SheppardMullin

Open Source Software Policies – Why You Need Them And What They Should Include

June 2019

By: James G. Gatto

The chances are high that your company uses open source software ("OSS") in some capacity. While the benefits of OSS are clear, it is also clear that OSS can pose significant legal risks that must be addressed. The best way to manage these risks is to have a clearly written and enforced OSS policy.

In general terms, OSS refers to software that is licensed under an OSS license. OSS refers to a type of license. It is not a type of software. The same software can be distributed under different licenses, at the election of the initial developer.

Many different types of OSS licenses exist. However, there are common attributes among most OSS licenses. Two of the main common attributes are that: (1) recipients can freely use, modify and distribute the software; and (2) the source code (i.e. the human readable code) is made available to enable the exercise of these rights. This distinguishes OSS from proprietary software. With proprietary software licenses, typically copying, modifying or redistributing is prohibited and only the object code (i.e., the machine readable code or "compiled form") is distributed. The significance of this is that to effectively modify the software, a developer typically would need access to the source code.

To understand why these policies are necessary, it is first necessary to understand the risks of not having one. The following are *some* of the key issues to understand.

Why OSS Policies are a Must To Avoid Legal Risk

Tainting

Perhaps the biggest risk in using OSS is that it may impact proprietary software, including the potential requirement to make the source code for that software available to others. This is often referred to as OSS "tainting" of proprietary software. Some OSS licenses (e.g., the GPL license) require that if any software contains or is derived from any GPL-licensed code, then that software must be licensed under the terms of the GPL license. Two significant ramifications of this are that: i) the source code for that software must be made available to recipients of the software; and ii) recipients must have the right to copy, modify and redistribute that software at no charge. This can be devastating if that software is intended to be proprietary software.

This risk is not theoretical. A number of OSS enforcements have been successful. There is a growing trend in the enforcement of OSS license compliance. The trend is a movement from enforcement by OSS advocacy groups (such as the Free Software Foundation or the Software Freedom Law Center) to enforcement by commercial entities against other companies, such as a decision we reported in *Artifex Software, Inc. v. Hancom, Inc*.

OSS Concerns with SaaS

Under the GPL licenses, and many other OSS licenses, obligations that can result in tainting are triggered when software that contains or is derived from the GPL code is *distributed*. However, a growing number of OSS licenses (e.g., the Affero GPL license) include obligations that are triggered when such software is accessed by a third party over a network. For these "network access" licenses, obligations may be triggered by running OSS in a cloud or SaaS deployment, even if such OSS is not actually distributed. Due to the fact that with most cloud-based deployments the software is not distributed, many developers are lulled into a false sense of security that there are no OSS implications with such deployments. The reality is there are a growing number of OSS licenses that have significant legal implications, even when the OSS is not distributed, but accessed over a network. For more information on these issues, see Not Every OSS Cloud Has A Silver Lining.

New Use Cases

The legal ramifications of using OSS under any particular license depends on the use case. Typically, running OSS internally within an organization, without distribution or third party access, imposes few if any legal obligations. Often, these uses are routinely approved by OSS policies. However, it is important to recognize that future business plans may change this use. For instance, the OSS may later be packaged and distributed (e.g., white-labelled) or the OSS may be used to run an online service for third parties. A change in use case may trigger different legal obligations depending on the terms of the relevant OSS license. These future uses may cause problems if the OSS legal issues are not analyzed as this shift in business strategy occurs. If there is no policy in place to revisit the suitability of OSS as use cases change, unintended consequences can result.

Patent Issues With Open Source Licenses

Significant patent issues can arise with OSS licenses. Many OSS licenses include patent express patent license grants and some arguably trigger an implied license. Certain OSS licenses require that you grant others a patent license relating to the use of certain OSS Components, any modifications you make and/or software in which the OSS components are included. In some cases, the license extends only to the OSS Component and/or modifications. In other cases, it can extend more broadly to software that includes the OSS component. Some patent license grants cover existing patents, but some also cover future acquired patents.

Certain OSS licenses seek to deter a licensee from asserting certain patent infringement claims relating to the use of the OSS components by terminating the licensee's rights to use the OSS if it makes such an assertion. These provisions are often referred to as patent retaliation clauses. The scope of the patent retaliation provisions varies among OSS licenses. Many companies are surprised at the scope of these patent provisions, which in some cases can be quite broad. Depending on the OSS license, these patent deterrent provisions can arise when you use OSS, release software under an OSS license, you contribute code to an OSS project or based on other conditions. Historically, OSS was not involved in patent infringement litigation as much as commercial software. This is changing. For all of these reasons, the interplay between OSS and patents has become more complex.

Assumption of Legal Obligations

Usually, OSS is provided as-is and with disclaimers of warranties, indemnities, or other liabilities. However, certain OSS licenses require that if recipients make a commercial distribution of software including OSS Components, the recipients may assume certain legal obligations such as indemnifying upstream developers for certain legal claims. One example is the Eclipse Public License v 1.0 which states in part:

> While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering.

Compliance Obligations

Certain OSS licenses require compliance with various obligations, including the obligations to keep the license information and copyright notices intact, provide attribution notices that identify the copyright holder, identify modifications you make to the software, refrain from using the developer's name to promote your software, in some cases to make source code available and/or other obligations. It is important to comply with these obligations. The primary basis for OSS license enforcement actions is lack of compliance with license obligations.

Dual Licenses

A growing number of OSS is distributed under a dual (or multi) license scenario. Sometimes the licenses are two different OSS licenses. Sometimes, there is one or more OSS license and a commercial license. In some instances, a downstream user is able to freely select between two (or more) licenses. In other cases, a choice has been made that is binding on the recipient. For example, in some cases, if you use the OSS with other OSS, you can use an OSS license. But if you desire to use the OSS with commercial software, you need to obtain a commercial license.

