26 No. 6 Intell. Prop. & Tech. L.J. 31

Intellectual Property & Technology Law Journal
June, 2014

A PRACTICAL APPROACH TO WORKING WITH OPEN SOURCE SOFTWARE

Gregory P. Silberman[a1]

Open source software (OSS) has become an integral part of the global economy. Engineers and business leaders appreciate the efficiency and cost savings of being able to build upon a developed body of source code that they can use, modify, and distribute on a royalty free basis. However, despite the perceived advantages, using open source software is not without risk. Understanding the legal issues associated with using and developing OSS is important for any company that depends upon software for its business. This article is intended to give a broad overview of the steps a company should take to avoid or mitigate the most common OSS risks and liabilities.

Open Source Software Licenses

While the OSS movement may embrace the idea of the free exchange of information, it is important to remember that OSS is not shareware or public-domain software and always is subject to the terms of a license agreement. The original OSS authors retain significant rights in the software, and its use and distribution is subject to the terms of the applicable OSS license. OSS licenses generally can be divided into "copyleft" and "permissive" licenses.

The most widely used OSS license, the GNU General Public License (GPL) and its progeny, are copyleft licenses. Copyleft licenses require licensees to distribute the software and any derivative works under the same terms with which the software was acquired. This usually means that a developer distributing software governed by a copyleft license will have to provide access to the source code and grant a royalty-free license to modify and redistribute the software. Copyleft licenses also may require a licensee to grant broad intellectual property rights to the licensee's own IP or prohibit a licensee from fully exercising its own IP. Copyleft licenses also may require a party that modifies the software to distribute source code for some or all of the modifications that the party makes to the software. These types of terms in copyleft licenses prevent modifications to OSS from being maintained as a trade secret.

A further example of the dramatic impact copyleft licenses can have on intellectual property rights can be seen in the GPL (v3), which provides that whenever a party conveys software covered by the GPL that they have written or modified, they must provide every recipient with all patent licenses necessary to exercise the rights that the GPL gives them. Beyond the GPL, an increasing number of OSS licenses include defensive termination provisions which provide that the license to distribute or even use the software may be terminated in the event the licensee asserts a claim for patent infringement. The scope and triggering mechanisms for such termination provisions vary widely amongst the licenses.

The Berkeley Software Distribution (BSD) License is an example of a permissive OSS license. Permissive licenses generally allow licensees to distribute derivative works as they see fit, without prescribing terms beyond the manner of copyright notice and author attributions. These types of licenses often are considered “safer” because they do not include terms that impact intellectual property rights in the same way as copyleft licenses.

Regardless of the style of license, working with OSS is distinctly different from working with proprietary software. Often OSS is difficult to identify and the circumstances under which it is licensed typically fall outside of most software procurement policies.

OSS can be difficult to identify because it is freely and widely available, and there is nothing ***32** particular about the way in which it is created or used that distinguishes it from proprietary software. Software engineers are sometimes tempted to take shortcuts by incorporating OSS source code into their projects. Other than copyright notices and references to license terms in the comments to the source code, it may be impossible to identify OSS once it is incorporated into a larger work. Moreover, there also is no guarantee that there will be any such notices to identify a particular piece of software as OSS. The authors of the code may not have included them or they have been removed by subsequent users.

As opposed to proprietary software, which is the subject of a negotiated license agreement or is purchased off the shelf subject to a shrink wrap license, most OSS licenses are neither purchased nor negotiated and do not require a signature to establish a contract. OSS licenses often rely upon the use and distribution of the software to establish legally binding obligations. The potential impact upon a company’s intellectual property rights combined with the fact that OSS licenses are entered into outside of most companies’ software procurement policies necessitates the need for a company to have an open source usage policy.

Policies, Procedures, and Guidelines

Every company that creates or uses software should have an open source usage policy. Having a written policy, including appropriate procedures and guidelines, is necessary to avoid the unintended consequences of incorporating OSS into a company’s products. Even if a company does not intend to use or create any OSS, it needs a policy to ensure that this corporate objective is achieved. The most important step in preparing a written policy is considering how the obligations of various OSS licenses may impact the business model and goals of a company.

A company that generates revenue from licensing proprietary software will need to address how the incorporation of OSS, which may require the distribution of source code developed by the company, would impact its current licensing structure. If software license fees are a significant source of revenue, a company most likely will want to have a policy that requires the careful scrutiny of each proposed instance of using OSS in the company’s products to ensure that revenue from licensing fees is not jeopardized. Conversely, a company that generates most of its revenue from the sales of hardware may not be as concerned with licensing obligations that require them to distribute source code. While a hardware manufacture may not be concerned about obligations to deliver source code to its customers, it may be very concerned about licensing provisions that require it to grant broad intellectual property licenses on a royalty-free basis upon distribution of source code.

