marketplace. In such cases, David McGowan may have said it best:

"If the F/OSS community wants to be in commercial space, community members will have to learn to deal calmly with IP litigation. The F/OSS production model will work where it makes sense, and it will not work where it doesn't. It's really just that simple. Particular claims in individual suits—even one against a flagship program such as the GNU/Linux OS—will not determine the fate of the community. Such cases present factual issues that will get resolved one way or another; they do not represent a crisis for F/OSS production as a whole. Norm entrepreneurial rhetoric that plays off such cases should be treated as entertainment. Enjoy it if you like it, take inspiration from it if you must, but don't confuse it with the way things actually get done."

12 Todd Weiss. "LinuxWorld: A defiant IBM says Linux indemnification is unnecessary," *ComputerWorld*, (21, January, 2004), http://www.computerworld.com/softwaretopics/os/linux/story/0,10801,89269,00.html, (accessed 12, May, 2006)

About the Author Stephen Walli

Stephen Walli is Vice President Open Source Development Strategy at Optaros. Mr. Walli was an advocate for open source at Microsoft, where he was focused on "shared source" business strategies and was responsible for technical implementation of open source-related community projects. Stephen was a long time participant and officer at the IEEE and ISO POSIX standards groups, representing both USENIX and EurOpen (E.U.U.G.) and has been a regular speaker and writer on open systems standards since 1991.

About Optaros

Optaros is an international consulting and systems integration firm that provides enterprises with best-fit solutions to IT business challenges, maximizing the benefits of open source software. Whether your organization has had little exposure to open source software or has open source-based solutions currently in place, Optaros has the business and IT problem solving experience to advise on the areas where open source and open standards can be effective and how to proactively manage the use and benefits of open source software.

Optaros offers a third alternative to the "build versus buy" decision with our proven assembly methodology (OptAM). Within our core practice areas, Optaros ensures successful solution delivery by leveraging our pre-selected open source solution sets and customizing to your specific business requirements.

Contact Optaros

- United States: Brian Otis, Vice President of Sales and Business Development
  email: botis@optaros.com
  phone: (617) 227-1855 x110
- Geneva, Switzerland: Kay Flieger
  email: kflieger@optaros.com
  phone: (617) 227-1855 x225
- Zurich, Switzerland: Heinz Rudin
  email: hrudin@optaros.com
  phone: (617) 227-1855 x224

Disclaimer:

Optaros makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.