January 31, 2005

PALAMiDA

Best Practices of Securing Your Software Intellectual Property Integrity

Palamida, Inc.
612 Howard Street, Suite 100
San Francisco, CA 94105
info@palamida.com
415-777-9400
www.palamida.com

Intellectual Property Integrity

Introduction

Never before have Best Practices for managing and monitoring intellectual property (IP) licenses for software been more critical. IP licensing woes have ensnared companies as disparate as IBM, AutoZone, Cisco, DaimlerChrysler, MySQL, Progress Software and Compuware.

SCO's $5 billion IP software infringement suit against IBM represents the most stunning legal case, but even the smaller MySQL vs. Progress Software lawsuit cost Progress more than $10 million in legal fees, code redevelopment and product delays.

These legal cases reflect a major change in how software is created: Today most software is assembled from pre-existing components, not written from scratch. Third-party components provide tremendous benefits, but they carry significant risks. For most companies, the burgeoning use of third-party components has overwhelmed homegrown, manual systems and business processes for monitoring external components and their licenses.

This rapid shift has left many CEOs, legal counsel and IT managers flying blind about the status of IP licenses in their applications. Legal oversight is playing catch-up to this revolution in software development—just as new legal requirements such as Sarbanes-Oxley require corporate officers to certify that controls are in place to prevent fraud.

Three irreversible trends in IP licensing have turned up the heat on both legal and technology executives:

1. Software components (both open source and commercial) are easily downloaded over high-speed Internet connections. A recent Gartner Group study found that 70% of all new applications contain a mix of homegrown and external software components. Why? Tested, proven components boost reliability, add functionality and significantly cut time to market and development costs.
2. The open source software movement has vastly increased the availability of components. Thousands of new open source components are released every week, and developers use them. Troublingly, a recent Evans Data Corp. survey revealed that more than 60% of enterprise-class developers are using open source components today—with or without their managers' knowledge.

3. The huge growth in outsourced and offshore development requires extra care in validating IP code status. Contract and offshore developers work cheaper, but companies exercise less control over them. More than 300 of the Fortune 500 do business with Indian IT services companies, according to a 2004 Gartner study. Out-law.com, an IT legal resource, found that almost 70% of responding software developers keeps a personal collection of software components that they reuse on different employers' applications without the legal owner's knowledge or permission.

The growing use of software components, the natural result of these three trends, raises the risk of IP license infringement. Every software component, open source or commercial,

comes with a software license that has unique terms and conditions that can significantly influence a product's value, price and distribution.

Discovery

The legal implications of this new style of software development influence both independent software vendors (ISVs) and in-house developers creating proprietary applications. Consider these real-world situations that demonstrate how IP licensing issues touch companies today:

- **Prove you're Clean:** A small ISV is trying to sell its software to a Fortune 500 company. Because of the perceived risk of buying third-party software, the potential buyer demands an audit for possible license violations before signing the contract. Manual code review takes time and often proves unreliable. The small ISV cannot afford to prolong the sales process. Palamida provides the fastest and most reliable solution to validate "clean" code.

- **Hold that Acquisition:** A large networking company is negotiating to acquire another firm. The buyer's intellectual property attorney called Palamida for an IP audit of the seller's source code before closing the deal.

- **Kill that Litigation:** A large software company is being sued by a smaller firm that claims its code was poached illegally by the bigger business. The defendant's legal counsel has called on Palamida as forensics tool to prove its innocence.

- **Slow that Roll-out**: A major corporation is rolling out a new internal application to 10,000 desktops. Hours before release, the company discovers that the new application includes a commercial component that is free for evaluation but requires a stiff licensing fee upon redistribution. The company now uses Palamida to avoid similar problems in the future.

- **Get Socked by SOX:** New mandates in the Sarbanes-Oxley Act require companies to attest that they have controls in place to prevent fraud, potentially including claims about component licenses in their software. Palamida's solutions give managers the confidence to certify IP integrity.

How To Guarantee Trouble
1. Assume someone has already addressed the problem.
2. Accept assurances of vendors, employees and contractors without checking.
3. Ignore IP license issues in an acquisition.
4. Don't involve Legal. Keep IP license issues within the software group.
5. Let Legal handle IP licenses later.
6. Audit IP licenses only once a year.

Best Practices

Widespread component-based development is relatively new, but Best Practices are beginning to emerge. Specific steps to control IP license issues can be grouped into three phases: Get Set, Get Clean and Stay Clean.

In the Get Set phase, companies create a baseline to describe their status today in managing IP licenses. This first phase has two steps:

1. The corporate legal and software development organizations jointly review the existing IP license policy or work together to create a new one.
2. Simultaneously, the company audits its existing code base for all applications to answer the question, "What do we have today?"

In the second or Get Clean phase, activities build on what was learned in phase 1. Steps include:

3. Fix IP license issues uncovered in the audit. This may mean swapping out components with licenses that don't meet the corporate IP license policy, substituting homegrown code or third-party components with friendlier licenses.
4. Typically, companies begin with development projects currently underway. But getting clean extends to older code in existing applications.
5. The Get Clean process involves a lot of back-and-forth discussion between the legal department and software development organizations. The most aggressive practitioners investigate how to make these regular communications "privileged" and covered by attorney-client privilege.