How a company uses intellectual property should figure significantly in the development of its OSS usage policy. The most obvious impact on the intellectual property of a company is the requirement to grant a royalty-free copyright license. As opposed to most proprietary software licenses that only grant a use right to a specific end user, most open source licenses permit use, modification, and redistribution of the software. Additionally, companies should address the role patents play in their intellectual property strategy. A company that has a large patent portfolio will have to take into consideration the potential of OSS licenses to require or imply the grant of patent licenses. Even companies that do not use patents as part of their intellectual property strategy still need to consider the impact of having to grant such licenses. In addition to granting copyright and patent licenses, the decision to distribute software under a license that requires distribution of source code can directly impact a company’s trade secrets. Disclosing source code effectively destroys any trade secrets embodied in the source code. Therefore, a company must evaluate whether the disclosed source code contains any trade secret information.

In drafting an OSS policy, it is important to consider the scenarios a company may face. Will the company license software it creates under an open source license, and which license will it use? Are company employees allowed to participate in open source community projects outside of the workplace? Probably the most important scenario to consider is how the company will deal with developer requests to include OSS in company products.

As discussed, the decision to include OSS in company products will depend on the company's business and licensing models. Depending on the open source license, it might make a difference how ***33** the code is incorporated into the program. The complexity of open source licenses requires both legal and technical evaluations. Most usage policies should require approval for each specific instance open source code is incorporated into a company product. The approval process should be implemented through a set of procedures and guidelines that ensure that open source is used in a uniform fashion throughout an organization.

Considering the legal implications of the license governing a particular piece of OSS, a well-formed policy also should include guidelines addressing the provenance of open source code used by a company. Source code of questionable or unknown origin should be thoroughly scrutinized before being used to ensure that it does not violate any third-party intellectual property rights. If the author of a contribution made to an open source project included material that was rightfully the property of his employer, a company's use of the contributed source code could result in liability for copyright infringement.

In preparing an OSS policy, it is important to identify what open source licenses are involved and focus on the ones that are most likely to have a significant impact on the value of the subject company or asset. While broad distinctions can be drawn between copyleft and permissive licenses, the obligations imposed by individual licenses are meaningfully distinct and require close attention. A company's open source usage policy should constantly evolve to address the specific licenses that govern the OSS the company uses or creates.

Working with Open Source Software

The procedures established by an open source policy should include a mechanism for developers to request approval to incorporate OSS into a company product. Review of the approval request should be governed by written guidelines that reflect the company's business plan and detail acceptable and unacceptable requests. The procedures established for responding to requests for the incorporation of OSS into a product should be structured so as to promote making and responding to such requests as early in the development process as possible to avoid last minute delays. If the incorporation of OSS code into a company product is not discovered until just prior to release, it could delay shipment of the product or timely completion of a project. It is always easier to address questions regarding the use of OSS earlier in development than just before a product is slated to ship.

To the extent a company approves requests for the incorporation of OSS code into a product, that use needs to be carefully documented. At a minimum, the company needs to identify where and how the OSS code was used in the product and archive a copy of the code and associated license. It also is useful for the company to maintain a record of how the code was acquired and any modifications that were made to it. It is strongly recommended that the company develop a system that keeps track of all OSS in its products. Such a system will make it easier for the company to identify and meet the associated compliance obligations and to respond to a potential purchaser or licensee inquiries regarding the OSS license dependencies of the product.

A company may determine that its reliance on licensing revenue proscribes using any copyleft code, but that it is comfortable with the attribution requirements in permissive licenses. Alternatively, another company may determine that there are some circumstances in which incorporation of copyleft code is acceptable. Even when a company is accepting of the obligation to distribute source and grant broad licenses, there is still the matter of how to do so in an efficient manner. Procedures and guidelines should take into account the use and distribution obligations for the applicable OSS licenses.

A usage policy also should address internal use of OSS. There is a wide variety of OSS, including development tools, that employees may want to use in developing a company's products. Many of these tools are used only in the development process and do not incorporate any OSS into the software being developed by the employees. A policy can either allow tools to be used without limitation as long as no OSS is incorporated into any products or provide a list of approved tools that have been reviewed and determined not to cause OSS code to be incorporated into software developed with the tools.

