



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

The chances are high that your company uses open source in some capacity. While the benefits of open source are clear, it is also clear that open source can pose significant legal risks that must be addressed. The best way to manage these risks is to have a clearly written and enforced open source policy. To understand why these policies are necessary, it is first necessary to understand the risks.

Why Open Source Policies are a Must To Avoid Risk

Tainting

Perhaps the biggest risk in using open source software (“OSS”) is that it may impact proprietary software, including the potential requirement to make the source code for that available to others. This is often referred to as open source “tainting” of proprietary software.

Some open source 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 of the significant ramifications of this are that: 1. the source code for that software must be made available to recipients of the software; and 2. 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 open source enforcements have been successful. There is a growing trend in the enforcement of open source license compliance. The trend is a movement from enforcement by open source advocacy groups (such as the [Free Software Foundation](#) or the [Software Freedom Law Center](#)) to enforcement by commercial litigation, such as a decision we recently [reported](#) in *Artifex Software, Inc. v. Hancom, Inc.*

Patent Rights

Many open source licenses also include patent grant and patent “non-assertion” provisions. Many companies are surprised at the scope of these patent provisions, which in some cases can be quite broad. Several recent patent litigations have evolved into open source issues. These issues can arise when you use OSS, release software under an open source license or you contribute code to an open source project.

Open Source Concerns with SaaS

Although most open source license obligations trigger when OSS is distributed, a growing number of open source licenses (e.g., the Affero GPL license) include provisions that trigger when the output of software is provided to a third party over a network. For these types of licenses, obligations may trigger by merely running OSS, such as in a SaaS deployment, even if such OSS is not actually distributed.

New Business Case

Even when software is planned to be used internally only (e.g., not distributed and not used in a SaaS deployment), future business plans may change. For instance, the business may decide to commercialize the software or a separate business around the software may be spun off. These future uses may cause problems if the open source legal issues are not analyzed as this shift in business strategy occurs.

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

Sheppard Mullin's open source team has helped numerous organizations to set up and implement these programs and routinely delivers on site presentations to educate employees on these issues and the policies.

What an Open Source Policy Should Provide

An open source policy should provide requirements/guidance on the approved uses of OSS for your company. For example, an open source policy should address the following:

1. Identify and Educate Stakeholders – crafting a good open source policy starts with identifying the key stakeholders (business, legal, technical, etc.) and educating them on the opportunities and risks with open source. We often provide different open source presentations to C-level personnel, legal and technical.
2. Identify Open Source Business Objectives – companies must identify the key business and legal objectives that will drive the open source policy. The business issues will 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
 - c. Maintaining the ability to enforce patents without loss of open source licenses
 - d. Avoiding unacceptable legal obligations/liabilities (e.g. providing indemnities)
 - e. Minimizing risks associated with OSS compliance obligations
 - f. Minimizing risks when contributing to open source projects
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 licenses¹ 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.
 - a. 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 open source legal risks vary greatly depending on how a company uses open source (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.

¹ Identify potential open source licenses to consider – hundreds of OSS license versions exist. Often a company will identify the licenses most frequently used by its developers to create a manageable universe of licenses to address for preapproval.

4. 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 open source licenses and ensure that your company's use or distribution of open source does not inadvertently grant undesired patent licenses. Some patent license grants cover existing patents, but some also cover future acquired patents. Some grant a license to what you contribute. Some are broader and cover recipients derivative works as well.
5. Compliance – For approved OSS, it is still necessary to ensure compliance with the open source license terms. Developing an efficient process for doing so is important.
6. Third Party Dealings – The policy should also address ensuring open source issues are adequately addressed in third party contracts, development agreements, distribution agreements, acquisitions and other transactions
7. Open Source Licensing – The policy should address procedures for approval of releasing company software under an open source license and criteria for license selection.
8. Contributions to Open Source Projects – The policy should address considerations for contributing software to open source projects and an approval process depending on the relevant license and the value of the contribution (bug fixes vs. important new functionality).
9. Efficiency Considerations – Where feasible it is best to integrate the open source policy processes into existing workflow. Each company has different existing processes for workflow and product approvals. It is efficient to develop open source policies that fit within the existing workflows to the maximum extent possible.
10. Code scan policy – the policy should address whether and when to conduct code scans to ensure identification of all open source components used in a software product.
11. Written Policy and Education – once the policy is developed it must be reduced to writing and disseminated. 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.

The foregoing is not necessarily a comprehensive list, but includes common elements of many companies' open source policies. Each company (and sometimes different business units within a company) must customize a policy based on their unique business issues and existing workflows.

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

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.

Authors



James Gatto

Open Source Team Leader
202-747-1945
jgatto@sheppardmullin.com



Hean Koo

Open Source Team Lead Associate
202-747-2647
hkoo@sheppardmullin.com