The third phase, Stay Clean, involves creating conditions and business processes so the effort to Get Clean isn't wasted. It institutionalizes "clean" practices. To Stay Clean, companies should:

6. Create a business process to monitor and vet new components as they are downloaded and before they are incorporated in applications.
7. Document and retain records for how new components are introduced.
8. Create a culture where compliance is routine. No more private caches of ever-ready but unapproved components.
9. Believe assurances, but verify them. The business process to vet new components should include review and oversight by managers or a compliance officer.
10. Stay current with the rapidly evolving world of open source. The environment changes daily with new components, new IP licenses, new industry initiatives.

In the ongoing Stay Clean phase, Best Practices go into a feedback loop. Auditing the code base reveals new IP license issues that a corporate IP policy must address. As new kinds of licenses emerge and new components are introduced, the corporate IP license policy must be adapted. Then the code base needs to be re-audited to comply with the revised IP policy.

How Palamida Helps

Palamida solutions help companies protect and regain control over their software intellectual property (IP) assets. The Palamida IP Amplifier can automate key parts of any Best Practices routine to prevent IP license violations. Best Practices also require a corporate IP policy on acceptable licenses for software components, business processes to implement that policy, and a corporate culture that encourages compliance.

Palamida's IP Amplifier automatically detects, assesses and reports on third-party components, both open source and commercial, and their associated IP licenses. IP Amplifier protects companies against unintentional violations of software licenses and unearths undesirable IP licenses already in their code base.

Used in conjunction with appropriate internal business processes, Palamida solutions map directly to industry Best Practices.

In the Get Set phase, companies can audit their applications with Palamida's software or have Palamida run an audit as a service. But each company must set its own corporate IP policy to complete this first phase.

In the second or Get Clean phase, companies apply their unique corporate IP license policy and Palamida's audit to identify and fix problems discovered in the audit.

Palamida's solution makes the Stay Clean phase much easier. Over the life cycle of an application Palamida solutions detect, assess and report on new components as they enter the development environment. Palamida solutions integrate easily with existing development and business processes. Palamida even detects when fragments of a third-party component have been improperly added to the code base.

As a company works on the "people issues" around business processes and company culture, Palamida automates the task of tracking new components and IP licenses. Through monthly updates of Compliance Library, Palamida helps companies stay abreast of the ever-changing world of open source.

Finally, Palamida solutions take the pain out of the continuing feedback loop of finding new licenses, evolving IP license policy and re-auditing the company's code base.

Key Product Modules for Palamida IP Amplifier	
Compliance Library	Holds billions of source code snippets for automated source code fingerprinting.
	Contains millions of source code files of commonly used open source components.
	Contains tens of thousands of the most commonly used components
	Catalogs in-house components.
	Requires less than 1 gigabyte of disk space.
	Lists license text, publisher and contact information for all major open source licenses.
	Allows companies to customize metadata information such as software patents, royalty obligations, etc.
	Uses patent-pending CodeRank™ to minimize time-consuming "false positives."
Detector Module	Analyzes binary code, source code, images, icons, archives, XML and text documents for licensing issues.
	Verifies whether source code is wholly or partially derived from third-party components using patent-pending CodeRank™ technology.
	Lets users share component, license and metadata information for a company-wide overview of IP assets and licensing obligations.

What Palamida Delivers

Palamida Capability	Customer Benefit
Audit code base to create baseline inventory of external components, licenses.	Keeps executives from "flying blind" about what's in their software code.
Establish a system to conduct ongoing IP audits as the code base evolves.	Relieves anxiety and liability by providing continued confidence of IP integrity.
Tracks home-grown and acquired components.	Simplifies monitoring by keeping all IP assets in a single tool.
Screen new external components and licenses before they enter the code base.	Creates "Just In Time Compliance" to assure that IP integrity and corporate reputations are not threatened.
Manage external components and licenses to comply with corporate IP license policy.	Generates tangible evidence that anti-fraud procedures are in place, relieving corporate officers from liability for inadequate controls.
Detect when portions of open source or commercial components have been improperly included in the code base.	Provides early warning of IP issues that could derail a critical development effort.
Conduct ongoing, automated compliance assessments.	Assures that the investment in achieving IP integrity is not squandered.

Summary

Today CEOs, CFOs and General Counsel face new legal requirements to verify that their internal controls are in place to prevent fraud. At the same time, software development practices are morphing rapidly. Old procedures and technologies are no longer adequate to verify with certainty that all components in applications carry appropriate licenses.

Palamida's solutions give senior executives the tools to say with confidence that they have adequately protected their companies (and themselves) against future claims of fraud or collusion over software IP licenses.

In short, Palamida smoothes the path to IP integrity, working alongside key internal business practices, to assure senior management they can answer the question, "Who Really Owns Your Software?"

About Palamida

Formed in early 2003, Palamida is an early mover in the software Intellectual Property risk management and compliance market. Our investors include Hummer Winblad, Walden VC and Stanford University. Our customers include Fortune 500, Independent Software Vendor and System Integration companies. Please contact us for more information at www.palamida.com.