Contributing Back to the Community

The OSS model is a community-based model. Many developers that use OSS also want to contribute back to the community. This can be beneficial, but can create legal issues in some situations. First, it is important to understand that there are different scenarios under which an entity can contribute OSS, including:

a. **Company Managed OSS Project** - Company develops software, releases it under an OS license and runs a managed project for the software (with contributions from others);
b. **Company Distributes Under OSS License** - Company develops software, releases it under an OSS license for others to use and modify, with no continuing commitment by company to manage a project around the OSS;
c. **Company Modifies Existing OSS** - Company modifies/enhances an existing OSS application and releases a modified version under OS license (this could include a fork of an existing OS application or making bug fixes/patches);
d. **Company Contribution to Managed Project** - Company contributes to an existing OSS managed project, which may have a Contributors License Agreement (CLA)
e. **Personal Contribution** - Company employee wishes to contribute OS personally

The legal (and business) considerations for contributing OSS differ under these different scenarios.

For these and other reasons, knowing, approving and managing the OSS your company uses, modifies, contributes, and/or distributes is critical. To do this, your company must have an OSS policy.

What an OSS Policy Should Provide

The considerations for an OSS policy will vary by company and in some cases by business group within a company. The following is a general guideline of some of the common elements of an OSS policy (primarily from a legal perspective). It is not necessarily comprehensive. Other business and technical issues need to be considered as well. For example, an OSS policy may address the following:

1. **Identify and Educate Stakeholders** – crafting a good OSS policy starts with identifying the key stakeholders (business, legal, technical, etc.) and educating them on the opportunities and risks with OSS. It is often critical to get high-level buy in to have an effective policy that is actually implemented. It is also important, as much as possible, to integrate the policy into existing work flow. This can vary widely by company and/or business unit.

2. **Identify OSS Business Objectives** – companies must identify the key business and legal objectives that will drive the OSS policy. The issues may vary widely by company. Some of the potential legal objectives may include:
   a. Avoiding an obligation to release proprietary source code in connection with OSS
   b. Avoiding the need to grant patent licenses (for some businesses that are not patent centric, this may not be as important).
   c. Maintaining the ability to enforce patents without loss of OSS licenses
   d. Avoiding unacceptable legal obligations/liabilities (e.g. providing indemnities)
   e. Minimizing OSS compliance obligations and/or ensuring compliance when applicable.
   f. Minimizing risks when contributing OSS under different scenarios
   g. Reassessing the legal risks with certain OSS as business use cases change.
3. **Approval Process** – The policy should provide an approval process for all OSS that is used, distributed and/or contributed. This can range from pre-approval of some licenses[1] and/or some use cases (e.g., where OSS is used internally only or is a standalone tool) to submitting a request for approval to the legal department on a case-by-case basis. This is one of the toughest choices and requires a balance between efficiency and legal certainty.
4. **Identification of OSS and Its Use** - The policy should require identification of all OSS that is used, modified, contributed, or distributed by your company and the relevant license that governs use of that OSS component. It should also require identification of how the OSS is used. The OSS legal risks vary greatly depending on how a company uses OSS (e.g. internal use, SaaS deployments, external distribution and whether the OSS is standalone, linked to proprietary software or compiled with proprietary software) and the particular licenses. Any change in use case should trigger a new review.
5. **Patent Considerations** – Depending on whether your company owns patents related to what the OSS is used for, you may need to deal with certain OSS licenses differently than if you do not. It is important to understand the scope of the patent license provisions in the relevant OSS licenses and ensure that your company's use, distribution or contribution of OSS does not inadvertently grant undesired patent licenses.
6. **Compliance** – For approved OSS, it is necessary to ensure compliance with the OSS license terms. Developing an efficient process for doing so is important.
7. **Third Party Dealings** – The policy should also address ensuring OSS issues are adequately addressed in third party contracts, development agreements, distribution agreements, acquisitions and other transactions. At a minimum, you want to be informed of any potential OSS to be used (and the relevant license) and have the right to approve or reject such use.
8. **Contributions of OSS** – The policy should address business considerations and procedures for approval of releasing company developed software under an OSS license and creating or contributing to managed OSS projects. It is important to establish criteria for selection of an appropriate OSS license under which to do so and to understand any obligations on licenses impose on your contributions. Some OSS projects have a contribution license agreement. If so, this needs to be reviewed and approved. The approval process for contributions may also vary depending on the relative value of the contribution (bug fixes vs. important new functionality).
9. **Efficiency Considerations** – Where feasible it is best to integrate the OSS policy processes into existing workflow. Each company has different existing processes for workflow and product approvals. It is efficient to develop OSS policies that fit within the existing workflows to the maximum extent possible.

[1] For example, some permissive licenses such as the BSD and MIT licenses are often approved for all use cases.

10. **Code Scan Policy** – the policy should address whether and when to conduct code scans to ensure identification of all OSS components used in a company's software product and their respective licenses.
11. **Written Policy and Education** – once the policy is developed, it must be reduced to writing, disseminated to employees and enforced. It is also highly advisable to conduct training for the relevant employees so they understand the policy and the reasons for it, as well as the risks associated with non-compliance.

For more information on these issues or to schedule a customized presentation for your company please contact us.

For further details, please contact:

James G. Gatto
Open Source Team Leader
202.747.1945
jgatto@sheppardmullin.com

Sheppard Mullin has a robust Open Source Team that advises clients on the full range of open source legal issues, including developing open source policies, advising on the approval and use of open source; M&A and finance transactions open source diligence, remediation and contractual provisions; patent issues with open source; distribution of software under open source licenses; contributions to open source projects and much more.