Education and Training

Developing open source policies, procedures, and guidelines is a beginning, not an end. Once ***34** the policy is in place, it is essential to educate the company's employees about the issues and procedures related to OSS. Training programs should be tailored to specific groups within the company. The OSS training provided to developers and engineers will be different from the program provided to members of the business team, which will be different from the training provided to the legal department. Each group has different technical backgrounds and will benefit from a training program tailored to their role within the company. Training programs should be presented in a manner to encourage a partnership between software development and legal departments.

Due Diligence

While many companies recognize the importance of addressing the legal issues surrounding the use of OSS in their own products, many of these same companies overlook the potential risks and liabilities posed by OSS they acquire from others. A company's open source usage policy needs to address not only the internal use of OSS but code that is acquired from third parties. These third-party sources of software include software licensors (including hardware manufactures that have OSS embedded in the products), outsourced software development teams and software acquired through business acquisitions. Although many OSS related risks and liabilities acquired from third parties can be addressed through warranties and indemnifications, those posed by property acquired through business acquisitions may be more difficult to address depending on the size and scale of the transaction.

The best tool for evaluating the risks and liabilities posed by OSS in a corporate transaction is the due diligence process. To make the most of this process, the party conducting due diligence needs to be very specific with its questions and must ensure that the person responding to the questions verify the answers with the developers and engineers rather than merely accepting generalized statements from personnel that might not have the actual information. The best source of information about a company's use of OSS will come from the policies and documentation it has in place to govern the usage of OSS. These can be cross-checked by in-depth scans of the target company's code base for use of OSS. Such scans often are performed by specialized third-party consulting firms as part of the technical due diligence process.

If there is no policy in place, there is a good chance that the company, at least at the management level is going to be uncertain as to what OSS may be present in their products. If the company has a thorough, well-defined policy and has followed its own policies and procedures, then it is likely that the potential risks associated with using OSS will be mitigated. The thoroughness of the policies and procedures and the degree to which they have been complied with will provide a strong indicator of the potential risks and liabilities created by the target company's use of OSS.

Representations, warranties and indemnification clauses in acquisition transactions should be tailored to take into account any potential risk identified by the due diligence. In the event of significant risk, the results of a due diligence investigation may be useful to craft-specific remediation covenants or indemnities or even to adjust the price of the transaction.

Auditing Open Source Usage

While having a policy and educating employees about legal and technical issues related to the use of OSS is important, auditing form compliance is necessary in order to ensure that the policy is appropriate and effective. The three main areas of audit with relation to OSS are compliance with company polices, compliance with OSS licensing terms, and the technical review of products prior to shipping.

Auditing for compliance with corporate policies ensures that the procedures the company has established are actually being followed and determines whether or not they are effective. If procedures are not effective, it is necessary to determine whether it is a problem with the procedures, including the methods used to educate employees about the procedures, that are the problem. It is important to determine whether the failure is with the procedure or the employees. If it is the procedure that is the problem, then the procedure needs to be fixed. If the problem is with the employee failing to follow the procedure, then the matter should be dealt with in the same manner as an employee that fails to follow other important corporate policies.

***35** Auditing for product compliance with OSS licensing requirements should be a straightforward matter if all of the OSS dependencies for the product have been documented. If a product is out of compliance, the first step is to remedy the noncompliance. The second step is to determine how noncompliance occurred. The final step is to prevent future noncompliance through changes to the company's OSS usage policy and/or employee education.

Conducting a technical audit should be simple if a company has clearly documented all uses of OSS in the product. This technical audit should also include a review of how the company will comply with the applicable OSS licensing obligations, such as attribution and source code distribution. In addition to reviewing the written documentation, a meeting with members of the development team to confirm that the company's OSS usage policy can provide additional assurance that the company's policies have been followed. Finally, a company may want to use some form of automated tool to scan the product's source code prior to release. There are a variety of tools that perform this task ranging in sophistication from simple text parsing applications, which search file headers and comments for copyright notices and license names, to more sophisticated tools that perform comparisons between the product software and well-known OSS code bases.

Conclusion

Having a comprehensive OSS usage policy is the key to successfully working with OSS. If the procedures and guidelines for implementing the policy reflect the company's business model and tolerance for risk, the company should be able to take advantage of the benefits of OSS in a rational, efficient manner. Creating and implementing such a policy is no small task; however, the value addressing the risks and liabilities attendant with the use of OSS in advance of any problems is worth the effort.

Footnotes

[a1] **Gregory P. Silberman** is a partner in Jones Day's Licensing & Technology Transactions and Privacy & Data Security practice groups, where his practice emphasizes the representation of high technology companies in the legal and business issues related to technology development, licensing, distribution, and transfer. He may be contacted at *gpsilberman@jonesday.com.*

26 No. 6 IPTLJ 31

End of Document

Wolters Kluwer
Law & Business
Aspen Publishers